jc658 U.S. PTO
03/19/03

10390807 .031903

PATENTS

j1032 U.S. PTO
10/390807
03/19/03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Ron M. Redlich, et al.

Serial No.:

Filed: Herewith

For: Data Security System and Method for Portable Device

TRANSMITTAL AND CERTIFICATE OF EXPRESS MAILING

BOX PATENT APPLICATION
Commissioner for Patents
Washington, D.C. 20231

Sir:

I HEREBY CERTIFY that the below listed documents are being ~~deposited with the United States Postal Service "Express Mail Post Office to Address," Mailing Label No. EL220374395US, under 37 C.F.R. 1.10~~ mailed via Fed Express, next day delivery on March 17, 2003 and are addressed to Box Patent Application, Commissioner for Patents, Washington, D.C. 20231.

X Patent application (137 pgs.; 146 clms.)

X Twenty (20) sheets drawings -(18 formal; 2 informal)

X Declaration and Power of Attorney for Patent Application (2 pgs.)

X Assignment to Digital Doors, Inc. w/assignment cover sheet (5 pages)

X IDS and Form PTO-1449 (7 pgs.) with thirty-six (36) references

X Please charge Deposit Account No. 03-1231 in the amount of $1,759.00

X Fee calculation letter (1pg.) (duplicate)

X Return receipt postcard.

X Please charge any underpayments or credit any overpayments to Deposit Account No. 03-1231. A duplicate copy of this transmittal is enclosed.

Respectfully submitted,

By_____
Ellen Kotler

By_____
Robert C. Kain, Jr.
Reg. No. 30,648
FLEIT, KAIN, GIBBONS, GUTMAN & BONGINI, P.L.
750 S.E. Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Facsimile: (954) 768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-2-cip-5 express maill transmittal to pto.wpd

IPR2023-00967
International Business Machines Corporation v. Digital Doors, Inc.
IBM's Exhibit 1002
Ex. 1002, Page 1

FLEIT, KAIN, GIBBONS, GUTMAN & BONGINI P.L.
ATTORNEYS AT LAW
Miami • Fort Lauderdale • Boca Raton

750 Southeast Third Avenue
Suite 100
Fort Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Toll Free: (800) 846-0900
Facsimile: (954) 768-0158
www.FocusOnIP.com
Robert C. Kain, Jr. rkain@FocusOnIP.com
William R. Trueba, Jr. wtrueba@FocusOnIP.com

March 17, 2003

Commissioner for Patents
Washington, D.C. 20231

Transmitted herewith for filing are papers related to the patent application of:

Inventor(s): Ron M. Redlich and Martin A. Nemzow
For: Data Security System and Method for Portable Device
Our Ref: 6851-2-cip-5

The filing fee for the enclosed patent application has been calculated as shown below:

			Small Entity		Other than Small Entity	
	No. Filed	No. Extra	Rate	Fee	Rate	Fee
Basic Fee				$375		$750
Total Claims	146- 20 =	126	x 9 =	$1134	x 18 =	$
Ind. Claims	08- 03 =	05	x 42 =	$ 210	x 84 =	$
____Multiple claims presented			x140 =	$	x 280 =	$
			Total	$1719	Total	$

Please charge Deposit Account No. 03-1231 in the amount of $,1759.00 to cover the filing fee (plus applicable Assignment recording fee). Please charge any additional filing fees required under 37 CFR 1.16 to Deposit Account No. 03-1231. A duplicate copy of this letter is enclosed.

Small Entity under 37 C.F.R. §1.27. YES __X____ NO _____

Respectfully submitted,

Fleit, Kain, Gibbons, Gutman & Bongini, P.L.

By _____
Robert C. Kain, Jr.
Reg. No. 30,648

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-2-cip-5 fee calculation for pto.wpd

DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE

[001] This is a continuation-in-part of patent application no. 10/277,196 filed on January 2, 2003 and patent application no. 10/115,192 filed on May 23, 2002 and 10/155,525 filed on May 23, 2002, and is a regular patent application claiming the benefit of provisional patent applications 60/400,062 filed on August 2, 2002, 60/400,112 filed on August 2, 2002, 60/400,406 filed on August 2, 2002, and 60/400,407 filed on August 2, 2002, and is a continuation-in-part of patent application no. 10/008,209 filed on December 6, 2001 and 10/008,218 filed on December 6, 2001, and is a continuation-in-part of patent application no. 09/916,397 filed July 27, 2001 which is a regular patent application is based upon provisional patent application no. 60/260,398, filed June 5, 2001; application no. 60/287,813, filed on May, 2, 2001; application no. 60/267,944, filed February 12, 2001; application no. 60/247,242, filed November 13, 2000 and application no. 60/247,232, filed November 13, 2000.

[002] The present invention relates to a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects in portable computing devices. The invention extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data. Scrubbing security icons from maps, credit card data or financial data from text, a data object or data stream is also discussed herein.

Background of the Invention

[003] The extensive use of computers and the continued expansion of telecommunications networks, particularly the Internet, enable businesses, governments and individuals to create documents (whether text, images, data streams or a combination thereof, sometimes identified as

[redacted]

"data objects") and distribute those documents widely to others. Although the production, distribution and publication of documents is generally beneficial to society, there is a need to limit the distribution and publication of security sensitive words, characters or icons. Concerns regarding the privacy of certain data (for example, an individual's social security number, credit history, medical history, business trade secrets and financial data) is an important issue in society. In another words, individuals and businesses have a greater concern regarding maintaining the secrecy of certain information in view of the increasing ease of distribution of documents through computer networks and the Internet.

[004] U.S. Patent No. 6,055,544 to DeRose et al. discloses the generation of chunks of a long document for an electronic book system. DeRose '544 discloses solutions available to book publishers to publish books in electronic format on the worldwide web. One of the problems is that the books are published as small document fragments rather than publishing an entire book which, due to the formatting, protocol and command structure on the Internet, downloads an entire book to the user. The problem involved with publishing small documents is that there is no relationship to other portions of the book. See col. 3, lines 51-55 and col. 4, lines 3-5. One methodology to solve the problem involves inserting hypertext links in the book. This places a large burden on the book publisher. Col. 4, lines 19-21. Accordingly, it is an object of DeRose '544 to provide a mechanism for accessing only a portion of a large, electronically published document and automatically determining what portion of the document to download to the user based upon user selections that is, previous portions and subsequent portions of the document are downloaded with the selected portion, without maintaining separate data files for each portion of the document. Col. 4, lines 34-39. In other words, if a person wanted to access chapter 4 of a text, the system in DeRose '544

[redacted]

would display chapter 4, chapter 3 (the preceding chapter) and chapter 5 (the subsequent chapter). This publishing of portions of the document utilizes a subset of marked up elements established as being significant and a second subset of elements being less significant. For example, "Title elements" define a table of contents. A first representation of the document structure defined by all of the marked up elements may be used in combination with a second representation of the document structure defined only by the significant elements to control selection of portions of the documents such that previous and subsequent portions may be selected and rendered in a consistent and intuitive manner." Col. 4, lines 38-55. A computer system stores a first representation of the hierarchy of all elements in the electronic document. As example, this may be each chapter in its entirety. The computer also stores a second representation of the hierarchy of only significant elements in the electronic document. As an example, this may be a listing of each chapter without the text associated with the chapter. In response to request for a portion of the document, the computer system selects the portion defined by the significant element in the second representation. For example, if the user requested chapter 4, the entirety of chapter 4 would be downloaded from the web server to the client computer. In addition to rendering or publishing the selected chapter, the computer system looks to the relationship of the elements in the first representation of the hierarchy (the list of all chapters) and downloads from the web server the adjacent chapters. In this example, this would involve downloading chapters 3 and chapter 5. In a further embodiment, the computer system selects only a leaf element of the second representation as a significant element during the download. See the Summary of the Invention, col. 4, line 40 through col. 6, line 14.

[005] U.S. Patent No. 5,832,212 to Cragun et al. discloses a censoring browser method for viewing downloaded and downloading Internet documents. The abstract describes the system as

including a user profile including user selected censoring parameters. Data packet contents are received from the Internet and the packets are compared with the user selected censoring parameters. Responsive to the comparison, the received data packet contents are processed and selectively displayed. The user selected censoring parameters include censored words and word fragments, and user selected categories. Compared word and word fragments can be removed and selectively replaced with predefined characters or acceptable substitute words. Tallies of weights for user selected categories are accumulated and compared with used selected threshold values. A predefined message can be displayed responsive to an accumulated tally exceeding a user selected threshold value without displaying the received data packet contents.

[006] U.S. Patent No. 6,094,483 to Fridrich discloses an encryption methodology hiding data and messages in images. In one application of the system in Fridrich '483, a method is disclosed of embedding a secret digital square image with 256 gray levels within an image carrier. The secret image is first encrypted using a chaotic Baker map. The resulting image is a random collection of pixels with randomly distributed gray levels without any spatial correlations. The carrier image is twice the size (height and width or 2nX2m) the secret image with 256 gray levels. The carrier image is modified according to a mathematical formula.

[007] U.S. Patent No. 5,485,474 to Rabin discloses a scheme for information dispersal and reconstruction. Information to be transmitted or stored is represented as N elements of a field or a computational structure. These N characters of information are grouped into a set of n pieces, each containing m characters. col. 1, lines 37-46. The system is used for fault tolerance storage in a partitioned or distributed memory system. Information is disbursed into n pieces so that any m pieces suffice for reconstruction. The pieces are stored in different parts of the memory storage

[redacted]

medium. A fairly complex mathematical algorithm is utilized to provide reconstruction of the information utilizing no fewer than m pieces.

[008] U.S. Patent No. 6,192,472 B1 to Garay et al. discloses a method and apparatus for the secure distributed storage and retrieval of information. Garay '472 identifies the problem as how to store information in view of random hardware or telecommunications failures. Col. 1, lines 17-20. The initial solution is to replicate the stored data in multiple locations. Col. 1, lines 28-31. Another solution is to disburse the information utilizing in Information Disbursal Algorithm (IDA). The basic approach taking in IDA is to distribute the information F being stored among n active processors in such a way that the retrieval of F is possible even in the presence of up to t failed (inactive) processors. Col. 1, lines 40-44. Another issue is the utilization of cryptographic tools. With the use of tools called distributed fingerprints (hashes), the stored data is distributed using the fingerprints and coding functions to determine errors. In this way, the correct processors are able to reconstruct the fingerprint using the code's decoding function, check whether the pieces of the file F were correctly returned, and finally reconstruct F from the correct pieces using the IDA algorithm. Col. 2, lines 50-59. Garay '472 also discloses the use of Secure Storage and Retrieval of Information (SSRI) with the added requirement of confidentiality of information. Col. 3, line 56. With this added requirement, any collision of up to t processors (except ones including the rightful owner of the information) should not be able to learn anything about the information. Confidentiality of information is easily achieved by encryption. Col. 3, lines 56-61. The issue involves encryption key management, that is, the safe deposit of cryptographic keys. Garay '472 discloses confidentiality protocol utilizing distributed key management features. This mechanism allows the user to keep his or her decryption key shared among several n servers in such a way that when the user wants to

[redacted]

decrypt a given encrypted text, the user would have to interact with a single server (the gateway) to obtain the matching plaintext while none of the servers (including the gateway) gets any information about the plaintext. Col. 4, lines 5-14.

[009] U.S. Patent No. 5,996,011 to Humes discloses a system and a method for filtering data received over the Internet by a client computer. The system restricts access to objectionable or target data received by a client computer over an Internet by a web server by filtering objectionable data from the data received. The Humes '011 system filters the data "on the fly." Further, the Humes '011 system can be applied to process any type of target data from the data received and displayed to the user. Col. 2, lines 32-44. If the web page requested by the user contains only a minimum amount of objectionable or target data, the user receives only a portion of the filtered web page for viewing. Hume '011 also provides that if the web page contains a large amount of objectionable material, the system blocks the entire display of the web page on the user's computer monitor. Col. 2, lines 56-62. Hume '011 provides three levels of filtering. At the first level, if the domain name contains objectionable words or material, the initial download from the domain is blocked. At the second level, the text in the download is filtered and objectionable words are replaced with a predetermined icon, for example, "----". Col. 3, lines 32-35. The filter uses a dictionary. Col. 3, lines 45-48. The filtered out words are counted. If the final score of "filtered out" material exceeds a predetermined threshold, the entire page is blocked from the user's view. Col. 4, lines 2-4.

[010] U.S. Patent No. 5,905,980 to Masuichi, et al., discloses a document processing apparatus for processing various types of documents, a word extracting apparatus for extracting a word from a text item including plural words, a word extracting method used in the document

[redacted]

processing apparatus, and a storage medium for storing a word extracting program. Extracted words are associated with other words via an algorithm. The extracted words and associated words are used as a search index for the document.

[011] U.S. Patent No. 5,996,011 to Humes discloses a computer based system and method for filtering data received by a computer system, and in particular, for filtering text data from World Wide Web pages received by a computer connected to the Internet, for purposes of restricting access to objectionable web sites.

[012] U.S. Patent No. 6,148,342 to Ho discloses a system for managing sensitive data. The system prevents a system administrator from accessing sensitive data by storing data and identifier information on different computer systems. Each query from a user's terminal is encrypted using two codes, the first code readable only by an identifier database and a second code readable only by a data access database. The data is routed from the user's source terminal to the identifier database at the first computer. The first computer/identifier database first verifies the user's ID and the security clearance for the requested information and substitutes a second internal ID to the data packet/query. The modified query is then presented to the data access database (the second computer) and, subject to a second security clearance, the response to the data query is sent back to the user's source terminal.

[013] A publication entitled "Element-Wise XML Encryption" by H. Maruyama T. Imamura, published by IBM Research, Tokyo Research Laboratory, April 20, 2000 discloses a protocol or process wherein certain parts of an XML document are encrypted and the balance of the plaintext is not encrypted. The protocol is useful in three party transactions, for example, when a buyer sends an order in an XML document to a merchant which contains the buyer's credit card

[redacted]

information. The credit card information is sent to a credit company and the merchant does not need to know the credit number as long as he obtains clearance or authorization from the credit card company. Another instance is an access control policy which requires a certain part of an XML document to be readable only by a privileged user (for example, a manager could access the salary field in an employee records but others could only access name, phone and office fields). The Imamura article discusses encryption protocol, the delivery of keys and the utilization of compression. The article does not discuss separate storage of the critical data apart from the plaintext of the XML document.

[014] The Ingrain i100 Content Security Appliance product brochure, available in June, 2001, discloses a system coupled to multiple web servers (computers) to accelerate secured transactions between multiple client computers (over the Internet) and prevents Secure Sockets Layer SSL performance bottlenecks by performing high-performance SSL handshakes and encrypting all data sent to back end servers using long-lived SSL session.

[015] An article entitled "Survivable Information Storage Systems" by J. Wylie M. Bigrigg, J. Strunk, G. Ganger, H. Kiliccote, and P. Khosla, published August, 2000 in COMPUTER, pp. 61-67, discloses a PASIS architecture which combines decentralized storage system technologies, data redundancy and encoding and dynamic self-maintenance to create survivable information storage. The Bigrigg article states that to achieve survivability, storage systems must be decentralized and must spread information among independent storage nodes. The decentralized storage systems partition information among nodes using data distribution and redundancy schemes commonly associated with disc array system such as RAID (redundancy array of independent discs) insuring scalable performance for tolerance. P. 61. Thresholding schemes - also known as secret sharing

schemes or information disbursal protocols - offer an alternative to these approaches which provide both information confidentiality and availability. These schemes and codes, replicate, and divide information to multiple pieces or shares that can be stored at different storage nodes. The system can only reconstruct the information when enough shares are available. P. 62. The PASIS architecture combines decentralized storage systems, data redundancy and encoding and dynamic self-maintenance to achieve survivable information storage. The PASIS system uses threshold schemes to spread information across a decentralized collection of storage nodes. Client-side agents communicate with the collection of storage node to read and write information, hiding decentralization from the client system. P. 62. The device maintains unscrubable audit logs --that is, they cannot be erased by client-side intruders -- security personal can use the logs to partially identify the propagation of intruder-tainted information around the system. P. 63. The article states that, as with any distributed storage system, PASIS requires a mechanism that translates object names -- for example file names -- to storage locations. A directory service maps the names of information objects stored in a PASIS system to the names of the shares that comprised the information object. A share's name has two parts: the name of the storage node on which the share is located and the local name of the share on the storage node. A PASIS file system can embed the information needed for this translation in directory entries. P.63. To service a read request, the PASIS call client (a) looks up in the directory service the names of the n shares that comprise the object; (b) sends read requests to at least m of the n storage nodes; (c) collects the responses and continues to collect the responses until the client has collected m distinct shares; and (d) performs the appropriate threshold operation on the received shares to reconstruct the original information. P. 63. The p-m-n general threshold scheme breaks information into n shares so that (a) every

[redacted]

shareholder has one of the n shares; (b) any m of the shareholders can reconstruct the information; and (c) a group of fewer than p shareholders gains no information. P. 64. Secret-sharing schemes are m-m-n threshold schemes that trade off information confidentiality and information availability: the higher the confidentiality guaranty, the more shares are required to reconstruct the original information object. Secret sharing schemes can be thought of as a combination of splitting and replication techniques. P. 64. The article discusses the technique of decimation which divides information objects into n pieces and stores each piece separately. Decimation decreases information availability because all shares must be available. It offers no information theoretic confidentiality because each share expresses 1/n of the original information. P. 64. Short secret sharing encrypts the original information with a random key, stores the encryption key using secret sharing, and stores the encrypted information using information disbursal. P. 64. An extension to the threshold schemes is cheater detection. In a threshold scheme that provides cheater detection, shares are constructed in such a fashion that a client reconstructing the original information object can tell, with high probability, whether any shares have been modified. This technique allows strong information integrity guarantees. Cheater detection can also be implemented using cryptographic techniques such as adding digest to information before storing it. P. 65. For the highest architecture to be effective as possible, it must make the full flexibility of threshold schemes available to clients. The article believes this option requires automated selection of appropriate threshold schemes on a per object basis. This selection would combine object characteristics and observations about the current system environment. For example, a client would use short secret sharing protocol to store an object larger than a particular size and conventional secret sharing protocol to store smaller objects. The size that

[redacted]

determines which threshold scheme to use could be a function of object type, current system performance, or both. P. 67.

[016] The MAIL sweeper and MIME sweeper programs by ReSoft International uses a keyword search engine to review e-mails for certain words or phrases. IF the e-mail does not clear the filter, the addressee data must clear a data base check to protect the privacy and/or confidentiality of the e-mail data. See re-soft.com/product/mimesweep. The Aladdin eSafe Appliance restricts outgoing e-mails from sending classifier or prohibited content. See aks.com/news/2001/esafe.

[017] With respect to GPS or global positioning systems, U.S. Patent No. 5,982,897 to Clark; U.S. Patent No. 6,370,629 to Hastings; U.S. Patent No. 6,154,172 to Piccionelli; U.S. Patent No. 5,887,269 to Brunts; U.S. Patent No. 5,842,023 to Tsumura; U.S. Patent No. 5,778,304 to Grube; and U.S. Patent No. 5,757,916 to MacDoran disclose the use of GPS triggered systems which deny access to information when that information is requested by a portable computing device, or limit the delivery of information to a portable device based upon the location of the device obtained from a GPS locator chip or system. Encryption of data to and from GPS located devices is also dislosed in one or more of the GPS references.

Objects of the Invention

[018] It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.

[019] It is another object of the present invention to provide a method for securing data on a single personal computer (PC), on a plurality of computers linked together through a local area network (LAN) or a wide area network (WAN) or the Internet.

[redacted]

[020] It is a further object of the present invention to provide a method for securing data utilizing a client-server computer system. The client-server computer system may be implemented over the Internet. The security system may be provided to the public, to government or to private entities as an Application Service Provider or ASP over the Internet.

[021] It is a further object of the present invention to provide a method for securing data which is highly flexible and programmable by a user.

[022] It is an additional object of the present invention to enable the user to establish (a) the scope of the security sensitive words, characters or icon, data objects, (b) the future use (or destruction or encryption) of a filter enabling extraction of security sensitive data, (c) the selection of storage locations (local, removable, in an LAN, a WAN or on the Internet) for extracted data and remainder or common data and (d) one or multiple levels of security limiting full reconstruction and enabling partial reconstruction of the extracted data and the remainder or common data.

[023] It is another object of the present invention to establish and manage the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels.

[024] It is another object to provide an adaptive system responsive to hacking attempts and hacking attacks.

[025] These steps may be completely automated (after some parameters are set or programmed by a system administrator), may be fully programmable by the user, or may be a combination of automated and manual controls implemented by the systems administrator and/or the user-client.

[026] It is an object of the present invention to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data. For example, financial data maintained by an institute, can be parsed with an algorithm, the parsed segments dispersed off-site and away from the financial institute, and, upon appropriate security clearance, the dispersed data can be reconstructed to duplicate the data. Large distribution of parsed data is contemplated by this aspect of the invention. The original data remains stable, operable and immediately useful. The securing dispersed data is a back-up of the original data.

[027] It is a further object of the present invention to secure e-mail data transmissions and web browser transmissions by extraction of security sensitive data, facilitating the remote storage of said data and sending remainder data to the e-mail addressee or the recipient.

[028] It is another object of the present invention to use fine-grained selection of security critical data, extraction and encryption and separate storage of the secured data. The parsing or filtering of plaintext, data object, file or data stream thereby bridges the gap between full encryption of the plaintext etc. and no encryption. The present system is therefore a more efficient use of processing speeds, times, and storage resources.

[029] It is a further object to create a credit card number or financial data scrubber. The scrubber may be employed to remove any security critical data.

[030] It is another object of the present invention to permit the user to decide on and select a level of risk he or she believes appropriate by selecting no, minimal, intermediate or maximum levels of data security.

[redacted]

[031] It is another object of the present invention to permit the user to access data security risks, access data processing resources (processing time, storage facilities, data access time, etc.) and select a security level which balances risks and resources.

[032] It is a further object of the present invention to secure files and data objects in portable computing devices. This object is accomplished, in whole or in part, by the system or method which extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data.

[033] It is another object of the present invention to permit the scrubbing security icons from maps, credit card data or financial data from text, a data object or data stream.

Summary of the Invention

[034] The method for securing data in a computer system in one embodiment includes establishing a group of security sensitive words, characters, icons, data streams or data objects, filtering the data input from a data input device and extracting the security sensitive data. The extracted data is separated from the remainder data and is separately stored. In one embodiment on a personal computer (PC) system, the extracted data and the remainder or common data is stored in different, distributed memory segments. In a network implementation, the extracted data may be stored in one computer and the remainder or common data may be stored in another computer. In a client-server implementation, the server may direct storage of the extracted data to a different location than the remainder data, either on the server or on a further memory system (computer) interconnected to the server or on the client computer and in distributed memory segments. A map may be generated by a software module or sub-system indicating the location of the extracted data and the remainder data in the network. The filter may be destroyed (via a deletion routine) or may

[redacted]

be retained for future use by the user. If retained, encryption is preferred. The map may be stored on the client computer or the user's PC or may be stored on the server. Copies of the map may be removed (deleted) from the user's PC or the client computer. The map may be encrypted. The extracted data and/or the remainder data may be removed (deleted or scrubbed) from the originating computer. Encryption can be utilized to further enhance the security levels of the system. All transfers of the filter between the client to the server may be encrypted, and all data (whether extracted data or remainder data) may be encrypted prior to storage in the distributed memory. Any transfer of extracted data or remainder data or maps or filters may include an encryption feature. Reconstruction of the data is permitted only in the presence of a predetermined security clearance. A plurality of security clearances might be required which would enable a corresponding plurality of reconstructing users to view all or portions of the data. Persons with low level security clearance would only be permitted to have access to low level extracted data (low level security sensitive data) and the common data. Persons with high level security clearances would be permitted access to the entire document reconstituted from the extracted data and the remainder data. A computer readable medium containing programming instructions carrying out the methodology for securing data is also described herein. An information processing system for securing data is also described.

[035] In another embodiment, the method for securing data in a computer network and transparently establishing and managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know, security levels, by necessity, utilizes communities of interest representing a plurality of users having corresponding similar security levels, each with a respective security clearance. In other words, all members of Community A have the same security level and security clearance, which is different than the users of Community B which have a different

[redacted]

security level and security clearance. The method and the computer media containing programming instructions includes filtering data from the data input computer, extracting security sensitive words, phrases, characters, icons, or data objects and forming subsets of extracted data and remainder data. The subsets of extracted data are stored in one or more computer memories in the network identified as extracted stores. The remainder data is also stored in the network if necessary. Reconstruction of some or all of the data via one or more of the subsets of extracted data and the remainder data is permitted only in the presence of a predetermined security clearance from the plurality of security levels. The cryptographically separated, need to know, security levels correspond to respective ones of the plurality of security levels and the method includes, in one embodiment, encrypting subsets of extracted data with corresponding degrees of encryption associated with the plurality of security levels. During reconstruction, all or a portion of the plaintext data is decrypted only in the presence of the respective security level. The information processing system which secures data per the community of interest security level in the includes a data filter for the data input from the data input computer which extracts the security sensitive words, phrases, icons or data objects. A system and a methodology for storing the subsets of extracted data and remainder data is provided and a compiler permits reconstruction of some or all of the plain text data in the presence of an appropriate security clearance level. Multiple level encryption in one document is also available.

[036] An adaptive method of securing data responsive to a plurality of hacking events utilizes a hacking monitor which generates a corresponding plurality of hack warnings dependent upon the severity of the hacking attack. Based upon respective ones of the hacking or hack warnings, data is filtered to extract security sensitive words, phrases etc. and the extracted data and the remainder data (if necessary) is stored based on the degree of hack warning. Reconstruction is

permitted of some or all the data utilizing the extracted data and the remainder data only in the presence of the predetermined security clearance level. Automatic reconstruction is permitted after the hack attack terminates. The method sometimes includes encrypting extracted data dependent upon the degree or severity of the hack warning and decrypting that data during reconstruction. A computer readable medium containing programming instructions similar to the method is also provided. The information processing system includes a filter which is adjusted based upon the degree of hack warning to extract security sensitive words. A storage system stores extracted data and remainder data (if necessary) based upon the level of the hack warning and a compiler is used to reconstruct the data in the presence of the appropriate security clearance level.

[037] The parsing and dispersion aspects of the present invention enable the user to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data. The original data may be maintained in its original state and stored as is customary, encrypted or destroyed. For example, financial data maintained by an institute in its original state, and a copy thereof can be parsed with an algorithm, the parsed segments dispersed off-site, (that is, separated and stored in extract and remainder stores or computer memories), away from the financial institute, and, upon appropriate security clearance, the dispersed data can be reconstructed to duplicate the data. Large distribution of parsed data is contemplated by this aspect of the invention. The original data remains stable, operable and immediately useful in its stored location. The secured and dispersed data is a back-up of the original data. Destruction of the original source is also an alternative embodiment.

[038] Another embodiment of the present invention operates in an e-mail or a web browser environment. In a specific embodiment, the invention operates as a credit card or financial data

scrubber. The e-mail data has one or more security sensitive words, characters or icons and the method or computer program works in a distributed computer system with a remote memory designated as an extract store. The method extracts the security sensitive words, characters or icons from said e-mail data to obtain extracted data and remainder data therefrom. The extracted data is stored in the extract store. The methodology emails the remainder data to the addressee. the addresses is permitted to retrieve the extracted data from said extract store only in the presence of a predetermined security clearance and hence, reconstruct the e-mail data with said extracted data and remainder data. The program and method on the user's e-mail device extracts the security sensitive data, facilitates storage of the extracted data in said extract store and, emails the remainder data to the addressee. Rather than extracting security data, the method and program may parse the data. The method and program for safeguarding data entered via a browser involves extracting security sensitive data, facilitating the storage of such data in the remote store, and forwarding the remainder data to a targeted destination in the distributed computer system. The scrubber may utilize a pop-up window to enable user activation of the scrubber on an email or a web browser communication.

[039] In a computer system with a portable computing device, the method secures security sensitive words, characters, icons, data streams or data objects by determining when the portable computing device is within or without a predetermined region and then extracting the security sensitive data from the file, text, data object or whatever. The extracted data is separated from the remainder data and is separately stored either on media in a local drive or remotely, typically via wireless communications network, to a remote store. In a military application, security icons on a map are extracted, remotely stored and therefore access to the secured data is limited geographically

and further by password or pass code control. Encryption can be utilized to further enhance the security levels of the system. Extraction may be automatic, that is, when the portable device is beyond a predetermined territory, or it may be triggered by an event, such a "save document" or a time-out routine. Reconstruction of the data is permitted only in the presence of a predetermined security clearance and within certain geographic territories. A computer readable medium containing programming instructions carrying out the methodology for securing data is also described herein. An information processing system for securing data is also described.

[040] The present invention can be configured in various forms. The following descriptions discuss various aspects of the invention and further advantages thereof.

[041] The present invention enables the user to obtain automatic classification and declassification of documents on the fly. The extraction process downgrades and declassifies documents on the fly (in real time) so that they are useless to unauthorized parties. Presentation by a user of a valid security clearance enables substantially instant and seamless reconstitution of the security sensitive content.

[042] The present invention can be configured to automatically secure unstructured documents and freeform documents, for example, e-mail, instant messaging, or Word documents (input documents).

[043] The present invention may also be configured to automatically secure structured documents and transactional documents for example, database records or XML documents (input documents).

[044] The present invention introduces flexibility into security management, risk management of data, data storage, and data flows and enable automatic responsiveness to threats.

[redacted]

The innovation enables automatic response to security challenges and threats. The innovation can maintain, upgrade and downgrade the levels of security through implementation of a leveled granular extraction process and a controlled-release mechanism. Attacks or other external events can trigger a response in the form of higher extraction levels, expanding the type of content extracted, and constricting the release of important and critical data control from storage. How much and what to extract depends on the level of threat or perceived risk. In same manner, the amount and type of content released from storage and reconstituted depends on the level of threat or risk perceived by the system. The system delivers a level of security protection specifically matched to meet security needs as dictated by the changing security threats, environment, policy and organizational needs.

[045] The present invention enables a user to introduce and maintain multiple levels and standards of security. It is common knowledge that the highest security is delivered through total separation. Whereas this concept has only been implemented physically or by isolating computer environments, the invention achieves this concept of total separation within open and networked computer environments. The invention can implement a total physical and logical separation of important and critical data from its context and can preclude access to that information without a needed granular access permission. The invention is also effective for sounds and images (data objects or data streams with security words, characters, terms, icons or other data objects).

[046] Some aspects of the present invention introduce a new method and apparatus to monitor security sensitive content through a process of analysis and categorization of each word or character, in a document. The invention enables processing of every character, word, number, as they are entered into a document and categorizes each into one of many pre- set categories. Categories can include surnames, locations, currency, defined terminology, and unknown words or phrases.

[redacted]

[047] The present invention, in some embodiments, introduces a method and apparatus for plain text extraction and dispersion of security sensitive data. Maximum security with traditional methods encumbers free flow of information and business efficiency. Encryption burdens computer systems with high performance overhead, and its use is limited to the parties who have decryption capabilities. The invention offers a new solution. It enables leveled security in plain-text format, in addition to none, some, or all of pre-existing encryption, decryption, firewalls, and other security infrastructure. The level of security is determined by the extent of the security sensitive items, selection process; the extent of dispersal to various distributed storage locations; the rules for controlled-release from storage; and the access rules governing the reconstitution of extracts into the secured document.

[048] In this configuration of the invention, the extractions are dispersed to distributed storage on a granular level. The rest of the document can be stored at its original location and/or other storage locations. Dispersal of extractions introduces new barriers not existing in current security. In certain situations, an attacker has first to find the (encrypted) map to the locations, then locate and access the distributed storage, get the data released from the controlled-release storage, and finally reintegrate the extracts into the appropriate documents.

[049] Further, the present invention enables the user to implement a method and apparatus for targeted extraction and encryption of security sensitive items. The extraction capabilities of the system enable different workflow modes. The system enables extraction and encryption of important and critical content. In essence, only the critical content is extracted and/or encrypted, whereas the rest of the document remains as plaintext. This capability enables the following: advantages and flexibility; and the ability to share the document within the organization or transmit it to outsiders

[redacted]

while still maintaining security over the most important and critical content of the document. This is an automatic process for controlling the content of outgoing e-mail. The document owner releases the important and critical content by enabling access to it to defined parties at defined times within defined threat modes.

[050] The present invention, in some implementations, introduces a method and apparatus for encrypting document or extractions with multiple encryption types. The invention can deliver the highest level of security by using multiple types of encryption (and/or multiple keys) for one line, paragraph or document. Maximum security is delivered through automatic selection of security sensitive items, and encrypting these extractions with one or more types of encryption. The remainder data can also be encrypted. Multiple encryption types within one document statistically precludes deciphering that document regardless of the available computer power. Common encryption methods are vulnerable through existing technologies, social engineering methods, carelessness, and workflow habits. Furthermore, simple encryption becomes more vulnerable (including triple DES) assuming future mathematical breakthroughs or quantum computing. Existing methods to crack block ciphers are being improved to compromise the future AES Rinjdael standard.

[051] The present invention also enables the user to configure the system to introduce a method and apparatus for content dispersion. The innovation enables control over specific important and critical content items within the general contents of documents or digital files in a computer or within a network. The immediate controlled-release of those important content items according to specific identification and access criteria proactively safeguards the security and the value of documents or digital files. The content control enables broad dissemination of the digital files in closed networks, as well as open networks including the Internet, without compromising the security

[redacted]

of the important and critical information in the digital file. The dispersal channels can include any of all of the following: networks, Internet, Virtual Private Channel. Telephone lines, Optical lines, Wireless, Fax, Documents, Verbal communication.

[052] The present invention, when configured in an appropriate manner, introduces a method and apparatus for enhancing the survivability capabilities of an organization and its networks. If networks get damaged, the decryption capability, such as PKI, is likely to be compromised, or at a minimum, suspended. In such instances, the invention enables continuation of work on channels, which need not be secure. In addition, the dispersion of information guarantees maximum partial reconstitution to documents and transactions, or total reconstitution to documents and transactions benefitting from backup at distributed storage facilities.

[053] The present invention, in the appropriate environment, introduces a method and apparatus for delivering security for inter-connecting networks. It enables security for closed networks connecting to the Internet and other open networks. The Internet infrastructure and open networks are not secure. Even secured closed networks, such as VPNs, are not secured enough. The critical content of documents is the critical asset of the organization and must be highly secured, with maximum reliability, full transparency and instant accessibility. To remain competitive, organizations must maximize utility of the critical data within their documents, files, databases and servers. The securing of such documents must not be at the expense of compromising the access or processing speed of such documents. The invention enables work in plain text, as well as with encryption. Working in plain text reduces the computing performance overload.

[054] Some aspects of the present invention introduce a method and apparatus for delivering information flow control in decentralized environments. Protection of privacy and

confidentiality of information represents a long-standing challenge, The challenge has become much bigger with the expansion of the Internet, which has created decentralized networks. Parties, who do not know or trust each other, have to exchange information. The invention enables free flow and sharing of information between parties by removing burdening security restrictions and creating top security with a controlled-release of the security sensitive content in the documents. The technology enables top security through introduction of user and organization's ownership and control of the critical granular data in documents.

[055] The system, in certain embodiments, introduces an additional layer of access controls at the granular level of the user document. In order to view the reconstructed critical information the user would need to be verified by additional access controls at the data storage level. The user access code or a physical key enables release of data from the storage. Today's access controls do not stop the user from distributing documents to other parties. The inventions fined grained controlled-release mechanism releases the critical information, only under a required set of circumstances and access validation. The invention enables the user ownership of his security sensitive critical data and conditions for its release and dissemination. The user has the option to hide the critical data through declassification process and release through a reclassification process in which the critical data would be reconstituted in the document.

[056] The present invention, when configured by the user, introduces a method and apparatus for delivering compartmentalization of security sensitive content by leveled access to users. The invention creates leveled sharing of information, for example such that persons with level 3 access will have keys for encryption type RSA persons with level access 2 will have access to Blowfish encryption within one document.

[redacted]

[057] The present invention, in certain embodiments, introduces a method and apparatus for enabling more use of distributed and dispersed storage including ASPs (application service providers). There is a major human tendency to refrain from sending important documents to web storage locations because of potential security breaches. This cultural issue is both driven by psychological issues and well-founded security concerns. The retention of those documents as is in physical proximity or locked security, provides actual security but precludes gaining any utility from those documents in a functional business setting. Instead the invention enables functional distribution of those documents without the security sensitive data, and a controlled-release of some or all of the extractions in a granular way in order to support business activities while retaining security.

[058] The present invention, in certain configurations, introduces a method and apparatus for enabling lower storage costs. The extraction process declassifies and downgrades mission critical documents. The downgrading and transformation of a critical document into a non-critical document, enables storage in less secured and lower cost storage. Taking advantage of this security-initiated, extraction process can yield substantial storage cost savings. The invention enables a high return on investment ROI for system storage cost arbitrage. Splitting the data into critical and non-critical enables 20 to 90% savings on storage cost.

[059] The present invention, in certain circumstances, delivers an automated security risk management system that creates added in-depth security defenses at the semantic-level as well as creation of controlled-release mechanisms at the storage-level with significantly reduced performance overhead requirements.

[redacted]

[060] Certain embodiments of the present invention present a technology which answers the security demands as required by Committee on Information Systems Trustworthiness of the National Research Council. The Committee's report, Trust in Cyberspace (1999), defines the security paradigms needed for a safe future. The report states: The substantial commercial off-the-shelf (COTS) makeup of a network information systems, the use of extensible components, the expectation of growth by accretion, and the likely absence of centralized control, trust, or authority demand a new approach to security: risk mitigation rather than risk avoidance; technologies to hinder attacks, rather than prevent them outright; add-on technologies and defense in depth; relocation of vulnerabilities rather than their elimination; none of the existing or security technologies addresses these needs in whole. The invention breakthroughs this barrier by providing a single system which implements each one of those four elements in a unified way. The invention controls information flow in centralized and decentralized environments, through controlled-release of information within distributed systems.

[061] The present invention can be implemented to enable certain security measures while accommodating the performance needs of a network. The invention provides a method and apparatus to ease overhead performance on congested computer networks. It can adjust the security defenses based on the performance needs of the network. Many security systems overburden the already burdened computing environment in terms of computational overhead, labor, and training requirements. The invention enables to ease the overhead performance of a network by transforming from high overhead performance, encryption methods, and other security methods, to the method presented by this invention.

[redacted]

[062] Certain aspects of the present invention minimize the time of exposure of the important content within a document. The invention enables to separate the important content from the rest of the document for substantial periods of time, thereby minimizing substantially the exposure to risk. It is possible for example to extract the important content from the document and release it for reconstitution only when the user will open the document. In such situations the important content could for example be time and unexposed for over 99% of the time and exposed for less than 1% of the time, which lowers the risk substantially.

[063] Further, embodiments of the present invention provide a security risk management method and system to minimize security risks. The invention enables minimization of security risks by: Automatic separation and extraction of granular critical data from the core document. Dispersal of the extracted critical data groups to different secured storage locations. Reconstitution of the critical data in document for limited time, to minimize exposure to risk. Partial reconstitution, of the critical data, in core document, through a controlled release of granular critical data. Granular controlled release of data to specific authorized people only.

[064] The present invention, in certain configurations, provides a controlled release security mechanism to enable the release of content and granular content from storage locations in a centralized and decentralized environment. The controlled release mechanism enables release of the appropriate content to the authorized party at the right time under the right circumstances.

[065] The present invention sometimes provides a security solution against damage by insiders. Studies show that insiders cause 70%-85% of the damage. These nine innovations are described in detail as follows: The invention enables insiders and employees to work with documents while managers and owners control the release of the critical prioritized information. The control is

granular, thereby enabling continued work with the rest of the content in the document. The objective is to empower the user with the highest security while enabling him maximum sharing and delivery flexibility. This enables free flow of information between closed networks and public networks, such as the Internet, without compromising the security through extraction of important and critical content. The user can transport documents through various networks and e-mail services knowing that the critical information, which is still under control, and is not compromised.

[066] The present invention can be configured to provide an automatic security system in order to overcome human flaws that create security vulnerabilities. Human engineering flaws are the cause of 90% of security vulnerabilities. For example, passwords are exposed through human fault enabling reading of plain text before it is encrypted. The invention enables an automatic process of appropriate response to security threats in an objective way and on an on going basis.

[067] Certain aspects of the present invention provide an automatic security system in order to reduce human labor, and training costs.

[068] The present invention provides, in one or more embodiments, protection for important granular content within a document. A feature left out in computer development is the protection and automatic protection of granular important content in a document. In every facet of life critical assets are immediately protected. For example, credit cards and cash are protected in a wallet, important items at home are placed in closets, wall units, cabinets and safes. The present system extracts the digital equivalent of these items, e.g., extracts all credit card data, and stores the extracted data in secure location(s).

[069] In general, the present invention provides an alternative method to encryption. Mathematical security and encryption could be broken. Discovery of a mathematical equation for

[redacted]

a shortcut of the factoring of prime numbers would be make mathematical security and encryption extremely vulnerable.

[070] In 1999 a 512-bit RSA key was broken- at that time 95% of keys in e-commerce were 512 bits long. U.S. government 56-bit Data Encryption Standard was cracked in just 22 hours by the Freedom Foundation.100, 000 PCs were connected with a supercomputer which enabled the testing of 245 billion keys per second.

[071] The invention, in a larger sense, provides an automated security risk management system. The system automatically responds to attacks by matching the defenses level to the level of threats The system responds to security threats through the following mechanisms: (1) controlled extraction of sensitive security data: in normal circumstances, extractions will take place according to pre-set rules; in threat situations, additional extractions will take place to deliver higher security; in an attack, additional substantial amounts of critical data will be extracted to deliver the highest security; (2) controlled dispersal to storage locations; in normal circumstances, dispersal to different storage locations according to pre-set rules will take place; in threat and attack situations, more dispersal to more storage locations, via additional communication channels will take place; and (3) controlled release of extracts for reconstitution; controlling amount of extracts released for reconstitution; controlling time of exposure of extracts in reconstitution; limiting access to specific people; and limiting access to specific times.

[072] The present invention also defends, in certain embodiments, against devices like keyboard sniffers and mouse sniffers that can read information keyed into the computer and transmit it to an adversary. The invention enables to input security sensitive items through data input devices

other than the keyboard. For example credit card numbers can be inputted through a hand held wireless devise. The inputted data would be transferred to storage for possible reconstitution.

[073] The present invention can also be configured to defend against devices that intercept electromagnetic signals from computers, monitors, printers, and keyboards. For example the Van Eck receptors which can read information off the screen the display screen. The invention enables separation contents of document into two or more displays thereby limiting the potential damage of electromagnetic eavesdropping.

[074] The present invention, in many embodiments, enables the controlled release of data objects, full or partial release of plaintext source documents to persons or organizations with the appropriate security clearances.

[075] Another object of the present invention is to enable the control of information flow over a PC, a network, a LAN, a WAN and over the Internet.

[076] A further object of the present invention is to enable the interoperability of several secured networks based upon the relative security clearances of each network.

[077] It is another object of the present invention to provide a process for synthesizing a document.

Brief Description of the Drawings

[078] Further objects and advantages of the present invention can be found in the detailed description of the preferred embodiments when taken in conjunction with the accompanying drawings in which:

[079] FIG. 1A diagrammatically illustrates a basic system diagram showing filtering and storing extracted data and remainder or common data and, in an enhanced embodiment, generating and storing a map.

[080] FIG. 1B diagrammatically illustrates a system diagram showing reconstruction of the data, various security clearances and both electronic reconstruction and visual reconstruction.

[081] FIG. 2 diagrammatically illustrates a system showing major components of a single personal computer (PC) system, a networked system with several PCs (a LAN or WAN) and the network coupled to a telecommunications system and the Internet and shows the interconnection with a server and multiple, Internet-connected memory units.

[082] FIG. 3 diagrammatically illustrates a basic flowchart showing reconstruction for various security levels.

[083] FIG. 3A diagrammatically illustrates interleaving distinct data into different memory locations in a video memory.

[084] FIG. 4 diagrammatically illustrates a flowchart showing one embodiment of the principal portions of the data security program.

[085] FIG. 5 diagrammatically illustrates a flowchart showing the basic elements of the reconstruction process for the data security program.

[086] FIG. 6 is a computer network diagram showing various user communities.

[087] FIG. 7a diagrammatically illustrates a flowchart showing the key component steps for the multiple layer security program for the community of users.

[088] FIG. 7b diagrammatically illustrates a multiple level security system accessed by users having different security clearances (which also represents a data mining system and operation).

[redacted]

[089] FIG. 8 diagrammatically illustrates a flowchart showing the key components of an adaptive security program adaptable to various levels of electronic attacks, hacker or hack attacks.

[090] FIG. 9 diagrammatically illustrates a flowchart showing the key components of a multiple encryption program using multiple types of encryption in one document or data object.

[091] FIG. 10 diagrammatically illustrates a chart showing the key components of the parsing, dispersion, multiple storage and reconstruction (under security clearance) of data.

[092] FIGS. 11A and 11B diagrammatically illustrate a flowchart showing the key components of one embodiment of the e-mail security system (jump points 11-A and 11-B link the flow charts).

[093] FIGS. 12A and 12B diagrammatically illustrate a flowchart showing the key components of one embodiment of the invention implements the security system on a web browser (jump point 12-A links the flow charts).

[094] FIG. 13 diagrammatically shows several revenue systems which may be employed with the data security systems described herein.

[095] FIG. 14 diagrammatically illustrates a portable computing device (or the critical parts thereof, see FIG. 2 for further details) associated with the portable data security locator system and method.

[096] FIG. 15 diagrammatically illustrates a basic flow chart for the portable security system program in accordance with the basic principles of the present invention.

Detailed Description of the Preferred Embodiments

[097] The present invention relates to a data security system, a methodology of securing data on a personal computer (PC) system, on a computer network (LAN or WAN) and over the

[redacted]

Internet and computer programs and computer modules and an information processing system to accomplish this security system.

[098] It is important to know that the embodiments illustrated herein and described herein below are only examples of the many advantageous uses of the innovative teachings set forth herein. In general, statements made in the specification of the present application do not necessarily limit any of the various claimed inventions. Moreover, some statements may apply to some inventive features but not to others. In general, unless otherwise indicated, singular elements may be in the plural and vice versa with no loss of generality. In the drawings, like numerals refer to like parts or features throughout the several views.

[099] The present invention could be produced in hardware or software, or in a combination of hardware and software, and these implementations would be known to one of ordinary skill in the art. The system, or method, according to the inventive principles as disclosed in connection with the preferred embodiment, may be produced in a single computer system having separate elements or means for performing the individual functions or steps described or claimed or one or more elements or means combining the performance of any of the functions or steps disclosed or claimed, or may be arranged in a distributed computer system, interconnected by any suitable means as would be known by one of ordinary skill in the art.

[100] According to the inventive principles as disclosed in connection with the preferred embodiment, the invention and the inventive principles are not limited to any particular kind of computer system but may be used with any general purpose computer, as would be known to one of ordinary skill in the art, arranged to perform the functions described and the method steps described. The operations of such a computer, as described above, may be according to a computer

[redacted]

program contained on a medium for use in the operation or control of the computer as would be known to one of ordinary skill in the art. The computer medium which may be used to hold or contain the computer program product, may be a fixture of the computer such as an embedded memory or may be on a transportable medium such as a disk, as would be known to one of ordinary skill in the art.

[101] The invention is not limited to any particular computer program or logic or language, or instruction but may be practiced with any such suitable program, logic or language, or instructions as would be known to one of ordinary skill in the art. Without limiting the principles of the disclosed invention any such computing system can include, inter alia, at least a computer readable medium allowing a computer to read data, instructions, messages or message packets, and other computer readable information from the computer readable medium. The computer readable medium may include non-volatile memory, such as ROM, flash memory, floppy disk, disk drive memory, CD-ROM, and other permanent storage. Additionally, a computer readable medium may include, for example, volatile storage such as RAM, buffers, cache memory, and network circuits.

[102] Furthermore, the computer readable medium may include computer readable information in a transitory state medium such as a network link and/or a network interface, including a wired network or a wireless network, that allow a computer to read such computer readable information.

[103] In the drawings, and sometimes in the specification, reference is made to certain abbreviations. The following Abbreviations Table provides a correspondence between the abbreviations and the item or feature.

Abbreviations Table

A-com	computer or memory store for common or remainder data
ASP	application service provider - server on a network
B-ext	computer or memory store for extracted data
bd	board
CD-RW	compact disk drive with read/write feature for CD disk
comm.	communications, typically telecommunications
CPU	central processing unit
doc	document
dr	drive, e.g., computer hard drive
DS	data storage
e	encryption
ext-data	extracted data
I/O	input/output
I-com	Internet storage for common or remainder data
I-ext	Internet storage for extracted data
loc	location
mem	memory
MLS	multilevel security
obj	object, for example, a data object
pgm	program
re	regarding or relating to
recon	reconstruct

rel	release
req	request
rev	review
sec	security
SL	security level (sometimes S1 for security level 1, etc.)
sys	system
t	time
tele-com	telecommunications system or network
URL	Uniform Resource Locator, x pointer, or other network locator

Basic Operational Theory

[104] FIG. 1A diagrammatically illustrates the basic processes for establishing a secure storage of information, generally identified herein as "data." "Data," as used herein, includes any data object, e.g., text, images, icons, moving images, multiple images, data representing sound, video, electronic streams of information, etc. Sound bites and video images may also be extracted data. A source document 100 containing data, sometimes referred to as a "plaintext," is passed through a filter 102. Although it is convenient to discuss and understand the invention herein in connection with a plaintext document, the document 100 is a data object. It is not limited to an electronic document representing words. The document 100 represents a data object that may be, e.g., text, images, icons, moving images, multiple images, data representing sound, video etc. The term "data object" as used in the claims is broadly defined as any item that can be represented in an electronic format such that the electronic format can be manipulated by a computer as described herein. The data object, or as discussed herein, the "plaintext" is sent to a filter. Filter 102, in a most

[redacted]

basic sense, separates out common text or remainder data 104 from uncommon text, words, characters , icons or data objects. The security sensitive words, characters, icons or data objects are separated from remainder or common text 104 as extracted text 106. It should be noted that although the word "text" is utilized with respect to remainder text 104 and extracted text 106, the text is a data object and includes words, phrases, paragraphs, single characters, portions of words, characters, whole or partial images, icons or data objects. In a basic implementation, filter 102 may utilize a dictionary such that words present in the dictionary (common words) are separated from the source plaintext document 100 and placed into remainder document or common data file 104. The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted data file 106. For example, a business may wish to impose a security system on a contract document such that the names of the contracting parties (not found in the dictionary) and the street names (not found in the dictionary) would be stored in extracted data text file 106. The common text or remainder data would be stored in remainder data file 104. In the illustrated embodiment, remainder data file 104 also includes place holders which enables the extracted data to be easily inserted or set back into the remainder data file.

Input or Initial Processing Considerations

[105] The security sensitive words, characters, icons or data objects may be any word, phrase, letter, character, icon, data object (full or partial), image or whatever, as pre-defined or as established by the user. The user may specifically design the filter, begin with a dictionary to define common terms, identify any additional security sensitive words, letters, images, icon, data objects, partial versions of the foregoing or any other granular aspect of the plaintext. After defining the filter and accepting the data input, the system filters the plaintext and separates extracted data (security

sensitive items) from the remainder data. The filter may also include elements of artificial intelligence (AI). For example, the user may select one word as a security word and the AI filter may automatically select all synonymous words. The AI filter may enable the user to define a filter in real time at the entry of data via a keyboard. For example, the user may select to secure (i.e., extract and store) some proper names and may instruct the filter to secure names such as Block, Smythe and Cherry. During input of the plaintext, the system may detect Smith and ask the user if he or she wants to secure (a) all proper names in a common name dictionary collection and/or (b) all names with spellings similar to the filter input data, Block, Smythe and Cherry. As is known in the art, AI typically uses inference engines to define one pathway or to outline a course of action. The filter or extraction engine discussed herein can be configured with AI, inference engines, neural network systems or other automatic systems to carry out the functionality described herein for the dynamic operation of the security system.

[106] The system and methodology described herein also encompasses parsing the plain text document by bit count, word, word count, page count, line count, paragraph count and parsing based upon any identifiable document characteristic, capital letters, italics, underline, etc. Algorithms may be implemented to parse the plain text document. The target of the parsing algorithm (a bit count, word, letter, etc.) is equivalent to the "security word, character or icon, data object" discussed herein. The parsing occurs with the filtering of the plain text source document 100 and the subsequent storage of extracted data apart from remainder data.

Storage

[107] In a basic configuration, the common text or the remainder data is stored in common storage memory 108. This common or remainder data store is identified as A-com generally

[redacted]

referring to a segmented memory in a PC or a computer A in a network (LAN or WAN). It should be understood that reference to "remainder data" is simply a short-hand representation of data that is not extracted or filtered by the system. Accordingly, "remainder data" is simply that data which can be viewed, manipulated or further processed by the user inputting or initially processing the data. Remainder data storage 108 may include a confirm storage signal function 111 to send back a confirm storage signal to the data input device generating source plaintext document 100. The extracted data file 106 is stored in a different memory computer storage 110 (B-ext). In a preferred embodiment, memory segment 108 (A-com) is at a different location than computer storage memory segment 110 (B-ext). In a PC embodiment, memory A-com is a different memory segment than memory B-ext. In a networked embodiment, computer storage 108 may be on a different computer as compared with computer storage 110. In an Internet embodiment, common text or cleansed text storage is at one web site (which may be one computer) and the extracted, high security data is stored at another web site, buried web page or other Internet-accessible memory store location. In any event, the remainder text is stored in a memory A-com and the extracted data or high security words, characters , icons or data objects are stored in memory B-ext. After storage of the extracted data in memory 110, a confirmation indicator 113 may be generated to the client computer or the computer handling source plaintext input document 100 (the originating computer system).

[108] As a simple example, the program configured in accordance with the present invention, could automatically detect entry of all credit card numbers types into a user's computer. The filter is set to detect the unique credit card sequence and data string. Assuming that the user's computer is operating a browser and the user is communicating with a server on the Internet, the user's computer would filter out the credit card number and send the number to a secure storage site.

The secure storage site is owned, operated or leased by a trusted party. The extracted data, i.e., the credit card data, is stored at the trusted site. The URL or other identifying data is sent to the vendor from which the user wants to purchase goods and services over the Internet. When the vendor seeks to complete the transaction, the vendor sends a request code to the secure site, the trusted party at the secure extracted data storage site debits the user's credit card account (or otherwise debits the user's bank account) and sends an approval code to the vendor. In this manner, the vendor is never given the user's credit card – the card number is sent to a trusted party automatically by the filter in the security program described herein. The security program may be incorporated in a browser to automatically protect credit card data, personal data (as a method to become anonymous on the Internet), etc. from being deliberately broadcast to others on the Internet or to block others from snooping into the user's personal data while the user communicates over the Internet.

[109] In a further enhancement of the present invention, the computer or data input device handling source plaintext document 100 may also record the location of A-com 108 and B-ext 110. The location data is called herein a "map." A memory mapping function is utilized. The map may be stored in a third memory location 112. Memory location map 112 may be a segment of the memory of the data input computer originating plaintext 100. The map may be encrypted for security reasons.

Extraction and Storage Enhancements

[110] As a further enhancement of the present invention, the user, prior to initiating the security system, may be given a choice of filtering out all the uncommon words or words not found in the dictionary and adding certain security sensitive words, characters, icons or data objects to filter 102. The added words or terms are filtered out with the uncommon words. Of course, the user may

be required to manually input all security words or download the security word filter from the Internet or another system on the LAN. For security systems having multiple security levels, a plurality of filters would be created, each filter associated with a different security level. Further, multiple security levels would require, in addition to remainder text document or data 104, a plurality of extracted data documents 106. The common or remainder text document or data 104 would still be stored in remainder computer storage A-com 108. However, each extracted data document 106 would be stored in a respective, separate computer memory segment or computer B-ext 110. Separate storage of a plurality of extracted data at multiple, separate locations in B-ext is one of the many important features of the present invention.

[111] The ability of the program to locate security sensitive words or characters can be enhanced by using a telephone book, properly dissected, to identify a collection of last names. Cities and towns and street names can also be identified in this manner. The compilation of last names and cities, towns and streets can be used as a list of critical, security sensitive words. The filter is represented by this compilation of words. Similar techniques may be used to create filters for scientific words, or words unique to a certain industry, or country.

[112] In view of increasing levels of security relating to (a) the storage location A-com; (b) the transfer of remainder text document 104 to memory computer storage A-com 108; (c) the storage of map 112 (possibly encrypted); (d) the creation, storage or transfer of filter 102 (possibly encrypted); (e) the storage of extracted data at memory storage B-ext (whether singular or plural storage sites); and (f) the transfer of extracted data thereto, the system may include an encryption e feature. The encryption e function 115, 117 and 118 is diagrammatically illustrated in FIG. 1A.

[113] The program of the present invention can be set to extract critical data (a) when the plaintext or the source document (data object) is created; (b) when the source document or data object is saved; (c) on a periodic basis; (d) automatically; (e) per user command; (f) per ascertainable or programmable event; and (g) a combination of the foregoing. Timing for storage of the extracted data is based on these aspects. Reconstruction of the data object or plaintext may be (a) automatic and substantially transparent to the user; (b) based upon manual entry of security clearance data; (c) periodic; or (d) a combination of the foregoing dependent upon outside events and who is the author of the data object or other definable aspects of the data object, its environment of origination, current and anticipated security threats and its environment of proposed reconstruction. The timing for the extraction, storage and reconstruction is oftentimes dependent upon the level of security required by the user and/or his or her organization.

[114] The system and method creates a high level of security by automatic selection and removal of critical and prioritized contents from a data objects stream, whether it be a digital document, digital file, database, sound bite, video clip, other structured, or streaming data formats. The system and method enables a controlled release of the extracted data objects, enabling instant display of the instantaneous returned contents, contingent on verification of user identity, access rights, time of operation, location of source and or user, destination of source and or user, and determine threat modes. The system and method delivers high security by removal of the selected prioritized content from memories. The copies and traces of the selected extracted contents are eradicated from the computer memory while the separated extract data stream is transferred to a safe removed storage memory media. The extract, extracts, and any part thereof, will be return transferred to user display as soon as identity and access rights are validated.

[redacted]

[115] A replacement of the extract (sometimes called a placeholder) can also be substituted on-the-fly to provide updated results, misinformation, dis-information, messages, alerts, links (to reports, data mining, search engines, web sites, and hyperlinks understood in the current art), advertisements, and personalization and customization. The validation can be done instantly by password, challenge questions and answers, remote verification (phone, video, or personal contact with user), or by biometrics means.

[116] The extraction of data objects within data streams includes words, structured data objects, characters, numbers, bullet points, footnotes, prices, images, sound segments, video segments, and selected digital data packets. The extraction is conducted by separating a source (original) data stream into two or more extracts data streams. The different data object extractions are separated into groups reflecting predefined contextual categories and restitution applications (such as to enable customization and personalization for the same or different users). The modified source (original) stream typically contains the majority of data objects of the source stream, whereas the extract streams contains a minority of the data objects which represent selected and categorized information and information deemed to be of prioritized importance.

[117] The extracted categorized data objects are separated into one or more contiguous data streams. The extracted data stream or streams are scattered to one or more storage memory memories. The extracted data can be transported and shuttled between different storage or projection apparatus, as directed automatically by various constraints including: security risk criteria of threats and attacks, sources, targets, users, policies, time of day, and threat modes.

[118] The extracted data, in some cases, is transported to an online removable storage and under extreme security threats to an off-line/off-network, digital or physical vaulted storage.

[redacted]

Transport and shuttle is based on the level of security alert. The use and release of the vaulted extractions is controlled by a set of rules or organizational policy which includes the following options among others: (a) A vaulting of some, all, or specific data object extracts for long or short periods of time. (b) Release of extractions into a display, in which the extracted data objects will reconstitute with the modified original data stream, the original data objects stream or original document. (c) Release of extractions into a projection display in order to project with the modified data stream, the original document while maintaining complete separation of the modified source data stream (the source modified by the extraction of data objects and insertion of placeholders) and the extracted data object streams. (d) Release of extractions into a projection display in order to project a reconstitution of the original document, in other words to create altered versions of the original document, while maintaining complete separation of the modified data stream and the extracted streams. (e) In situations of high security threats, release of extractions into another projection display, PDA, floppy disk, paper document a wireless display, an overlay transparency while maintaining logical and physical separation of delivery streams. This will enable working with a representation of the initial source, but not the initial source itself, while understanding the prevalent, critical extracted information without comprising security to the initial source material by exposing sensitive, identifying, or critical information. (f) The distribution of sources, modified sources, or extracts to remote and distributed viewing devices. (g) Enable the ongoing operation of information delivery and display in defiance of known ongoing or unknown security flaws, breaches, or events compromising the general state of security. (h) The delivery of distinct and separate data streams, delivered on the same or different channels and media, each with minimal, limited, or even substantial usefulness in and by itself, that can be overlaid logically or physically to reconstitute the

identifying data stream and display. Separate display devices can be used to create a composite image or they can be overlaid to physically separate display devices to reconstitute a useful composite display.

[119] The objective is to create security for the single computer or extended network. When an intruder penetrates preexisting firewalls and other security systems, the data object and streams, digital documents, and digital files which will be valueless and prioritized data objects rendered unidentifiable, the penetration is valueless because the critical strategic information has been exported to a vaulted storage. Competitors or hackers, who learn that a computer or network is protected by the system and method, might decide to attack another target instead. This is comparable to a situation in which a bank robber, who finds out that the bank vault is empty, will most probably look for another bank.

[120] The system and method has a menu of different options including the ability to extract: (a) All existing databases on the computer or network. (b) All newly loaded, mounted, or integrated data to the computer or network. (c) All plug-in memory devices (temporary or permanent) containing data. (d) All new and imported data to the computer or network. (e) All new work and output created by the computer or network. (f) All data being transported in/out of the computer or network including electronic mail. (g) All data being transmitted in/out of the computer or network including electronic mail.

[121] The system and method releases the extracted data streams, subject to a controlled-release mechanism and process. The release mechanism is contingent on parameters including; rights to access specific contents, timing criteria, security restrictions, and preset policies. The release of the extracted data objects permits restitution of the source data stream in variations of the source that

are full, partial, or modified representations of that source data stream. The release provides for various levels (through user configuration) of separation between the modified source data stream and the extracted data streams. The system enables the maximum grade of security by means of the option of a visual merged projection of said different data streams, while maintaining a strict physical and logical separation between the data streams.

Basic Reconstruction

[122] FIG. 1B generally diagrammatically illustrates the major features of a reconstruction routine or system. The user, typically at a computer terminal, inputs a reconstruction request 120. The system first executes a security clearance protocol routine 122 in order to determine whether the user has the proper security clearance. The security clearance may be thought of as a security clearance control. If multiple users are permitted access to the documents and those multiple users have different security clearances, the security clearance protocol determines the level of security clearance and, hence, the full or partial reconstruction of the plaintext. The security code input by the user is checked against a security code database or list 124. Clearance is provided in step 126. The location of the map and, hence, the location of the remainder data A-com 108 and extraction is provided to the user's computer in step 128. This may include obtaining a copy of the map 130 showing the location of memory segments in (a) the local computer; (b) the LAN or WAN; or (c) the Internet storage sites. The storage segments are A-com 108 and B-ext 110. The common or remainder data is downloaded or transferred or made available to the user's computer as shown at the output of map location and data step 128. Typically, the extracted or security sensitive data from B-ext is downloaded. As described hereinafter, the data can be reconstructed as a complete electronic document in function 130 or may be reconstructed only as a visual reconstruction in step

[redacted]

132. Visual reconstruction is discussed later. Function 130 operates as a compiler to gather the extracted data and remainder data into a single plaintext document. If the data object represents sound or audio signals, reconstruction and play back may require a speaker output in function block 130. In a telecommunications implementation of the present invention, the input would include a microphone or audio detector (supplemental to the input device for document 100), an analog to digital converter (possibly with a voice to digital converter), the filter, extractor, storage facilities at least for the extracted data, and at the output of the system, a converter to audio and an audio announcer. The recipient of the secured data stream or message would be required to clear a security clearance and possibly obtain a decoding key prior to listening to the entire, decoded message. The key and the security data is separately downloaded to the recipient's device.

[123] If remainder data in A-com memory 108 and extracted data in B-ext computer memory 110 is encrypted, the reconstruction process includes a decryption step. Encryptors and decryptors are relatively well known by persons of ordinary skill in the art. Further, the filter 102 (FIG. 1A) may include some encryption routine operating on the data object (plaintext) during the filtering. A simple encryption may include substituting "dummy" text or images for the security words and keeping a pointer to an encryption key document mapping the security words with the dummy words. The filter may be stored or may be destroyed at the option of the user. Storage of the filter impacts the degree of security of the entire data system but storage of the same filter enables the user to reuse the filter at a later time. Encryption of the stored filter increases the security of the data. Creation and storage of map in memory 112 also impacts the degree of security of the system. However, if the filter 102 is destroyed and all copies of the map are destroyed on the user's computer originating plaintext document data 100, and the map is stored offsite in a third computer memory

[redacted]

location 112, this offsite map storage may enhance the degree of security of the data. The originating computer processing plaintext 100 may be scrubbed to remove all reference and copies of the plaintext, remainder text, extracted data map storage data, etc., i.e., a deletion routine may be employed on the data input computer.

System Configurations

[124] FIG. 2 diagrammatically illustrates a personal computer or PC computer system 140, a second PC or computer 142, and a third PC -3. PCs 140, 142 and PC-3 are connected together via a network 145(LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to a telecommunications system 148 which leads to Internet 150. The Internet is a global computer network. Internet 150 is coupled to a plurality of servers, one of which is server 152. Server 152 may be designated as an application service processor ASP. Internet 150 also includes various computer memory storage devices such as computer storage I-com 154, computer storage I-ext 156 and computer storage map 158. Computer storage enabling the store of extracted data includes a security level clearance module 157. Similarly, map computer storage 158 includes security level clearance module 159.

[125] As stated earlier, the present data security system can be implemented on a single personal computer 140. In this case, different memory segments or hard drive 168 may be used for A-com and B-ext. Typically, PCs include a keyboard or data input device 161, a display 163, a central processing unit CPU 165, a video board 167 having video board memory 169, a fixed disc hard drive 168, a RAM 166, and input/output device 164, a removable memory media floppy drive 162 and a removable compact disk (CD) read-write (CD-RW) device or drive 160. The system may

include other removable disk drives, tape drives, or flash memory units. Internal units CPU 165, video board 167, hard drive 168, RAM 166 input/output device 164, floppy drive 162 and CD-ROM device 160 are all coupled together via an internal bus 171. Bus 171 represents a plurality of buses as is known to persons of ordinary skill in the art.

[126] One methodology of implementing the present invention utilizes distinct memory segments which may be designated in one or more of the following: hard drive 168, memory in a removable disk in floppy drive 162, memory in a removable CD disc in CD-RW device 160, and, to a very limited extend, RAM 166. In this manner, the user may select, generally at the outset of the process, that the extracted data memory storage B-ext 110 be stored on a floppy (removable memory) via floppy drive 162 or a CD via CD-RW drive 160. The user can then simply remove the floppy or the CD and carry it with him or her. To reconstruct the data, the operative program, generally discussed above would have access to the floppy or the CD and particularly the memory location of the data on the floppy and the CD in order to reconstruct the entire plaintext document 100 (see FIG. 1A). Alternatively, different portions of hard drive 168 may store A-com and B-ext. Of course, the computer system may utilize tape drives and memories or flash card, programmable memory.

[127] In a local area network or wide area network implementation, PC 142 includes memory similar to memory units described in PC 140 and a memory segment may be set aside in PC 142 separate from the common data or remainder data storage typically placed on hard drive 168 in PC 140. As a further expansion of the present invention, the extracted data (that is, the high security data), may be stored on computer storage I-ext memory unit 156 via Internet 150, telecommunications system 148 and router/server 146. In this manner, the common data or

[redacted]

remainder data is stored on hard drive 168 and the highly sensitive data is stored off site in a secured location. Access to that secured location may be limited via security layer 157. If the user implements an encryption system (see encryption e 118 in FIG. 1A), the extracted data is further secured by the encryption during the transfer from computer 140 through network 145, router/server 146, telecommunication system 148, Internet 150 and ultimately to computer storage I-ext 156.

[128] The present invention may also be embodied utilizing an Application Service Provider on server 152 and in a client-server network.

[129] An implementation of the present invention over Internet 150 most likely includes the use of a uniform research locator or URL for map memory computer 158, computer storage I-ext 156, computer storage I-com 158 and ASP server 152. In a client-server environment, server 152 acts as a server generally commanding the operation of client computer 140. Of course, persons of ordinary skill in the art recognize that the server may be located on the local area network 145 rather than being interconnected with Internet 150 as shown in FIG. 2. The claims appended hereto are meant to cover the alternative embodiments.

[130] As an example of a client-server or web-based implementation of the present invention, the user at computer 140 may define the filter 102 as described above, and input data (plaintext) via keyboard 161 or load plaintext data from floppy drive 162 or CD-ROM drive 160 into RAM 166. In any event, whether the plaintext data is input via keyboard 161 or copied or accessed from floppy drive 162 or CD-RW drive 160, the plaintext data is filtered as discussed above in connection with FIG. 1A. Prior to filtering, it would be appropriate for the user at computer 140 to identify where the remainder data or common data will be stored and where the extracted or high security data would be stored. A simple program may automatically select the secure store location.

The system is sufficiently flexible to enable the user to select local storage on different memory segments of PC 140 (hard drive 168, floppy drive 162, CD-RW drive 160) or be flexible enough to enable user at computer 140 to designate off site storage of the high security data (extracted data) and/or the common or remainder data. An automatic store routine may only require the user to accept or reject to preferred first security level, second security level and higher security level stores. The off site data storage process may include activating server 152 and enabling the server to take over the process directly from user 140. In other words, the user at computer 140 could call up the URL of the server 152, the server could request certain user information (user name, password), and would request data from the client computer to establish the filter pursuant to input selected by the user. The client computer may (a) filter the plaintext thereat or (b) send the data to the server for filtering. The server could store data either locally on computer 140 or remotely at computer memories 154, 156. After storage of the data at any of these locations, the server 152 may establish a map and store the map in memory location 158. Of course, remainder data (cleansed, plaint-text data)and the map may be stored at ASP 152 or client computer 140. The map, if stored at map storage 158, may be downloaded to the user at computer 140. The filter may be stored at computer 140 or may be stored at a secured location on server 152. Alternatively, the map could be destroyed on user computer 140. The filter could also be destroyed on user computer 140. Of course, the filter could be stored in a fourth remote location (not shown), different from I-com 154, I-ext 156 and map computer memory 158. Storage of the map and decryption keys is a critical, high security task. Appropriate security measures should be utilized to protect those items. Local removable memory storage on disc in floppy drive 162 or disc in CD-RW 160 may be reasonable. All traces of the map, the filter, the encryption key, the extracted data, and possibly the remainder data may be scrubbed

or deleted from all computer memories (by write-over or disc reformat routines) other than the "com" and "ext" storage sites. Deletion of all URLs, links, x-pointers, etc. is also recommended for high security applications. Deletion systems are known to persons of ordinary skill in the art. For multiple security levels, multiple web site for storage of cleansed plaintext, first, second, third and higher security level extract text is preferable. Where the community of interest has access to the targeted and protected data via the Internet, multiple secured storage locations, multiple stores for filters, for encryption keys and for maps locating the secured stores is provided by multiple storage locations distributed throughout the Internet.

[131] To reconstruct the document, the user at computer 140 would be required to call up the URL of server 152 and input the appropriate security code. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations I-com 154, I-ext 156 and map memory 158. The system compiles the entirety of the plaintext document by gathering the dispersed components thereof or compiles partial reconstructious for different levels of security. By implementing different security levels, the system is dynamic enough such that server 152 can easily locate the various extracted data levels based upon various security codes representing different security levels, as those codes are input by the user at computer 140. Multiple security codes, at the inception and during the process, may be utilized. The user may be required to input security codes at multiple times during the reconstruction or compilation process.

[132] It should be noted that computer storage 154, 156 and 158 may be located on the same computer or may be located on different computers spread throughout the Internet. If the storage units are different computers spread throughout the Internet, computer storage 154, 156 and

158 would each have their own URL or Uniform Resource Locator. In any event, during reconstruction, the server 152 gathers the information and downloads the information into RAM 166 of computer 140. This download may include a first download of the common or remainder data from I-com 154. At a separate time, which may or may not include a decryption routine, the extracted from I-ext 156 is downloaded. Preferably, other than inputting initial security codes and any required or desired intermediate security codes, the system operates automatically without further input from the operator at client computer 140. The download of both data sets may be simultaneous in that the download is not humanly perceivable. This is especially true if storage in different memory locations in PC 140 is utilized.

[133] The role of server 152 may be expanded or reduced dependent upon the desires of the user and the degree of security necessary. For example, server 152 may only enable separate storage of extracted data in I-ext 156. In this limited role, server 152 would require the input of a proper security code and clearance prior to identifying and enabling the download of extracted data from I-ext 156.

[134] In an expanded mode, server 152 may be involved in filtering the data, extracting the security sensitive words, characters , icons or data objects to obtain extracted data and remainder data thereat, separately storing the extracted data from the remainder data (extracted data being placed in computer memory I-ext 156 and remainder data being stored in common remainder data memory I-com 154) and then permitting reconstruction via separate or combined downloads of the remainder data and the extracted data into computer 140.

[135] The innovation is a system and method for automatically or manually controlled selection, extraction, storage, and release of selected and prioritized information. The system extracts

selected information from data streams, in computers, computer networks communication devices, and networks, as well as electronic mail systems. The system and method can reside on a single computer, be distributed across multiple platforms, be distributed across multiple networks, or reside as a remote process (known as a hosted application service process in the state of the art).

Reconstruction Techniques

[136] FIG. 3 diagrammatically illustrates a system diagram for various reconstruction routines. A complete reconstruction is shown as security level path A. This involves an electronic integration of plaintext in step 202 resulting from the complete electronic reconstruction of document 100. For example, a merge may occur between the extracted data and the remainder data or common text data. The document is completely compiled in this process. Placeholders in the remainder document are utilized to locate and insert the extracted data. Most likely, there will be no process controls imposed on the integrated document as shown in step 204. In other words, if the user at computer 140 has the proper security clearance, he or she could download or recreate the entire original source, plaintext document and the user would be entitled to edit the document or change it in any way or copy it and reproduce it.

[137] The second level of security, path B, results in storage of the common or remainder data in a different memory location on the hard drive 168 as compared with the extracted data. This is noted in step 206. Another words, in a simple example, hard drive 168 or RAM 166 would hold a copy of a remainder data document and another copy of the extracted data document, that is, two separate documents. Since two documents are available in RAM 166 or hard drive 168, these documents are stored in different locations in the memory. In step 208, a map showing the memory location of the common or remainder document and the extracted data document is provided to

[redacted]

computer 140. Step 210 commands the processor CPU 165 in computer 140 to interleave the extracted data with the common or remainder data in the video board memory. In this process, the extracted data would typically have placeholders for the missing remainder data. Otherwise, control codes to locate the extracted data into the remainder data would be executed by CPU 165 to properly place the extracted data into the "visual space" of the placeholders in the remainder data document. The extracted data document may have placeholder for the remainder data. Some type of register between the two image documents may be necessary. The compiler, in this embodiment, gathers the document elements and visually compiles and presents the plaintext to the user.

[138] FIG. 3A diagrammatically shows that video board memory 169 is loaded with remainder or common data 1 and a different location of the video memory is loaded with extracted data 1. The next video memory location is loaded with common data 2 and then a different video memory location is loaded with extraction data 2. Since the refresh rate of computer monitor 163 is fast, the display 163 will show the common or the remainder data and then show the extracted data such that the user could not humanly perceive a difference in the document. However, the user could not copy the document from display screen 163 (a "screen shot") since the document is never electronically integrated into a single document. There is only a visual presentation of the combined document by interleaving the extracted data with the common or remainder in the video memory 169. Step 212 notes that the user may be limited in his or her ability to process, edit and store the reconstructed and presented plaintext document.

[139] Security level path C recognizes in step 214 that the data is stored in different memory or computer locations. In this situation, two video boards, video board A and video board B are shown as board 216 and 218. Video board 216 drives display monitor 220. Video board 218

[redacted]

drives display monitor 222. Display screens 220, 222 are overlaid atop each other. Video board 216 is fed with common or remainder data from the remainder data store (see I-com store 154 in FIG. 2) and video board 218 is fed with the extracted data from the extracted data store, for example, I-ext store 156. In this manner, as noted in step 224, the user is presented only with a visual presentation or compilation of the plaintext. Since there was physical separation between video monitor 222 and video monitor 220, there is no electronic integration at all of the plaintext document. Hence, the ability for the user to do any significant editing on the plaintext document is blocked or prohibited because the user only has access to either the data on video board 216 or the video board 218.

[140] Security level path D shows that the extracted data may be parsed or further separated based on a plurality of security clearances in step 226. Step 228 recognizes that the system can repeat process and security process paths A, B and C only with portions of the extracted data presented to the user based upon the user's security clearance.

General Operation

[141] FIG. 4 diagrammatically illustrates the major components of a flowchart for the data security program. It should be noted that this flowchart may be truncated to limit user selection of certain items. The system would be pre-set to contain these features. Step 230 initializes the system. Step 232 enables the user to designate various levels of security for the activity which he or she will soon engage. The system, in step 234, enables the user to define the levels of security parameters. The following Security Table gives some examples of the type of security that may be available to the user.

Security Table

to whom

to where

when (time of day, day of week, month, floating but predetermined time frame)

why (purpose, match purpose to other security parameters or to certain predetermined criteria)

how (through what medium (LAN, WAN, Internet, direct dial link), download to what site or destination)

how long (duration) the reconstruction process will be permitted per each security clearance level

how much (different security levels enable reconstitution of documents and data with different amounts of secure data therein)

timing systems may require synchronization for a standard clock (i.e., atomic clock)

[142] As an example of a truncated or pre-set program, a client-server system over the Internet may have URLs designating storage sites and an ASP 152 (FIG. 2) controlling storage. In this pre-set system, the user does not select the sites. The sites may be randomly selected by ASP 152. The ASP may use artificial intelligence AI to locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc. Higher security alerts trigger the AI configured storage locator and facilitator to locate memory stores in higher secured places. These higher security facilities may be more costly, may be located in more stable countries or on more stable servers and may have greater degrees of encryption capabilities.

[143] The user, in step 326 can designate the location of the filter, the common storage area for the remainder data, the extraction data storage and potentially multiple data storage areas or segments. The user may enable an AI filter design. Step 238 permits the user to engage or disengage encryption and, if engaged, establish the degree of encryption for the system. Step 240 enables the user to define the parameters of the filter. The user can retrieve a preexisting filter or may define a new filter for each data security session. These filters may consist of dictionaries or any type of compilation of words, characters, icon, data objects or pixel formation or any indication that can be perceived by the computer system. Granular extraction of data elements in a data object may be permitted. Step 242 recognizes that the user either inputs a preexisting plaintext document or types data into the system. In any event, the plaintext document is fed through the filter. Step 246 extracts the security data from the input document. Step 248 stores the extracted data. The extracted data may be encrypted prior to storage. Step 250 conducts an error check on the extracted data. This error check is helpful in discerning problems in the storage of the data prior to closing down the data

[redacted]

security system. Step 252 stores the common data or the remainder data. Step 254 conducts an error check on the common or remainder data. The decision step 256 determines whether the user has selected a "destroy filter" command. If not, the filter is stored with or without encryption in step 257. If YES, the filter is destroyed with a deletion routine. Typically, deletion is complete erasure of all traces of the file including, in high security systems multiple write-overs or disc reformatting. Step 258 stores a map. The map may be stored locally or remotely as described earlier. The system ends in step 260. All traces of these data elements or objects may be swiped clean or removed from whatever computer system generated the data objects or processed them, other than the memory storage locations. Deletion of data also includes the concept of deletion of data transmission paths, URLs, storage site locations and all temporary memory stores. Deletion of file location in the root directory of hard drive 168 of computer 140 is preferable in high security systems.

[144] FIG. 5 diagrammatically illustrates basic flowchart features for the reconstruction process. Step 302 accepts a request to reconstruct the secured data. Step 304 queries a local map and the security system or protocol. In a preferred embodiment the user would have to input several passwords, one of them being a local password on computer 140. A local map which may be accessed only through the password, may simply identify the URL of server 152. Decision step 306 determines whether the local password is acceptable. If not, and error step is indicated in step 307, the attempt to log on to the security system is noted in step 309 (an audit trail), and the system either branches to repeat step 311 or bars the user from further activity in step 313.

[145] Returning to decision step 306, if the password is locally acceptable, the YES branch is taken and the system executes step 308 which releases a reconstruction request to the common storage facility I-com 154 or A-com 108 (FIGS. 2 and 1A-B). The system in step 310 logs the user in, as well as time and date and the data regarding the request. In step 312, a download from the common data storage is provided to RAM 166 or hard drive 168.

[redacted]

[146] In step 314, a query is made to obtain the remote map from the remote security system. The decision step 316 indicates that the user again successfully inputs his or her security code. If not, error routine 317 is activated, the password failure is noted in step 319 (an audit trial), and the user is given an opportunity to repeat in step 321 or is barred or prohibited from further activity in step 323. If the user has correctly input the security code, the system in step 318 releases the keys (to decrypt) and the map and releases the reconstruction request to the remote storage for the extracted data. This could be computer storage I-ext 156 or computer storage B-ext 110. In step 320, the user's access to the extracted data is logged in along with the time and day and type of data request. In step 322, the system downloads the extracted data into RAM 166 and/or hard drive 168 of computer 140. In step 324, an error routine is operated on the extracted data in order to insure that the extracted data properly matches the common or remainder previously stored. Decision step 326 determines whether the error routine properly generates the correct count or output. If not, the system in step 327 indicates an error, in step 329 the system deletes the common files and the extracted files and the system in step 331 logs in the failed attempt. If the error checking routine on the extracted data is acceptable, the YES branch is taken from decision step 326 and the system, in step 328, proceeds to display the plaintext document or to integrate the plaintext document pursuant to the security clearance initially input by the user. Step 330 ends this process. The end process may entail encrypting the data again and swiping clean all traces of data objects from the memory stores and computer handling units. Of course, every use of encryption requires decryption of the data prior to reconstruction.

[147] The system may incorporate various types of security systems or routines.

pass word

pass phrase

multiple choice questions and answers

[redacted]

initial, intermediate and subsequent security clearance routines

biometric security routines (voice, fingerprint, signature, eye or retina scan)

[148] The reconstruction routines may be interrupted or the security system automatically activated or initiated upon the occurrence of externally generated triggers or upon certain predetermined conditions or conditional events. Limited extraction, security clearance, release of data and reconstruction limits may be imposed. Artificial intelligence (AI) engines, inference engines or neural networks may be implemented to vary the permitted level of reconstruction via the security clearances. In other words, the AI system, as applied to reconstruction, may, relatively independent of the filter and storage processes, increase the necessary security levels permitted to access and generate full or partial plaintext recreation.

[149] The display systems 220, 222 in FIG. 3 include CRT monitors, LCD screens, projection screens and combinations of those systems.

[150] The audit trail to monitor reconstruct and reconstruction attempts may include adding a time/data stamp to the remainder data and/or the extracted data prior to storage and a cross-check to the audit trail log during the reconstruction process.

[151] Placeholders in the remainder document may be:

blank spaces

data symbols or elements "---" or "xxx"

false data

clearly erroneous data "ABC Company" or "Baker"

chaff or hash marks

messages

bar code

serialization data

alerts

links to other data objects

null set indicators "[ ]"

URL or website addresses

[152] It is believed that the present invention is faster, during reconstruction, than standard encryption techniques, on the order of 100 to 1,000 faster.

Automatic Features

[153] The system and method described herein may operate substantially automatically, that is, without operator intervention, other than the security clearance function. The clearance function does require some type of operator authentication prior to retrieval of the extracted and remainder data.

[154] The system and the method may operate automatically in that the plaintext or originating data could be identified by a party desiring security. The system could obtain that data from any data input device (hard drive memory, floppy drive memory, flash card memory, personal data assistant (PDA), or any other type of data input device), filter the data, separate the extracted text or the remainder text, encrypt (or not encrypt) the data, separately store the extract and remainder data (all automatically, that is, without operator intervention). Hence, it is not necessary that the system operate with significant operator or manual intervention. Of course, the system may also operate on a plaintext document or data object that is being created "in real time" by an operator and keyboard, mouse or other type of data input device.

[155] The automatic operation of the system and the method can be caused by a triggering event. This triggering event may be a security attack (generating a trigger to start the gathering of plaintext, filtering, extraction and storing) or may be any other type of trigger such as a building

[redacted]

burglar alarm, door alarm, fire alarm, or virus detection algorithm trigger. The event may be a time of day, week or month. It may be n seconds after the user stops typing on a keyboard. It may be a timed back-up feature.

Multiple Security Levels

[156] Multiple filters may be utilized in the system and in connection with the method. These multiple filters may be useful in the operation of the system with a plurality of security levels. Each filter could filter out different levels of security sensitive items and each bundle or group of security sensitive items (from each distinct filter) could be stored at different computer storage locations. Multiple filters, multiple security levels and multiple storage areas may also include multiple encryption routines and decryption routines. Encryption and decryption routines can be related to the level of security of a particular group of data.

[157] Multiple maps may also be provided for singular or multiple storage of extracted data and remainder data. These maps may or may not indicate the originating point of the data. Maps can be parsed such that an intruder, upon discovery of a single map or map portion, could not locate the storage locations of all piece of the extracted data and remainder data. maps may also be encrypted. The map may also be stored at a distinct map store location.

[158] The concept of partial reconstruction also includes the concept that a portion of the plaintext would be reconstructed and the unreconstructed portions of the plaintext could be encrypted or could show blanks or other symbolic indicators. See the placeholder table above.

[159] Partial reconstruction of the plaintext also includes a concept that the security sensitive items or materials may be subject to different types of encryption. Hence, a single plaintext document may have multiple levels of security and multiple levels of encryption wherein each encryption has a different level of security assigned to it.

[160] The present invention can also be configured to provide a computer network which transparently establishes and manages the separation of user-based communities of interest. The separation is accomplished by extraction pursuant to security levels, dispersion of data into secure storage facilities (memory stores) and reconstruction based upon the assigned security level. A low level security clearance results in only partial reconstruction of the plain text or source document. These user-based communities of interest are a plurality of users each having respective security clearances. As described above, each successively higher level of security clearance permits the user to see greater degrees of reconstructed plain text obtained from the extracted data stored in extract stores and the remainder data from the remainder stores. By integrating encryption (and necessarily decryption), separation of user-based communities of interest are established such that the users in a particular community are permitted access to some or all of the plain text data based crypto-graphically separated communities and need to know security levels.

[161] FIG. 6 is an exemplary computer network diagram showing various user communities. The telecommunications network 402 is connected to the server application server provider ASP 452 and to various networks and personal computers or PCs. the PCs may be computer work stations. Network A 404 is coupled to telecommunications network 402 via an input/output unit 406. Network A is coupled to various PCs identified in FIG. 6 as PC-4, PC-5 and PC-6. Of course, Network A could be coupled to other PCs not illustrated in FIG. 6. As described earlier, server 452 can facilitate remote or offsite storage of extract data and remainder data in store 1, store 2 and/or store 3. Further, the map showing the storage location may be encrypted and stored in any one or more of these stores. Also as described earlier, the memory in one of the PCs, for example PC-4, PC-5 could be utilized to store extract data and remainder data from PC-6 and PC-6 can be configured as the input data computer. Hence, the present system and methodology encompasses the concept of local storage and remote storage. On the local level, the storage begins

by storing the extract data at different locations in the hard drive of the PC. The next level higher is storing the extract data in removable computer media such as floppy disk, removable tape drives, CDs etc. associated with the PC accepting data or associated with a server on Network A. The next higher level of extract store is storage of the extract data on a server or other computer in a particular network. If PC-6 is designated as the input computer, the extract data may be stored on PC-4. Of course, PC-4 could be designated as the server for Network A.

[162] PC-7, PC-8 and PC-9 are coupled to telecommunications network 402. Network C 408 and Network B 410 is coupled to communications network 402. The lines, one of which is line 409 extending from Network C 408, represent a plurality of computers or workstations coupled to Network C. Line 411 represents a plurality of workstations or computers coupled to Network B 410. In an e-mail implementation of one embodiment of the present invention, PC-7, PC-8, etc. may represent computerized devices accepting e-mail (personal data assistant, pager, cell phone, etc.). The sender and the e-mail addressee may utilize simple computerized systems to communicated via e-mail. Further, the network may be any telecommunications network including wire, cable, cellular, wireless, satellite, IR or RF systems.

[163] FIG. 7a diagrammatically illustrates a flow chart showing the key component steps for the multiple layer security program for the community of users. The "community of interest" system described herein enables persons and organizations at the same security level to share data on a peer to peer level. Further the security system may operate automatically, with respect to extraction, storage and reconstruction, such that the peer to peer dissemination of data objects is quickly and readily available to all at the same or higher security levels. Step 420 initializes the program. Step 422 enables the user, administrator or system operator to designate multiple levels of security, that is, multiple words, characters, icon, data objects, or whatever, for each security level and further to define encryption for each security level. The designation step 422 also includes

identifying the communities of interest and the particular security level and security clearance for each community of interest. One example of various security levels for communities is set forth below in the Community Security Level Table which is keyed to the computer network diagram of FIG. 6.

Community Security Level Table

Security level	Community Group
High	PC-7; PC-8
Medium high	all high group plus Network B
Medium	all above plus Network A
Low	all with nominal clearance
Special set medium	PC-7; PC-9; Network B

[164] Further, designation step 422 will include identifying the words, phrases, icons or data objects subject to security concerns and the potential location of the extract data and, if necessary the remainder data and the degree of encryption. The following Selection Table provides some examples.

Selection Table

Level of encryption/storage	type or category of word or phrase; input specific word, phrase
High, web-based storage	dollar values, names of streets, countries, "Smith" and 5 words about "Smith," "avocado"
Medium high, remote storage	all addresses, all names
Medium network storage	all family names, all client names
Low, encrypt and separate store in local memory	all items not in dictionary

[165] As an example of various encryption methodologies, the following Encryption Table is illustrative.

Encryption Table

DES, random pad A ("r. pad A")

Huffman, r. pad B

Crypto API, r. pad 7

Two fish, r. pad C-2

Blowfish

RC4

Skipjack

Ghost

[166] In FIG. 7a, step 424 executes or enables the security program with multiple filters, multiple encryption levels and multiple storage levels. Each one of these filters, encryption levels and storage levels correspond to the security level for the various communities of interest. Step 425 responds to an inquiry from a user to reconstruct the document. Step 426 accesses the user's security clearance and the particular inquiry. Decision 428 determines whether the inquiring party is entitled to full or partial access to the source document. If not, the NO branch is taken and the system, in step 429 adds placeholder substitutions. Step 429 may be optional. If YES, the system reconstruct pursuant to the clearance level in step 430. The following provides an example of multiple level encryption utilizing placeholder substitution.

Example: Multiple Level Encryption

Applicants must be _____ zzxx xx _____xxx _____ _____ _____ citizens and have a high school diploma or equivalent. They must possess a valid subsubsub driver's license and qualify for top SUBWORD_____ clearance.

[167] With this multiple level encryption, substitutions may be utilized "subword" to indicate to the user with a less than superior security level that a certain word, term or phrase has been extracted and stored by he or she is entitled to know that substitute word, term or phrase has been inserted into the plain text document. Of course, any type of substitution character may be used for the placeholder.

[168] In step 432, the system displays the plain text in a normal format or utilizing a split or bifurcated video memory or utilizing overlay display screen. FIG. 3 and the description of that figure set forth above describes the normal display in steps 202, 204, the split video memory display in steps 206, 208, 210 and 212 and the overlay display system in steps 214, 216, 218.

[169] The system, in step 434, monitors and logs the location of the user making the inquiry, the type of inquiry, the time, day, date, clearance level and access level and logs all modifications to the plain text source document. One example of the log is set forth below in the Security Report Table.

Security Report Table

Privacy Scrubber Report

source file: path\filename

scrubbed file: path\filename-scrub

source file: date, time, size

process: date, time

user: name

system: name

Recovery File

(a) storage location, type of encryption, random key

(b) storage location B....

[redacted]

(c) store C .....

(d) store D .....

[170] Step 436 enables the security program and parses and extracts the data per the security program, filters the data, extracts it and codes it disperses it and stores it as discussed above. The multiple layer security program ends in step 440.

[171] The following Security Level Access Placeholder Table is another example of the type of placeholder substitutions that may be available. The example in the Security Table Access Placeholder Table may be used in conjunction with step 429.

Security Level Access Placeholder Table

[security level 2] intelligence located [security level 4] 20 miles from [security level 4]. He is using the name [security level 4], and dressed as a [security level 4] preacher. With him are his lieutenants, [security level 4] and [security level 4]. He is communicating with the international media through Mr. [security level 4], who resides at [security level 3], [security level 4], [security level 4]. Telephone is [security level 1] and Facsimile is [security level 1].

[172] It should be noted that in order to reconstruct some or all of the plain text source data, some or all of the subsets of extracted data from the extract stores will be utilized dependent upon the respective security level of the inquiring party or user.

Sharing Data with Different Security Levels - Data Mining

[173] The present invention can be configured to overcome obstacles to intelligence sharing and data sharing between parties by enabling the parties to identify granular critical data and control the release the granular critical electronic data subject to a sharing arrangement with other parties. In some instances, the controlled release process is designed to implement an agreed upon plan to share secured data based upon arms length negotiations between the parties. The invention enables a party to release specific granular data such as a name, address, or date without releasing the entire

[redacted]

"classified" document. In a commercial context, this is akin to data mining in that the inquiring party seeks limited data (not the entire data file, record or document) and is willing to pay for the "mined" data. As an example of a security intelligence system, a local police chief may release granular critical data about a suspect to a federal agency, when in return the federal authority will release further intelligence "mined" or obtained for the secured data storage, about the suspect. The controlled release of data from the higher security level party (the FBI) may be an intelligence document or a granular part of it (a partial reconstruction provided to the local police). The rational behind this implementation of the invention is that there are many obstacles for sharing intelligence and information. There are even many more hurdles when it comes to sharing of raw intelligence. The invention creates a leveled playing field in, which the different parties must share and exchange information in order to achieve their objectives.

[174] The invention can be configured to resolve the major challenges facing government by enabling sharing of information between its different organizations in relationship to fighting terrorism. The invention for example can enable organizations, connected to the Homeland Security Department, to search data bases of various other government, state and local organizations, eliminating the fear of the "source" organizations, owning or controlling the source or plaintext documents that their proprietary data or granular critical data is released without their specific permission. The invention enables open negotiations between the parties regarding what data to release and for what consideration. When several organizations are seeking access to a specific document, the invention and can allow a controlled release of different granular data to different parties for different considerations and benchmarks.

[175] The invention's mechanism of controlled release of the located document/data enables other parties to search their documents without the fear that sensitive information will be released to the searching party. This invention is designed to foster sharing of documentation

between different parties, taking into consideration the need to limit the access of other parties to the total content of the owner's document.

[176] The invention is a machine and process and its purposes and advantages may be as follows: (a) To automatically control selection of data objects within a data stream and release them in a controlled method only to authorized parties. (b) To automatically separate data objects within a data stream into two or more digital data streams according to the importance and categorization of contents, through extraction and removal of the prioritized content and its replacement by appropriate placeholders. (c) To automatically control selected contents in E-mail, and enable its release in a controlled method only to authorized parties. (d) To enable users to leverage the growth in computer and telecommunications connectivity and electronic commerce by reducing security risks. (e) To enable users to release documents, digital files, and data streams into closed and opened digital networks with the confidence that important, identifying, and critical contents in that documents, digital files, and data streams is secure and will be seen only by authorized parties. (f) To enable real time simultaneous customization and personalization of selected contents within a data stream to different parties, allowing instant display of the selected content or part of it based on, and tailored made to the status of the user or receiving party. (g) To secure the important and critical contents of a document or digital file by transporting said contents into a separated data stream and removing said data stream to a removed storage memory, while eradicating any copies, temporary caches, or traces of the removed extracts on the original computer or machine. (h) To enable instant return transfer to the display or to another display all or part of extracted content instantly with verification of authorized user. (i) To create a projection of the original document, digital file, data objects within a data stream, or variations of it through combined projection of the splinted data streams, while maintaining separation between the data streams. (j) To create an alternative method for security, instead of encryption, which is secure, cost effective, less time-consuming, and flexible.

[redacted]

(k) To enable automatic timed removal of specific content items, automatically or manually selected from a document, digital file, or data objects within a data stream. (l) To enable an automatic timed reconstruction (reconstitution) of the said document, digital file, or data objects within a data stream.

[177] Another object of this invention is as a system and method for automatically creating customized and personalized versions of a document, data object, or data stream. In real time, simultaneous versions of the original are created and altered, then disseminated based on the status of the different users and their access privileges. The system and method enables content management and control by automatically locating content items prioritized by importance, transporting them to a secure memory, and releasing them under explicit controls or preset rules.

[178] Another object of the invention is as a system and method for control, analysis and management of important and prioritized information within documents, files, data object, and data streams. The system and method, enables the processing of all data objects at the time in which they are created or imported into the system. The early stage processing, enables early stage inventorying of prioritized contents as well as early stage pattern recognition. Extracting critical information, such as credit card numbers, last names, first names, social security numbers, phones numbers, transaction dollar amounts and addresses, enables the system and method to aggregate data in categories and analyze the data in different optional methodologies including pattern recognition.

[179] Another object of the invention is as a system and method for comprehensive monitoring of various activities including business activities in real time. With this level of detail, the system and method becomes a management information tool and information/data command and control center. The said system and method can include an alert system, which in effect creates a real time apparatus for command and control of the systems activities. In real time, and at any point in time, the user can get a comprehensive view of different activities including: (a) How many transactions are being processed, their content, their context, identity of the involved parties identity, their profiles, and

[redacted]

the personnel involved. (b) How much money is being transacted. (c) When, in terms of dates, relevant to the transaction. (d) Where, in terms of geographical location, the transactions are taking place. (e) Where, in terms of geographical location, monies or goods are being transferred. (f) Which departments in the organization are involved.

Multilevel Security through Sanitization with Reconstruction of Sanitized Content

[180] A multilevel security (MLS) technology secures the targeted, filtered content with extraction and dispersal to storage, bypassing the use of classification labels, in order to achieve stronger security of the source document or data. During the process of developing security technologies for defending critical infrastructure, it was discovered that the business model was too complex and there was a need to redefine and create new systems and methods for doing business. As a result, the present invention provides a system and codifies methods and business processes to automatically identify, extract, store critical data (as an input security system) and permit reconstruction of critical data only in the presence of certain security clearances (as the output of the security system).

[181] The invention is a method and process to establish a stronger multilevel security (or MLS) architecture and product, than is currently available. The invention introduces multilevel security through sanitization of critical content of a source or plaintext document (or data object) with the unique ability to reconstruct all or part of the original document in conformance to the classification level of the user. A user with top classification may view the entire document, while a user with a lower level classification will view a sanitized document, tailor made automatically for his clearance level. The invention secures the targeted filtered content of a document, file, or data stream, through extraction and dispersal to storage, bypassing the common use of classification labels in order to achieve stronger security. The invention enables secure document storage and secure message transfers between users and networks with different security classification levels while protecting the information on a need to know basis.

[182] Currently multilevel security MLS systems are using multiple PCs for each user, and using physically separate systems for processing data at each classification level. The inventive system, in several embodiments, eliminates the need for the use of multiple computers. All the documents in the user's PC are automatically secured with a granular classification process generally described above with identification of special security data, extraction from the source document or data object, and then separate storage of the security data. The classified granular content is dispersed to different secure, distributed storage locations. The classification level of a user will determine his right and ability to access and release the stored critical extracted content from the various storage locations for reconstruction. A user with top classification will view the entire document, while a user with a lower level classification will view a sanitized document, tailor made automatically for his clearance level.

[183] Types of government security levels are: Top Secret (TS); Secret (S); Confidential (C); and Unclassified (UC). Business identifies security levels as: Restricted to Management (R, for example, attorney-client privilege); Proprietary (P); Sensitive (S); and Public (P). These MLS security levels may be supplemented with "need to know" classification labels, organizational limits (Army, Navy, DoD) and time limits. Prior art security systems identified each file with: owner, size, date and time of creation and security attributes. The Bell Lapadula (BPL) security model uses concepts such as domination of the MLS security level over both a process and the subject (a data object). Some examples of various processes are read, execute, overwrite, append, write, kill (delete), etc. Some examples of process rules under the BPL model are: NRU - No Read Up (a lower security level cannot read a document at a higher security level); NWD - No Write Down (a higher level cannot write down to a lower MLS level).

[184] The invention herein does not use the "classification labels" of the prior art. Instead it creates a situation in which the user gets access rights to specific distributed storage locations based upon his MLS level, each access right can be classified with a different classification level.

[185] FIG. 7b diagrammatically illustrates a multiple level security system accessed by users having different security clearances (which also represents a data mining system and operation). Source data 100 passes through security program 200. Critical, important data objects or elements are extracted and dispersed into storage 801. In the illustrated embodiment, storage 801 has four security levels SL1 - SL4, level SL4 being the most secure data requiring the highest security clearance. Between each level is an MLS or multiple level security guard. The guard (physical or software configured) limits transfer of data objects there between. Upon a request or inquiry from user 1, 2 or 3, each having a security clearance s1, s2 or s3, respectively, the query or request for access to data Q1, Q2, or Q3 is sent to security clearance process 803. The process 803 detects and confirms the user's clearance level and passes a cleared query to storage 801. Cleared data (an entire document/data object or a portion thereof or simply one secured data (i.e., a name)), is sent as Data 1, 2 or 3 to clearance process 803. If clearance is still valid, data 1, 2 or 3 is sent to the respective user.

[186] FIG. 7b can be a data mining system in that the user is permitted to mine the "cleared" data from storage 801. Data mining may be a monetary charge associated with the clearance function in process 803.

[187] In a secured system, the documents in the user's PC may be in "declassified" to his security level 99.9% of the time. The "declassified" or available documents are reconstituted through a controlled release of the critical data from storage, and re-classified only when the user presents his identification and his classification level is being verified. Reclassification is automatic at the user's PC. The result is that the user's PC or workstation can operate in classified and un-classified modes. It is unclassified when the documents are declassified and when the documents are reconstituted the user is working in a classified mode.

[redacted]

[188] The invention introduces a new paradigm whereby computers that are classified as secret or top secret, in actuality will contain 99.9% of the time declassified documents. This capability strengthens substantially the security of such classified systems.

[189] The invention can resolve the major challenges facing government in enabling sharing of information between its different organizations in relationship to conducting military operations as well as fighting terrorism. The invention for example can enable organizations connected to the Department of Defense (DOD) or the Homeland Security Department to search into data bases of various other government, state and local organizations, eliminating the fear of the organizations owning the documents that their proprietary data or granular critical data would be released without their specific permission. The invention's mechanism of controlled release of the located document/data enables other parties to search their documents without the fear that sensitive information will be released to the searching party. This invention is designed to foster sharing of documentation between different parties, taking into consideration the need to limit the access of other parties to the total content of the owner's document. The invention enables overcoming the obstacles of existing multiple level security MLS systems by enabling sharing of sensitive data, and granular data between parties in a much more flexible way which also enables much greater access to information not enabled by the current MLS systems. The invention includes a controlled release mechanism for release of data in conformance to benchmarks, which can include submitting of access identification, the giving of consideration, submitting of other information, etc.

[190] The invention creates better collaboration between users and organizations based on a better flow of information. It enables better efficiency enabling easier communication between users and networks with different levels of classification while maintaining the highest levels of security. The invention enables a much better management of documents in storage and in transport including e-mail. The invention introduces automation to the sanitization process and an automatic reconstruction process.

The automation will avoid human error both intentionally as well as unintentionally. The automation will enable a substantial reduction in costs, furthermore the ability to create a multilevel security environment in one PC or workstation will save costs of purchasing operating and maintaining multiple machines as is the current practice.

[191] The challenge of many organizations is in getting mission critical and time sensitive information speedily to the users who need it. In many cases the needed non- classified or low-level classified information is stored in systems but is not provided to the user who needs it, because the information is in documents which are highly classified. This creates situations in which users are unable to access information, which they need to accomplish their tasks, because of a technological classification barrier. This over classification of information results in hampering critical tasks and activities, as well as creating system redundancies inefficiencies. The DoD (Department of Defense) multiple level security (MLS) was based upon the Bell-Lapadula (BPL) Model. Many believe that the BLP security model is superior to other models. The Bell-Lapadula Model and the existing MLS uses labels to classify users and subject matter. A professional attacker will use his efforts to change or damage the labels in- order to compromise the machines secured information.

[192] The architecture or the present invention extracts and physically separates data whereby content is being recognized not by labels by automatically based on the semantic content of the plaintext.

[193] In the DoD's MLS, data of multiple security levels are processed and transferred by the system, which separates the varying security levels and controls access to the data. In the prior art MLS system, some applications process only one level of data at a time, (for example, when a user edits a document with a word processing tool, the data in the document are treated as if they were a single level, the classification of the document itself). Other applications treat individual data elements at their actual levels. For example, a word processor enforces paragraph and page MLS classification labels, or an MLS

[redacted]

data base brings together data elements of different security levels to allow an analyst a multilevel view of the information.

[194] The vulnerabilities of MLS: The components in the MLS system contain the data in their memories and disks, and the data could be compromised if adequate physical security is not maintained. An attacker who gets access to the system might be able to locate the data or its copies.

[195] MLS guards control the flow of information across security boundaries. These MLS guards are known.

[196] One concern with the Bell-Lapadula Model and the existing MLS is the use of labels to classify users and subject matter. A professional attacker will use all his efforts to change or damage the labels in- order to compromise the machines secured information. The invention introduces an architecture whereby content is being recognized not by labels by automatically based on the semantic contents of the plain text. The invention sanitizes and enables reconstitution upon valid authentication. It is the only architecture and system which enables both sanitization and reconstitution according to user's verified access identification. The conventional way of classifying documents with high classification (TS), limits the low level clearance users (C) from accessing substantially un-classified information "granular data" which is in the classified document. Furthermore, the invention enables maximum sharing of unclassified information which lies dormant in classified documents. Top security-secret information is dispersed to distributed storage in many locations. The invention is designed to avoid any one point of failure. The theory behind the architecture is the creation of substantial lines of defense in depth. The attacker will need to break through many obstacles before accessing all the dispersed data of the document. Additional levels of security are provided with multi-type encryption. The system and process introduces the capability to encrypt different parts of a document with different types of encryption. Multi type encryption creates a major barrier to an attacker. Should he wish to break the encryption, he would need many super computers. Should the attacker look for implementation

mistakes, even if he finds few, he will still not get access to the total plain text. The inventive system provides flexibility. The system and process delivers flexibility to accommodate changing circumstances. By controlling the level of the granularity, the user can boost the level of security according to changing circumstances. For example, if a competitor becomes a partner the user enables him access to more storage locations, by changing the matrix.

[197] The system and process integrates the Internet for dispersal and hiding of contents. If a party needs more information it could be released granularly. There is no need to release the whole secret document. The system and process does not use labeling but rather extracts the critical to storage. The system avoids situations, in which, attackers may manipulate the labels or the labeling system. Furthermore, the release of information is based on changing circumstances (time, location-GPS, event).

The invention is a machine and process and its purposes and advantages may be as follows: (a) To automatically control selection of data objects within a data stream and release them in a controlled method only to authorized parties. (b) To automatically separate data objects within a data stream into two or more digital data streams according to the importance and categorization of contents, through extraction and removal of the prioritized content and its replacement by appropriate placeholders. (c) To automatically control selected contents in E-mail, and enable its release in a controlled method only to authorized parties. (d) To enable users to leverage the growth in computer and telecommunications connectivity and electronic commerce by reducing security risks. (e) To enable users to release documents, digital files, and data streams into closed and opened digital networks with the confidence that important, identifying, and critical contents in that documents, digital files, and data streams is secure and will be seen only by authorized parties. (f) To enable real time simultaneous customization and personalization of selected contents within a data stream to different parties, allowing instant display of the selected content or part of it based on, and tailored made to the status of the user or receiving party. (g) To secure the important and critical contents of a document or digital file by transporting said contents

into a separated data stream and removing said data stream to a removed storage memory, while eradicating any copies, temporary caches, or traces of the removed extracts on the original computer or machine. (h) To enable instant return transfer to the display or to another display all or part of extracted content instantly with verification of authorized user. (i) To create a projection of the original document, digital file, data objects within a data stream, or variations of it through combined projection of the splinted data streams, while maintaining separation between the data streams. (j) To create an alternative method for security, instead of encryption, which is secure, cost effective, less time-consuming, and flexible. (k) To enable automatic timed removal of specific content items, automatically or manually selected from a document, digital file, or data objects within a data stream. (l) To enable an automatic timed reconstruction (reconstitution) of the said document, digital file, or data objects within a data stream.

The invention differs from the current implementations of multilevel security MLS systems based on the Bell-Lapadula Model, and the prior art use of labels to classify users and subject matter. A professional attacker will use all his efforts to change or damage the labels in- order to compromise the machines secured information. The present invention introduces an architecture whereby content is being recognized not by labels by automatically based on the semantic contents of the plain text. The invention enables overcoming the obstacles of existing multiple level security systems by enabling sharing of sensitive data, and granular data between parties in a much more flexible way which also enables much greater access to information not enabled by the current MLS systems. The invention includes a controlled release mechanism for release of data in conformance to benchmarks, which can include submitting of access identification, the giving of consideration, submitting of other information, etc. The invention creates better collaboration between users and organizations based on a better flow of information. It enables better efficiency enabling easier communication between users and networks with different levels of classification while maintaining the highest levels of security. The invention enables

Ex. 1002, Page 82

a much better management of documents in storage and in transport including e-mail. The invention introduces automation to the sanitization process and an automatic reconstruction process. The automation will avoid human error both intentionally as well as unintentionally. The automation will enable a substantial reduction in costs, furthermore the ability to create a multilevel security environment in one PC or workstation will save costs of purchasing operating and ,maintaining multiple machines as is the current practice.

Adaptive Data Security

[198] The present invention can also be configured as an adaptive security program which adapts and adjusts the security provisions based upon intrusion into a particular network or attempts to electronically attack or hack into that network or successful hack events. Programs are available to track electronic attacks or hacking attempts. One of these programs is manufactured by Cisco and identified as the Cisco Intrusion Detection System (IDS). The Cisco IDS system can work on a server or on PCs in a network. The Cisco IDS is an electronic intrusion detector, or an electronic attack detector or a hacking monitor. The hack or attack monitor is software loaded into a designated computer.

[199] The output of the electronic attack or hacking monitor loaded into PC 142 (FIG. 2) for example, or loaded into PC-6 acting as a server for Network A 404 in FIG. 6, generates a plurality of attack warnings. The attack warnings progressively and incrementally indicate the severity and degree of intrusion and hacking attacks directed to the computer system. The following Security Level Table illustrates an example of various responses to increasing levels of attacks. These increasing security responses include engaging the filter and extracting critical data and storing it locally; the next level involves storing the critical data on removable storage media; the next higher level involves offsite storage of all security data; the subsequent security alert results in multiple offsite storage for multiple levels of security or critical data and the highest level involves offsite storage of both common data (remainder data) and security data. Of course, other combinations responsive to the hack attack may be

[redacted]

provided. The electronic attack monitor may use artificial intelligence AI to (a) assess the severity of the attack, (b) plan an appropriate "secure data" response, (c) select the degree of filter, extraction and/or encryption, and (d) locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, both intra and inter network, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc. Higher security alerts trigger the AI security monitor to heighten the security level (or to decrease that security level in view of a reduction or withdrawal of an electronic attack). Aspects of AI systems, inference engines and neural networks are discussed above in conjunction with the AI configured filter. These AI aspects can be utilized with an AI configured security sensor.

Security Level Table

Attack (low threat level) Level One

engage filter

local storage - disk drive

encrypt map

Attack (moderate threat level) Level Two

same as Level One but use removable storage media (local)

Attack (nominal attack) Level Three

Engage higher level filter

Off site storage, single storage for all security data

Attack (moderate attack) Level Four

Multiple off site storage, multiple levels of security data

Attack (severe attack) Level Five

Off site storage both common data and security data

Ex. 1002, Page 84

[200] Hence, the filtering of data is based upon respective ones of the plurality of attack or hack warnings and the extraction of data and degree of extraction is dependent upon respective ones of the plurality of attack - hack warnings. Storage of the extracted data and the remainder data is also based upon the degree of attack which is reflected in the attack - hack warning issued by the monitor.

[201] FIG. 8 diagrammatically illustrates a flow chart showing the key components of the adaptive security program adaptable to various levels of hacker of electronic attacks. Step 460 senses all intrusions and attempts, that is, electronic attacks, hack attacks or hacking actions on a computer or a computer network. This step is equivalent to the output of the attack - hack monitor. Step 462 assesses the current network performance, adjusts the storage location for the extract data (the location of the extract store), the encryption level (the degree of encryption) and the storage of the map showing the extract data storage (if necessary) and storage of remainder data, if necessary given the severity of the attack. For example, during high utilization of the computer network (high utilization in a server computer in a server-client environment), local storage of extracted data may be preferable as compared with offsite storage of critical data. However, if the attack occurs during non-working hours, the performance of the network is very high, and the security system could utilize all the resources in the computer network to achieve the security goal of safe guarding the data during the attack. System resources include processing resources (for encryption/decryption), bandwidth resources to store extract data and any other resources that are critical for the utilization of the security system described herein. Decision step 464 determines whether a threat or attack as occurred. If not, the system takes the NO branch returns to step 460. If YES, the system in step 466 assigns an attack level or a hack warning level to the threat or attack. The system in decision step 468, monitors the network during the attack. If the network performance or the computer performance does not change, the YES branch is taken. If the computer performance or network performance changes based upon or during the attack, the NO branch

[redacted]

is taken and the system returns to step 466 which reassigns an attack level or a warning level to the next higher or significantly higher warning levels.

[202] After decision step 468, the system executes step 470 which assigns the security level and implements the security program based upon the attack. It should be noted that the administrator establishes the degree of security level, the encryption, the extract store and remainder store (if necessary) for various levels of attacks or hack warnings. The security level assigned to a particular attack warning is implemented in step 470. Decision step 472 determines whether the security program's communication path is clear. For offsite storage of extract and/or remainder data, a communication path is important. If the path is blocked or compromised by the attack, the NO branch is taken and the system in step 473 reassigns the security level to a next higher level or a different, safer security level and returns to step 470. If the security and communications path is clear, the YES branch is taken from decision step 472 and, in step 474, the system maintains the security program. Decision step 476 determines whether sufficient time has passed from the attack. If not, the system loops to step 474. If YES, the system executes step 478 which either permits reconstruction of the user operating the plain text or source document or automatically reconstructs those documents that were filtered, parsed, extracted, and subject to outside storage. The system ends in step 480. To provide additional security, the attack monitor can be configured to monitor security warnings from trusted parties such as MicroSoft, Norton, NASA, DoD, CDC, FBI, etc. Emails or electronic communications from trusted parties can trigger higher levels of security. the attack monitor described above can be configured to accept messages from trusted parties. These messages are equivalent to detecting an electronic attack.

[203] Further, the attack - hack monitor can be configured to monitor and assess other environmental conditions such as fire, power failure, equipment failure, unauthorized physical entry into the building, plant, or computer room. These exterior threats or events are monitored by the attack monitor since they may quickly develop into an electronic attack on the secured data retained by the computer system. In

Ex. 1002, Page 86

response to these exterior events, the attack monitor generates corresponding attack warnings similar in nature to the hack attack warnings discussed above.

[204] There are various methodologies that may be utilized in the adaptive system. The tables that follow set forth these various security methodologies.

Standard Automatic Defenses Matrix

Mode	Normal	Threat	Attack
Encryption	Targeted Encryption	Full Encryption	Multi Type Encryption
Extraction	Plain-text Extraction	Extraction of Encrypted Data	Extraction of Multi Type Encryption
Distributed Dispersion	Single Storage Location	Several Storage Locations	Many Storage Locations
Display	Single display	Color/Dither Protection	Multiple Displays

Optional Automatic Defenses Matrix

Mode	Normal	Threat	Attack
Substitution of Code Words	None	Partial	Many
Substitution of Misinformation	None	Partial	Many
Controlled Release-Storage	Full	Partial	Conditional
Storage Locations	2	4	10 or more
Time for release	Anytime	Working Hours	Conditional
Authorized Users	Many	Partial	Conditional
What to Release	All	Partial	Conditional
Secret Sharing	None	Two Users	As Configured

[redacted]

Security Meter Module Table

	Normal Mode	Threat Mode	Attack Mode
ENCRYPTION	Targeted encryption	Full encryption	Multi layer encryption
	(Secret sharing)	(Secret sharing)	(Secret sharing)
EXTRACTION	Plain-text extraction	Extraction of encrypted Data	Extraction of multi encryption
Distributed Storage	1 critical storage	few critical storage	many critical storage
Controlled Release-Storage			
	Storage # ID		
	Time for release		
	Authorized Users		
	What to release		
	Special conditions	2 users online	3 or more users
Display	single display	single display	multiple displays
Substitution of code words	No	No	No

Normal Work Mode

	Extraction				Storage				
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable	Local
social security	X						X		
credit card	X						X		
included	X						X		
last name	X						X		
number	X						X		
telephone			X					X	
name			X					X	
URL			X					X	
e-mail			X					X	
uppercase			X					X	
initial capital			X					X	
currency				X					X
postal code				X					X
address				X					X
location				X					X
date				X					X

Ex. 1002, Page 90

Threat Mode

	Extraction				Storage				
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable	Local
social security	X							X	
credit card	X							X	
included	X							X	
last name	X							X	
number	X							X	
telephone		X						X	
name		X						X	
URL		X						X	
e-mail		X						X	
uppercase		X						X	
initial capital		X						X	
currency			X						X
postal code			X						X
address			X						X
location			X						X
date			X						X

Attack Mode

	Extraction				Storage			
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable
social security	X					X		
credit card	X					X		
included	X					X		
last name	X					X		
number	X					X		
telephone	X						X	
name	X						X	
URL	X						X	
e-mail	X						X	
uppercase	X						X	
initial capital	X						X	
currency		X					X	
postal code		X					X	
address		X					X	
location		X					X	
date		X					X	

[205] Another object of the system and method is to enhance the survivability of a system, network, or an organization through distribution of critical information. The objective is to enable a network or organization to carry on its critical missions even while under attacked or damaged. Survivability is the ability of a system to execute its mission and provide critical operational services during and after a successful intrusion or damage. Providing critical operational services includes maintaining availability of information and data such as credit card numbers, names, phone numbers, transaction amounts, shipment details without compromising the security of the information and data.

[206] The invention is designed to enable a network to adapt to ongoing attack and react in a way that permits critical missions to continue. With the current state of the art, when firewalls or other security measures are compromised, no real obstacles curtail or hinder intruders. The system and method is very adaptable and flexible to provide additional layers of security, privacy, anonymity, redundancy, and backup through the selection, extraction, storage, transportation, and reconstruction processes. The dynamic architecture of the invention enables it to conduct an automatic real time configuration of its extraction/transport/recovery activities, in response to the challenge of attacks.

[207] The invention's survivability modes enable: (a) Presetting of rules for computer or network functioning under attack or alert. (b) An automatic assessment of damage and automatic reaction to enable functionality of critical missions.

Multiple Security Features for Data

[208] FIG. 9 diagrammatically illustrates a flowchart showing the key components of a multiple encryption program using multiple types of encryption in one document or data object. Multiple levels, types or modes of encryption are utilized in the same document or data object to enable securing data and transparently managing the separation of user-based communities of interest based upon cryptographically separated, need to know security levels. These security levels are associated with a plurality of encryption types or with different cipher keys using the same encryption. An example of a multiple level encrypted document is shown above in the Multiple Level Encryption sample. Different levels or modes or types of encryption are listed in the Encryption Table above.

[209] Step 510 in FIG. 9 initializes the system by organizing different security levels with different encryption types and cipher keys. Also, the program sets filters to create the multiple encryption or ML document or data object. Step 512 filters the document or data object. Step 514 encrypts the extracted data for each security level. These steps 510, 512 and 514 utilize many of the routines discussed above in connection with FIGS. 4 and 7, steps 232, 234, 236, 238, 240, 422 and 424. Step 516 recognizes that

the secured document or data object may be stored for later use (with associated multiple decryption), published, distributed, or otherwise utilized to achieve the primary purpose of the document, i.e., to communicate information or to safely store security critical information. Step 518 permits the user, with the proper security clearance to retrieve the document or data object. Step 520 illustrates that the user must retrieve his or her cipher key to decode all or a portion of the ML encrypted document or data object. This step may be manual which engages the user to into certain codes or may be automatic such that the user's computer automatically, without operator input, decodes all or part of the document or data object. Step 522 decrypts the document pursuant to the user's security clearance. Step 524 recognizes that the user may review, re-publish, store, comment on, re-encrypt or otherwise deal and handle the full or partially decoded document or data object. The program ends or otherwise continues with other programs set forth herein. It should be noted that storage of the extracted data may be included in the flow path of the program in FIG. 9 is necessary.

[210] FIG. 10 diagrammatically illustrates a chart showing the key components of the parsing, dispersion, multiple storage and reconstruction (under security clearance) of data. Document or data object 100, in function element 550, is created or obtained by the input computer device. The document is stored in a normal manner in customary data store 552. A parsing algorithm function 554 is utilized in parsing step 556. The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and splits, cuts and segments (that is, parses) the document by bit count, word, word count, page, line count, paragraph count, any identifiable document or icon characteristic, or other identifiable feature such as capital letters, italics, underline, etc.. Hence, the parsed document 100 constitutes at least remainder data and data which is extracted or parsed or segmented out. A plurality of data extracts may be obtained. The parsed data (which is both the extract data and remainder data) is then dispersed into storage facilities data store DS 1, 2, 3, 4, etc. Preferably, the parsed documents are encrypted as shown by "e" in FIG. 10. In order to facilitate the potential reconstitution of document 100, a map is stored in a map storage 558.

[redacted]

Hence, the dispersement 560 largely spreads out or distributes the parsed document 100 to a plurality of memories in the distributed computer system. These memories may be removable memory devices (floppy disc, removable tape drive, CDs) or may be more fixed devices such as hard drives, Internet storage facilities, etc. Preferably, the map is also encrypted.

[211] Reconstruction step 562 enables a person with the appropriate security to obtain the map from map storage 558, decode the map, gather the dispersed, parsed segments of document 100 and compile the document. This is noted in function 564.

[212] Since the original document 100 is stored in a customary manner in data storage 552, the parsed document stored in multiple data storage units DS1-DS4 provides a unique backup for document 100. The algorithm can employ many different mathematical constructions but is, in the current embodiment, primarily based upon one or more of a bit count, a word, a word count, a page count, a line count, a paragraph count, and identifiable document characteristic, and identifiable word characteristic, and identifiable icon characteristic and identifiable data object characteristic, capital letters, italics, and underline found in the plaintext document or data object. Further, the parsing algorithm can generate different security levels wherein parsed segments are stored at different storage facilities having various degrees of security clearance. This establishes a hierarchy of data storage units and corresponding degrees of security clearances. The parsing algorithm may identify unique words or strings of data, i.e., credit card numbers. The hierarchy of security clearances may involve first a password, second a biometric confirmation such as a voice match and a third highly unique biometric characteristic such as a fingerprint or retinal scan. The parsing system enables a large distribution of data in a secured environment. In this manner, if the original data object 100 at customary data storage 552 is destroyed, a person with an appropriate security clearance can reconstitute the original data document 100 due to the secured parsing and dispersal of document 100 through data storage units DS1-DS4 and map storage

[redacted]

558. The parsing may occur on a granular level. In particular, the parsing may occur on a financial document in electronic form.

Financial Document Table

Startcode; Abel, Robert, NMI; 100567; TRANSFER803; To8900586943; FROM3897622891; $700.00; endcode

[213] In the Financial Document Table, the start code and end code is typically represented by a digital code unique to the communications channel, the name on the account has no middle initial (NMI) and the various words "transfer 803" and "to 8900586943" and the words "from" and "$" are represented by predefined numeric or alpha numeric codes. The electronic financial document complies with an established protocol. In any event, financial documents are often times transmitted through electronic communications and telecommunications channels. The present invention, in one embodiment, enables a higher level of security by parsing the financial document or data stream. Further, a higher level of security may be employed by extracting identified text or characters and storing the extracted text as discussed above in connection with FIGS. 1A, 1B and 2.

[214] To some extent, the present system can also be utilized for key management and encryption systems.

[215] In a broad sense, the parsing methodology disclosed herein is not based upon the separation of critical versus non-critical or classified versus non-classified security information. The primary focus of the parsing methodology is (1) automatic transparent parsing of data content into granular data groups which are thereafter dispersed to different storage locations in order to maintain a very high level of security with or without encryption; (2) dispersal of the segmented data to different storage locations each which, potentially, demand additional identification or security clearance prior to the release of the stored segmented data, including, possibly, the creation of a digital bureaucracy, in order to hinder or circumvent digital attacks on the plaintext document or data object; (3) proposing and implementing a system

[redacted]

wherein the user has a very basic appliance since most of the user's data is stored both locally (customary data storage 552; FIG. 10) and parsed and stored in a distributed system (DS1-DS4) and wherein an important asset is the map stored in map location 558; (4) enabling an institutional system to parse highly confidential information and extract the same in granular form and disperse the same throughout the Internet or other storage locations with or without encryption without compromising the document's security privacy and integrity.

[216] The process involves parsing the documents or content into granular data groups and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file; dispersing the granular data groups into different storage locations; creation of a map of dispersal to the different storage locations (wherein the map is secured and encrypted and stored); and reconstructing the documents or data content. The reconstruction utilizes the map of dispersed and distributed storage and requires the presentation of security clearances such as passwords, biometric information and/or physical identifiers for access at the storage level and potentially at all the other data storage sites. The data is compartmentalized through distributed storage and sometimes requires separate security clearance. This need for presenting additional security clearance at different storage locations (DS1-DS4) creates a digital bureaucratic process which enhances the security level of the entire system. The selection and extraction of data and dispersal of that data to select storage locations can be established under different criteria. For example, one level of criteria extracts last name, address and social security numbers. Another criteria extracts every other line, every third word, etc. The parsing algorithm can utilize random selection or systematic selection as long as the parsing algorithm is documented and utilized in reconstruct step 562. The parsing algorithm may be stored with map and map store 558 or may be stored separately. An additional feature, as discussed above, involves utilizing place holders or adding substitute content to the remainder data of the parsed document 100. The use of place holders and substitute content may be thought of as an algorithm for the parsing. By using place holders

and substitute data, private or highly confidential data is masked insuring privacy, security, and confidentiality. The ability to parse the information and/or extract security information is important for financial transactions. The transactions which require account numbers (see Financial Document Table above) are useless without the account numbers. The security of the account numbers, whether identified and extracted or severely parsed and segmented, stored and reconstituted under security clearances, is enhanced by the present system.

[217] To achieve a very high level of security, the system can optionally incorporate a two-man key system. The system automatically separates the selected data stream into one or more data groups and extracts one or more of these data groups and disperses them into data storage DS1-DS4. To release the extracted data groups and/or critical content, the reconstruct step 562 may require two persons submitting identification credentials or security clearances. This two-man key method is a further protection against identity theft and insider attacks. The two-men key system can be implemented on a regular basis or on an emergency basis when there is need for a higher level of security.

[218] Financial documents sometimes include substantial amounts of numerical data such as financial projections, balance sheets, electronic funds transfer messages, etc. It should be noted that the extraction may be based upon a particular item such a digit and a nine digit number representing money or may be parsed automatically based upon some parsing facility. Of course, the financial document may also be viewed as a data stream with delimiters ";" separating fields in the data stream. The parsing algorithm may work on the data in each field as well as different fields in the entire data stream.

[219] Most storage facility systems require a map in order to reconstruct the original plaintext document 100. The map may be encrypted and may require a secret key sharing scheme for access thereto. Further, the map may be a physical map (a printout) or may be stored on a removable data storage medium, rather than be an electronic representation. In some instances, a map is not necessary. For example, if the security data or the parsed or segmented data were automatically stored on a floppy

disc, the originator of plaintext document 100 could move the floppy disc from the computer system thereby physically safeguarding the security data or the segmented, parsed data. Without the disc, another person or the originator of plaintext document 100 could not reconstitute the document. The originator may deliver the floppy disc to another in order to permit reconstitution. The same is true regarding removable tapes and CD-ROMs.

[220] Advantages of the present parsing system, methodology and program, include the ability to connect to unsecured networks without adversely affecting the overall security of the plaintext document 100; less dependence on existing security system including fire walls; the reduction of the requirement to keep daily updates regarding vulnerabilities of the computer system originating plaintext document 100; the security of plaintext document 100 is not dependent upon the number of access points into the network or number of users located on the network originating plaintext document 100; there is no damage to the parsed and stored backup version of plaintext document 100 if new security systems are installed wrong or misconfigured and there is no damage if system administrators turn OFF the existing security systems or improperly install or operate the security systems.

[221] The parsing system can operate as a main security operation or an emergency backup system or as a customary backup system. The plaintext source document or data object may be preserved with or without encryption, or destroyed as a further data security step. The parsing and disbursement of data protects plaintext document 100 and insures the survivability of plaintext document 100 if the system originating plaintext document 100 comes under significant electronic or physical attack. That is, if customary data storage 552 is destroyed electronically or physically, the survivability of data in the plaintext document 100 is established by the present system. The storage of granular data groups most likely would defeat any attempt to view the entire content of plaintext document 100. Only verified user users with a confirmed security clearances or identifications verified at reconstruct step 562 and in data storage sites DS1-DS4 are permitted to reconstruct plaintext document 100. Further, the parsing of the

system can be triggered based upon an electronic attack, an electronic hack or a physical environmental detection scheme. This system immediately protects of the critical data plaintext document 100 with a transparent, automatic parsing, dispersal and storage system.

[222] It should be noted that various aspects of the methodology and program described above in connection with FIGS. 1A-9 can be incorporated into the parsing methodology and program in order to enhance or modify the system.

Email, Web-based and Other Types of Applications

[223] FIGS. 11A and 11B diagrammatically illustrate a flowchart showing the key components of one embodiment of the present invention, that is, an e-mail security system. FIG. 11A is linked to FIG. 11B via jump points 11-A and 11-B. The method of securing e-mail data operates on a distributed computer system which at least includes a remote memory designated as an extract store. Of course, the extract store may comprise a plurality of extract stores operative in conjunction with a plurality of security clearance levels. A singular security level is identified in FIG. 11A. Further, the e-mail may be subject to a parsing algorithm which, as discussed above, is generally independent of the identification of security sensitive data. However, with respect to the parsing aspect of the present invention, the original e-mail data is split into extracted data and remainder data and the extracted data is stored in an extract store. Hence, the parsing algorithm operates essentially independent of the content whereas the secured e-mail program operates based upon content identification. Although FIGS. 11A and 11B primarily relate to identification of security data, the same is true regarding the use of securing e-mail data with a parsing algorithm.

[224] The e-mail security system begins with step 602 wherein the system or program is turned ON or is activated. Step 603 recognizes that the user originating plaintext document 100 (not shown) has set a security filter identifying one or more security sensitive words, characters or icons. In step 604, the user composes the e-mail representative of plaintext document 100. In step 606, the user selects the "send"

[redacted]

command in the typical e-mail program. As is customary, the system in step 608 conducts a spell checking routine prior to sending the e-mail. In step 610, the system conducts a security check on the plaintext document or composed e-mail generated in step 604. The filter is used in step 604. In step 612, security words are highlighted or distinguished in the e-mail prior to the actual sending of the e-mail to the addressee. This step 612 is optional. In step 614, the user selects the security words for data to be extracted out. The highlighting step facilitates this selection. In step 616, the system extracts the security data and, preferably, in step 618, the security data is encrypted. Step 618 is optional. In a parsing application to secure e-mail, the parsing algorithm operates automatically at step 610 thereby eliminating steps 612 and 614. The extracting step 616 simply represents that the segmented data obtained from the original plaintext e-mail generated at step 604 is separated from remainder data.

[225] After encryption step 618, the e-mail security system generally operates in one of three manners. Other systems may be formulated based upon the systems and subsystems discussed herein. In one methodology, a second e-mail is created (see step 629), in a second methodology the secured data in encrypted form is attached or appended to the original e-mail containing remainder data (step 621) or, in a third methodology, the encrypted security data is simply added to or inserted into the end of the remainder data of the e-mail (step 623). The methodology of generating a second e-mail is initially discussed.

[226] A second e-mail having encrypted security data is created in step 620. Further, the system in step 622 adds a hyperlink to the remainder data in the original e-mail created in step 604. The hyperlink presents a pointer for the addressee to a secured application service provider or ASP. See the discussion of FIG. 2 above. The ASP represents a data storage facility for the secured e-mail data. In step 624, the remainder data from the original e-mail is sent to the addressee in a normal manner. This step also includes the concept that the second e-mail containing the encrypted security data is sent to the ASP. In

step 626, the addressee receives the remainder e-mail which includes a hyperlink to the secured data ASP. The system jumps at jump step 11-A from FIG. 11-A to FIG. 11-B.

[227] In step 628, the addressee receives the remainder e-mail, visits the ASP via the hyperlink and clears the security levels at the secured ASP. In step 630, the secured data ASP obtains a map for each secured data e-mail (since the original e-mail may be broken up into a plurality of extracted, secured data e-mails) obtains all secured data e-mail and decrypts the same. In step 632, the secured ASP downloads the secured data as an e-mail to the addressee. In step 634, the addressee system compiles the original plaintext e-mail 100. A reconstruction program may be necessary to decode the secured data and insert the data into the document via the placeholders.

[228] Optionally, the decryption could occur at the recipient's e-mail device somewhat prior to the reconstitution of the e-mail plaintext document 100 during step 634. This requires the addressee to have the encryption routine and the correct key or decrypt code. The e-mail security system described above may include many of the features discussed earlier in connection with FIGS. 1-9. For example, both the security data and the remainder e-mail data can be encrypted prior to transmission to the addressee and the secured data ASP. The encryption may include multiple levels of encryption and decryption may require multiple levels of security clearance. The encryption may be mixed in the remainder e-mail. Partial as well as full reconstruction is enabled as discussed above in connection with FIG. 3.

[229] From the senders or originator's viewpoint, the e-mail facility described herein facilitates the storage of the extracted data at one or more secured sites.

[230] Another implementation of the secured e-mail system attaches the encrypted and secured data to the remainder e-mail data as indicated in step 621. E-mail attachments are well known. Alternatively, the encrypted secured data may be embedded or copied in encrypted form at the end of the remainder data in the original e-mail as indicated in step 623. In either case, in step 625, the e-mail is sent to the addressee. In step 627, the addressee opens the attachment. In step 629, the system of the recipient

decrypts the secured data attachment or the embedded data attachment. In step 631, the recipient's system integrates the now decrypted secured data with the remainder data. Of course, this a compilation step. Place holders or other position indicators are customarily utilized. Appending the encrypted security data is generally equivalent to attaching a file to the original e-mail which constitutes, after extraction, the remainder data. Including the encrypted security data is adding the security data to the original e-mail at a predetermined location (either the top of the e-mail, the bottom of the e-mail or some predetermined line number).

[231] It should be appreciated that the e-mail security system may work automatically or may be selected manually by the user. The highlighting or special distinguishing manner for the security words in step 612 is optional. By highlighting the security words, the user may select or deselect those words for extraction. At the addressee's side, the addressee's system may be configured to automatically seek out the secured data ASP, enter security clearance data, download the secure data and integrate the secure data in the remainder data e-mail. The present invention contemplates automatic as well as manual steps in steps 626, 628, 630, 632 and 634. The hyperlink with the original remainder e-mail essentially maps the remainder data to the secured data and the remote storage locations handling the secure data. Multiple security clearances may be required of the recipient or addressee. The e-mail system can be combined with other features of the security system discussed above such as multiple security data locations, secret key sharing schemes, multiple encryption of the data in a single document, multiple security clearance levels required for a plurality of storage facilities, the two man key system, automation of key management and a plurality of levels of access to the data such as partial reconstruction in step 634 and full reconstruction.

[232] FIGS. 12A and 12B diagrammatically illustrate a flowchart showing the key components of one embodiment of the system and the invention which implements the security system on a web browser. Jump point 12-A links FIG. 12A to FIG. 12B. The system, at step 700 is ON. The filters establishing

either the parsing or the identification of security data are established in the filter set step 701. In step 702, the user inputs data into open field of an HTML display page which the user has previously downloaded from a web server. In step 704, the user may select "secure now" turning ON the system or the system may automatically be ON such that the filter is screening all the data input by the user in the open field. In step 706, the system scans all the open field data, locates security data and extracts security data. In step 708, place holders are added to replace the extracted security data in the remainder data and a hyperlink is added to the open field remainder data providing a link to the secure data ASP. In step 710, the user selects the "send button" or any other indicator on the HTML page triggering an operation which transmits the open field data (which is now remainder data) to the web server. In step 712, the web server and particularly the common gateway interface (CGI) receives the remainder data fields, identifies the place holders in the data and the hyperlink to the secure data ASP. In step 714, the web server receiving the data from user's browser goes to the secure data ASP, inputs and clears any security level, and obtains the secured data. In step 716, the web server reconstructs the open field data which generally is represented by plaintext document 100. In step 718, the web server processes the data as necessary. Many of the features discussed above in connection with FIGS. 1A-11A may be implemented on the browser system.

[233] The credit card scrubber or financial data scrubber operates in a similar manner to the email and browser data security system described above. The credit card or financial data scrubber (herein collectively "CC scrubber") typically operates on a defined sequence of numbers. For example, if a credit card number is 17 digits, whenever the email or browser security system or program detects17 sequential numerical digits (a pre-set filter), a pop-up window may appear enabling the user to select or turn ON the scrubber. If ON, the data security program strips or parses the credit card number and sends, for example, five of the 17 digits to a secure store. Placeholders or substitute characters may be inserted into the remainder CC data. To reconstitute the entire CC data, the intended recipient would be required

Ex. 1002, Page 104

to pass security clearance levels at the secure store. Of course, the CC scrubber could be set to detect bank account numbers, personal or business account holder names, pre-set passwords, etc. In an OFF state, the CC scrubber would let pass the CC number, account number or pre-set data stream or string. The user may select (i) always ON; (ii) pop-up window, select ON or OFF per transaction; (iii) pop-up window to select OFF (default being ON); or (iv) always OFF but minor reminder (audible sound, icon appearance, etc.) of data security risk. The CC scrubber may encrypt the extracted data for security. Other visual ques may rather than a pop-up window may be used (for example, a drop down menu). The scrubber can also be deployed on wireless devices to scrub sensitive data such as credit card and other financial data.

[234] FIG. 13 diagrammatically shows several revenue systems which may be employed with the data security systems described herein. Many types of revenue systems may be employed in conjunction with the present invention. FIG. 13 shows two basic systems, one at the data input stage and the second at the data output or reconstruction phase. Release of the reconstructed document or portions thereof are based upon security clearance and compensation. Within each revenue subsystem are two types of revenue generators, an advertising revenue generator and a user charge generator. The user charge system contemplates charging or assessing a fee to the user's employer or organization. Therefore, the system operator may select up to four (4) revenue generation systems (ads at the input, charges at the input, ads at the output and charges at the output). It is well known that vendors selling goods and services over the Internet are willing to pay a certain percentage of their sales revenue to other entities referring customers to the vendor's web sites. The concept of display ads in FIG. 13 includes this revenue stream. The system operator may choose all, one, several or none of these revenue systems to be deployed in conjunction with the data security system described earlier herein. Other revenue system may also be utilized. The steps in the revenue system described herein may be reorganized to attain higher consumer and user acceptance and/or to maximize the revenue to the system operator.

[redacted]

[235] Decision step 730 determines whether the system is deployed at the data input phase or not. It is clear that the system operator may utilize the data reconstruction revenue system and hence the decision step 730 is not necessary. If the data input system is employed, step 732 displays the ad to the user. The user may be uploading a complete document to an application server on the Internet or may be using a application service provider on the Internet or an private LAN to secure his or her data. The display ad 732 step enables the user to click on the ad and visit the vendor, thereby potentially generating a referral fee. See referral fee branch 757. Step 734 requires password clearance. Step 736 processes the document or data object with the security system. The user may input the document real time or input it to the application server or may upload the complete document to the server. Alternatively, the ad could be buried in the email or application program run on the user's computer and the user would be shown an ad and given a link to the vendor's Internet site. Selecting the link points the user's browser to the vendor's site.

[236] Step 738 shows display ad 2 to the user thereby potentially generating referral revenue for the system operator. Step 740 notes that the user exits the revenue system. Step 742 determines whether the system charges the user for the security service. If YES, the program processes the charge in step 745 (charge systems are known). If NO, the system ends or returns to other programs in step 747.

[237] The NO branch from determination step 730 leads to the receipt of a reconstruction request by the user in step 750. Step 752 determines whether the user will be charged. If YES, the system executes step 745. If NO, the system displays the ad 1 in step 754. Referral generation is noted by branch 757 from step 754. In step 756, the user's password is subject to clearance. In step 758, the user's request is processed, the document or data object is reconstructed (fully or partially as described earlier), and in step 759 the system displays ad 2. In step 762, the user's activity is logged in to the system. Step 764 determines whether the charge to the user is reduced (because he or she viewed the ads) and if not, the

system ends in step 747, if YES, the system processes the charge in step 745. Alternatively, the user may be shown display ads and/or charged for services upon storage of extracted data. Step 750 includes this concept.

Portable Computing Device Environment

[238] The invention can be applied to portable computing devices to secure files and data objects in such devices. The invention extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data based upon the location of the portable device, typically detected by a global position signal generator (GPS) or based upon triangulation data from several broadcast points. Scrubbing security icons from maps, credit card data or financial data from text, a data object or data stream is part of the portable security system.

[239] As used herein, the term "portable computing device" means a laptop computer, a PC with a movable feature, such as a PC mounted in a car, plane, truck or trailer, PDAs or personal data assistants, mobile or cellular phones configured with a memory, a processor and some type of GPS or locator system to determine where the phone or cellular unit is located within a territory and digital pagers having similar electronic systems.

[240] The present invention can be linked with a location sensing circuit, such as a global position sensor or system (GPS) or other type of location sensing system, such as a system which utilizes triangulated signals. The concept is a location based access oriented security such as an automated trigger (which activates the security program discussed hereinabove when the portable computing device is beyond a predetermined region); an automated safety system; a trip wire; an interlock; a method to disable systems, activity or access to data; and means to limit functionality or access in whole or in granular parts. The portable security system operates on text, data objects, images or other digitally

[redacted]

configured data objects. Security access is limited by a location way point (in relation to a reference point) or a calculated range (using satellite GPS, high altitude services, or earth-based range finding GLS (geographic location services)) about a way point with physical means or mathematical calculations to define a geographic area by equations or geometric shapes or aggregated ranges (the shapes including rectangles, solids, cubes, circles, oval, spherical region or other areas defined by algorithms). Physical and logical access or entry control to weapons, devices, vehicles, computers, equipment, tools, data, networks, local access, remote access beyond a physical location (reference point), can be enabled or disabled with the system of the present invention. The regions (sometimes identified as a single predetermined region or a plurality of predetermined regions), can consist of complex definitions of three dimensional areas of arbitrary shape and sizes, as long as those regions can be defined by algorithms. The region can also be defined as an area circumscribed internally by a perimeter or by an area external to that perimeter. In other words, access can be denied if the portable device is within a certain region as compared with denying access when the device is beyond a predetermined regions. The claims are meant to cover both situations.

[241] FIG. 14 diagrammatically illustrates a portable computing device 810 at location B. The portable computing device 810 includes, in the illustrated embodiment, a GPS system (or a receiver system) 812 coupled to a bus 814 and further coupled to memory 816, a processor 818 and an input/output system 820. Input/output 820 is coupled to, among other things, a key board or key pad, a display, and possibly a transmitter and receiver subsystem. As is known, GPS Systems detect satellite positioning signals and generate an output indicative of the location of the GPS system. In the illustrated embodiment, this location is location B in FIG. 14.

[242] A simple implementation of the present security system provides d1 from location A, defined by building 822, certain security events occur, e.g., automatic extraction and a denial of

[redacted]

reconstruction rights. In one example, GPS subsystem 812 continually monitors the location of portable device 810. When the location of device 810 exceeds a predetermined distance (d1-limit), the program operating in memory, 816 operable by processor 818 either extracts data and stores the extracted data as discussed in detail above or prohibits reconstruction of data as requested by the operator of portable device 810. Alternatively, automatic extraction may occur without prohibiting reconstruction due to device 810 being located beyond the predetermined region d1-limit. The portable computing device 810 in FIG. 14 may have many other electronic components such as those shown in FIG. 2 in connection with computer 165. Alternatively, the security system can be configured in a reverse manner such that the extraction of security information is triggered when portable 810 is within a predetermined region (less than d1-max) close to location A and building 822, that is, the security system disclosed above is triggered to extract information when distance d1 is less than d1-max.

[243] The security system can also be configured such that GPS or locator system 812 detects a variable distance such as distance d2 between truck 824 and location B of portable device 810. In this sense, the location of portable device 810 is obtained by GPS circuit 812 and further some type of communications must be established between truck 824 at location C and the portable device 810. For example, the receiver coupled to input/output 820 receives this information from location of truck 824 and location C. This reference location C is then processed in conjunction with the location data from GPS circuit 812 by processor 818 and memory 816. The same results as discussed above in conjunction with fixed reference location A can be achieved with a variable reference location C. Truck 826 at variable location D enables the system to provide an additional level of security. In other words, within distance d2 (d2-limit), the operator of portable device 810 may be able to reconstruct information upon request. However, if portable device 810 intrudes upon or is less than distance d3 (d3-max) the distance between location B and location D, the security system may trigger an immediate extraction routine

thereby disbursing, on a granular basis, the secured words, data objects or whatever and further prohibit reconstruction. Of course, the security system could be configured simply to extract the information and permit reconstruction. Otherwise, the security system could be configured to simply extract information and prohibit reconstruction. In this manner, the security system discussed in conjunction with the portable computing device 810 can have multiple triggers or location established events enabling the security program to extract security information or disabling the security program to prohibit reconstruction based upon a fixed location A or one or more variable locations C, D.

[244] Another configuration of the present invention utilizes triangulation to obtain location B for the portable computing device 810. In a triangulation situation, the receiver system 812 for the locator receives signals from one or more fixed locations, and preferably three locations diagrammatically illustrated by tower T1, T2 and T3 in FIG. 14. The triangulation of signals to obtain location B is known in the art. However, the combination of such location position coupled to extraction of security data and/or reconstruction of security data based upon certain location parameters is part of the present invention.

[245] For illustration purposes only, the present security system for the portable computing device 810 can remotely store extracted security information. Remote store 828 coupled to receiving tower T1 illustrates this concept.

[246] FIG. 15 diagrammatically illustrates a basic flow chart for the portable security system program utilized in connection with portable computing device 810. Decision step 830 determines whether a certain event has occurred. This event may include a power ON for the portable computing device, may be a "save document" command, may be a screen ON event or may be a timed function. For example, if the portable computing device 810 is continually ON, the program may periodically poll the locator circuit (GPS 812) and determine whether location B is within or beyond the predetermined

regions (d-max or d-limit). Step 832 activates the GPS or the triangulation circuit to obtain current location data. This may include locating variable locations C, D. Step 833 obtains territory limits for various security levels. As discussed earlier, security level SL1 is public or non-confidential information, security SL2 confidential or proprietary information, level SL3 is secret information and level SL4 is top secret information. This system can be configured such that various territories or predetermined regions correspond to respective ones of the security levels SL1-SL4.

[247] Decision step 834 determines whether location B of portable computing device 810 is within or without the predetermined territory limits or predetermined region. If YES, the system determines in decision step 836 whether the user has initiated a reconstruction request. If not, the system returns to a point preceding decision step 830, the detect event function or step. If YES, the system, in step 838, reconstructs the document only if location B is beyond a predetermined region. Of course, a negative operation could occur in that reconstruction would be prohibited if location B was within a predetermined region. The claims appended hereto are meant to cover both within a region and without a region and independently, extract or permit reconstruction. Step 840 secures the reconstructed file again as necessary.

[248] Returning to decision step 834, if location B is not within the predetermined regions or territories defined by security levels SL1-SL4, the NO branch is taken and decision step 842 determines whether portable computing device 810 has any unsecured files. If YES, the system executes step 844 which is extract and store the security sensitive words, data objects etc. in accordance with security levels SL2-SL4. As stated above, the storage could be on media in a local drive or can be remotely distributed to memory segments designated as a remote extract store. If the NO branch is taken from decision step 842, the system executes decision step 846 which determines whether the user has requested a reconstruction of data. If not, the program ends or returns to the event detection step 830. If YES, the

[redacted]

system executes step 848 which determines whether a lower security clearance is available within the current territory, determines whether the user has the proper pass code to access the reconstruction and process the reconstruction or whether the system prohibits all reconstruction. Partial reconstruction for lower security items may be permitted. For example, reconstruction at top secret level SL4 may be prohibited when distance d2 is greater than d2-limit but reconstruction at a lower security level such as confidential level SL2 may be permitted beyond limit d2-limit. In this sense, the present invention can be configured to generate extraction for various security levels at various predetermined regions based upon a fixed reference point or a variable reference point. Alternatively, reconstruction can be permitted or denied based on a plurality of security levels and a plurality of corresponding regions or distances. The term "mobile predetermined region" is sometimes utilized in conjunction with variable regions d2 and d3.

[249] As an example, the data object retained by portable computing device 810 may be a map having security sensitive icons on the map. These icons are extracted if location B is less than a predetermined defined distance d3-limit between variable location D and location B. If location B is beyond d3-minimum, the map can be view by the operator on portable device 810. If location B is less than distance d3-minimum, the security icons are removed from the map. In a similar sense, security sensitive credit card characters can be extracted from plain text documents carried on portable computing device 810 when device 810 is a certain distance beyond d1-limit from fixed reference point A. This location A may be a bank headquarters. Encrypting and decrypting the data based upon the geographic event is also contemplated by the present invention. Of course, portable device 810 may be a plurality of portable devices linked via a hard wire network or via a wireless network. The same security program disclosed above in herein can be utilized with one computer or a series of computers. Further, portable computing device 810 can include a plurality of memory segments (see FIG. 3A) and may include a

plurality of display screens as discussed above in conjunction with FIG. 3. The extraction and storage and reconstruction of streaming data is possible as is operation on voice data. Additionally, the portable computing device may set off an audible and/or visual alarm prior to extraction of data. For variable territories or predetermined regions, step 832 or 833 may include gathering information regarding the variable location of vehicles 824, 826 prior to determining the territorial limits for various security levels SL2, SL3 and SL4.

[250] The claims appended hereto are meant to cover modifications and changes within the scope and spirit of the present invention.

[redacted]

What is claimed is:

1. A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said computer system having at least one portable computing device locatable with substantially current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store, respectively;

permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance and only when said portable computing device is not beyond said predetermined region.

2. A method for securing data as claimed in claim 1 wherein said substantially current location data is generated with the acquisition of a global positioning signal.

3. A method for securing data as claimed in claim 1 including acquiring said substantially current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

4. A method for securing data as claimed in claim 1 wherein said extract store is operable in a local data drive on said portable computing device and said storing occurs on said local data drive.

5. A method for securing data as claimed in claim 4 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

6. A method for securing data as claimed in claim 1 wherein said extract store is a remote memory and the method includes transmitting said extracted data to the remote extract store.

7. A method for securing data as claimed in claim 6 wherein said transmitting occurs as a wireless data transmission.

8. A method for securing data as claimed in claim 7 including encrypting said extracted data prior to transmitting.

9. A method for securing data as claimed in claim 6 including receiving said extracted data as necessary during reconstruction.

10. A method for securing data as claimed in claim 1 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

11. A method for securing data as claimed in claim 1 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

12. A method for securing data as claimed in claim 11 wherein the step of obtaining occurs before the step of determining.

13. A method for securing data as claimed in claim 1 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

14. A method for securing data as claimed in claim 1 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

15. A method for securing data as claimed in claim 1 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

16. A method of securing data as claimed in claim 1 wherein said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels.

17. A method of securing data as claimed in claim 16 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said subsets of extracted data only in the presence of said predetermined security level of said plurality of security levels.

18. A method of securing data as claimed in claim 17 including encrypting said subsets of extracted data and remainder data prior to storing.

[redacted]

19. A method as claimed in claim 16 wherein the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

20. A method of securing data as claimed in claim 1 operating over a plurality of computers interconnected together.

21. A method for securing data as claimed in claim 1 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

22. A method of securing data as claimed in claim 1 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

23. A method as claimed in claim 1 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

24. A method as claimed in claim 1 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

25. A method for securing data as claimed in claim 1 including acquiring said substantially current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

26. A method for securing data as claimed in claim 25 wherein said extract store is operable in a local data drive on said portable computing device and said storing occurs on said local data drive.

[redacted]

27. A method for securing data as claimed in claim 26 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

28. A method for securing data as claimed in claim 27 wherein said extract store is a remote memory and the method includes transmitting said extracted data to the remote extract store.

29. A method for securing data as claimed in claim 28 wherein said transmitting occurs as a wireless data transmission.

30. A method for securing data as claimed in claim 29 including encrypting said extracted data prior to transmitting.

31. A method for securing data as claimed in claim 30 including receiving said extracted data as necessary during reconstruction.

32. A method for securing data as claimed in claim 31 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

33. A method for securing data as claimed in claim 31 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

34. A method for securing data as claimed in claim 33 wherein the step of obtaining occurs before the step of determining.

35. A method for securing data as claimed in claim 34 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

36. A method for securing data as claimed in claim 34 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

37. A method for securing data as claimed in claim 36 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

38. A method of securing data as claimed in claim 37 wherein said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels.

39. A method of securing data as claimed in claim 38 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all

of said subsets of extracted data only in the presence of said predetermined security level of said plurality of security levels.

40. A method of securing data as claimed in claim 39 including encrypting said subsets of extracted data and remainder data prior to storing.

41. A method as claimed in claim 40 wherein the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

42. A method of securing data as claimed in claim 41 operating over a plurality of computers interconnected together.

43. A method for securing data as claimed in claim 42 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

44. A method of securing data as claimed in claim 43 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

45. A method as claimed in claim 44 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

46. A method as claimed in claim 44 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

47. A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said

computer system having at least one portable computing device locatable with substantially current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store, respectively;

when said portable computing device is not beyond said predetermined region, permitting full or partial reconstruction of said data via said extracted data and remainder data in the presence of a predetermined security clearance.

48. A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said computer system having at least one portable computing device locatable with substantially current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, extracting said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store.

[redacted]

49. A method for securing data as claimed in claim 48 including acquiring said substantially current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

50. A method for securing data as claimed in claim 48 wherein said extract store is operable in a local data drive on said portable computing device and said storing occurs on said local data drive.

51. A method for securing data as claimed in claim 50 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

52. A method for securing data as claimed in claim 48 wherein said extract store is a remote memory and the method includes transmitting said extracted data to the remote extract store.

53. A method for securing data as claimed in claim 52 wherein said transmitting occurs as a wireless data transmission.

54. A method for securing data as claimed in claim 53 including encrypting said extracted data prior to transmitting.

55. A method for securing data as claimed in claim 48 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

56. A method for securing data as claimed in claim 48 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

57. A method for securing data as claimed in claim 56 wherein the step of obtaining occurs before the step of determining.

[redacted]

58. A method for securing data as claimed in claim 48 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

59. A method for securing data as claimed in claim 48 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

60. A method for securing data as claimed in claim 48 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

61. A method of securing data as claimed in claim 48 wherein said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with a plurality of security levels.

62. A method of securing data as claimed in claim 61 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels.

63. A method of securing data as claimed in claim 62 including encrypting said subsets of extracted data and remainder data prior to storing.

64. A method of securing data as claimed in claim 48 operating over a plurality of computers interconnected together.

65. A method for securing data as claimed in claim 48 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

66. A method of securing data as claimed in claim 48 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

67. A method for securing data as claimed in claim 49 wherein said extract store is operable in a local data drive on said portable computing device and said storing occurs on said local data drive.

68. A method for securing data as claimed in claim 67 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

69. A method for securing data as claimed in claim 49 wherein said extract store is a remote memory and the method includes transmitting said extracted data to the remote extract store.

70. A method for securing data as claimed in claim 69 wherein said transmitting occurs as a wireless data transmission.

71. A method for securing data as claimed in claim 70 including encrypting said extracted data prior to transmitting.

72. A method for securing data as claimed in claim 71 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

73. A method for securing data as claimed in claim 72 wherein said plurality of predetermined regions is a plurality of mobile predetermined region and the method includes obtaining data representing said plurality of mobile predetermined region.

74. A method for securing data as claimed in claim 73 wherein the step of obtaining occurs before the step of determining.

[redacted]

75. A method for securing data as claimed in claim 74 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

76. A method for securing data as claimed in claim 74 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

77. A method for securing data as claimed in claim 74 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

78. A method of securing data as claimed in claim 77 wherein said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with a plurality of security levels.

79. A method of securing data as claimed in claim 78 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels.

80. A method of securing data as claimed in claim 79 including encrypting said subsets of extracted data and remainder data prior to storing.

81. A method of securing data as claimed in claim 80 operating over a plurality of computers interconnected together.

82. A method for securing data as claimed in claim 81 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

83. A method of securing data as claimed in claim 82 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

84. A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which is stored in said extract store and said remainder store, respectively, said computer system having at least one portable computing device locatable with substantially current location data, comprising:

determining when said portable computing device is within a predetermined region based upon said current location data;

permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance and only when said portable computing device is not beyond said predetermined region.

85. A computer readable medium containing programming instructions for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said computer system having at least one portable computing device locatable with substantially current location data, the programming instructions comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data

[redacted]

and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store, respectively;

permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance and only when said portable computing device is not beyond said predetermined region.

86. A computer readable medium with programming steps as claimed in claim 85 wherein said substantially current location data is generated with the acquisition of a global positioning signal.

87. A computer readable medium with programming steps as claimed in claim 85 including acquiring said substantially current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

88. A computer readable medium with programming steps as claimed in claim 85 wherein said extract store is operable in a local data drive on said portable computing device and said storing occurs on said local data drive.

89. A computer readable medium with programming steps as claimed in claim 88 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

90. A computer readable medium with programming steps as claimed in claim 85 wherein said extract store is a remote memory and the steps include transmitting said extracted data to the remote extract store.

91. A computer readable medium with programming steps as claimed in claim 90 wherein said transmitting occurs as a wireless data transmission.

92. A computer readable medium with programming steps as claimed in claim 91 including encrypting said extracted data prior to transmitting.

[redacted]

93. A computer readable medium with programming steps as claimed in claim 90 including receiving said extracted data as necessary during reconstruction.

94. A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

95. A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

96. A computer readable medium with programming steps as claimed in claim 95 wherein the step of obtaining occurs before the step of determining.

97. A computer readable medium with programming steps as claimed in claim 85 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

98. A computer readable medium with programming steps as claimed in claim 85 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

[redacted]

99. A computer readable medium with programming steps as claimed in claim 85 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

100. A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels.

101. A computer readable medium with programming steps as claimed in claim 100 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said subsets of extracted data only in the presence of said predetermined security level of said plurality of security levels.

102. A computer readable medium with programming steps as claimed in claim 101 including encrypting said subsets of extracted data and remainder data prior to storing.

103. A computer readable medium with programming steps as claimed in claim 100 wherein the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

104. A computer readable medium with programming steps as claimed in claim 85 configured to operate over a plurality of computers interconnected together.

105. A computer readable medium with programming steps as claimed in claim 85 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

106. A computer readable medium with programming steps as claimed in claim 85 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

107. A computer readable medium with programming steps as claimed in claim 85 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

108. A computer readable medium with programming steps as claimed in claim 85 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

109. A computer readable medium with programming steps for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said computer system having at least one portable computing device locatable with substantially current location data, the programming steps comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, extracting said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store.

[redacted]

110. A computer readable medium with programming steps as claimed in claim 109 including acquiring said substantially current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

111. A computer readable medium with programming steps as claimed in claim 109 wherein said extract store is operable in a local data drive on said portable computing device and said storing occurs on said local data drive.

112. A computer readable medium with programming steps as claimed in claim 111 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

113. A computer readable medium with programming steps as claimed in claim 109 wherein said extract store is a remote memory and the method includes transmitting said extracted data to the remote extract store.

114. A computer readable medium with programming steps as claimed in claim 113 including encrypting said extracted data prior to transmitting.

115. A computer readable medium with programming steps as claimed in claim 109 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

116. A computer readable medium with programming steps as claimed in claim 109 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

[redacted]

117. A computer readable medium with programming steps as claimed in claim 109 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

118. A computer readable medium with programming steps as claimed in claim 109 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

119. A computer readable medium with programming steps as claimed in claim 109 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

120. A computer readable medium with programming steps as claimed in claim 109 wherein said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with a plurality of security levels.

121. A computer readable medium with programming steps as claimed in claim 120 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the method including encrypting said subsets of extracted data with corresponding degrees of encryption associated with said plurality of security levels.

122. A computer readable medium with programming steps as claimed in claim 121 including encrypting said subsets of extracted data and remainder data prior to storing.

123. A computer readable medium with programming steps as claimed in claim 109 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

[redacted]

124. An information processing system for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder store and an extract store, said computer system having at least one portable computing device locatable with substantially current location data, comprising:

means for determining when said portable computing device is beyond a predetermined region based upon said current location data;

means for extracting, coupled to said means for determining, said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store, respectively;

means for permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a predetermined security clearance and only when said portable computing device is not beyond said predetermined region.

125. An information processing system as claimed in claim 124 including a global positioning signal generator, said substantially current location data being generated by said global positioning signal generator and applied to said means for determining.

126. An information processing system as claimed in claim 124 including means for acquiring said substantially current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

127. An information processing system as claimed in claim 124 wherein said portable computing device includes a local data drive and local drive media, said means for extracting storing said security sensitive words, characters, data objects or icons on said media in said local data drive.

[redacted]

128. An information processing system as claimed in claim 127 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

129. An information processing system as claimed in claim 124 including a remote memory in said computer system, said portable computing device including a data transmitter, said means for extracting storing said security sensitive words, characters, data objects or icons in said remote memory via said data transmitter.

130. An information processing system as claimed in claim 129 wherein said data transmitter transmits data via a wireless communications channel.

131. An information processing system as claimed in claim 130 including means for encrypting said extracted data prior to transmitting.

132. An information processing system as claimed in claim 129 including means for receiving said extracted data as necessary during reconstruction.

133. An information processing system as claimed in claim 124 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the means for determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said means for extracting and storing being triggered based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said means for reconstructing being activated based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

134. An information processing system as claimed in claim 124 wherein said predetermined region is a mobile predetermined region and the system includes means for obtaining data representing said mobile predetermined region.

135. An information processing system as claimed in claim 124 wherein said data is a map with security sensitive icons associated therewith, said means for extracting acting upon said map and extracting said security sensitive icons from said map when said portable computing device is beyond said predetermined region.

136. An information processing system as claimed in claim 124 wherein said data is a document file with security sensitive credit card data characters associated therewith, said means for extracting acting upon said security sensitive credit card data characters and extracting the same from said document file when said portable computing device is beyond said predetermined region.

137. An information processing system as claimed in claim 124 including means for encrypting said extracted data before or during said storage and means for decrypting said extracted data as necessary during reconstruction by said means for reconstructing.

138. An information processing system as claimed in claim 124 wherein said predetermined security level is one of a plurality of security levels, said means for extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and said means for reconstructing acts upon some or all of said subsets of extracted data only in the presence of a respective predetermined security level of said plurality of security levels.

139. An information processing system as claimed in claim 138 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said subsets of extracted data, the system including means for encrypting said subsets of extracted data with corresponding degrees of

encryption associated with said plurality of security levels, and including means for decrypting, during reconstruction with said means for reconstructing, of some or all of said subsets of extracted data only in the presence of said predetermined security level of said plurality of security levels.

140. An information processing system as claimed in claim 139 including means for encrypting said subsets of extracted data and remainder data prior to storing.

141. An information processing system as claimed in claim 138 wherein said means for reconstructing permits a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

142. An information processing system as claimed in claim 124 utilizing a plurality of computers interconnected together.

143. An information processing system as claimed in claim 124 including an automatic means for determining and means for extracting and storing actuated upon power up or geographic location of said at least one portable computing device.

144. An information processing system as claimed in claim 124 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the means for reconstructing interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

145. An information processing system as claimed in claim 124 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the means for reconstructing including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

146. An information processing system for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with memories designated as a remainder

[redacted]

store and an extract store, said computer system having at least one portable computing device locatable with substantially current location data, comprising:

means for determining when said portable computing device is beyond a predetermined region based upon said current location data and generating a trigger;

means for extracting, upon said trigger when said portable computing device is beyond said predetermined region, said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data and said remainder data in said extract store and said remainder store.

[redacted]

ABSTRACT

The method, used with a portable computing device, secures security sensitive words, icons, etc. by determining device location within or without a predetermined region and then extracting the security data from the file, text, data object or whatever. The extracted data is separated from the remainder data and stored either on media in a local drive or remotely, typically via wireless network, to a remote store. Encryption is used to further enhance security levels. Extraction may be automatic, when the portable device is beyond a predetermined territory, or triggered by an event, such a "save document" or a time-out routine. Reconstruction of the data is permitted only in the presence of a predetermined security clearance and within certain geographic territories. A computer readable medium containing programming instructions carrying out the methodology for securing data is also described herein. An information processing system for securing data is also described.

\\Tiger\data share\RCK\CLIENTS\Redlich\Patents\6851-2cip5-pa.wpd

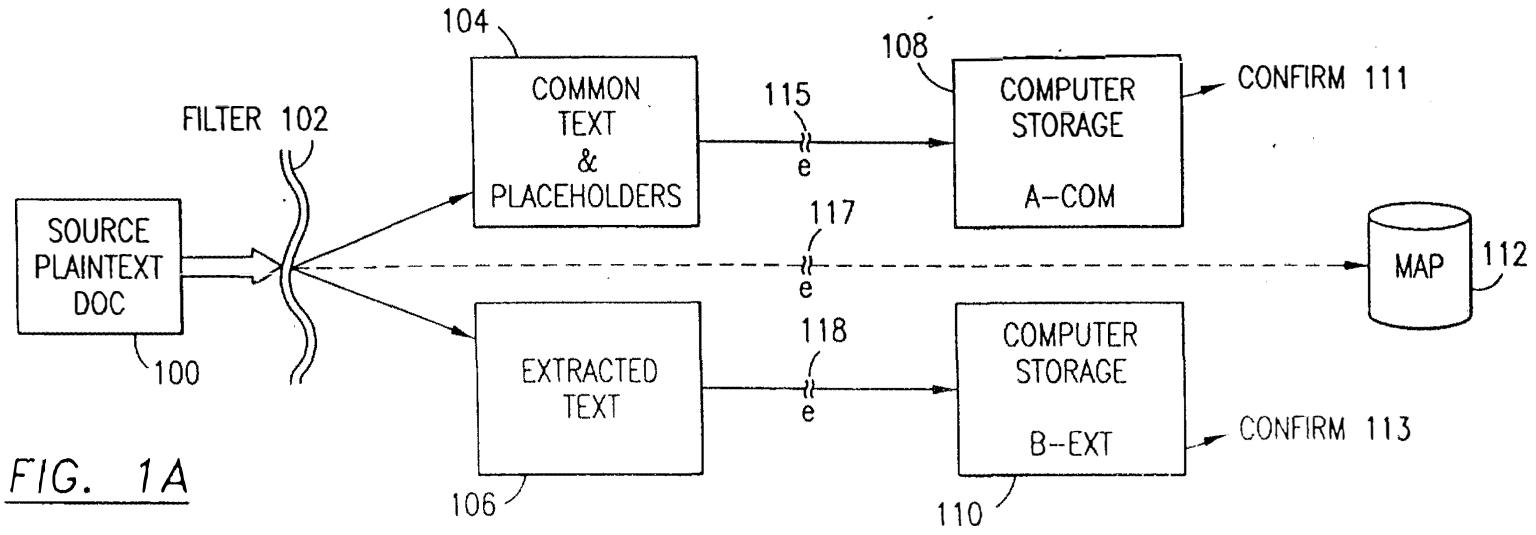


FIG. 1A

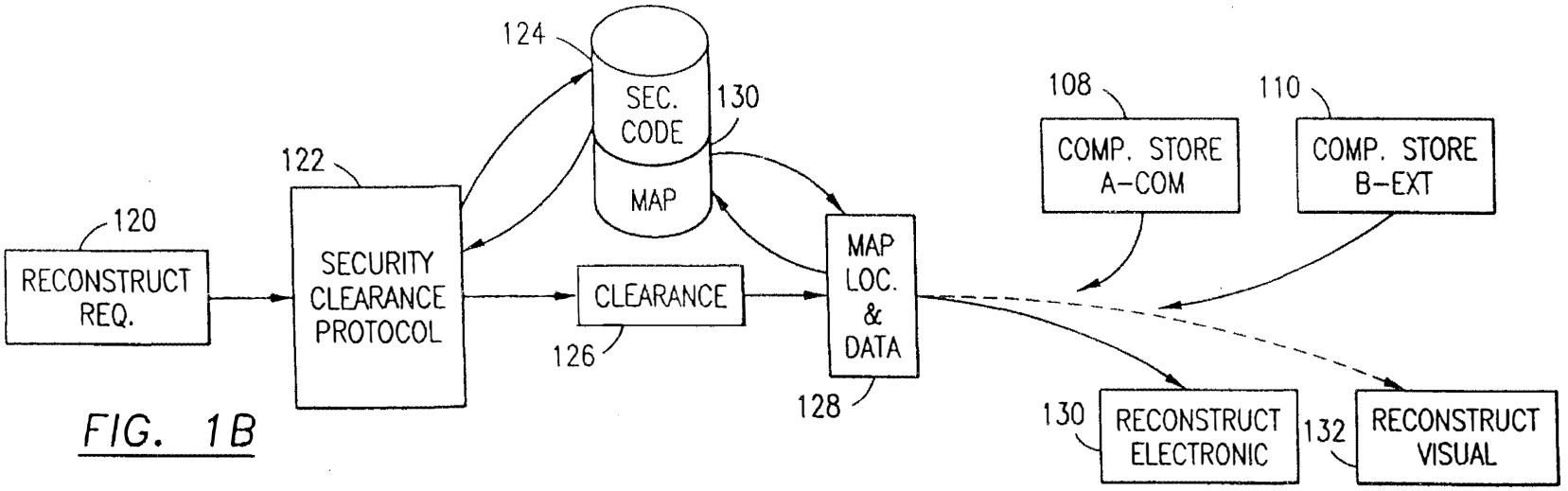


FIG. 1B

EXHIBIT 1008, PAGE 140

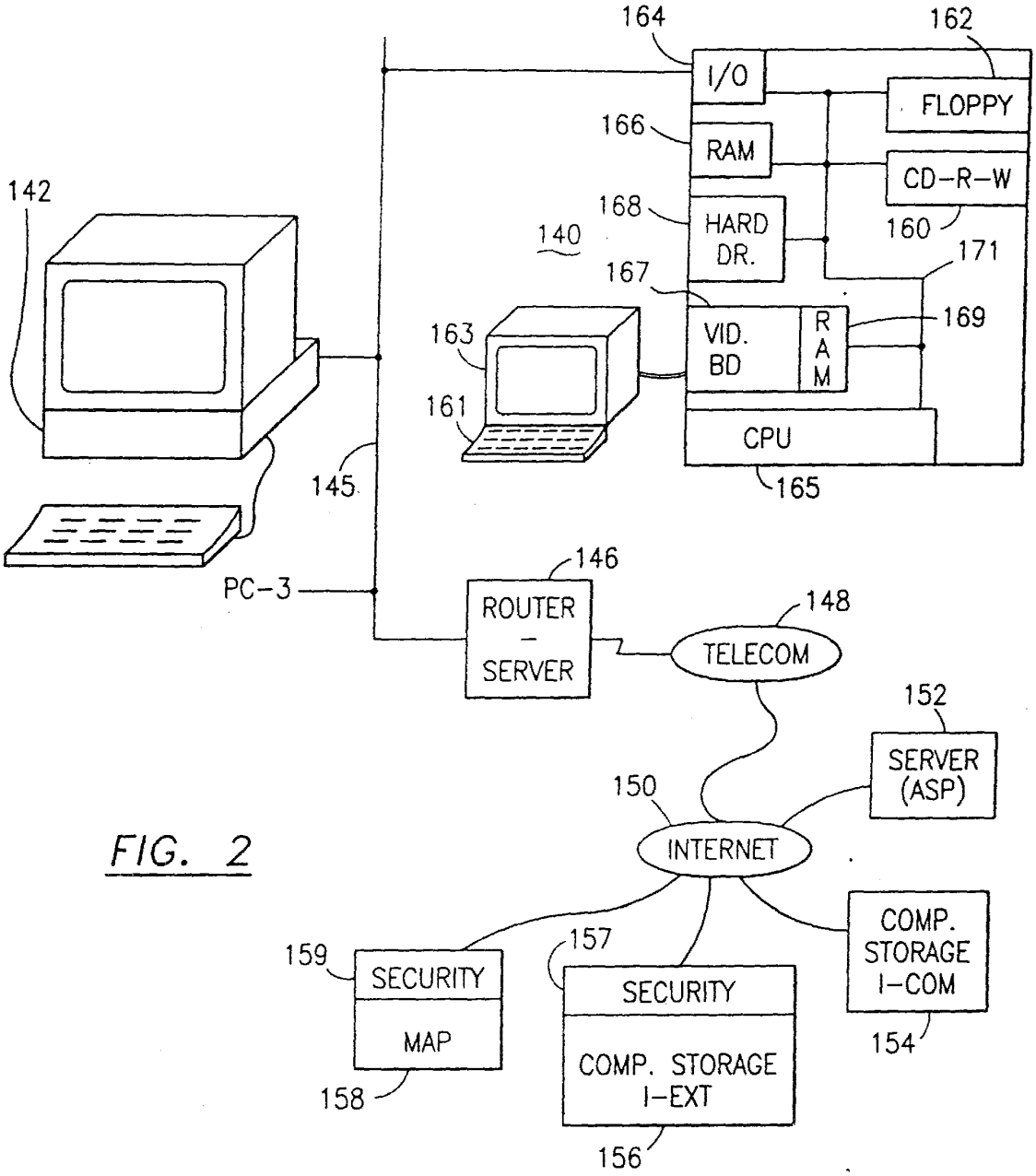
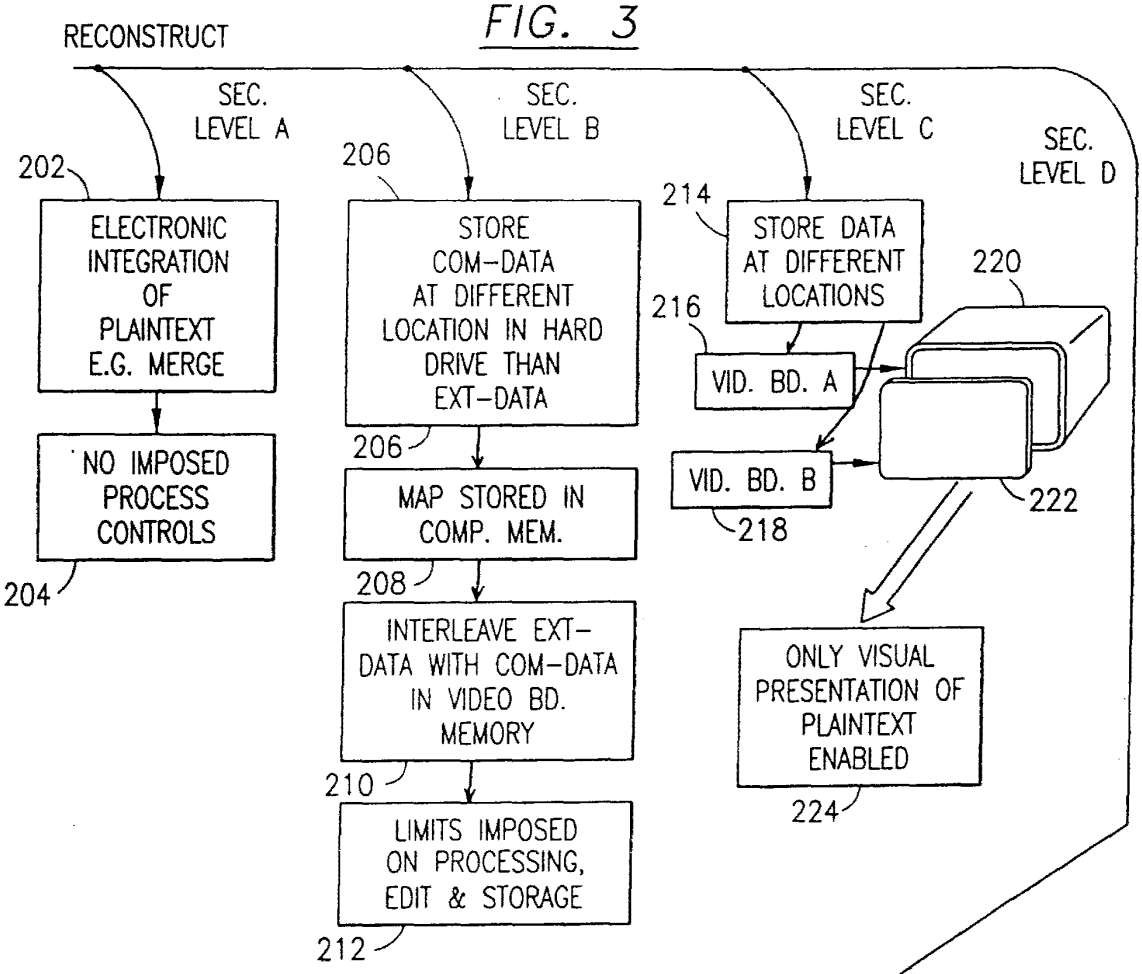

164
162
I/O
FLOPPY
166
RAM
CD-R-W
142
168
HARD DR.
140
160
171
167
169
VID. BD
R A M
163
161
CPU
145
165
146
PC-3
ROUTER – SERVER
148
TELECOM
152
SERVER (ASP)
150
INTERNET
COMP. STORAGE I-COM
159
157
SECURITY
MAP
SECURITY
COMP. STORAGE I-EXT
154
158
156

FIG. 2

FIG. 3


RECONSTRUCT
SEC. LEVEL A
SEC. LEVEL B
SEC. LEVEL C
SEC. LEVEL D
202
ELECTRONIC INTEGRATION OF PLAINTEXT E.G. MERGE
NO IMPOSED PROCESS CONTROLS
204
206
STORE COM-DATA AT DIFFERENT LOCATION IN HARD DRIVE THAN EXT-DATA
206
MAP STORED IN COMP. MEM.
208
INTERLEAVE EXT-DATA WITH COM-DATA IN VIDEO BD. MEMORY
210
LIMITS IMPOSED ON PROCESSING, EDIT & STORAGE
212
214
STORE DATA AT DIFFERENT LOCATIONS
216
VID. BD. A
VID. BD. B
218
220
222
ONLY VISUAL PRESENTATION OF PLAINTEXT ENABLED
224
228
PARSE EXT-DATA PER SECURITY CLEARANCE
226
REPEAT PROCESS A, B OR C WITH ONLY PORTIONS OF EXT-DATA PRESENTED TO USER BASED ON SEC. CLEARANCE

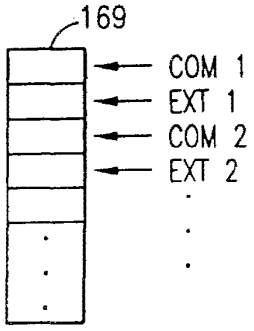
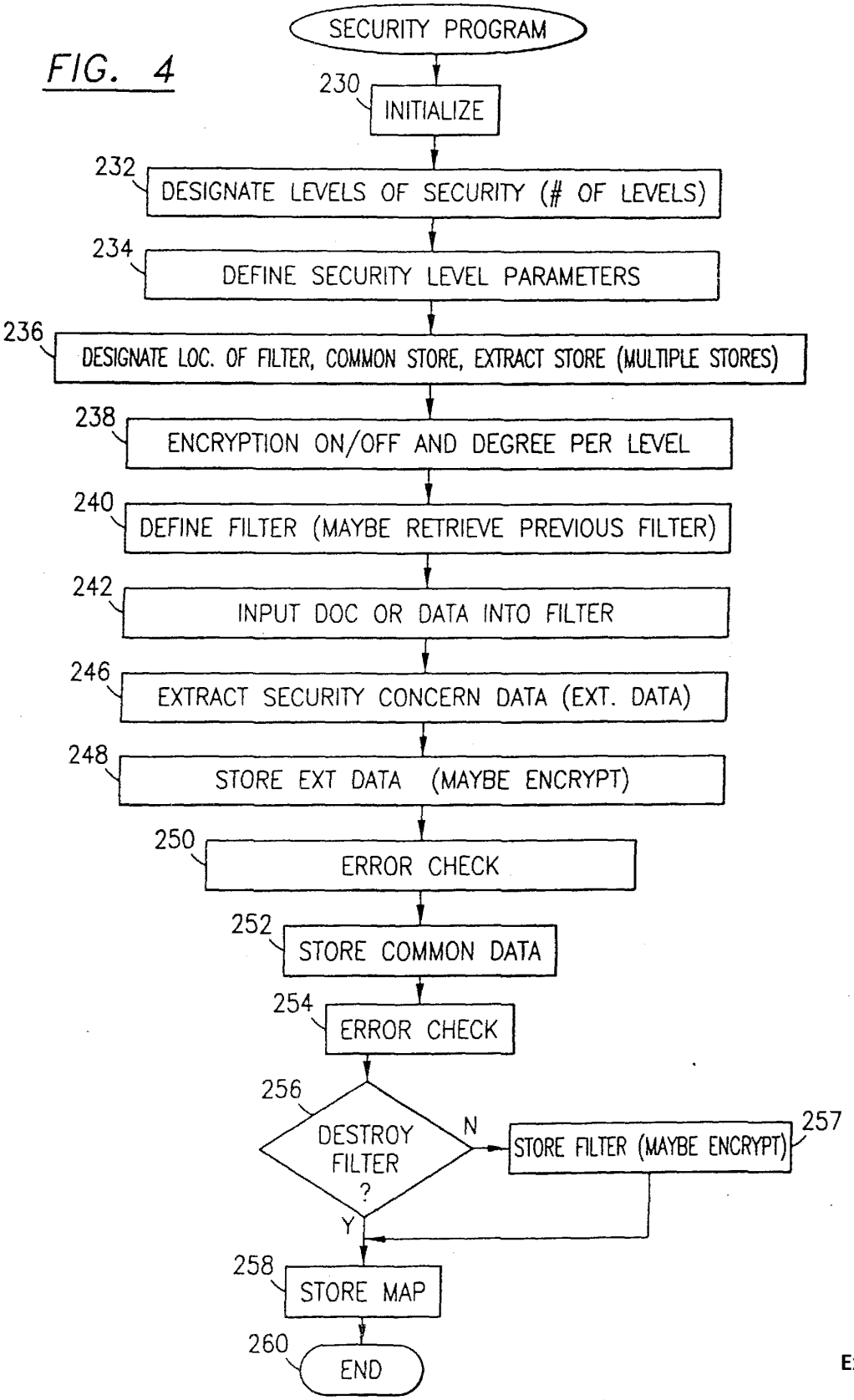

169
COM 1
EXT 1
COM 2
EXT 2

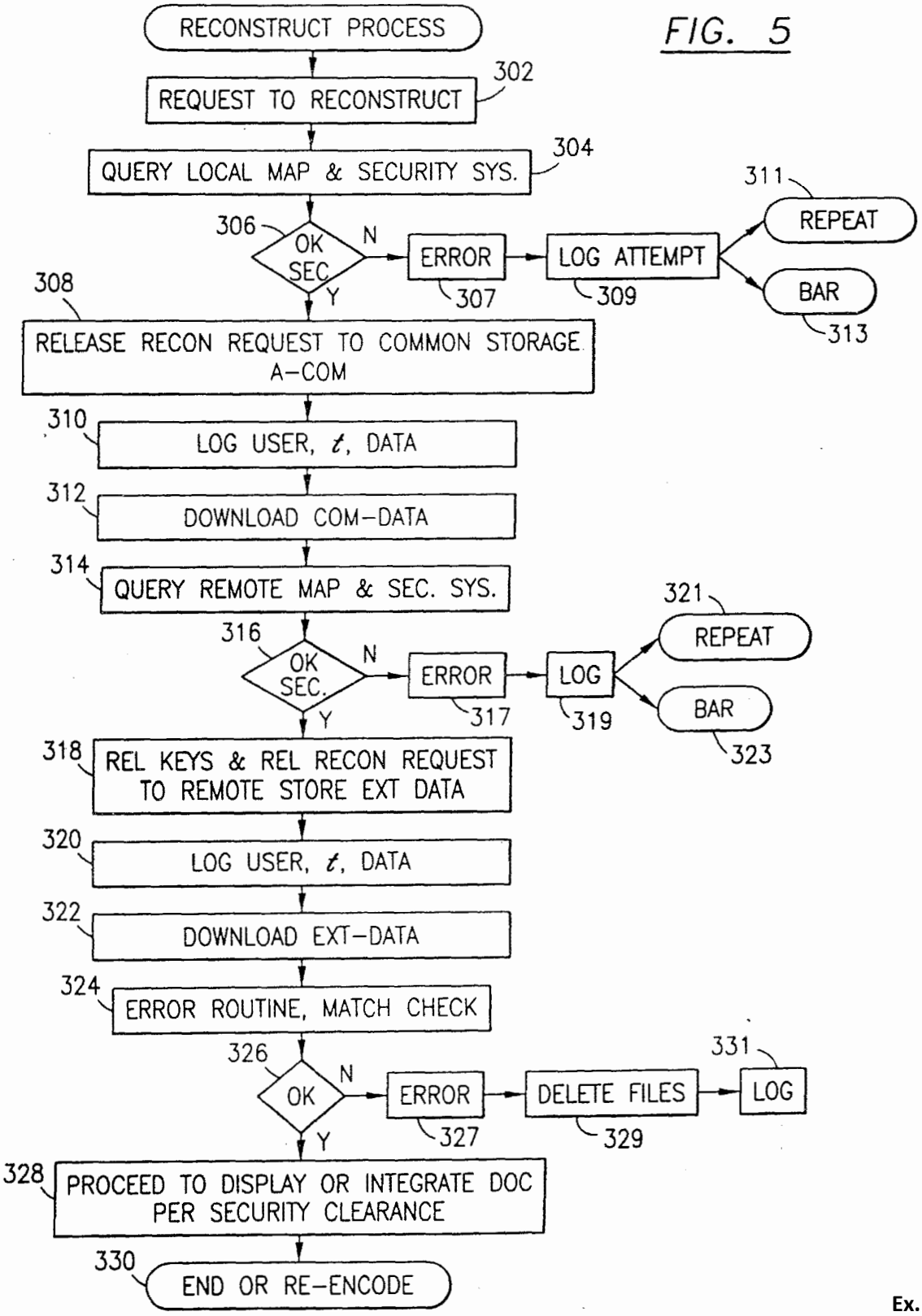
FIG. 3A

FIG. 4


SECURITY PROGRAM
230
INITIALIZE
232
DESIGNATE LEVELS OF SECURITY (# OF LEVELS)
234
DEFINE SECURITY LEVEL PARAMETERS
236
DESIGNATE LOC. OF FILTER, COMMON STORE, EXTRACT STORE (MULTIPLE STORES)
238
ENCRYPTION ON/OFF AND DEGREE PER LEVEL
240
DEFINE FILTER (MAYBE RETRIEVE PREVIOUS FILTER)
242
INPUT DOC OR DATA INTO FILTER
246
EXTRACT SECURITY CONCERN DATA (EXT. DATA)
248
STORE EXT DATA (MAYBE ENCRYPT)
250
ERROR CHECK
252
STORE COMMON DATA
254
ERROR CHECK
256
DESTROY FILTER ?
N
257
STORE FILTER (MAYBE ENCRYPT)
Y
258
STORE MAP
260
END

US 6,148,377

FIG. 5



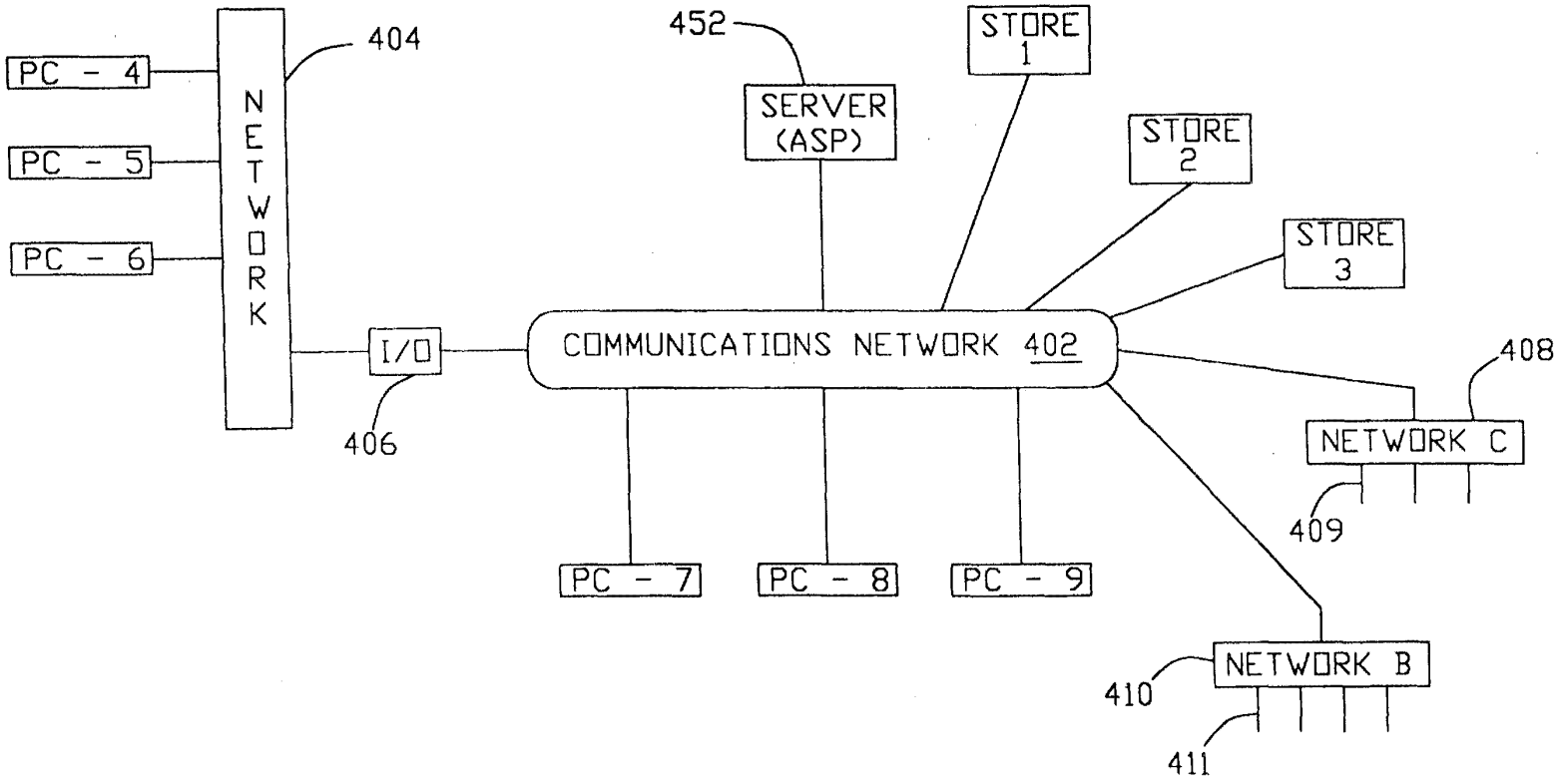


FIG.6

Ex. 1002, Page 145

FIG. 7a

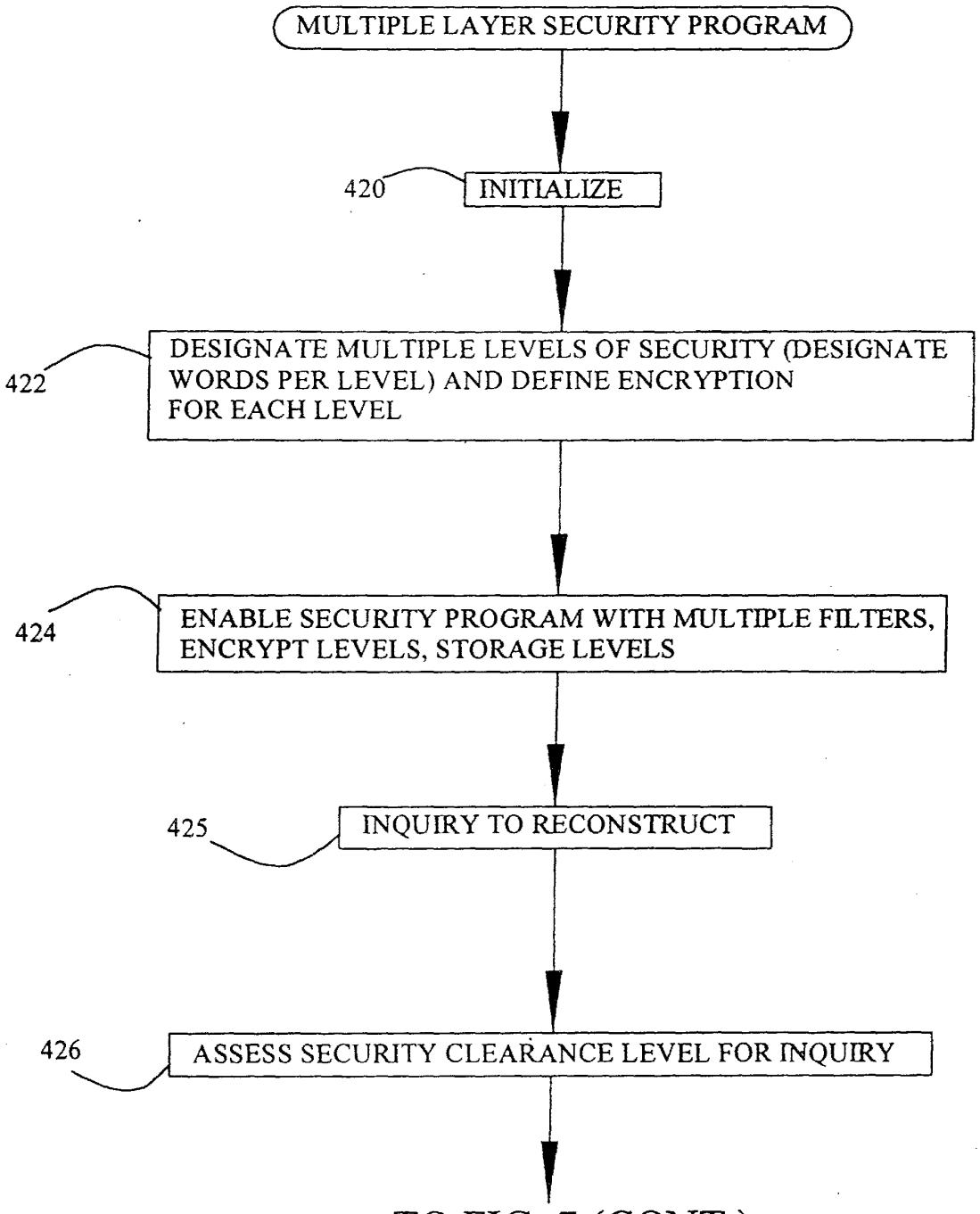
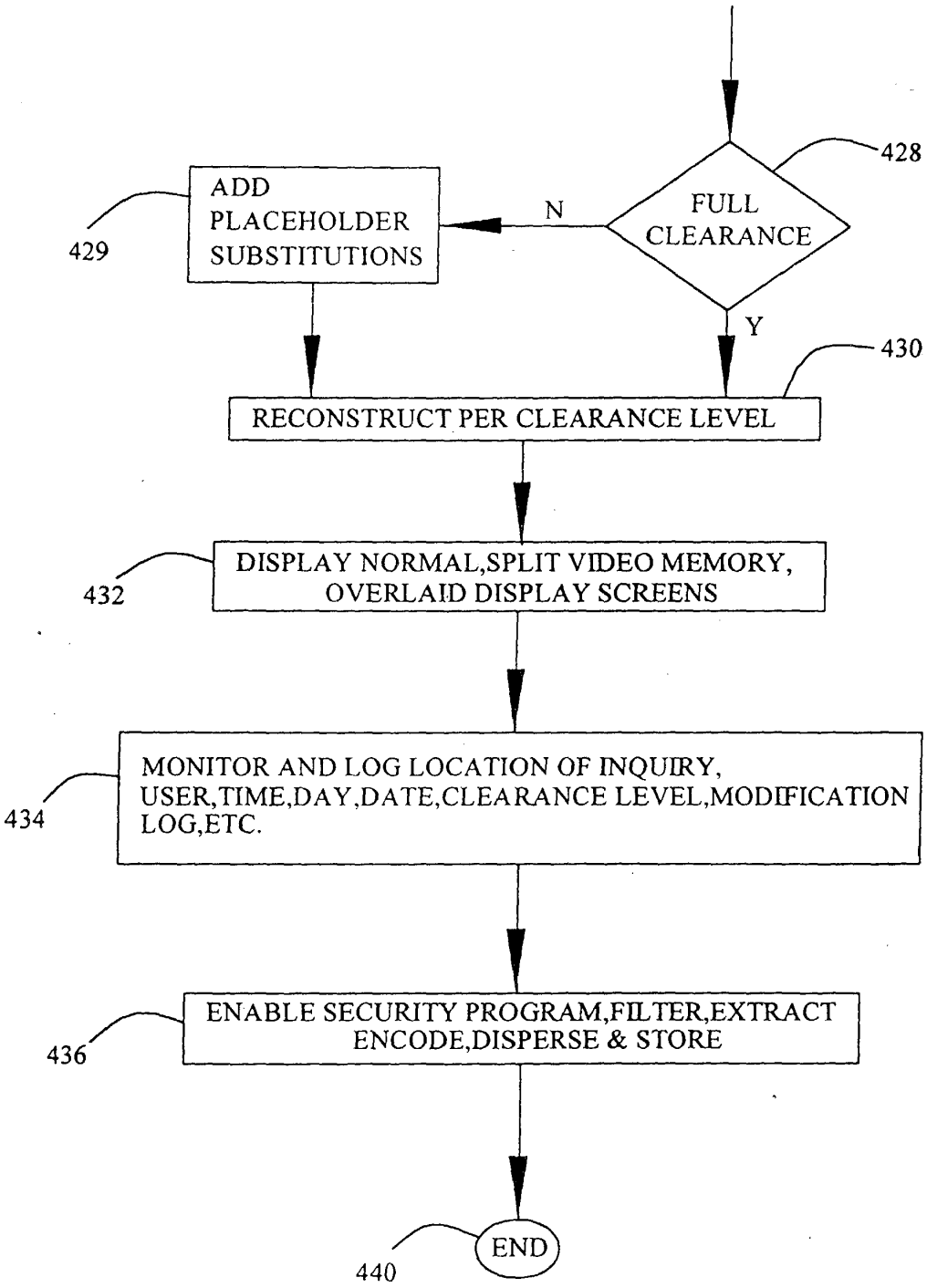

MULTIPLE LAYER SECURITY PROGRAM
420
INITIALIZE
422
DESIGNATE MULTIPLE LEVELS OF SECURITY (DESIGNATE WORDS PER LEVEL) AND DEFINE ENCRYPTION FOR EACH LEVEL
424
ENABLE SECURITY PROGRAM WITH MULTIPLE FILTERS, ENCRYPT LEVELS, STORAGE LEVELS
425
INQUIRY TO RECONSTRUCT
426
ASSESS SECURITY CLEARANCE LEVEL FOR INQUIRY
TO FIG. 7a(CONT.)

FIG. 7a(CONT.)


428
FULL CLEARANCE
N
ADD PLACEHOLDER SUBSTITUTIONS
429
Y
430
RECONSTRUCT PER CLEARANCE LEVEL
DISPLAY NORMAL,SPLIT VIDEO MEMORY, OVERLAID DISPLAY SCREENS
432
MONITOR AND LOG LOCATION OF INQUIRY, USER,TIME,DAY,DATE,CLEARANCE LEVEL,MODIFICATION LOG,ETC.
434
ENABLE SECURITY PROGRAM,FILTER,EXTRACT ENCODE,DISPERSE & STORE
436
END
440

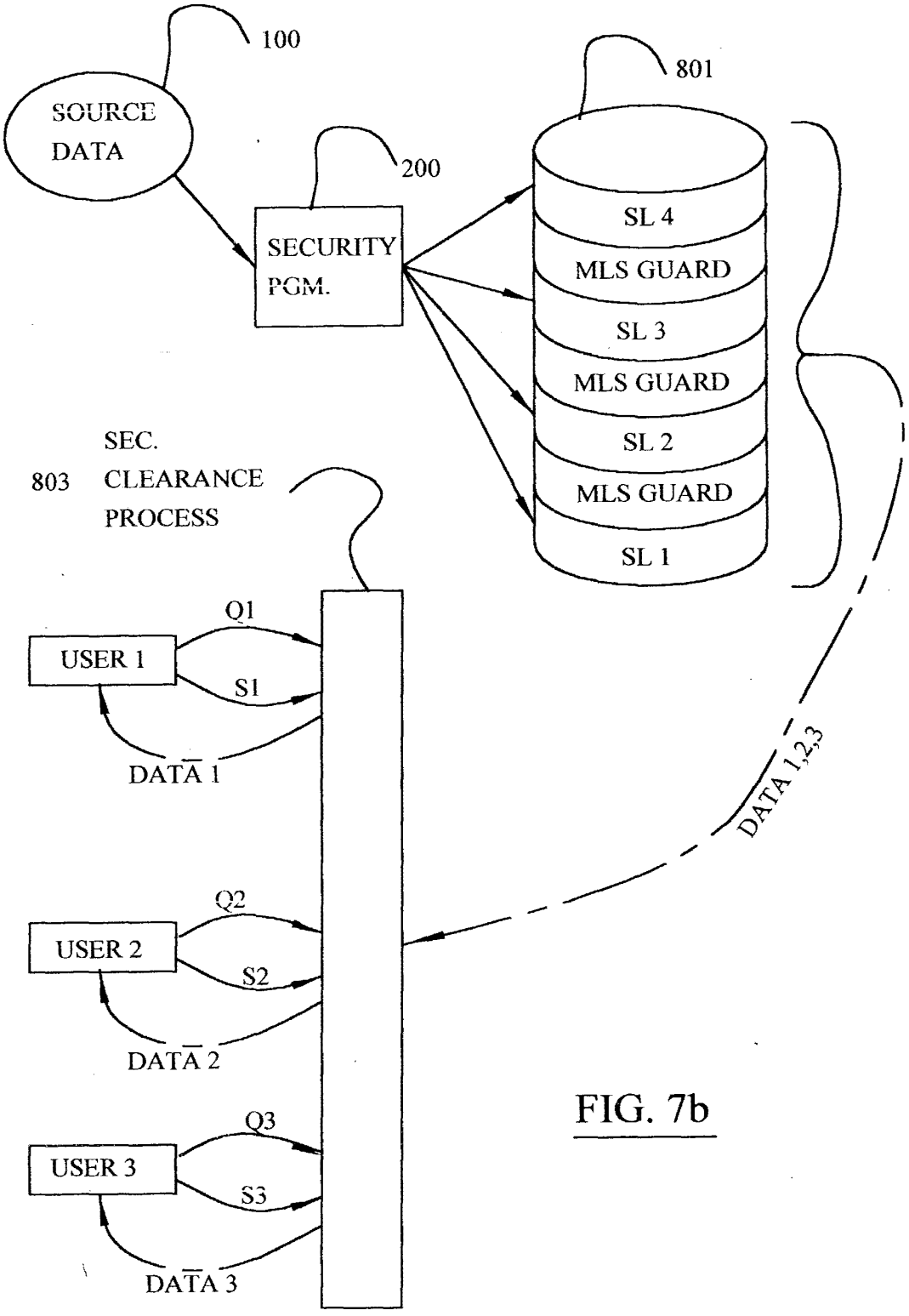

100
SOURCE DATA
200
SECURITY PGM.
801
SL 4
MLS GUARD
SL 3
MLS GUARD
SL 2
MLS GUARD
SL 1
803
SEC. CLEARANCE PROCESS
Q1
USER 1
S1
DATA 1
DATA 1,2,3
Q2
USER 2
S2
DATA 2
Q3
USER 3
S3
DATA 3

FIG. 7b

FIG. 8

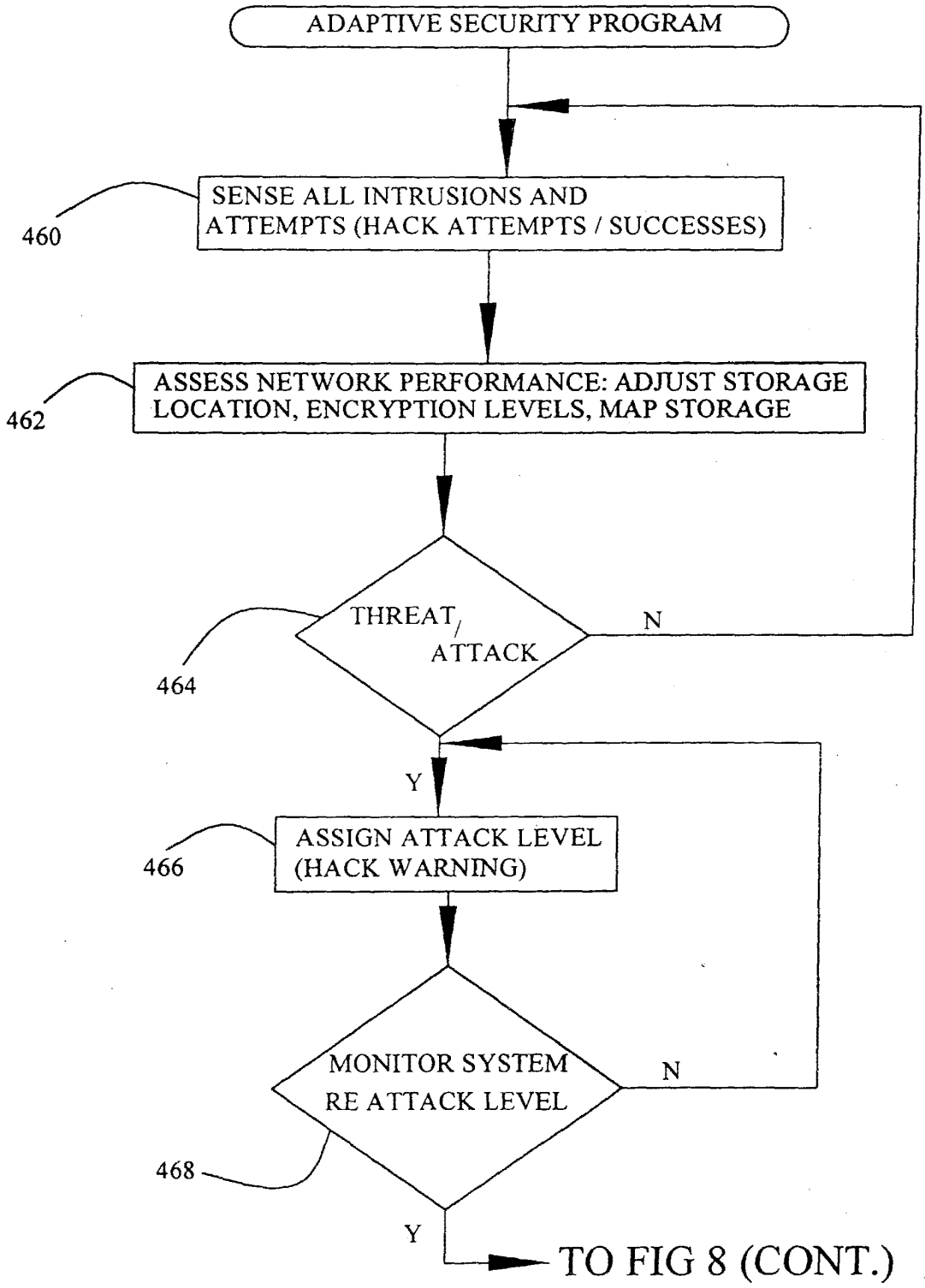

ADAPTIVE SECURITY PROGRAM
460
SENSE ALL INTRUSIONS AND ATTEMPTS (HACK ATTEMPTS / SUCCESSES)
462
ASSESS NETWORK PERFORMANCE: ADJUST STORAGE LOCATION, ENCRYPTION LEVELS, MAP STORAGE
464
THREAT/ ATTACK
N
Y
466
ASSIGN ATTACK LEVEL (HACK WARNING)
MONITOR SYSTEM RE ATTACK LEVEL
N
468
Y
TO FIG 8 (CONT.)

FIG. 8 (CONT.)

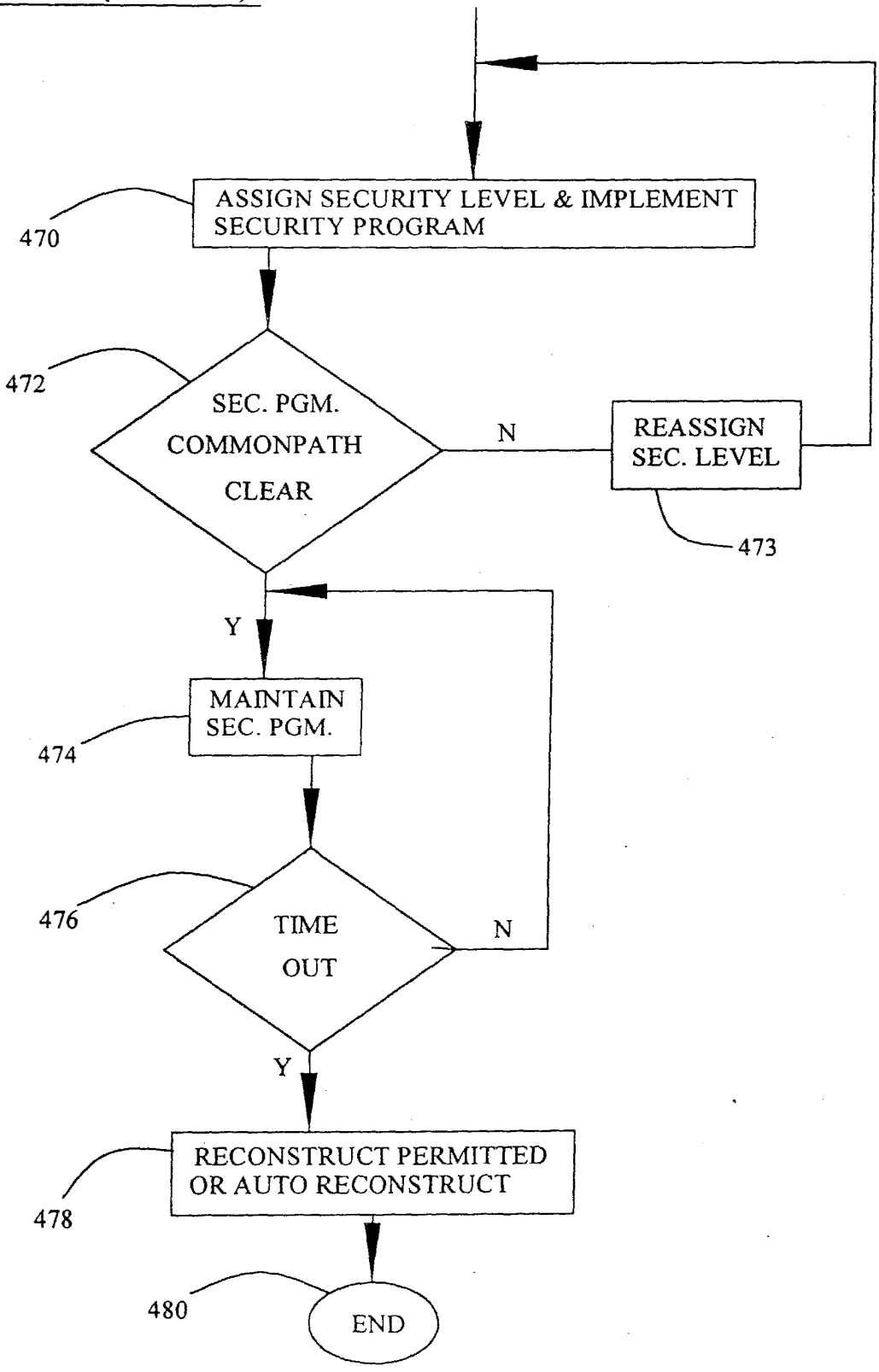

ASSIGN SECURITY LEVEL & IMPLEMENT SECURITY PROGRAM
470
SEC. PGM. COMMONPATH CLEAR
472
N
REASSIGN SEC. LEVEL
473
Y
MAINTAIN SEC. PGM.
474
TIME OUT
476
N
Y
RECONSTRUCT PERMITTED OR AUTO RECONSTRUCT
478
END
480

FIG. 9

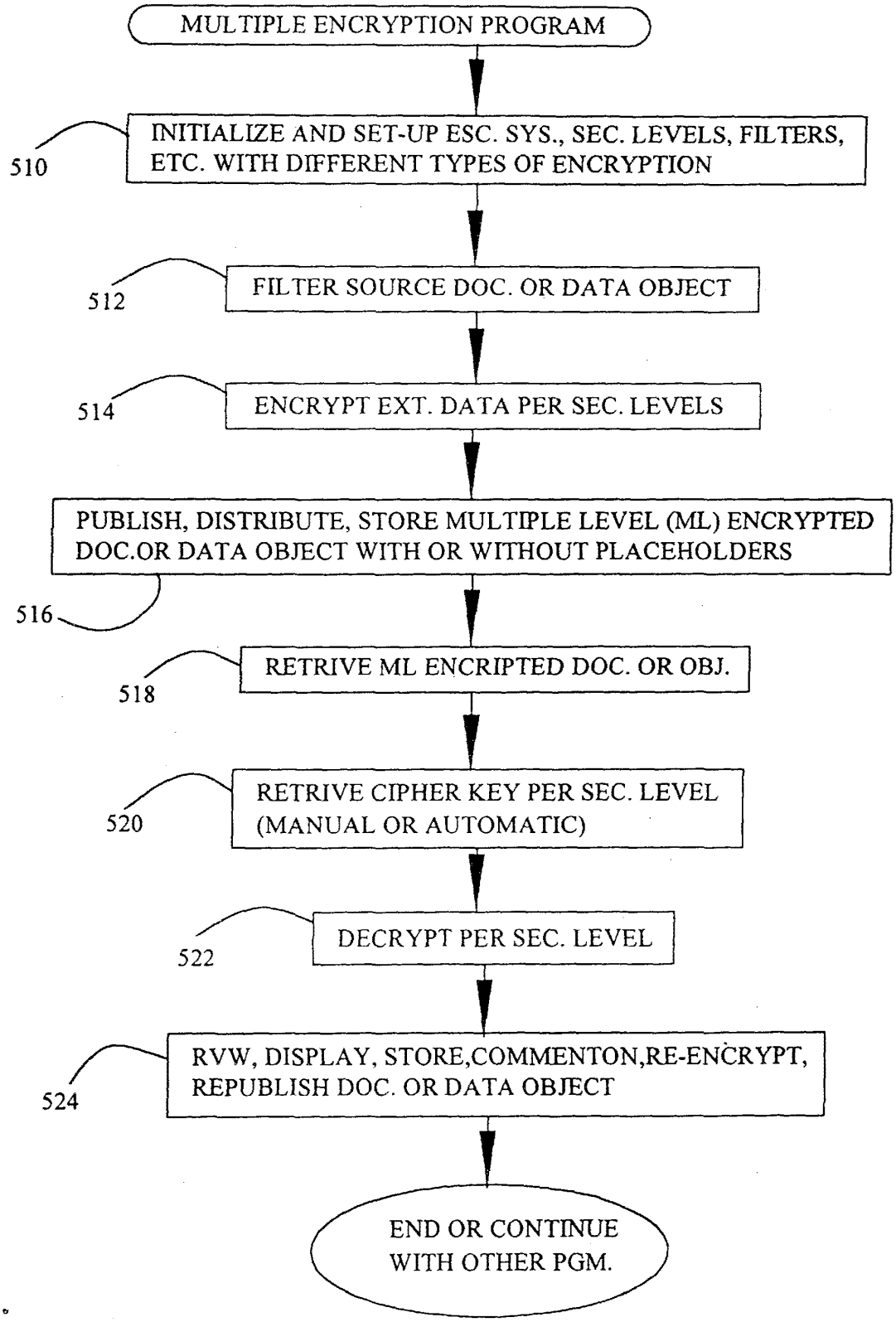
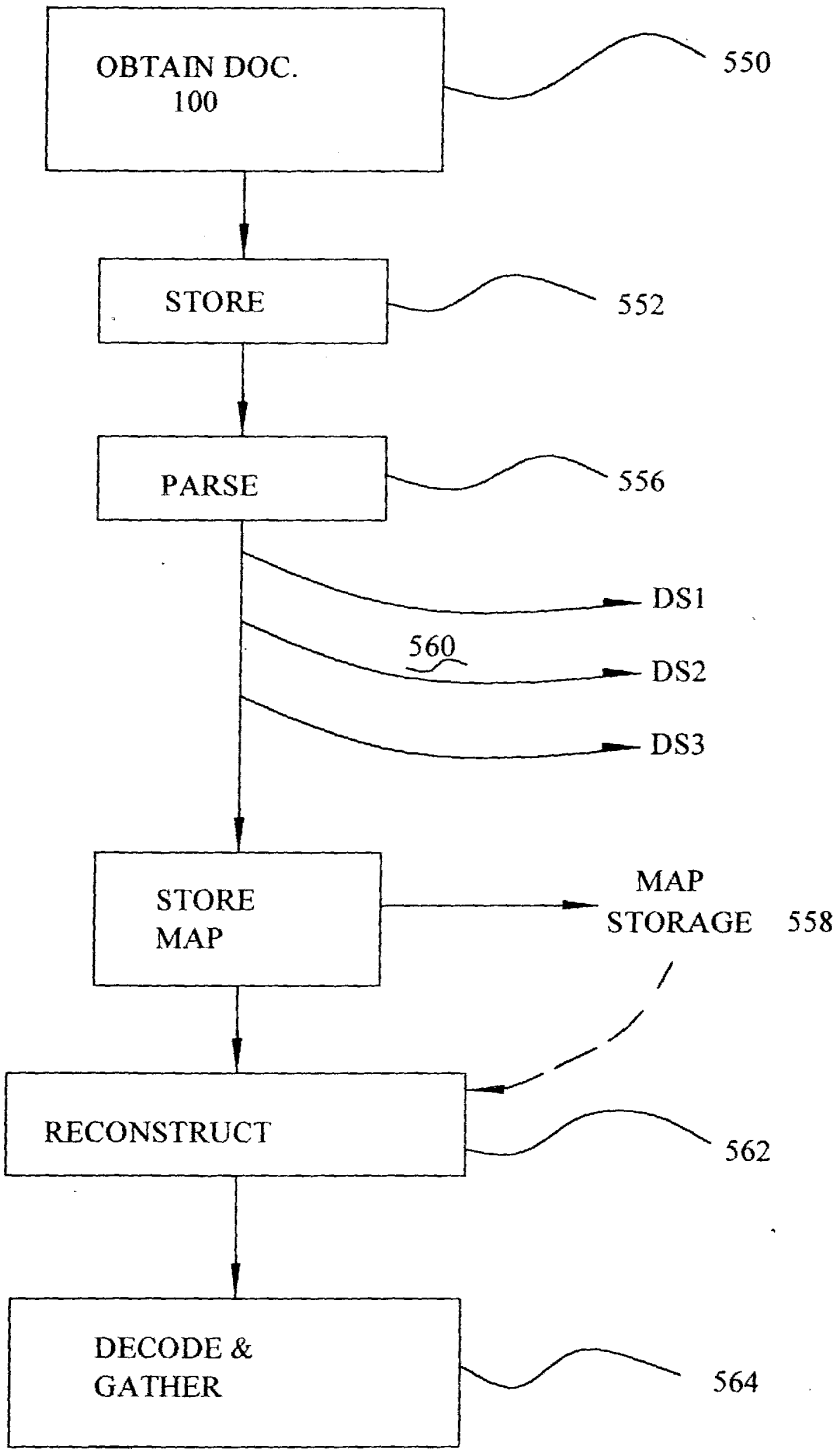

MULTIPLE ENCRYPTION PROGRAM
510
INITIALIZE AND SET-UP ESC. SYS., SEC. LEVELS, FILTERS, ETC. WITH DIFFERENT TYPES OF ENCRYPTION
512
FILTER SOURCE DOC. OR DATA OBJECT
514
ENCRYPT EXT. DATA PER SEC. LEVELS
PUBLISH, DISTRIBUTE, STORE MULTIPLE LEVEL (ML) ENCRYPTED DOC.OR DATA OBJECT WITH OR WITHOUT PLACEHOLDERS
516
518
RETRIVE ML ENCRIPTED DOC. OR OBJ.
520
RETRIVE CIPHER KEY PER SEC. LEVEL (MANUAL OR AUTOMATIC)
522
DECRYPT PER SEC. LEVEL
524
RVW, DISPLAY, STORE,COMMENTON,RE-ENCRYPT, REPUBLISH DOC. OR DATA OBJECT
END OR CONTINUE WITH OTHER PGM.

FIG. 10


OBTAIN DOC.
100
550
STORE
552
PARSE
556
DS1
560
DS2
DS3
STORE
MAP
MAP
STORAGE
558
RECONSTRUCT
562
DECODE &
GATHER
564

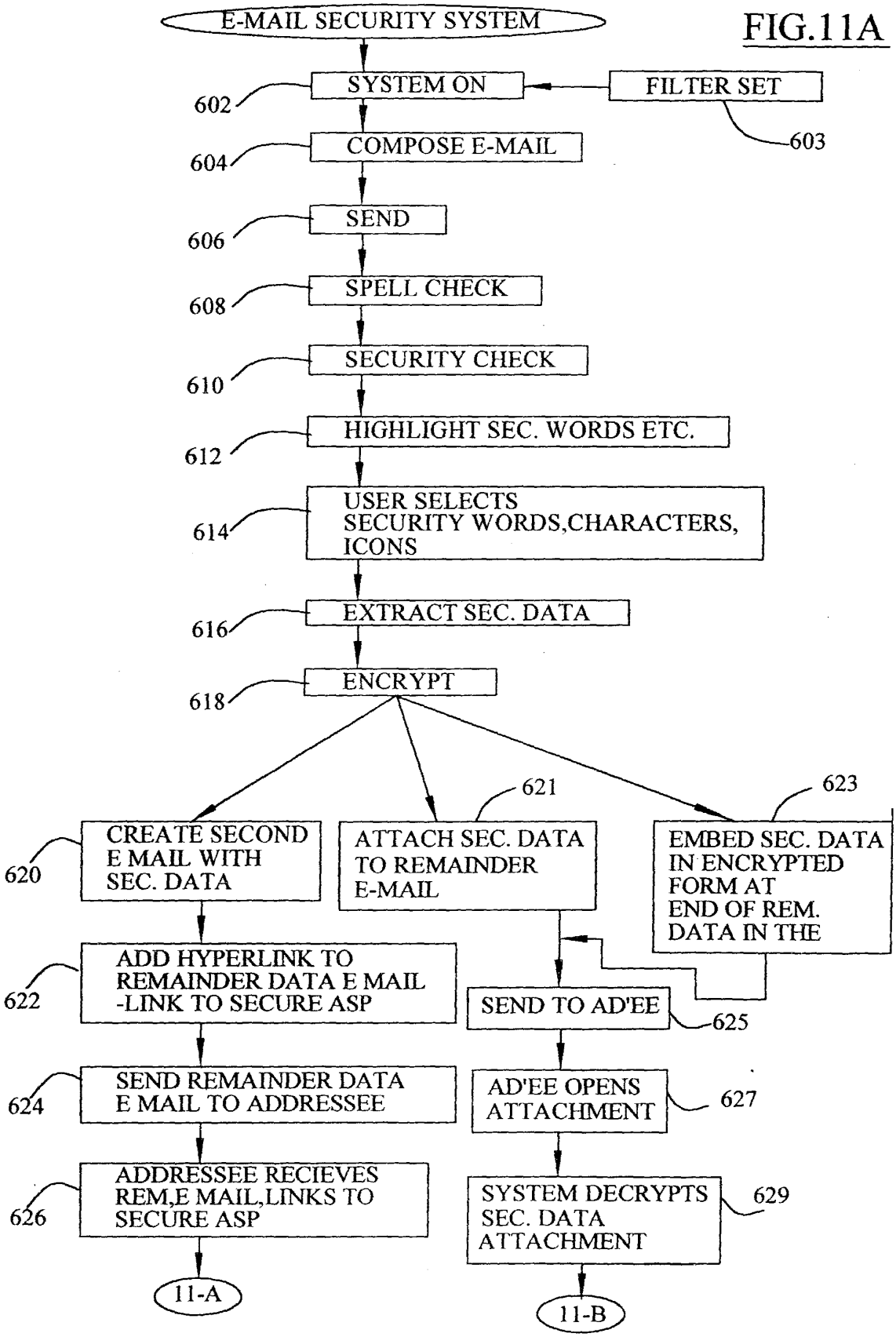

E-MAIL SECURITY SYSTEM
SYSTEM ON
FILTER SET
602
603
COMPOSE E-MAIL
604
SEND
606
SPELL CHECK
608
SECURITY CHECK
610
HIGHLIGHT SEC. WORDS ETC.
612
USER SELECTS SECURITY WORDS,CHARACTERS, ICONS
614
EXTRACT SEC. DATA
616
ENCRYPT
618
621
623
CREATE SECOND E MAIL WITH SEC. DATA
620
ATTACH SEC. DATA TO REMAINDER E-MAIL
EMBED SEC. DATA IN ENCRYPTED FORM AT END OF REM. DATA IN THE
ADD HYPERLINK TO REMAINDER DATA E MAIL -LINK TO SECURE ASP
622
SEND TO AD'EE
625
SEND REMAINDER DATA E MAIL TO ADDRESSEE
624
AD'EE OPENS ATTACHMENT
627
ADDRESSEE RECIEVES REM,E MAIL,LINKS TO SECURE ASP
626
SYSTEM DECRYPTS SEC. DATA ATTACHMENT
629
11-A
11-B

FIG.11A

FIG.11B

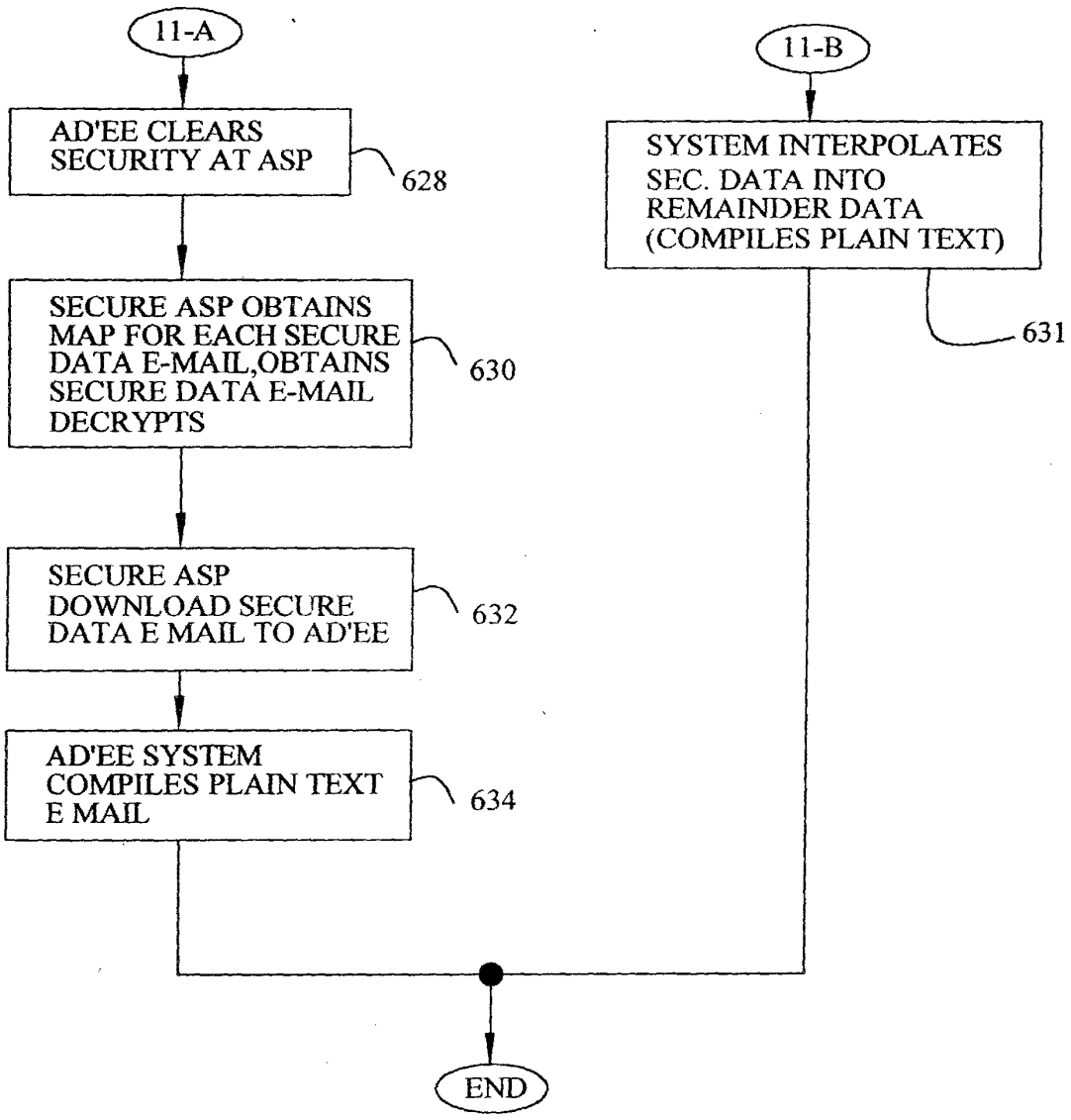

11-A
AD'EE CLEARS SECURITY AT ASP
628
SECURE ASP OBTAINS MAP FOR EACH SECURE DATA E-MAIL,OBTAINS SECURE DATA E-MAIL DECRYPTS
630
SECURE ASP DOWNLOAD SECURE DATA E MAIL TO AD'EE
632
AD'EE SYSTEM COMPILES PLAIN TEXT E MAIL
634
11-B
SYSTEM INTERPOLATES SEC. DATA INTO REMAINDER DATA (COMPILES PLAIN TEXT)
631
END

FIG.12A

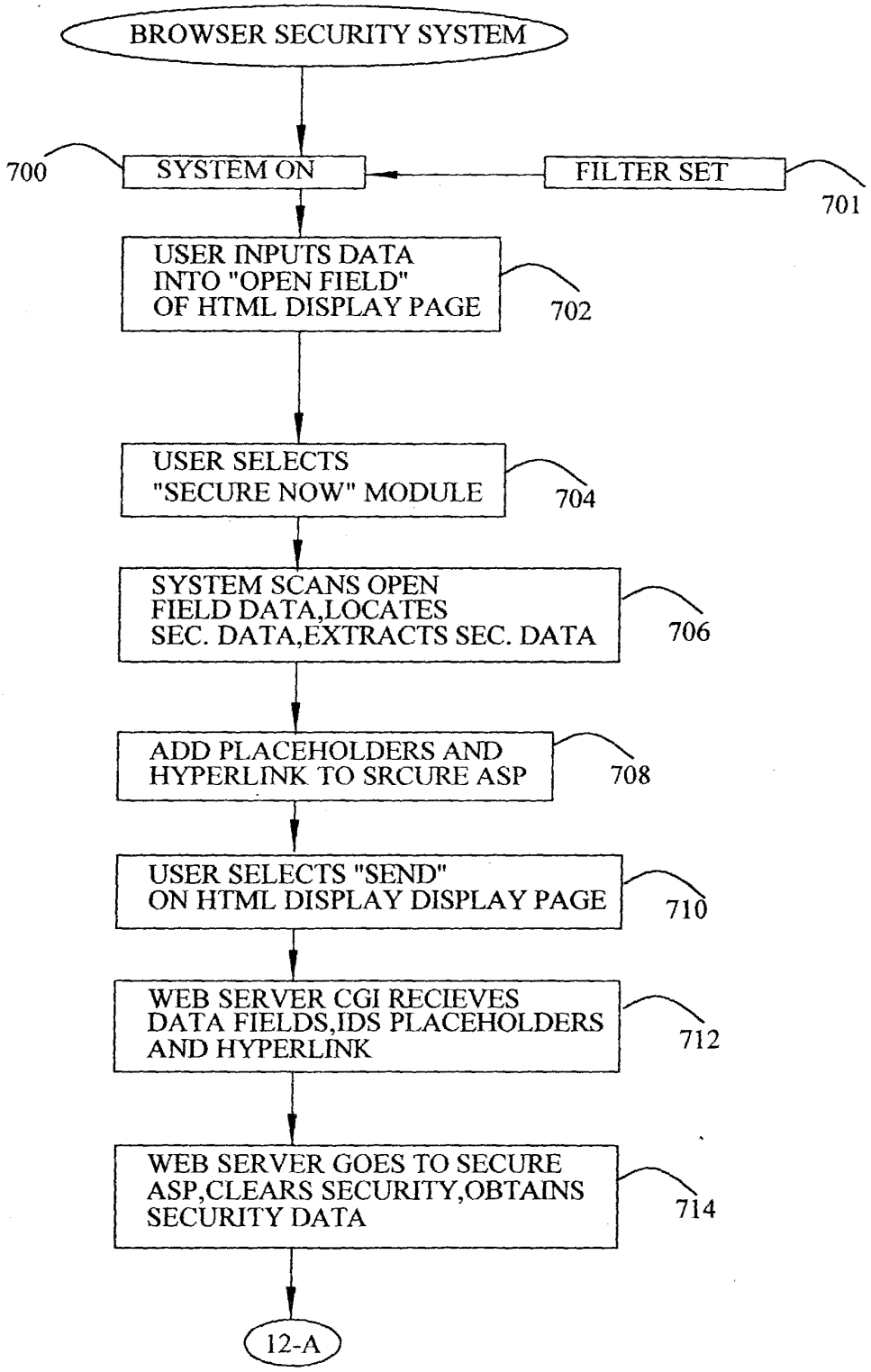
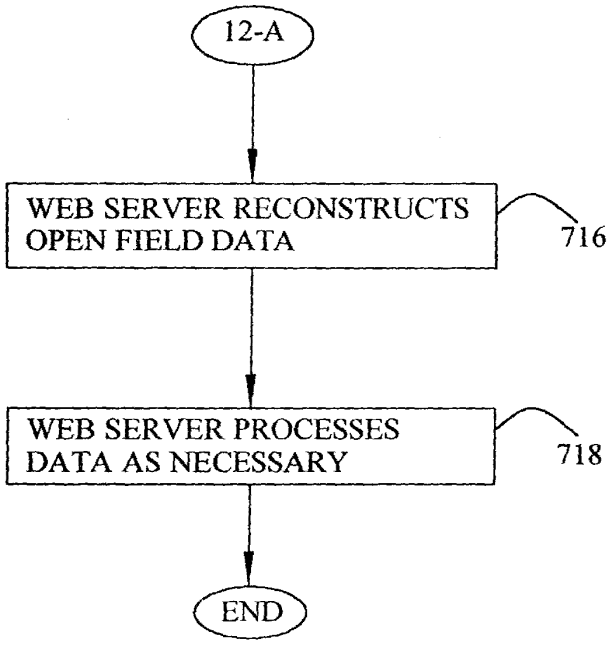

BROWSER SECURITY SYSTEM
700
SYSTEM ON
FILTER SET
701
USER INPUTS DATA INTO "OPEN FIELD" OF HTML DISPLAY PAGE
702
USER SELECTS "SECURE NOW" MODULE
704
SYSTEM SCANS OPEN FIELD DATA,LOCATES SEC. DATA,EXTRACTS SEC. DATA
706
ADD PLACEHOLDERS AND HYPERLINK TO SRCURE ASP
708
USER SELECTS "SEND" ON HTML DISPLAY DISPLAY PAGE
710
WEB SERVER CGI RECIEVES DATA FIELDS,IDS PLACEHOLDERS AND HYPERLINK
712
WEB SERVER GOES TO SECURE ASP,CLEARS SECURITY,OBTAINS SECURITY DATA
714
12-A

FIG.12B


12-A
WEB SERVER RECONSTRUCTS OPEN FIELD DATA
716
WEB SERVER PROCESSES DATA AS NECESSARY
718
END

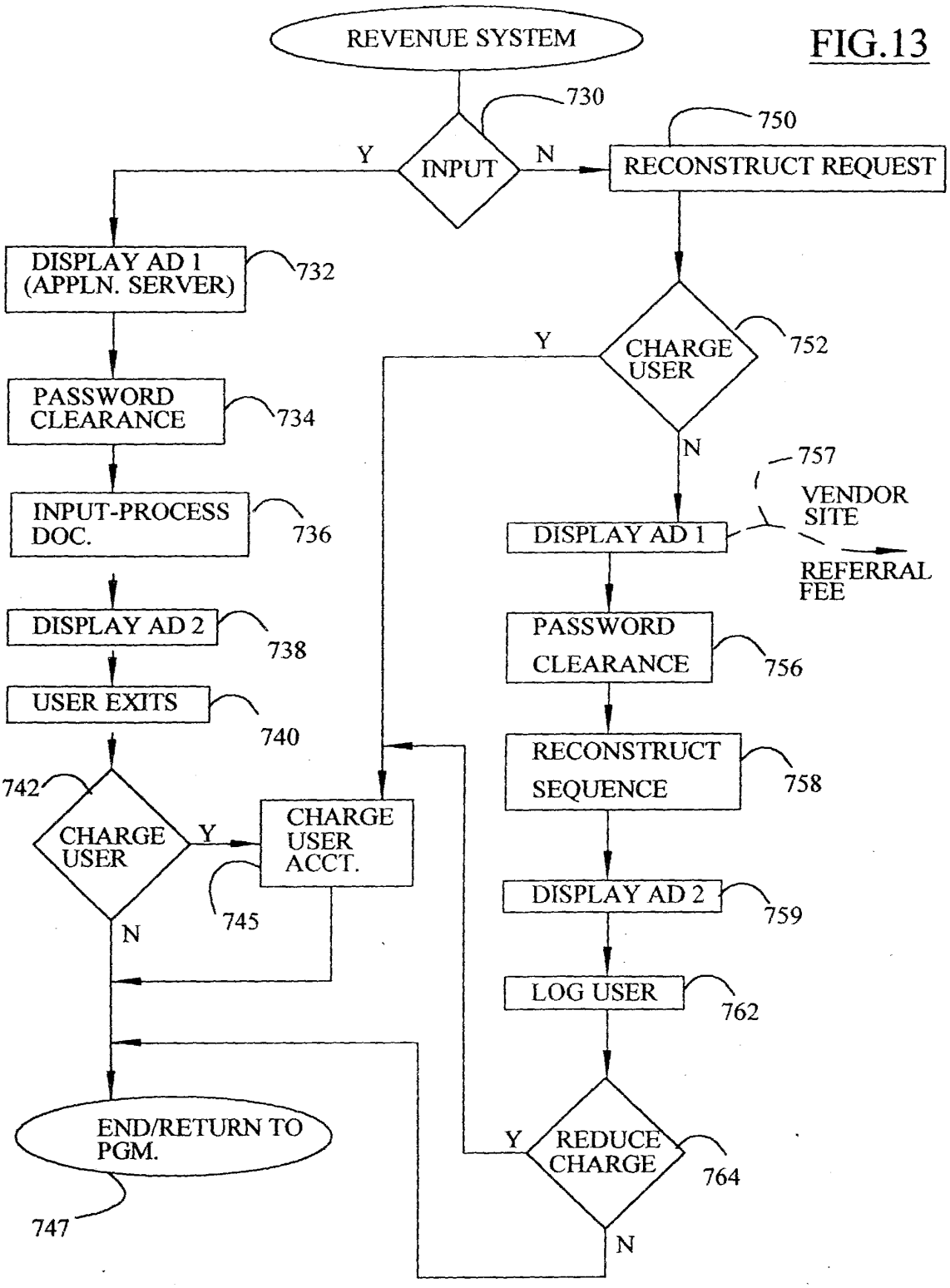

REVENUE SYSTEM
730
INPUT
Y
N
750
RECONSTRUCT REQUEST
DISPLAY AD 1 (APPLN. SERVER)
732
PASSWORD CLEARANCE
734
INPUT-PROCESS DOC.
736
DISPLAY AD 2
738
USER EXITS
740
742
CHARGE USER
Y
CHARGE USER ACCT.
745
N
747
END/RETURN TO PGM.
CHARGE USER
752
Y
N
757
VENDOR SITE
REFERRAL FEE
DISPLAY AD 1
PASSWORD CLEARANCE
756
RECONSTRUCT SEQUENCE
758
DISPLAY AD 2
759
LOG USER
762
REDUCE CHARGE
764
Y
N

FIG.13

SCANNED

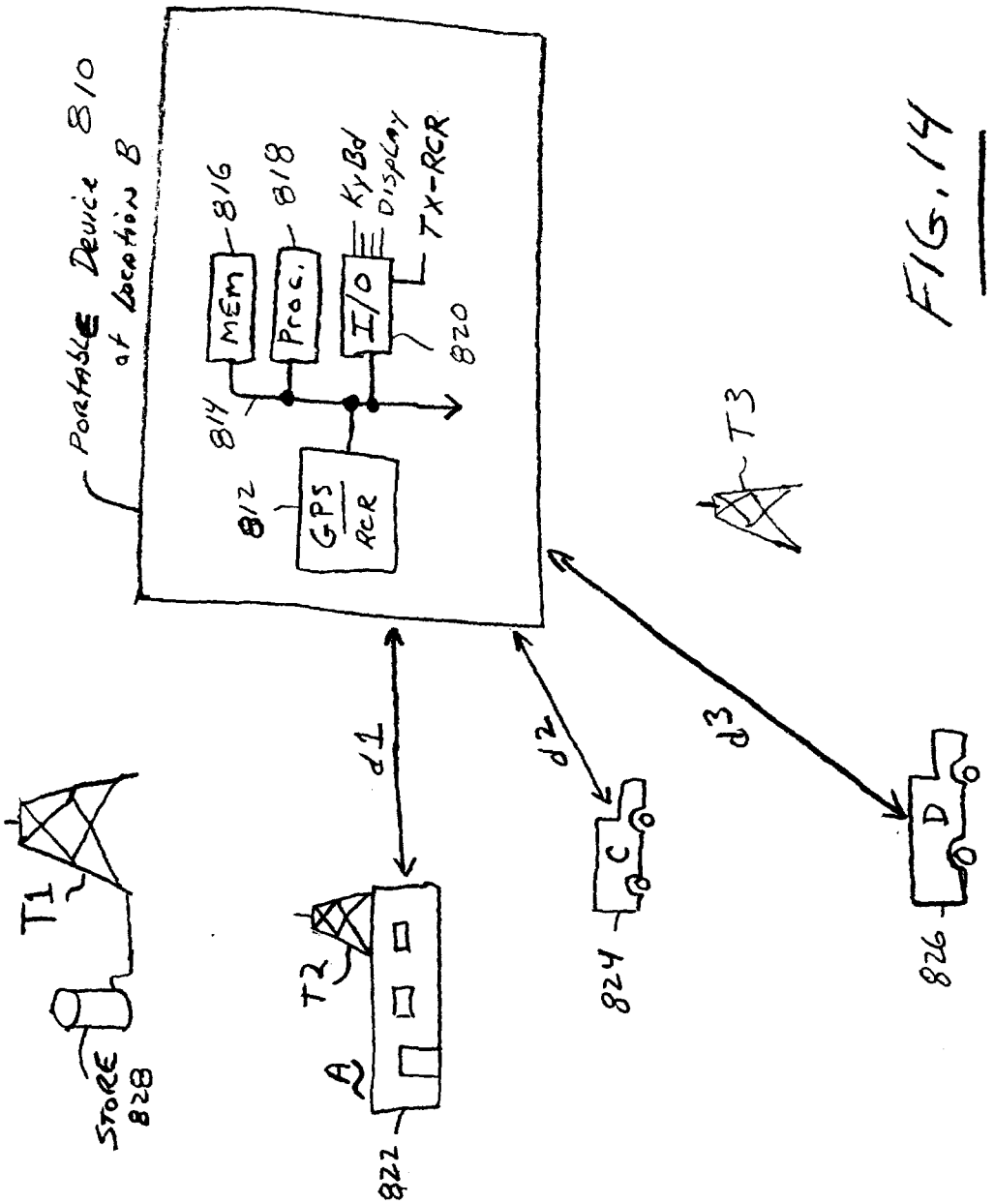


FIG. 14

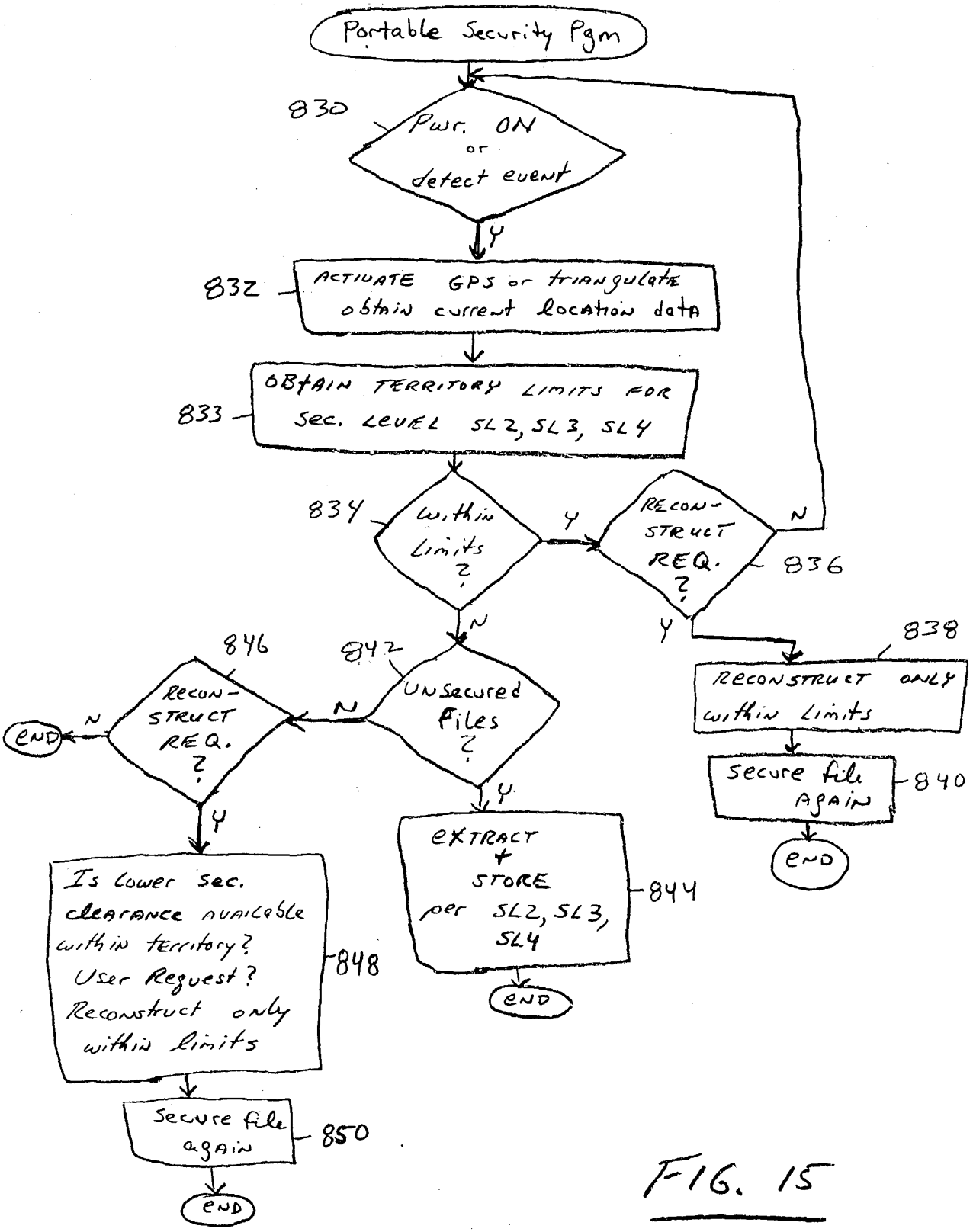

Portable Security Pgm
830
Pwr. ON or detect event
Y
832
ACTUATE GPS or triangulate obtain current location data
833
OBTAIN TERRITORY LIMITS FOR Sec. LEVEL SL2, SL3, SL4
834
Within Limits ?
Y
RECON-STRUCT REQ. ?
N
836
N
Y
838
RECONSTRUCT ONLY within Limits
Secure file AGAIN
840
END
842
UNSecured Files ?
N
846
RECON-STRUCT REQ. ?
N
END
Y
Y
EXTRACT + STORE per SL2, SL3, SL4
844
END
Is Lower Sec. clearance AVAILABLE within territory? User Request? Reconstruct only within limits
848
Secure file again
850
END

FIG. 15

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled Data Security System and Method For Portable Device the specification of which

(check one) ☒ is attached hereto.

☐ was filed on _____

as Application Serial No. _____

and was amended on _____. (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
_____	_____	_____	☐	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
_____	_____	_____	☐	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

10/277,196	01/02/03	pending
(Application Serial No.)	(Filing Date)	(Status)
09/916,397	07/27/01	pending
(Application Serial No.)	(Filing Date)	(Status)
10/008,209	12/6/01	pending
(Application Serial No.)	(Filing Date)	(Status)
10/008,218	12/6/01	pending
(Application Serial No.)	(Filing Date)	(Status)
10/115,192	05/23/02	pending
(Application Serial No.)	(Filing Date)	(Status)
10/155.525	05/23/02	pending
(Application Serial No.)	(Filing Date)	(Status)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

60/260,398, filed June 5, 2001 60/287,813, filed May 2, 2001 60/267,944, filed February 12, 2001

[redacted]

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

60/260,398, filed June 5, 2001 (Provisional Application No.)
60/287,813, filed May 2, 2001 (Provisional Application No.)
60/267,944, filed February 12, 2001 (Provisional Application No.)

60/247,242, filed November 12, 2000 (Provisional Application No.)
60/247,232, filed November 13, 2000 (Provisional Application No.)
60/400,062, filed August 2,2002 (Provisional Application No.)

60,400,112, filed August 2, 2002 (Provisional Application No.)
60/400,406, filed August 2, 2002 (Provisional Application No.)
60/400,407, filed August 2, 2002 (Provisional Application No.)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.
POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.
Robert C. Kain, Jr., Reg. No. 30,648; Martin Fleit, Reg. No. 16,900; Jon A. Gibbons, Reg. No. 37,333; Jose Gutman Reg. No. 35,171; Steve Bongini, Reg. No. 40,917; and Paul D. Bianco, Reg. 43,5000.

Send Correspondence to: Robert C. Kain, Jr., **Customer Number 004897**
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Direct Telephone Calls to: Robert C. Kain, Jr., (954) 768-9002

Ron M. Redlich
Full name of sole or first inventor

Inventor's signature ← Date 3.11.03

Miami Beach, FL
Residence

U.S.
Citizenship

4201 Collins Avenue, Apt. 2103
Post Office Address

Miami Beach, FL 33140

Martin A. Nemzow
Full name of second joint inventor, if any

Inventor's signature ← Date 3-11-2003

Miami Beach, FL
Residence

U.S.
Citizenship

2915 Flamingo Drive
Post Office Address

Miami Beach, FL 33140
(Supply similar information and signature for third and subsequent joint inventors.)

jc658 U.S. PTO
03/19/03

10390807.031903

PATENTS

j1032 U.S. PTO
10/390807
03/19/03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Ron M. Redlich, et al.

Serial No.:

Filed: Herewith

For: Data Security System and Method for Portable Device

TRANSMITTAL AND CERTIFICATE OF EXPRESS MAILING

BOX PATENT APPLICATION
Commissioner for Patents
Washington, D.C. 20231

Sir:

I HEREBY CERTIFY that the below listed documents are being ~~deposited with the United States Postal Service "Express Mail Post Office to Address," Mailing Label No. EL220374395US, under 37 C.F.R. 1.10~~ mailed via Fed Express, next day delivery on March 17, 2003 and are addressed to Box Patent Application, Commissioner for Patents, Washington, D.C. 20231.

X Patent application (137 pgs.; 146 clms.)

X Twenty (20) sheets drawings -(18 formal; 2 informal)

X Declaration and Power of Attorney for Patent Application (2 pgs.)

X Assignment to Digital Doors, Inc. w/assignment cover sheet (5 pages)

X IDS and Form PTO-1449 (7 pgs.) with thirty-six (36) references

X Please charge Deposit Account No. 03-1231 in the amount of $1,759.00

X Fee calculation letter (1pg.) (duplicate)

X Return receipt postcard.

X Please charge any underpayments or credit any overpayments to Deposit Account No. 03-1231. A duplicate copy of this transmittal is enclosed.

Respectfully submitted,

By_____
Ellen Kotler

By_____
Robert C. Kain, Jr.
Reg. No. 30,648
FLEIT, KAIN, GIBBONS, GUTMAN & BONGINI, P.L.
750 S.E. Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Facsimile: (954) 768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-2-cip-5 express maill transmittal to pto.wpd

FLEIT, KAIN, GIBBONS, GUTMAN & BONGINI P.L.
ATTORNEYS AT LAW
Miami • Fort Lauderdale • Boca Raton

750 Southeast Third Avenue
Suite 100
Fort Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Toll Free: (800) 846-0900
Facsimile: (954) 768-0158
www.FocusOnIP.com
Robert C. Kain, Jr. rkain@FocusOnIP.com
William R. Trueba, Jr. wtrueba@FocusOnIP.com

March 17, 2003

Commissioner for Patents
Washington, D.C. 20231

Transmitted herewith for filing are papers related to the patent application of:

Inventor(s): Ron M. Redlich and Martin A. Nemzow
For: Data Security System and Method for Portable Device
Our Ref: 6851-2-cip-5

The filing fee for the enclosed patent application has been calculated as shown below:

			Small Entity		Other than Small Entity	
	No. Filed	No. Extra	Rate	Fee	Rate	Fee
Basic Fee				$375		$750
Total Claims	146- 20 =	126	x 9 =	$1134	x 18 =	$
Ind. Claims	08- 03 =	05	x 42 =	$ 210	x 84 =	$
____Multiple claims presented			x140 =	$	x 280 =	$
			Total	$1719	Total	$

Please charge Deposit Account No. 03-1231 in the amount of $,1759.00 to cover the filing fee (plus applicable Assignment recording fee). Please charge any additional filing fees required under 37 CFR 1.16 to Deposit Account No. 03-1231. A duplicate copy of this letter is enclosed.

Small Entity under 37 C.F.R. §1.27. YES __X____ NO _____

Respectfully submitted,

Fleit, Kain, Gibbons, Gutman & Bongini, P.L.

By _____
Robert C. Kain, Jr.
Reg. No. 30,648

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-2-cip-5 fee calculation for pto.wpd

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

03/25/2003 MAHMED1 00000035 031231 10390807

01 FC:2001 375.00 CH
02 FC:2202 1134.00 CH
03 FC:2201 210.00 CH

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

1, 47, 48, 54, 85, 104, 107, 140

PATENT APPLICATION FEE DETERMINATION RECORD
Effective January 1, 2003

Application or Docket Number

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	146	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	146 minus 20=	* 126
INDEPENDENT CLAIMS	8 minus 3 =	* 5
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	$375	OR	BASIC FEE	$750
X$ 9=	1134	OR	X$18=	
X42=	210	OR	X84=	
+140=	—	OR	+280=	
TOTAL	719	OR	TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Best Available Copy

#2

j1032 U.S. PTO
10/390807
03/19/03

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron Redlich, et al.

Serial No.

Filed: Herewith

For: DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97.

Patent No.	Inventor	Issue Date
6,192,472 B1	Garay et al.	Feb. 20, 2001
6,148,342	Ho	Nov. 14, 2000
6,094,483	Fidrich et al.	Jul. 25, 2000
6,055,544	DeRose et al.	Apr. 25, 2000
5,996,011	Humes	Nov. 30, 1999
5,905,980	Masuichi et al.	May 18, 1999
5,832,212	Cragun et al.	Nov. 3, 1998
5,485,474	Rabin	Jan. 16, 1996

5,892,908	Hughes et al.	Apr. 6, 1999
5,423,032	Byrd et al.	Jun. 6, 1995
6,044,375	Shmueli et al.	Mar. 28, 2000
5,715,399	Bezos	Feb. 3, 1998
5,982,897	Clark	November 9, 1999
6,370,629B1	Hastings et al.	April 9, 2002
6,154,172	Piccionelli et al.	November 28, 2000
5,887,269	Brunts et al.	March 23, 1999
5,842,023	Tsumura	November 24, 1998
5,778,304	Grube et al.	July 7, 1998
5,757,916	MacDoran et al.	
5,933,498	Schneck et al.	August 3, 1999
6,078,907	Lamm	June 20, 2000
5,581,682	Anderson et al.	December 3, 1996
US 2002/0073313 A1	Brown et al.	June 13, 2002
WO 00/75779 A2	PCT	

-Ingran i100, Content Security Appliance (2 pages)

-Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)

-Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)

-ZD Net Interactive week - IBS, SAP: XML to Boost Security, integration.

-Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999.

-Cisco Systems' Intrusion Detection System (IDS) Host Sensor 2.0 product data sheet and technical overview, 10 pgs., July 3, 2000, www.cisco.com.

-"Protecting Privacy using the Decentralized Label Model" A. Myers, Cornell Univ. 1/1/2000.

-Mimesweeper Product Data sheet, Resoft Int'l LLC., Nov. 12, 2001 re-soft.com/product/mimeswep.

-Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July 2000.

-Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys., Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.

-Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001.

-Intelligence Community System for Information Sharing (ICSIS) Relationship to the Global Information Grid (GIG), White Paper, 27 March 2001

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. A copy of each listed patent or publication or other item of information in written form, or of at least the portions thereof listed above, is filed with this Information Disclosure Statement. If two or more patents or publications are considered substantially cumulative, a copy of a representative one is included with

this statement and others are merely listed above. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

FLEIT, KAIN, GIBBONS, GUTMAN & BONGINI, P.L.

By _____

Robert C. Kain, Jr.
Reg. No. 30,648
Suite 100
750 S.E. Third Avenue
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-2cip-5 IDS.wpd

j1032 U.S. PTO
10/390807
03/19/03

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,192,472 B1	2/20/2001	Garay et al.	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al.	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al.	707	1	
	5,832,212	11/3/1998	Cragun et al.	395	188.01	
	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
	WO 00/75779 A2		WIPO			

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ingram i100, Content Security Appliance (2 pages)	
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)	
	ZD Net Interactive iWeek - IBS, SAP: XML to Boost Security Integration (1 page)	
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	
	Cisco Systems' Intrusion Detection System (IDS) Host Sensor 2.0 product data sheet and technical overview, 10 pgs., July 3, 2000, www.cisco.com	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,892,908	4/6/1999	Hughes et al.	395	200.8	
	5,423,032	6/6/1995	Byrd et al.	395	600	
	6,044,375	3/28/2000	Shmueli et al.	707	101	
	5,715,399	2/3/1998	Bezos	395	227	
	5,982,897	11/9/99	Clark	380	21	
	6,370,629B1	4/9/02	Hastings et al.	711	163	
	6,154,172	11/28/00	Piccionelli et al.	342	357.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	"Protecting Privacy using the Decentralized Label Model" A. Myers, Cornell Univ. 1/1/2000	
	Mimesweeper Product Data sheet, Resoft Int'l LLC., Nov. 12, 2001 re-soft.com/product/mimeswep.	
	Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July 2000.	
	Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys., Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.	
	Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001.	
	Intelligence Community System for Information Sharing (ICSIS) Relationship to the Global Information Grid (GIG), White Paper, 27 March 2001	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,887,269	3/23/99	Brunts et al.	701	208	
	5,842,023	11/24/98	Tsumura	395	712	
	5,778,304	7/7/98	Grube et al.	455	33.1	
	5,757,916	5/26/98	MacDoran et al.	380	25	
	5,933,498	8/3/99	Schneck et al	380	4	
	6,078,907	6/20/00	Lamm	705	40	
	5,581,682	12/3/96	Anderson et al.	395	792	
	0073313 A1	6/13/02	Brown et al.	713	165	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER DATE CONSIDERED

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75779 A2

(51) International Patent Classification[7]: G06F 9/46

(21) International Application Number: PCT/US00/15224

(22) International Filing Date: 2 June 2000 (02.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/137,568 4 June 1999 (04.06.1999) US

(71) Applicant *(for all designated States except US)*: IWITNESS, INC. [US/US]; Suite 2N, 2995 Wilderness Place, Boulder, CO 80301 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: LAMBERT, Francis, T. [US/US]; 1901 Spruce Street, Boulder, CO 80302 (US). ARCHER, Emory, Scott [US/US]; 4799 White Rock Circle, #E, Boulder, CO 80301 (US).

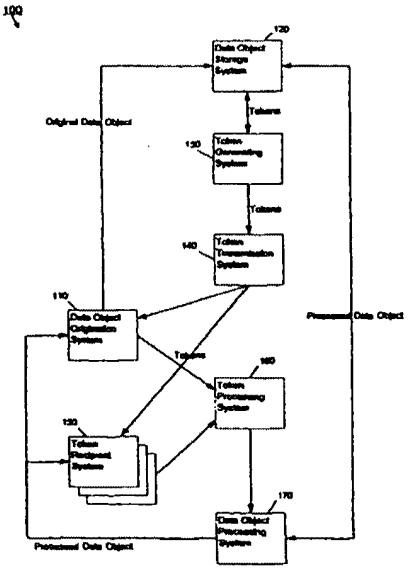
(74) Agents: SABETT, Randy, V. et al.; Cooley Godward LLP, One Freedom Square-Reston Town Center, 11951 Freedom Drive, Reston, VA 20190-5601 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: TOKEN BASED DATA PROCESSING SYSTEMS AND METHODS



(57) Abstract: A token based data processing system is disclosed that uses data object tokens (DOTs) to manage the associated data objects within the data processing system. The numerous advantages of a token based data processing system stem from the ability to utilize a DOT separate from its associated data object. A data processing system according to the present invention can include a data object origination system, a data object storage system, a token generating system, a token transmission system, one or more token recipient systems, a token processing system, and a data object processing system. The token generating system can generate a DOT that contains metadata corresponding to the information that the token generating system receives regarding the data object, including its attributes, the parameters stored with it, and other information regarding its originating system and its recipient system. After being distributed by a token transmission system, token recipient systems can analyze and process the DOTs in lieu of the associated data objects.

WO 00/75779 A2

IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TOKEN BASED DATA PROCESSING SYSTEMS AND METHODS

RELATED APPLICATION

The present application claims priority to Provisional Application No. 60/137,568, filed June 4, 1999, which is incorporated herein by reference in its entirety.

BACKGROUND

Field of the Invention

This invention relates to a data processing system containing diverse data objects and to methods for using those data objects. More specifically, the invention relates to a data processing system where the system utilizes data objects called "tokens" to perform processes related to, and upon, other data objects to which the tokens refer.

Description of the Related Art

The advent of electronic data interchange, the growth of electronic communications, the growth of the number of electronic communication users, the growth of the availability of information, and the growth in the size, number and types of data objects has greatly increased the requirements of both data storage and data communication bandwidth. Typical use of these data objects requires processing and transfer of the data object itself, often due to the complexity or sensitivity of the data content of the object, or to the limitations of the data systems used to manipulate the data object. These systems generally require transfer or transmission of the entire data object for a user to be able to edit, preserve, alter, or "own" the data on the person's

local computing system. Examples of these systems can include any that use e-mail attachments, ftp file transfer, and http file transfer.

Unfortunately, a modern data object storage event or a transmission event, such as an electronic document transfer via e-mail, may contain a large volume of data that one entity wishes to transfer to another entity. This type of transfer forces both the sending and receiving parties to expend substantial resources in terms of CPU usage, data storage, and transmission bandwidth at both ends of the transmission. The cost and lost productivity from these types of transmissions will increase as the number and size of these transmissions increase, as is the case in modern data communications.

Additionally, the originator of the transmitted data may wish to keep the transfer of the data secure and private. This requires sending the data using encryption, which requires additional CPU usage. The originator may also wish to guarantee that the transmitted data arrived exactly as sent, which requires that all of the data be sent, verified, and the verification returned to the originating system each time the data is transmitted. These security and authentication technologies must also be present on the receiving system. Prior to the data being released to the transmission network, the originator must have knowledge that the receiving system is capable of reliably authenticating, decrypting, and controlling access to the recipient's copy of the data object.

In many cases, the receiver of the data in this type of transmission is forced to receive all of the transmitted data whenever the originator sends it, regardless of whether or not it is convenient for the receiver at that time. An example of this is a mobile computer user being forced to download a large e-mail attachment over an expensive hotel data line so that they can retrieve all of their e-mail. Another example

is a wireless data transceiver being forced to download unnecessary data when only limited bandwidth is available.

In the case where a data object is transmitted to multiple recipients, the originator is required to transmit the data object multiple times, thereby expending valuable CPU and bandwidth resources in a the concentrated time period of transmission Also, each recipient is required to receive and store its copy of the transmitted object, thereby using bandwidth and data storage resources at each recipient. If the recipients are receiving diverse variations on a data object, the originator is required to create, store, and transmit the separate variations of the data object.

It is also possible that the volume of data in the transmitted data object is too large for the receiving system to efficiently store, or that numerous accumulated objects are too large for the system to efficiently store, and that it would be desirable to have another system with greater storage capacity hold the object and provide authorized access to the object only as needed.

It is also possible that the originator of the data would want to control the access and use of the object by the receiver, or create an audit trail of the receiver's use of the data object. The originator may wish that various receiving parties have access only to portions of the data object specific to the nature of the receiver. The originator or the receiver may desire to provide authentication relating to a data object without transmitting or storing the object itself.

Mechanisms have existed in the past for providing information about stored data objects. For example, a computer file (one type of data object) under the Disk Operating System (DOS) or the Windows operating system has certain flags associated

with it to indicate information about that file. The flags indicate, for example, whether the file is "read only", whether it has been archived, and whether it can be written. The UNIX operating system utilizes a similar approach of storing flags with files. However, the flags in all of these systems are rudimentary, and they are not easily extensible. The flags also tend to be stored as part of the object to which they refer and are therefore cumbersome to process without access to the file itself.

Other types of data objects contain elements that refer to other data objects within the context of the containing object. An example of this could be a filename combined with disk sector locations in a storage directory object, such as a file allocation table. Another example could be a hyperlink with addressing information contained within an HTML object. These object elements act as "pointers" to an object, but do not function outside of the context of the containing object. They also require a process to access the referenced object to perform processes or analysis on the referenced object. They do not act as a "surrogate" for the object, allowing processes to perform functions on an object without accessing the object itself.

Unfortunately, current data network transmission and storage systems fail to provide a robust, extensible, and universally compatible means for those users or systems transmitting and receiving data to efficiently use data objects in such as way as to conserve CPU usage, bandwidth usage, and storage through the use of smaller, more efficient objects containing metadata about the data object that can be processed separately from the data object itself. This smaller, more efficient object can contain metadata for use in access control, use auditing, redactability (or the filtering of content in an object), recipient and sender authentication, workflow logic, data integrity, and

timing of data delivery, among others. Consequently, a need exists for a data processing and transfer system that overcomes the foregoing drawbacks.

SUMMARY OF THE INVENTION

The present invention provides a data processing system that can allow a user to manipulate a data object through the use of one or more separate data objects comprised of metadata about the original data object. The metadata can represent many attributes of a data object, including, but not limited to, information about the content of the data object and the context of its occurrence. It can also represent information about searchable elements in the data object or information on the use history of the object. Some specific examples of metadata can include object identification, access parameters, authentication requirements and values (for both originator and user), encryption methods and keys, access history, integrity checking values, redaction values (or restricting access to certain elements or properties of the original data object), and token validity expiration period. In an embodiment, the DOT can also contain references (such as hyperlinks) to other locations where other metadata values can be found. Systems holding metadata values can also control access to and log use of those metadata values in other locations according to the contents of the token. A data processing system according to the present invention can combine diverse metadata into a discrete and processable data object called a Data Object Token (DOT) that refers to one or more data objects. The DOT includes metadata that provides information about a data object.

In one embodiment, a data object originator can submit a data object to a token based data processing system, which can optionally store the data object and generate

one or more tokens containing metadata of varying complexity referring to the stored data object. The one or more tokens can then be returned to the originator, or sent directly to token recipients, or stored separately in the data object storage system for later use. This Data Object Token, the DOT, can be used by the originator or by token recipients to interact with the data object that is optionally stored on a system storage device such as a central data depository attached to a network, or in another location specified in the DOT according to the protocol used to locate a data object, including a URL, a storage device identifier, or other data object locating protocols. The DOT user can submit the DOT to the token based data processing system to retrieve, view, alter, delete, or otherwise interact with the data object. The token based data processing system can analyze the metadata values contained in the DOT to determine use of the data object, including allowing access, processing authentication values, performing redaction, transmiting the object or portions thereof, destroying the data object, or otherwise manipulating the data object. It can also store and transmit metadata about data object as a smaller, discrete object that can be managed using native and pre-existent file and transmission processes.

One advantage of a token based data processing system is that it allows users of data objects to have access to and control over data objects without being required to expend local storage or bandwidth resources in the process. A DOT can be of very small size and still refer to a much larger data object in a remote location, while providing many capabilities to the local processes that would otherwise require the presence of the data object on the local system. A DOT can be very efficiently transmitted to multiple users, requiring much less storage and bandwidth than multiple transmissions of the referenced data object.

Another advantage is that the user of the DOT can retrieve, download, view, or otherwise process the referenced data object at their convenience by submitting the DOT to the token based data processing system. Another advantage is that the user can receive a DOT that allows them to decide upon the usefulness of, and securely retrieve, the referenced data object without requiring them to download the data object at time of originator transmission to them.

Furthermore, a token based data processing system can contain the authentication values and methods for both the originator and the DOT user that validate access and other rights to the data object. The token based data processing system can validate the DOT as it contains the originator authentication, as well as validate other parameters of the DOT based on the user authentication, before access, processing, or retrieval of the original data object is allowed.

The DOT can also contain data redaction information tailored to the nature of the DOT user. The DOT can provide the system information as to which portions of the data object the user will be allowed access. This relieves the data object storage system from the requirement of having to store and process redaction information for every potential user of the data object.

A further advantage is that the DOT can contain data object routing information for workflow and rules processing of data objects. The process can be more efficient and less bandwidth intensive if a token representing the workflow data object is passed around instead of the object itself.

Another advantage is that the DOT can append data object usage information to itself whenever it is used, and thereby become a self-contained data object usage audit

trail. This usage information could contain user identity and authentication, and time and type of use of use of both the token and the referenced object.

Yet another advantage is that the data object originator can stipulate in the DOT an expiration or starting time for processing of the referenced data object. This allows an originator to control the timing of various aspects of processing the stored data object, as well as avoid the need to provide a local copy of the data object to the DOT user.

Another advantage to using a DOT as a surrogate for a data object is that it avoids exposure of the data object to potential security and privacy problems inherent in the transmission of data over public networks such as the Internet. For example, even if a DOT is sent to the wrong recipient, or "sniffed" from the public network, the referenced object cannot be processed or retrieved since the unauthorized token possessor will not have the correct authentication to access the object.

Another advantage to using the DOT as a surrogate to the referenced data object is that the DOT can contain searchable elements of the original data object, such as keywords or text, and allow searching of the original data object, or a set of data objects, without requiring access to them. This allows searching to be distributed to the token user machine, thus conserving bandwidth and CPU usage at the object storage system.

Another advantage of using a DOT to retrieve an object is that an integrity value, such as a hash digest, of the retrieved data object can be compared to an integrity value in the token user's DOT to determine if the data object was received correctly.

Another advantage of using a DOT approach is that a token generating system can be embedded in an e-mail server, allowing the e-mail system to embed a DOT in

the place of large e-mail attachments. This conserves bandwidth and storage for both the sender and receiver.

Another advantage of DOTs is that they can be used as an electronic payment system due to their high level of security and ability to provide an audit trail. For example, the DOT can represent a portion of a pre-paid monetary amount represented by the referenced data object, such as a bank account. The payment DOT can be submitted to a token processing system that reduces the bank account balance by the amount embedded in the DOT, and then expires the DOT by placing its unique identifier on an expired DOT list. This would allow cashless payment in electronic business transactions, without exposing any sensitive financial information to a public network.

Another advantage of using DOTs is that they decouple the object storage technology from the object access technology, allowing object storage technologies to change without changing the way the stored objects are accessed by the users, and allowing the access objects, or DOTs, to remain valid and functional over long periods of time, even if the storage systems that they access change.

Another advantage of using DOTs is they it allow users to maintain representations of libraries of objects on a local system for off-line browsing, management, and processing.

Additional aspects and embodiments of the present invention will become apparent upon a review of the following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a functional block diagram of an embodiment of the present invention.

Fig. 2 depicts the process flow of a system according to the present invention.

Fig. 3 depicts the basic structure of a data object token.

Fig. 4 is a notational representation of the structure of one embodiment of a data object token.

Fig. 5 is a notational representation of additional elements in the structure of one embodiment of a data object token.

Fig. 6 is a command table for use in an embodiment of the present invention.

Fig. 7 is a flow chart of an embodiment of a token generating system.

Fig. 8 is a flow chart of an embodiment of a token processing system.

Fig. 9 is a flow chart of an embodiment of a token recipient system.

DETAILED DESCRIPTION

Fig. 1 depicts a block diagram of an embodiment of a token based data processing system 100 according to the present invention. Token based data processing system 100 can contain data object origination system 110, data object storage system 120, token generating system 130, token transmission system 140, token recipient system 150, token processing system 160, and data object processing system 170.

Data object origination system 110 can be any device or system that can be utilized to process information and produce data objects, including but not limited to such things as a personal computer, a mainframe computer, or an embedded computing system connected to a network. Data object origination system 110 can further include numerous processes that utilize data objects. For example, data object origination

system 110 could be utilized to create a data object and store that data object in data object storage system 120. Similarly, data object origination system 110 could also be utilized to download and store information, in the form of one or more data objects, from a data network. In particular, data object origination system 110 can utilize and store various data objects including, but not limited to, database files, electronic documents, e-commerce transactions (such as stock trades or merchandise purchases), electronic records (such as medical records or personal histories), multi-part records from document imaging systems, Web sites, sequences of HTTP data, or digitized video and audio data.

Following the creation or reception of one or more data objects in data object origination system 110, the data objects can be stored in data object storage system 120, which can be a local data storage system or a remote data storage system. For example, in the case of a personal computer, a local data object storage system 120 can include a hard drive, or a combination of a floppy disk drive and a floppy disk. Alternatively, a remote version of data object storage system 120 can include storage on a Local Area Network (LAN) or on a Wide Area Network (WAN) using such mechanisms as file servers or digital tape libraries.

In addition to receiving and storing the data objects, data object storage system 120 can expose the data objects to token generating system 130. Token generating system 130 can analyze and process the information about the data object, such as its attributes, the parameters stored with it, and other information regarding its originating system and its recipient system. Token generating system 130 can then generate metadata corresponding to that information, and create a data object called the Data Object Token (DOT) that contains the metadata associated with the data object. Token

generating system 130 can further process the DOT to embed data values that provide or ensure such things as security, privacy, reliability, or efficiency. Numerous means exist for providing these attributes, including encryption, digital signatures, hash digests, other authenticating technologies, compression, or other processing technologies. As one particular example, token generating system 130 can provide authentication, integrity, and non-repudiation information about the data objects using a public key digital signature. Upon successfully verifying the digital signature, the recipient of the digital signature can have the additional assurance of the authenticity of the originator, of the integrity of the data object, and that the data object creation cannot be repudiated.

Once processed, token generating system 130 can further present the DOT to data object storage system 120 and to token transmission system 140 for transmission to one or more token recipient systems 150. Data object storage system 120 or token transmission system 140 can store the DOT or a portion of the DOT for later use, thereby avoiding later reprocessing of the data object.

Token generating system 130 can read the object to be tokenized from data object storage system 120. Token generating system 130 can then determine from a token reference file the types and fields of metadata desired to be embedded in the token. A token reference file can be viewed as a template that contains rules governing the creation or transformation of tokens, including but not limited to encoding of the DOT (e.g. using XML, ASN.1, or comma-separated); required data and metadata fields; organizing structure of metadata fields; and mappings of data types and structures from the source data object to a token. Token generating system 130 can then read the metadata from the object and write it into a file that will become the DOT.

This metadata can include a unique identifier for the object, object location information, object hash digest values, or other metadata fields as required. Token generating system 130 can then determine from the token reference file if it is required to generate metadata from processing the referenced data object's content or metadata fields. Token generating system 130 can then read the content or metadata from the object, process it as required (such as, for example extracting keywords from content text, or reducing images for more efficient searching), and then embed the processed metadata into the token extension fields (see Fig. 3) in the DOT file. The metadata can be written in popular data formats, such as XML or comma delimited fields.

Token generating system 130 can then determine from the token reference file whether token generating system 130 is required to retrieve metadata external to the object, such as the date, a stock price, a digital certificate, encryption keys, other authentication data, or other data as is available to token generating system 130 and required by the token reference file. Token generating system 130 can then embed the externally retrieved data into the appropriate fields in the DOT file. It can also use predetermined time stamp and authentication fields, as well as token extension fields as required. Token generating system 130 can also embed additional metadata into the token file extension fields, such as token validity period, redaction values, or workflow logic to be used when referencing the original data object. Token generating system 130 then can embed its version number in the token file to allow later processing by token processing system 160 and, particularly, to differentiate among different versions of tokens.

Token generating system 130 can then digitally sign the DOT file by methods well known in the art of digital signing, including without limitation, encrypting, with a

private key from a public key infrastructure (PKI) key pair, a combination of a hash digest of the token with a digital certificate, and embedding the digital signature data into the token file. Token generating system 130 can then encrypt the entire token file using well known encryption algorithms, such as triple DES or the RC5 encryption methods.

The DOT file generated by token generating system 130 can then be stored in the data object storage system 120, in the data object generation system 110, or in token generating system 130 itself to await further processing.

Once token generating system 130 creates a DOT, token transmission system 140 can read the DOT from token generating system 130 and determine from a token transmission reference file whether or not the DOT is required to be transmitted to a token recipient system 150, or stored for later use. A token transmission reference file, similar to a token reference file, can contain template rules, such as recipient types, required transmission metadata, and required authentication, that would govern the transmission of DOTs. If the DOT is to be transmitted, the token transmission system 140 can embed information on accessors to the data object in the DOT as required. This information can be used by token processing system 160 to determine the authorization and access rights of the submitted DOT. The token transmission system 140 can embed multiple object accessors values to allow use of the DOT by multiple users or systems. The DOT can then be encrypted in the public key of the transmission destination system, and can then be securely and reliably transmitted to one or more token recipient systems 150 using either a standard communications protocol, such as FTP, e-mail attachment, or HTTP, or by using a proprietary communications protocol.

A token recipient system 150 system can include a system capable of receiving, storing, or processing a DOT. The token transmission system 140 can determine addressing and routing information for the destination token recipient systems 150 from a token transmission reference file, or from the token reference file contained in token generating system 130. In one embodiment, data object origination system 110 can also be a token recipient system. In an embodiment, token transmission system 140 can further verify and log reception of the DOT by one or more token recipient systems 150.

Token recipient system 150 can receive, store, and optionally process or otherwise condition a DOT. Processing on a DOT could include searching on metadata or content from the object embedded in the DOT. This searchable metadata or content could include, for example, text, keywords, or images from the original data object. Other types of processing that could be performed on a DOT by the token recipient system include embedding recipient reception information, such as time stamp and digital signature, appending additional accessors to the referenced object if the recipient system is so authorized, or forwarding the DOT to another token recipient system. The optional processing performed by token recipient system 150 can include other types of analysis and processing of the information contained in the DOT, including its metadata. Since token recipient system 150 can perform its analysis and processing on the metadata contained within the DOT (which is acting as a surrogate for the data object itself), no resources within data object storage system 120 would need to be used.

For example, in one embodiment, token recipient system 150 can contain an e-mail computer application that receives DOTs associated with e-mail messages. In this

case, each message could be a data object. The metadata contained within a particular DOT that is associated with a specific e-mail message can contain information about the e-mail message, including but not limited to such things as the date, time, subject, sender, and, in particular, any attachments associated with the e-mail message. The DOTs can be used by a token recipient system to search for a particular e-mail message or for a group of messages. However, this search could be done solely within the token recipient system using metadata embedded in the DOTs associated with the data objects (i.e. the e-mail messages), not on the messages themselves, which can be stored on a remote data object storage system 120. Also, using this approach, any attachments to the e-mail message would only need to be stored in the data object storage system, not sent to a token recipient system nor stored at the data object origination system.

Furthermore, in one particular embodiment related to e-mail, a token generating system can be embedded in an e-mail server to allow automated storage and tokenization of e-mail, including, without limitation, any of its components such as header, body, or attachments. Token generating system 130 embedded in the e-mail server can read the e-mail objects controlled by the server, generate a DOT for the e-mail object, replace the original e-mail object with the DOT, and store the e-mail object in a more efficient data object storage system location, such as a digital tape library. The e-mail user can then use the DOT from within the e-mail client application to access or process the e-mail data object. Searching for e-mail content within a group of e-mails can be accomplished by searching the search metadata embedded in the DOTs in the e-mail client application, thereby avoiding the CPU and bandwidth costs associated with searching the group of e-mails on the e-mail server or at the data object storage system. This process of substituting DOTs for data objects such as e-mails can

be applied to many types of data objects, including without limitation, scanned or imaged documents, electronic documents, database tables, electronic spreadsheets, web sites, and other types of data objects specified by the user of a token based data object management system.

Upon the completion of a search and a determination that one or more specific e-mail messages, or other type of data objects, need retrieval or processing, token recipient system 150 can submit one or more DOTs to token processing system 160 which can then cause data object storage system 120 to be accessed and the referenced data objects to be processed according to the instructions in the DOT, or transmitted to a data object processing system 170 as requested in the submitted DOT.

After token recipient system 150 submits a DOT to token processing system 160 to retrieve a data object from data object storage system 120, token processing system 160 can interpret the metadata contained in the DOT. Using the metadata, token processing system 160 can submit processing commands to data object processing system 170 according to the metadata contained in the DOT. These commands could include, for example, transmit, redact, alter, or destroy a data object as shown in Fig. 6.

Alternatively, a token recipient system can submit a DOT to a token processing system to retrieve a set of DOTs associated with the submitted DOT. This referenced set of DOTs can reference data objects or other DOTs, or a combination thereof, as required by the system.

Data object processing system 170 can interact with the data object stored in data object storage system 120 according to the commands submitted by token processing system 160. For example and without limitation, in response to a particular

command, data object processing system 170 can transmit, redact, alter, or destroy the data object stored on the data object storage system, according to the authorizations embedded in the submitted DOT, and as interpreted by the token processing system 160, which can pass the commands to the data object storage system 120.

In another embodiment where data object storage system 120 contains data object processing system 170, data object storage system 120 can process the referenced data object according to the instructions embedded in the DOT. For example, if data object storage system 120 is instructed to transmit the object, it can place the object into a data transmission process as is commonly known to the art, or it can encrypt the object using an encryption value submitted with the token, such as the destination system public key, or it can transmit the encrypted object to a system different from the system that submitted the token, or it can transmit the object to multiple systems. Similarly, data object storage system 120 can redact the stored object by recomposing the object prior to transmission, according to redaction rules embedded in the token. An example without limitation of this can be the removal of personal information from a data object for transmission of the data object from within the European Community to a destination outside of the European Community, thereby complying with the European Privacy Act, or other regulations that require redaction of information in transmission or storage.

Data object storage system 120 can additionally alter the data object by changing its retention information, its authorized accessor list, its storage format or location, or even its content if required by the system. Data object storage system 120 can even destroy the data object according to the processing instructions embedded in the submitted token.

Fig. 2 depicts a process flow diagram of an embodiment of the present invention. In data object origination system 210, a data object can be created. Once created, that data object can be transmitted to data object storage system 220. Once received, data object storage system 220 can process the data object so as to enhance the security and reliability of the data object storage process by, for example, performing encryption, compression, hashing, or mirroring, or by digitally signing the data object. For example, the well known DES encryption algorithm can be used to encrypt the data object. In addition, the well known RSA public key digital signature algorithm can be used to digitally sign the data object in data object storage system 220. Following the processing performed on the data object by data object storage system 220, the data object can be stored. The data object storage system can then place the processed object where it will be read by token generating system 230.

Token generating system 230 can generate tokens in standard data formats. For example, token generating system 230 can generate XML-based tokens based on the content of the data objects. To do so, token generating system 230 first reads the stored data object in data object storage system 220. It then analyzes the data object and the associated token reference files. The token reference files can contain instructions and information that can allow the token generating system to determine how the DOT will be constructed from the data object. Once analyzed, token generating system 230 can generate the necessary XML tags to be placed in the DOT for the particular system. In other embodiments, a token generating system can also, for example, generate fixed length fields, comma delimited fields, and other data formats that are commonly used by computer applications. In general, a token generating system can produce any type of DOT that may be needed for a particular data processing system.

In addition, token generating system 230 can encrypt, compress, hash and otherwise process one or more DOTs so as to enhance the security and reliability of the DOTs. Similar to the processing that can be done on the data object itself, the well known DES encryption algorithm can be used to encrypt the DOT. In addition, the well known RSA public key digital signature algorithm can be used to digitally sign the DOT in token generating system 230.

Furthermore, in an embodiment of the present invention, token generating system 230 can embed in the DOT time relevant attributes of the DOT, the data object, or the token recipient system's 250 ability to manipulate it. These time relevant attributes could include, for example, a time stamp of the DOT generation time, expiration of the DOT, the data object, or authentication metadata as determined by the contents of the token reference file. These time relevant attributes could also include "no access until" information that could not allow the token submitting entity to manipulate the data object until a certain time or event.

In an embodiment, once token generating system 230 has generated a DOT, token transmission system 240 can sense the DOT and can cause token generating system 230 to pass the DOT to token transmission system 240. To do so, token transmission system 240 can poll the system holding the DOT and retrieve the DOT in a data "pull" operation once it is available. Token transmission system 240 can then determine the destination for the DOT, followed by determining the methods to be used for the delivery of the DOT, according to mechanisms such as the transmission reference file in the token transmission system, or from the token reference file in the token generating system, or from a workflow logic file. Token transmission system 240 can then transmit DOTs using any well known data transmission technologies,

including, without limitation, the FTP protocol, the HTTP protocol, the SSL protocol, a virtual private network (VPN), or Secure Shell tunneling in the Unix operating system. In another embodiment, a token transmission system can send the DOT as an attachment to an e-mail message. Alternatively, a token transmission system can send a notification to a token recipient system of a token pending transmission to which token recipient system 250 must respond to release or access the token, and a token transmission system 240 can then issue a receipt describing the token delivery event.

After receipt of a DOT from a token transmission system, another token recipient system, or any other means of transmitting a token, such as in an e-mail as an attachment, token recipient system 250 can authenticate the DOT using any authentication techniques that may have been applied by token generating system 230. Once authenticated, token recipient system 250 can store the DOT and subsequently submit the DOT to token processing system 260 for data object manipulation.

In addition to submitting the DOT for data object manipulation, a token recipient system can also add new metadata to the received DOT, or alter the DOT according to the token recipient system's authority to do so as determined by the authorization metadata embedded in the DOT, and optionally transmit that updated DOT to another token recipient system or to the token processing system 260. This can allow metadata within a DOT to accumulate without having to access the associated data object from storage. A data processing system utilizing this type of DOT approach could undergo a change of the native platform and data formats of data object storage system 220 without impacting the capabilities of pre-existing DOTs used to manage and process the data objects within the system, provided the new native platform and data formats remained compatible with the required versions of the DOT structure.

In one embodiment, workflow logic can be embedded within the token or can be captured in an external file. Workflow logic refers to workflow processing rules stored and interpreted both inside and outside of a DOT, and that can affect both the internal operations of the token based data processing system and the overall workflow distribution patterns of tokens and data objects within an organization.

For example, workflow logic could be used by an organization to manage the workflow associated with a particular project. Workflow routing instructions could be embedded in the DOT if it is advantageous for the logic to be contained in the DOT, or the DOT could reference an external workflow logic file that could be dynamically updated. The DOT can reference an object or a set of objects intended to be the subject of a workflow process. This can allow the workflow system to distribute metadata about workflow-related data objects without expending the CPU and bandwidth to distribute the actual data object(s) themselves. The token recipient system 250 itself can execute the workflow logic embedded in the DOT, such as forwarding a DOT automatically to another token recipient system if the referenced data object is not accessed within a certain period of time, or other similar workflow logic.

Upon receiving the DOT from token recipient system 250, token processing system 260 can perform on the DOT any type of processing that might be necessary. For example, the DOT can be decrypted, uncompressed, or otherwise processed to restore it to its original form in response to security and reliability processing performed by the token generating system. The type of processing required can be determined by token processing system 260 by reading the metadata embedded in the DOT, such as the version number, or other metadata indicating how the DOT has been previously processed.

As another example, token processing system 260 can authenticate the entity submitting the DOT using digital certificates, recipient supplied passwords, biometric measurements, or any combination thereof, according to values contained in the token. Alternatively, the entity originating the DOT can be authenticated using digital certificates, recipient supplied passwords, biometric measurements, or any combination thereof, according to values contained in the token.

In yet another embodiment, token processing system 260 can create and append metadata to the DOT that can describe the use of the DOT and the data object. This metadata can be used create a self-contained audit trail within the token. For example, this self-contained audit trail can be comprised of use metadata and authentication values embedded into the token during a workflow execution by the associated token recipient systems.

Token processing system 260 can, in another embodiment, process metadata that describes the token submitting entity's access rights to the referenced data object. Those access rights can be used by data object processing system 270 to control access to all or portions of the data object. Metadata can also be used to describe the time attributes of a DOT, the referenced data object or the authenticating metadata. Token processing system 260 can interpret this time-based metadata to determine proper usage of the token and the associated data object.

The results of the token processing done by token processing system 260 can be passed as commands to data object processing system 270. Upon receiving one or more of these commands, data object processing system 270 can authenticate the command using any well known authentication technique already described herein. Upon successful authentication, data object processing system 270 can determine what

action needs to be taken to respond to the command. For example, destroying or deleting the referenced object from the object store, or appending the audit trail information embedded in the submitted DOT are actions that can be taken in response to a command.

One frequent action by data object processing system 270 can be the accessing of one or more data objects in data object storage system 220. If data object processing system 270 determines that the proper conditions have been met, including, for example, appropriate authentication information, one or more data objects can then be accessed in data object storage system 220. Once accessed, the requested actions can be performed on the accessed data objects by data object processing system 270 and those actions can also be logged by data object processing system 270. Finally, any results of the processing performed by data object processing system 270 can be passed back to token processing system 260. In another embodiment, data object processing system 270 can transmit one or more data objects to the token submitting entity. Prior to doing so, data object processing system 270 can optionally encrypt, compress, hash, sign, or otherwise process the data object to enhance security and reliability in transmission and delivery.

Figure 3 depicts a DOT 300 in accordance with the present invention. The basic DOT structure consists of a version field 304, token information 308, object accessors 328 , token and referenced object use information 352, and optional token extensions 368.

Version field 304 indicates the version of the data object token protocol to which DOT 300 conforms. The inclusion of version field 304 permits a token processing system to properly parse the DOT.

Token information 308 contains the fields necessary for a token processing system to assess the validity of the DOT and the data object to which the DOT is associated. Data object identifier 312 can contain a unique value or character string that identifies the data object to which it refers. Validity information 316 allows a system to make the determination of whether the DOT is valid. For example, validity information 316 can contain date and time information, such that a validity period can be established. Alternatively, validity information 316 can contain a hash digest of the object and the DOT that can be used for purposes of determining data integrity of a received object or DOT.

Data object and DOT authentication information 320 can contain any type of data that can be used to authenticate the data object or the DOT itself. In an embodiment, data object authentication information can contain a public key from a PKI key pair. In another embodiment, data object authentication information 320 can contain a digital signature. The authentication information can be used to authenticate the system creating the referenced data object, the system generating the DOT, or the system submitting the DOT to a token processing system or token recipient system. Timestamp 324 can provide information to an entity about the time of creation of the token. A data object originator could use the timestamp, for example, to prove that a data object representing a transaction was created at a specific time on a specific date.

The next main component of the DOT is object accessor 328. This can provide information about the entity or entities permitted to access and use the data object referenced by the DOT. In an embodiment, there may be multiple instantiations of object accessor 328 for each permitted accessor of the data object. Each object accessor 328 can contain information about the accessor 332, access rights 336,

authentication requirements 340, accessor authentication information 344, and timestamp 348. In an embodiment, the object accessor metadata can contain a list of workflow destinations upon which workflow distribution processing can be based.

Accessor 332 can contain information that identifies the entity being given rights to access the data object. This entity identifier could identify a system, a process, a class of processes, a specific user, a group of users, a reference to a dynamically alterable accessor list, or the general public. For example, accessor 332 can contain a name, an e-mail address, and a unique identifier. In another embodiment, accessor 332 can contain a digital certificate.

Access rights 336 can provide information to the token processing system regarding the rights that the accessor identified by accessor 332 has to the data object to which the DOT refers. Access rights 336 can include, for example, general rights, such as those used to access, download, modify, or destroy a data object. In addition, access rights 336 can include other, more specific rights that are unique to the particular data processing system. For example, a DOT used in a stock trading system might contain rights particular to a stock trader, such as buy unrestricted, buy limited, sell unrestricted, or sell limited. In another example, access rights can also stipulate authorization of the token recipient system to alter the metadata in the token, or the authorization to append audit trail metadata, as required by the system. Authentication requirements 340 provide information about the type of authentication required to be used by the token user to prove that it is the entity identified by accessor 332. Numerous, well understood, technologies exist to provide authentication in several different formats. For example, a particular data processing system may require something to be known by the token user, such as a password or personal identification

number (PIN). Alternatively, a data processing system may require the user to have an object, such as a smart card or a hardware "dongle". Finally, a data processing system might require physical information from the token user (i.e. a biometric), such as a fingerprint, a retinal scan, or a voice print.

Accessor authentication information 344 provides information about the entity that created the object accessor entry. This can be used to audit the granting of rights to access the referenced data object.

Timestamp 348 can provide information to an entity about the time of creation of the object accessor 328 metadata. A token processing system could use the timestamp, for example, to prove that the authentication information 344 was historically valid at the time of its creation. For example, if a digital certificate is used as authentication information 344, time stamp 348 can be used at a later time to determine if the digital certificate had expired or been revoked at the time of object accessor 328 metadata creation.

The next component of DOT 300 in an embodiment of the present invention, token use information 352, contains information about the use of the DOT and use of the data object to which the DOT refers. Token use information 352 can include information on the type of access requested 356 by the token user. Once authenticated using access authentication information 360, a token processing system can utilize token use information 352 to determine how it should process the object referenced by the DOT. This could include uploading the object to the token submitter, changing data in the object, or destroying the object.

One or more token extensions 368 allow the DOT to provide additional information beyond the standard DOT including, but not limited to, such things as

redaction instructions and audit trail data related to the associated data object. The format of each token extension 368 can consist of extension type 372, extension data 376, and extension authentication information 380. Within token extension 368, extensible metadata can be stored that can then be interpreted by the token recipient system or the token processing system. Some examples of the use of token extension 368 include DOT expiration values for a particular system, searchable content metadata values, workflow logic, additional (system specific) access rights, externally retrieved metadata, and any other fields that may be added by a token recipient system.

Fig. 4 and Fig. 5 provide a description of one embodiment of a DOT that can be associated with a Verified Data Object (VDO), as implemented by iWitness, Inc. of Boulder, Colorado in its electronic records management products. The descriptions in Fig. 4 and Fig. 5 use the well known Abstract Syntax Notation 1 (ASN.1) that is defined in "CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1)", published in 1988. The ASN.1 descriptions in Fig. 4 and Fig. 5 depict a Verified Data Object Token (VDOT).

Fig. 4 depicts the basic VDOT structure 410, which includes the two main components of tokenInfo and accessors. The tokenInfo component can provide information specific to the VDO, while the accessors component can provide information about the entities that may access the VDO. As shown in 420, the tokenInfo component can include globally unique object identifier vdo_id, the interval of time during which the token is valid, a digital signature and certificate identifying the creation event, and a timestamp. The vdo_id element can be used to uniquely identify the particular VDO to which the VDOT refers and can contain a randomly generated ASCII character string that had been verified as being unique. In a different

embodiment, the vdo_id could be a consecutive number applied to a particular VDO amongst a large set of other VDOs. The validFrom and validTo components together provide the validity period for the VDOT user to access the particular VDO. In an embodiment, if the UniversalTime value within the data processing system utilizing the VDO is less than the validFrom time or greater than the validTo time, the entity submitting the token in an attempt to access the associated VDO would be denied that access.

The signerInfo component provides the digital signature and information about the signer who applied the digital signature used to verify the VDO. In an embodiment, signerInfo can be the signer information defined in "PKCS #7: Cryptographic Message Syntax Standard: An RSA Laboratories Technical Note", Version 1.5, Revised November 1, 1993, which specifies, amongst other things, the signer's digital certificate, the algorithm used to sign the VDO, and the digital signature itself.

The accessors component within VDOT basic structure 410 specifies a collection of entities along with their access rights and authentication requirements for the specified VDO. As shown in accessor information 430, those entities can be identified in a table consisting of a set of DataObjectTokenAccessor elements, wherein each DataObjectTokenAccessor element can contain a PKCS #6 certificate, the access rights needed to access the VDO, the authentication requirements for the particular VDO, the PKCS #7 signer information, the PKCS #6 certificate of the signer of the VDOT, and a timestamp.

Access rights listing 440 for a particular VDOT can provide information on how a particular entity may use the VDOT in an embodiment of the invention. Only entities identified by the distinguished name and serial number from their enclosed PKCS #6

certificate can make use of the VDOT, including, for example, the ability to retrieve the corresponding VDO. Those entities are limited to their corresponding access rights, which are signed by the entity responsible for their assignment.

Authentication requirements 450 for a particular VDOT provides information on how a particular entity must authenticate itself prior to its use of the VDOT. Any use of the token, whether for VDO retrieval or communication to another entity, may require the using entity to satisfy one or more authentication requirements, such as knowledge of a password, a physical match of biometric data, or an external key. Additionally, each entry in the accessor table can be signed by its creator.

Fig. 5 depicts an ASN.1 description of the token use information 510 element and the token extension 520 element in accordance with an embodiment of the present invention. Token use information 510 can contain request information that indicates how a VDOT user would like to use the corresponding VDO and authentication information that allows the token processing system to determine the validity of the request. Token use information 510 can be included upon initial generation of the VDOT or can be appended at some later time after VDOT creation.

In an embodiment of the invention, one or more instantiations of the optional token extension 520 element can be included in a VDOT. In a VDOT, extType can specify the extension type of this particular extension.

Fig. 6 shows a command table implemented in one embodiment of the present invention that contains commands for performing various operations on a data object. A data object processing system can use the information shown in 610 to execute the commands on the specified data object. Transmit object command 620 can result in a data object being transmitted to the destination specified by the destination argument,

and can include information on authorization, transmission time, recipient requirements, and transport mechanism. Destroy object command 630 can result in the destruction of a data object, and can include information on authorization, destruction time, and disposition rules. Copy object command 640 can result in the copying of a data object from one location to the location specified by the destination argument. Alter object command 650 can result in one or more modifications to the data object, and can include information on the module to perform the operation, a reference to the data object, the actual alteration to be performed on the data object, and any necessary parameters. Redact object command 660 can result in certain information within a data object being removed while the rest of the data remains, and can include the module to perform the redaction, a reference to the data object, the redaction to be performed on the data object, and any necessary parameters. Finally, object encryption command 670 can result in the encryption or digital signing of a data object, and can include the operation to be performed on the data object, the method or algorithm to be used, the key to be used to perform the cryptographic operation, and whether to just perform a hash on the data object for data integrity purposes.

Figure 7 depicts a flow chart of the processing that can occur in a token generating system utilized for workflow processing. In step 704, the token generating system can receive a DOT generation request, which contains request attributes specifying the data object to be analyzed, the token reference file that defines the structure and required contents of the generated DOT, and possibly other control data. In order to ensure the security of the token generating system, and thus the security of the DOT and its future use in other systems, the DOT generation request is validated in step 712 through one or more of the various authentication means available including,

but not limited to, public key digital signatures. Once the DOT generation request is validated, the data object to which it refers is analyzed in step 716 to determine the viability of the request. In particular, as shown in the substeps in 720, the DOT generation request is checked against workflow logic (if any), the data object is then checked against workflow logic carried in the DOT generation request (if any), and finally, the data object is assessed to determine if it contains the necessary data/metadata to fulfill the request according to the token reference file. If the request cannot be fulfilled, a result indicating this can be returned in step 736.

If the authentication and subsequent analysis succeed, the token generation system can proceed to generate the requested DOT in step 724. As shown in substeps 728, all requested metadata that is derived directly from the data object can first be retrieved and attached. Then, all requested metadata that is derived external to the data object (if any) can be attached, possibly including workflow logic defined in the token request file. Finally, any requested DOT access rights can be constructed and attached. The newly formed DOT can then be digitally signed in step 732 by the token generation system, and possibly encrypted and enveloped following the Cryptographic Message Syntax as defined in PKCS #7. As shown in step 736, the DOT can then be returned synchronously to the originator of the DOT request and/or asynchronously transmitted through a token transmission system (as shown in the substeps in 740). Control could then be returned to the token transmission system in step 744.

Figure 8 depicts a flow chart of the processing that can occur in a token processing system utilized for workflow processing. In step 804, the token recipient system can send a processing request. In step 808, the token processing system can receive a processing request, which can contain, as shown in 812, a request DOT and

request attributes specifying one or more operations to be performed on the data object that the DOT references. Before processing, the token processing system can validate the public-key digital signatures on the DOT in step 816, to ensure the authenticity of the DOT and the authenticity of the requestor. Once validated, the token recipient system can open the cryptographic envelope of the DOT in step 816 (if it is encrypted) with the private-key that corresponds to the public-key used in securing the DOT for transmission. This ensures that the token can only be used by the intended token processing system.

Once validated and decrypted, the token processing system can check the token-embedded or external file workflow logic in step 820 and in the substeps shown in 824. The token processing system can then interpret the processing request according to the workflow logic of the token in step 828 in order to cause the data object processing system in 836 to perform the requested operations in step 832, such as fetch data/metadata, update metadata, destroy object, and transmit object/token, all of which can be performed on the data object within the data object processing system.

Results of the data object operation can be validated by the token processing system in step 840 to ensure their authenticity and conformance to the requirements of the request. The results can then be returned in step 844, and in particular, as shown in substeps 848, the results can be returned synchronously to the originator of the processing request and/or asynchronously transmitted as an updated token through a token transmission system. Once the results have been returned, control can return to the token transmission system in step 852.

Figure 9 depicts a flow chart of the processing that can occur in a token recipient system utilized for workflow processing. The token transmission system can

send a DOT in step 904 and token recipient system can receive a DOT from the token transmission system in step 908. Before processing, the token recipient system can validate the public-key digital signatures on the DOT in step 912, to ensure the authenticity of the DOT and the authenticity of the sender. Once validated, the token recipient system can open the cryptographic envelope of the token in step 912 (if it is encrypted) with the private-key that corresponds to the public-key used in securing the token for transmission. This ensures that the token can only be used by the intended token recipient system.

Once validated and decrypted, the token recipient system checks both the token-embedded and external file workflow logic for conflicts in steps 916 and the substeps in 920. If non-critical conflicts are found, resolution may require priority-based assessment or possibly user intervention. The token recipient system can then process the token according to the workflow logic in step 924. As shown in the substeps in 928, processing can include presentation to the user, storage for archival or for later use. At some point, the user of the token recipient system or the system itself can use the received (and possibly stored) token to request one or more operations on the data object to which it refers, as shown in step 932. This processing can be done through the token processing system as shown in step 936.

While the invention has been described in detail, including references to specific embodiments, it will be apparent to one skilled in the art that changes and modifications can be made to the invention without departing from the spirit and scope thereof. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method of managing one or more data objects within a data processing system using one or more data object tokens, the method comprising the steps of:

generating one or more data objects within a data object origination system;

storing said data objects in a data object storage system;

analyzing said data objects to determine information to be placed in one or more data object tokens;

generating said one or more data object tokens;

transmitting said one or more data object tokens to one or more token recipient systems;

processing said one or more data object tokens; and

processing said one or more data objects based upon said data object tokens.

2. A method as in claim 1, wherein said storing step further comprises storing said data objects in a local storage system.

3. A method as in claim 1, wherein said storing step further comprises storing said data objects in a remote storage system over a network.

4. A method for generating one or more data object tokens associated with a data object, the method comprising:

receiving a token generation request;

validating said token generation request;

analyzing said data object to determine information to be placed in said one or more data object tokens;

populating said data object token with metadata;

creating validation information related to said data object token; and

returning a completed data object token.

5. A method as in claim 4, wherein said validating step further comprises the step of verifying a digital signature using a public key.

6. A method as in claim 4, wherein said analyzing step further comprises the step of determining information to be redacted in said data object.

7. A method as in claim 4, wherein said analyzing step further comprises the step of determining information to be altered in said data object.

8. A method as in claim 4, wherein said populating step further comprises the step of appending one or more optional token extensions.

9. A method for processing one or more data object tokens associated with a data object, the method comprising:

receiving a token processing request;

validating said token processing request;

interpreting said token processing request to determine the operations to be performed on one or more data objects;

commanding said operations to be performed on said one or more data objects by a data object processing system;

validating the results of said operations; and

returning the resulting data object.

10. A method for limiting access by a user to data objects in a data processing system, the method comprising:

storing said data object securely within said data processing system;

creating a data object token corresponding to said data object, said data object containing authentication requirements;

distributing said data object token;

receiving an access request from a data object token user, said request containing data object token user authentication information and access authentication information;

authenticating said access request;

processing the data object to secure it for use by the data object token user; and

transmitting said processed data object to said data object token user.

11. A method as in claim 10, wherein said storing step further comprises performing local encryption on said data object.

12. A method as in claim 10, wherein said storing step further comprises locating said data object behind a firewall.

13. A method as in claim 10, wherein said first validation step further comprises verification of a first public key digital signature, and wherein said second validation step further comprises verification of a second public key digital signature.

14. A method for validating the use of a data object using a data object token in a token based data processing system, the method comprising:

performing a first validation on data object originator authentication information contained within said data object token; and

performing a second validation on data object token user authentication information contained within said data object token.

15. A method as in claim 14, wherein said first validation step further comprises verification of a first public key digital signature, and wherein said second validation step further comprises verification of a second public key digital signature.

16. A method of retrieving a data object in a token-based data processing system, the method comprising the steps of:

receiving a data object token from a token generating system;

storing said data object token;

appending data object token user authentication information;

submitting said data object token to a token processing system; and

receiving said data object.

17. A method as in claim 16, wherein said data object token user information comprises a public key digital signature.

18. A method for distributing analysis and processing activities related to one or more data objects stored in a data object storage system within a token based data processing system, comprising the steps of:

receiving one or more data object tokens in a token recipient system;

storing said data object tokens; and

processing said data object tokens within said token recipient system.

19. A method as in claim 18, wherein said processing step further comprises the steps of:

extracting metadata associated with said one or more data objects from said one or more data object tokens;

performing an analysis on said metadata; and

accessing one or more data objects within said data object storage system based upon said analysis.

20. A method as in claim 18, wherein:

said processing step further comprises a search through data object tokens containing electronic mail header information based on a set of search criteria; and

said accessing step further comprises accessing e-mail messages meeting said search criteria.

21. A token based data processing system that manages one or more data objects within a data processing system using one or more data object tokens, comprising:

a data object origination system for generating one or more data objects;

a data object storage system for storing said one or more data objects;

a token generating system for generating one or more data object tokens;

a token transmission system for transmitting said one or more data object tokens to one or more token recipient systems;

a token processing system for processing said one or more data object tokens; and

a data object processing system for processing said one or more data objects based upon the processing of said one or more data object tokens.

22. A token based data processing system as in claim 21, wherein said data object storage system is contained within said data object origination system.

23. A token based data processing system as in claim 21, wherein said data object storage system is located over a network remotely from said data object origination system.

24. A token based data processing system as in claim 21, wherein said data objects further comprise scanned or imaged documents.

25. A token generating system for generating one or more data object tokens that refer to one or more data objects, comprising:

a means for receiving a token generation request;

a means for validating said token generation request;

a means for analyzing said data object to determine information to be placed in said one or more data object tokens;

a means for populating said data object token with metadata;

a means for creating validation information related to said data object token; and

a means for returning a completed data object token.

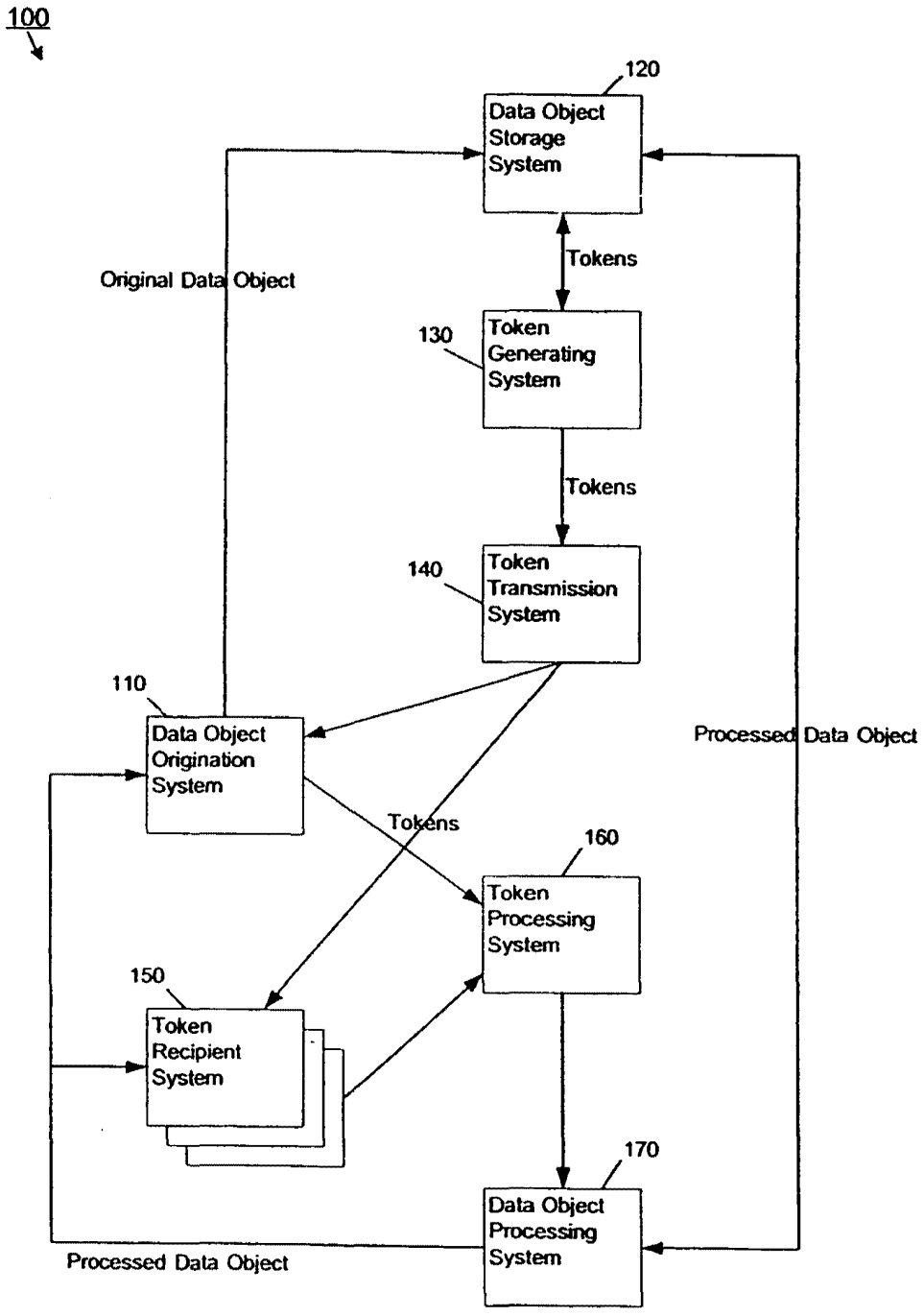

100
120
Data Object Storage System
Tokens
Original Data Object
130
Token Generating System
Tokens
140
Token Transmission System
110
Data Object Origination System
Processed Data Object
Tokens
160
Token Processing System
150
Token Recipient System
170
Data Object Processing System
Processed Data Object

Figure 1

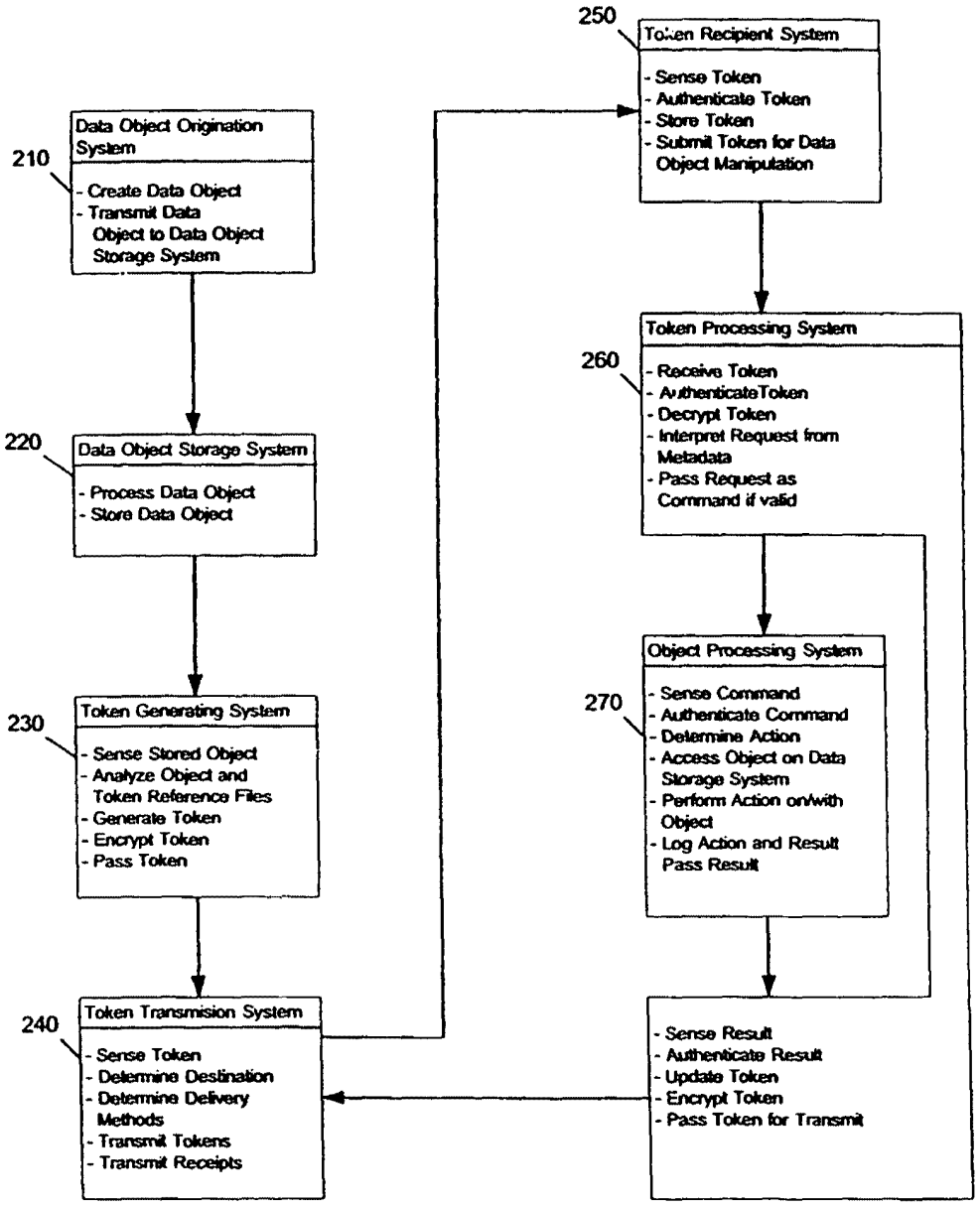

250
Token Recipient System
- Sense Token
- Authenticate Token
- Store Token
- Submit Token for Data Object Manipulation
Data Object Origination System
210
- Create Data Object
- Transmit Data Object to Data Object Storage System
Token Processing System
260
- Receive Token
- AuthenticateToken
- Decrypt Token
- Interpret Request from Metadata
- Pass Request as Command if valid
220
Data Object Storage System
- Process Data Object
- Store Data Object
Object Processing System
270
- Sense Command
- Authenticate Command
- Determine Action
- Access Object on Data Storage System
- Perform Action on/with Object
- Log Action and Result
Pass Result
230
Token Generating System
- Sense Stored Object
- Analyze Object and Token Reference Files
- Generate Token
- Encrypt Token
- Pass Token
240
Token Transmision System
- Sense Token
- Determine Destination
- Determine Delivery Methods
- Transmit Tokens
- Transmit Receipts
- Sense Result
- Authenticate Result
- Update Token
- Encrypt Token
- Pass Token for Transmit

Figure 2

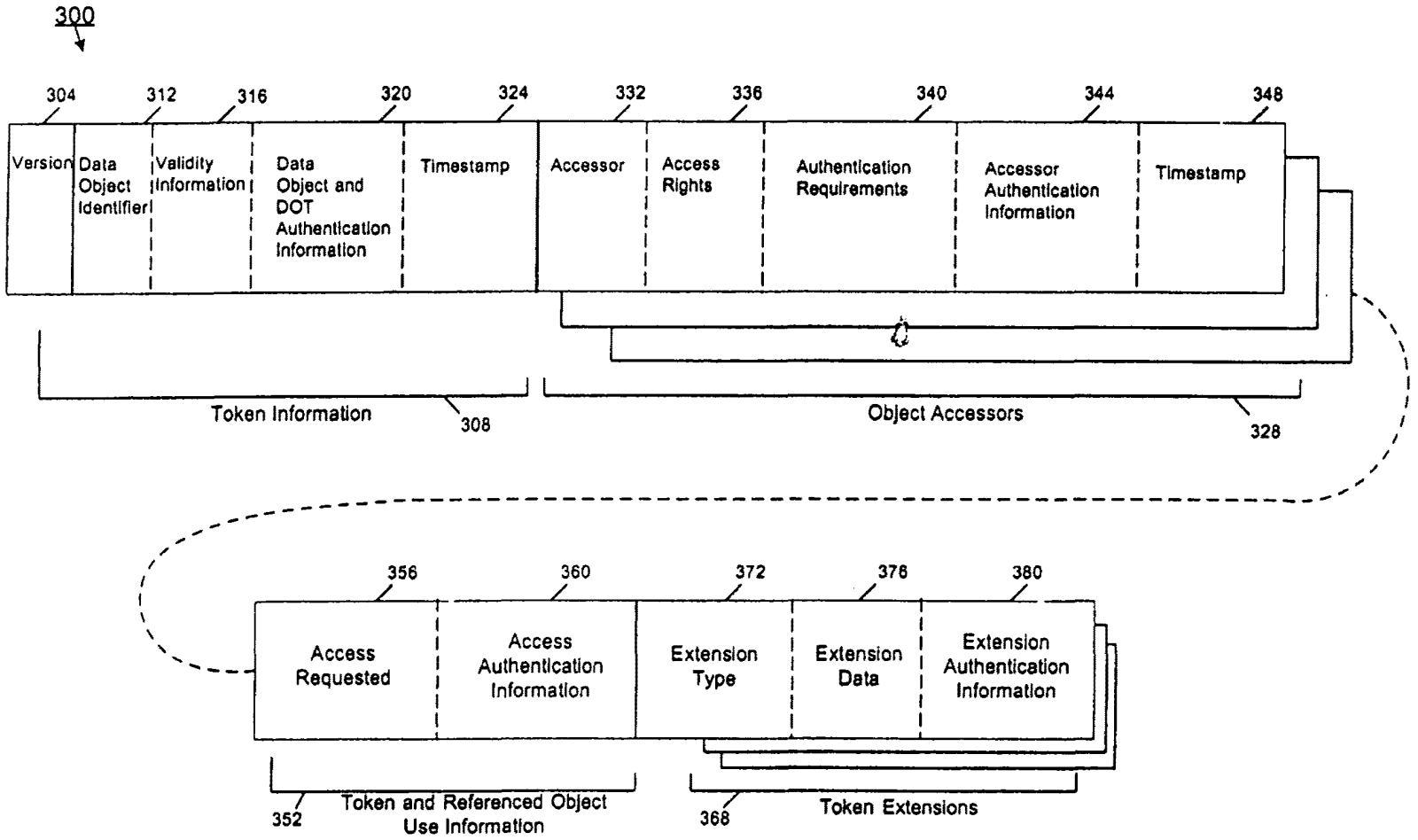

300
304
312
316
320
324
332
336
340
344
348
Version
Data Object Identifier
Validity Information
Data Object and DOT Authentication Information
Timestamp
Accessor
Access Rights
Authentication Requirements
Accessor Authentication Information
Timestamp
Token Information
308
Object Accessors
328
356
360
372
376
380
Access Requested
Access Authentication Information
Extension Type
Extension Data
Extension Authentication Information
352
Token and Referenced Object Use Information
368
Token Extensions

Figure 3

SUBSTITUTE SHEET (RULE 26)

410

```
DataObjectToken::= SEQUENCE {
        version         OCTET STRING,
        tokenInfo       DataObjectTokenInfo,
        accessors       DataObjectTokenAccessors,
        useInfo         DataObjectTokenUseInfo OPTIONAL,
        objectExt       DataObjectTokenExtensions OPTIONAL
        }
```

420

```
DataObjectTokenInfo ::= SEQUENCE {
        vdo_id          OCTET STRING,
        validFrom       UniversalTime,
        validTo         UniversalTime
        extAttributes   InfoExtAttributes,
        signerInfo      PKCS_7_SignerInfo,
                        // sig on previous
attributes
        signerCert      PKCS_6_Certificate,
        timeStamp       VerifiedTimeStamp,
        }

InfoExtAttributes ::= Attributes

Attributes ::= SET OF Attributes
Attribute ::= SEQUENCE {
        key     OCTET STRING,
        value OCTET STRING
        }
```

430

```
DataObjectTokenAccessors ::= SET OF
                        DataObjectTokenAccessor
DataObjectTokenAccessor ::= SEQUENCE {
        accessor                PKCS_6_Certificate,
        accessRights            AccessRights,
        authRequirements        AuthRequirements
        signerInfo              PKCS_7_SignerInfo,
        signerCert              PKCS_6_Certificate
        timestamp               VerifiedTimeStamp,
        }
```

440

```
AccessRights ::= SET OF AccessRight
AccessRight ::= SEQUENCE {
        type ENUMERATED {
                read_whole,
                read_partial,
                update_whole,
                update_partial,
                propagate_access_same,
                propagate_access_limited
                },
        extended UserObject     // extended info
                                   regarding
                                        partials/limited
        }
```

450

```
AuthRequirements ::= SET OF AuthRequirement
AuthRequirement ::= SEQUENCE {
        type ENUMEPATED {
                basic,          // certificate signature
                                   (always at least
                                   this)
                password,
                biometric,
                external_key,
                other
                },
        extended UserObject     // extended info
                                        regarding other
        }
```

Figure 4

510

```
DataObjectTokenUseInfo ::= SEQUENCE {
        accessRequested         Access,
        authentication          UserObject,
        accessorInfo                    PKCS_7_SignerInfo,
        accessorCert                    PKCS_6_Certificate
        }

Access ::= SEQUENCE {
        type ENUMERATED {
                read_whole,
                read_partial,
                update_whole,
                update_partial
                },
        extended UserObject
                }
```

520

```
DataObjectTokenExtensions ::= SET OF DataObjectTokenExtension
DataObjectTokenExtension ::= SEQUENCE {
        extType         OCTET STRING,
        extData         UserObject,
        signerInfos     PKCS_7_SignerInfos,
        signerCerts     PKCS_6_Certificates
        }

PKCS_7_SignerInfos ::= SET OF PKCS_7_SignerInfo
PKCS_6_Certificates ::= SET OF PKCS_6_Certificate
```

Figure 5

SUBSTITUTE SHEET (RULE 26)

SUBSTITUTE SHEET (RULE 26)

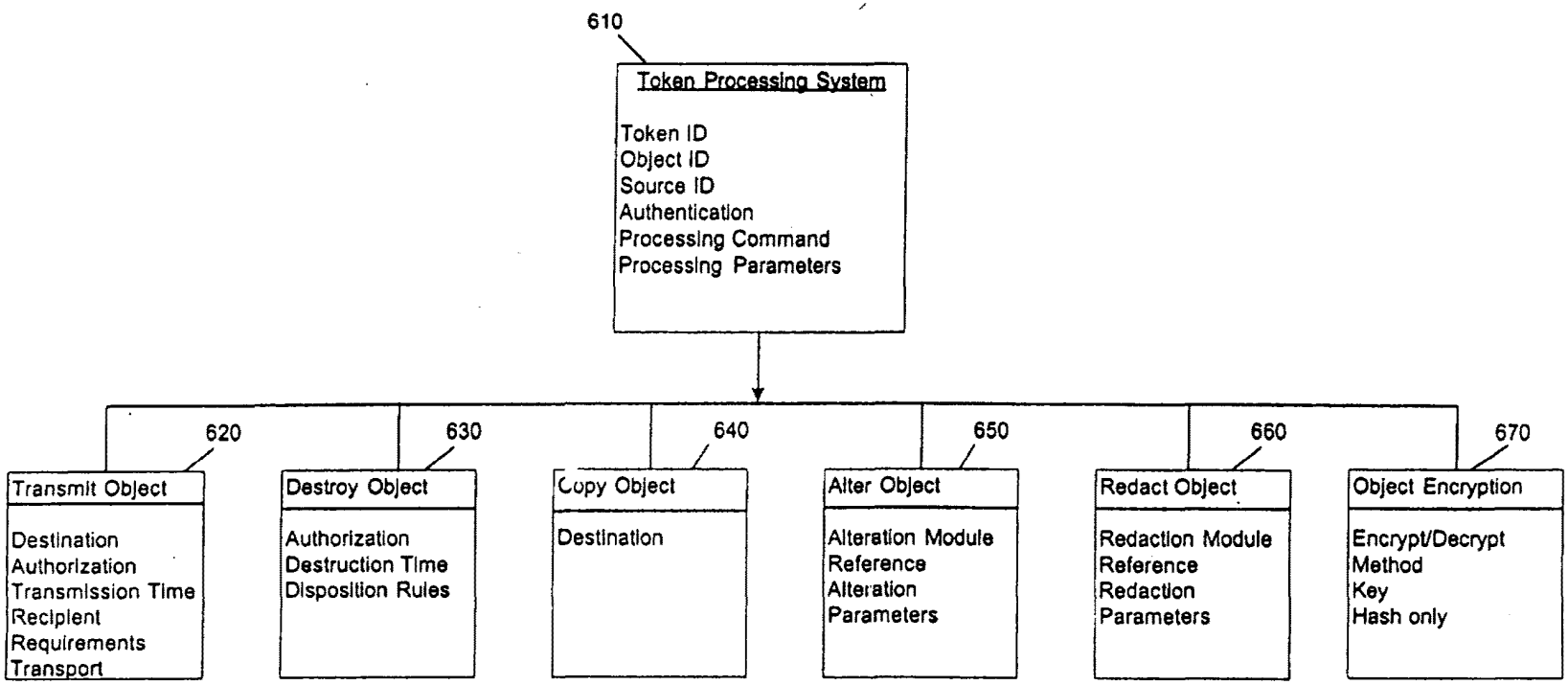


Figure 6

Partial Token Based Data Processing System Command Table

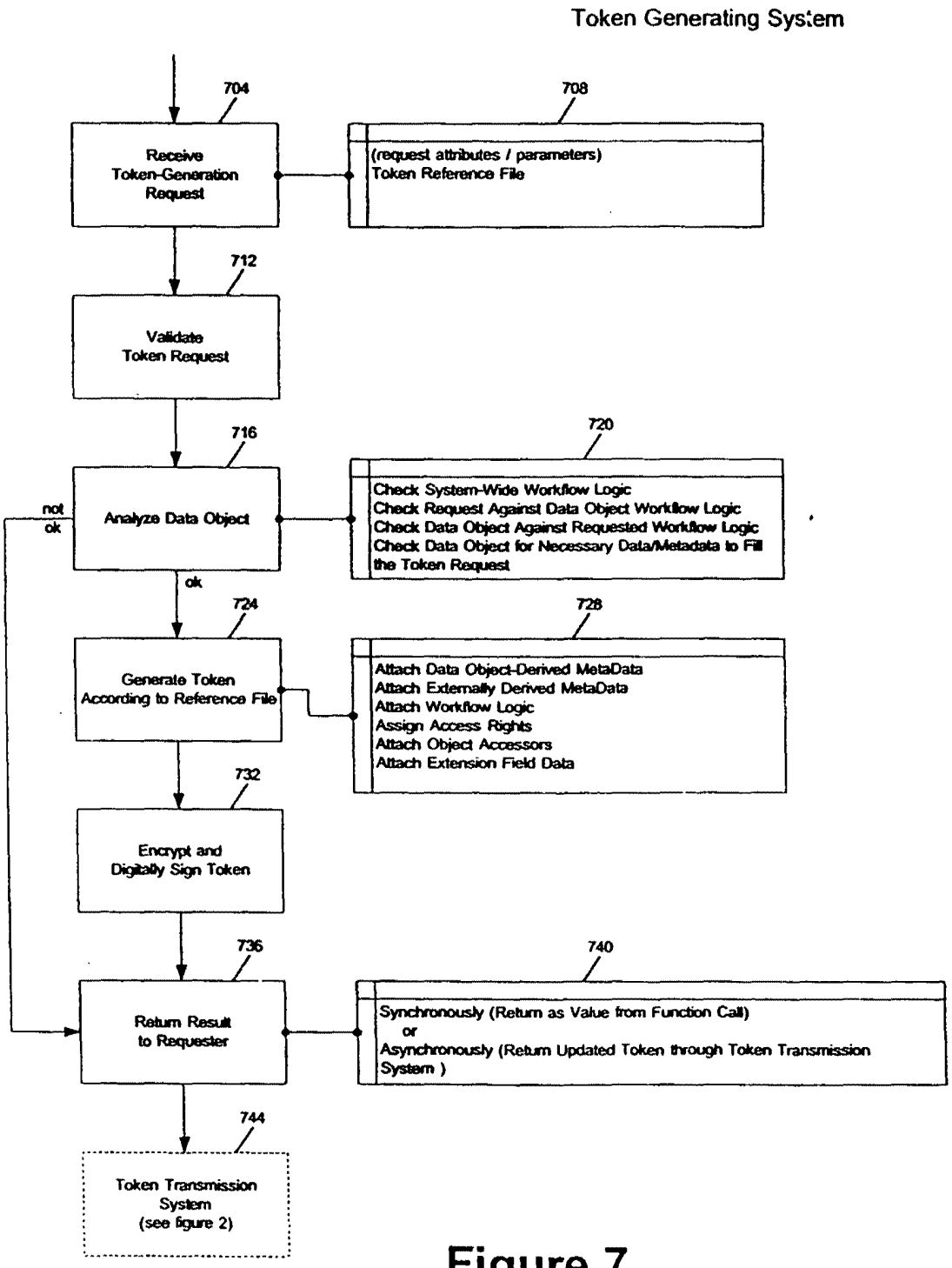

Token Generating System
704
Receive Token-Generation Request
708
(request attributes / parameters)
Token Reference File
712
Validate Token Request
716
Analyze Data Object
not ok
ok
720
Check System-Wide Workflow Logic
Check Request Against Data Object Workflow Logic
Check Data Object Against Requested Workflow Logic
Check Data Object for Necessary Data/Metadata to Fill the Token Request
724
Generate Token According to Reference File
728
Attach Data Object-Derived MetaData
Attach Externally Derived MetaData
Attach Workflow Logic
Assign Access Rights
Attach Object Accessors
Attach Extension Field Data
732
Encrypt and Digitally Sign Token
736
Return Result to Requester
740
Synchronously (Return as Value from Function Call)
or
Asynchronously (Return Updated Token through Token Transmission System)
744
Token Transmission System
(see figure 2)

Figure 7

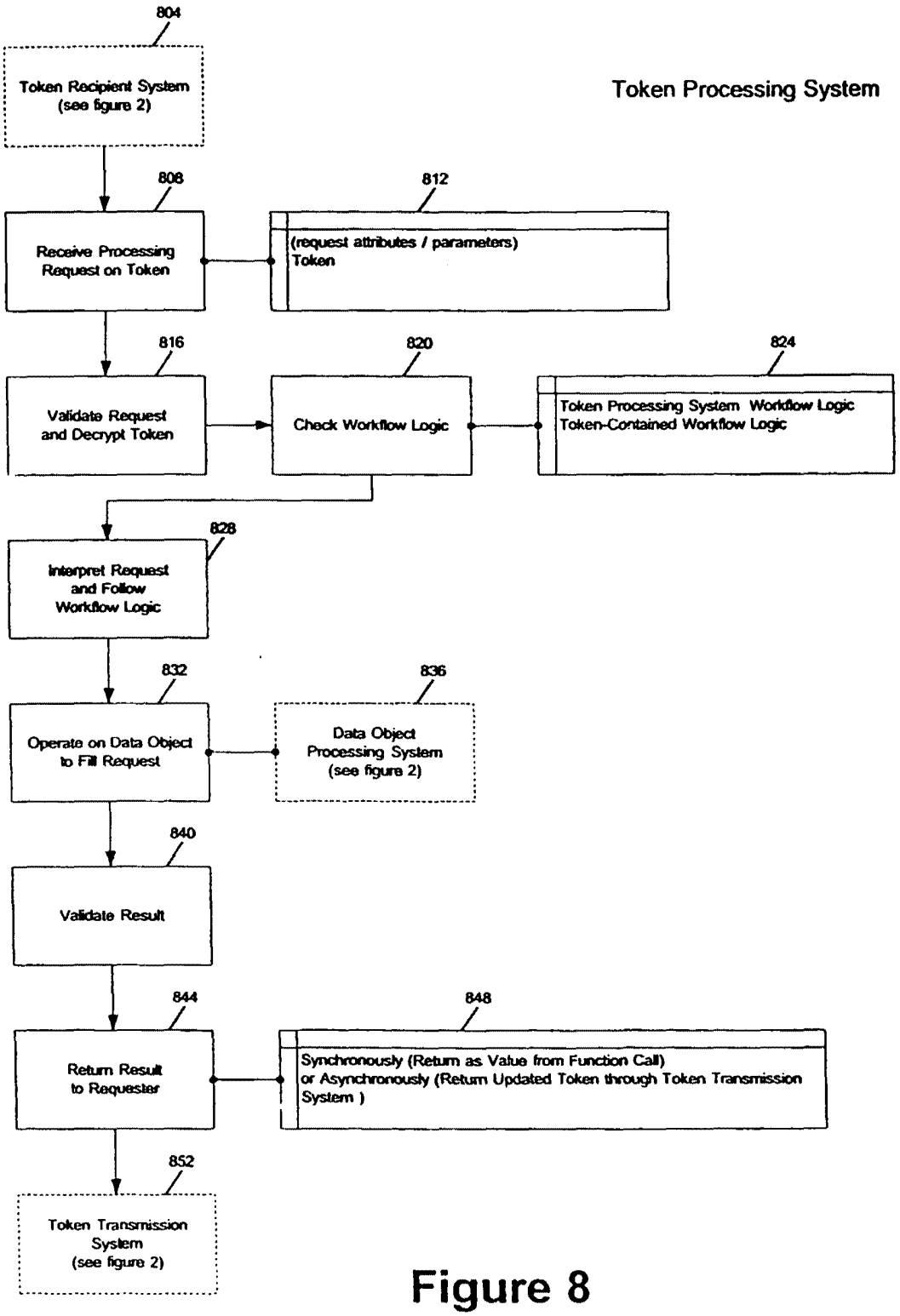

804
Token Recipient System
(see figure 2)
Token Processing System
808
Receive Processing
Request on Token
812
(request attributes / parameters)
Token
816
Validate Request
and Decrypt Token
820
Check Workflow Logic
824
Token Processing System Workflow Logic
Token-Contained Workflow Logic
828
Interpret Request
and Follow
Workflow Logic
832
Operate on Data Object
to Fill Request
836
Data Object
Processing System
(see figure 2)
840
Validate Result
844
Return Result
to Requester
848
Synchronously (Return as Value from Function Call)
or Asynchronously (Return Updated Token through Token Transmission
System)
852
Token Transmission
System
(see figure 2)

Figure 8

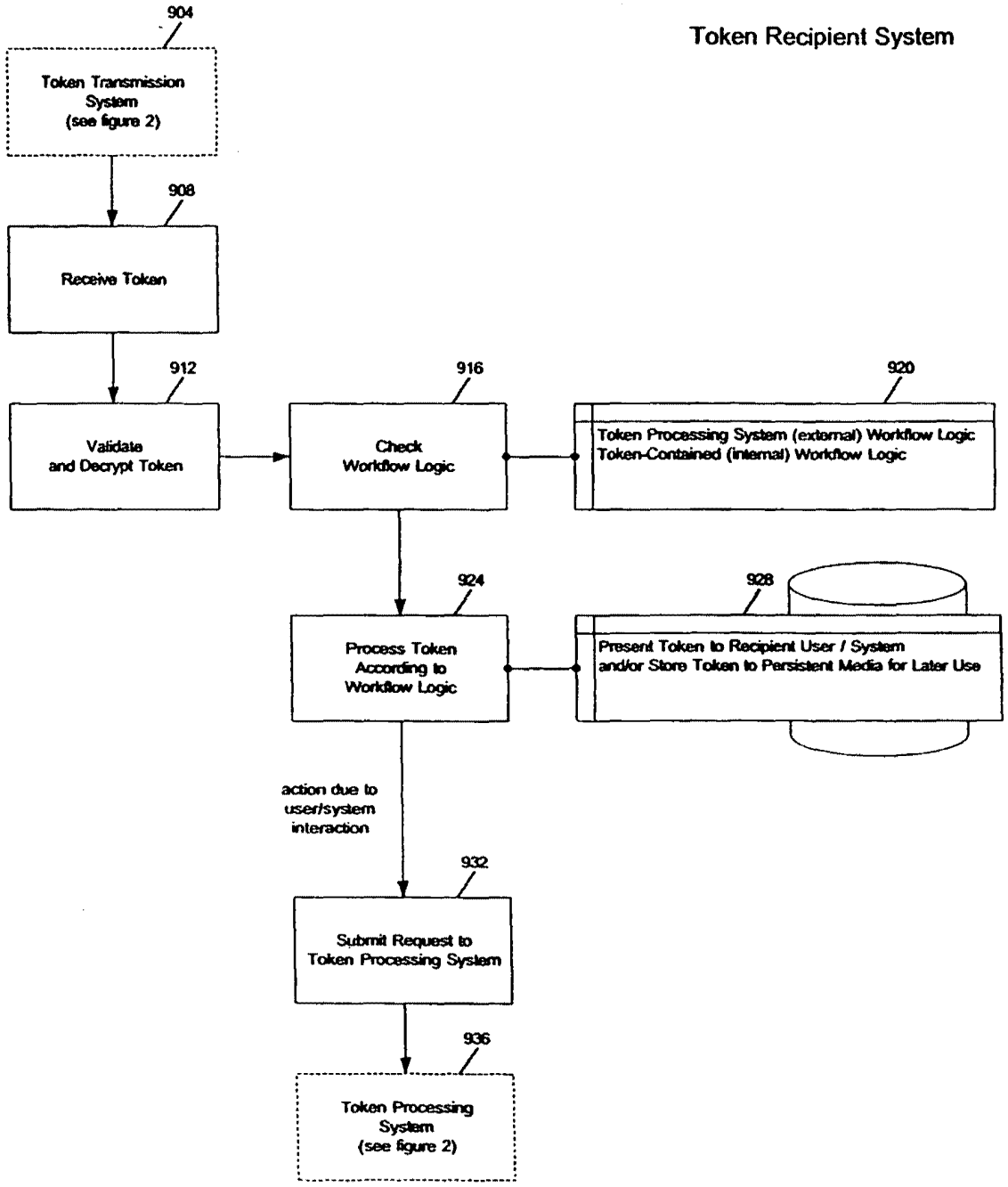

Token Recipient System
904
Token Transmission System (see figure 2)
908
Receive Token
912
Validate and Decrypt Token
916
Check Workflow Logic
920
Token Processing System (external) Workflow Logic
Token-Contained (internal) Workflow Logic
924
Process Token According to Workflow Logic
928
Present Token to Recipient User / System and/or Store Token to Persistent Media for Later Use
action due to user/system interaction
932
Submit Request to Token Processing System
936
Token Processing System (see figure 2)

Figure 9

OIPE JC1 90
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

2141
#5
PATENTS 30
12-2-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003 Group 2143

For: Data Security System and Method for Portable Device

TRANSMITTAL LETTER

RECEIVED
DEC 0 1 2003
Technology Center 2100

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Please find enclosed for filing:

RECEIVED
DEC 0 2 2003

X Submission of Formal Drawings with certificate of mailing (1 pg.)

X Twenty (20) sheets formal drawings

X Return Receipt Postcard

X Please credit any overpayments or charge any underpayments to Deposit Account No. 03-1231

This Transmittal Letter is submitted in duplicate.

Respectfully submitted,

By _____

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Docket No.: 6851-2-CIP-5

OIPE JC130
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Mail Stop PGPUB Drawings, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 26, 2003.

Robert C. Kain, Jr.
Reg. No. 30,648

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-2-cip-5 TRANS.DRW.wpd

RECEIVED
DEC 0 1 2003
Technology Center 2100

OIPE JC100
NOV 28 2003
PATENT & TRADEMARK OFFICE

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807
Confirmation No. 6441

Filed: March 19, 2003 Group 2143

For: Data Security System and Method for Portable Device

SUBMISSION OF FORMAL DRAWINGS

RECEIVED
DEC 0 1 2003
Technology Center 2100

Mail Stop PGPUB Drawings
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed please find twenty (20) sheet(s) of formal drawings for the captioned case.

Respectfully submitted,

By _____

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Mail Stop PGPUB Drawings, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 26, 2003.

_____

Robert C. Kain, Jr.
Reg. No. 30,648

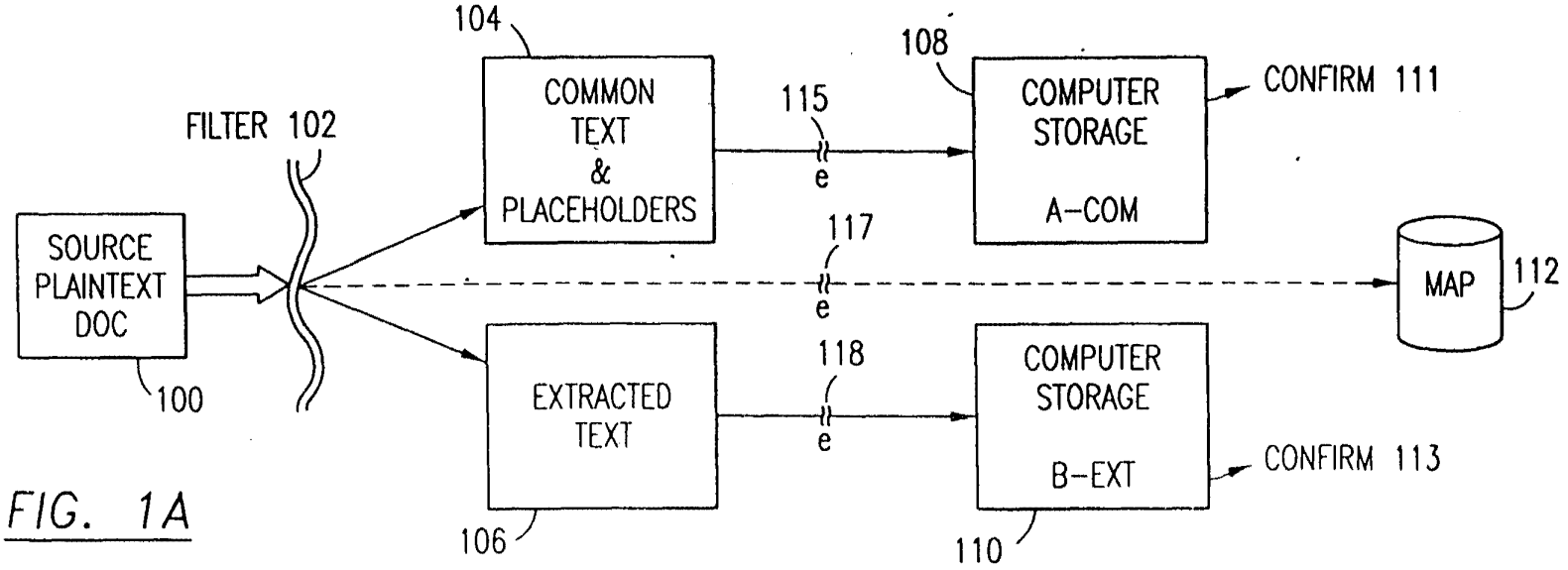


FIG. 1A

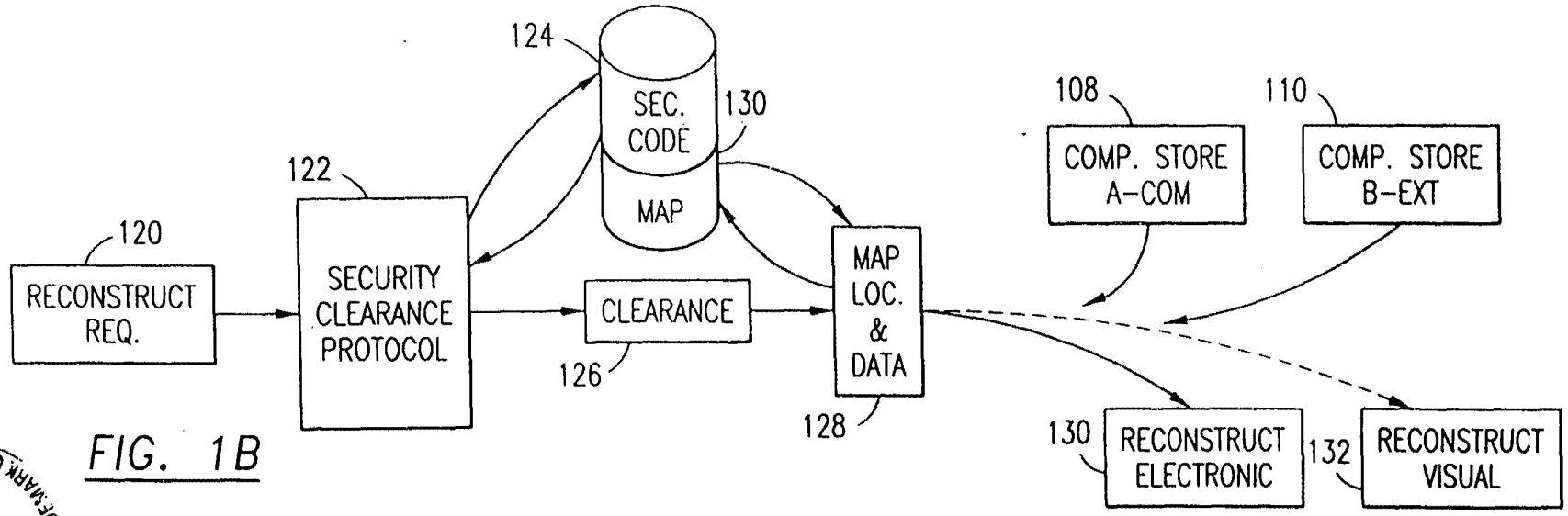


FIG. 1B

OIPE
NOV 28 2003
PATENT & TRADEMARK OFFICE

OIPE JC180
NOV 20 2003
PATENT & TRADEMARK OFFICE

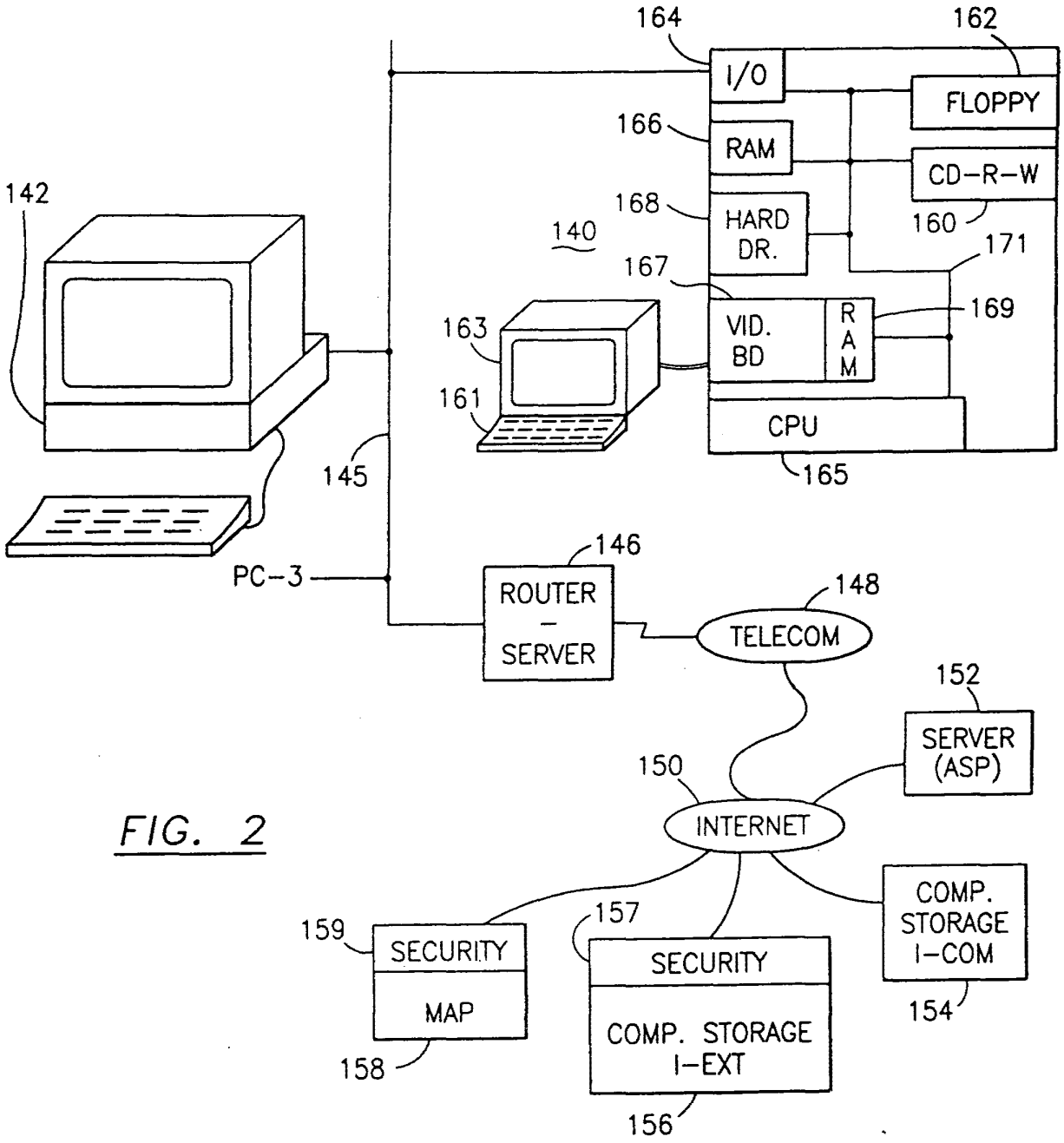


FIG. 2

OIPE JC130
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG. 3

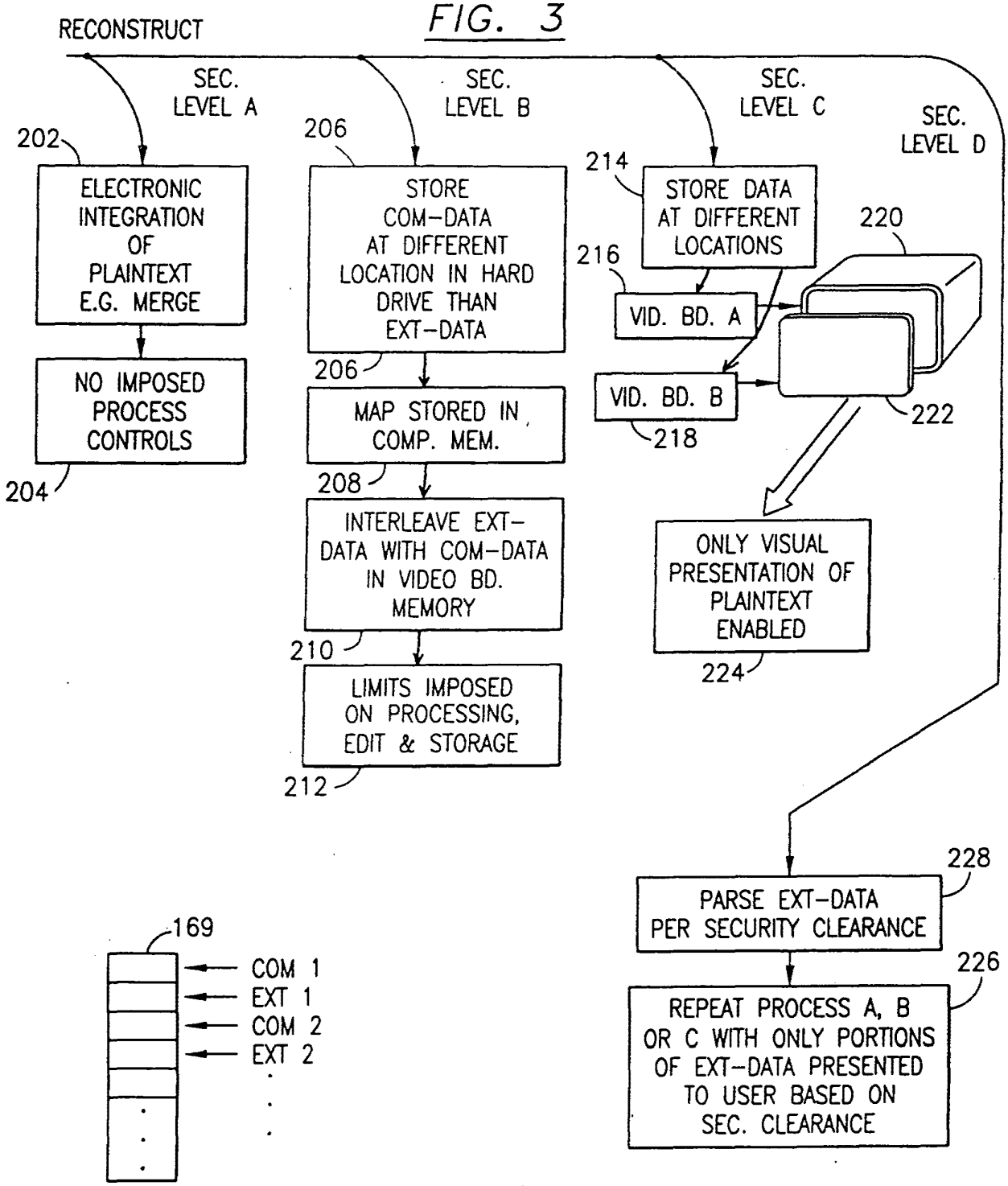
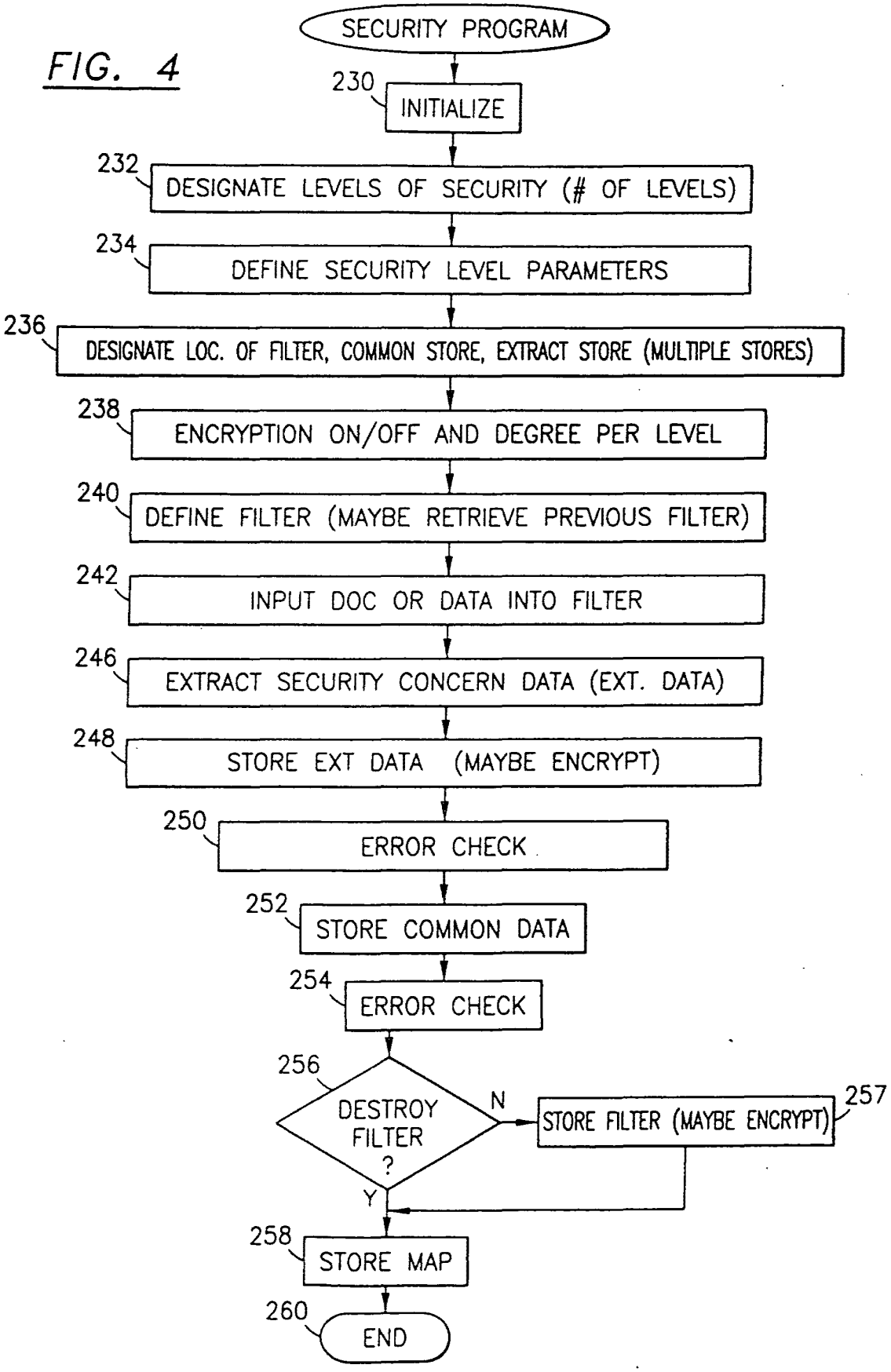


FIG. 3A

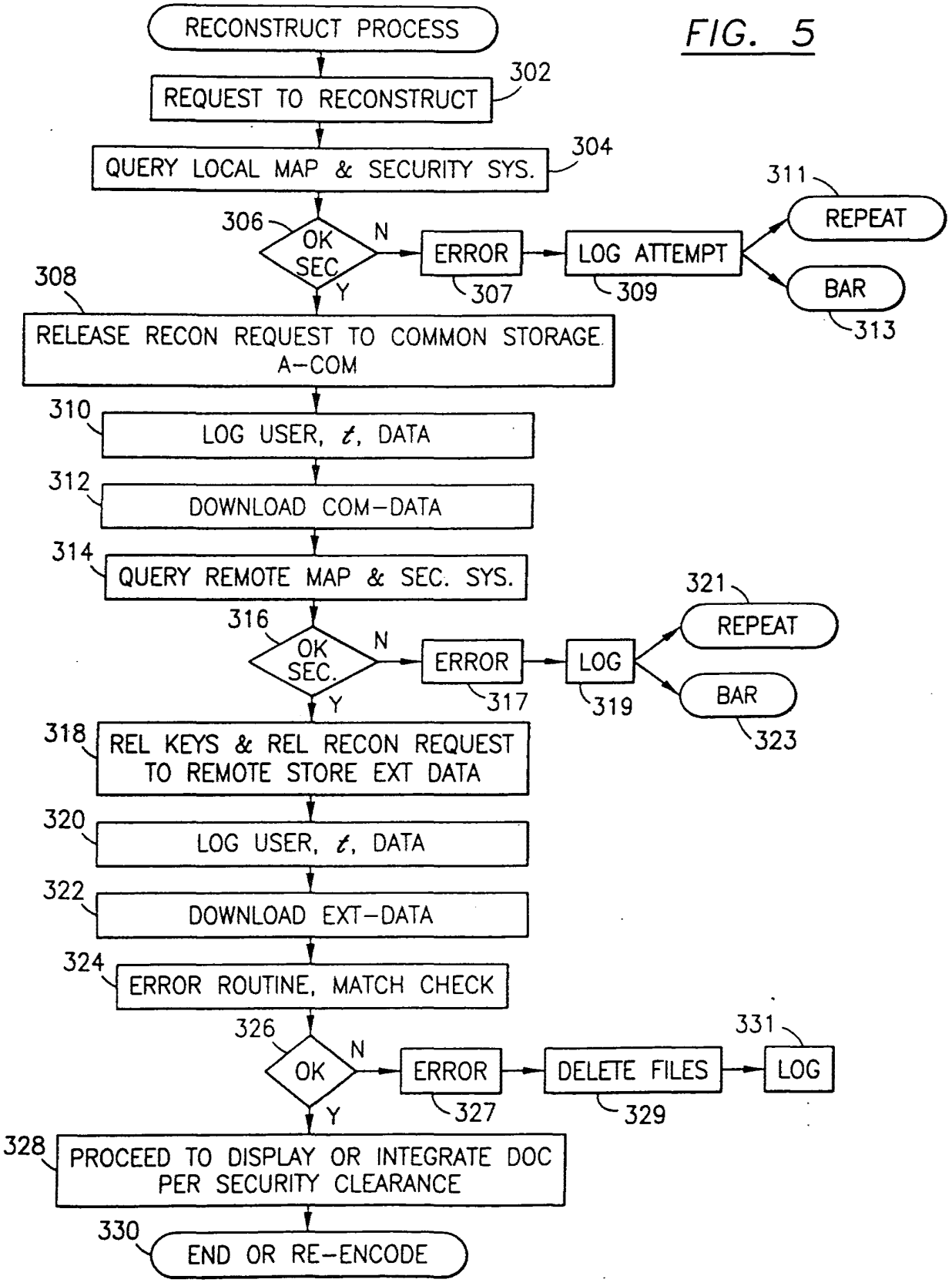
OIPE JC130
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG. 4



OIPE JC100
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG. 5



PATENT & TRADEMARK OFFICE
NOV 28 2003

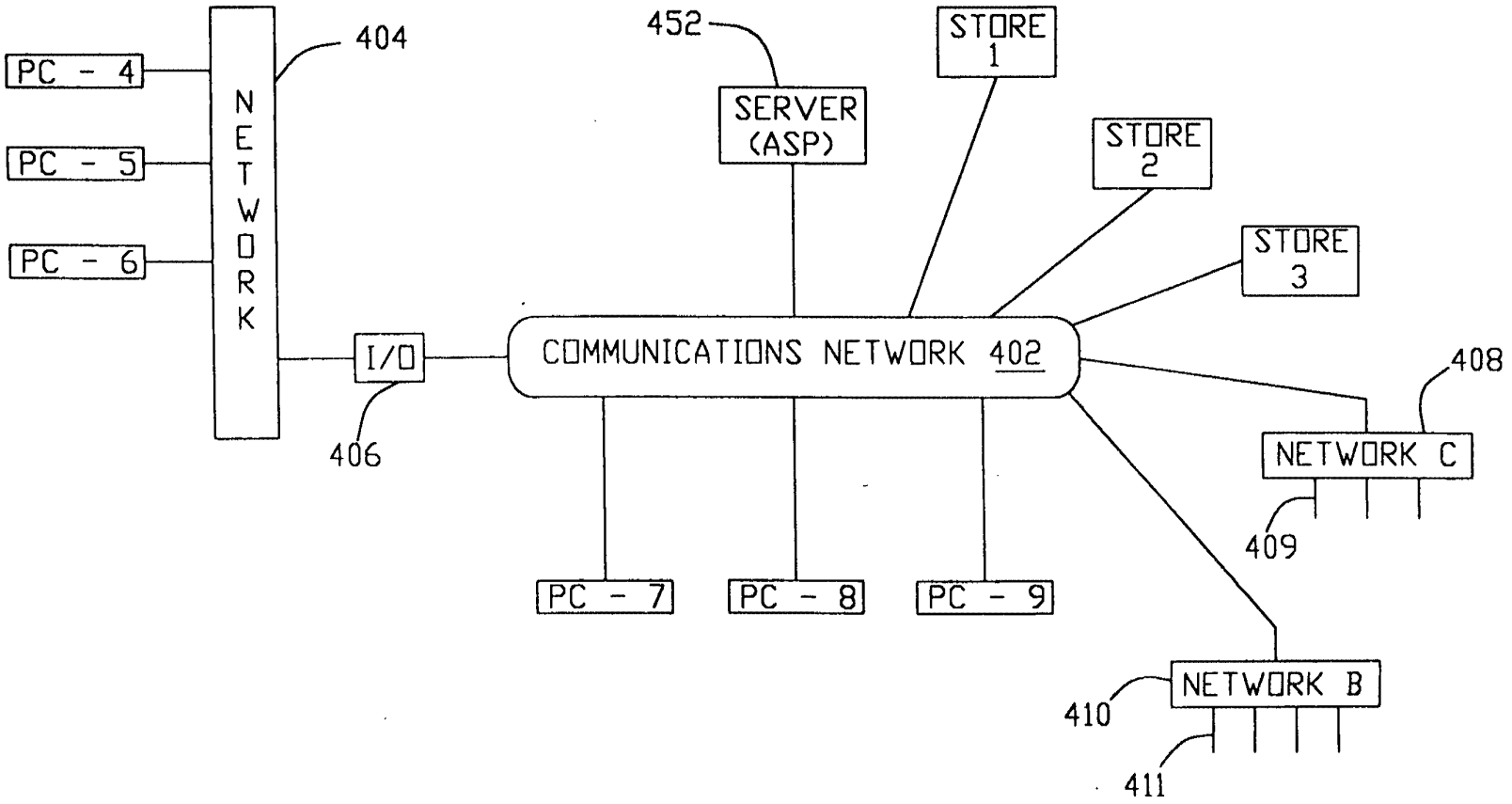
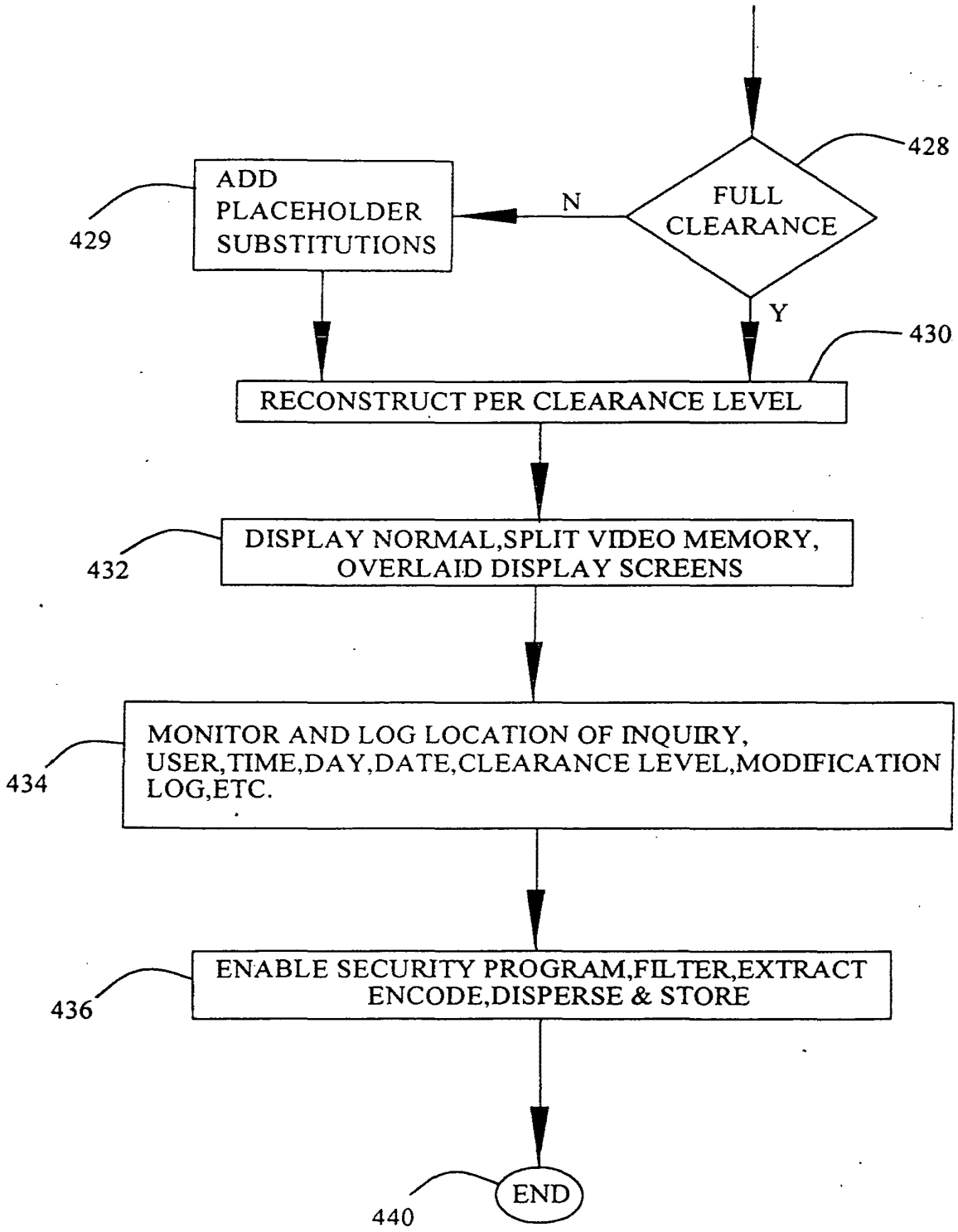


FIG.6

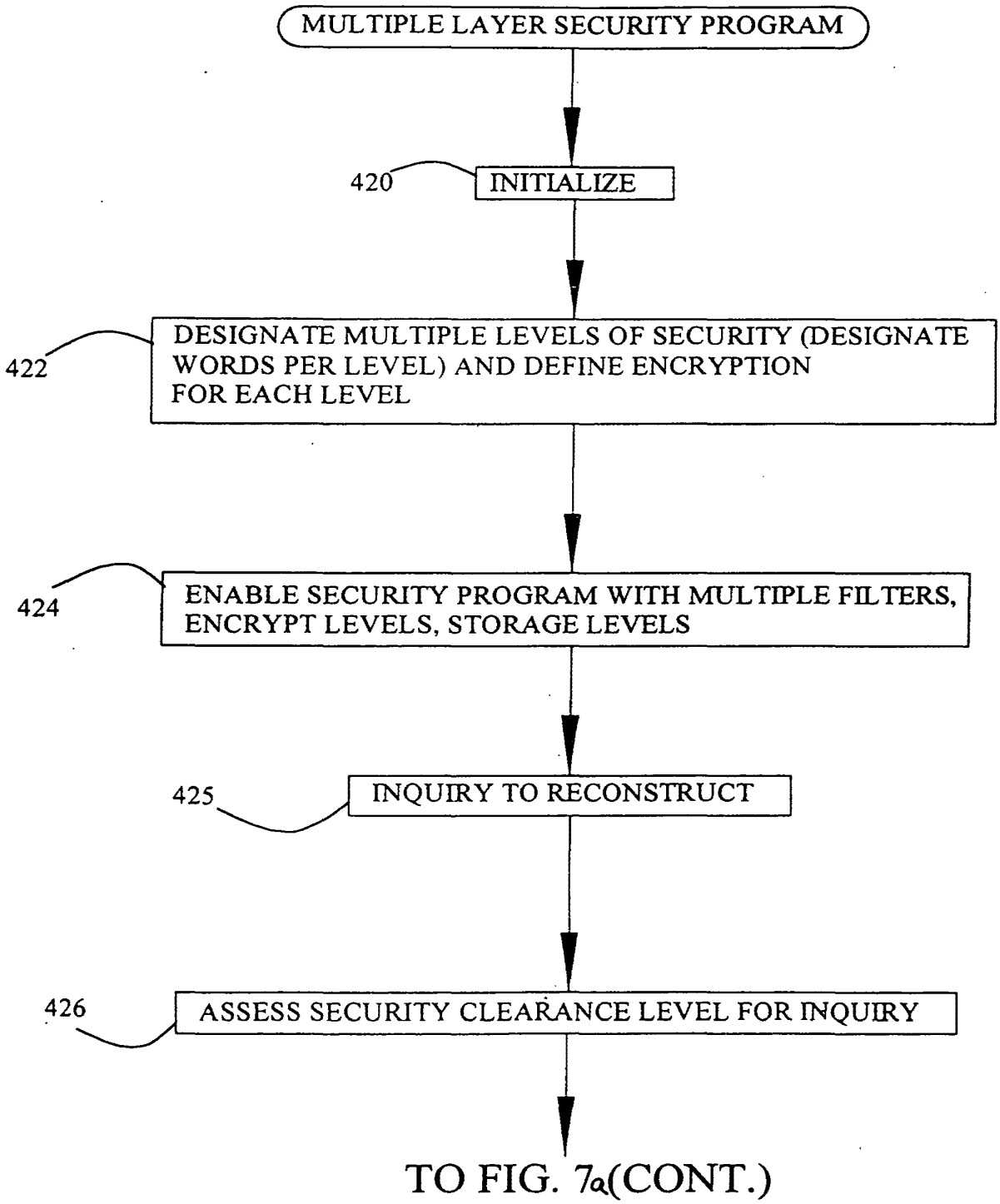
OIPE JC130
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG. 7a(CONT.)



OIPE JC130
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG. 7a



OIPE JC130
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

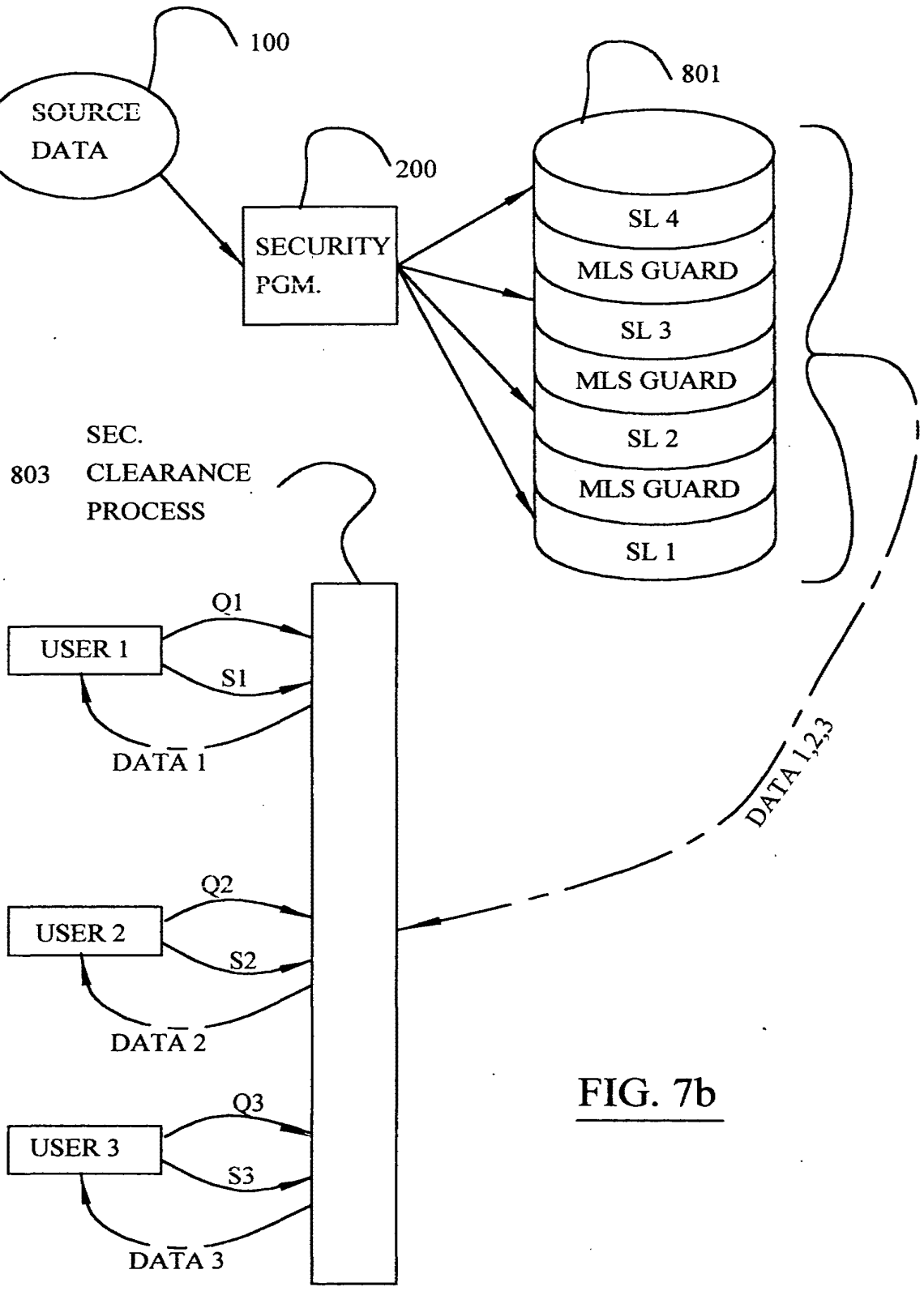
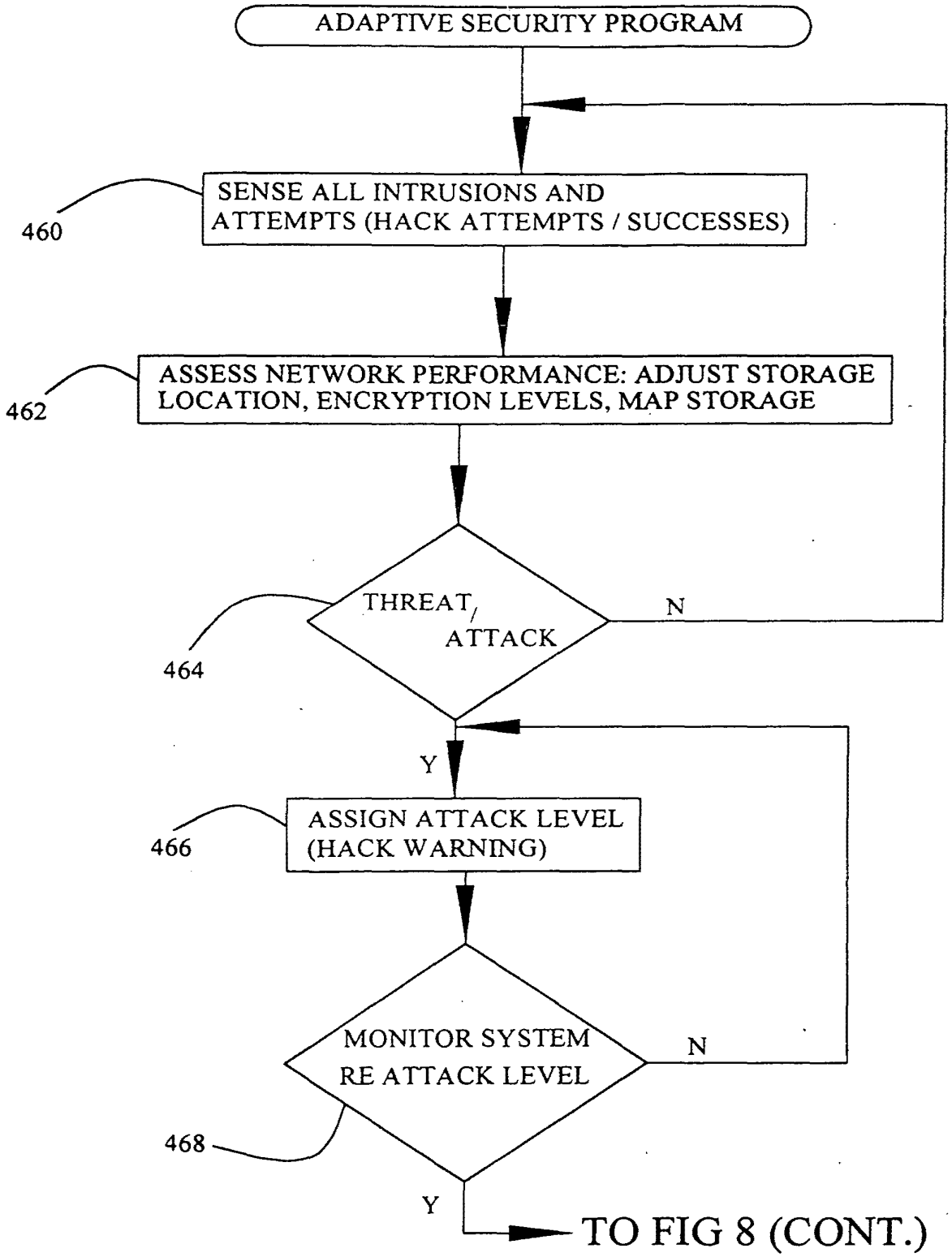


FIG. 7b

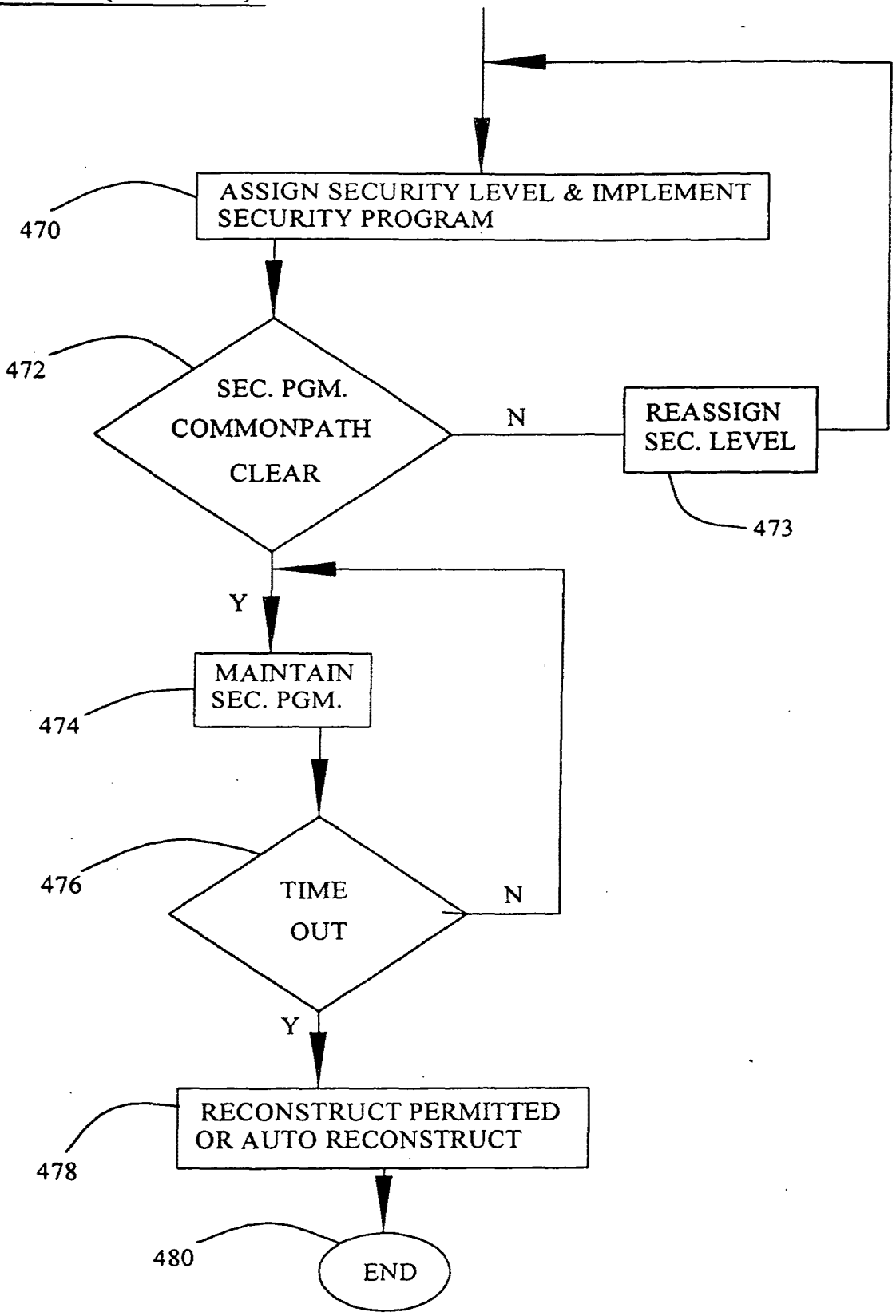
OIPE JC130
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG. 8



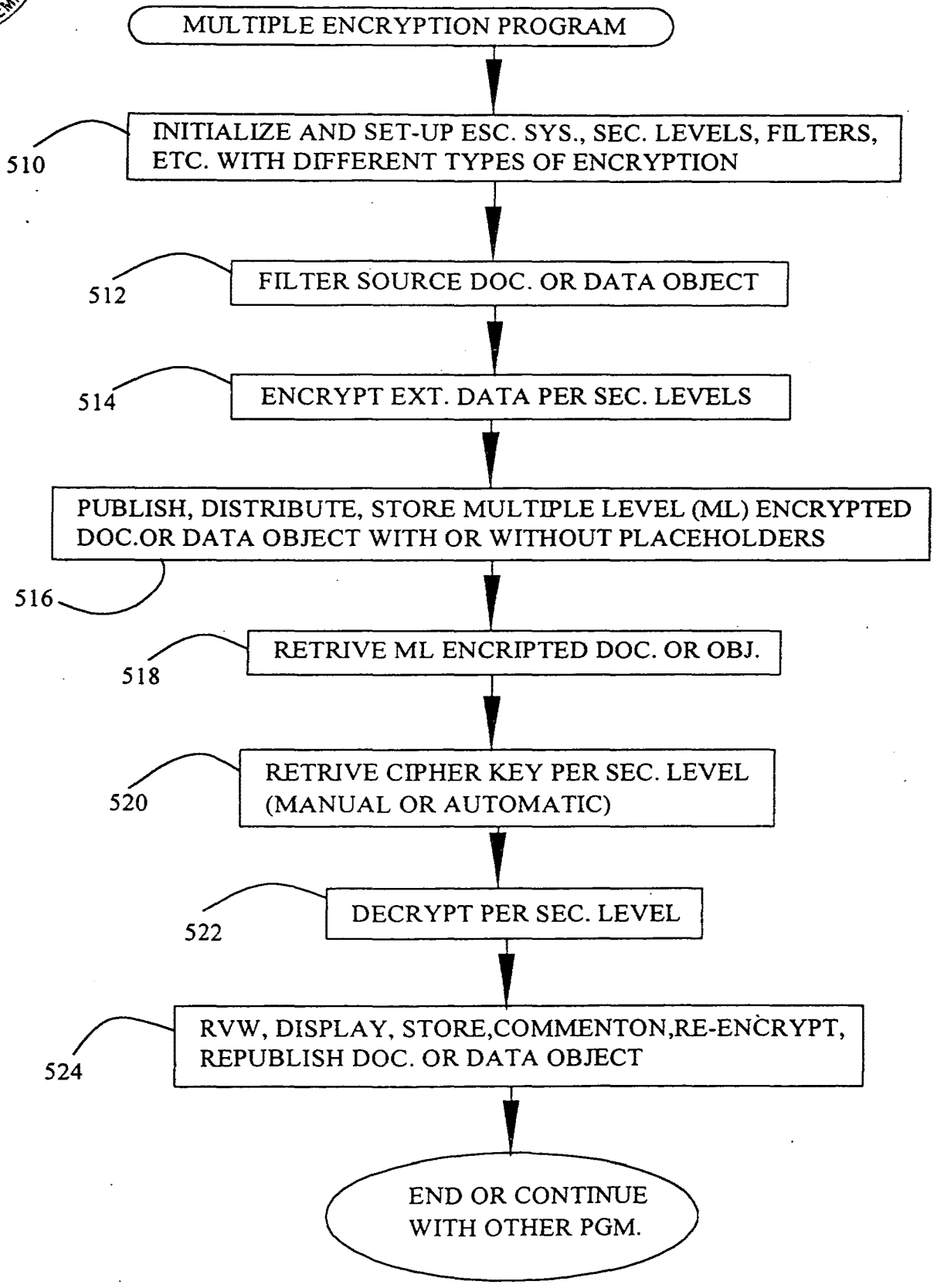
OIPE JC190
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

FIG. 8 (CONT.)



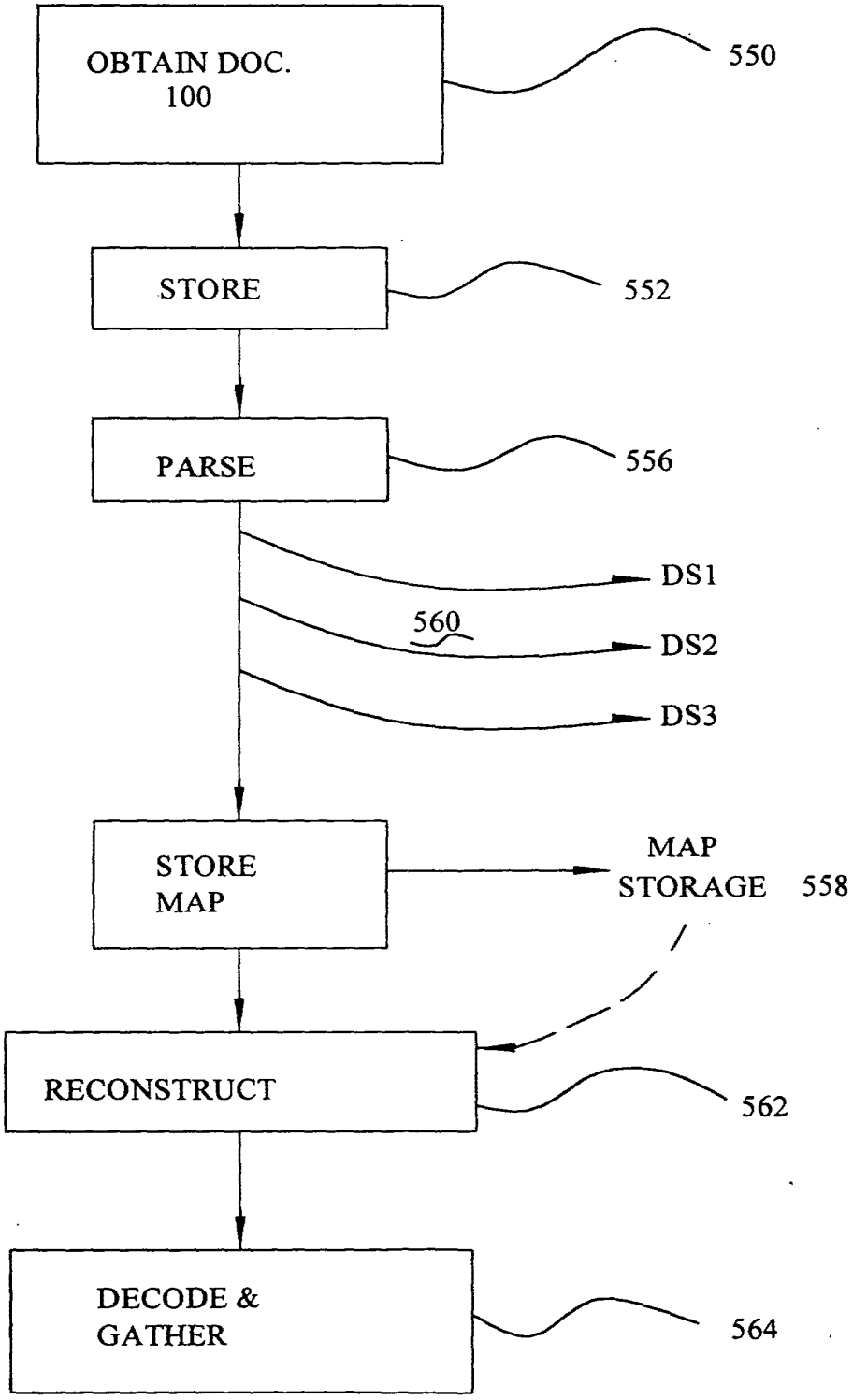
OIPE JC1 30
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

FIG. 9



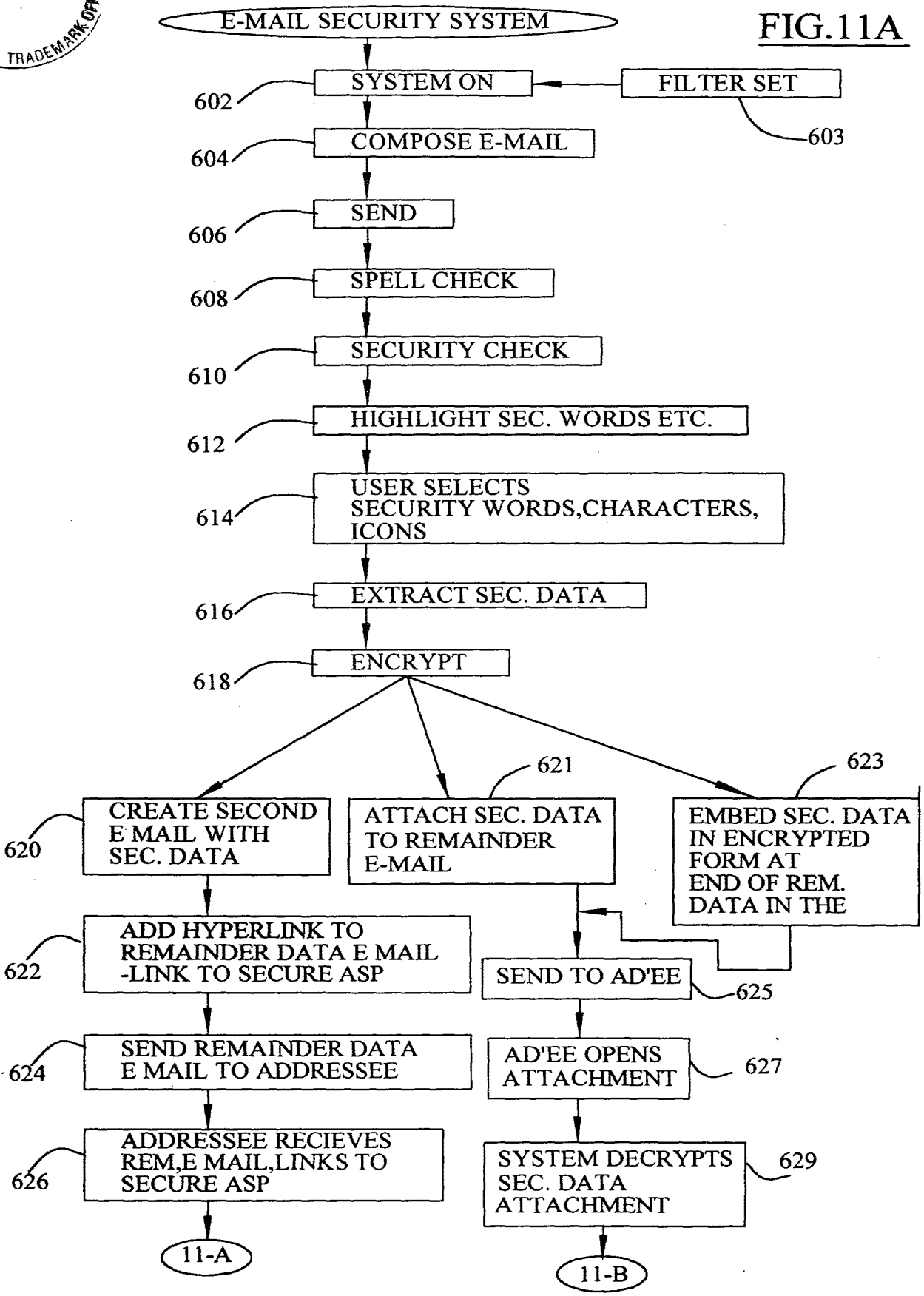
OIPE JC130
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

FIG. 10



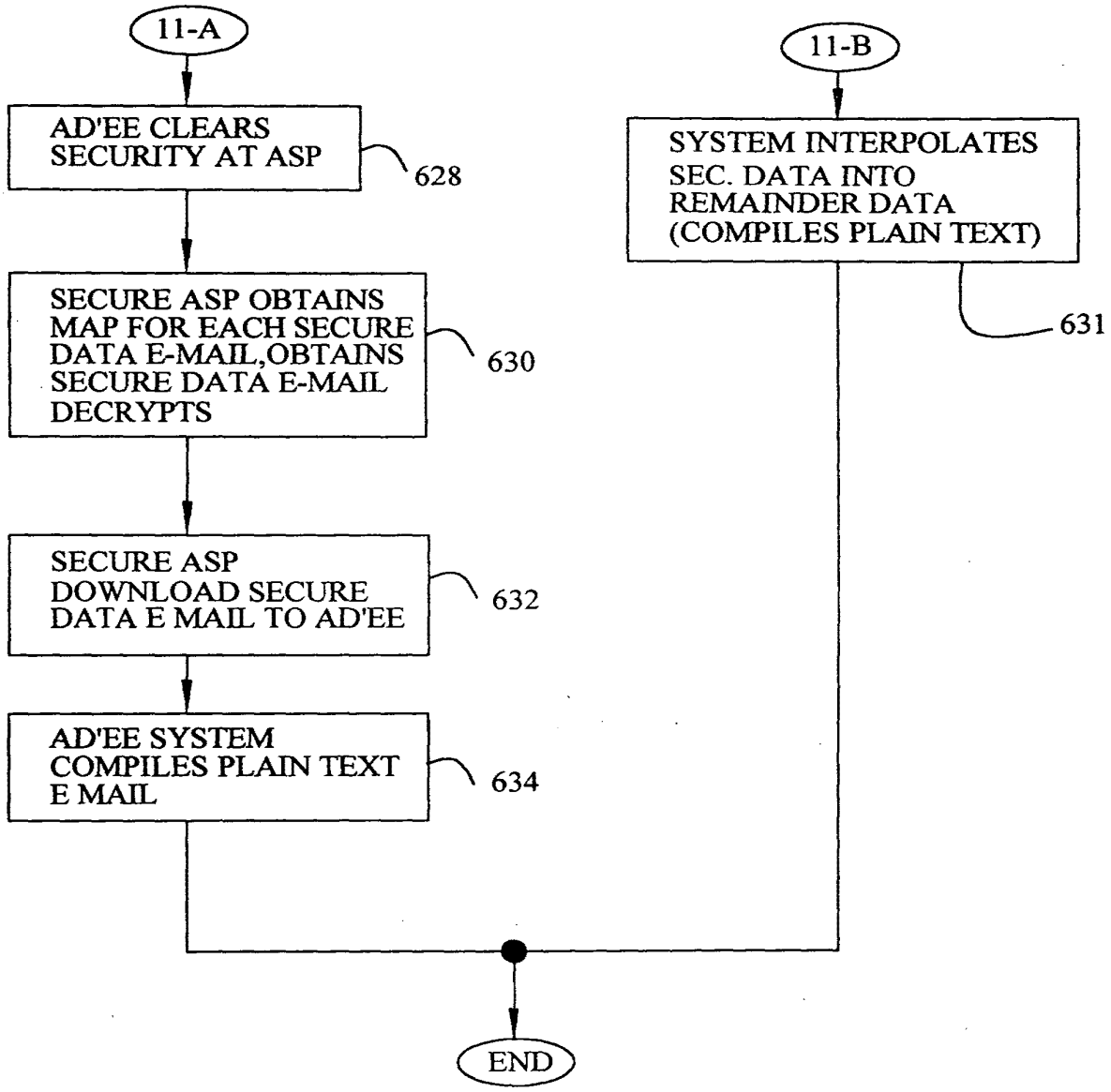
OIPE JC130
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

FIG.11A



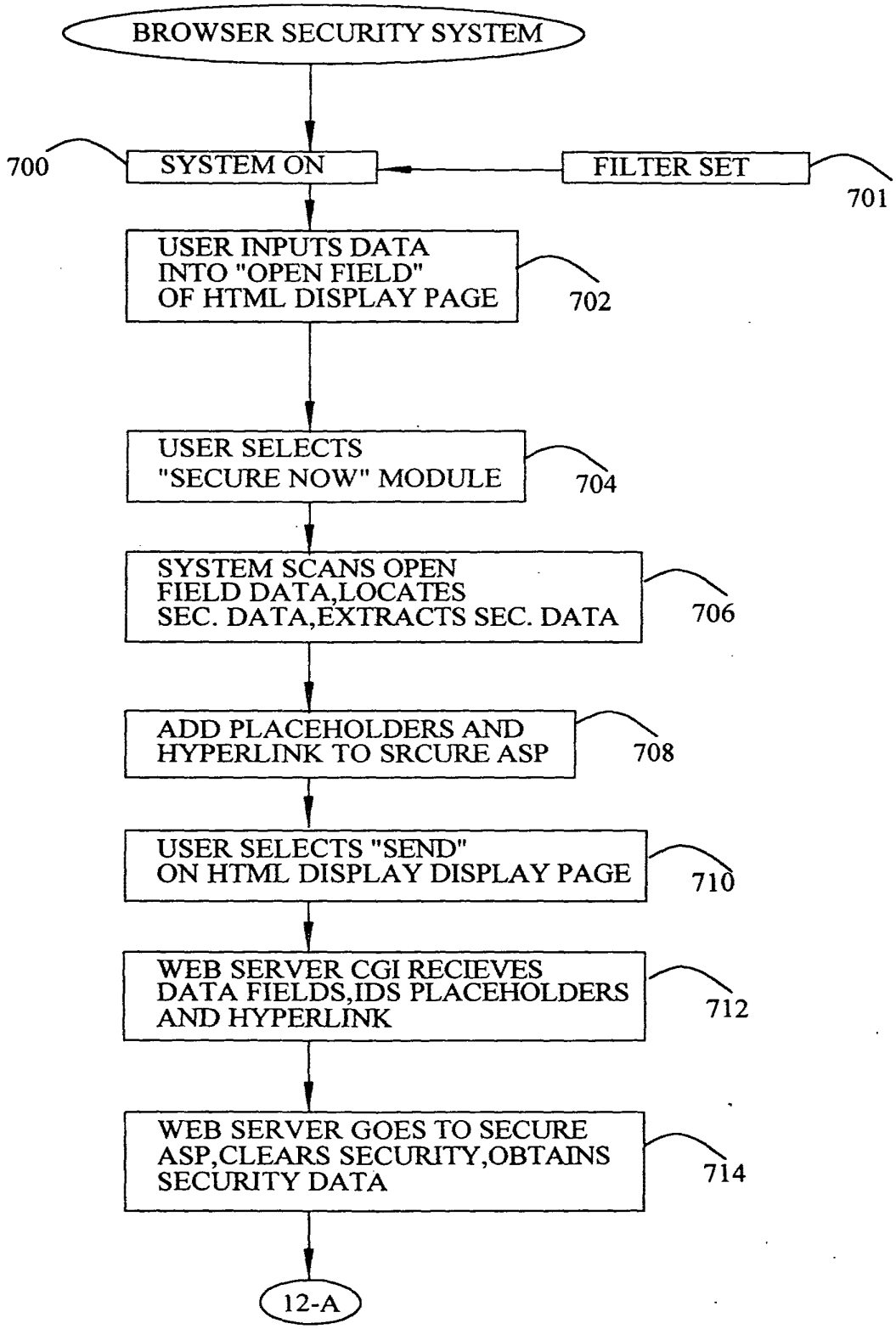
OIPE JC130
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

FIG.11B



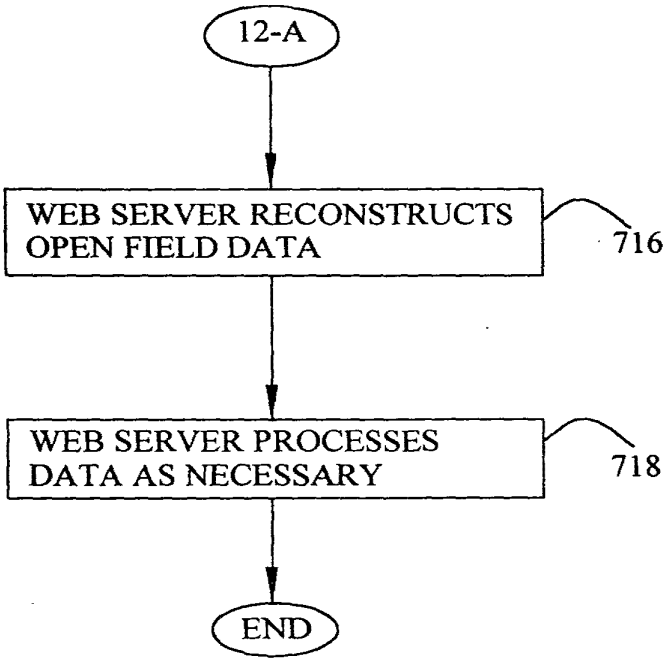
OIPE JC190
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

FIG.12A



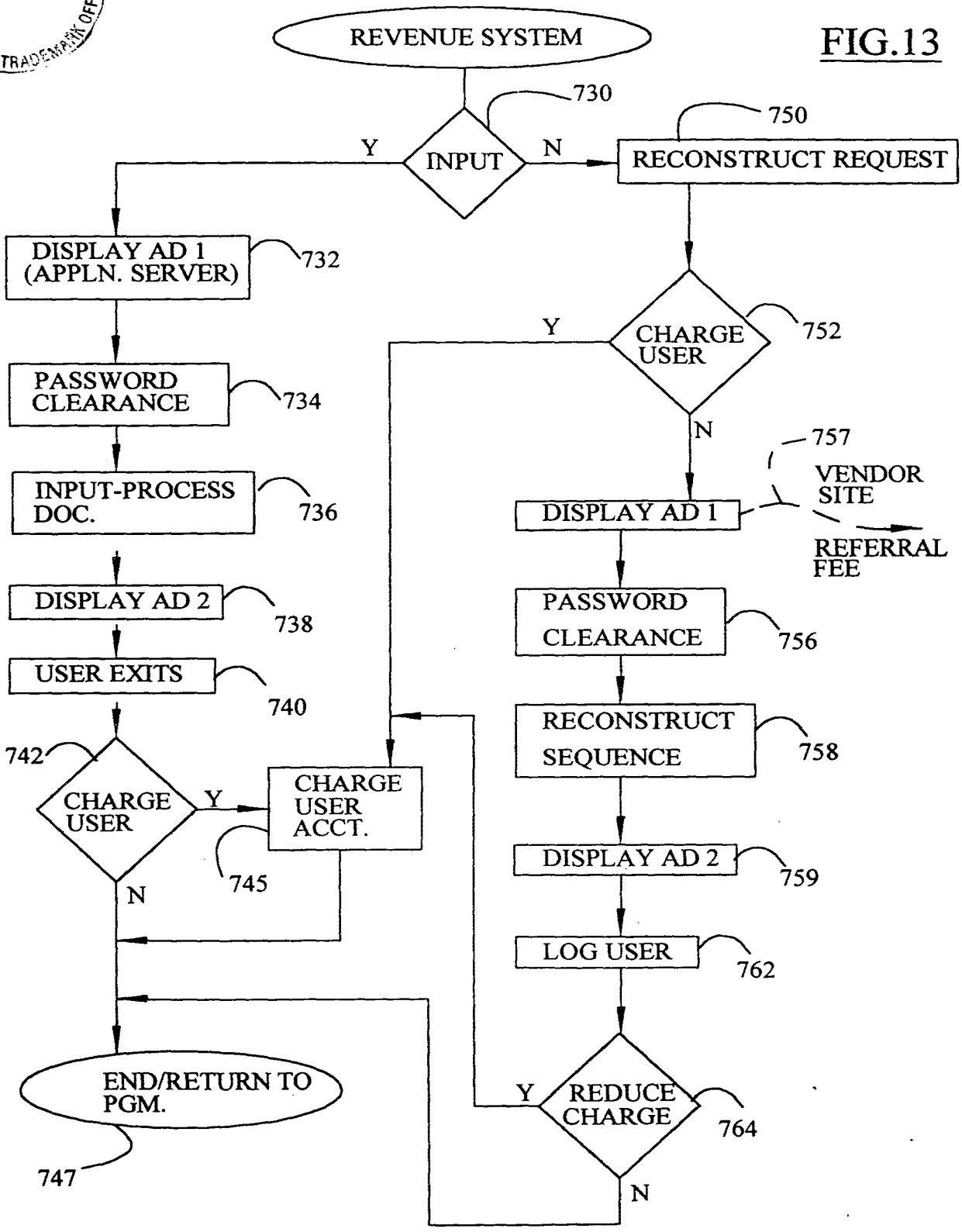
OIPE JC130
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG.12B



OIPE JC190
NOV 28 2003
PATENT & TRADEMARK OFFICE

FIG.13



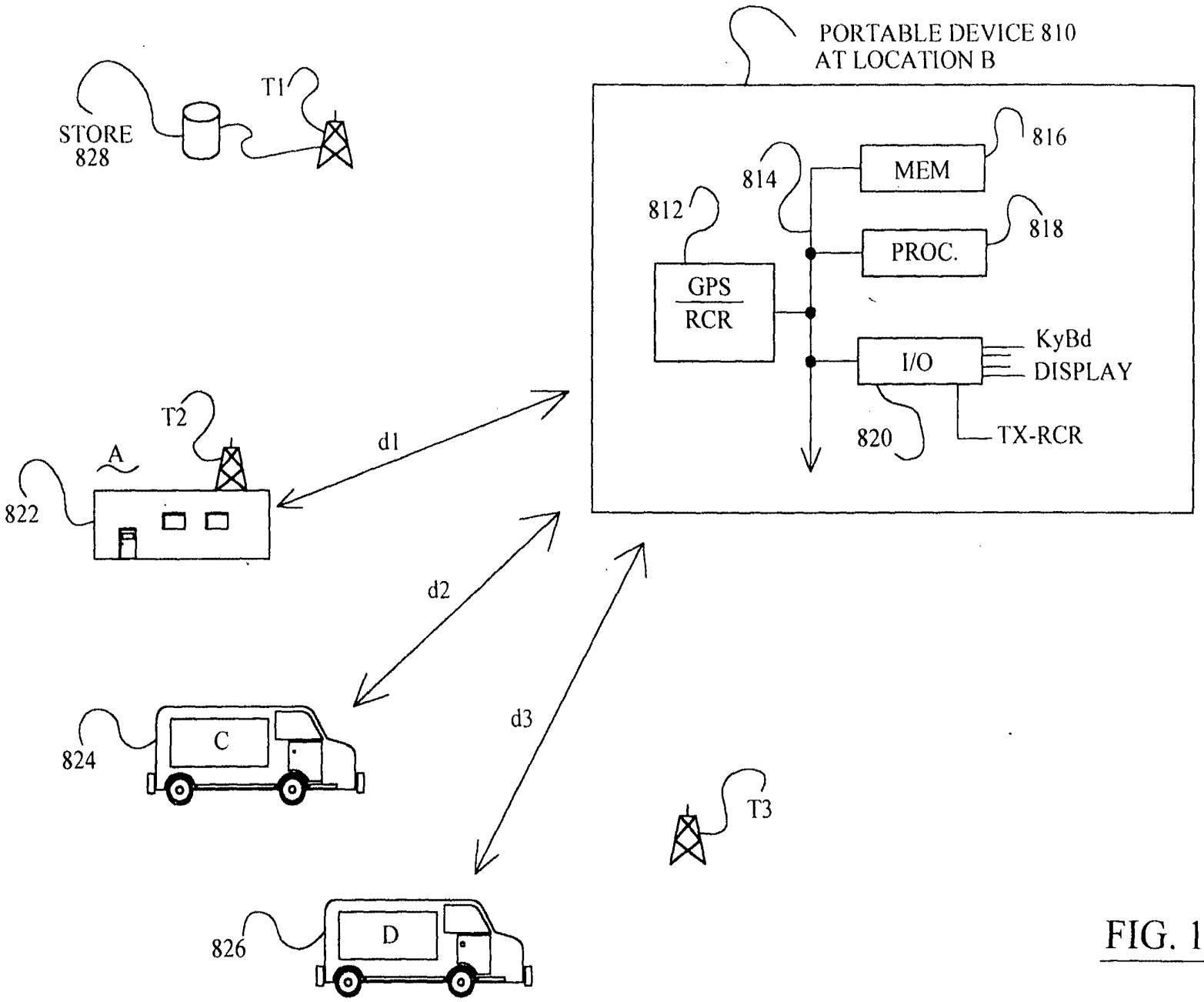


FIG. 14

PATENT & TRADEMARK OFFICE NOV 2 8 2003 OIPE JC13

OIPE JC1300
NOV 2 8 2003
PATENT & TRADEMARK OFFICE

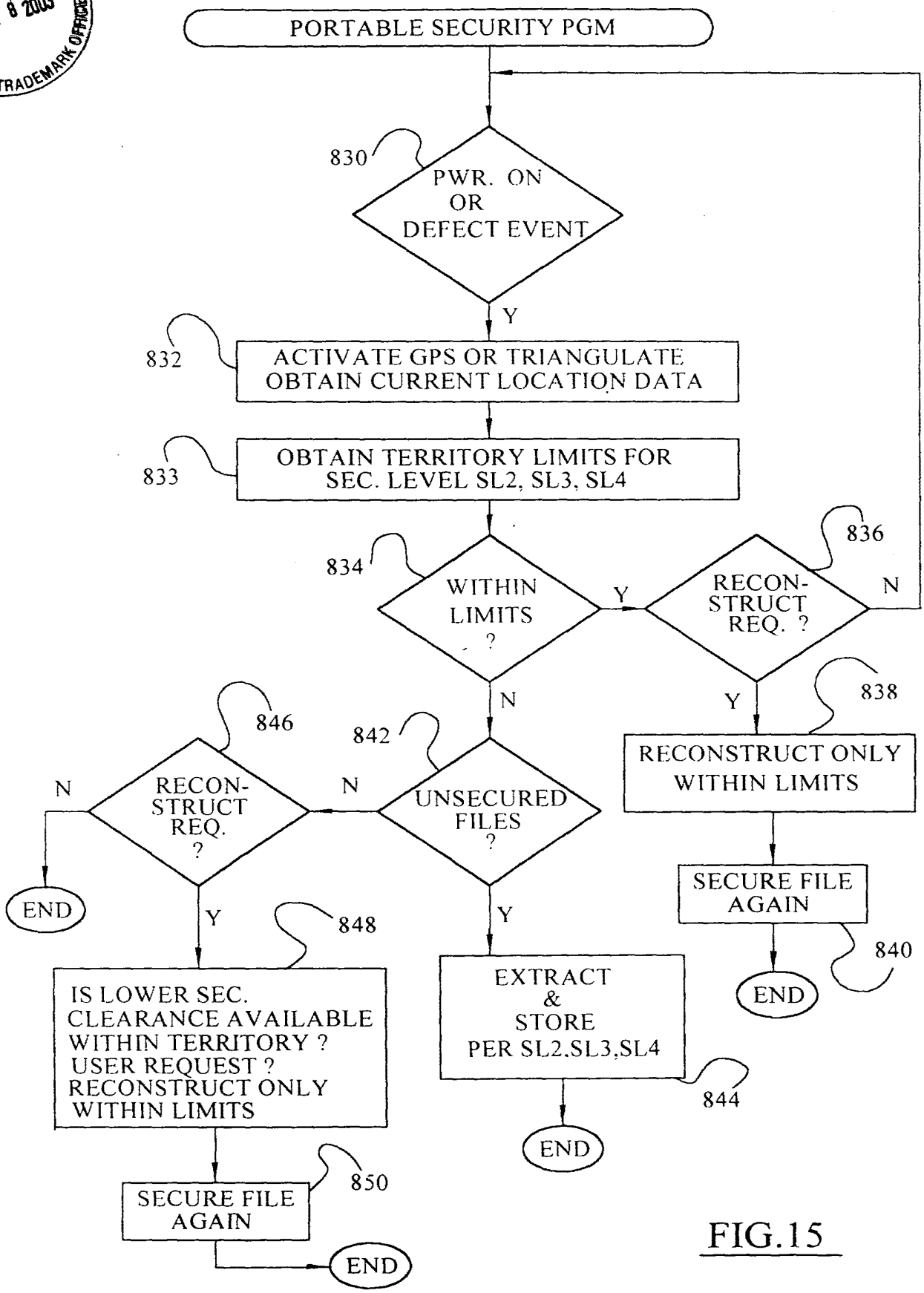


FIG.15

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807 Group Art 2143

Confirmation No.: 6441

Filed: March 19, 2003

For: Data Security System and Method for Portable Device

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97.

Patent No.	Inventor	Issue Date
6192472	Garay et al.	Feb. 20, 2001
6148342	Ho	Nov. 14, 2000
6094483	Fidrich et al.	Jul. 25, 2000
6055544	DeRose et al.	Apr. 25, 2000
5996011	Humes	Nov. 30, 1999
5905980	Masuichi et al.	May 18, 1999

5832212	Cragun et al.	Nov. 3, 1998
5485474	Rabin	Jan. 16, 1996
5933498	Schneck et al	Aug. 3, 1999
US2002/0073313	Brown et al.	Jun. 13, 2002
WO 00/75779-A2	Lambert	Dec. 14, 2000

-Ingrian i100, Content Security Appliance (2 pages)

-Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)

-Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)

-ZD Net Interactive Week - IBS, SAP: XML to Boost Security, integration.

-Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999.

-MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001.

-Cisco IDS Host Sensor Product, October 16, 2001.

The examiner in Serial No. 09/916,397 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,602298 to Kirshenbaum
U.S. Patent No. 6,078,907 to Lamm
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)
The Uniform Resource Locator article "FOLD OC" (attached to Office Action)

The examiner in Serial No. 10/008,209 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz

U.S. Patent No. 6,078907 to Lamm (PRIMARY REFERENCE)
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)
The Uniform Resource Locator article "FOLD OC" (attached to Office Action)

The examiner in Serial No. 10/008,218 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,078,907 to Lamm
U.S. Patent No. 6,301,668 to Gleichauf
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
U.S. Patent No. 6,714,977 to Fowler
The 1996 book, Applied Cryptography, by Schneier (attached to Office Action)
The Uniform Resource Locator article "FOLD OC" (attached to Office Action)
Wylie "Survivable Information Storage Systems" (cited by Redlich)

The examiner in Serial No. 10/155,192 cited the following references:

U.S. Patent No. 6,073,165 to Narasimhan
U.S. Patent No. 5,960,080 to Fahlman (PRIMARY REFERENCE)
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Patent No. 6,487,538 to Gupta
U.S. Patent No. 6,771,290 to Hoyle
Published U.S. Application 2002/0116641 to Mastrianni

The examiner in Serial No. 10/155,525 cited the following references:

U.S. Patent No. 6,073,165 to Narasimhan
U.S. Patent No. 5,960,080 to Fahlman (PRIMARY REFERENCE)
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Published Patent Application 2002/0116641 to Mastrianni
U.S. Published Patent Application 2004/0054630 to Ginter
Microsoft Word "Learning Microsoft Word 7.0"

The examiner in Serial No. 10/277,196 cited the following references:

U.S. Patent No.5,960,080 to Fahlman
U.S. Patent No.5,581682 to Anderson
U.S. Patent No.6,253,203 to O'Flaherty
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 6,044,375 to Shmueli

U.S. Patent No. 6,662,189 to Oyanagi
U.S. Patent No. 5,036,315 to Gurley

Related Cases

Our Ref.	Serial No.	Filed
-02-div1	tba	tba
-02-div2	tba	tba
-02-con	tba	tba
-02-cip5	10/390,807	March 19, 2004
-02-cip7	10/998,366	Nov. 26, 2003
-02-cip8	10/998,365	Nov. 26, 2004
-02-cip9	10/998,363	Nov. 26, 2004
-03	10/396,088	Mar. 25, 2003

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By _____

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip5-IDS.wpd

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ingrian i100, Content Security Appliance (1 pages)	
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigrigg, John D. Strunk, Gregory R. Ganger, Han Kiloccote Pradeep K. Khosla (8 pages)	
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)	
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	The 1996 book, Applied Cryptography, by Schneier	
	The Uniform Resource Locator article "FOLD OC"	
	Microsoft Word "Learning Microsoft Word 7.0"	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
	6,662,189	12/9/03	Oyanagi	707	102	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER DATE CONSIDERED

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip5-Form-PTO-1449.wpd

Electronic Acknowledgement Receipt

EFS ID:	1160782
Application Number:	10390807
Confirmation Number:	6441
Title of Invention:	Data security system and method for portable device
First Named Inventor:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-2-cip-5
Receipt Date:	18-AUG-2006
Filing Date:	19-MAR-2003
Time Stamp:	11:11:29
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Information Disclosure Statement (IDS) Filed	6851-02-cip5-IDS.pdf	271699	no	8

Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement (IDS) Filed	PA-Ingrian-I100-content-security-appliance.pdf	104559	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Information Disclosure Statement (IDS) Filed	PA-Element-Wise-XML-Encryption.pdf	235982	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Information Disclosure Statement (IDS) Filed	PA-Survivable-Information-Storage-Systems.pdf	548011	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Information Disclosure Statement (IDS) Filed	PA-ZD-Net-Interactive-Week.pdf	67921	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Information Disclosure Statement (IDS) Filed	PA-Mostly-Static-Decentralized-Myers.pdf	2216378	no	43
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Information Disclosure Statement (IDS) Filed	PA-Mimesweeper.pdf	630873	no	12
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

8	Information Disclosure Statement (IDS) Filed	PA-Cisco-IDS-Host-Sensor-Product.pdf	510120	no	10
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
9	Information Disclosure Statement (IDS) Filed	PA-Applied-Cryptography-Schneier.pdf	362813	no	5
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
10	Information Disclosure Statement (IDS) Filed	PA-FOLDOC.pdf	87383	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
11	Information Disclosure Statement (IDS) Filed	PA-Learning-Microsoft-Word.pdf	228594	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
		Total Files Size (in bytes):	5264333		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	52397	(extract$4 filter$4) with location	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 14:42
S2	752	S1 same GPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 14:45
S3	16	S2 same reconstruct$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 14:44
S4	403	S1 with GPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 14:45
S5	13	S4 same (security sensitiv$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 14:47
S6	48	GPS same gambling	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 07:58
S7	2	(("5960080") or ("6253203")).PN.	US-PGPUB; USPAT	OR	OFF	2006/12/08 10:07
S8	48	(REDLICH near RON) (NEMZOW nearMARTIN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:13
S9	23	("5423032"|"5485474"|"5581682"|"5715399"|"5757916"|"5778304"|"5832212"|"5842023"|"5887269"|"5892908"|"5905980"|"5933498"|"5982897"|"5996011"|"6044375"|"6055544"|"6078907"|"6094483"|"6148342"|"6154172"|"6192472"|"6370629"|"0073313").PN.	US-PGPUB; USPAT	OR	ON	2006/12/08 10:13

EAST Search History

S10	474	access near control$4 same GPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:20
S11	52	S10 same filter$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:23
S12	543	(726/27).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/12/08 10:25
S13	12	S12 and GPS!	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:25
S14	481	(715/751).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/12/08 10:25
S15	22	S14 and GPS!	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:25
S16	1267	(715/530).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/12/08 10:26
S17	13	S16 and GPS!	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:26
S18	380	(713/166).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/12/08 10:26
S19	7	S18 and GPS!	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:26
S20	3218	(709/229).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/12/08 10:26
S21	100	S20 and GPS!	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/08 10:26

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	03/19/2003	Ron M. Redlich	6851-2-cip-5	6441

4897 7590 01/23/2007

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/390,807	REDLICH ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-146 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-146 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 3/19/03, 8/18/06.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-146 are pending.

Claim Objections

2. Claim 25 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 3. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 28-46 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly

connected, to make and/or use the invention. Claim 28 states that the extract store is a remote memory however claims 26 and 27 (from which claim 28 depends from) state that the extract store is local, the specification does not state anywhere how it is possible for the extract store to be both local and remote.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-146 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. The term "substantially" in claims 1, 47, 48, 84, 85, 109, 124, and 146 is a relative term which renders the claim indefinite. The term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Appropriate changes are required because one of ordinary skill in the art would not know to what degree "substantially current" means.

8. It is noted that many dependent claims also use "substantially" when referring back to the current location data, corresponding changes must be made to these claims as well.

9. Any claims not specifically addressed are rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 85-123 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The above-mentioned claims relate to a computer-readable medium, based on the specification this medium can be non-volatile or volatile memory, or it can be a transitory state medium. The final transitory state medium does not require the medium to be in a physical state therefore the claims are, at best, functional descriptive material and are not statutory.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-15, 20, 21, 25-37, 47-60, 64, 65, 67-77, 84-99, 104, 105, 109-119, 123-137, 142, 143, and 146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fahlman et al. (US 5960080) in view of Hastings et al. (US 6370629), and further in view of O'Flaherty et al. (US 6253203).

As per claims 1, 47, 48, 84, 85, 109, 124, and 146, Fahlman et al. discloses a method of securing data having one or more security sensitive words, data objects, characters or icons, comprising in a computer system with memories designated as a remainder store and an extract store, comprising: permitting extraction of said security sensitive words, characters, data objects, or icons from said data to obtain extracted data and remainder data therefrom and storing the extracted and remainder data; permitting full or partial reconstruction of said data in

the presence of a predetermined security clearance (see column 3 lines 27-26, column 5 lines 27-32 and Figures 2 and 6).

Fahlman et al. fails to disclose the use of a portable computing device; determining when the device is beyond a certain location; providing data when the device is not beyond the location and the remainder store and extract store are stored in separate locations.

However, Hastings et al. teaches the use of a portable computing device; determining when the device is beyond a certain location; providing data when the device is not beyond the location (see column 1 lines 39-57) and O'Flaherty et al. teaches the remainder store and extract store are stored in separate locations (see column 14 lines 26-57).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to secure the data of Fahlman et al. based on location information and to store the extracted data in a separate location.

Motivation to do so would have been to allow different information to be allowed in different locations (see Hastings et al. see column 1 lines 39-57) and to prevent the ability to ascertain the identity of a customer (see O'Flaherty et al column 14 lines 26-57).

As per claims 2, 3, 25, 49, 86, 87, 110, 125, and 126, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses the use of GPS (see Hastings et al. see column 1 lines 39-57 and Abstract).

As per claims 4-6, 26-28, 50-52, 67-69, 88-90, 111-113, and 127-129, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses storing the extracted data in memory (see Fahlman et al. column 6 lines 39-42).

As per claims, 7, 29, 53, 70, 91, and 130, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system fails to explicitly disclose the use of wireless data transmission. However, Official Notice is taken that at the time of the invention it would have been obvious to one of ordinary skill in the art to use wireless data transmission. Motivation to do so would have been to allow for mobile data stores.

As per claims 8, 9, 15, 30, 31, 37, 54, 60, 71, 77, 92, 93, 99, 114, 119, 131, 132 and 137 the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses encrypting and decrypting the extracted data and receiving the extracted data (see Fahlman et al. column 6 lines 53-61 and Figure 6).

As per claims 10, 32, 55, 72, 94, 115, and 133, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction and storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions (see Fahlman et al. column 3 lines 27-26, column 5 lines 27-32 and Figures 2 and 6 and Hastings see column 1 lines 39-57).

As per claims 11, 12, 33, 34, 56, 57, 73, 74, 95, 96, 116, 134, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses obtaining the region information before the determining step (see Hastings see column 1 lines 39-57).

As per claims 13, 14, 35, 36, 58, 59, 75, 76, 97, 98, 117, 118, 135, and 136, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses extracting different types of data (see Fahlman et al. column 3 lines 27-34) but fails to explicitly disclose extracting map information and credit card information. However, Official Notice is taken that at the time of the invention it would have been obvious to one of ordinary skill in the art to extract map and credit card data. Motivation to do so would have been that this information could be useful to adversaries.

As per claims 20, 21, 64, 65, 104, 105, 123, 142, and 143, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system discloses the computers are interconnected and the extracting occurs automatically (see Fahlman Figures 6 and 2).

13. Claims 16-19, 38-43, 61-63, 78-82, 100-103, 120-122, and 138-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system as applied to claims above, and further in view of Kluttz et al. (US 6598161).

As per claims 16-19, 38-41, 61-63, 78-80, 100-103, 120-122, and 138-141 the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system fails disclose encrypting said subsets of extracted data with corresponding degrees of encryption

associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said subsets of extracted data only in the presence of said predetermined security level of said plurality of security levels.

However, Kluttz et al. teaches such an encryption scheme (see column 2 lines 5-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use encryption to provide the different security levels.

Motivation to do so would have been to allow for different levels of access (see Kluttz et al. column 1 lines 62-64).

As per claims 42, 43, 81, and 82 the modified Fahlman et al., Hastings et al., O'Flaherty et al., and Kluttz et al. system discloses the computers are interconnected and the extracting occurs automatically (see Fahlman Figures 6 and 2).

14. Claims 22, 44, 66, 83, and 106 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system (alone or in combination with Kluttz et al.) as applied to claims above, and further in view of Shmueli et al. (US 6044357).

As per claims 22, 44, 66, 83, and 106, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system (alone or

in combination with Kluttz et al.) fails to disclose the explicit use of one of an inference engine, neural network and artificial intelligence process.

However, Shmueli et al. teaches the use of a neural network (see column 4 lines 15-28).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use a neural network in the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system (alone or in combination with Kluttz et al.).

Motivation to do so would have been automatically extract data from a document (see Shmueli et al. column 2 lines 49-63).

15. Claims 23, 24, 45, 46, 107, 108, 144, and 145 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system (alone or in combination with Kluttz et al. and Shmueli et al) as applied to claims above, and further in view of Gurley (US 5036315).

As per claims 23, 45, 107, and 144, the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system (alone or in combination with Kluttz et al. and Shmueli et al.) fails to disclose one of said computers includes a display fed from a video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to

be coupled to said video memory, said compiler having means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

However, Gurley teaches such a display method (see Gurley abstract and Figure 1 number 100).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the display of Gurley in the modified Fahlman et al., Hastings et al., and O'Flaherty et al. system (alone or in combination with Kluttz et al. and Shmueli et al.).

Motivation to do so would have been to display overlapped information (see Gurley abstract).

As per claims 24, 46, 108, and 145, the modified Fahlman et al., Hastings et al., O'Flaherty et al., and Gurley system (alone or in combination with Kluttz et al. and Shmueli et al.) discloses computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another said at least two displays (see Gurley abstract and Figure 1 number 100).

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 48, 63, 78, 90, 153, 224, of Patent No. 7103915. Although the conflicting claims are not identical, they are not patentably distinct from each other because they perform the same filtering and extracting steps and actions.

3. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 29, 47, 72, 73 of Patent No. 7140044. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps and actions.

4. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 23, 46, of Patent No. 7146644. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps and actions.

5. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 12, 20, 26, 31, 36, 41, 51, 58, 64, 69, 73, 82 of copending Application No. 10155525. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

6. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 7, 16, 22 of copending Application No. 10155192. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

7. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 15, 27, 41, 53, and 67 of copending Application No. 10277196. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

8. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 15, 25, 26, 27, 41, 51, 52, 67, 77, 78 of copending Application No. 10998365. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

9. Claims 1, 47, 48, 84, 85, 109, 124, and 146 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 5, 7, 9, of copending Application No. 10998366. Although the conflicting claims are not identical, they are not patentably distinct from each other because they each perform the same filtering and extracting steps and actions.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

10. Due to the vast number of applications that qualify as a provisional double patenting rejection only the independent claims of the present application have been rejected.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Schneier et al. and Bednarek et al. (WO 9953624) disclose controlling access based on a GPS signal.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

J1032 U.S. PTO
10/390807
03/19/03

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number 10/390807
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mpp	6,192,472 B1	2/20/2001	Garay et al.	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al.	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al.	707	1	
	5,832,212	11/3/1998	Cragun et al.	395	188.01	
mpp	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
mpp	WO 00/75779 A2		WIPO			

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mpp	Ingram i100, Content Security Appliance (2 pages)
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)
	ZD Net Interactive iWeek - IBS, SAP: XML to Boost Security Integration (1 page)
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999
mpp	Cisco Systems' Intrusion Detection System (IDS) Host Sensor 2.0 product data sheet and technical overview, 10 pgs., July 3, 2000, www.cisco.com

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number 10/390 807
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mp	5,892,908	4/6/1999	Hughes et al.	395	200.8	
	5,423,032	6/6/1995	Byrd et al.	395	600	
	6,044,375	3/28/2000	Shmueli et al.	707	101	
	5,715,399	2/3/1998	Bezos	395	227	
	5,982,897	11/9/99	Clark	380	21	
	6,370,629B1	4/9/02	Hastings et al.	711	163	
mp	6,154,172	11/28/00	Piccionelli et al.	342	357.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mp	"Protecting Privacy using the Decentralized Label Model" A. Myers, Cornell Univ. 1/1/2000	
	Mimesweeper Product Data sheet, Resoft Int'l LLC., Nov. 12, 2001 re-soft.com/product/mimeswep.	
	Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July 2000.	
	Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys., Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.	
	Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001.	
mp	Intelligence Community System for Information Sharing (ICSIS) Relationship to the Global Information Grid (GIG), White Paper, 27 March 2001	

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number 10/390807
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mmp	5,887,269	3/23/99	Brunts et al.	701	208	
	5,842,023	11/24/98	Tsumura	395	712	
	5,778,304	7/7/98	Grube et al.	455	33.1	
	5,757,916	5/26/98	MacDoran et al.	380	25	
	5,933,498	8/3/99	Schneck et al	380	4	
	6,078,907	6/20/00	Lamm	705	40	
	5,581,682	12/3/96	Anderson et al.	395	792	
mmp	0073313 A1	6/13/02	Brown et al.	713	165	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mp	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
mp	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mp	MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
mp	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
MM	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
MM	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

MM	Ingrian i100, Content Security Appliance (1 pages)
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigrigg, John D. Strunk, Gregory R. Ganger, Han Kiloccote Pradeep K. Khosla (8 pages)
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)
MM	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999

EXAMINER _____ DATE CONSIDERED 12/7/06

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mgp	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
mgp	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mgp	The 1996 book, Applied Cryptography, by Schneier	
	The Uniform Resource Locator article "FOLD OC"	
mgp	Microsoft Word "Learning Microsoft Word 7.0"	

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
	6,662,189	12/9/03	Oyanagi	707	102	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER _____ DATE CONSIDERED 12/7/06

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip5-Form-PTO-1449.wpd

Notice of References Cited	Application/Control No. 10/390,807	Applicant(s)/Patent Under Reexamination REDLICH ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,871,398 A	02-1999	Schneier et al.	463/16
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
*	N	WO 9953624 A1	10-1999	World Intellect	BEDNAREK et al.	
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								
	60	✓								
	61	✓								
	62	✓								
	63	✓								
	64	✓								
	65	✓								
	66	✓								
	67	✓								
	68	✓								
	69	✓								
	70	✓								
	71	✓								
	72	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007								
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								
	91	✓								
	92	✓								
	93	✓								
	94	✓								
	95	✓								
	96	✓								
	97	✓								
	98	✓								
	99	✓								
	100	✓								
	101	✓								
	102	✓								
	103	✓								
	104	✓								
	105	✓								
	106	✓								
	107	✓								
	108	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007								
	109	✓								
	110	✓								
	111	✓								
	112	✓								
	113	✓								
	114	✓								
	115	✓								
	116	✓								
	117	✓								
	118	✓								
	119	✓								
	120	✓								
	121	✓								
	122	✓								
	123	✓								
	124	✓								
	125	✓								
	126	✓								
	127	✓								
	128	✓								
	129	✓								
	130	✓								
	131	✓								
	132	✓								
	133	✓								
	134	✓								
	135	✓								
	136	✓								
	137	✓								
	138	✓								
	139	✓								
	140	✓								
	141	✓								
	142	✓								
	143	✓								
	144	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007								
	145	✓								
	146	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

SEARCHED

Class	Subclass	Date	Examiner
726	27	12/8/06	MJP
715	751, 530	12/8/06	MJP
713	166	12/8/06	MJP
709	229	12/8/06	MJP

SEARCH NOTES

Search Notes	Date	Examiner
BRS search USPAT, USPGPUB, EPO, JPO, IBM, DERWENT see attached search history	12/8/06	MJP
all claims have been reviewed for 35 USC non-statutroy subject matter	12/8/06	MJP

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

AMENDMENT

Commissioner for Patents
Alexandria, VA 22313-1450

This Amendment responds to the Office Action dated March 19, 2007. A Request for a One Month Extension of Time is concurrently filed herewith. If the $60.00 fee charged to Deposit Account no. 03-1231 is inadequate, please debit or credit Deposit Account no. 03-1231. Applicant adds new claims 147 - 172 to this application but cancels three (3) claims. Please charge Deposit Account no. 03-1231 for the $675.00 fee (one independent claim and a total of 23 newly added claims). Applicant submits a Terminal Disclaimer herewith. Please charge the $65.00 fee to Deposit Account no. 03-1231. If any fee is inadequate, please debit or credit Deposit Account no. 03-1231. The total fee to be charged is $800.00. This filing includes:

(a) Amendment Cover page - transmittal (1 pg., p. 1)

(b) Specification (8 pgs., pp. 2 - 9)

(c) Claims (34 pgs., pp. 10 - 43)

(d) Remarks (19 pgs., pp. 44 - 62)(includes Appendix Showing Support)

(e) Request for a One Month Extension of Time (1 pg.)

(f) Replacement Formal Drawings (21 pgs.)

(g) Terminal Disclaimer (3 pgs.)

CLAIMS

1. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

2. (currently amended) A method for securing data as claimed in claim 1 wherein said ~~substantially~~ current location data is generated with the acquisition of a global positioning signal.

3. (currently amended) A method for securing data as claimed in claim 1 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

4. (currently amended) A method for securing data as claimed in claim 1 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

5. (currently amended) A method for securing data as claimed in claim 4 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

6. (currently amended) A method for securing data as claimed in claim 1 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

7. (original) A method for securing data as claimed in claim 6 wherein said transmitting occurs as a wireless data transmission.

8. (currently amended) A method for securing data as claimed in claim 7 including encrypting said corresponding extracted data prior to transmitting.

9. (currently amended) A method for securing data as claimed in claim 6 including receiving said corresponding extracted data as necessary during reconstruction.

10. (currently amended) A method for securing data as claimed in claim 1 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon

respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

11. (original) A method for securing data as claimed in claim 1 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

12. (original) A method for securing data as claimed in claim 11 wherein the step of obtaining occurs before the step of determining.

13. (original) A method for securing data as claimed in claim 1 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

14. (original) A method for securing data as claimed in claim 1 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

15. (original) A method for securing data as claimed in claim 1 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

16. (currently amended) A method of securing data as claimed in claim 1 wherein ~~said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are~~

~~utilized only in the presence of a respective predetermined security level of said plurality of security levels~~ said predetermined region is one a plurality of regions which includes at least one security protocol extraction region and at least one security protocol reconstruction region, the step of determining determines when said portable computing device is beyond at least one security protocol extraction region and applies the respective protocol to said data, and the step of determining further determines when said portable computing device is beyond at least one security protocol reconstruction region and applies the respective protocol to full or partial reconstruction of said data.

17. (currently amended) A method of securing data as claimed in claim 16 wherein said predetermined security clearance is one of a plurality of security clearances, said plurality of security levels is associated with corresponding degrees of encryption, ~~as are said subsets of extracted data,~~ the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

18. (currently amended) A method of securing data as claimed in claim 17 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

19. (currently amended) A method as claimed in claim 16 wherein said predetermined security clearance is one of a plurality of security clearances, the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

20. (original) A method of securing data as claimed in claim 1 operating over a plurality of computers interconnected together.

21. (original) A method for securing data as claimed in claim 1 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

22. (original) A method of securing data as claimed in claim 1 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

23. (original) A method as claimed in claim 1 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

24. (original) A method as claimed in claim 1 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

25. (currently amended) A method for securing data as claimed in ~~claim 1~~ claim 2 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

26. (currently amended) A method for securing data as claimed in claim 25 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

27. (currently amended) A method for securing data as claimed in claim 26 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

28. (currently amended) A method for securing data as claimed in ~~claim 27~~ claim 3 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

29. (original) A method for securing data as claimed in claim 28 wherein said transmitting occurs as a wireless data transmission.

30. (currently amended) A method for securing data as claimed in claim 29 including encrypting said corresponding extracted data prior to transmitting.

31. (currently amended) A method for securing data as claimed in claim 30 including receiving said corresponding extracted data as necessary during reconstruction.

32. (currently amended) A method for securing data as claimed in ~~claim 31~~ claim 3 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

33. (original) A method for securing data as claimed in claim 31 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

34. (original) A method for securing data as claimed in claim 33 wherein the step of obtaining occurs before the step of determining.

35. (original) A method for securing data as claimed in claim 34 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

36. (original) A method for securing data as claimed in claim 34 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

37. (original) A method for securing data as claimed in claim 36 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

38. (cancelled without prejudice to reinstate the same at a later time, i.e., without disclaimer)

39. (currently amended) A method of securing data as claimed in ~~claim 38~~ claim 37 wherein said predetermined security clearance is one of a plurality of security clearances, said plurality of security levels is associated with corresponding degrees of encryption, ~~as are said subsets of extracted data,~~ the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting,

during the reconstruction, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

40. (currently amended) A method of securing data as claimed in claim 39 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

41. (currently amended) A method as claimed in claim 40 wherein said predetermined security clearance is one of a plurality of security clearances, the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

42. (original) A method of securing data as claimed in claim 41 operating over a plurality of computers interconnected together.

43. (original) A method for securing data as claimed in claim 42 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

44. (original) A method of securing data as claimed in claim 43 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

45. (original) A method as claimed in claim 44 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

46. (original) A method as claimed in claim 44 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid

displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

47. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

when said portable computing device is not beyond said predetermined region, permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data in the presence of a predetermined security clearance access control corresponding to said respective security level .

48. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with

security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, extracting said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store~~ in respective extract stores corresponding to a respective security level of said extract stores.

49. (currently amended) A method for securing data as claimed in claim 48 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

50. (currently amended) A method for securing data as claimed in claim 48 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

51. (currently amended) A method for securing data as claimed in claim 50 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

52. (currently amended) A method for securing data as claimed in claim 48 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

53. (original) A method for securing data as claimed in claim 52 wherein said transmitting occurs as a wireless data transmission.

54. (currently amended) A method for securing data as claimed in claim 53 including encrypting said corresponding extracted data prior to transmitting.

55. (currently amended) A method for securing data as claimed in claim 48 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction occurs or said ~~and~~ storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

56. (original) A method for securing data as claimed in claim 48 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

57. (original) A method for securing data as claimed in claim 56 wherein the step of obtaining occurs before the step of determining.

58. (original) A method for securing data as claimed in claim 48 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

59. (original) A method for securing data as claimed in claim 48 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

60. (currently amended) A method for securing data as claimed in claim 48 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary. ~~during reconstruction~~.

61. (cancelled without prejudice to reinstate the same at a later time, i.e., without disclaimer)

62. (currently amended) A method of securing data as claimed in ~~claim 61~~ claim 48 wherein said respective security level is one of a ~~said~~ plurality of security levels ~~is~~ associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels.

63. (currently amended) A method of securing data as claimed in claim 62 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

64. (original) A method of securing data as claimed in claim 48 operating over a plurality of computers interconnected together.

65. (original) A method for securing data as claimed in claim 48 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

66. (original) A method of securing data as claimed in claim 48 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

67. (currently amended) A method for securing data as claimed in claim 49 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

68. (currently amended) A method for securing data as claimed in claim 67 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

69. (currently amended) A method for securing data as claimed in claim 49 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

70. (original) A method for securing data as claimed in claim 69 wherein said transmitting occurs as a wireless data transmission.

71. (currently amended) A method for securing data as claimed in claim 70 including encrypting said corresponding extracted data prior to transmitting.

72. (currently amended) A method for securing data as claimed in claim 71 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

73. (original) A method for securing data as claimed in claim 72 wherein said plurality of predetermined regions is a plurality of mobile predetermined region and the method includes obtaining data representing said plurality of mobile predetermined region.

74. (original) A method for securing data as claimed in claim 73 wherein the step of obtaining occurs before the step of determining.

75. (original) A method for securing data as claimed in claim 74 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

76. (original) A method for securing data as claimed in claim 74 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

77. (original) A method for securing data as claimed in claim 74 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

78. (cancelled without prejudice to reinstate the same at a later time, i.e., without disclaimer)

79. (currently amended) A method of securing data as claimed in ~~claim 78~~ claim 74 wherein said respective security level is one of a ~~said~~ plurality of security levels ~~is~~ associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels.

80. (currently amended) A method of securing data as claimed in claim 79 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

81. (original) A method of securing data as claimed in claim 80 operating over a plurality of computers interconnected together.

82. (original) A method for securing data as claimed in claim 81 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

83. (original) A method of securing data as claimed in claim 82 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

84. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores , ~~said extract store and said remainder store, respectively,~~ said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is within a predetermined region based upon said current location data;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

85. (currently amended) A computer readable medium ~~containing~~ encoded with programming instructions for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective

~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, the programming instructions comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

86. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein said ~~substantially~~ current location data is generated with the acquisition of a global positioning signal.

87. (currently amended) A computer readable medium with programming steps as claimed in claim 85 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

88. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

89. (currently amended) A computer readable medium with programming steps as claimed in claim 88 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a flash memory drive, a tape drive and a read-write CD-ROM drive.

90. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

91. (original) A computer readable medium with programming steps as claimed in claim 90 wherein said transmitting occurs as a wireless data transmission.

92. (currently amended) A computer readable medium with programming steps as claimed in claim 91 including encrypting said corresponding extracted data prior to transmitting.

93. (currently amended) A computer readable medium with programming steps as claimed in claim 90 including receiving said corresponding extracted data as necessary during reconstruction.

94. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction

is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

95. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

96. (original) A computer readable medium with programming steps as claimed in claim 95 wherein the step of obtaining occurs before the step of determining.

97. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

98. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

99. (original) A computer readable medium with programming steps as claimed in claim 85 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

100. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein said respective security level is ~~predetermined security level is~~ one of a plurality of security levels operative during recoonstruction.~~, said extracting extracts said security sensitive~~

~~words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels~~ .

101. (currently amended) A computer readable medium with programming steps as claimed in claim 100 wherein said plurality of security levels is associated with corresponding degrees of encryption ~~as are said subsets of~~ for said extracted data, the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

102. (currently amended) A computer readable medium with programming steps as claimed in claim 101 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

103. (original) A computer readable medium with programming steps as claimed in claim 100 wherein the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

104. (original) A computer readable medium with programming steps as claimed in claim 85 configured to operate over a plurality of computers interconnected together.

105. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

106. (original) A computer readable medium with programming steps as claimed in claim 85 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

107. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

108. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

109. (currently amended) A computer readable medium encoded with programming steps for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, the programming steps comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, extracting said security sensitive words, characters, data objects or icons from said data to obtain extracted data and

remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store~~ in respective extract stores corresponding to a respective security level of said extract stores .

110. (currently amended) A computer readable medium with programming steps as claimed in claim 109 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

111. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

112. (currently amended) A computer readable medium with programming steps as claimed in claim 111 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

113. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

114. (original) A computer readable medium with programming steps as claimed in claim 113 including encrypting said extracted data prior to transmitting.

115. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

116. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

117. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

118. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

119. (currently amended) A computer readable medium with programming steps as claimed in claim 109 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary. ~~during reconstruction.~~

120. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein ~~said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with a plurality of security levels~~ said respective security level is one of a plurality of security levels associated with said respective extract stores.

121. (currently amended) A computer readable medium with programming steps as claimed in claim 120 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the method including encrypting said ~~subsets of~~

extracted data with corresponding degrees of encryption associated with said plurality of security levels.

122. (currently amended) A computer readable medium with programming steps as claimed in claim 121 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

123. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

124. (currently amended) An information processing system for securing data having one or more security sensitive words, characters, data objects or icons in a computer system a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

means for determining when said portable computing device is beyond a predetermined region based upon said current location data;

means for extracting, coupled to said means for determining, said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

means for permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance

access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

125. (currently amended) An information processing system as claimed in claim 124 including a global positioning signal generator, said ~~substantially~~ current location data being generated by said global positioning signal generator and applied to said means for determining.

126. (currently amended) An information processing system as claimed in claim 124 including means for acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

127. (currently amended) An information processing system as claimed in claim 124 wherein said portable computing device includes a local data drive and local drive media as one of said respective extract stores, said means for extracting storing said security sensitive words, characters, data objects or icons on said media in said local data drive.

128. (currently amended) An information processing system as claimed in claim 127 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a flash memory drive, a tape drive and a read-write CD-ROM drive.

129. (currently amended) An information processing system as claimed in claim 124 including a remote memory as one of said plurality of extract stores in said computer system, said portable computing device including a data transmitter, said means for extracting storing said security sensitive words, characters, data objects or icons in said remote memory via said data transmitter.

130. (original) An information processing system as claimed in claim 129 wherein said data transmitter transmits data via a wireless communications channel.

131. (currently amended) An information processing system as claimed in claim 130 including means for encrypting ~~said~~ corresponding extracted data prior to transmitting.

132. (currently amended) An information processing system as claimed in claim 129 including means for receiving said corresponding extracted data as necessary during reconstruction.

133. (original) An information processing system as claimed in claim 124 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the means for determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said means for extracting and storing being triggered based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said means for reconstructing being activated based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

134. (original) An information processing system as claimed in claim 124 wherein said predetermined region is a mobile predetermined region and the system includes means for obtaining data representing said mobile predetermined region.

135. (original) An information processing system as claimed in claim 124 wherein said data is a map with security sensitive icons associated therewith, said means for extracting acting upon said map and extracting said security sensitive icons from said map when said portable computing device is beyond said predetermined region.

136. (original) An information processing system as claimed in claim 124 wherein said data is a document file with security sensitive credit card data characters associated therewith, said means for extracting acting upon said security sensitive credit card data characters and extracting the same from said document file when said portable computing device is beyond said predetermined region.

137. (currently amended) An information processing system as claimed in claim 124 including means for encrypting ~~said~~ corresponding extracted data before or during said storage and means for decrypting said corresponding extracted data as necessary during reconstruction by said means for reconstructing.

138. (currently amended) An information processing system as claimed in claim 124 wherein said predetermined security level is one of a plurality of security levels, each associated with a corresponding extract store, ~~said means for extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels,~~ and said means for reconstructing acts upon some or all of said ~~subsets of~~ extracted data only in the presence of a respective predetermined security level of said plurality of security levels.

139. (currently amended) An information processing system as claimed in claim 138 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the system including means for encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including means for decrypting, during reconstruction with said means for reconstructing, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

140. (currently amended) An information processing system as claimed in claim 139 including means for encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

141. (original) An information processing system as claimed in claim 138 wherein said means for reconstructing permits a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

142. (original) An information processing system as claimed in claim 124 utilizing a plurality of computers interconnected together.

143. (original) An information processing system as claimed in claim 124 including an automatic means for determining and means for extracting and storing actuated upon power up or geographic location of said at least one portable computing device.

144. (original) An information processing system as claimed in claim 124 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the means for reconstructing interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

145. (original) An information processing system as claimed in claim 124 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the means for reconstructing including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

146. (currently amended) An information processing system for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~

extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

means for determining when said portable computing device is beyond a predetermined region based upon said current location data and generating a trigger;

means for extracting, upon said trigger ~~when said portable computing device is beyond said predetermined region~~, said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store~~ in respective extract stores corresponding to a respective security level of said extract stores.

147. (new) A computerized method of securing data in a plurality of security controlled data stores with access controls thereat, said data potentially having sensitive content such as sensitive words, data objects, characters, images, data elements or icons, comprising:

storing separately sensitive content in secure data stores of said plurality of security data stores;

permitting reconstruction of some or all of said data with appropriate access controls applied to respective secure data stores; and

said storing or reconstruction based upon territorial protocol and a geographic location signal or a triggering event.

148. (new) A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering or extracting said sensitive content in said secure data stores.

149. (new) A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of removing or copying said sensitive content in said secure data stores.

150. (new) A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering and transferring or extracting and transferring said sensitive content in said secure data stores.

151. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or both of partially or completely storing said sensitive content in said secure data stores.

152. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes partially or completely storing said sensitive content in said secure data stores with at least one of encryption or parsing of data.

153. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores.

154. (new) A computerized method of securing data as claimed in claim 147 including manually or automatically at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores.

155. (new) A computerized method of securing data as claimed in claim 147 including at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; and wherein

said sensitive content has different levels of sensitive content therein corresponding to respective ones of said secure data stores.

156. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is defined as at least one of security sensitive content, content of significance, trade secret content, personal identifying information, content subject to regulatory provisions, or back-up content and said respective ones of said secure data stores are correspondingly designated as at least one of security sensitive stores, stores for content of significance, trade secret stores, personal identifying information stores, regulatory provision stores, or back-up stores.

157. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes at least one or more of storing in predetermined security data stores, storing in a predetermined manner by random selection of security data stores, storing by data class in said security data stores, storing data by data type in said security data stores, or storing by level of security in said security data stores.

158. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in said security data stores in a predetermined manner with an algorithmic selection.

159. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in optical media data stores.

160. (new) A computerized method of securing data as claimed in claim 147 wherein storing of said sensitive content is done separately with respect to at least one of remainder data, left-over data,

non-sensitive content data, surplus data, residue data, remnant data, or data complementary to sensitive content data.

161. (new) A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution, regeneration, compilation, reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores.

162. (new) A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes the use of at least one of predetermined access controls, assigned access controls, access controls generated with said storing of said secure data, or access controls and encryption.

163. (new) A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution, regeneration, compilation, reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores.

164. (new) A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to respective secure data stores in at least one of the following manners:

said access controls applied sequentially to respective secure data stores;

said access controls applied concurrently to respective secure data stores;

said access controls applied to respective secure data stores subsequent to application of a security protocol;

said secure data stores are mapped and said access controls are applied to obtain the mapped secure data stores; or

said access controls are applied subsequent to an exchange of compensation or an exchange of data.

said access controls applied to respective secure data stores subsequent to application of a hierarchical security protocol.

165. (new) A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to at least one or more of predetermined respective secure data stores, associated respective secure data stores, correlated respective secure data stores, or designated respective secure data stores.

166. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores.

167. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores.

168. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores.

169. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and

said server controlling the application of said access controls.

170. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

select sensitive words, data objects, characters, images, data elements or icons;

defined sensitive words, data objects, characters, images, data elements or icons;

known sensitive words, data objects, characters, images, data elements or icons;

certain sensitive words, data objects, characters, images, data elements or icons;

a collection of sensitive words, data objects, characters, images, data elements or icons;

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons; or

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons having different hierarchal or orthogonal levels of sensitive content.

171. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

portions of predetermined sensitive words, data objects, characters, images, data elements or icon

s; or

words, data objects, characters, images, data elements or icons which are not from a plurality of predetermined words, data objects, characters, images, data elements or icons.

172. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is related to sensitive words, data objects, characters, images, data elements or icons, by at least or more of a function or a meaning.

REMARKS

This Amendment responds to the Office Action dated March 19, 2007.

Applicant has amended the patent specification to correct spelling errors and to clarify certain items. Support for changes in substance are found in the specification at the following locations: in ¶ 003, see ¶ 104 (also subject to amendment herein); in ¶ 104, see reference to "data object" in that same ¶; in ¶ 154, see that same ¶; and, in ¶ 247, see that same ¶. No new matter is introduced into the application by these changes to the specification.

With respect to ¶ 001, Applicant requests that the priority of this application be changed as noted in ¶ 001. A Supplemental Declaration will be filed in the future to conform to the changes in priority.

Replacement formal drawings are submitted herewith. In FIG. 3, the numerals 226 and 228 have been reversed to conform to the specification.

Applicant has added new claims 148 - 172. Support for these claims is set forth in the attached Appendix. No new matter is added to this case by the addition of these claims. Support for the substantive changes to claims 1 - 147 are also shown in the Appendix.

In the Office Action, the examiner stated that claims 25 and 3 are similar. Applicant has amended claim 25 to depend from claim 2 which changes the scope of the claim.

In the Office Action, the examiner indicated that claims 26 and 28 conflict relative to local storage. Claim 28 is amended and is now dependent upon claim 3 which does not refer to local data storage.

In the Office Action, the examiner objected to the word "substantially" in the claims. The claims have been amended to delete this word.

In the Office Action, the examiner indicated that claims 85 - 123 were not statutory subject matter. Independent claim 85 has been amended as follows:

> 85. (currently amended) A computer readable medium ~~containing~~ encoded with programming instructions for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, the programming instructions comprising:
> determining when said portable computing device is beyond a predetermined region based upon said current location data; ...

The PTO Guidelines regarding statutory subject matter indicate that:

> Functional descriptive material claimed in combination with an appropriate computer readable medium to enable the functionality to be realized is patent eligible subject matter if it is capable of producing a useful, concrete and tangible result when used in the computer system. Compare Warmerdam to In re Lowry 32 USPQ2d 1031 where a memory with a data structure that increased computing efficiency was patentable. The computer readable medium must be physical structure which provides the functional descriptive material in usable form to permit the functionality to be realized with the computer. A program product which does not explicitly include such a medium, a program per se, a signal or other type of transmission media that fails to include the hardware necessary to realize the functionality (e.g., a transmitter or a receiver), and a piece of paper with the functional descriptive material written on it are all examples of media which are not believed to enable the functionality to be realized with the computer.

PTO Overview of Interim Guidelines for Subject Matter Eligibility Guidelines (herein "PTO Overview"), pg. 10.

Therefore, the recitation in amended claims 85 and 109 that the computer readable medium is encoded with programming instructions overcomes the Section 101 rejection. Independent claim 109 has been amended to read "A computer readable medium encoded with programming steps for securing data" to overcome this rejection.

In the Office Action on pages 5-12, the patent examiner rejected claims 1-146 as being non-patentable under Section 103 in view of certain prior or pre-existing technology or art disclosed in the following references:

U.S. Patent No. 5,960,080 to Fahlman et al. ("Fahlman '080")
U.S. Patent No. 6,370,629 to Hastings et al. ("Hastings '629")
U.S. Patent No. 6,253,203 to O'Flaherty et al. ("O'Flaherty '203")
U.S. Patent No. 6,598,161 to Kluttz et al. ("Kluttz '161")
U.S. Patent No. 6,044,357 to Shmueli et al. ("Shumueli '357")
U.S. Patent No. 5,036,315 to Gurley ("Gurley '315")

SUMMARY

In summary, none of the references show, teach or suggest "a plurality of security controlled memories as respective extract stores with security access controls thereat, ... [and] storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores;" per claims 1, 47, 48, 84, 85, 109, 124, and 147, and, in claims 1, 47, 84, 85 and 124, "permitting full or partial reconstruction ... only in the presence of a predetermined security clearance access control corresponding to said respective security level .. when said portable computing device is not beyond said predetermined region." New claim 147 also includes the concept of multiple secure access extract stores (see "plurality of security controlled data stores with access controls thereat"), and the steps of [i] "storing separately sensitive content in secure data stores of said plurality of security data stores; [ii] permitting reconstruction of some or all of said data with appropriate access controls applied to respective secure data stores; and [iii] said storing or reconstruction based upon territorial protocol and a geographic location signal or a triggering event." The claimed concept of multiple extract stores, with multiple security access controls,

triggered to store critical data in respective secure access control extract stores is unique and patentable.

In summary, Fahlman '080 does not show, teach or suggest multiple extractions of security sensitive content to respective security level extract stores (multiple extract stores and respective security levels), and the requirement that the user apply a password or other security measure ("security clearance access control") before full or partial reconstruction of the data. Fahlman '080 does not disclose nor discuss multiple security level storage and retrieval.

Fahlman '080

Fahlman '080 does not show, teach or suggest multiple security levels, multiple extraction of security data, storage at multiple levels, and presentment of security clearance codes for said respective security level. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

In Fig. 1, step 111 of Fahlman "automatically" merges sensitive information into non-sensitive information. In FIG. 2, step 217, the Fahlman system again "automatically" merges secured data with un-secured data. Fahlman discusses merging secured data with unsecured data at col. 2, line 22, col. 2, line 34, and col. 2, line 49, and col. 2, line 54 and col. 2, line 40. Fahlman '080 discloses identifying security information and extracting that information and replacing it with placeholders. Col. 2, line 37 and col. 3, line 47. "The sanitized message is then transmitted with a low level of security." Col. 3, line 54. The sensitive information is stripped from the original message and stored in a separate location or together with the sanitized message. Col. 3, line 64. A map showing the location of the security information is also stored with the secured information.

Col. 3, line 63. "Then, in step 111, the sensitive terms received from the second path are merged with the sanitized message to create a final confidential message." Col. 4, line 1. The examiner should note that Fahlman does not discuss reconstruction or merger in the presence of any type of security clearance. In contrast, the present invention requires "permitting full or partial reconstruction ... only in the presence of a predetermined security clearance access control corresponding to said respective security level .. when said portable computing device is not beyond said predetermined region." See claims 1, 47, 84, 85 and 124.

Fahlman also states: "Then, in step 217, the sensitive terms are automatically merged back into the serviced message to create a final message." Col. 5, line 27. No discussion of multi-level security clearance is noted in Fahlman. The same is true regarding merger of security information and non-secured information at col. 6, line 62. Fahlman does not require presentment of the proper, respective security clearance prior to the merging of secret and non-secret data.

Fahlman does not separately store different levels of secret, extract data. Fahlman (1) identifies secret words, (2) replaces the words with placeholders, then (3) transmits the "sanitized message." Fig. 1, step 107, Fig. 2, step 209, col 2, line 19, col. 2, line 34, col. 2, line 49, col. 3, line 54 (transmission - no storage of non-secure data), col. 4, line 64 (transmission - no separate storage).

Fahlman does not discuss multiple security levels nor multiple storage sites at each security level. Since multiple security levels are not addressed in Fahlman, multiple security clearance access controls to obtain "access" to multiple levels of secured data is not discussed. Since Fahlman does not use any type of password or security clearance procedures, there is no reconstruction available.

Fahlman extracts only a single level of data and transfers it separately from the non-secure data (data is transmitted by Fahlman, not stored "in a remainder store") but never discusses password control to access either type of data. It is respectfully submitted that it is improper to select disparate parts from the complicated system of Fahlman '080 and "cobble together" the claimed invention. There is no suggestion nor motivation to do so absent the disclosure of the present invention.

Each of the references, Fahlman '080, Hastings '629, O'Flaherty '203, Kluttz '161, Shmueli '357, and Gurley '315 describe complete systems and there is no reason to add to or substitute portions of one disclosure with another. There is no evidence that a person of skill in the art would take certain aspects of one reference and add those features to another reference.

Hastings '629

Hastings '629 does not show multiple levels of extraction to enable "storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores" per claims per claims 1, 47, 48, 84, 85, 109, 124, and 147. Hastings '629 states:

> Once the packet from the crypto-board 80 is authorized based on the signature and the initialization vector, the decoder 32 compares the time and position data received from the crypto-board 80 with the policy 155 which applies 50 to the files 144 or to a subset of files 144 (step 460). **If the user is authorized to access the files** 144, then the data is unlocked (step 470), decrypted with decryption keys 52 (step 480) and supplied to the user's application program 34 and displayed (step 490).

Hastings '629, col. 6, line 45 (herein "6/45")(emphasis added).

Hastings '629 does not deal with the storage of information – only the retrieval of information.

> In general, in one aspect of the invention, the invention features controlling access to stored information by determining an actual geographic position where the stored information is located based on signals received at a receiver supplying reliable position information.

Hastings '629, 1/29

Although Hastings '629 discusses storing or downloading data with geographic access controls and password controls, it does not discuss nor explain extraction of data to "security controlled memories as respective extract stores" which extraction and further processing is limited by geographic triggers per the invention.

O'Flaherty '203

O'Flaherty '203 does not show extraction of security sensitive content into various extract stores having respective security levels and access controls. O'Flaherty '203 does not show full or partial reconstruction with a geographic trigger and access control for the respective secure extract store. O'Flaherty '203 states:

> In an alternate embodiment, the security and privacy protection features of the extended database 106 and data view suite 108 are further enhanced with the use of data encryption. This may be performed by encrypting the data in a given row with an encryption code, or by providing each data field with a unique encryption number. Alternatively, the data may be encrypted at different hierarchical levels of security so as to enforce the privacy preferences of the consumer.

O'Flaherty '203, 10/40.

> In another embodiment, the separate trusted database 704 and anonymized database 708 are used in a multi level security privacy system, where the encryption, macros, data views, and/ or separate database techniques disclosed herein combined to meet the privacy requirements of different jurisdictions, for different retail outlets, or to accommodate different individual preferences.

O'Flaherty '203, 14/58

The citation at col 14, lines 25 - 57 by the patent examiner does not discuss multiple security levels. In fact, that portion of O'Flaherty '203 discusses anonymized database 708, containing pseudonyms and data 706, being different than trusted database 702, containing pseudonyms and genuine customer ids (identification data). There is no discussion in O'Flaherty '203 of (a) multiple extraction per security level nor (b) multiple, dispersed storage of security

data, per security level, nor (c) reconstruction using multiple security clearances or access controls for multiple secure extract stores.

Therefore, O'Flaherty '203 discusses the use of different encryption in a single database for "different hierarchical levels of security"(O'Flaherty '203, 10/40), but does not discuss different extract stores, one for each security level, PLUS extraction PLUS dispersal nor does O'Flaherty '203 discuss full or partial reconstruction. The general reference in O'Flaherty '203 to a "multi level security privacy system, where the encryption, macros, data views, and/ or separate database techniques" is not sufficiently clear to show singular extraction, per security level, storage per security level nor full or partial reconstruction per security level/security clearance.

The referenced "separate database techniques" (see quote, O'Flaherty '203, 14/58 above) does not clearly describe multiple extraction, separate extract stores, nor certain reconstruction techniques as per the presently claimed system. O'Flaherty '203 does describe different encryption in a single database for multiple levels of security (O'Flaherty '203, 10/40) but this is not the same as extraction per security level, storage per security level and full or partial reconstruction per security level/security clearance. O'Flaherty '203 describes a single storage facility with multiple security levels (by encryption) therein. O'Flaherty '203, 10/40.

The present invention claims "a plurality of security controlled memories as respective extract stores with security access controls thereat, ... [and] storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores;" per claims 1, 47, 48, 84, 85, 109, 124, and 147, and, in claims 1, 47, 84, 85 and 124, "permitting full or partial reconstruction ... only in the presence of a predetermined security clearance access

control corresponding to said respective security level .. when said portable computing device is not beyond said predetermined region." New claim 147 also includes the concept of multiple secure access extract stores and the steps of (i) storing separately sensitive content in secure data stores of said plurality of security data stores; (ii) permitting reconstruction with appropriate access controls applied to respective secure data stores; wherein (iii) storing or reconstruction is based upon territorial protocol or a triggering event.

Kluttz '161 does not show, teach or suggest multi-level extract stores nor permitting reconstruction of said data via said extract data stores only in the presence of predetermined security clearances. Kluttz '161 shows utilizing multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

U.S. Patent No. 5,036,315 to **Gurley** does not cure the defects identified above and the differences with respect to the present invention. Gurley does not show, teach or suggest (a) extracting data; (b) multiple extract stores; (c) multiple security access clearances for the extract stores. Also, Gurley '315 does not show (d) reconstruction of said data via the multiple extract stores with special security access. Gurley '315 discusses a video display control which accepts and processes two (2) video signals, one displayed in a defined window of the second video display.

Shmueli '357 discusses taking a computer readable document, parsing the document into blocks, such as text blocks (5/5 - 8), bounding the blocks (5/9), parsing the data in each block by

word or symbol (5/20), then comparing each word to an authority list (5/25). "The authority list is essentially a dictionary that lists many of the linguistic functions for words. The authority list can be very detailed and can be customized by users to suit the types of documents they use most frequently and user-defined metadata." Shmueli '357, 5/26. Earlier, Shmueli '357 defines "metadata" as "data about data." Shmueli '357, 1/12. Hence, the function of each word or symbol in the block is identified by the authority list and the resultant is metadata, that is, data about the data in the block. The combination of the text block and "information derived from each block" (5/57), is combined together to form a compound. Shmueli '357, 5/58 - 65. "The compounds are then processed through a trained neural network." Shmueli '357, 6/1.

> When all of the compounds have been processed through the neural net, metadata may be determined by selecting from the word guesses, compound guesses and document guesses having the highest word, compound, and document confidence factors, respectively. Alternatively, however, the metadata guesses may be improved prior to determining the metadata through additional analysis that will ultimately result in improved accuracy and reliability of the metadata extracted from the document.

Shmueli '357, 8/40.

Contrary to the claims in the present case wherein the neural network assists in "extracting" (see claim 22, for example), Shmueli '357 defines metadata for a document block by having the neural network guess the type or classification of the word or symbol. Shmueli '357 does not discuss multiple security levels, extraction for each level and full or partial reconstruction based upon security clearance access protocol.

The Manual of Patent Examining Procedures ("MPEP") explains that it is not obvious to modify a system with a plurality of sensors controlling a plurality of valves to create the inventive and patentable single sensor which controls a plurality of valves:

> In *In re Kotzab,* 217 F.3d 1365, 55 USPQ2d 1313 (Fed.Cir. 2000), the claims were drawn to an injection molding method using a single temperature sensor to control a plurality of flow control valves. The primary reference disclosed a multizone device having multiple sensors, each of which controlled an associated flow control valve, and also taught that one system may be used to control a number of valves. The court found that there was insufficient evidence to show that one system was the same as one sensor. While the control of multiple valves by a single sensor rather than by multiple sensors was a "technologically simple concept," there was no finding "as to the specific, understanding or principle within the knowledge of the skilled artisan" that would have provided the motivation to use a single sensor as the system to control more than one valve. 217 F.3d at 1371, 55 USPQ2d at 1318.

MPEP § 2143.01.

In the present invention, Applicant has developed a system designed to safeguard security sensitive content with a plurality of security levels and specific dispersal and retrieval techniques, all triggered or keyed to geographic location data. If the system is programmed not to permit the user to "walk away" from the site with the secure data, the system extracts the data upon transit over the regional boundary. Access via reconstruction is permitted as per the program when the user in within the boundary. Of course, the reverse operation could be programmed such that if within the region, no extraction nor reconstruction is permitted. Permutations of these data security controls are also possible within the scope of the claims. The single data storage systems in the prior art references of Fahlman '080 and O'Flaherty '203 cannot be extended to the claimed multi-level security storage systems with different extract stores with different access controls. Hastings '629 does not extract and store based upon geographic trigger events. These references discloses single storage of security words not "a plurality of security controlled memories as respective extract stores with security access controls thereat." O'Flaherty '203 shows single storage because only one database is open at any one time.

> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990) (Claims were directed to an apparatus for producing an aerated cementitious composition by drawing air into the cementitious composition by driving the output pump at a capacity greater than the feed rate. The prior art reference taught that the feed means can be run at a variable speed, however the court found that this does not require that the output pump be run at the claimed speed so that air is drawn into the mixing chamber and is entrained in the ingredients during operation. Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.).

MPEP § 2143.01.

In the prior art cited herein, there is no suggestion of the desirability of multi-level secured data storage, extraction with each security level, and full or partial reconstruction using multiple extract stores/multiple security clearances. O'Flaherty '203 is a single data base, with multiple encryption levels. This system cannot be altered such that different memories, as different extract stores, are active and are accessible to the user, via multiple security clearances, at the same time to store or reconstruct data. The presently claimed theory modifies that reference to an unacceptable degree. "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)." MPEP § 2143.01. This change to O'Flaherty '203 modifies the operation of the reference improperly. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)." MPEP § 2143.01. Further, such modification of O'Flaherty '203 is not possible unless the examiner uses hindsight provided by the present invention.

Applicant respectfully requests that the examiner approve the patentability of claims 1 - 172.

In the Office Action, the examiner requested a terminal disclaimer to overcome a double patenting obviousness rejection. Applicant submits, under protest, a Terminal Disclaimer. Please charge the $65.00 fee to Deposit Account no. 03-1231. "The filing of a terminal disclaimer to obviate a rejection based on nonstatutory double patenting is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991). The court indicated that the 'filing of a terminal disclaimer simply serves the statutory function of removing the rejection of double patenting, and raises neither a presumption nor estoppel on the merits of the rejection.'" MPEP 804.02(II), p. 800-32.

[Space left blank]

APPENDIX SHOWING SUPPORT FOR NEW CLAIMS

Support for new claims 147 - 172 is shown in brackets herebelow. Support for the substantive changes to claims 1 - 146 are also shown below. There are other locations in the specification and drawings that support the concepts set forth in these claims. Claims having similar scope to these listed herein below are not listed. If the examiner has additional questions regarding support, Applicant requests that the examiner note such concerns and Applicant will respond with additional information.

1. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories [Fig. 1B] as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, [55, 56, 71, 114, 121, 122, 127, 148, 160] ...

5. (currently amended) A method for securing data as claimed in claim 4 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive. [101]

16. (currently amended) A method of securing data as claimed in claim 1 wherein ~~said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels~~ said predetermined region is one a plurality of regions which includes at least one security protocol extraction region and at least one security protocol reconstruction region, the step of determining determines when said portable computing device is beyond at least one security protocol extraction region and applies the respective protocol to said data, and the step of determining further determines when said portable computing device is beyond at least one security protocol reconstruction region and applies the respective protocol to full or partial reconstruction of said data. [see ¶¶ 238, 240 and 242]

147. A computerized method of securing data in a plurality of security controlled data stores with access controls thereat, said data potentially having sensitive content such as sensitive words, data objects, characters, images, data elements or icons, comprising:

storing separately sensitive content in secure data stores of said plurality of security data stores;

permitting reconstruction of some or all of said data with appropriate access controls applied to respective secure data stores; and

said storing or reconstruction based upon territorial protocol [249, 122] and a geographic location signal [238, 242] or a triggering event. [155, 246]

148. A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering or extracting said sensitive content in said secure data stores. [Fig. 1A]

149. A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of removing [29] or copying [37] said sensitive content in said secure data stores.

150. A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering and transferring or extracting and transferring said sensitive content in said secure data stores. [112]

151. A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or both of partially or completely storing said sensitive content in said secure data stores. [Fig. 1A]

152. A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes partially or completely storing said sensitive content in said secure data stores with at least one of encryption or parsing of data. [106, Fig. 10, 210]

153. A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores. [41, 182, 183]

154. A computerized method of securing data as claimed in claim 147 including manually or automatically at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores. [41, 182, 183]

155. A computerized method of securing data as claimed in claim 147 including at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; and wherein

said sensitive content has different levels of sensitive content therein corresponding to respective ones of said secure data stores. [Fig. 7]

156. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is defined as at least one of security sensitive content, content of significance, trade secret content [3], personal identifying information [3], medical content subject to regulatory provisions [3], or back-up content and said respective ones of said secure data stores are correspondingly designated as at least one of security sensitive stores, stores for content of significance, trade secret stores, personal identifying information stores, medical regulatory provision stores, or back-up stores. [223]

157. A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes at least one or more of storing in predetermined security data stores, storing in a predetermined manner by random selection of security data stores [142], storing by data class in said security data stores [223], storing data by data type in said security data stores [223], or storing by level of security in said security data stores. [223]

158. A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in said security data stores in a predetermined manner with an algorithmic selection. [130]

159. A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in optical media data stores. [130]

160. A computerized method of securing data as claimed in claim 147 wherein storing of said sensitive content is done separately with respect to at least one of remainder data, left-over data, non-sensitive content data, surplus data, residue data, remnant data, or data complementary to sensitive content data. [107]

161. A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution 34,41,44], regeneration, compilation [35,131], reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores. [47,51,55]

162. A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes the use of at least one of predetermined access controls [47,51,55], assigned access controls, access controls generated with said storing of said secure data, or access controls and encryption. [47,51,55]

163. A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution, regeneration, compilation, reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores. [Fig. 7]

164. A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to respective secure data stores in at least one of the following manners:

said access controls [47, 51, 55] applied sequentially to respective secure data stores; [121, 133]

said access controls applied concurrently to respective secure data stores; [121, 133]

said access controls applied to respective secure data stores subsequent to application of a security protocol; [121,002,032,122,144]

said secure data stores are mapped [Fig. 5, 144]and said access controls are applied to obtain the mapped secure data stores; [121,002,032,122,144] or

said access controls are applied subsequent to an exchange of compensation or an exchange of data. [Fig. 13, 234, 235, 173]

said access controls applied to respective secure data stores subsequent to application of a hierarchical security protocol. [212]

165. A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to at least one or more of predetermined respective secure data stores [130, 133], associated respective secure data stores [130, 133], correlated respective secure data stores [130, 131], or designated respective secure data stores. [38, 126, 130]

166. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system [20]with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and [34, 130]

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores. [131]

167. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores. [131]

168. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores. [131]

169. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer

and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and [131]

said server controlling the application of said access controls. [131]

170. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

select sensitive words, data objects, characters, images, data elements or icons;

defined sensitive words, data objects, characters, images, data elements or icons; [46]

known sensitive words, data objects, characters, images, data elements or icons; [46]

certain sensitive words, data objects, characters, images, data elements or icons;

a collection of sensitive words, data objects, characters, images, data elements or icons; [111, 105]

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons; or [46]

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons having different hierarchal [30,35, 110, 156] or orthogonal levels [35, 160] of sensitive content.

171. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

portions of predetermined sensitive words, data objects, characters, images, data elements or icons; or [104]

words, data objects, characters, images, data elements or icons which are not from a plurality of predetermined words, data objects, characters, images, data elements or icons. [46]

172. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is related to sensitive words, data objects, characters, images, data elements or icons, by at least or more of a function or a meaning. [104, 105]

Respectfully submitted,

By _____

Robert C. Kain, Jr., Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002,
Facsimile: 954-768-0158

Docket No.: 6851-2-CIP-5

Certificate of e-Filing

I hereby certify that this correspondence is being e-filed with Commissioner for Patents, Alexandria, VA on May 14, 2007.

_____

Robert C. Kain, Jr.
Reg. No. 30,648

F:\RCK\CLIENTS\Redlich\Patents\6851-02-cip5-Amdt-1st-051007.wpd

Replacement Sheet

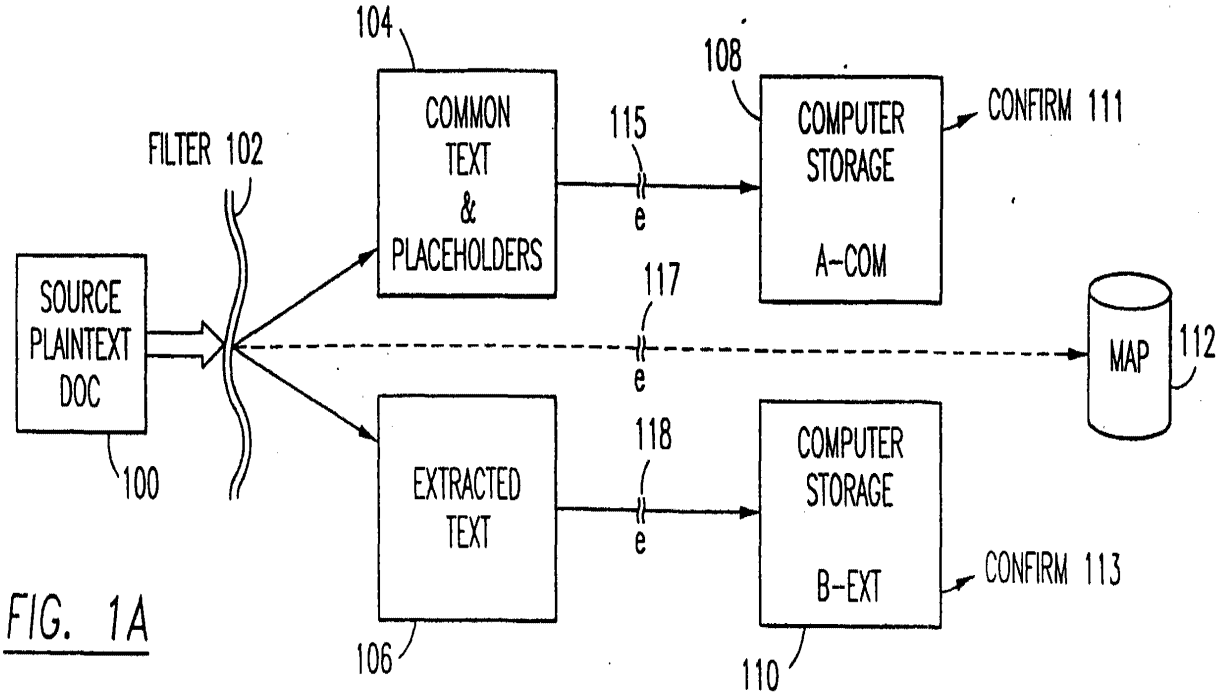


FIG. 1A

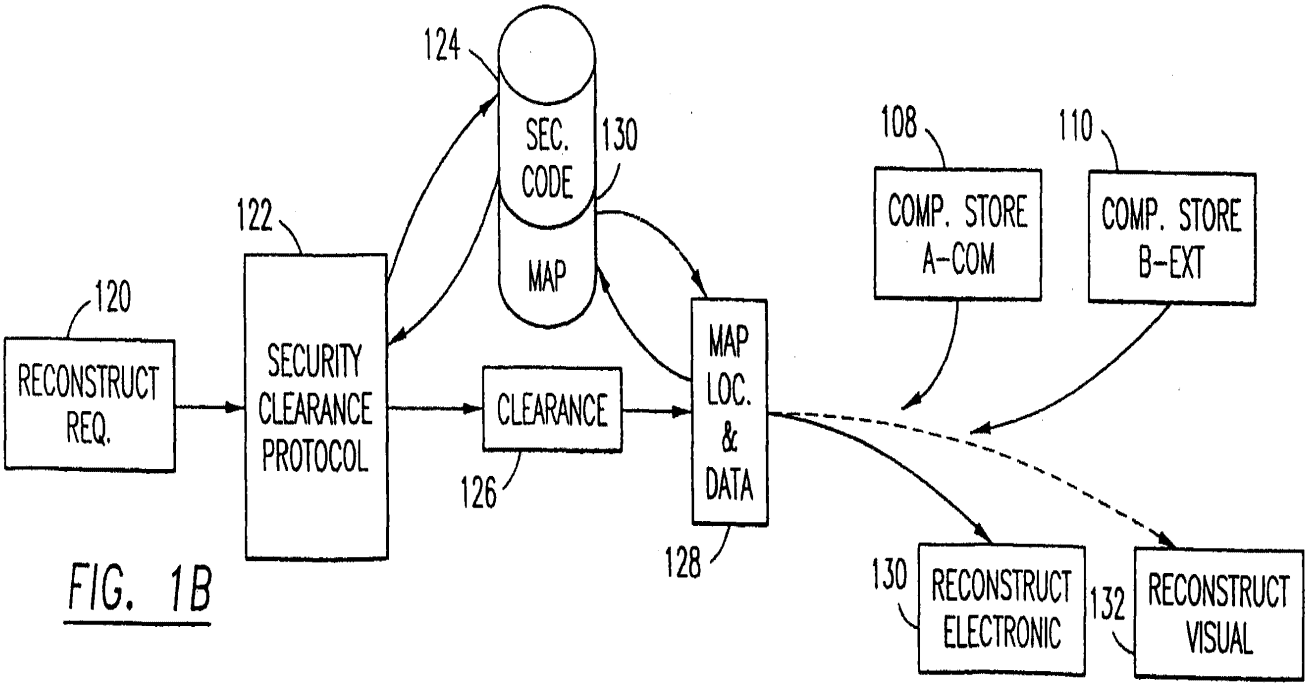


FIG. 1B

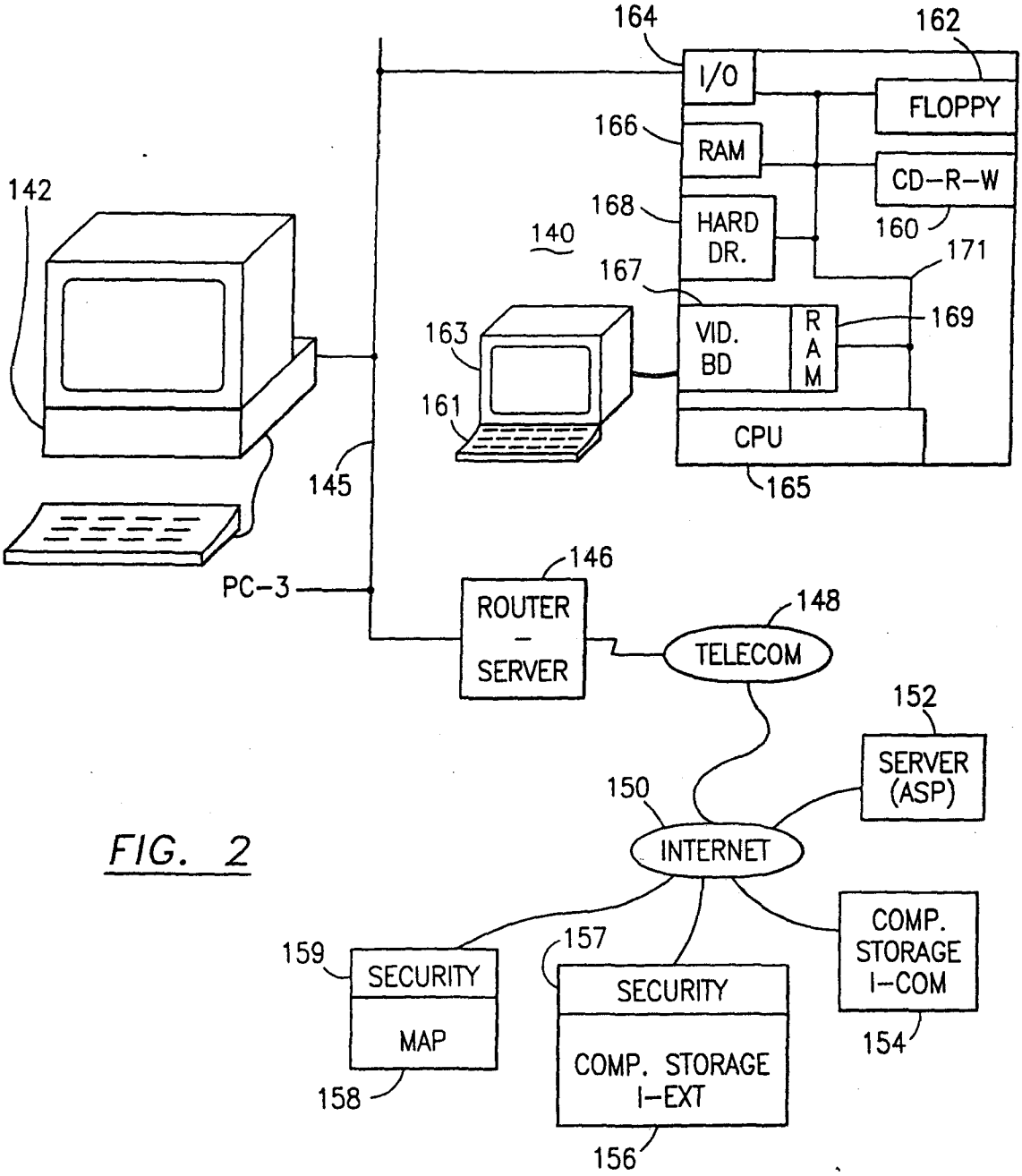
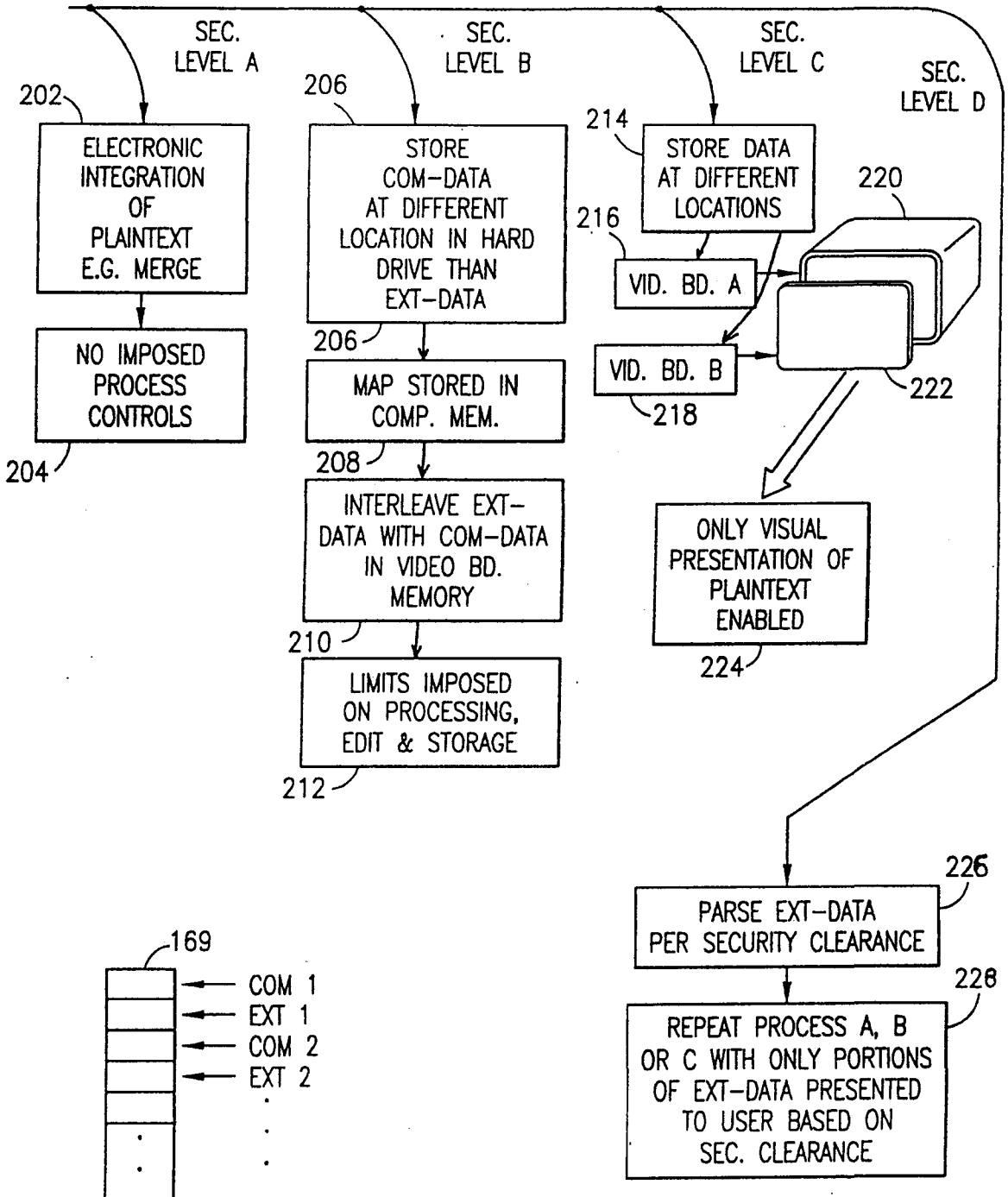

164
162
I/O
FLOPPY
166
RAM
CD-R-W
142
168
HARD DR.
160
140
171
167
163
VID. BD
R A M
169
161
CPU
145
165
146
PC-3
ROUTER – SERVER
148
TELECOM
152
SERVER (ASP)
150
INTERNET
159
SECURITY
MAP
158
157
SECURITY
COMP. STORAGE I-EXT
156
COMP. STORAGE I-COM
154

FIG. 2

FIG. 3


RECONSTRUCT
SEC. LEVEL A
SEC. LEVEL B
SEC. LEVEL C
SEC. LEVEL D
202
ELECTRONIC INTEGRATION OF PLAINTEXT E.G. MERGE
NO IMPOSED PROCESS CONTROLS
204
206
STORE COM-DATA AT DIFFERENT LOCATION IN HARD DRIVE THAN EXT-DATA
206
MAP STORED IN COMP. MEM.
208
INTERLEAVE EXT-DATA WITH COM-DATA IN VIDEO BD. MEMORY
210
LIMITS IMPOSED ON PROCESSING, EDIT & STORAGE
212
214
STORE DATA AT DIFFERENT LOCATIONS
216
VID. BD. A
VID. BD. B
218
220
222
ONLY VISUAL PRESENTATION OF PLAINTEXT ENABLED
224
226
PARSE EXT-DATA PER SECURITY CLEARANCE
228
REPEAT PROCESS A, B OR C WITH ONLY PORTIONS OF EXT-DATA PRESENTED TO USER BASED ON SEC. CLEARANCE

169
COM 1
EXT 1
COM 2
EXT 2

FIG. 3A

FIG. 4

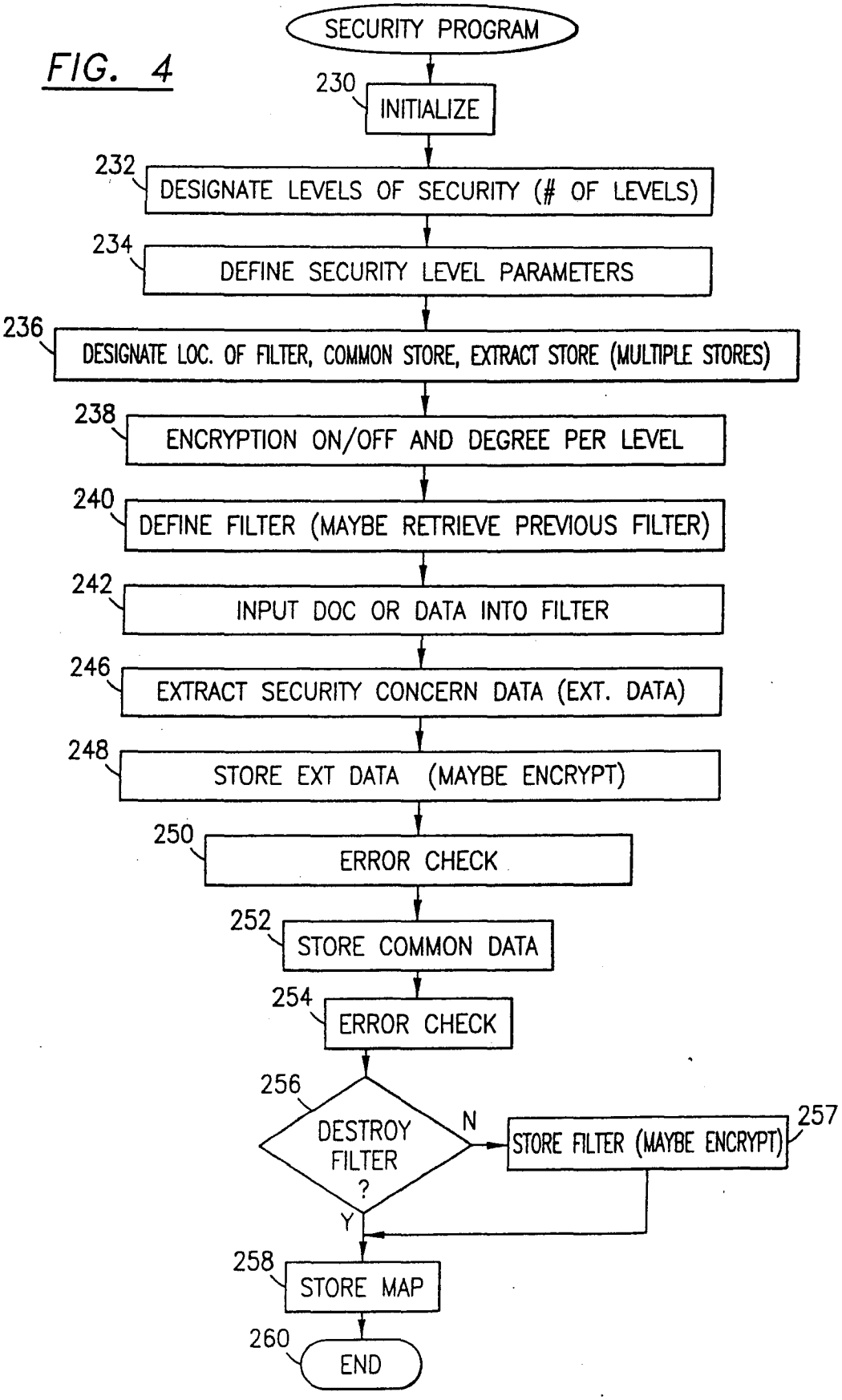
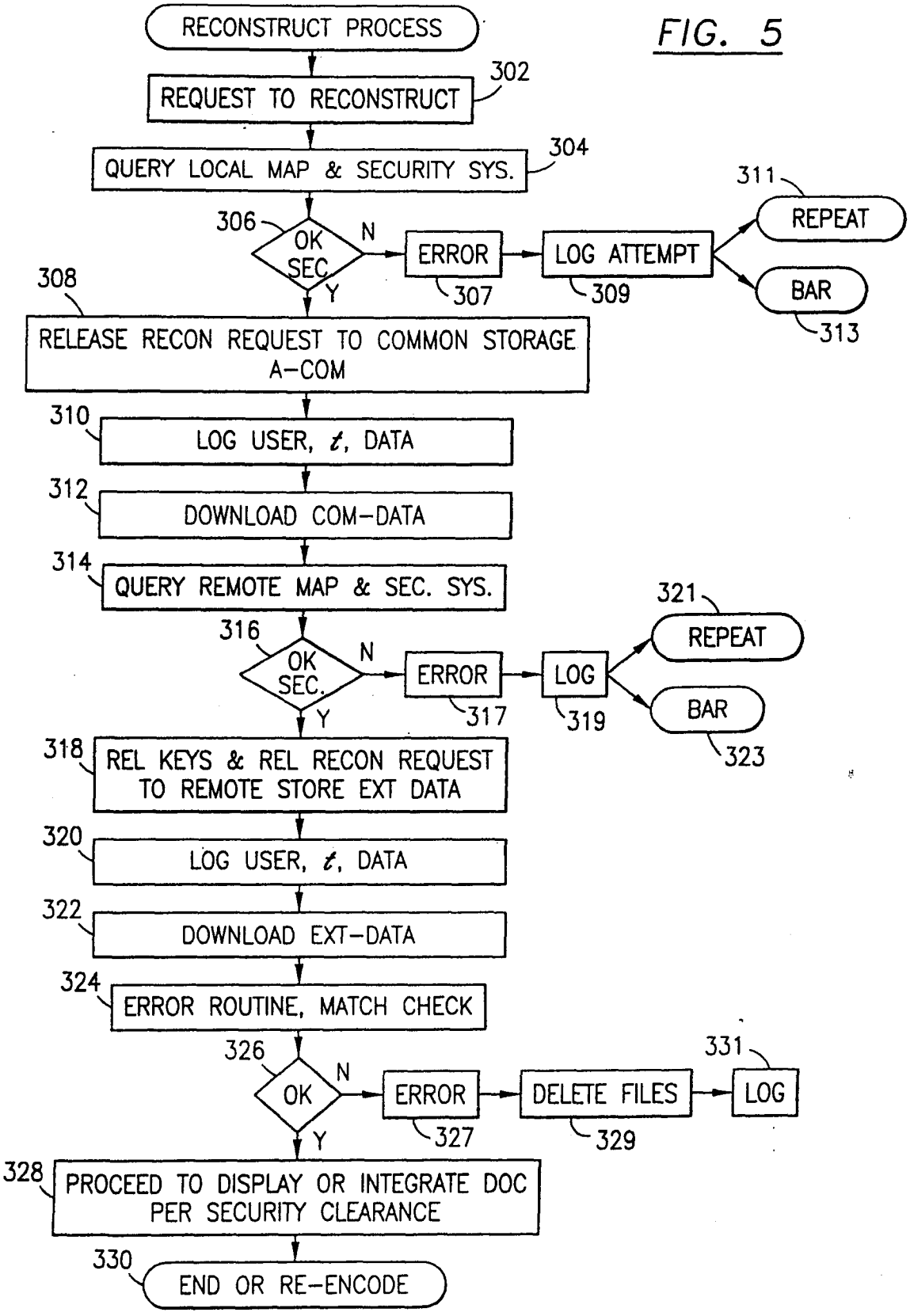

SECURITY PROGRAM
230
INITIALIZE
232
DESIGNATE LEVELS OF SECURITY (# OF LEVELS)
234
DEFINE SECURITY LEVEL PARAMETERS
236
DESIGNATE LOC. OF FILTER, COMMON STORE, EXTRACT STORE (MULTIPLE STORES)
238
ENCRYPTION ON/OFF AND DEGREE PER LEVEL
240
DEFINE FILTER (MAYBE RETRIEVE PREVIOUS FILTER)
242
INPUT DOC OR DATA INTO FILTER
246
EXTRACT SECURITY CONCERN DATA (EXT. DATA)
248
STORE EXT DATA (MAYBE ENCRYPT)
250
ERROR CHECK
252
STORE COMMON DATA
254
ERROR CHECK
256
DESTROY FILTER ?
N
257
STORE FILTER (MAYBE ENCRYPT)
Y
258
STORE MAP
260
END

FIG. 5


RECONSTRUCT PROCESS
REQUEST TO RECONSTRUCT
302
QUERY LOCAL MAP & SECURITY SYS.
304
306
OK SEC.
N
Y
ERROR
307
LOG ATTEMPT
309
311
REPEAT
BAR
313
308
RELEASE RECON REQUEST TO COMMON STORAGE A-COM
310
LOG USER, t, DATA
312
DOWNLOAD COM-DATA
314
QUERY REMOTE MAP & SEC. SYS.
316
OK SEC.
N
Y
ERROR
317
LOG
319
321
REPEAT
BAR
323
318
REL KEYS & REL RECON REQUEST TO REMOTE STORE EXT DATA
320
LOG USER, t, DATA
322
DOWNLOAD EXT-DATA
324
ERROR ROUTINE, MATCH CHECK
326
OK
N
Y
ERROR
327
DELETE FILES
329
331
LOG
328
PROCEED TO DISPLAY OR INTEGRATE DOC PER SECURITY CLEARANCE
330
END OR RE-ENCODE

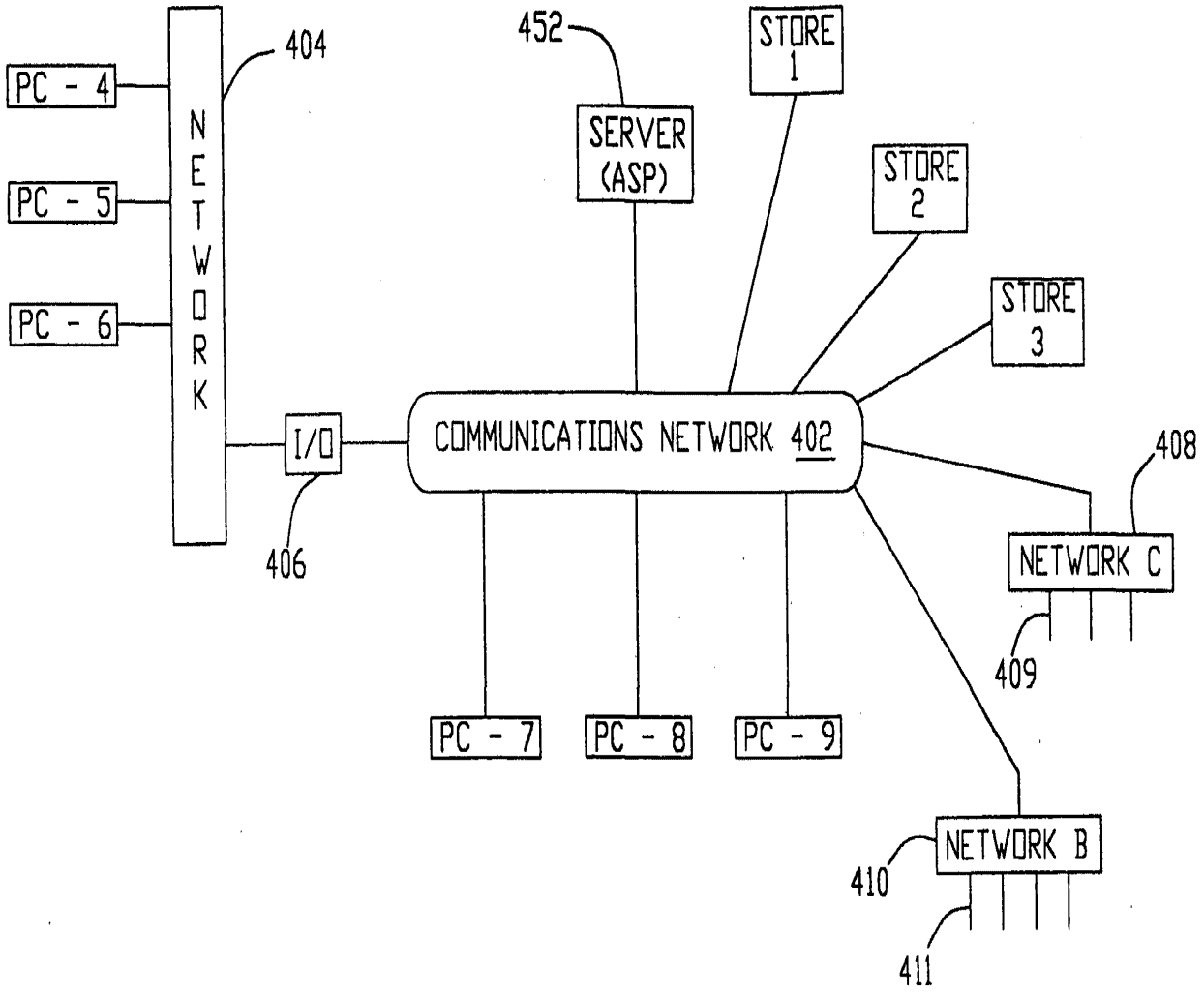


FIG.6

Replacement Sheet

FIG. 7a

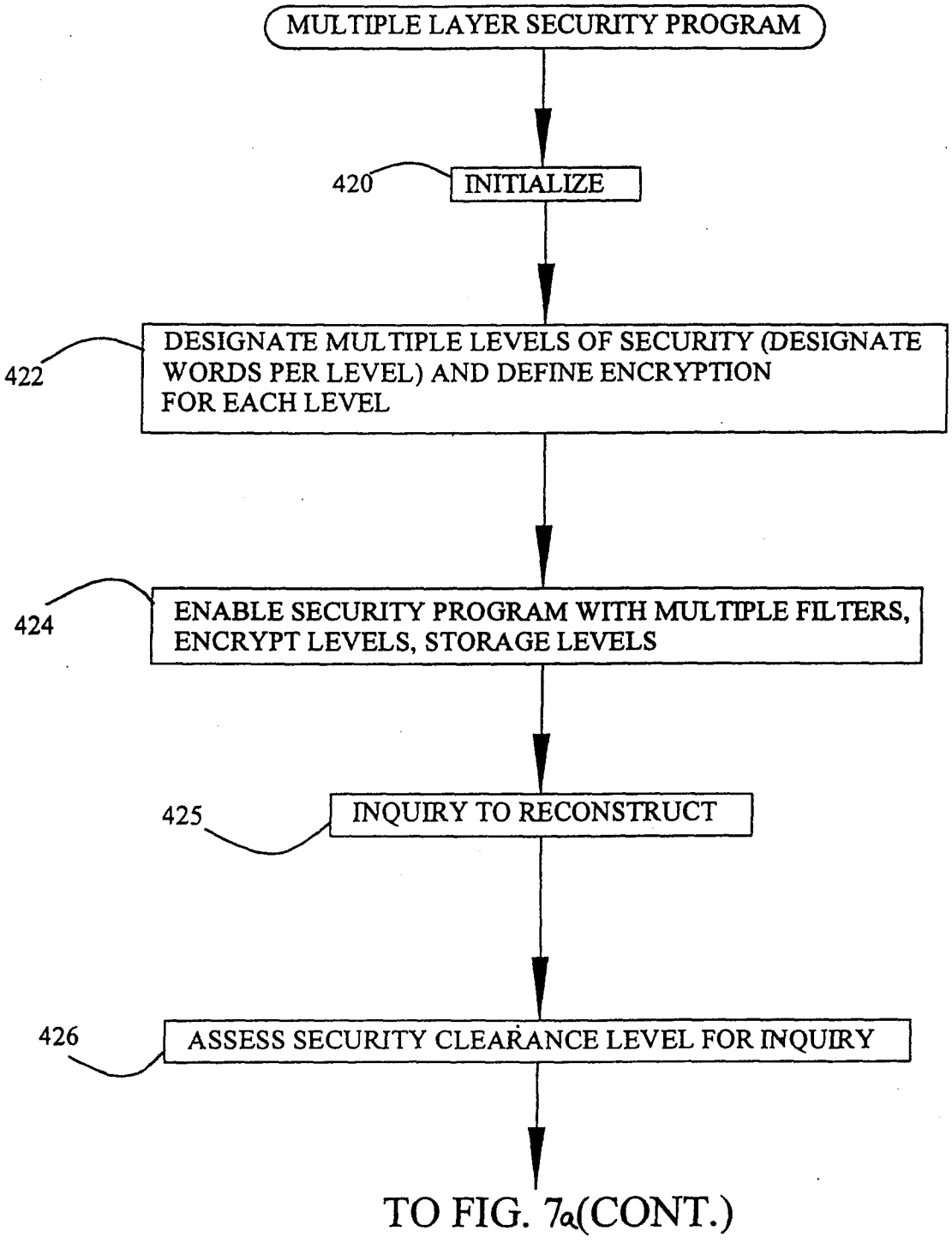
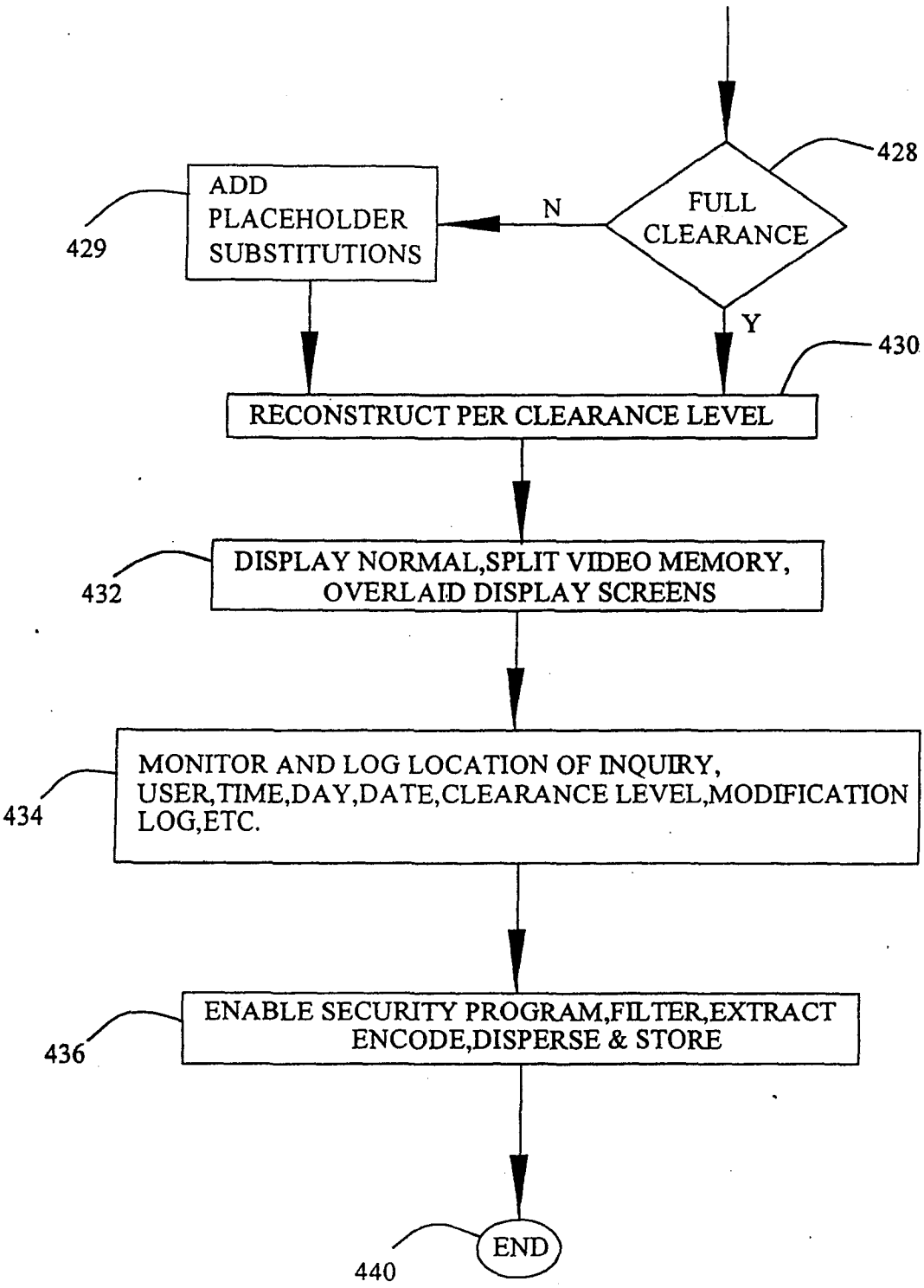

MULTIPLE LAYER SECURITY PROGRAM
420
INITIALIZE
422
DESIGNATE MULTIPLE LEVELS OF SECURITY (DESIGNATE WORDS PER LEVEL) AND DEFINE ENCRYPTION FOR EACH LEVEL
424
ENABLE SECURITY PROGRAM WITH MULTIPLE FILTERS, ENCRYPT LEVELS, STORAGE LEVELS
425
INQUIRY TO RECONSTRUCT
426
ASSESS SECURITY CLEARANCE LEVEL FOR INQUIRY
TO FIG. 7a(CONT.)

FIG. 7a(CONT.)


428
FULL CLEARANCE
N
ADD PLACEHOLDER SUBSTITUTIONS
429
Y
430
RECONSTRUCT PER CLEARANCE LEVEL
DISPLAY NORMAL,SPLIT VIDEO MEMORY, OVERLAID DISPLAY SCREENS
432
MONITOR AND LOG LOCATION OF INQUIRY, USER,TIME,DAY,DATE,CLEARANCE LEVEL,MODIFICATION LOG,ETC.
434
ENABLE SECURITY PROGRAM,FILTER,EXTRACT ENCODE,DISPERSE & STORE
436
END
440

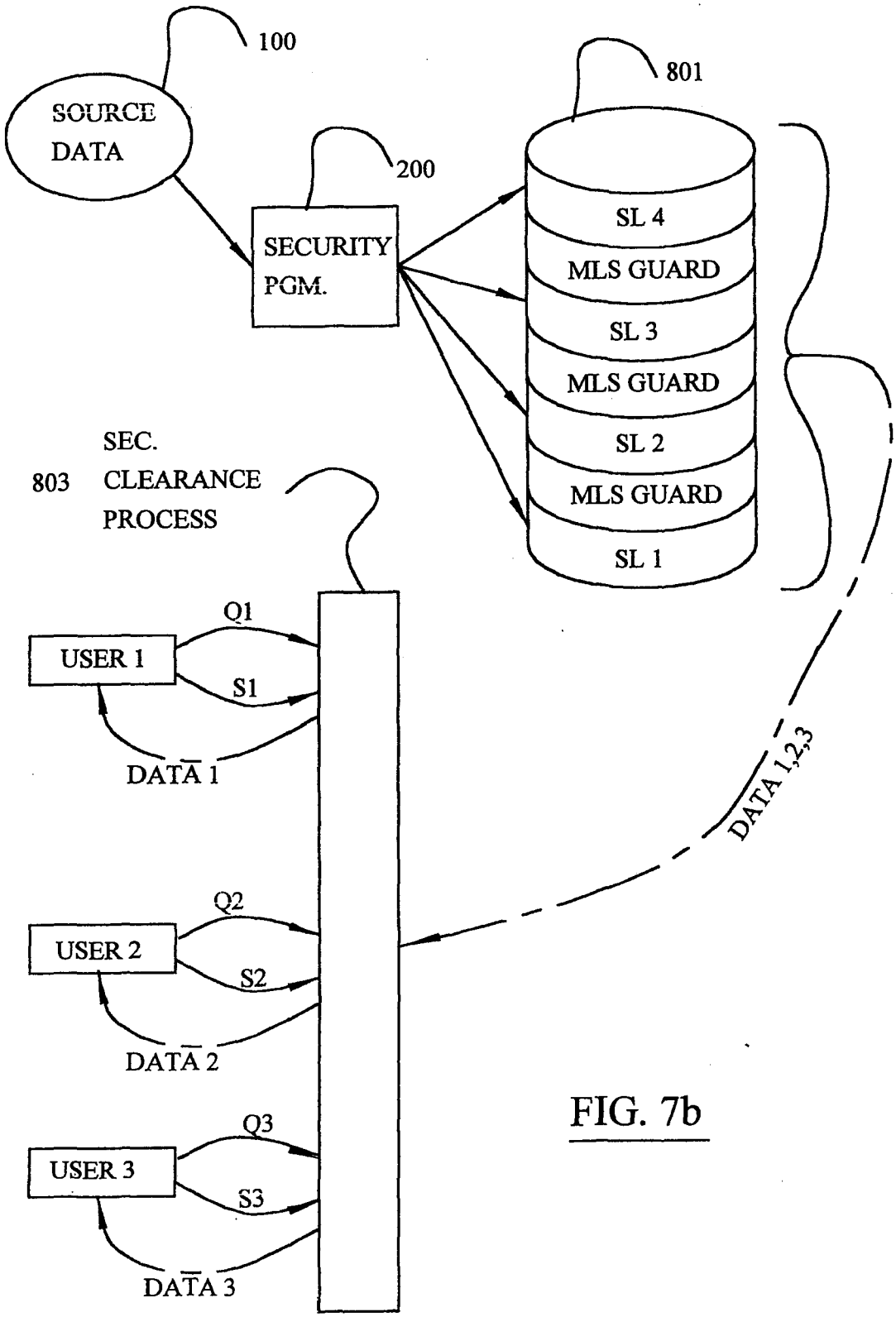

100
SOURCE DATA
200
SECURITY PGM.
801
SL 4
MLS GUARD
SL 3
MLS GUARD
SL 2
MLS GUARD
SL 1
803
SEC. CLEARANCE PROCESS
Q1
USER 1
S1
DATA 1
Q2
USER 2
S2
DATA 2
Q3
USER 3
S3
DATA 3
DATA 1,2,3

FIG. 7b

FIG. 8

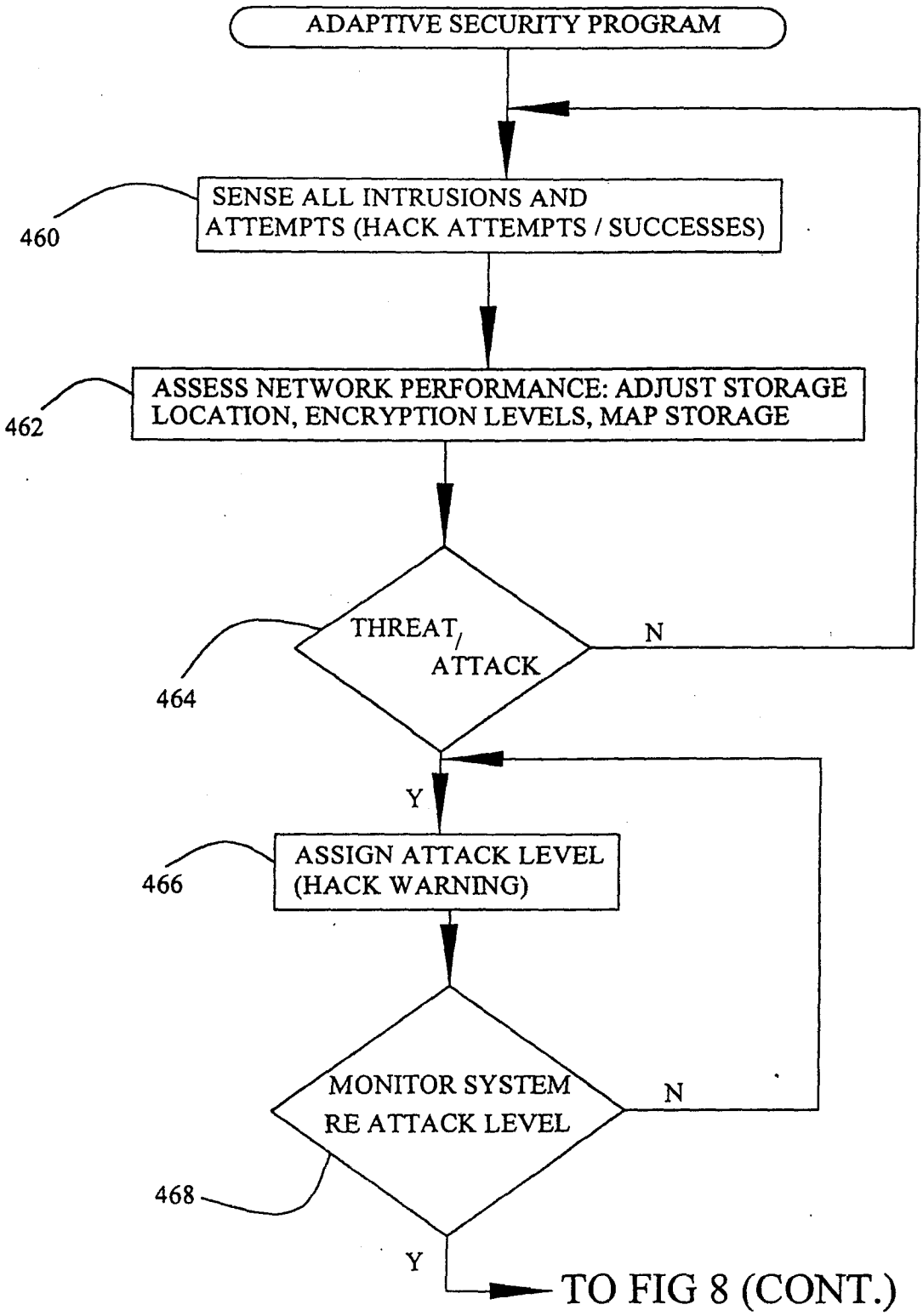

ADAPTIVE SECURITY PROGRAM
460
SENSE ALL INTRUSIONS AND ATTEMPTS (HACK ATTEMPTS / SUCCESSES)
462
ASSESS NETWORK PERFORMANCE: ADJUST STORAGE LOCATION, ENCRYPTION LEVELS, MAP STORAGE
464
THREAT/ ATTACK
N
Y
466
ASSIGN ATTACK LEVEL (HACK WARNING)
MONITOR SYSTEM RE ATTACK LEVEL
N
468
Y
TO FIG 8 (CONT.)

FIG. 8 (CONT.)

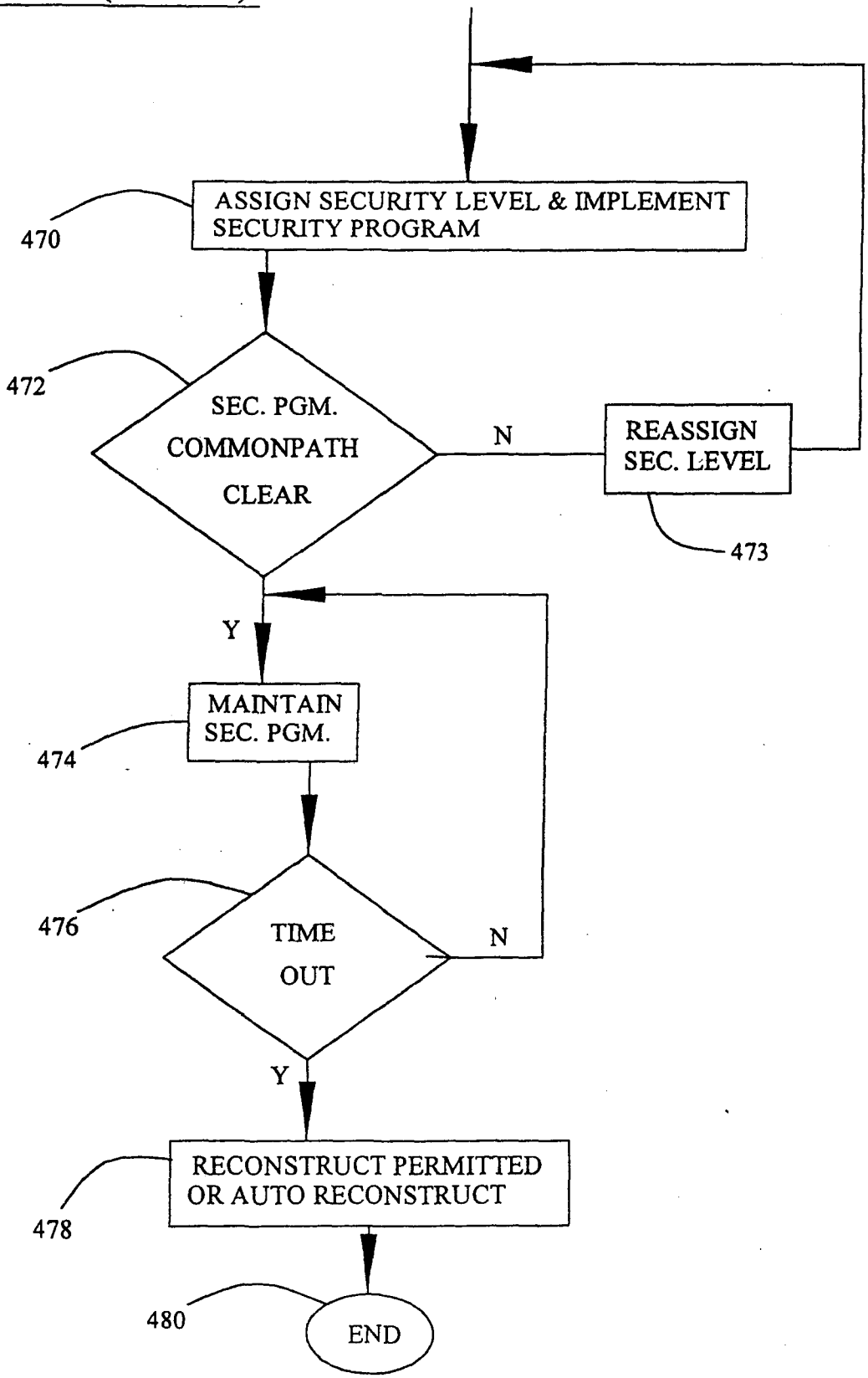

ASSIGN SECURITY LEVEL & IMPLEMENT SECURITY PROGRAM
470
472
SEC. PGM. COMMONPATH CLEAR
N
REASSIGN SEC. LEVEL
473
Y
MAINTAIN SEC. PGM.
474
476
TIME OUT
N
Y
RECONSTRUCT PERMITTED OR AUTO RECONSTRUCT
478
480
END

FIG. 9

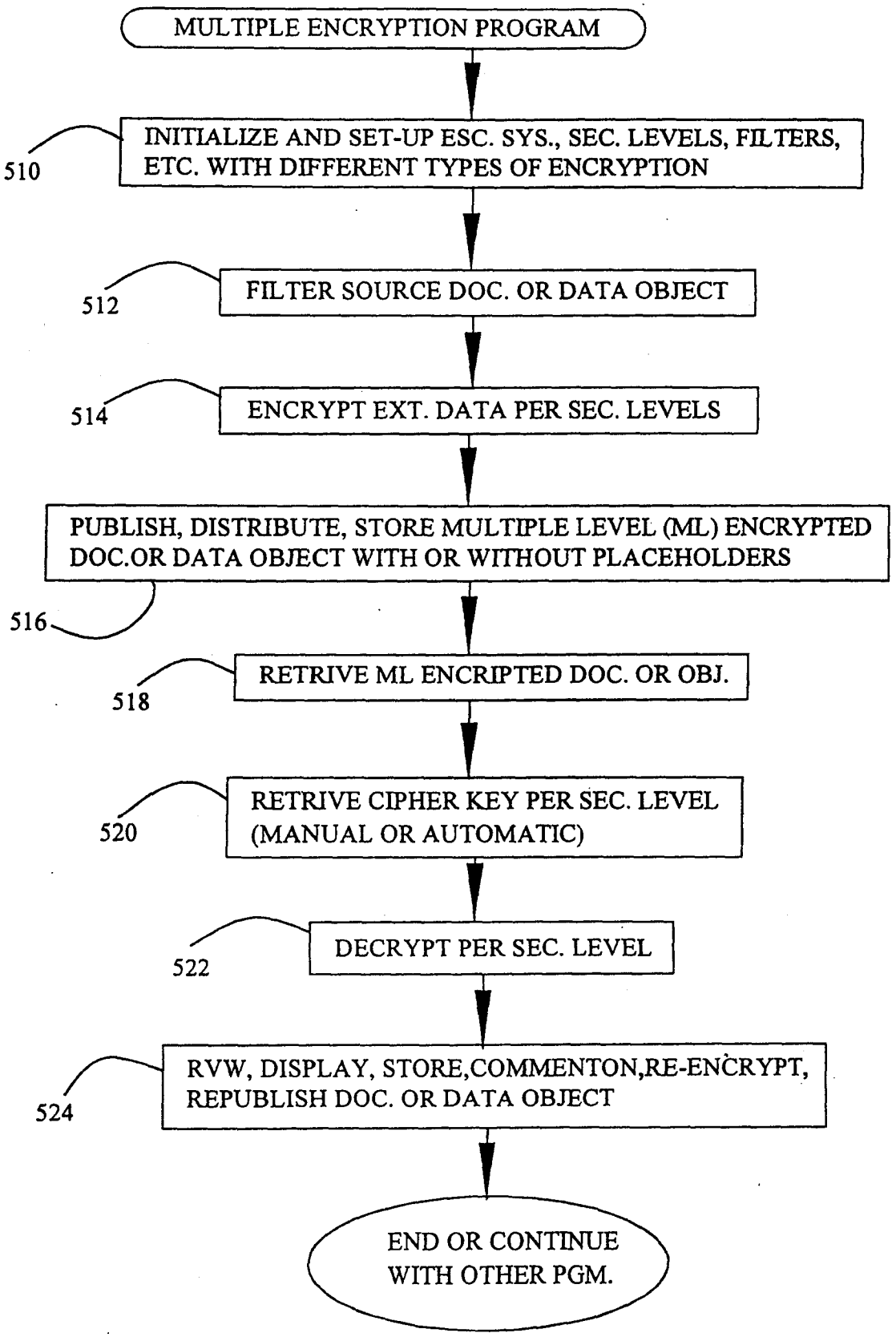

MULTIPLE ENCRYPTION PROGRAM
510
INITIALIZE AND SET-UP ESC. SYS., SEC. LEVELS, FILTERS, ETC. WITH DIFFERENT TYPES OF ENCRYPTION
512
FILTER SOURCE DOC. OR DATA OBJECT
514
ENCRYPT EXT. DATA PER SEC. LEVELS
516
PUBLISH, DISTRIBUTE, STORE MULTIPLE LEVEL (ML) ENCRYPTED DOC.OR DATA OBJECT WITH OR WITHOUT PLACEHOLDERS
518
RETRIVE ML ENCRIPTED DOC. OR OBJ.
520
RETRIVE CIPHER KEY PER SEC. LEVEL (MANUAL OR AUTOMATIC)
522
DECRYPT PER SEC. LEVEL
524
RVW, DISPLAY, STORE,COMMENTON,RE-ENCRYPT, REPUBLISH DOC. OR DATA OBJECT
END OR CONTINUE WITH OTHER PGM.

FIG. 10

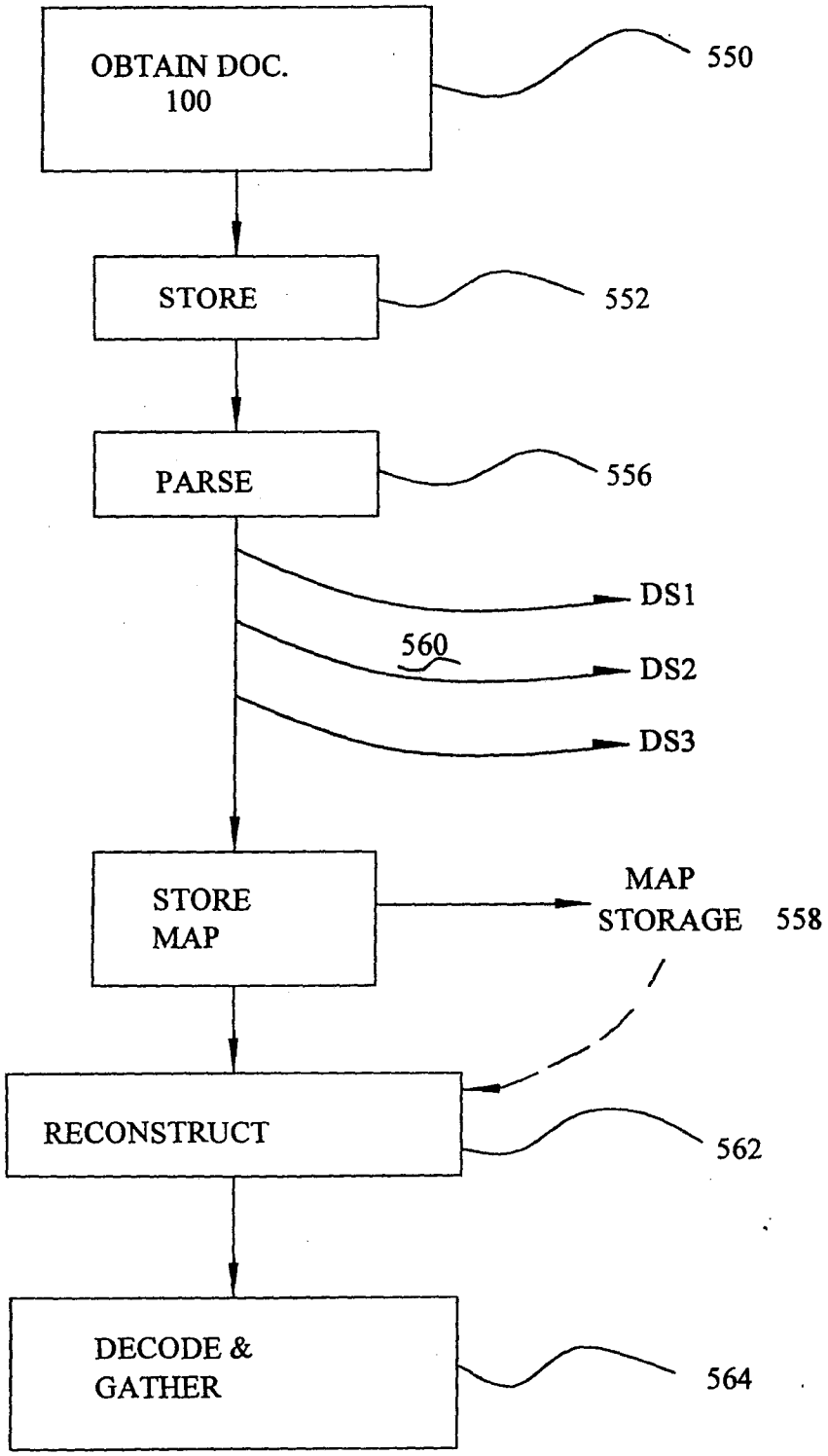

OBTAIN DOC. 100
550
STORE
552
PARSE
556
DS1
560
DS2
DS3
STORE MAP
MAP STORAGE 558
RECONSTRUCT
562
DECODE & GATHER
564

FIG.11A

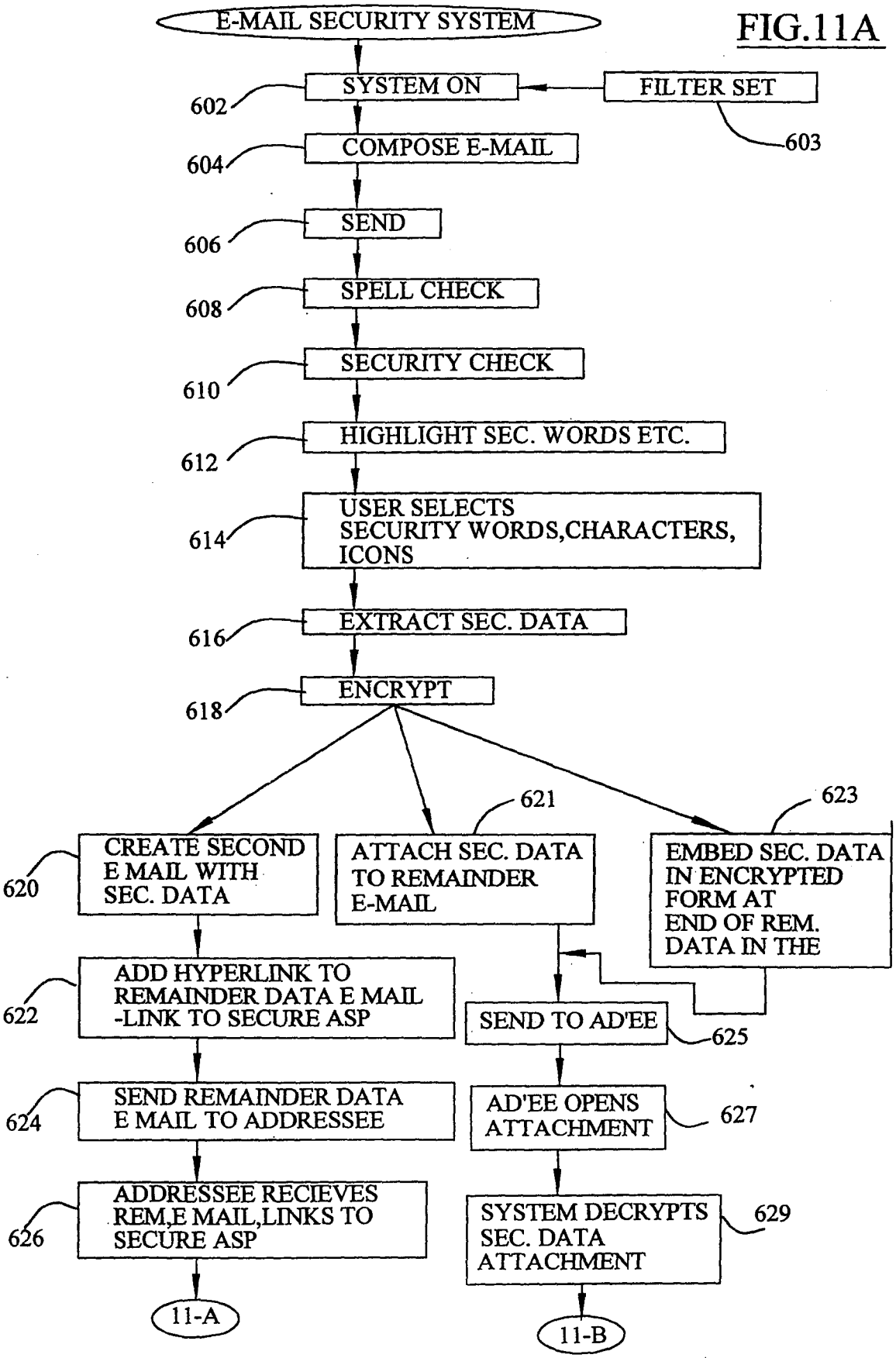

E-MAIL SECURITY SYSTEM
SYSTEM ON
FILTER SET
602
603
COMPOSE E-MAIL
604
SEND
606
SPELL CHECK
608
SECURITY CHECK
610
HIGHLIGHT SEC. WORDS ETC.
612
USER SELECTS SECURITY WORDS,CHARACTERS, ICONS
614
EXTRACT SEC. DATA
616
ENCRYPT
618
621
623
CREATE SECOND E MAIL WITH SEC. DATA
620
ATTACH SEC. DATA TO REMAINDER E-MAIL
EMBED SEC. DATA IN ENCRYPTED FORM AT END OF REM. DATA IN THE
ADD HYPERLINK TO REMAINDER DATA E MAIL -LINK TO SECURE ASP
622
SEND TO AD'EE
625
SEND REMAINDER DATA E MAIL TO ADDRESSEE
624
AD'EE OPENS ATTACHMENT
627
ADDRESSEE RECIEVES REM,E MAIL,LINKS TO SECURE ASP
626
SYSTEM DECRYPTS SEC. DATA ATTACHMENT
629
11-A
11-B

FIG.11B

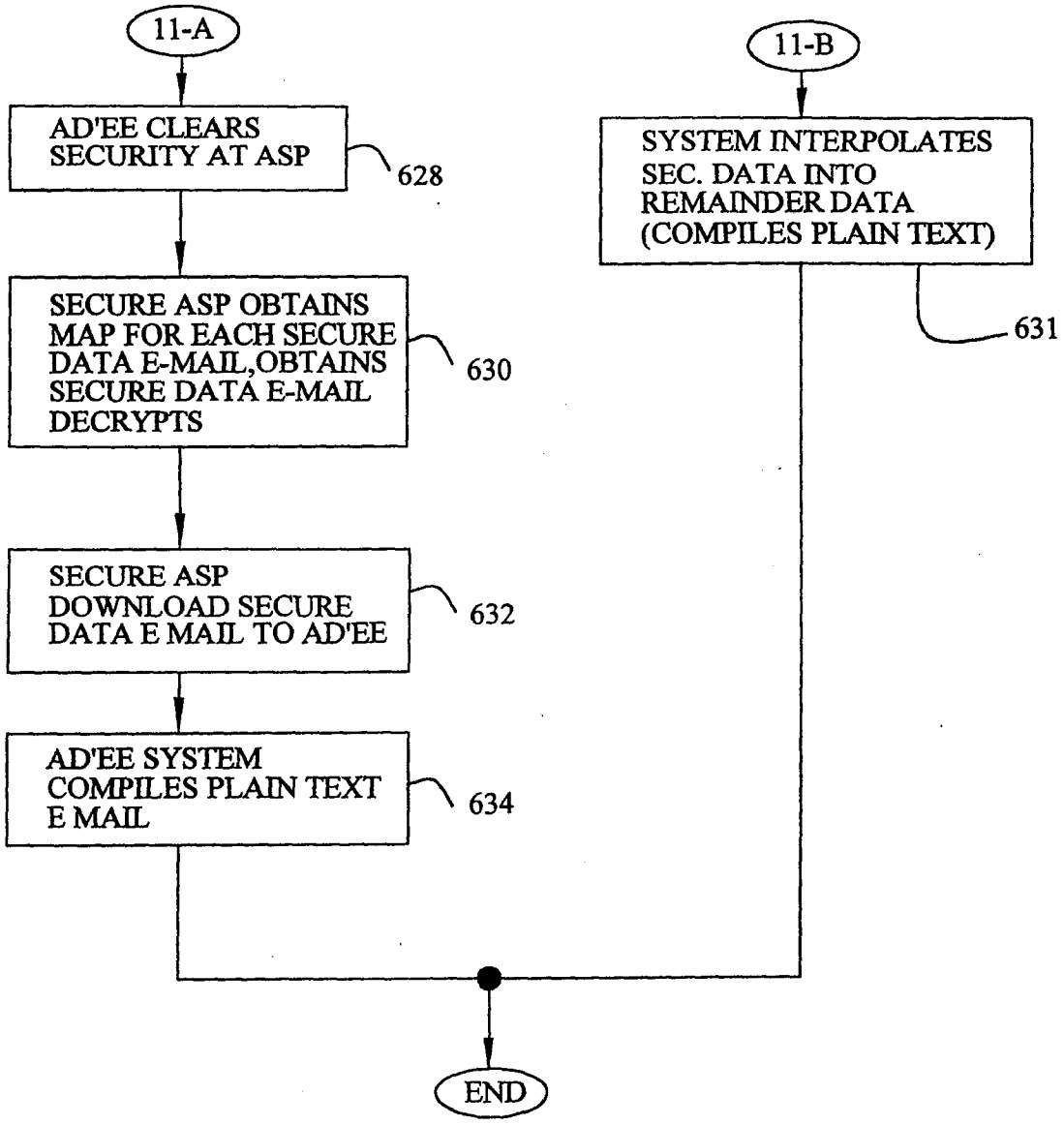

11-A
AD'EE CLEARS SECURITY AT ASP
628
SECURE ASP OBTAINS MAP FOR EACH SECURE DATA E-MAIL,OBTAINS SECURE DATA E-MAIL DECRYPTS
630
SECURE ASP DOWNLOAD SECURE DATA E MAIL TO AD'EE
632
AD'EE SYSTEM COMPILES PLAIN TEXT E MAIL
634
11-B
SYSTEM INTERPOLATES SEC. DATA INTO REMAINDER DATA (COMPILES PLAIN TEXT)
631
END

FIG.12A

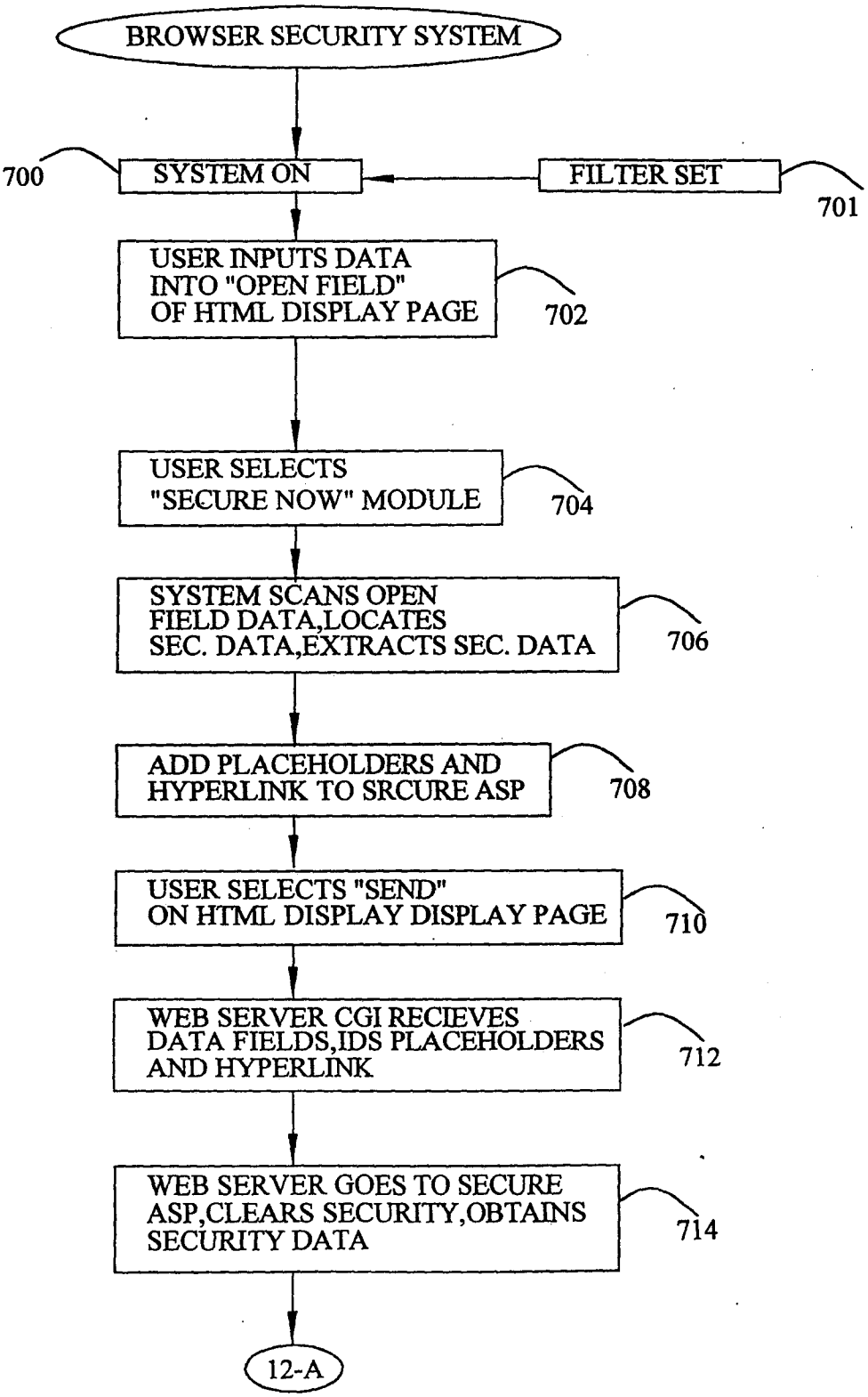

BROWSER SECURITY SYSTEM
700
SYSTEM ON
FILTER SET
701
USER INPUTS DATA INTO "OPEN FIELD" OF HTML DISPLAY PAGE
702
USER SELECTS "SECURE NOW" MODULE
704
SYSTEM SCANS OPEN FIELD DATA,LOCATES SEC. DATA,EXTRACTS SEC. DATA
706
ADD PLACEHOLDERS AND HYPERLINK TO SRCURE ASP
708
USER SELECTS "SEND" ON HTML DISPLAY DISPLAY PAGE
710
WEB SERVER CGI RECIEVES DATA FIELDS,IDS PLACEHOLDERS AND HYPERLINK
712
WEB SERVER GOES TO SECURE ASP,CLEARS SECURITY,OBTAINS SECURITY DATA
714
12-A

FIG.12B

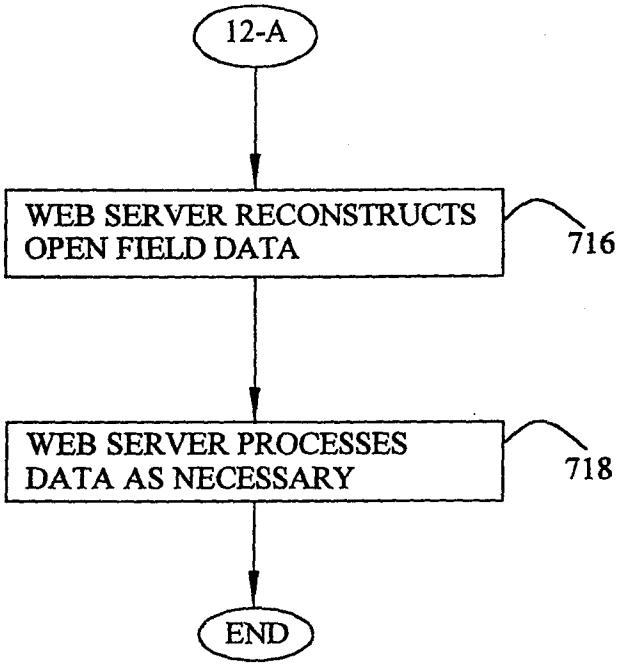
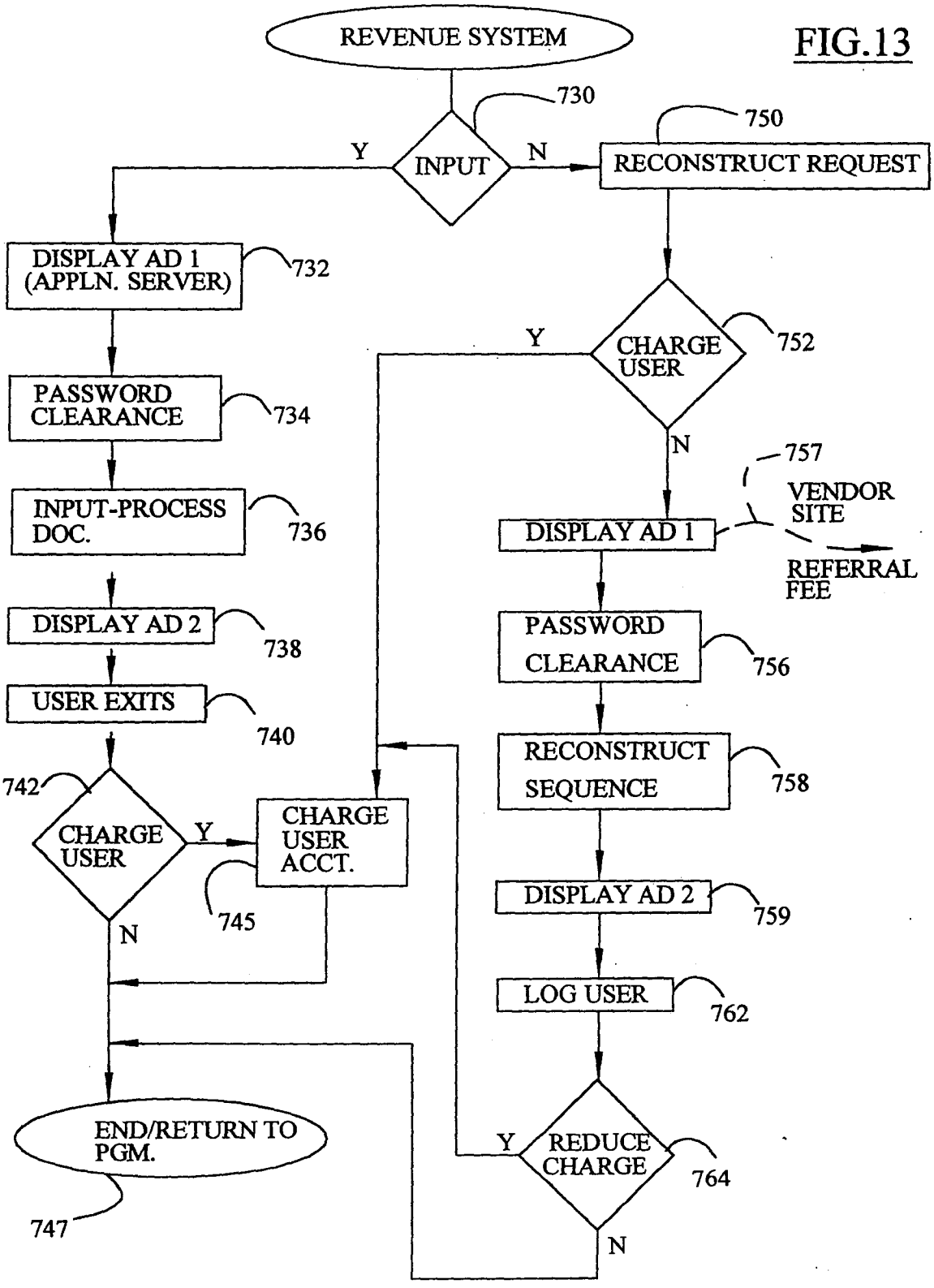

12-A
WEB SERVER RECONSTRUCTS OPEN FIELD DATA
716
WEB SERVER PROCESSES DATA AS NECESSARY
718
END

FIG.13


REVENUE SYSTEM
730
INPUT
Y
N
750
RECONSTRUCT REQUEST
DISPLAY AD 1 (APPLN. SERVER)
732
PASSWORD CLEARANCE
734
INPUT-PROCESS DOC.
736
DISPLAY AD 2
738
USER EXITS
740
742
CHARGE USER
Y
CHARGE USER ACCT.
745
N
747
END/RETURN TO PGM.
Y
CHARGE USER
752
N
757
VENDOR SITE
DISPLAY AD 1
REFERRAL FEE
PASSWORD CLEARANCE
756
RECONSTRUCT SEQUENCE
758
DISPLAY AD 2
759
LOG USER
762
Y
REDUCE CHARGE
764
N

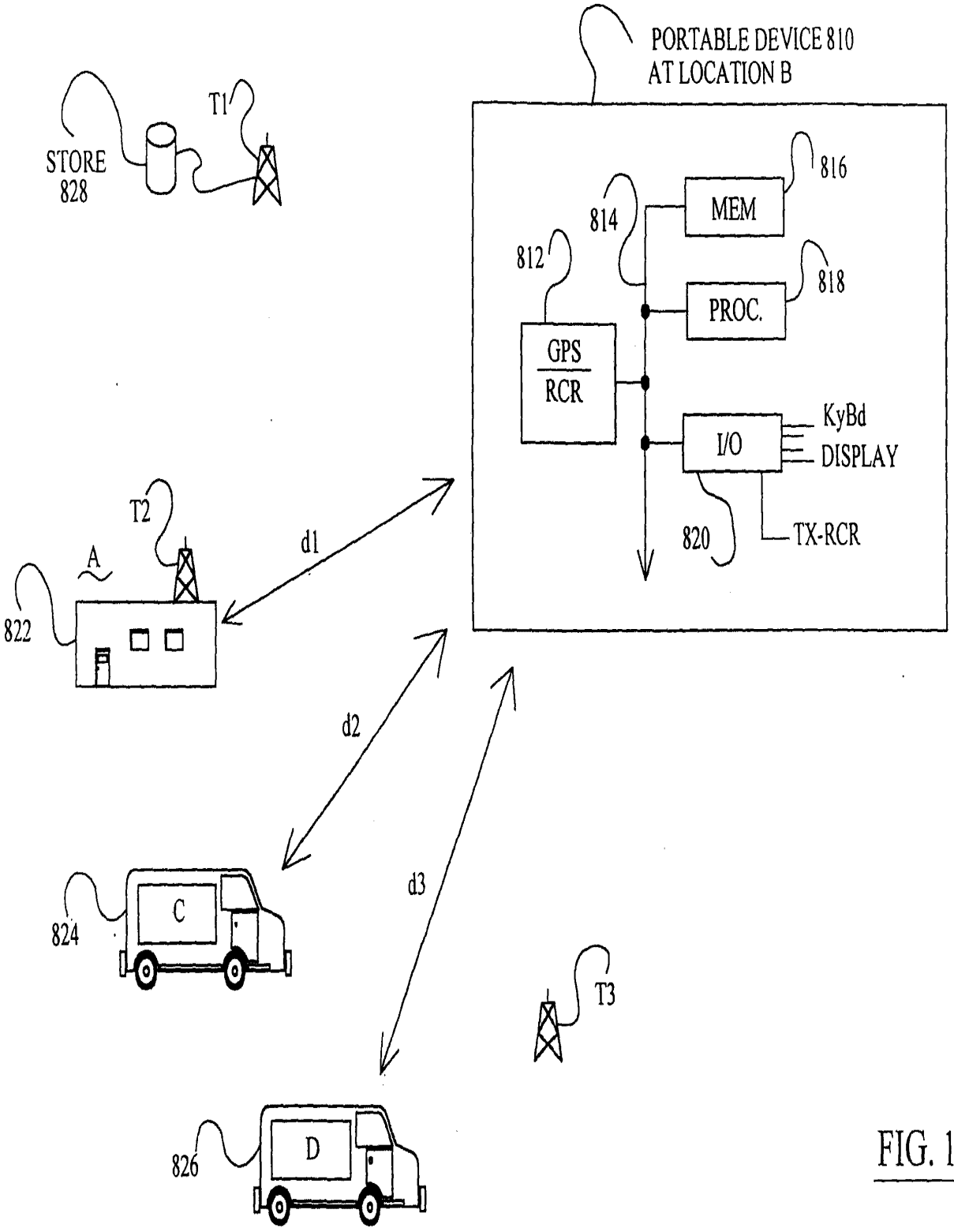

PORTABLE DEVICE 810
AT LOCATION B
816
MEM
814
812
818
PROC.
GPS
RCR
KyBd
I/O
DISPLAY
820
TX-RCR
STORE
828
T1
T2
A
822
d1
d2
d3
C
824
T3
D
826

FIG. 14

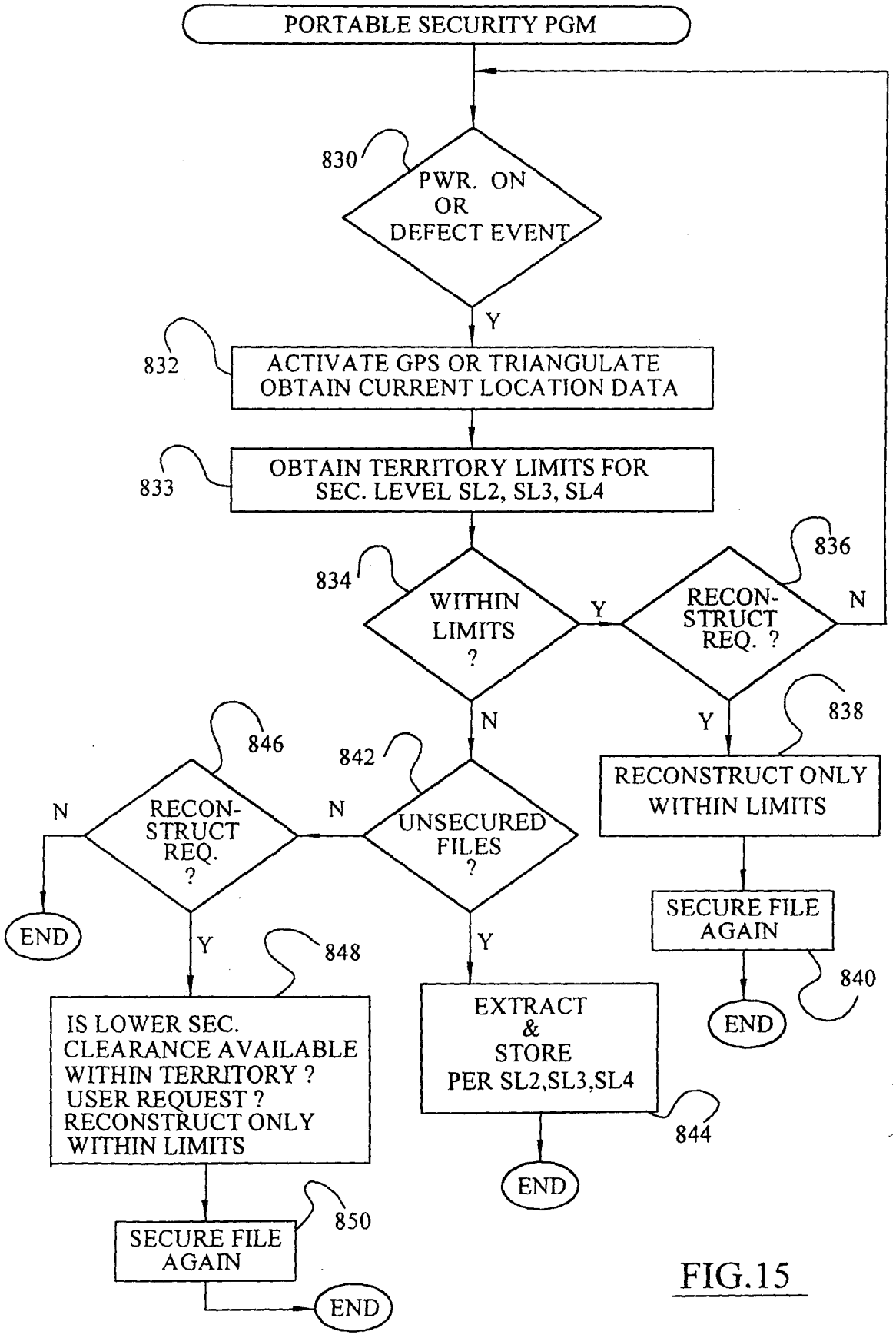

PORTABLE SECURITY PGM
830
PWR. ON OR DEFECT EVENT
Y
832
ACTIVATE GPS OR TRIANGULATE OBTAIN CURRENT LOCATION DATA
833
OBTAIN TERRITORY LIMITS FOR SEC. LEVEL SL2, SL3, SL4
834
WITHIN LIMITS ?
Y
836
RECON-STRUCT REQ. ?
N
Y
838
RECONSTRUCT ONLY WITHIN LIMITS
SECURE FILE AGAIN
840
END
N
842
UNSECURED FILES ?
N
846
RECON-STRUCT REQ. ?
N
END
Y
848
IS LOWER SEC. CLEARANCE AVAILABLE WITHIN TERRITORY ? USER REQUEST ? RECONSTRUCT ONLY WITHIN LIMITS
Y
EXTRACT & STORE PER SL2,SL3,SL4
844
END
SECURE FILE AGAIN
850
END

FIG.15

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

REQUEST FOR EXTENSION OF TIME

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a request for extension of time pursuant to 37 CFR §1.136. Please charge $60.00 for a one month extension of time pursuant to 37 CFR §1.17(a) to Deposit Account No. 03-1231 and please debit or credit any underpayment or overpayment to Deposit Account No. 03-1231.

Respectfully submitted,

By ___/Robert Kain / _____

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Mail Stop PGPUB Drawings, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 14, 2007.

____/Robert Kain/_____
Robert C. Kain, Jr.
Reg. No. 30,648

F:\RCK\CLIENTS\Redlich\6851-02-cip5-Req-Ext-Time-051007.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

TERMINAL DISCLAIMER

Commissioner for Patents
Alexandria, VA 22313-1450
Sir:

Petitioner, Digital Doors, Inc., a Florida corporation, having its principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, FL 33140, represents that it is the owner by assignment of all rights to application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004.

The captioned application was assigned to Digital Doors, Inc. and the assignment was filed with the original application. The evidentiary document accompanying or referred to in the instant terminal disclaimer has been reviewed by the undersigned and it is certified that to the best of assignee, Digital Doors, Inc.'s knowledge and belief, title is in the assignee.

Petitioner, Digital Doors, Inc., hereby disclaims the terminal part of any patent granted on the above identified application, which would extend beyond the expiration date of any patent granted on application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004, and, except as provided below, hereby agrees that any patent so granted on the above identified application shall be enforceable only for and during such period and that the listed patents will remain commonly owned.

Petitioner, Digital Doors, Inc., is a small entity.

Petitioner does not disclaim any terminal part of any patent granted on the above identified application prior to the expiration date of the full statutory term of any patent granted on application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004, in the event that any latter patent: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. §1.321(a), has all claims canceled by a reexamination certificate, is reissued, or is otherwise terminated prior to the expiration of its statutory term as presently shortened by any terminal disclaimer, except for the separation of legal title stated above.

Petitioner expressly reserves and does not waive the right to extend the term of any patent granted on application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004, or any patent granted on the above identified application under any statute which permits such an extension of term.

I hereby declare that all statements made herein of our own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Digital Doors, Inc.

Dated: __May 14, 2007

By: __/Robert C. Kain/ _____
Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

F:\RCK\CLIENTS\Redlich\6851-02-cip5-Term-Discl-051407.wpd

SPECIFICATION

[0001] This is a continuation-in-part of patent application no. 10/277,196 filed on ~~January 2, 2003~~ December 31, 2002 and patent application no. ~~10/115,192~~ 10/155,192 filed on May 23, 2002 and 10/155,525 filed on May 23, 2002, now U.S. Patent No. 7,191,252 and is a regular patent application claiming the benefit of provisional patent applications 60/400,062 filed on August 2, 2002, 60/400,112 filed on August 2, 2002, 60/400,406 filed on August 2, 2002, and 60/400,407 filed on August 2, 2002, and is a continuation-in-part of patent application no. 10/008,209 filed on December 6, 2001, now U.S. Patent No. 7,140,044, and 10/008,218 filed on December 6, 2001, now U.S. Patent No. 7,146,644, and is a continuation-in-part of patent application no. 09/916,397 filed July 27, 2001, now U.S. Patent No. 7,103,915, which is a regular patent application is based upon provisional patent application no. 60/260,398, filed ~~June 5, 2001~~ January 9, 2001 ; application no. 60/287,813, filed on May, 2, 2001; application no. 60/267,944, filed February 12, 2001; application no. 60/247,242, filed November 13, 2000 and application no. 60/247,232, filed November 13, 2000.

[0003] The extensive use of computers and the continued expansion of telecommunications networks, particularly the Internet, enable businesses, governments and individuals to create documents (whether text, characters, icons, images, data streams or a combination thereof, sound, video, and data objects in general, sometimes ~~identified~~ referred to generally herein as "data objects") and distribute those documents widely to others. Although the production, distribution and publication of documents is generally beneficial to society, there is a need to limit the distribution and publication of security sensitive words, characters or icons. Concerns regarding the privacy of

certain data (for example, an individual's social security number, credit history, medical history, business trade secrets and financial data) is an important issue in society. In another words, individuals and businesses have a greater concern regarding maintaining the secrecy of certain information in view of the increasing ease of distribution of documents through computer networks and the Internet.

[0008] U.S. Patent No. 6,192,472 B1 to Garay et al. discloses a method and apparatus for the secure distributed storage and retrieval of information. Garay '472 identifies the problem as how to store information in view of random hardware or telecommunications failures. Col. 1, lines 17-20. The initial solution is to replicate the stored data in multiple locations. Col. 1, lines 28-31. Another solution is to ~~disburse~~ disperse the information utilizing in Information ~~Disbursal~~ Dispersal Algorithm (IDA). The basic approach taking in IDA is to distribute the information F being stored among n active processors in such a way that the retrieval of F is possible even in the presence of up to t failed (inactive) processors. Col. 1, lines 40-44. Another issue is the utilization of cryptographic tools. With the use of tools called distributed fingerprints (hashes), the stored data is distributed using the fingerprints and coding functions to determine errors. In this way, the correct processors are able to reconstruct the fingerprint using the code's decoding function, check whether the pieces of the file F were correctly returned, and finally reconstruct F from the correct pieces using the IDA algorithm. Col. 2, lines 50-59. Garay '472 also discloses the use of Secure Storage and Retrieval of Information (SSRI) with the added requirement of confidentiality of information. Col. 3, line 56. With this added requirement, any collision of up to t processors (except ones including the rightful owner of the information) should not be able to learn anything about the

information. Confidentiality of information is easily achieved by encryption. Col. 3, lines 56-61. The issue involves encryption key management, that is, the safe deposit of cryptographic keys. Garay '472 discloses confidentiality protocol utilizing distributed key management features. This mechanism allows the user to keep his or her decryption key shared among several n servers in such a way that when the user wants to decrypt a given encrypted text, the user would have to interact with a single server (the gateway) to obtain the matching plaintext while none of the servers (including the gateway) gets any information about the plaintext. Col. 4, lines 5-14.

[0015] An article entitled "Survivable Information Storage Systems" by J. Wylie M. Bigrigg, J. Strunk, G. Ganger, H. Kiliccote, and P. Khosla, published August, 2000 in COMPUTER, pp. 61-67, discloses a PASIS architecture which combines decentralized storage system technologies, data redundancy and encoding and dynamic self-maintenance to create survivable information storage. The Bigrigg article states that to achieve survivability, storage systems must be decentralized and must spread information among independent storage nodes. The decentralized storage systems partition information among nodes using data distribution and redundancy schemes commonly associated with disc array system such as RAID (redundancy array of independent discs) insuring scalable performance for tolerance. P. 61. Thresholding schemes - also known as secret sharing schemes or information ~~disbursal~~ dispersal protocols - offer an alternative to these approaches which provide both information confidentiality and availability. These schemes and codes, replicate, and divide information to multiple pieces or shares that can be stored at different storage nodes. The system can only reconstruct the information when enough shares are available. P. 62. The PASIS architecture combines decentralized storage systems, data redundancy and encoding and dynamic

self-maintenance to achieve survivable information storage. The PASIS system uses threshold schemes to spread information across a decentralized collection of storage nodes. Client-side agents communicate with the collection of storage node to read and write information, hiding decentralization from the client system. P. 62. The device maintains unscrubable audit logs --that is, they cannot be erased by client-side intruders -- security personal can use the logs to partially identify the propagation of intruder-tainted information around the system. P. 63. The article states that, as with any distributed storage system, PASIS requires a mechanism that translates object names -- for example file names -- to storage locations. A directory service maps the names of information objects stored in a PASIS system to the names of the shares that comprised the information object. A share's name has two parts: the name of the storage node on which the share is located and the local name of the share on the storage node. A PASIS file system can embed the information needed for this translation in directory entries. P.63. To service a read request, the PASIS call client (a) looks up in the directory service the names of the n shares that comprise the object; (b) sends read requests to at least m of the n storage nodes; (c) collects the responses and continues to collect the responses until the client has collected m distinct shares; and (d) performs the appropriate threshold operation on the received shares to reconstruct the original information. P. 63. The p-m-n general threshold scheme breaks information into n shares so that (a) every shareholder has one of the n shares; (b) any m of the shareholders can reconstruct the information; and (c) a group of fewer than p shareholders gains no information. P. 64. Secret-sharing schemes ~~are m-m-n~~ are p-m-n threshold schemes that trade off information confidentiality and information availability: the higher the confidentiality guaranty, the more shares are required to reconstruct the original information object. Secret sharing schemes can be thought of as a combination of splitting

and replication techniques. P. 64. The article discusses the technique of ~~decimation~~ dissemination which divides information objects into n pieces and stores each piece separately. ~~Decimation~~ Dissemination decreases information availability because all shares must be available. It offers no information theoretic confidentiality because each share expresses 1/n of the original information. P. 64. Short secret sharing encrypts the original information with a random key, stores the encryption key using secret sharing, and stores the encrypted information using information disbursal. P. 64. An extension to the threshold schemes is cheater detection. In a threshold scheme that provides cheater detection, shares are constructed in such a fashion that a client reconstructing the original information object can tell, with high probability, whether any shares have been modified. This technique allows strong information integrity guarantees. Cheater detection can also be implemented using cryptographic techniques such as adding digest to information before storing it. P. 65. For the highest architecture to be effective as possible, it must make the full flexibility of threshold schemes available to clients. The article believes this option requires automated selection of appropriate threshold schemes on a per object basis. This selection would combine object characteristics and observations about the current system environment. For example, a client would use short secret sharing protocol to store an object larger than a particular size and conventional secret sharing protocol to store smaller objects. The size that determines which threshold scheme to use could be a function of object type, current system performance, or both. P. 67.

[0104] FIG. 1A diagrammatically illustrates the basic processes for establishing a secure storage of information, generally identified herein as "data." "Data," as used herein, includes any data object, e.g., text, images, icons, moving images, multiple images, data representing sound,

video, electronic streams of information, etc. Sound bites, data objects and video images may also be ~~extracted data~~ extracted as "data." A source document 100 containing data, sometimes referred to as a "plaintext," is passed through a filter 102. Although it is convenient to discuss and understand the invention herein in connection with a plaintext document, the document 100 is a data object. It is not limited to an electronic document representing words. The document 100 represents a data object that may be, e.g., text, images, icons, moving images, multiple images, data representing sound, video etc. The term "data object" as used in the claims is broadly defined as any item that can be represented in an electronic format such that the electronic format can be manipulated by a computer as described herein. The data object, or as discussed herein, the "plaintext" is sent to a filter. Filter 102, in a most basic sense, separates out common text or remainder data 104 from uncommon text, words, characters , icons or data objects. The security sensitive words, characters, icons or data objects are separated from remainder or common text 104 as extracted text 106. It should be noted that although the word "text" is utilized with respect to remainder text 104 and extracted text 106, ~~the text~~ the "text" is a data object and includes words, phrases, paragraphs, single characters, portions of words, characters, whole or partial images, icons, sound or video or data objects. In a basic implementation, filter 102 may utilize a dictionary such that words present in the dictionary (common words) are separated from the source plaintext document 100 and placed into remainder document or common data file 104. The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted data file 106. For example, a business may wish to impose a security system on a contract document such that the names of the contracting parties (not found in the dictionary) and the street names (not found in the dictionary) would be stored in extracted data text file 106. The

common text or remainder data would be stored in remainder data file 104. In the illustrated embodiment, remainder data file 104 also includes place holders which enables the extracted data to be easily inserted or set back into the remainder data file.

[0125] As stated earlier, the present data security system can be implemented on a single personal computer 140. In this case, different memory segments or hard drive 168 may be used for A-com and B-ext. Typically, PCs include a keyboard or data input device 161, a display 163, a central processing unit CPU 165, a video board 167 having video board memory 169, a fixed disc hard drive 168, a RAM 166, and input/output device 164, a removable memory ~~media floppy~~ media or floppy drive 162 and a removable compact disk (CD) read-write (CD-RW) device or drive 160. The system may include other removable disk drives, tape drives, or flash memory units. Internal units CPU 165, video board 167, hard drive 168, RAM 166 input/output device 164, floppy drive 162 and CD-ROM device 160 are all coupled together via an internal bus 171. Bus 171 represents a plurality of buses as is known to persons of ordinary skill in the art.

[0154] The system and the method may operate automatically in that the plaintext or originating data could be identified by a party desiring security. The system could obtain that data from any data input device (hard drive memory, floppy drive memory, flash card memory, personal data assistant (PDA), or any other type of data input device), filter the data, separate the extracted text or the remainder text, encrypt (or not encrypt) the data, separately store the extract and remainder data (all automatically, that is, without operator intervention). Hence, it is not necessary that the system operate with significant operator or manual intervention. Of course, the system may

also operate on a plaintext document or data object that is being created "in real time" by an operator and keyboard, mouse or other type of data input device. Since the present system can be configured to operate in real time, the system works on data packets of sensitive text, characters, icons, images or a combination thereof, sound, video, and data objects in general.

[0247] Decision step 834 determines whether location B of portable computing device 810 is within or without the predetermined territory limits or predetermined region. If YES, the system determines in decision step 836 whether the user has initiated a reconstruction request. If not, the system returns to a point preceding decision step 830, the detect event function or step. If YES, the system, in step 838, reconstructs the document only if location B is beyond a predetermined region. Of course, a negative operation could occur in that reconstruction would be prohibited if location B was within a predetermined region. The claims appended hereto are meant to cover both within a region and without a region and independently, extract or permit reconstruction. Step 840 secures the reconstructed file again as necessary. The term "beyond" includes both within a region or, if pre-programmed, without a region because the designated region may be "white," permitting (a) extraction at the transit over the regional boundaries or (b) reconstruction within the boundaries, or may be "black" forcing extraction automatically and prohibiting any reconstruction therein. Programmers know that white and black regions are interchangeable since the command to be executed could be a positive or a negative command (e.g, reconstruction permitted (white) vs. reconstruction not permitted (black)) .

Electronic Patent Application Fee Transmittal

Application Number:	10390807
Filing Date:	19-Mar-2003
Title of Invention:	Data security system and method for portable device
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-2-cip-5

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	60	60

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**60**

Electronic Acknowledgement Receipt

EFS ID:	1772946
Application Number:	10390807
International Application Number:	
Confirmation Number:	6441
Title of Invention:	Data security system and method for portable device
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-2-cip-5
Receipt Date:	14-MAY-2007
Filing Date:	19-MAR-2003
Time Stamp:	16:31:51
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$60
RAM confirmation Number	636
Deposit Account	031231
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Amendment - After Non-Final Rejection	6851-02-cip5-Amdt-1st-051007-trans.pdf	15026	no	1
Warnings:					
Information:					
2	Claims	6851-02-cip5-Amdt-1st-051007-clms.pdf	72149	no	34
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	6851-02-cip5-Amdt-1st-051007-rem.pdf	61420	no	19
Warnings:					
Information:					
4	Drawings	6851-02-cip5-dwg-050807.pdf	401176	no	20
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Extension of Time	6851-02-cip5-Req-Ext-Time-051007.pdf	29895	no	1
Warnings:					
Information:					
6	Terminal Disclaimer Filed	6851-02-cip5-Term-Discl-051407.pdf	113523	no	3
Warnings:					
Information:					
7	Specification	6851-02-cip5-Amdt-1st-051007-spec.pdf	30440	no	8
Warnings:					
Information:					
8	Fee Worksheet (PTO-06)	fee-info.pdf	8139	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	731768		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/390,807	03/19/2003	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	05/14/2007	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 169	Minus	** 169	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 7	Minus	***7	= 0	X $100 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
Wanda Meredith

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 07/02/2007

CBETANCO	SALE	#00000007	Mailroom Dt:	05/14/2007		031231	10390807
		01 FC : 2201		100.00 DA			
		02 FC : 2202		575.00 DA			

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Ron M. Redlich, et al.

Serial No.: 10/390,807

Filed: March 19, 2003

Confirmation No.: 6441

For: Data Security System and Method for Portable Device

TRANSMITTAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In further response to the Office Action dated March 19, 2007, attached please find the Supplemental Declaration and Power of Attorney for Patent Application.

I HEREBY CERTIFY that the below listed documents are being electronically filed on June 15, 2007 in the Patent and Trademark Office.

X Supplemental Declaration and Power of Attorney for Patent Application (2 pgs.)

X Please charge any underpayments or credit any overpayments to Deposit Account No. 03-1231.

Respectfully submitted,

By /Robert Kain/
Robert C. Kain, Jr.
Reg. No. 30,648
FLEIT, KAIN, GIBBONS, GUTMAN, BONGINI & BIANCO, P.L.
750 S.E. Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Facsimile: (954) 768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip5-Transmittal-Elec-Filing.wpd

SUPPLEMENTAL DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled Data Security System and Method For Portable Device the specification of which

(check one) ☐ is attached hereto.

☒ was filed on March 19, 2003

as Application Serial No. 10/390,807

and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
_____	_____	_____	☐	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
_____	_____	_____	☐	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

10/277,196	10/21/02	pending
(Application Serial No.)	(Filing Date)	(Status)
09/916,397	07/27/01	patented
(Application Serial No.)	(Filing Date)	(Status)
10/008,209	12/6/01	patented
(Application Serial No.)	(Filing Date)	(Status)
10/008,218	12/6/01	patented
(Application Serial No.)	(Filing Date)	(Status)
10/155,192	05/23/02	pending
(Application Serial No.)	(Filing Date)	(Status)
10/155,525	05/23/02	patented
(Application Serial No.)	(Filing Date)	(Status)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

60/260,398, filed Jan. 9, 2001 (Provisional Application No.) 60/287,813, filed May 2, 2001 (Provisional Application No.) 60/267,944, filed February 12, 2001 (Provisional Application No.)

60/247,242, filed November 13, 2000 (Provisional Application No.) 60/247,232, filed November 13, 2000 (Provisional Application No.) 60/400,062, filed August 2,2002 (Provisional Application No.)

60,400,112, filed August 2, 2002 (Provisional Application No.) 60/400,406, filed August 2, 2002 (Provisional Application No.) 60/400,407, filed August 2, 2002 (Provisional Application No.)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.
POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.
Robert C. Kain, Jr., Reg. No. 30,648; Martin Fleit, Reg. No. 16,900; Jon A. Gibbons, Reg. No. 37,333; Jose Gutman, Reg. No. 35,171; Steve Bongini, Reg. No. 40,917; and Paul D. Bianco, Reg. 43,5000.

Send Correspondence to: Robert C. Kain, Jr., **Customer Number 004897**
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Direct Telephone Calls to: Robert C. Kain, Jr., (954) 768-9002

Ron M. Redlich
Full name of sole or first inventor

Inventor's signature 06-11-2007 Date

Miami Beach, FL
Residence

U.S.
Citizenship

4201 Collins Avenue, Apt. 2103
Post Office Address

Miami Beach, FL 33140

Martin A. Nemzow
Full name of second joint inventor, if any

Inventor's signature 06-11-2007 Date

Miami Beach, FL
Residence

U.S.
Citizenship

2915 Flamingo Drive
Post Office Address

Miami Beach, FL 33140

(Supply similar information and signature for third and subsequent joint inventors.)

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip5-dec-050707.wpd

Electronic Acknowledgement Receipt

EFS ID:	1875951
Application Number:	10390807
International Application Number:	
Confirmation Number:	6441
Title of Invention:	Data security system and method for portable device
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-2-cip-5
Receipt Date:	15-JUN-2007
Filing Date:	19-MAR-2003
Time Stamp:	10:33:25
Application Type:	Utility

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	6851-02-cip5-Transmittal-Elec-Filing.pdf	15353	no	1
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Oath or Declaration filed	6851-02-cip5-Decl-ss.pdf	57990	no	2

Warnings:

Information:

Total Files Size (in bytes):	73343

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	03/19/2003	Ron M. Redlich	6851-2-cip-5	6441

4897 7590 06/22/2007

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
06/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of Non-Compliant Amendment (37 CFR 1.121)	Application No.	Applicant(s)	
	10/390,807	REDLICH ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

The amendment document filed on *14 May 2007* is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT:

- ☐ 1. Amendments to the specification:
  - ☐ A. Amended paragraph(s) do not include markings.
  - ☐ B. New paragraph(s) should not be underlined.
  - ☐ C. Other _____.
- ☐ 2. Abstract:
  - ☐ A. Not presented on a separate sheet. 37 CFR 1.72.
  - ☐ B. Other _____.
- ☐ 3. Amendments to the drawings:
  - ☐ A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).
  - ☐ B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.
  - ☐ C. Other _____.
- ☐ 4. Amendments to the claims:
  - ☐ A. A complete listing of all of the claims is not present.
  - ☐ B. The listing of claims does not include the text of all pending claims (including withdrawn claims)
  - ☐ C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).
  - ☐ D. The claims of this amendment paper have not been presented in ascending numerical order.
  - ☐ E. Other: _____.
- ☒ 5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4):
  The amendment ans certificate of e-Filing are unsigned.

For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance. If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.

2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a *Quayle* action. If any of above boxes 1. to 4. are checked, the correction required is only the **corrected section** of the non-compliant amendment in compliance with 37 CFR 1.121.

   Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.

   Failure to timely respond to this notice will result in:
   Abandonment of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or
   Non-entry of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

Legal Instruments Examiner (LIE), if applicable _____ Telephone No. _____

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

AMENDMENT

Commissioner for Patents
Alexandria, VA 22313-1450

This Amendment responds to the Office Action dated March 19, 2007. A Request for a One Month Extension of Time is concurrently filed herewith. If the $60.00 fee charged to Deposit Account no. 03-1231 is inadequate, please debit or credit Deposit Account no. 03-1231. Applicant adds new claims 147 - 172 to this application but cancels three (3) claims. Please charge Deposit Account no. 03-1231 for the $675.00 fee (one independent claim and a total of 23 newly added claims). Applicant submits a Terminal Disclaimer herewith. Please charge the $65.00 fee to Deposit Account no. 03-1231. If any fee is inadequate, please debit or credit Deposit Account no. 03-1231. The total fee to be charged is $800.00. This filing includes:

(a) Amendment Cover page - transmittal (1 pg., p. 1)

(b) Specification (8 pgs., pp. 2 - 9)

(c) Claims (34 pgs., pp. 10 - 43)

(d) Remarks (19 pgs., pp. 44 - 62)(includes Appendix Showing Support)

(e) Request for a One Month Extension of Time (1 pg.)

(f) Replacement Formal Drawings (21 pgs.)

(g) Terminal Disclaimer (3 pgs.)

SPECIFICATION

[0001] This is a continuation-in-part of patent application no. 10/277,196 filed on ~~January 2, 2003~~ December 31, 2002 and patent application no. ~~10/115,192~~ 10/155,192 filed on May 23, 2002 and 10/155,525 filed on May 23, 2002, now U.S. Patent No. 7,191,252 and is a regular patent application claiming the benefit of provisional patent applications 60/400,062 filed on August 2, 2002, 60/400,112 filed on August 2, 2002, 60/400,406 filed on August 2, 2002, and 60/400,407 filed on August 2, 2002, and is a continuation-in-part of patent application no. 10/008,209 filed on December 6, 2001, now U.S. Patent No. 7,140,044, and 10/008,218 filed on December 6, 2001, now U.S. Patent No. 7,146,644, and is a continuation-in-part of patent application no. 09/916,397 filed July 27, 2001, now U.S. Patent No. 7,103,915, which is a regular patent application is based upon provisional patent application no. 60/260,398, filed ~~June 5, 2001~~ January 9, 2001 ; application no. 60/287,813, filed on May, 2, 2001; application no. 60/267,944, filed February 12, 2001; application no. 60/247,242, filed November 13, 2000 and application no. 60/247,232, filed November 13, 2000.

[0003] The extensive use of computers and the continued expansion of telecommunications networks, particularly the Internet, enable businesses, governments and individuals to create documents (whether text, characters, icons, images, data streams or a combination thereof, sound, video, and data objects in general, sometimes ~~identified~~ referred to generally herein as "data objects") and distribute those documents widely to others. Although the production, distribution and publication of documents is generally beneficial to society, there is a need to limit the distribution and publication of security sensitive words, characters or icons. Concerns regarding the privacy of

certain data (for example, an individual's social security number, credit history, medical history, business trade secrets and financial data) is an important issue in society. In another words, individuals and businesses have a greater concern regarding maintaining the secrecy of certain information in view of the increasing ease of distribution of documents through computer networks and the Internet.

[0008] U.S. Patent No. 6,192,472 B1 to Garay et al. discloses a method and apparatus for the secure distributed storage and retrieval of information. Garay '472 identifies the problem as how to store information in view of random hardware or telecommunications failures. Col. 1, lines 17-20. The initial solution is to replicate the stored data in multiple locations. Col. 1, lines 28-31. Another solution is to ~~disburse~~ disperse the information utilizing in Information ~~Disbursal~~ Dispersal Algorithm (IDA). The basic approach taking in IDA is to distribute the information F being stored among n active processors in such a way that the retrieval of F is possible even in the presence of up to t failed (inactive) processors. Col. 1, lines 40-44. Another issue is the utilization of cryptographic tools. With the use of tools called distributed fingerprints (hashes), the stored data is distributed using the fingerprints and coding functions to determine errors. In this way, the correct processors are able to reconstruct the fingerprint using the code's decoding function, check whether the pieces of the file F were correctly returned, and finally reconstruct F from the correct pieces using the IDA algorithm. Col. 2, lines 50-59. Garay '472 also discloses the use of Secure Storage and Retrieval of Information (SSRI) with the added requirement of confidentiality of information. Col. 3, line 56. With this added requirement, any collision of up to t processors (except ones including the rightful owner of the information) should not be able to learn anything about the

information. Confidentiality of information is easily achieved by encryption. Col. 3, lines 56-61. The issue involves encryption key management, that is, the safe deposit of cryptographic keys. Garay '472 discloses confidentiality protocol utilizing distributed key management features. This mechanism allows the user to keep his or her decryption key shared among several n servers in such a way that when the user wants to decrypt a given encrypted text, the user would have to interact with a single server (the gateway) to obtain the matching plaintext while none of the servers (including the gateway) gets any information about the plaintext. Col. 4, lines 5-14.

[0015] An article entitled "Survivable Information Storage Systems" by J. Wylie M. Bigrigg, J. Strunk, G. Ganger, H. Kiliccote, and P. Khosla, published August, 2000 in COMPUTER, pp. 61-67, discloses a PASIS architecture which combines decentralized storage system technologies, data redundancy and encoding and dynamic self-maintenance to create survivable information storage. The Bigrigg article states that to achieve survivability, storage systems must be decentralized and must spread information among independent storage nodes. The decentralized storage systems partition information among nodes using data distribution and redundancy schemes commonly associated with disc array system such as RAID (redundancy array of independent discs) insuring scalable performance for tolerance. P. 61. Thresholding schemes - also known as secret sharing schemes or information ~~disbursal~~ dispersal protocols - offer an alternative to these approaches which provide both information confidentiality and availability. These schemes and codes, replicate, and divide information to multiple pieces or shares that can be stored at different storage nodes. The system can only reconstruct the information when enough shares are available. P. 62. The PASIS architecture combines decentralized storage systems, data redundancy and encoding and dynamic

self-maintenance to achieve survivable information storage. The PASIS system uses threshold schemes to spread information across a decentralized collection of storage nodes. Client-side agents communicate with the collection of storage node to read and write information, hiding decentralization from the client system. P. 62. The device maintains unscrubable audit logs --that is, they cannot be erased by client-side intruders -- security personal can use the logs to partially identify the propagation of intruder-tainted information around the system. P. 63. The article states that, as with any distributed storage system, PASIS requires a mechanism that translates object names -- for example file names -- to storage locations. A directory service maps the names of information objects stored in a PASIS system to the names of the shares that comprised the information object. A share's name has two parts: the name of the storage node on which the share is located and the local name of the share on the storage node. A PASIS file system can embed the information needed for this translation in directory entries. P.63. To service a read request, the PASIS call client (a) looks up in the directory service the names of the n shares that comprise the object; (b) sends read requests to at least m of the n storage nodes; (c) collects the responses and continues to collect the responses until the client has collected m distinct shares; and (d) performs the appropriate threshold operation on the received shares to reconstruct the original information. P. 63. The p-m-n general threshold scheme breaks information into n shares so that (a) every shareholder has one of the n shares; (b) any m of the shareholders can reconstruct the information; and (c) a group of fewer than p shareholders gains no information. P. 64. Secret-sharing schemes ~~are m-m-n~~ are p-m-n threshold schemes that trade off information confidentiality and information availability: the higher the confidentiality guaranty, the more shares are required to reconstruct the original information object. Secret sharing schemes can be thought of as a combination of splitting

and replication techniques. P. 64. The article discusses the technique of ~~decimation~~ dissemination which divides information objects into n pieces and stores each piece separately. ~~Decimation~~ Dissemination decreases information availability because all shares must be available. It offers no information theoretic confidentiality because each share expresses 1/n of the original information. P. 64. Short secret sharing encrypts the original information with a random key, stores the encryption key using secret sharing, and stores the encrypted information using information disbursal. P. 64. An extension to the threshold schemes is cheater detection. In a threshold scheme that provides cheater detection, shares are constructed in such a fashion that a client reconstructing the original information object can tell, with high probability, whether any shares have been modified. This technique allows strong information integrity guarantees. Cheater detection can also be implemented using cryptographic techniques such as adding digest to information before storing it. P. 65. For the highest architecture to be effective as possible, it must make the full flexibility of threshold schemes available to clients. The article believes this option requires automated selection of appropriate threshold schemes on a per object basis. This selection would combine object characteristics and observations about the current system environment. For example, a client would use short secret sharing protocol to store an object larger than a particular size and conventional secret sharing protocol to store smaller objects. The size that determines which threshold scheme to use could be a function of object type, current system performance, or both. P. 67.

[0104] FIG. 1A diagrammatically illustrates the basic processes for establishing a secure storage of information, generally identified herein as "data." "Data," as used herein, includes any data object, e.g., text, images, icons, moving images, multiple images, data representing sound,

video, electronic streams of information, etc. Sound bites, data objects and video images may also be ~~extracted data~~ extracted as "data." A source document 100 containing data, sometimes referred to as a "plaintext," is passed through a filter 102. Although it is convenient to discuss and understand the invention herein in connection with a plaintext document, the document 100 is a data object. It is not limited to an electronic document representing words. The document 100 represents a data object that may be, e.g., text, images, icons, moving images, multiple images, data representing sound, video etc. The term "data object" as used in the claims is broadly defined as any item that can be represented in an electronic format such that the electronic format can be manipulated by a computer as described herein. The data object, or as discussed herein, the "plaintext" is sent to a filter. Filter 102, in a most basic sense, separates out common text or remainder data 104 from uncommon text, words, characters , icons or data objects. The security sensitive words, characters, icons or data objects are separated from remainder or common text 104 as extracted text 106. It should be noted that although the word "text" is utilized with respect to remainder text 104 and extracted text 106, ~~the text~~ the "text" is a data object and includes words, phrases, paragraphs, single characters, portions of words, characters, whole or partial images, icons, sound or video or data objects. In a basic implementation, filter 102 may utilize a dictionary such that words present in the dictionary (common words) are separated from the source plaintext document 100 and placed into remainder document or common data file 104. The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted data file 106. For example, a business may wish to impose a security system on a contract document such that the names of the contracting parties (not found in the dictionary) and the street names (not found in the dictionary) would be stored in extracted data text file 106. The

common text or remainder data would be stored in remainder data file 104. In the illustrated embodiment, remainder data file 104 also includes place holders which enables the extracted data to be easily inserted or set back into the remainder data file.

[0125] As stated earlier, the present data security system can be implemented on a single personal computer 140. In this case, different memory segments or hard drive 168 may be used for A-com and B-ext. Typically, PCs include a keyboard or data input device 161, a display 163, a central processing unit CPU 165, a video board 167 having video board memory 169, a fixed disc hard drive 168, a RAM 166, and input/output device 164, a removable memory ~~media floppy~~ media or floppy drive 162 and a removable compact disk (CD) read-write (CD-RW) device or drive 160. The system may include other removable disk drives, tape drives, or flash memory units. Internal units CPU 165, video board 167, hard drive 168, RAM 166 input/output device 164, floppy drive 162 and CD-ROM device 160 are all coupled together via an internal bus 171. Bus 171 represents a plurality of buses as is known to persons of ordinary skill in the art.

[0154] The system and the method may operate automatically in that the plaintext or originating data could be identified by a party desiring security. The system could obtain that data from any data input device (hard drive memory, floppy drive memory, flash card memory, personal data assistant (PDA), or any other type of data input device), filter the data, separate the extracted text or the remainder text, encrypt (or not encrypt) the data, separately store the extract and remainder data (all automatically, that is, without operator intervention). Hence, it is not necessary that the system operate with significant operator or manual intervention. Of course, the system may

also operate on a plaintext document or data object that is being created "in real time" by an operator and keyboard, mouse or other type of data input device. Since the present system can be configured to operate in real time, the system works on data packets of sensitive text, characters, icons, images or a combination thereof, sound, video, and data objects in general.

[0247] Decision step 834 determines whether location B of portable computing device 810 is within or without the predetermined territory limits or predetermined region. If YES, the system determines in decision step 836 whether the user has initiated a reconstruction request. If not, the system returns to a point preceding decision step 830, the detect event function or step. If YES, the system, in step 838, reconstructs the document only if location B is beyond a predetermined region. Of course, a negative operation could occur in that reconstruction would be prohibited if location B was within a predetermined region. The claims appended hereto are meant to cover both within a region and without a region and independently, extract or permit reconstruction. Step 840 secures the reconstructed file again as necessary. The term "beyond" includes both within a region or, if pre-programmed, without a region because the designated region may be "white," permitting (a) extraction at the transit over the regional boundaries or (b) reconstruction within the boundaries, or may be "black" forcing extraction automatically and prohibiting any reconstruction therein. Programmers know that white and black regions are interchangeable since the command to be executed could be a positive or a negative command (e.g, reconstruction permitted (white) vs. reconstruction not permitted (black)) .

CLAIMS

1. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

2. (currently amended) A method for securing data as claimed in claim 1 wherein said ~~substantially~~ current location data is generated with the acquisition of a global positioning signal.

3. (currently amended) A method for securing data as claimed in claim 1 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

4. (currently amended) A method for securing data as claimed in claim 1 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

5. (currently amended) A method for securing data as claimed in claim 4 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

6. (currently amended) A method for securing data as claimed in claim 1 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

7. (original) A method for securing data as claimed in claim 6 wherein said transmitting occurs as a wireless data transmission.

8. (currently amended) A method for securing data as claimed in claim 7 including encrypting said corresponding extracted data prior to transmitting.

9. (currently amended) A method for securing data as claimed in claim 6 including receiving said corresponding extracted data as necessary during reconstruction.

10. (currently amended) A method for securing data as claimed in claim 1 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon

respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

11. (original) A method for securing data as claimed in claim 1 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

12. (original) A method for securing data as claimed in claim 11 wherein the step of obtaining occurs before the step of determining.

13. (original) A method for securing data as claimed in claim 1 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

14. (original) A method for securing data as claimed in claim 1 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

15. (original) A method for securing data as claimed in claim 1 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

16. (currently amended) A method of securing data as claimed in claim 1 wherein ~~said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are~~

~~utilized only in the presence of a respective predetermined security level of said plurality of security levels~~ said predetermined region is one a plurality of regions which includes at least one security protocol extraction region and at least one security protocol reconstruction region, the step of determining determines when said portable computing device is beyond at least one security protocol extraction region and applies the respective protocol to said data, and the step of determining further determines when said portable computing device is beyond at least one security protocol reconstruction region and applies the respective protocol to full or partial reconstruction of said data.

17. (currently amended) A method of securing data as claimed in claim 16 wherein said predetermined security clearance is one of a plurality of security clearances, said plurality of security levels is associated with corresponding degrees of encryption, ~~as are said subsets of extracted data,~~ the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

18. (currently amended) A method of securing data as claimed in claim 17 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

19. (currently amended) A method as claimed in claim 16 wherein said predetermined security clearance is one of a plurality of security clearances, the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

20. (original) A method of securing data as claimed in claim 1 operating over a plurality of computers interconnected together.

21. (original) A method for securing data as claimed in claim 1 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

22. (original) A method of securing data as claimed in claim 1 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

23. (original) A method as claimed in claim 1 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

24. (original) A method as claimed in claim 1 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

25. (currently amended) A method for securing data as claimed in ~~claim 1~~ claim 2 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

26. (currently amended) A method for securing data as claimed in claim 25 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

27. (currently amended) A method for securing data as claimed in claim 26 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

28. (currently amended) A method for securing data as claimed in ~~claim 27~~ claim 3 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

29. (original) A method for securing data as claimed in claim 28 wherein said transmitting occurs as a wireless data transmission.

30. (currently amended) A method for securing data as claimed in claim 29 including encrypting said corresponding extracted data prior to transmitting.

31. (currently amended) A method for securing data as claimed in claim 30 including receiving said corresponding extracted data as necessary during reconstruction.

32. (currently amended) A method for securing data as claimed in ~~claim 31~~ claim 3 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

33. (original) A method for securing data as claimed in claim 31 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

34. (original) A method for securing data as claimed in claim 33 wherein the step of obtaining occurs before the step of determining.

35. (original) A method for securing data as claimed in claim 34 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

36. (original) A method for securing data as claimed in claim 34 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

37. (original) A method for securing data as claimed in claim 36 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

38. (cancelled without prejudice to reinstate the same at a later time, i.e., without disclaimer)

39. (currently amended) A method of securing data as claimed in ~~claim 38~~ claim 37 wherein said predetermined security clearance is one of a plurality of security clearances, said plurality of security levels is associated with corresponding degrees of encryption, ~~as are said subsets of extracted data,~~ the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting,

during the reconstruction, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

40. (currently amended) A method of securing data as claimed in claim 39 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

41. (currently amended) A method as claimed in claim 40 wherein said predetermined security clearance is one of a plurality of security clearances, the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

42. (original) A method of securing data as claimed in claim 41 operating over a plurality of computers interconnected together.

43. (original) A method for securing data as claimed in claim 42 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

44. (original) A method of securing data as claimed in claim 43 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

45. (original) A method as claimed in claim 44 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

46. (original) A method as claimed in claim 44 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid

displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

47. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

when said portable computing device is not beyond said predetermined region, permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data in the presence of a predetermined security clearance access control corresponding to said respective security level .

48. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with

security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, extracting said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store~~ in respective extract stores corresponding to a respective security level of said extract stores.

49. (currently amended) A method for securing data as claimed in claim 48 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

50. (currently amended) A method for securing data as claimed in claim 48 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

51. (currently amended) A method for securing data as claimed in claim 50 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

52. (currently amended) A method for securing data as claimed in claim 48 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

53. (original) A method for securing data as claimed in claim 52 wherein said transmitting occurs as a wireless data transmission.

54. (currently amended) A method for securing data as claimed in claim 53 including encrypting said corresponding extracted data prior to transmitting.

55. (currently amended) A method for securing data as claimed in claim 48 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction occurs or said ~~and~~ storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

56. (original) A method for securing data as claimed in claim 48 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

57. (original) A method for securing data as claimed in claim 56 wherein the step of obtaining occurs before the step of determining.

58. (original) A method for securing data as claimed in claim 48 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

59. (original) A method for securing data as claimed in claim 48 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

60. (currently amended) A method for securing data as claimed in claim 48 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary. ~~during reconstruction~~.

61. (cancelled without prejudice to reinstate the same at a later time, i.e., without disclaimer)

62. (currently amended) A method of securing data as claimed in ~~claim 61~~ claim 48 wherein said respective security level is one of a ~~said~~ plurality of security levels ~~is~~ associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels.

63. (currently amended) A method of securing data as claimed in claim 62 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

64. (original) A method of securing data as claimed in claim 48 operating over a plurality of computers interconnected together.

65. (original) A method for securing data as claimed in claim 48 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

66. (original) A method of securing data as claimed in claim 48 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

67. (currently amended) A method for securing data as claimed in claim 49 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

68. (currently amended) A method for securing data as claimed in claim 67 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

69. (currently amended) A method for securing data as claimed in claim 49 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

70. (original) A method for securing data as claimed in claim 69 wherein said transmitting occurs as a wireless data transmission.

71. (currently amended) A method for securing data as claimed in claim 70 including encrypting said corresponding extracted data prior to transmitting.

72. (currently amended) A method for securing data as claimed in claim 71 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

73. (original) A method for securing data as claimed in claim 72 wherein said plurality of predetermined regions is a plurality of mobile predetermined region and the method includes obtaining data representing said plurality of mobile predetermined region.

74. (original) A method for securing data as claimed in claim 73 wherein the step of obtaining occurs before the step of determining.

75. (original) A method for securing data as claimed in claim 74 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

76. (original) A method for securing data as claimed in claim 74 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

77. (original) A method for securing data as claimed in claim 74 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

78. (cancelled without prejudice to reinstate the same at a later time, i.e., without disclaimer)

79. (currently amended) A method of securing data as claimed in ~~claim 78~~ claim 74 wherein said respective security level is one of a ~~said~~ plurality of security levels ~~is~~ associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels.

80. (currently amended) A method of securing data as claimed in claim 79 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

81. (original) A method of securing data as claimed in claim 80 operating over a plurality of computers interconnected together.

82. (original) A method for securing data as claimed in claim 81 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

83. (original) A method of securing data as claimed in claim 82 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

84. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores , ~~said extract store and said remainder store, respectively,~~ said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is within a predetermined region based upon said current location data;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

85. (currently amended) A computer readable medium ~~containing~~ encoded with programming instructions for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective

~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, the programming instructions comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, permitting extraction of said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

86. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein said ~~substantially~~ current location data is generated with the acquisition of a global positioning signal.

87. (currently amended) A computer readable medium with programming steps as claimed in claim 85 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

88. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

89. (currently amended) A computer readable medium with programming steps as claimed in claim 88 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a flash memory drive, a tape drive and a read-write CD-ROM drive.

90. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

91. (original) A computer readable medium with programming steps as claimed in claim 90 wherein said transmitting occurs as a wireless data transmission.

92. (currently amended) A computer readable medium with programming steps as claimed in claim 91 including encrypting said corresponding extracted data prior to transmitting.

93. (currently amended) A computer readable medium with programming steps as claimed in claim 90 including receiving said corresponding extracted data as necessary during reconstruction.

94. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said reconstruction

is permitted based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

95. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

96. (original) A computer readable medium with programming steps as claimed in claim 95 wherein the step of obtaining occurs before the step of determining.

97. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

98. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

99. (original) A computer readable medium with programming steps as claimed in claim 85 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary during reconstruction.

100. (currently amended) A computer readable medium with programming steps as claimed in claim 85 wherein said respective security level is ~~predetermined security level is~~ one of a plurality of security levels operative during recoonstruction.~~, said extracting extracts said security sensitive~~

~~words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels~~ .

101. (currently amended) A computer readable medium with programming steps as claimed in claim 100 wherein said plurality of security levels is associated with corresponding degrees of encryption ~~as are said subsets of~~ for said extracted data, the method including encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including decrypting, during the reconstruction, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

102. (currently amended) A computer readable medium with programming steps as claimed in claim 101 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

103. (original) A computer readable medium with programming steps as claimed in claim 100 wherein the step of reconstruction includes the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

104. (original) A computer readable medium with programming steps as claimed in claim 85 configured to operate over a plurality of computers interconnected together.

105. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

106. (original) A computer readable medium with programming steps as claimed in claim 85 wherein the step of extracting utilizes one of an inference engine, neural network and artificial intelligence process.

107. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

108. (original) A computer readable medium with programming steps as claimed in claim 85 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

109. (currently amended) A computer readable medium encoded with programming steps for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, the programming steps comprising:

determining when said portable computing device is beyond a predetermined region based upon said current location data;

when said portable computing device is beyond said predetermined region, extracting said security sensitive words, characters, data objects or icons from said data to obtain extracted data and

remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store~~ in respective extract stores corresponding to a respective security level of said extract stores .

110. (currently amended) A computer readable medium with programming steps as claimed in claim 109 including acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

111. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein ~~said extract store~~ one of said plurality of extract stores is operable in a local data drive on said portable computing device and said storing therein occurs on said local data drive.

112. (currently amended) A computer readable medium with programming steps as claimed in claim 111 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive.

113. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein ~~said extract store~~ one of said plurality of extract stores is a remote memory and the method includes transmitting ~~said~~ corresponding extracted data to the remote extract store.

114. (original) A computer readable medium with programming steps as claimed in claim 113 including encrypting said extracted data prior to transmitting.

115. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein said predetermined region is one a plurality of regions, the step of determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said extraction ~~and storage~~ occurs or said storage occurs based upon the location of said portable computing device beyond said respective ones of said plurality of regions.

116. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said predetermined region is a mobile predetermined region and the method includes obtaining data representing said mobile predetermined region.

117. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said data is a map with security sensitive icons associated therewith, said security sensitive icons being extracted from said map when said portable computing device is beyond said predetermined region.

118. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said data is a document file with security sensitive credit card data characters associated therewith, said security sensitive credit card data characters being extracted from said document file when said portable computing device is beyond said predetermined region.

119. (currently amended) A computer readable medium with programming steps as claimed in claim 109 including encrypting said extracted data before or during said storage and decrypting said extracted data as necessary. ~~during reconstruction.~~

120. (currently amended) A computer readable medium with programming steps as claimed in claim 109 wherein ~~said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with a plurality of security levels~~ said respective security level is one of a plurality of security levels associated with said respective extract stores.

121. (currently amended) A computer readable medium with programming steps as claimed in claim 120 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the method including encrypting said ~~subsets of~~

extracted data with corresponding degrees of encryption associated with said plurality of security levels.

122. (currently amended) A computer readable medium with programming steps as claimed in claim 121 including encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

123. (original) A computer readable medium with programming steps as claimed in claim 109 wherein said determining, extracting and storing occurs either automatically or upon power up of said at least one portable computing device.

124. (currently amended) An information processing system for securing data having one or more security sensitive words, characters, data objects or icons in a computer system a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

means for determining when said portable computing device is beyond a predetermined region based upon said current location data;

means for extracting, coupled to said means for determining, said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store, respectively~~ in respective extract stores corresponding to a respective security level of said extract stores;

means for permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance

access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

125. (currently amended) An information processing system as claimed in claim 124 including a global positioning signal generator, said ~~substantially~~ current location data being generated by said global positioning signal generator and applied to said means for determining.

126. (currently amended) An information processing system as claimed in claim 124 including means for acquiring said ~~substantially~~ current location data with one of the acquisition of a global positioning signal or the acquisition of triangulation data.

127. (currently amended) An information processing system as claimed in claim 124 wherein said portable computing device includes a local data drive and local drive media as one of said respective extract stores, said means for extracting storing said security sensitive words, characters, data objects or icons on said media in said local data drive.

128. (currently amended) An information processing system as claimed in claim 127 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a removable hard drive, a flash memory drive, a tape drive and a read-write CD-ROM drive.

129. (currently amended) An information processing system as claimed in claim 124 including a remote memory as one of said plurality of extract stores in said computer system, said portable computing device including a data transmitter, said means for extracting storing said security sensitive words, characters, data objects or icons in said remote memory via said data transmitter.

130. (original) An information processing system as claimed in claim 129 wherein said data transmitter transmits data via a wireless communications channel.

131. (currently amended) An information processing system as claimed in claim 130 including means for encrypting ~~said~~ corresponding extracted data prior to transmitting.

132. (currently amended) An information processing system as claimed in claim 129 including means for receiving said corresponding extracted data as necessary during reconstruction.

133. (original) An information processing system as claimed in claim 124 wherein said predetermined security clearance is one of a plurality of security clearances and said predetermined region is one a plurality of regions, said plurality of security clearances associated with respective ones of said plurality of regions, the means for determining determines when said portable computing device is beyond said respective ones of said plurality of regions, said means for extracting and storing being triggered based upon the location of said portable computing device beyond said respective ones of said plurality of regions, and said means for reconstructing being activated based upon respective security clearances and based upon the location of said portable computing device not being beyond predetermined respective ones of regions of said plurality of regions.

134. (original) An information processing system as claimed in claim 124 wherein said predetermined region is a mobile predetermined region and the system includes means for obtaining data representing said mobile predetermined region.

135. (original) An information processing system as claimed in claim 124 wherein said data is a map with security sensitive icons associated therewith, said means for extracting acting upon said map and extracting said security sensitive icons from said map when said portable computing device is beyond said predetermined region.

136. (original) An information processing system as claimed in claim 124 wherein said data is a document file with security sensitive credit card data characters associated therewith, said means for extracting acting upon said security sensitive credit card data characters and extracting the same from said document file when said portable computing device is beyond said predetermined region.

137. (currently amended) An information processing system as claimed in claim 124 including means for encrypting ~~said~~ corresponding extracted data before or during said storage and means for decrypting said corresponding extracted data as necessary during reconstruction by said means for reconstructing.

138. (currently amended) An information processing system as claimed in claim 124 wherein said predetermined security level is one of a plurality of security levels, each associated with a corresponding extract store, ~~said means for extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels,~~ and said means for reconstructing acts upon some or all of said ~~subsets of~~ extracted data only in the presence of a respective predetermined security level of said plurality of security levels.

139. (currently amended) An information processing system as claimed in claim 138 wherein said plurality of security levels is associated with corresponding degrees of encryption as are said ~~subsets of~~ extracted data, the system including means for encrypting said ~~subsets of~~ extracted data with corresponding degrees of encryption associated with said plurality of security levels, and including means for decrypting, during reconstruction with said means for reconstructing, of some or all of said ~~subsets of~~ extracted data only in the presence of said predetermined security level of said plurality of security levels.

140. (currently amended) An information processing system as claimed in claim 139 including means for encrypting said ~~subsets of~~ extracted data and remainder data prior to storing.

141. (original) An information processing system as claimed in claim 138 wherein said means for reconstructing permits a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

142. (original) An information processing system as claimed in claim 124 utilizing a plurality of computers interconnected together.

143. (original) An information processing system as claimed in claim 124 including an automatic means for determining and means for extracting and storing actuated upon power up or geographic location of said at least one portable computing device.

144. (original) An information processing system as claimed in claim 124 wherein said portable computing device is a computer which includes a display fed from video memory having a plurality of frame memory segments, the means for reconstructing interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments.

145. (original) An information processing system as claimed in claim 124 wherein said portable computing device is a computer which includes a data display system with at least two separate but visually overlaid displays, the means for reconstructing including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

146. (currently amended) An information processing system for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~

extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

means for determining when said portable computing device is beyond a predetermined region based upon said current location data and generating a trigger;

means for extracting, upon said trigger ~~when said portable computing device is beyond said predetermined region~~, said security sensitive words, characters, data objects or icons from said data to obtain extracted data and remainder data therefrom and storing said extracted data ~~and said remainder data in said extract store and said remainder store~~ in respective extract stores corresponding to a respective security level of said extract stores.

147. (new) A computerized method of securing data in a plurality of security controlled data stores with access controls thereat, said data potentially having sensitive content such as sensitive words, data objects, characters, images, data elements or icons, comprising:

storing separately sensitive content in secure data stores of said plurality of security data stores;

permitting reconstruction of some or all of said data with appropriate access controls applied to respective secure data stores; and

said storing or reconstruction based upon territorial protocol and a geographic location signal or a triggering event.

148. (new) A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering or extracting said sensitive content in said secure data stores.

149. (new) A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of removing or copying said sensitive content in said secure data stores.

150. (new) A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering and transferring or extracting and transferring said sensitive content in said secure data stores.

151. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or both of partially or completely storing said sensitive content in said secure data stores.

152. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes partially or completely storing said sensitive content in said secure data stores with at least one of encryption or parsing of data.

153. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores.

154. (new) A computerized method of securing data as claimed in claim 147 including manually or automatically at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores.

155. (new) A computerized method of securing data as claimed in claim 147 including at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; and wherein

said sensitive content has different levels of sensitive content therein corresponding to respective ones of said secure data stores.

156. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is defined as at least one of security sensitive content, content of significance, trade secret content, personal identifying information, content subject to regulatory provisions, or back-up content and said respective ones of said secure data stores are correspondingly designated as at least one of security sensitive stores, stores for content of significance, trade secret stores, personal identifying information stores, regulatory provision stores, or back-up stores.

157. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes at least one or more of storing in predetermined security data stores, storing in a predetermined manner by random selection of security data stores, storing by data class in said security data stores, storing data by data type in said security data stores, or storing by level of security in said security data stores.

158. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in said security data stores in a predetermined manner with an algorithmic selection.

159. (new) A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in optical media data stores.

160. (new) A computerized method of securing data as claimed in claim 147 wherein storing of said sensitive content is done separately with respect to at least one of remainder data, left-over data,

non-sensitive content data, surplus data, residue data, remnant data, or data complementary to sensitive content data.

161. (new) A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution, regeneration, compilation, reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores.

162. (new) A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes the use of at least one of predetermined access controls, assigned access controls, access controls generated with said storing of said secure data, or access controls and encryption.

163. (new) A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution, regeneration, compilation, reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores.

164. (new) A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to respective secure data stores in at least one of the following manners:

said access controls applied sequentially to respective secure data stores;

said access controls applied concurrently to respective secure data stores;

said access controls applied to respective secure data stores subsequent to application of a security protocol;

said secure data stores are mapped and said access controls are applied to obtain the mapped secure data stores; or

said access controls are applied subsequent to an exchange of compensation or an exchange of data.

said access controls applied to respective secure data stores subsequent to application of a hierarchical security protocol.

165. (new) A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to at least one or more of predetermined respective secure data stores, associated respective secure data stores, correlated respective secure data stores, or designated respective secure data stores.

166. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores.

167. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores.

168. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores.

169. (new) A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and

said server controlling the application of said access controls.

170. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

select sensitive words, data objects, characters, images, data elements or icons;

defined sensitive words, data objects, characters, images, data elements or icons;

known sensitive words, data objects, characters, images, data elements or icons;

certain sensitive words, data objects, characters, images, data elements or icons;

a collection of sensitive words, data objects, characters, images, data elements or icons;

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons; or

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons having different hierarchal or orthogonal levels of sensitive content.

171. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

portions of predetermined sensitive words, data objects, characters, images, data elements or icon

s; or

words, data objects, characters, images, data elements or icons which are not from a plurality of predetermined words, data objects, characters, images, data elements or icons.

172. (new) A computerized method of securing data as claimed in claim 147 wherein said sensitive content is related to sensitive words, data objects, characters, images, data elements or icons, by at least or more of a function or a meaning.

REMARKS

This Amendment responds to the Office Action dated March 19, 2007.

Applicant has amended the patent specification to correct spelling errors and to clarify certain items. Support for changes in substance are found in the specification at the following locations: in ¶ 003, see ¶ 104 (also subject to amendment herein); in ¶ 104, see reference to "data object" in that same ¶; in ¶ 154, see that same ¶; and, in ¶ 247, see that same ¶. No new matter is introduced into the application by these changes to the specification.

With respect to ¶ 001, Applicant requests that the priority of this application be changed as noted in ¶ 001. A Supplemental Declaration will be filed in the future to conform to the changes in priority.

Replacement formal drawings are submitted herewith. In FIG. 3, the numerals 226 and 228 have been reversed to conform to the specification.

Applicant has added new claims 148 - 172. Support for these claims is set forth in the attached Appendix. No new matter is added to this case by the addition of these claims. Support for the substantive changes to claims 1 - 147 are also shown in the Appendix.

In the Office Action, the examiner stated that claims 25 and 3 are similar. Applicant has amended claim 25 to depend from claim 2 which changes the scope of the claim.

In the Office Action, the examiner indicated that claims 26 and 28 conflict relative to local storage. Claim 28 is amended and is now dependent upon claim 3 which does not refer to local data storage.

In the Office Action, the examiner objected to the word "substantially" in the claims. The claims have been amended to delete this word.

In the Office Action, the examiner indicated that claims 85 - 123 were not statutory subject matter. Independent claim 85 has been amended as follows:

> 85. (currently amended) A computer readable medium ~~containing~~ encoded with programming instructions for securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, the programming instructions comprising:
> determining when said portable computing device is beyond a predetermined region based upon said current location data; ...

The PTO Guidelines regarding statutory subject matter indicate that:

> Functional descriptive material claimed in combination with an appropriate computer readable medium to enable the functionality to be realized is patent eligible subject matter if it is capable of producing a useful, concrete and tangible result when used in the computer system. Compare Warmerdam to In re Lowry 32 USPQ2d 1031 where a memory with a data structure that increased computing efficiency was patentable. The computer readable medium must be physical structure which provides the functional descriptive material in usable form to permit the functionality to be realized with the computer. A program product which does not explicitly include such a medium, a program per se, a signal or other type of transmission media that fails to include the hardware necessary to realize the functionality (e.g., a transmitter or a receiver), and a piece of paper with the functional descriptive material written on it are all examples of media which are not believed to enable the functionality to be realized with the computer.

PTO Overview of Interim Guidelines for Subject Matter Eligibility Guidelines (herein "PTO Overview"), pg. 10.

Therefore, the recitation in amended claims 85 and 109 that the computer readable medium is encoded with programming instructions overcomes the Section 101 rejection. Independent claim 109 has been amended to read "A computer readable medium encoded with programming steps for securing data" to overcome this rejection.

In the Office Action on pages 5-12, the patent examiner rejected claims 1-146 as being non-patentable under Section 103 in view of certain prior or pre-existing technology or art disclosed in the following references:

U.S. Patent No. 5,960,080 to Fahlman et al. ("Fahlman '080")
U.S. Patent No. 6,370,629 to Hastings et al. ("Hastings '629")
U.S. Patent No. 6,253,203 to O'Flaherty et al. ("O'Flaherty '203")
U.S. Patent No. 6,598,161 to Kluttz et al. ("Kluttz '161")
U.S. Patent No. 6,044,357 to Shmueli et al. ("Shumueli '357")
U.S. Patent No. 5,036,315 to Gurley ("Gurley '315")

SUMMARY

In summary, none of the references show, teach or suggest "a plurality of security controlled memories as respective extract stores with security access controls thereat, ... [and] storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores;" per claims 1, 47, 48, 84, 85, 109, 124, and 147, and, in claims 1, 47, 84, 85 and 124, "permitting full or partial reconstruction ... only in the presence of a predetermined security clearance access control corresponding to said respective security level .. when said portable computing device is not beyond said predetermined region." New claim 147 also includes the concept of multiple secure access extract stores (see "plurality of security controlled data stores with access controls thereat"), and the steps of [i] "storing separately sensitive content in secure data stores of said plurality of security data stores; [ii] permitting reconstruction of some or all of said data with appropriate access controls applied to respective secure data stores; and [iii] said storing or reconstruction based upon territorial protocol and a geographic location signal or a triggering event." The claimed concept of multiple extract stores, with multiple security access controls,

triggered to store critical data in respective secure access control extract stores is unique and patentable.

In summary, Fahlman '080 does not show, teach or suggest multiple extractions of security sensitive content to respective security level extract stores (multiple extract stores and respective security levels), and the requirement that the user apply a password or other security measure ("security clearance access control") before full or partial reconstruction of the data. Fahlman '080 does not disclose nor discuss multiple security level storage and retrieval.

Fahlman '080

Fahlman '080 does not show, teach or suggest multiple security levels, multiple extraction of security data, storage at multiple levels, and presentment of security clearance codes for said respective security level. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

In Fig. 1, step 111 of Fahlman "automatically" merges sensitive information into non-sensitive information. In FIG. 2, step 217, the Fahlman system again "automatically" merges secured data with un-secured data. Fahlman discusses merging secured data with unsecured data at col. 2, line 22, col. 2, line 34, and col. 2, line 49, and col. 2, line 54 and col. 2, line 40. Fahlman '080 discloses identifying security information and extracting that information and replacing it with placeholders. Col. 2, line 37 and col. 3, line 47. "The sanitized message is then transmitted with a low level of security." Col. 3, line 54. The sensitive information is stripped from the original message and stored in a separate location or together with the sanitized message. Col. 3, line 64. A map showing the location of the security information is also stored with the secured information.

Col. 3, line 63. "Then, in step 111, the sensitive terms received from the second path are merged with the sanitized message to create a final confidential message." Col. 4, line 1. The examiner should note that Fahlman does not discuss reconstruction or merger in the presence of any type of security clearance. In contrast, the present invention requires "permitting full or partial reconstruction ... only in the presence of a predetermined security clearance access control corresponding to said respective security level .. when said portable computing device is not beyond said predetermined region." See claims 1, 47, 84, 85 and 124.

Fahlman also states: "Then, in step 217, the sensitive terms are automatically merged back into the serviced message to create a final message." Col. 5, line 27. No discussion of multi-level security clearance is noted in Fahlman. The same is true regarding merger of security information and non-secured information at col. 6, line 62. Fahlman does not require presentment of the proper, respective security clearance prior to the merging of secret and non-secret data.

Fahlman does not separately store different levels of secret, extract data. Fahlman (1) identifies secret words, (2) replaces the words with placeholders, then (3) transmits the "sanitized message." Fig. 1, step 107, Fig. 2, step 209, col 2, line 19, col. 2, line 34, col. 2, line 49, col. 3, line 54 (transmission - no storage of non-secure data), col. 4, line 64 (transmission - no separate storage).

Fahlman does not discuss multiple security levels nor multiple storage sites at each security level. Since multiple security levels are not addressed in Fahlman, multiple security clearance access controls to obtain "access" to multiple levels of secured data is not discussed. Since Fahlman does not use any type of password or security clearance procedures, there is no reconstruction available.

Fahlman extracts only a single level of data and transfers it separately from the non-secure data (data is transmitted by Fahlman, not stored "in a remainder store") but never discusses password control to access either type of data. It is respectfully submitted that it is improper to select disparate parts from the complicated system of Fahlman '080 and "cobble together" the claimed invention. There is no suggestion nor motivation to do so absent the disclosure of the present invention.

Each of the references, Fahlman '080, Hastings '629, O'Flaherty '203, Kluttz '161, Shmueli '357, and Gurley '315 describe complete systems and there is no reason to add to or substitute portions of one disclosure with another. There is no evidence that a person of skill in the art would take certain aspects of one reference and add those features to another reference.

Hastings '629

Hastings '629 does not show multiple levels of extraction to enable "storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores" per claims per claims 1, 47, 48, 84, 85, 109, 124, and 147. Hastings '629 states:

> Once the packet from the crypto-board 80 is authorized based on the signature and the initialization vector, the decoder 32 compares the time and position data received from the crypto-board 80 with the policy 155 which applies 50 to the files 144 or to a subset of files 144 (step 460). **If the user is authorized to access the files** 144, then the data is unlocked (step 470), decrypted with decryption keys 52 (step 480) and supplied to the user's application program 34 and displayed (step 490).

Hastings '629, col. 6, line 45 (herein "6/45")(emphasis added).

Hastings '629 does not deal with the storage of information – only the retrieval of information.

> In general, in one aspect of the invention, the invention features controlling access to stored information by determining an actual geographic position where the stored information is located based on signals received at a receiver supplying reliable position information.

Hastings '629, 1/29

Although Hastings '629 discusses storing or downloading data with geographic access controls and password controls, it does not discuss nor explain extraction of data to "security controlled memories as respective extract stores" which extraction and further processing is limited by geographic triggers per the invention.

O'Flaherty '203

O'Flaherty '203 does not show extraction of security sensitive content into various extract stores having respective security levels and access controls. O'Flaherty '203 does not show full or partial reconstruction with a geographic trigger and access control for the respective secure extract store. O'Flaherty '203 states:

> In an alternate embodiment, the security and privacy protection features of the extended database 106 and data view suite 108 are further enhanced with the use of data encryption. This may be performed by encrypting the data in a given row with an encryption code, or by providing each data field with a unique encryption number. Alternatively, the data may be encrypted at different hierarchical levels of security so as to enforce the privacy preferences of the consumer.

O'Flaherty '203, 10/40.

> In another embodiment, the separate trusted database 704 and anonymized database 708 are used in a multi level security privacy system, where the encryption, macros, data views, and/ or separate database techniques disclosed herein combined to meet the privacy requirements of different jurisdictions, for different retail outlets, or to accommodate different individual preferences.

O'Flaherty '203, 14/58

The citation at col 14, lines 25 - 57 by the patent examiner does not discuss multiple security levels. In fact, that portion of O'Flaherty '203 discusses anonymized database 708, containing pseudonyms and data 706, being different than trusted database 702, containing pseudonyms and genuine customer ids (identification data). There is no discussion in O'Flaherty '203 of (a) multiple extraction per security level nor (b) multiple, dispersed storage of security

data, per security level, nor (c) reconstruction using multiple security clearances or access controls for multiple secure extract stores.

Therefore, O'Flaherty '203 discusses the use of different encryption in a single database for "different hierarchical levels of security"(O'Flaherty '203, 10/40), but does not discuss different extract stores, one for each security level, PLUS extraction PLUS dispersal nor does O'Flaherty '203 discuss full or partial reconstruction. The general reference in O'Flaherty '203 to a "multi level security privacy system, where the encryption, macros, data views, and/ or separate database techniques" is not sufficiently clear to show singular extraction, per security level, storage per security level nor full or partial reconstruction per security level/security clearance.

The referenced "separate database techniques" (see quote, O'Flaherty '203, 14/58 above) does not clearly describe multiple extraction, separate extract stores, nor certain reconstruction techniques as per the presently claimed system. O'Flaherty '203 does describe different encryption in a single database for multiple levels of security (O'Flaherty '203, 10/40) but this is not the same as extraction per security level, storage per security level and full or partial reconstruction per security level/security clearance. O'Flaherty '203 describes a single storage facility with multiple security levels (by encryption) therein. O'Flaherty '203, 10/40.

The present invention claims "a plurality of security controlled memories as respective extract stores with security access controls thereat, ... [and] storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores;" per claims 1, 47, 48, 84, 85, 109, 124, and 147, and, in claims 1, 47, 84, 85 and 124, "permitting full or partial reconstruction ... only in the presence of a predetermined security clearance access

control corresponding to said respective security level .. when said portable computing device is not beyond said predetermined region." New claim 147 also includes the concept of multiple secure access extract stores and the steps of (i) storing separately sensitive content in secure data stores of said plurality of security data stores; (ii) permitting reconstruction with appropriate access controls applied to respective secure data stores; wherein (iii) storing or reconstruction is based upon territorial protocol or a triggering event.

Kluttz '161 does not show, teach or suggest multi-level extract stores nor permitting reconstruction of said data via said extract data stores only in the presence of predetermined security clearances. Kluttz '161 shows utilizing multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

U.S. Patent No. 5,036,315 to **Gurley** does not cure the defects identified above and the differences with respect to the present invention. Gurley does not show, teach or suggest (a) extracting data; (b) multiple extract stores; (c) multiple security access clearances for the extract stores. Also, Gurley '315 does not show (d) reconstruction of said data via the multiple extract stores with special security access. Gurley '315 discusses a video display control which accepts and processes two (2) video signals, one displayed in a defined window of the second video display.

Shmueli '357 discusses taking a computer readable document, parsing the document into blocks, such as text blocks (5/5 - 8), bounding the blocks (5/9), parsing the data in each block by

word or symbol (5/20), then comparing each word to an authority list (5/25). "The authority list is essentially a dictionary that lists many of the linguistic functions for words. The authority list can be very detailed and can be customized by users to suit the types of documents they use most frequently and user-defined metadata." Shmueli '357, 5/26. Earlier, Shmueli '357 defines "metadata" as "data about data." Shmueli '357, 1/12. Hence, the function of each word or symbol in the block is identified by the authority list and the resultant is metadata, that is, data about the data in the block. The combination of the text block and "information derived from each block" (5/57), is combined together to form a compound. Shmueli '357, 5/58 - 65. "The compounds are then processed through a trained neural network." Shmueli '357, 6/1.

> When all of the compounds have been processed through the neural net, metadata may be determined by selecting from the word guesses, compound guesses and document guesses having the highest word, compound, and document confidence factors, respectively. Alternatively, however, the metadata guesses may be improved prior to determining the metadata through additional analysis that will ultimately result in improved accuracy and reliability of the metadata extracted from the document.

Shmueli '357, 8/40.

Contrary to the claims in the present case wherein the neural network assists in "extracting" (see claim 22, for example), Shmueli '357 defines metadata for a document block by having the neural network guess the type or classification of the word or symbol. Shmueli '357 does not discuss multiple security levels, extraction for each level and full or partial reconstruction based upon security clearance access protocol.

The Manual of Patent Examining Procedures ("MPEP") explains that it is not obvious to modify a system with a plurality of sensors controlling a plurality of valves to create the inventive and patentable single sensor which controls a plurality of valves:

> In *In re Kotzab,* 217 F.3d 1365, 55 USPQ2d 1313 (Fed.Cir. 2000), the claims were drawn to an injection molding method using a single temperature sensor to control a plurality of flow control valves. The primary reference disclosed a multizone device having multiple sensors, each of which controlled an associated flow control valve, and also taught that one system may be used to control a number of valves. The court found that there was insufficient evidence to show that one system was the same as one sensor. While the control of multiple valves by a single sensor rather than by multiple sensors was a "technologically simple concept," there was no finding "as to the specific, understanding or principle within the knowledge of the skilled artisan" that would have provided the motivation to use a single sensor as the system to control more than one valve. 217 F.3d at 1371, 55 USPQ2d at 1318.

MPEP § 2143.01.

In the present invention, Applicant has developed a system designed to safeguard security sensitive content with a plurality of security levels and specific dispersal and retrieval techniques, all triggered or keyed to geographic location data. If the system is programmed not to permit the user to "walk away" from the site with the secure data, the system extracts the data upon transit over the regional boundary. Access via reconstruction is permitted as per the program when the user in within the boundary. Of course, the reverse operation could be programmed such that if within the region, no extraction nor reconstruction is permitted. Permutations of these data security controls are also possible within the scope of the claims. The single data storage systems in the prior art references of Fahlman '080 and O'Flaherty '203 cannot be extended to the claimed multi-level security storage systems with different extract stores with different access controls. Hastings '629 does not extract and store based upon geographic trigger events. These references discloses single storage of security words not "a plurality of security controlled memories as respective extract stores with security access controls thereat." O'Flaherty '203 shows single storage because only one database is open at any one time.

> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990) (Claims were directed to an apparatus for producing an aerated cementitious composition by drawing air into the cementitious composition by driving the output pump at a capacity greater than the feed rate. The prior art reference taught that the feed means can be run at a variable speed, however the court found that this does not require that the output pump be run at the claimed speed so that air is drawn into the mixing chamber and is entrained in the ingredients during operation. Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.).

MPEP § 2143.01.

In the prior art cited herein, there is no suggestion of the desirability of multi-level secured data storage, extraction with each security level, and full or partial reconstruction using multiple extract stores/multiple security clearances. O'Flaherty '203 is a single data base, with multiple encryption levels. This system cannot be altered such that different memories, as different extract stores, are active and are accessible to the user, via multiple security clearances, at the same time to store or reconstruct data. The presently claimed theory modifies that reference to an unacceptable degree. "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)." MPEP § 2143.01. This change to O'Flaherty '203 modifies the operation of the reference improperly. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)." MPEP § 2143.01. Further, such modification of O'Flaherty '203 is not possible unless the examiner uses hindsight provided by the present invention.

Applicant respectfully requests that the examiner approve the patentability of claims 1 - 172.

In the Office Action, the examiner requested a terminal disclaimer to overcome a double patenting obviousness rejection. Applicant submits, under protest, a Terminal Disclaimer. Please charge the $65.00 fee to Deposit Account no. 03-1231. "The filing of a terminal disclaimer to obviate a rejection based on nonstatutory double patenting is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991). The court indicated that the 'filing of a terminal disclaimer simply serves the statutory function of removing the rejection of double patenting, and raises neither a presumption nor estoppel on the merits of the rejection.'" MPEP 804.02(II), p. 800-32.

[Space left blank]

APPENDIX SHOWING SUPPORT FOR NEW CLAIMS

Support for new claims 147 - 172 is shown in brackets herebelow. Support for the substantive changes to claims 1 - 146 are also shown below. There are other locations in the specification and drawings that support the concepts set forth in these claims. Claims having similar scope to these listed herein below are not listed. If the examiner has additional questions regarding support, Applicant requests that the examiner note such concerns and Applicant will respond with additional information.

1. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories [Fig. 1B] as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, [55, 56, 71, 114, 121, 122, 127, 148, 160] ...

5. (currently amended) A method for securing data as claimed in claim 4 wherein said local data drive is one drive from the group of a floppy drive, a hard drive, a flash memory drive, a removable hard drive, a tape drive and a read-write CD-ROM drive. [101]

16. (currently amended) A method of securing data as claimed in claim 1 wherein ~~said predetermined security level is one of a plurality of security levels, said extracting extracts said security sensitive words, data objects, characters or icons from said data to obtain (a) subsets of extracted data and (b) remainder data, said subsets of extracted data associated with said plurality of security levels, and during the reconstruction, some or all of said subsets of extracted data are utilized only in the presence of a respective predetermined security level of said plurality of security levels~~ said predetermined region is one a plurality of regions which includes at least one security protocol extraction region and at least one security protocol reconstruction region, the step of determining determines when said portable computing device is beyond at least one security protocol extraction region and applies the respective protocol to said data, and the step of determining further determines when said portable computing device is beyond at least one security protocol reconstruction region and applies the respective protocol to full or partial reconstruction of said data. [see ¶¶ 238, 240 and 242]

147. A computerized method of securing data in a plurality of security controlled data stores with access controls thereat, said data potentially having sensitive content such as sensitive words, data objects, characters, images, data elements or icons, comprising:

storing separately sensitive content in secure data stores of said plurality of security data stores;

permitting reconstruction of some or all of said data with appropriate access controls applied to respective secure data stores; and

said storing or reconstruction based upon territorial protocol [249, 122] and a geographic location signal [238, 242] or a triggering event. [155, 246]

148. A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering or extracting said sensitive content in said secure data stores. [Fig. 1A]

149. A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of removing [29] or copying [37] said sensitive content in said secure data stores.

150. A computerized method of securing data as claimed in claim 147 wherein said storing includes at least one or both of filtering and transferring or extracting and transferring said sensitive content in said secure data stores. [112]

151. A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or both of partially or completely storing said sensitive content in said secure data stores. [Fig. 1A]

152. A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes partially or completely storing said sensitive content in said secure data stores with at least one of encryption or parsing of data. [106, Fig. 10, 210]

153. A computerized method of securing data as claimed in claim 147 wherein said storing of said sensitive content in said secure data stores includes at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores. [41, 182, 183]

154. A computerized method of securing data as claimed in claim 147 including manually or automatically at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores. [41, 182, 183]

155. A computerized method of securing data as claimed in claim 147 including at least one of:

prior to storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; or

concurrent with storing, at least one or more of tagging, labeling, or classifying said sensitive content in said secure data stores; and wherein

said sensitive content has different levels of sensitive content therein corresponding to respective ones of said secure data stores. [Fig. 7]

156. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is defined as at least one of security sensitive content, content of significance, trade secret content [3], personal identifying information [3], medical content subject to regulatory provisions [3], or back-up content and said respective ones of said secure data stores are correspondingly designated as at least one of security sensitive stores, stores for content of significance, trade secret stores, personal identifying information stores, medical regulatory provision stores, or back-up stores. [223]

157. A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes at least one or more of storing in predetermined security data stores, storing in a predetermined manner by random selection of security data stores [142], storing by data class in said security data stores [223], storing data by data type in said security data stores [223], or storing by level of security in said security data stores. [223]

158. A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in said security data stores in a predetermined manner with an algorithmic selection. [130]

159. A computerized method of securing data as claimed in claim 147 wherein said storing of sensitive content in said secure data stores includes storing data in optical media data stores. [130]

160. A computerized method of securing data as claimed in claim 147 wherein storing of said sensitive content is done separately with respect to at least one of remainder data, left-over data, non-sensitive content data, surplus data, residue data, remnant data, or data complementary to sensitive content data. [107]

161. A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution 34,41,44], regeneration, compilation [35,131], reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores. [47,51,55]

162. A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes the use of at least one of predetermined access controls [47,51,55], assigned access controls, access controls generated with said storing of said secure data, or access controls and encryption. [47,51,55]

163. A computerized method of securing data as claimed in claim 147 wherein permitting reconstruction includes at least one of reassembly, reconstitution, regeneration, compilation, reorganization, reclamation or reformation of some or all of said data with appropriate access controls applied to respective secure data stores. [Fig. 7]

164. A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to respective secure data stores in at least one of the following manners:

said access controls [47, 51, 55] applied sequentially to respective secure data stores; [121, 133]

said access controls applied concurrently to respective secure data stores; [121, 133]

said access controls applied to respective secure data stores subsequent to application of a security protocol; [121,002,032,122,144]

said secure data stores are mapped [Fig. 5, 144]and said access controls are applied to obtain the mapped secure data stores; [121,002,032,122,144] or

said access controls are applied subsequent to an exchange of compensation or an exchange of data. [Fig. 13, 234, 235, 173]

said access controls applied to respective secure data stores subsequent to application of a hierarchical security protocol. [212]

165. A computerized method of securing data as claimed in claim 147 wherein said access controls are applied to at least one or more of predetermined respective secure data stores [130, 133], associated respective secure data stores [130, 133], correlated respective secure data stores [130, 131], or designated respective secure data stores. [38, 126, 130]

166. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system [20]with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and [34, 130]

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores. [131]

167. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores. [131]

168. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server permitting reconstruction of some or all of said data by controlling the application of said access controls to respective secure data stores. [131]

169. A computerized method of securing data as claimed in claim 147 wherein the method of securing data is deployed in a client-server computer system with at least one server computer

and a plurality of secure data stores, said server operatively coupled to at least one client computer and said secure data stores over a communications network,

said server effecting said storing of sensitive content in secure data stores of said plurality of security data stores; and [131]

said server controlling the application of said access controls. [131]

170. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

select sensitive words, data objects, characters, images, data elements or icons;

defined sensitive words, data objects, characters, images, data elements or icons; [46]

known sensitive words, data objects, characters, images, data elements or icons; [46]

certain sensitive words, data objects, characters, images, data elements or icons;

a collection of sensitive words, data objects, characters, images, data elements or icons; [111, 105]

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons; or [46]

a plurality of predetermined sensitive words, data objects, characters, images, data elements or icons having different hierarchal [30,35, 110, 156] or orthogonal levels [35, 160] of sensitive content.

171. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is at least one or more of:

portions of predetermined sensitive words, data objects, characters, images, data elements or icons; or [104]

words, data objects, characters, images, data elements or icons which are not from a plurality of predetermined words, data objects, characters, images, data elements or icons. [46]

172. A computerized method of securing data as claimed in claim 147 wherein said sensitive content is related to sensitive words, data objects, characters, images, data elements or icons, by at least or more of a function or a meaning. [104, 105]

Respectfully submitted,

By ____/Robert Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002,
Facsimile: 954-768-0158

Docket No.: 6851-2-CIP-5

Certificate of e-Filing

I hereby certify that this correspondence is being e-filed with Commissioner for Patents, Alexandria, VA on May 14, 2007.

___/Robert Kain/_____
Robert C. Kain, Jr.
Reg. No. 30,648

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

REQUEST FOR EXTENSION OF TIME

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a request for extension of time pursuant to 37 CFR §1.136. Please charge $60.00 for a one month extension of time pursuant to 37 CFR §1.17(a) to Deposit Account No. 03-1231 and please debit or credit any underpayment or overpayment to Deposit Account No. 03-1231.

Respectfully submitted,

By ___/Robert Kain / _____

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Mail Stop PGPUB Drawings, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 14, 2007.

____/Robert Kain/_____
Robert C. Kain, Jr.
Reg. No. 30,648

F:\RCK\CLIENTS\Redlich\6851-02-cip5-Req-Ext-Time-051007.wpd

Replacement Sheet

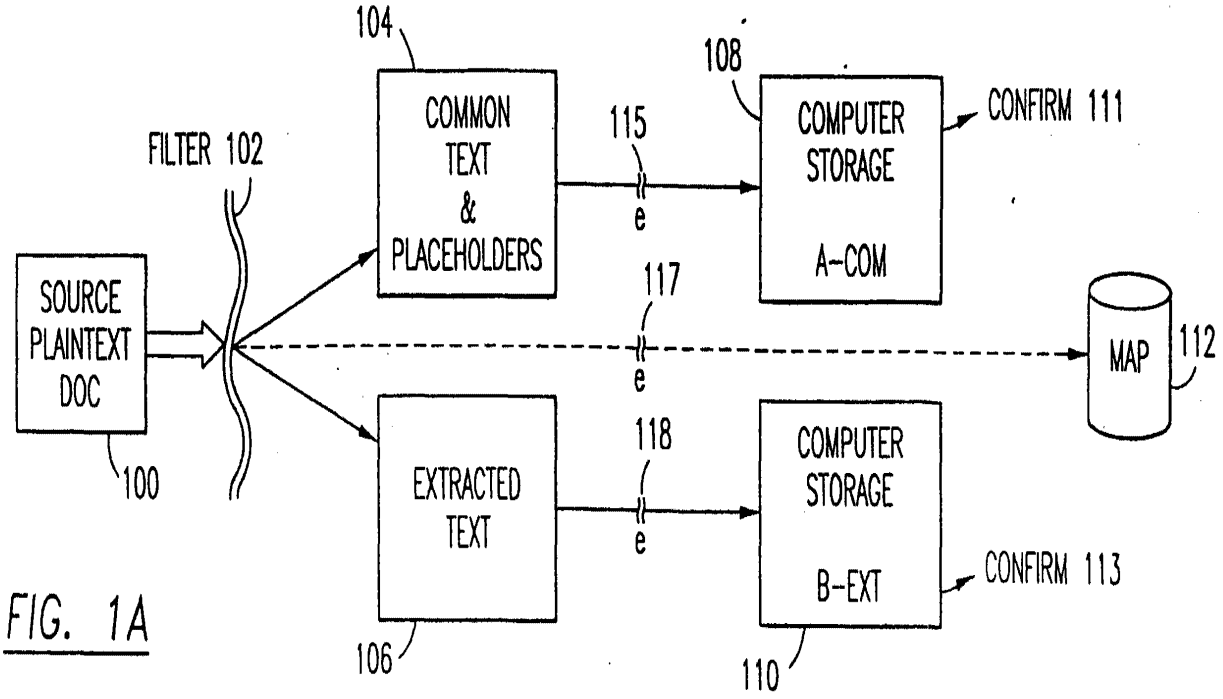


FIG. 1A

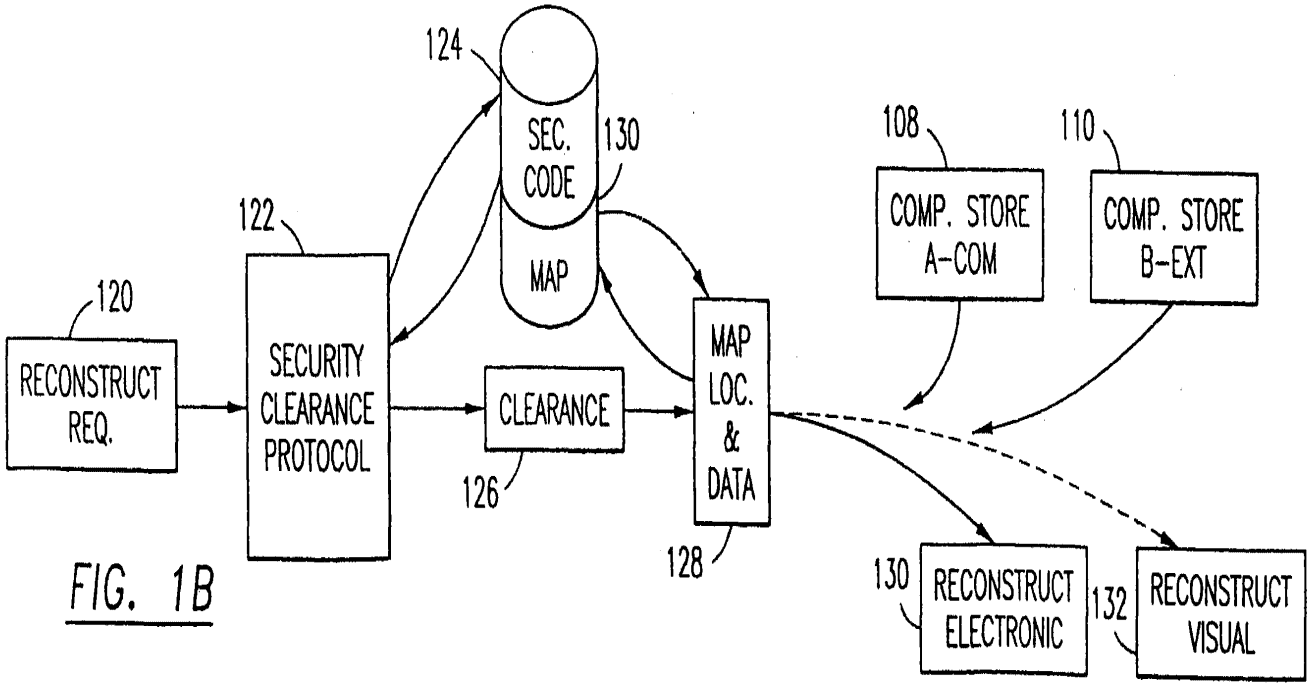


FIG. 1B

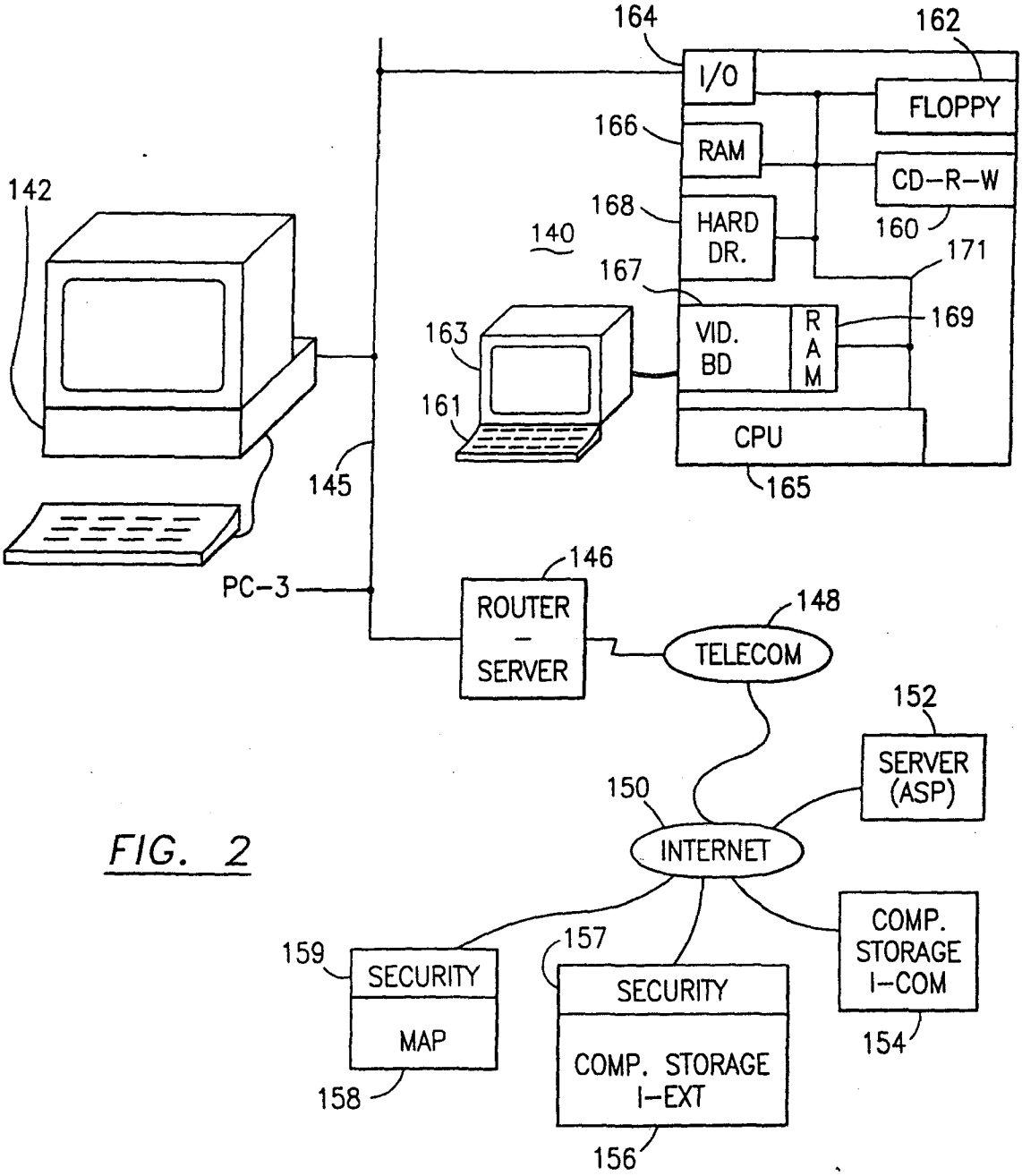
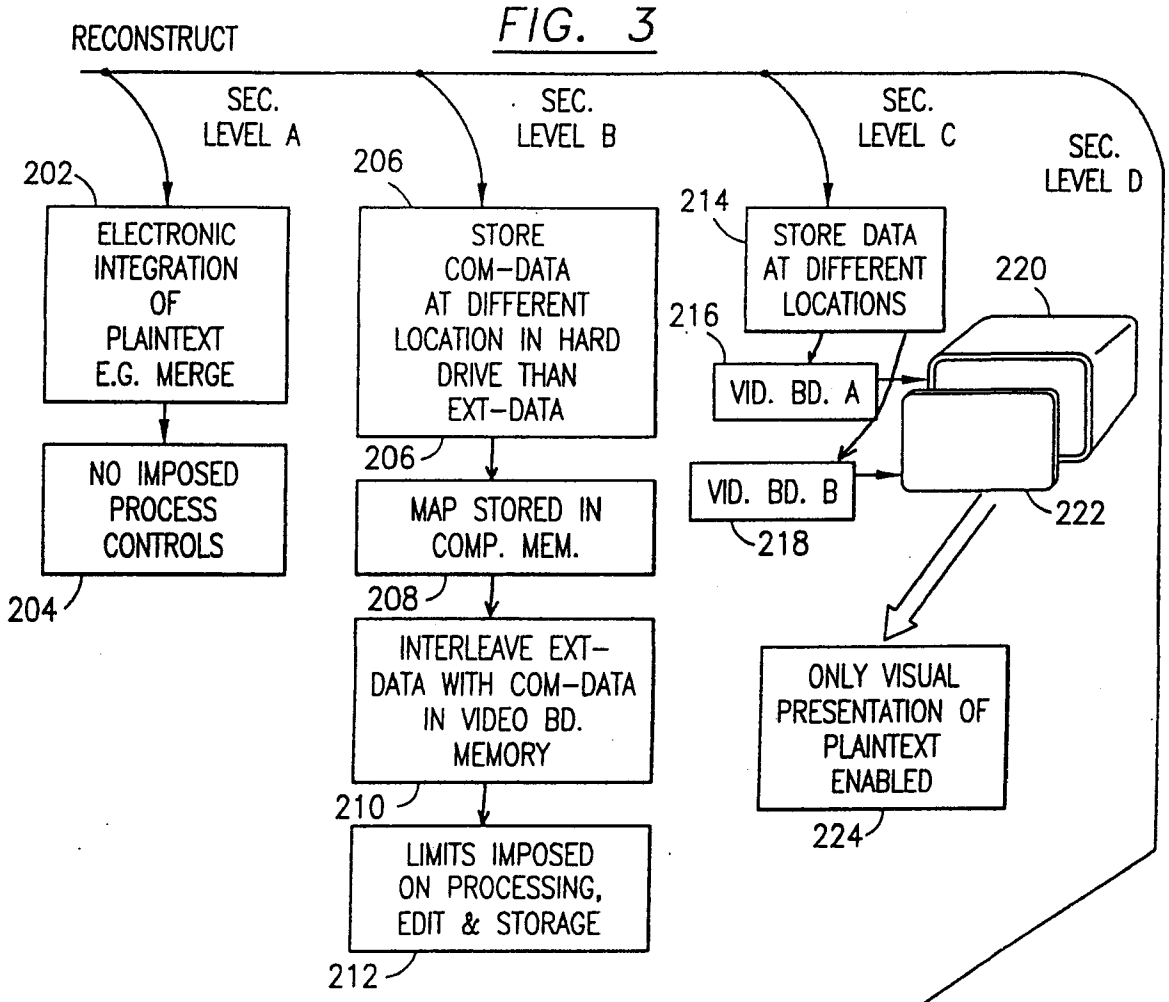

164
162
I/O
FLOPPY
166
RAM
CD-R-W
142
168
HARD DR.
160
140
171
167
163
VID. BD
R A M
169
161
CPU
145
165
146
PC-3
ROUTER – SERVER
148
TELECOM
152
SERVER (ASP)
150
INTERNET
COMP. STORAGE I-COM
159
157
SECURITY
MAP
SECURITY
COMP. STORAGE I-EXT
154
158
156

FIG. 2

FIG. 3


RECONSTRUCT
SEC. LEVEL A
SEC. LEVEL B
SEC. LEVEL C
SEC. LEVEL D
202
ELECTRONIC INTEGRATION OF PLAINTEXT E.G. MERGE
NO IMPOSED PROCESS CONTROLS
204
206
STORE COM-DATA AT DIFFERENT LOCATION IN HARD DRIVE THAN EXT-DATA
206
MAP STORED IN COMP. MEM.
208
INTERLEAVE EXT-DATA WITH COM-DATA IN VIDEO BD. MEMORY
210
LIMITS IMPOSED ON PROCESSING, EDIT & STORAGE
212
214
STORE DATA AT DIFFERENT LOCATIONS
216
VID. BD. A
VID. BD. B
218
220
222
ONLY VISUAL PRESENTATION OF PLAINTEXT ENABLED
224
226
PARSE EXT-DATA PER SECURITY CLEARANCE
228
REPEAT PROCESS A, B OR C WITH ONLY PORTIONS OF EXT-DATA PRESENTED TO USER BASED ON SEC. CLEARANCE

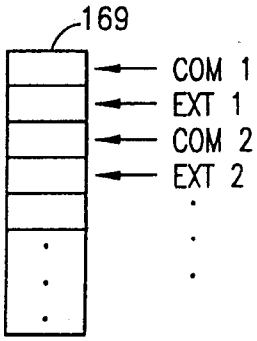

169
COM 1
EXT 1
COM 2
EXT 2

FIG. 3A

FIG. 4

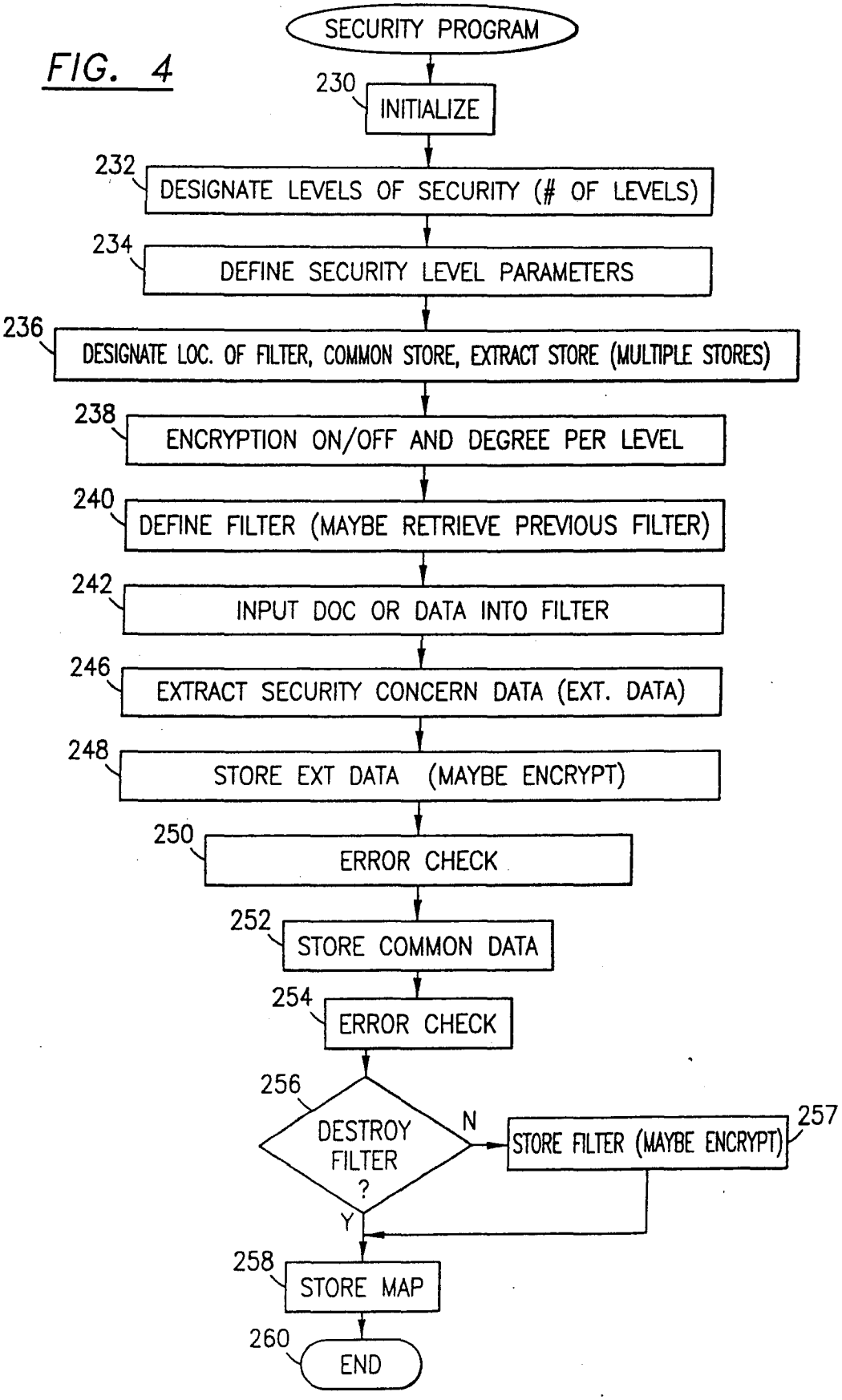
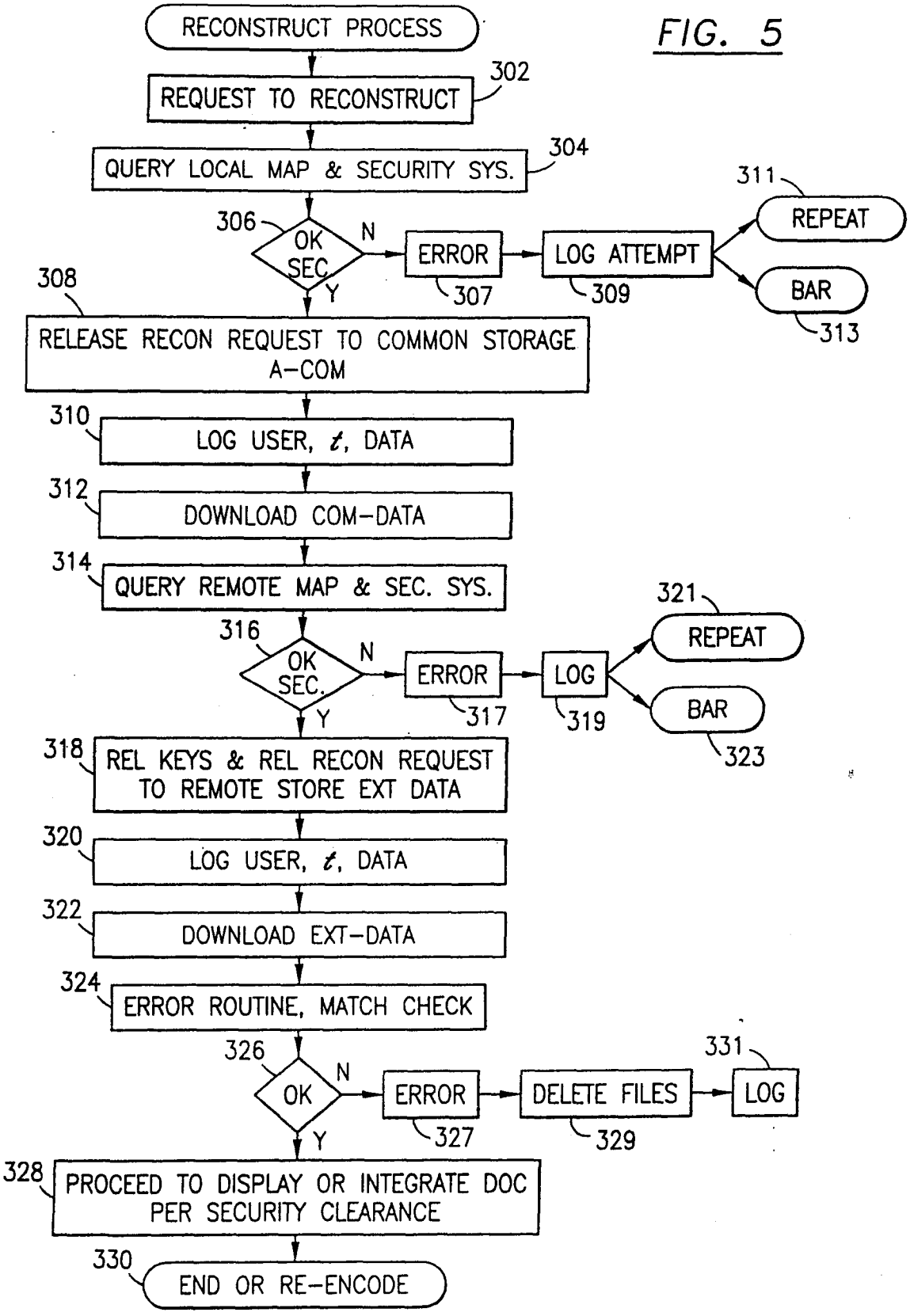

SECURITY PROGRAM
230
INITIALIZE
232
DESIGNATE LEVELS OF SECURITY (# OF LEVELS)
234
DEFINE SECURITY LEVEL PARAMETERS
236
DESIGNATE LOC. OF FILTER, COMMON STORE, EXTRACT STORE (MULTIPLE STORES)
238
ENCRYPTION ON/OFF AND DEGREE PER LEVEL
240
DEFINE FILTER (MAYBE RETRIEVE PREVIOUS FILTER)
242
INPUT DOC OR DATA INTO FILTER
246
EXTRACT SECURITY CONCERN DATA (EXT. DATA)
248
STORE EXT DATA (MAYBE ENCRYPT)
250
ERROR CHECK
252
STORE COMMON DATA
254
ERROR CHECK
256
DESTROY FILTER ?
N
257
STORE FILTER (MAYBE ENCRYPT)
Y
258
STORE MAP
260
END

FIG. 5


RECONSTRUCT PROCESS
REQUEST TO RECONSTRUCT
302
QUERY LOCAL MAP & SECURITY SYS.
304
306
OK SEC.
N
Y
ERROR
307
LOG ATTEMPT
309
311
REPEAT
BAR
313
308
RELEASE RECON REQUEST TO COMMON STORAGE A-COM
310
LOG USER, t, DATA
312
DOWNLOAD COM-DATA
314
QUERY REMOTE MAP & SEC. SYS.
316
OK SEC.
N
Y
ERROR
317
LOG
319
321
REPEAT
BAR
323
318
REL KEYS & REL RECON REQUEST TO REMOTE STORE EXT DATA
320
LOG USER, t, DATA
322
DOWNLOAD EXT-DATA
324
ERROR ROUTINE, MATCH CHECK
326
OK
N
Y
ERROR
327
DELETE FILES
329
331
LOG
328
PROCEED TO DISPLAY OR INTEGRATE DOC PER SECURITY CLEARANCE
330
END OR RE-ENCODE

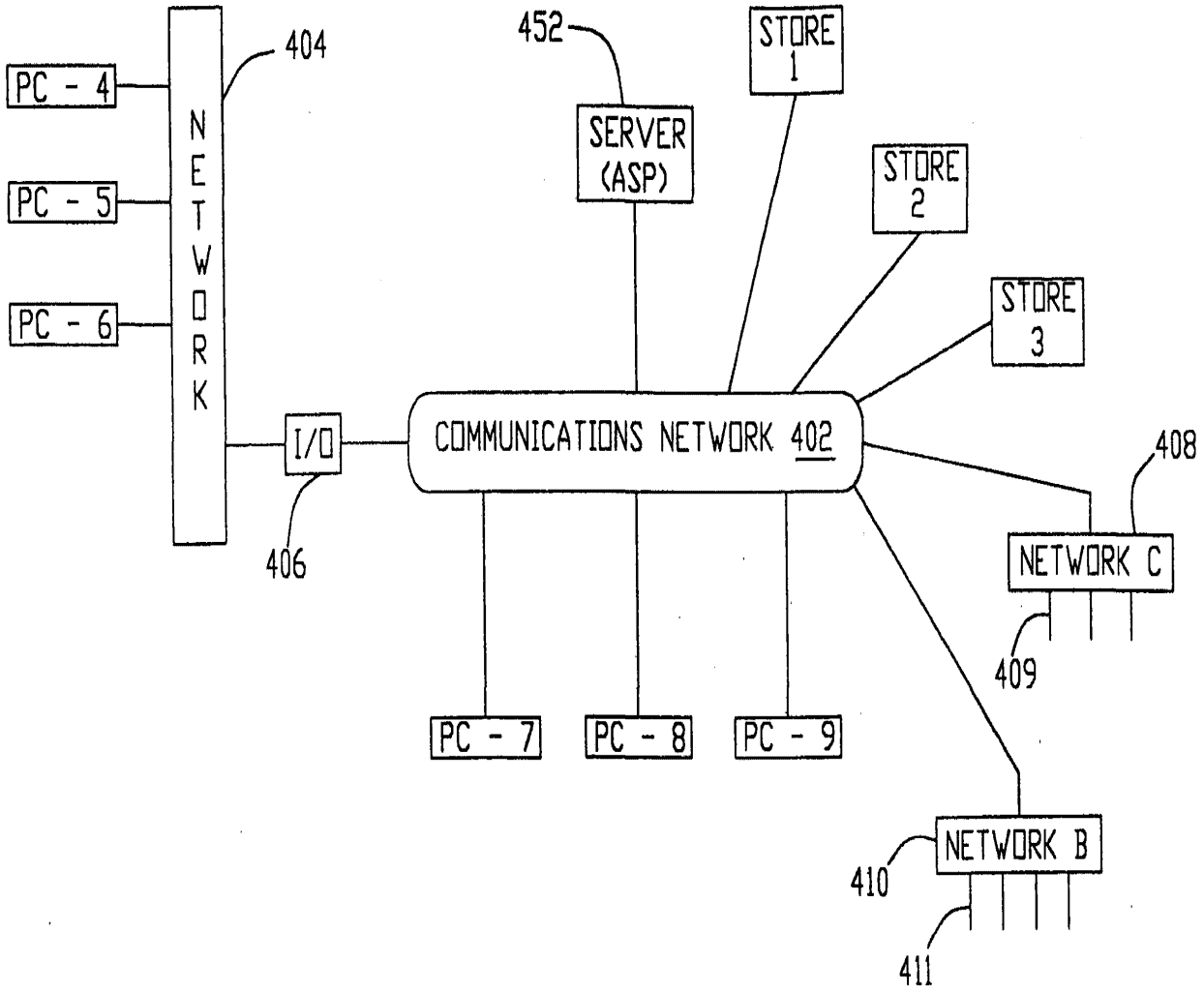


FIG.6

Replacement Sheet

FIG. 7a

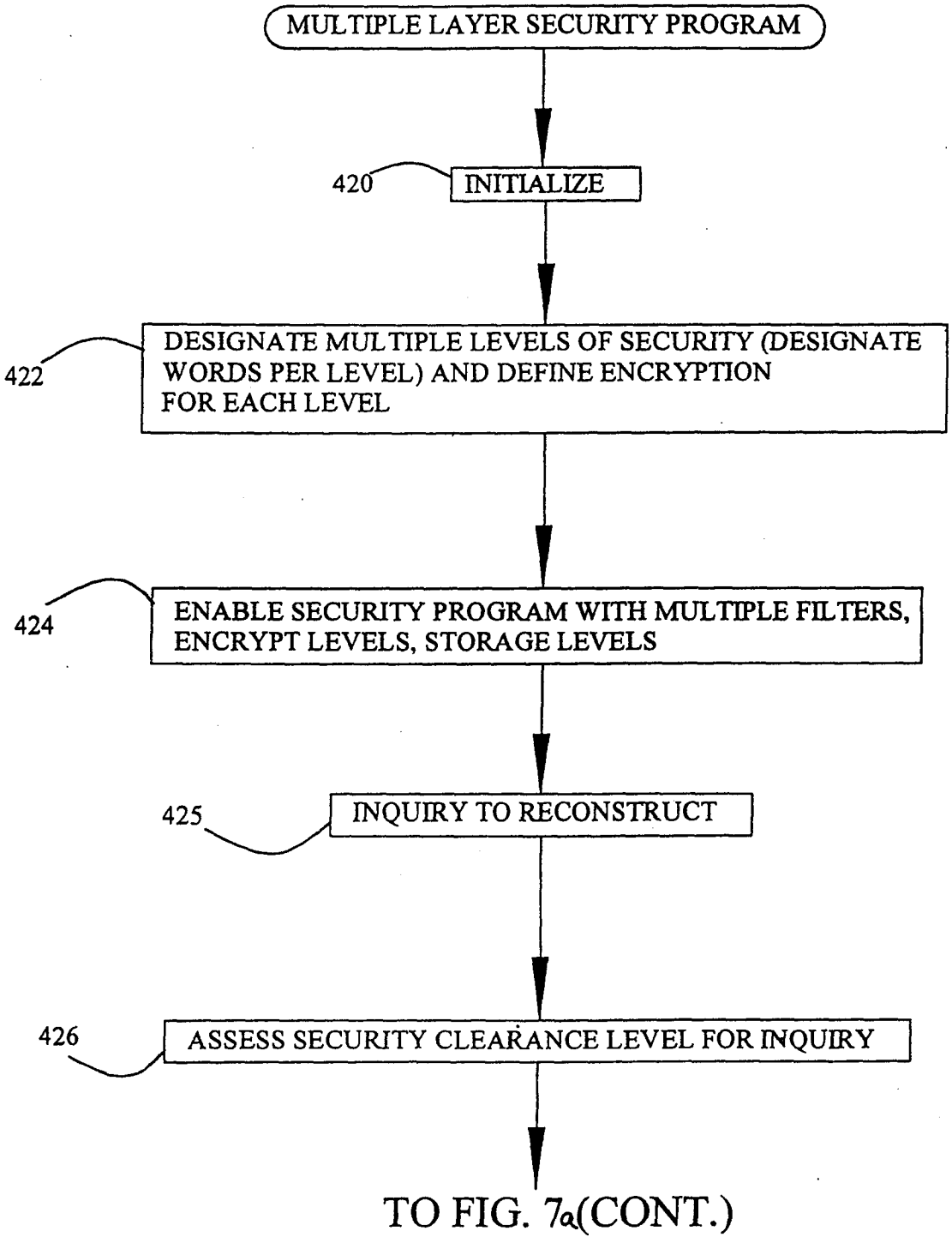
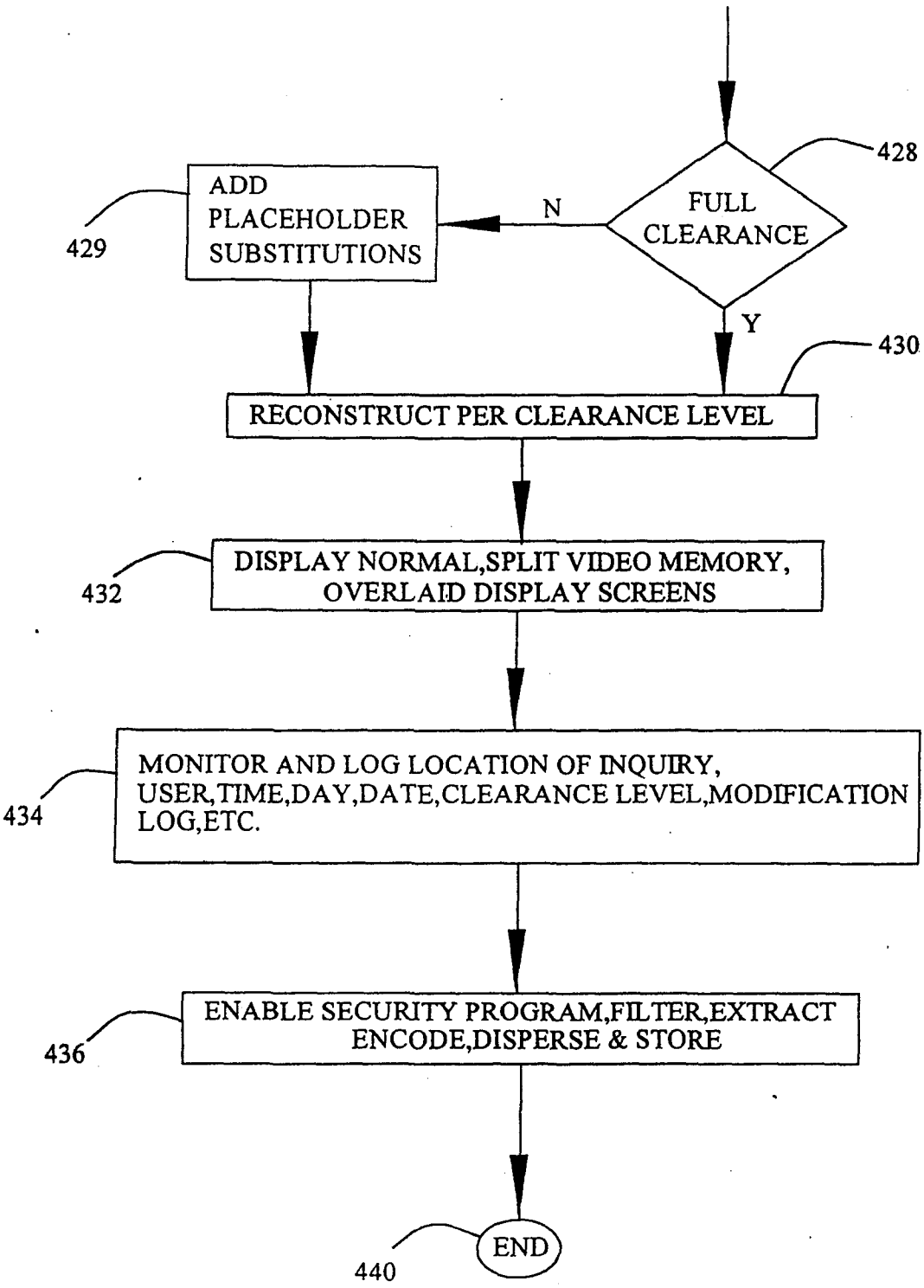

MULTIPLE LAYER SECURITY PROGRAM
420
INITIALIZE
422
DESIGNATE MULTIPLE LEVELS OF SECURITY (DESIGNATE WORDS PER LEVEL) AND DEFINE ENCRYPTION FOR EACH LEVEL
424
ENABLE SECURITY PROGRAM WITH MULTIPLE FILTERS, ENCRYPT LEVELS, STORAGE LEVELS
425
INQUIRY TO RECONSTRUCT
426
ASSESS SECURITY CLEARANCE LEVEL FOR INQUIRY
TO FIG. 7a(CONT.)

FIG. 7a(CONT.)


428
FULL CLEARANCE
N
ADD PLACEHOLDER SUBSTITUTIONS
429
Y
430
RECONSTRUCT PER CLEARANCE LEVEL
DISPLAY NORMAL,SPLIT VIDEO MEMORY, OVERLAID DISPLAY SCREENS
432
MONITOR AND LOG LOCATION OF INQUIRY, USER,TIME,DAY,DATE,CLEARANCE LEVEL,MODIFICATION LOG,ETC.
434
ENABLE SECURITY PROGRAM,FILTER,EXTRACT ENCODE,DISPERSE & STORE
436
END
440

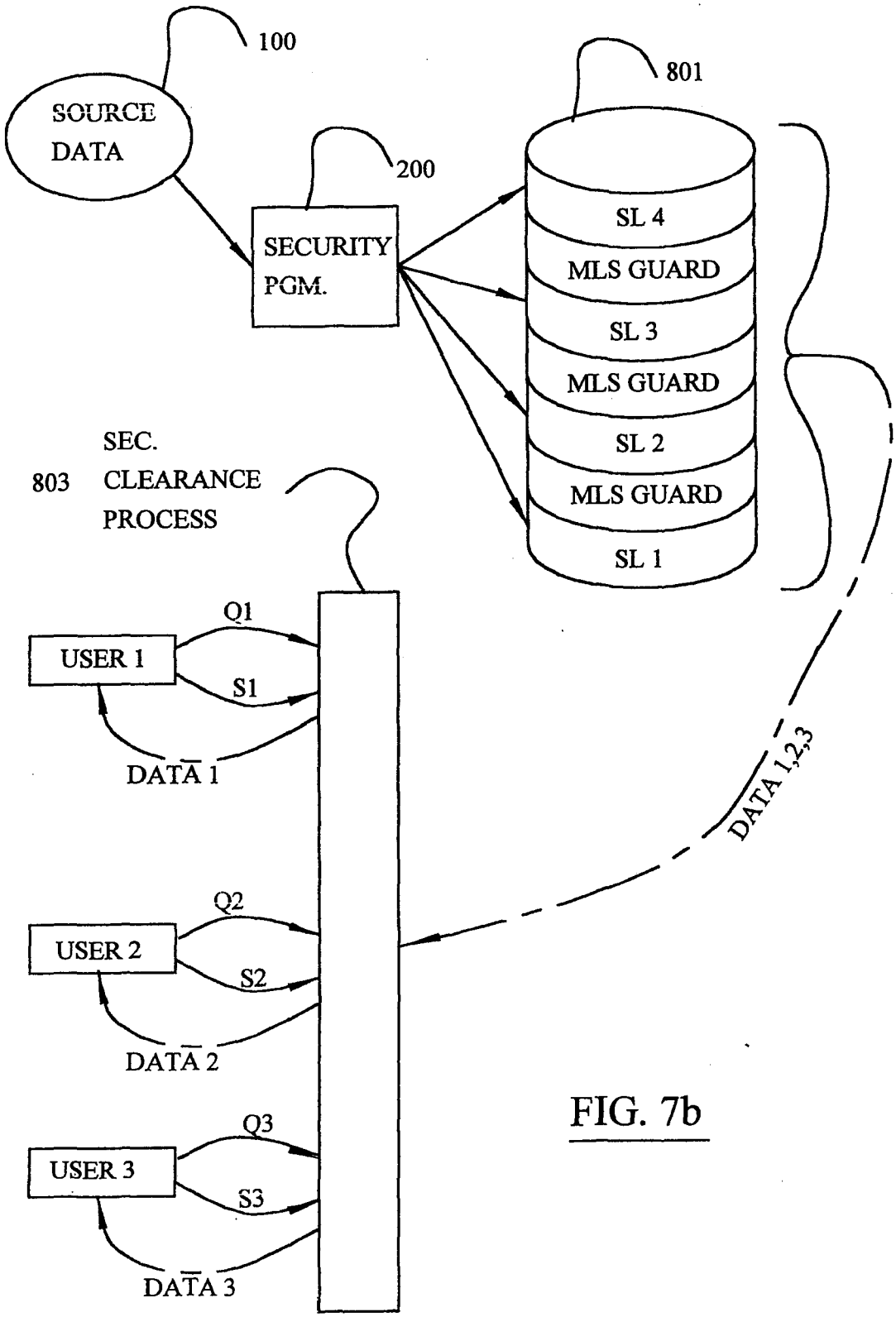

100
SOURCE DATA
200
SECURITY PGM.
801
SL 4
MLS GUARD
SL 3
MLS GUARD
SL 2
MLS GUARD
SL 1
803
SEC. CLEARANCE PROCESS
Q1
USER 1
S1
DATA 1
Q2
USER 2
S2
DATA 2
Q3
USER 3
S3
DATA 3
DATA 1,2,3

FIG. 7b

FIG. 8

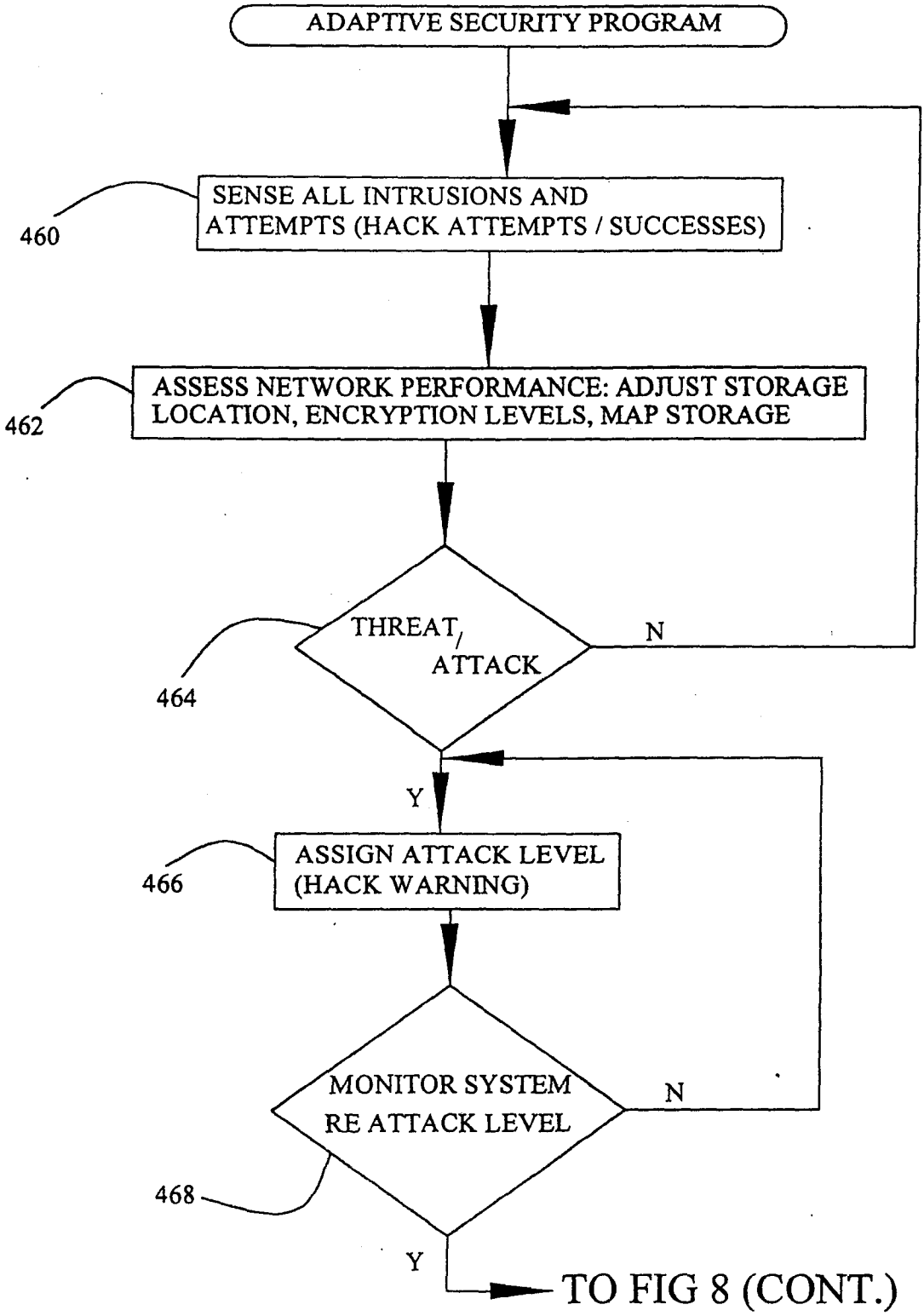

ADAPTIVE SECURITY PROGRAM
SENSE ALL INTRUSIONS AND ATTEMPTS (HACK ATTEMPTS / SUCCESSES)
460
ASSESS NETWORK PERFORMANCE: ADJUST STORAGE LOCATION, ENCRYPTION LEVELS, MAP STORAGE
462
THREAT/ ATTACK
N
464
Y
ASSIGN ATTACK LEVEL (HACK WARNING)
466
MONITOR SYSTEM RE ATTACK LEVEL
N
468
Y
TO FIG 8 (CONT.)

FIG. 8 (CONT.)

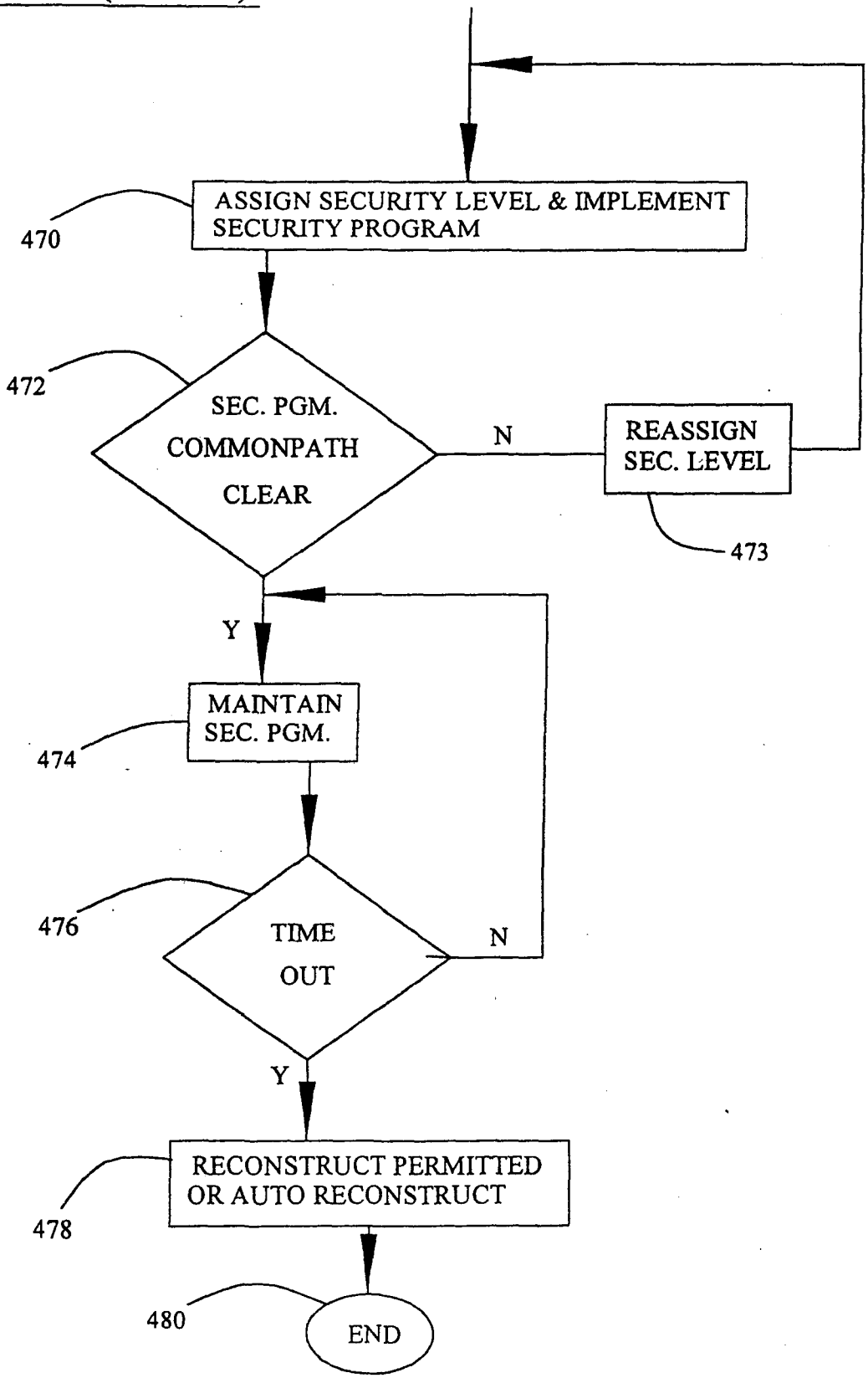

ASSIGN SECURITY LEVEL & IMPLEMENT SECURITY PROGRAM
470
472
SEC. PGM. COMMONPATH CLEAR
N
REASSIGN SEC. LEVEL
473
Y
MAINTAIN SEC. PGM.
474
476
TIME OUT
N
Y
RECONSTRUCT PERMITTED OR AUTO RECONSTRUCT
478
480
END

FIG. 9

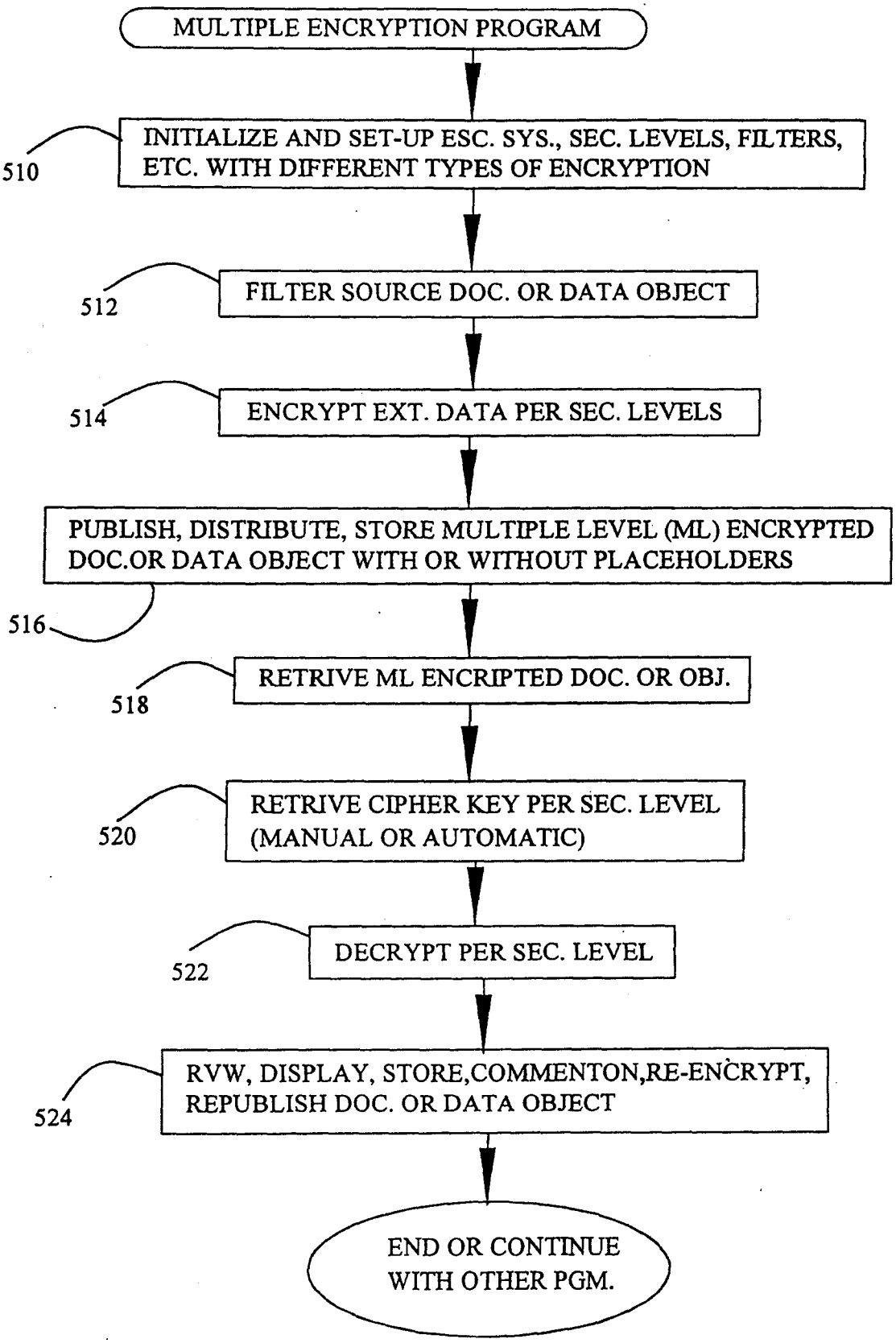

MULTIPLE ENCRYPTION PROGRAM
510
INITIALIZE AND SET-UP ESC. SYS., SEC. LEVELS, FILTERS, ETC. WITH DIFFERENT TYPES OF ENCRYPTION
512
FILTER SOURCE DOC. OR DATA OBJECT
514
ENCRYPT EXT. DATA PER SEC. LEVELS
PUBLISH, DISTRIBUTE, STORE MULTIPLE LEVEL (ML) ENCRYPTED DOC.OR DATA OBJECT WITH OR WITHOUT PLACEHOLDERS
516
518
RETRIVE ML ENCRIPTED DOC. OR OBJ.
520
RETRIVE CIPHER KEY PER SEC. LEVEL (MANUAL OR AUTOMATIC)
522
DECRYPT PER SEC. LEVEL
524
RVW, DISPLAY, STORE,COMMENTON,RE-ENCRYPT, REPUBLISH DOC. OR DATA OBJECT
END OR CONTINUE WITH OTHER PGM.

FIG. 10

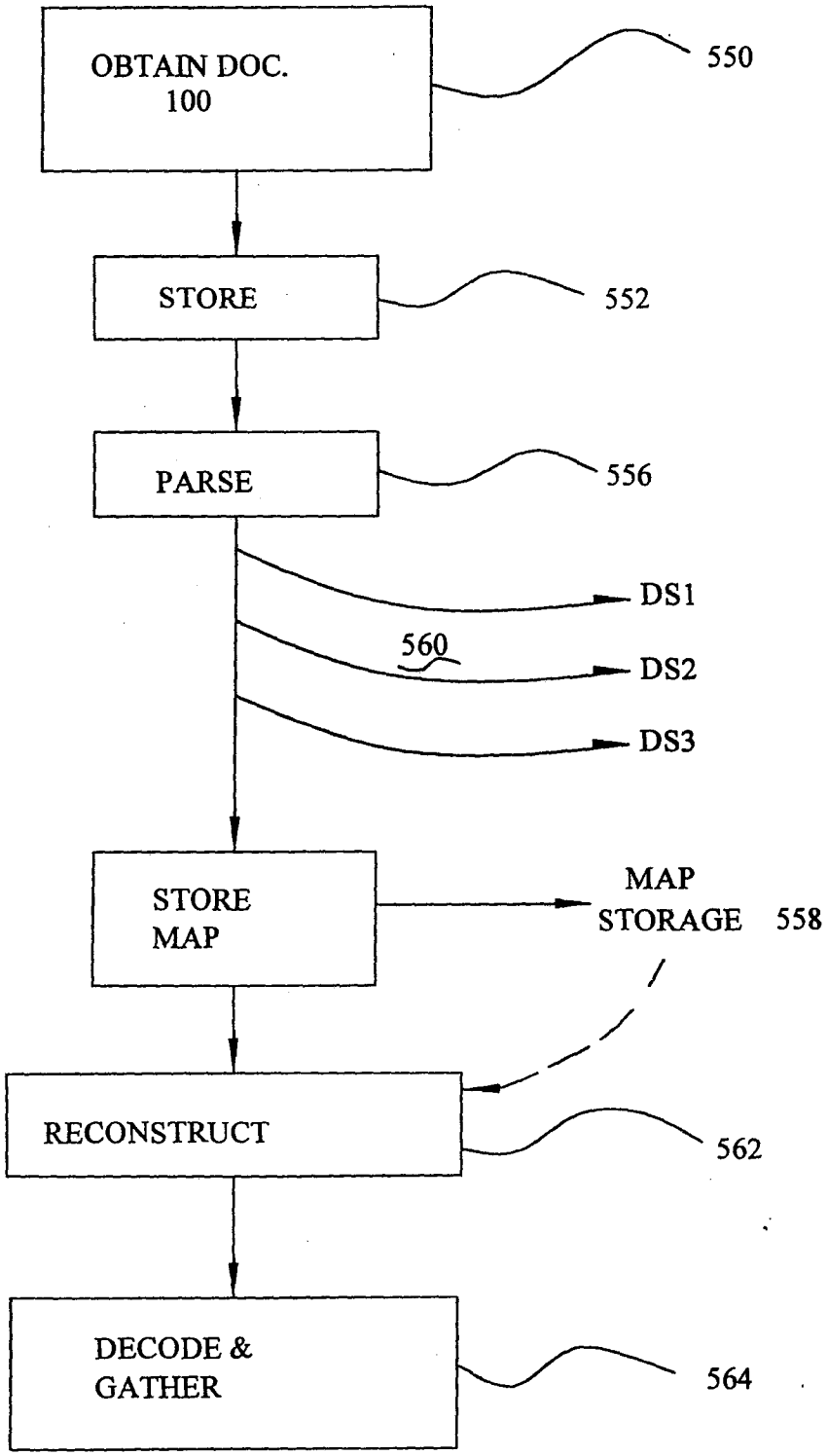

OBTAIN DOC.
100
550
STORE
552
PARSE
556
DS1
560
DS2
DS3
STORE
MAP
MAP
STORAGE
558
RECONSTRUCT
562
DECODE &
GATHER
564

FIG.11A

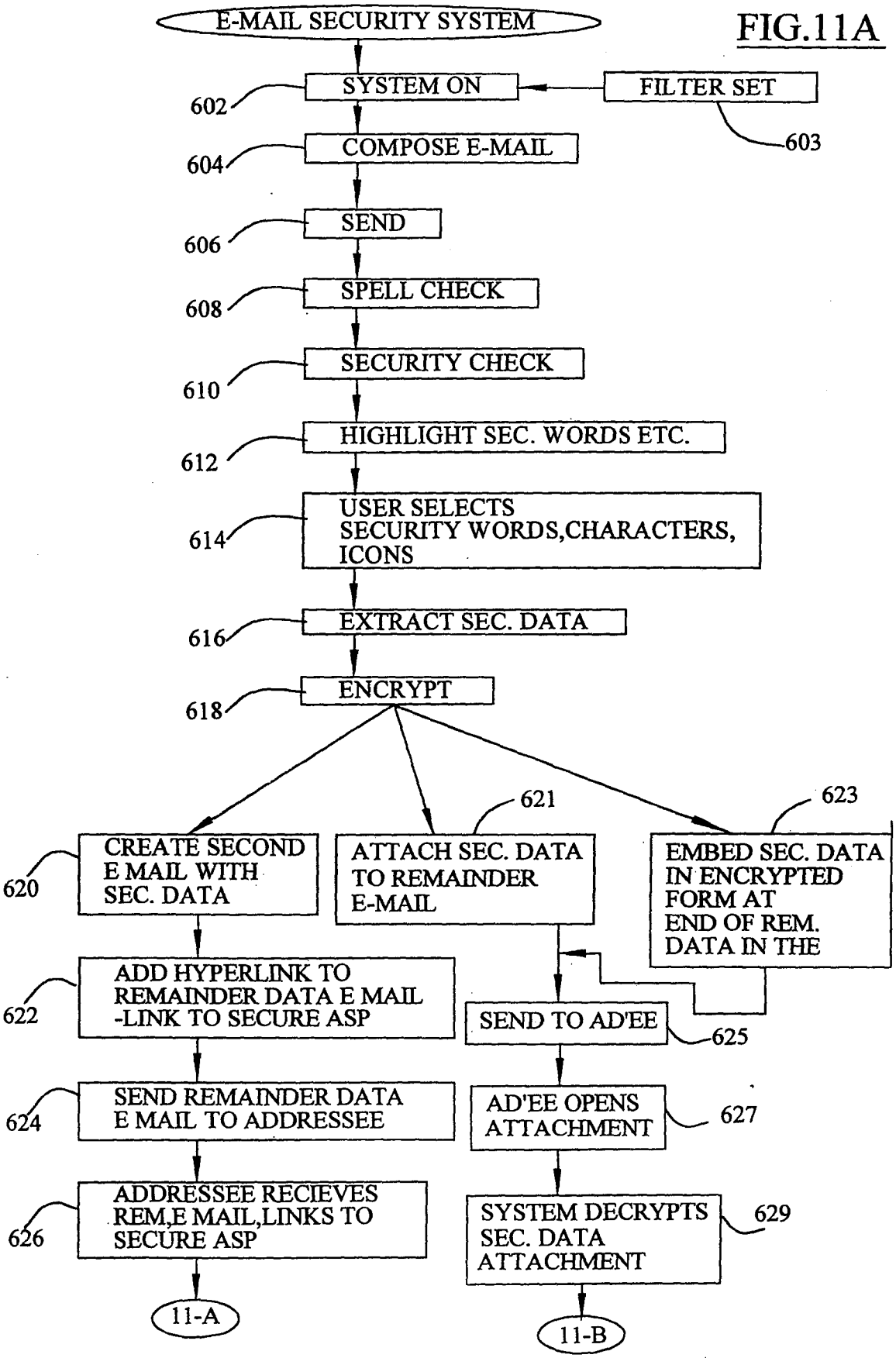

E-MAIL SECURITY SYSTEM
SYSTEM ON
FILTER SET
602
603
COMPOSE E-MAIL
604
SEND
606
SPELL CHECK
608
SECURITY CHECK
610
HIGHLIGHT SEC. WORDS ETC.
612
USER SELECTS SECURITY WORDS,CHARACTERS, ICONS
614
EXTRACT SEC. DATA
616
ENCRYPT
618
621
623
CREATE SECOND E MAIL WITH SEC. DATA
620
ATTACH SEC. DATA TO REMAINDER E-MAIL
EMBED SEC. DATA IN ENCRYPTED FORM AT END OF REM. DATA IN THE
ADD HYPERLINK TO REMAINDER DATA E MAIL -LINK TO SECURE ASP
622
SEND TO AD'EE
625
SEND REMAINDER DATA E MAIL TO ADDRESSEE
624
AD'EE OPENS ATTACHMENT
627
ADDRESSEE RECIEVES REM,E MAIL,LINKS TO SECURE ASP
626
SYSTEM DECRYPTS SEC. DATA ATTACHMENT
629
11-A
11-B

FIG.11B

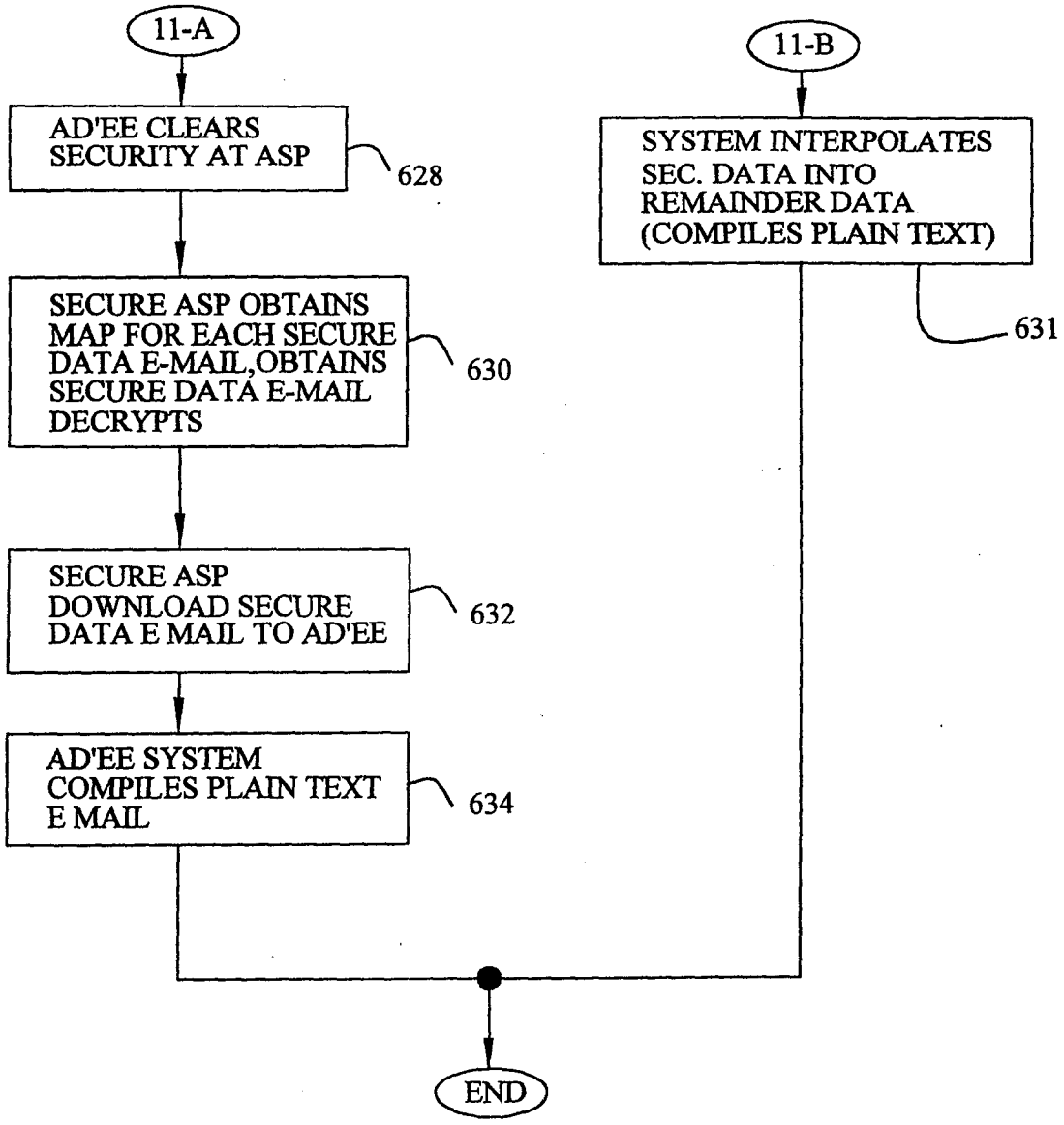

11-A
AD'EE CLEARS SECURITY AT ASP
628
SECURE ASP OBTAINS MAP FOR EACH SECURE DATA E-MAIL,OBTAINS SECURE DATA E-MAIL DECRYPTS
630
SECURE ASP DOWNLOAD SECURE DATA E MAIL TO AD'EE
632
AD'EE SYSTEM COMPILES PLAIN TEXT E MAIL
634
11-B
SYSTEM INTERPOLATES SEC. DATA INTO REMAINDER DATA (COMPILES PLAIN TEXT)
631
END

FIG.12A

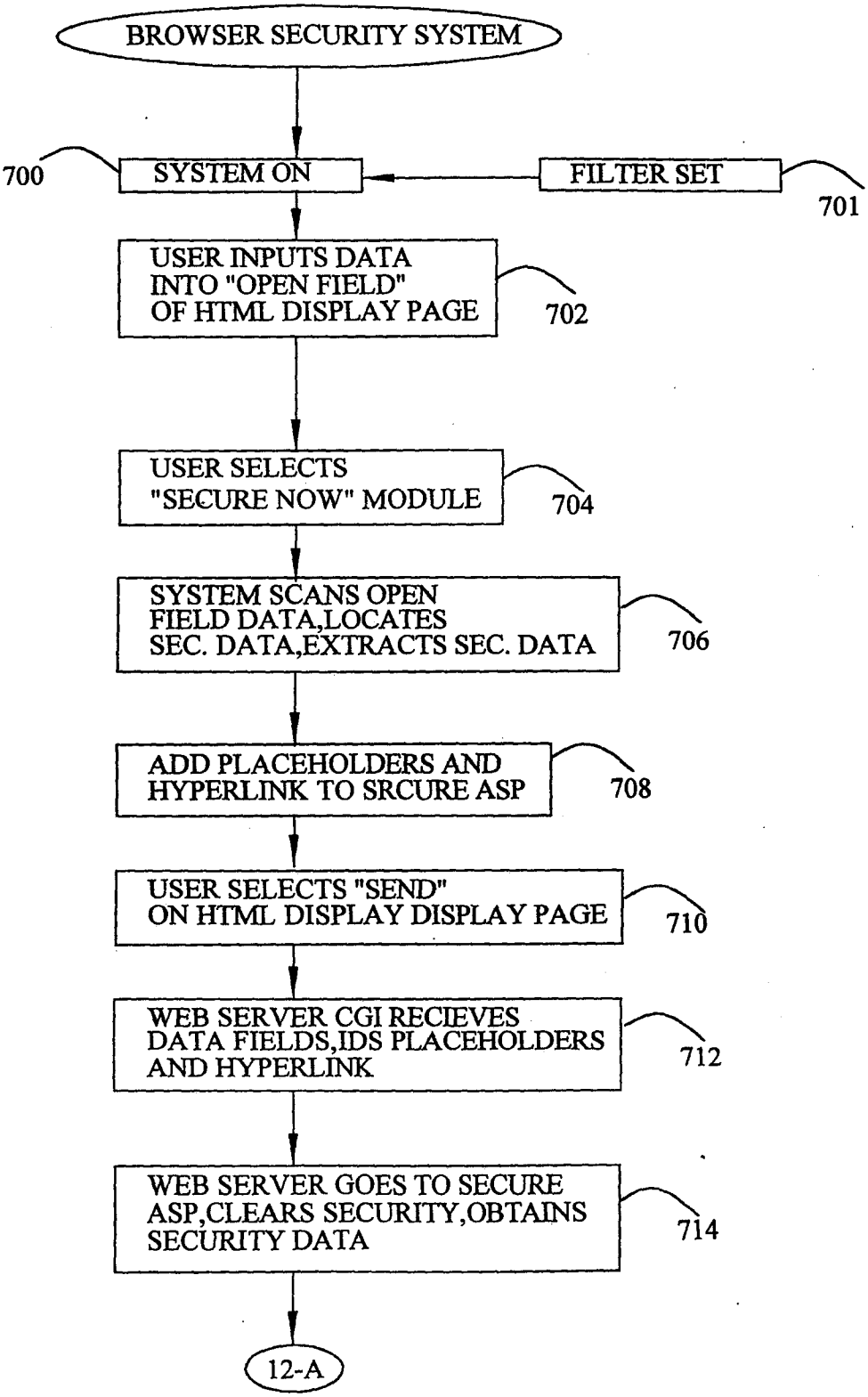

BROWSER SECURITY SYSTEM
700
SYSTEM ON
FILTER SET
701
USER INPUTS DATA INTO "OPEN FIELD" OF HTML DISPLAY PAGE
702
USER SELECTS "SECURE NOW" MODULE
704
SYSTEM SCANS OPEN FIELD DATA,LOCATES SEC. DATA,EXTRACTS SEC. DATA
706
ADD PLACEHOLDERS AND HYPERLINK TO SRCURE ASP
708
USER SELECTS "SEND" ON HTML DISPLAY DISPLAY PAGE
710
WEB SERVER CGI RECIEVES DATA FIELDS,IDS PLACEHOLDERS AND HYPERLINK
712
WEB SERVER GOES TO SECURE ASP,CLEARS SECURITY,OBTAINS SECURITY DATA
714
12-A

FIG.12B

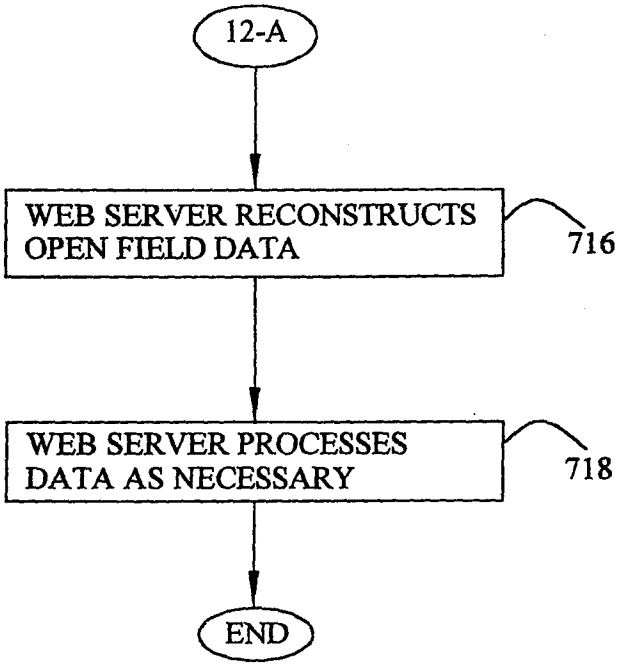
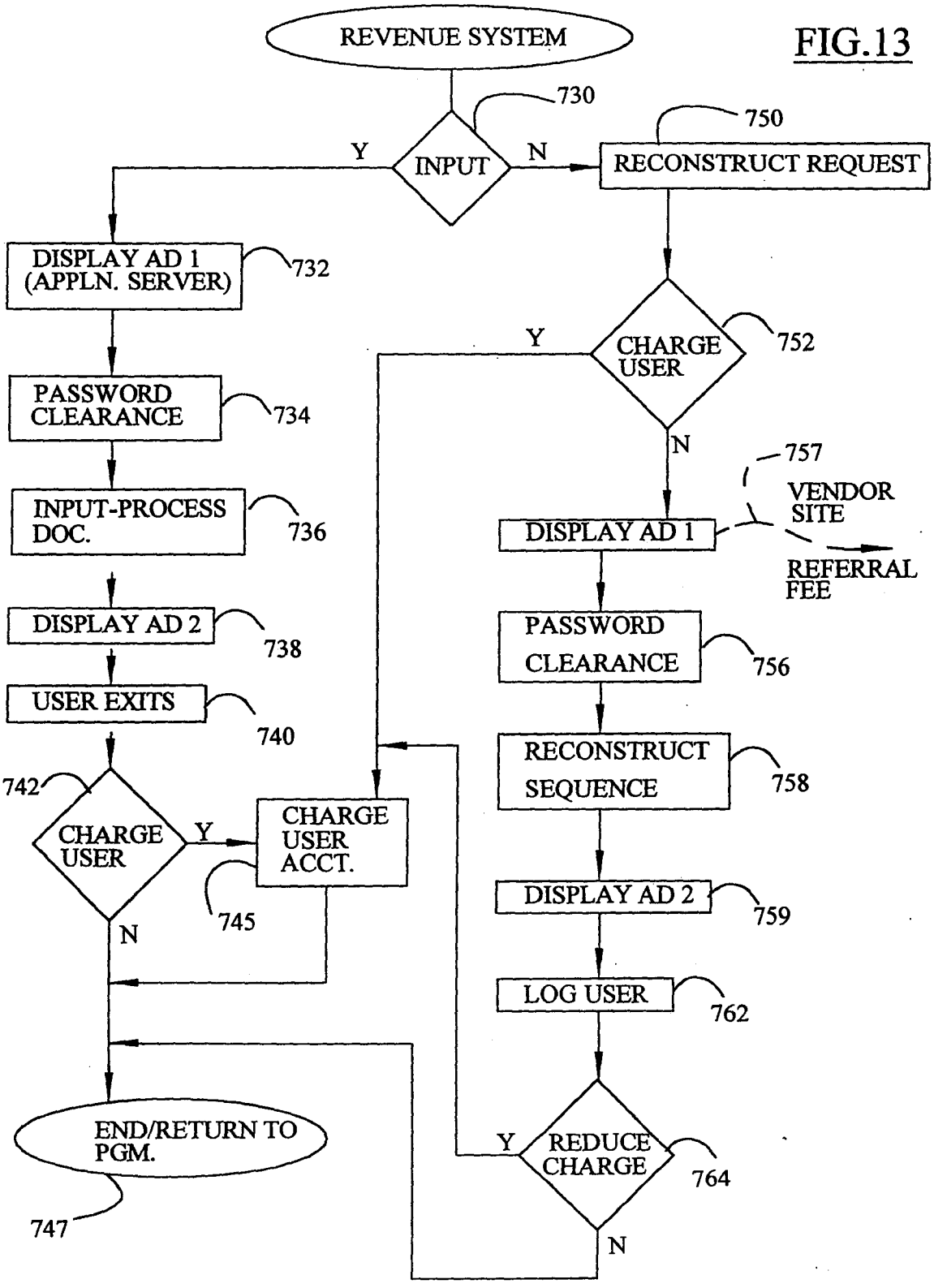

12-A
WEB SERVER RECONSTRUCTS OPEN FIELD DATA
716
WEB SERVER PROCESSES DATA AS NECESSARY
718
END

FIG.13


REVENUE SYSTEM
730
INPUT
Y
N
750
RECONSTRUCT REQUEST
DISPLAY AD 1 (APPLN. SERVER)
732
PASSWORD CLEARANCE
734
INPUT-PROCESS DOC.
736
DISPLAY AD 2
738
USER EXITS
740
742
CHARGE USER
Y
CHARGE USER ACCT.
745
N
END/RETURN TO PGM.
747
Y
CHARGE USER
752
N
757
VENDOR SITE
DISPLAY AD 1
REFERRAL FEE
PASSWORD CLEARANCE
756
RECONSTRUCT SEQUENCE
758
DISPLAY AD 2
759
LOG USER
762
Y
REDUCE CHARGE
764
N

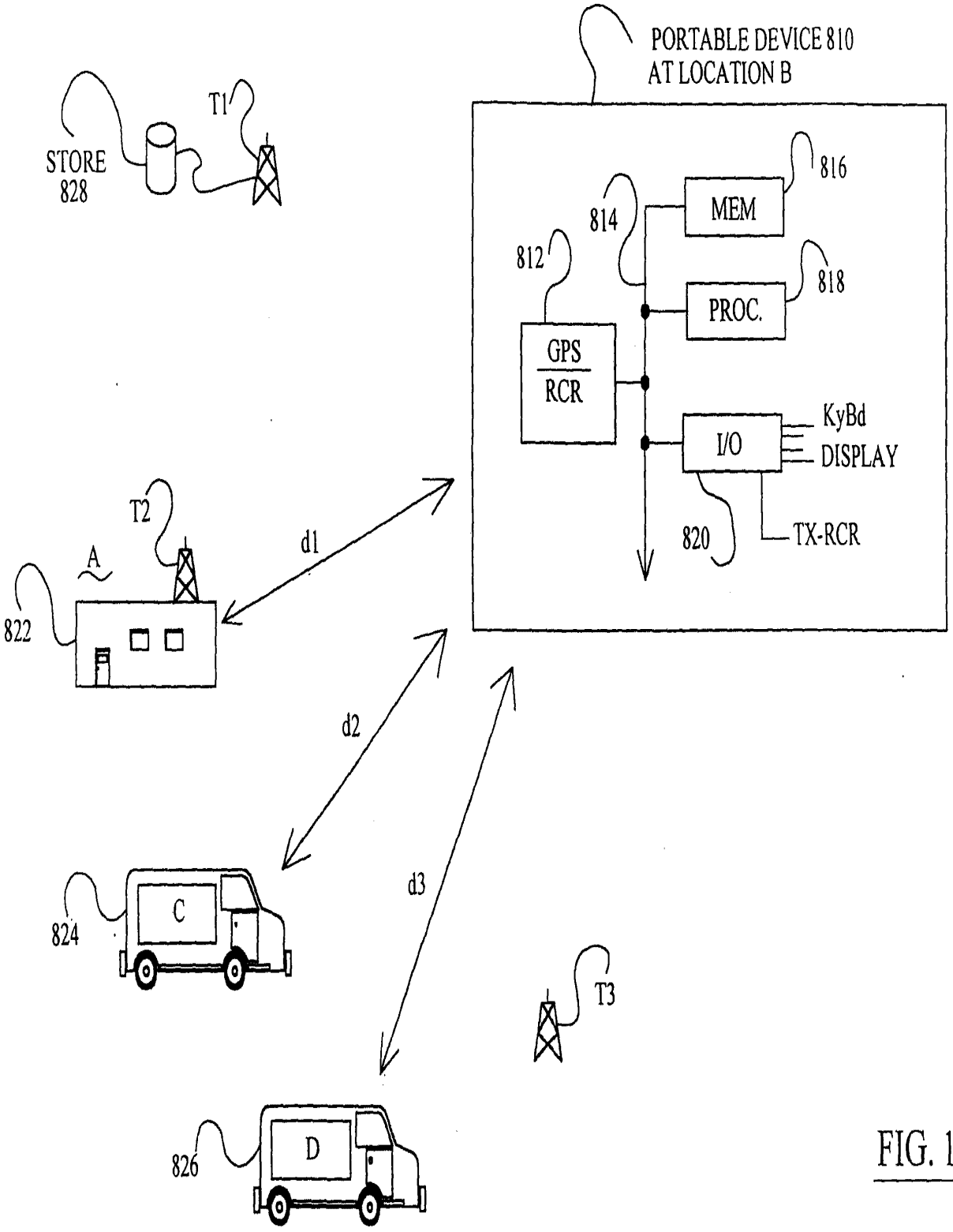

PORTABLE DEVICE 810
AT LOCATION B
816
MEM
814
812
818
PROC.
GPS
RCR
KyBd
I/O
DISPLAY
820
TX-RCR
STORE
828
T1
T2
A
822
d1
d2
d3
C
824
T3
D
826

FIG. 14

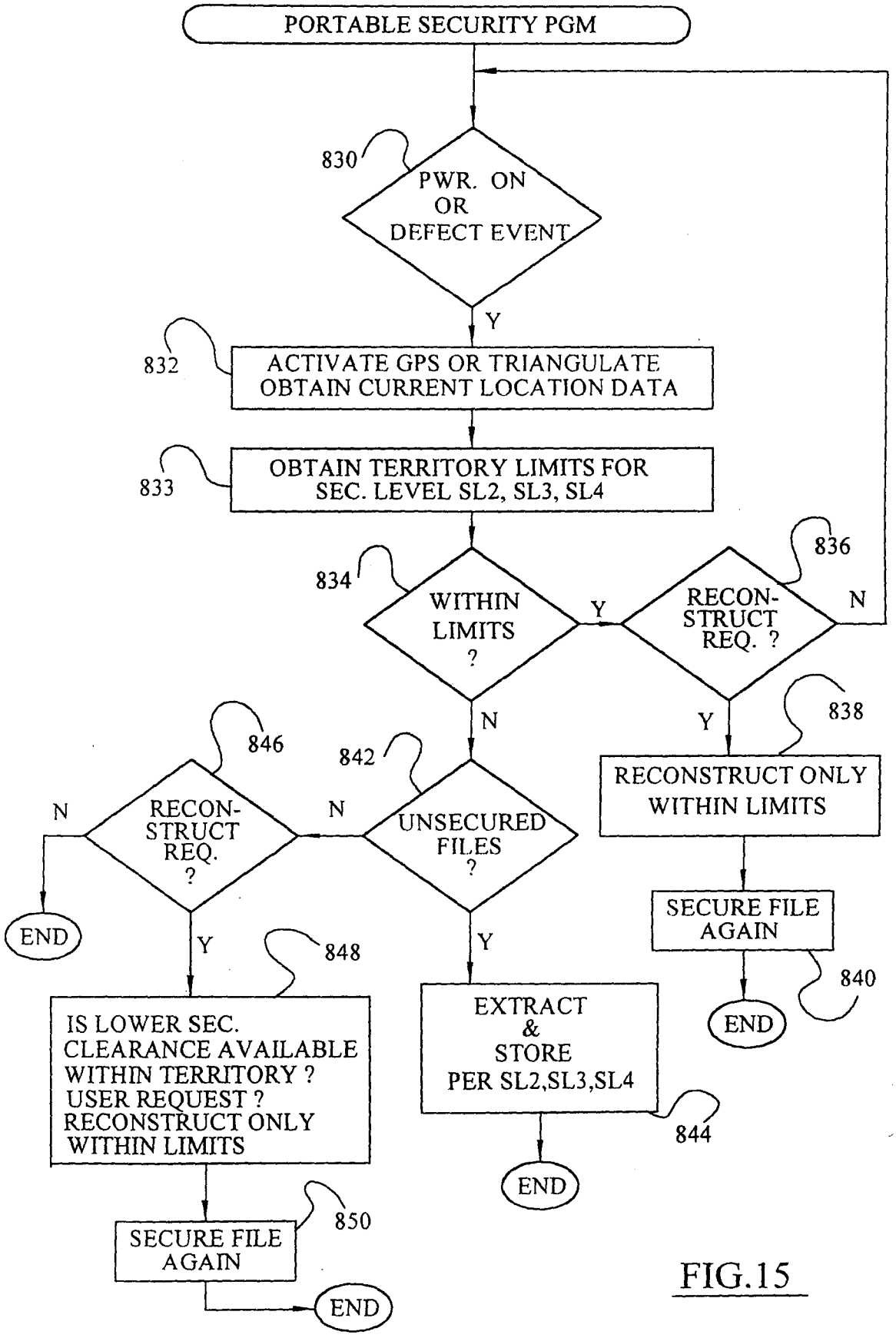

PORTABLE SECURITY PGM
830
PWR. ON OR DEFECT EVENT
Y
832
ACTIVATE GPS OR TRIANGULATE OBTAIN CURRENT LOCATION DATA
833
OBTAIN TERRITORY LIMITS FOR SEC. LEVEL SL2, SL3, SL4
834
WITHIN LIMITS ?
Y
836
RECON-STRUCT REQ. ?
N
Y
838
RECONSTRUCT ONLY WITHIN LIMITS
SECURE FILE AGAIN
840
END
N
842
UNSECURED FILES ?
N
846
RECON-STRUCT REQ. ?
N
END
Y
848
IS LOWER SEC. CLEARANCE AVAILABLE WITHIN TERRITORY ? USER REQUEST ? RECONSTRUCT ONLY WITHIN LIMITS
Y
EXTRACT & STORE PER SL2,SL3,SL4
844
END
SECURE FILE AGAIN
850
END

FIG.15

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

TERMINAL DISCLAIMER

Commissioner for Patents
Alexandria, VA 22313-1450
Sir:

Petitioner, Digital Doors, Inc., a Florida corporation, having its principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, FL 33140, represents that it is the owner by assignment of all rights to application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004.

The captioned application was assigned to Digital Doors, Inc. and the assignment was filed with the original application. The evidentiary document accompanying or referred to in the instant terminal disclaimer has been reviewed by the undersigned and it is certified that to the best of assignee, Digital Doors, Inc.'s knowledge and belief, title is in the assignee.

Petitioner, Digital Doors, Inc., hereby disclaims the terminal part of any patent granted on the above identified application, which would extend beyond the expiration date of any patent granted on application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004, and, except as provided below, hereby agrees that any patent so granted on the above identified application shall be enforceable only for and during such period and that the listed patents will remain commonly owned.

Petitioner, Digital Doors, Inc., is a small entity.

Petitioner does not disclaim any terminal part of any patent granted on the above identified application prior to the expiration date of the full statutory term of any patent granted on application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004, in the event that any latter patent: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. §1.321(a), has all claims canceled by a reexamination certificate, is reissued, or is otherwise terminated prior to the expiration of its statutory term as presently shortened by any terminal disclaimer, except for the separation of legal title stated above.

Petitioner expressly reserves and does not waive the right to extend the term of any patent granted on application Serial No. 09/916397, filed 07/27/2001, now U.S. Patent No. 7,103,915; Serial No. 10008209, filed on 12/06/2001, now U.S. Patent No. 7,140,044; Serial No. 10008218, filed 12/06/2001, now U.S. Patent No. 7,146,644; Serial No. 10155192, filed on 05/23/2002; Serial No. 10155525 filed on 05/23/2003, now U.S. Patent No. 7,191,252; Serial No. 10277196 filed on 12/31/2002; Serial No. 10998365 filed on 11/26/2004; and Serial No. 10998366 filed on 11/26/2004, or any patent granted on the above identified application under any statute which permits such an extension of term.

I hereby declare that all statements made herein of our own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Digital Doors, Inc.

Dated: __May 14, 2007

By: __/Robert C. Kain/ _____
Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

F:\RCK\CLIENTS\Redlich\6851-02-cip5-Term-Discl-051407.wpd

Electronic Patent Application Fee Transmittal

Application Number:	10390807
Filing Date:	19-Mar-2003
Title of Invention:	Data security system and method for portable device
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-2-cip-5

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Statutory disclaimer	2814	1	65	65
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**65**

Electronic Acknowledgement Receipt

EFS ID:	1914362
Application Number:	10390807
International Application Number:	
Confirmation Number:	6441
Title of Invention:	Data security system and method for portable device
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-2-cip-5
Receipt Date:	27-JUN-2007
Filing Date:	19-MAR-2003
Time Stamp:	10:42:17
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$65
RAM confirmation Number	6271
Deposit Account	031231
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	6851-02-cip5-resp-non-comply-062707.pdf	22032	no	1
Warnings:					
Information:					
2	Amendment - After Non-Final Rejection	6851-02-cip5-Amdt-1st-051007-trans.pdf	15026	no	1
Warnings:					
Information:					
3	Specification	6851-02-cip5-Amdt-1st-051007-spec.pdf	30440	no	8
Warnings:					
Information:					
4	Claims	6851-02-cip5-Amdt-1st-051007-clms.pdf	72149	no	34
Warnings:					
Information:					
5	Applicant Arguments/Remarks Made in an Amendment	6851-02-cip5-Amdt-1st-051007-remarks-062707.pdf	81768	no	19
Warnings:					
Information:					
6	Extension of Time	6851-02-cip5-Req-Ext-Time-051007.pdf	29895	no	1
Warnings:					
Information:					
7	Drawings	6851-02-cip5-dwg-050807.pdf	401176	no	20
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
8	Terminal Disclaimer Filed	6851-02-cip5-Term-Discl-051407.pdf	113523	no	3
Warnings:					
Information:					

9	Fee Worksheet (PTO-06)	fee-info.pdf	8135	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	774144	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Filed: March 19, 2003

Group 2137
Examiner M. Pyzocha

For: Data Security System and Method for Portable Device

Response

Commissioner for Patents
Alexandria, VA 22313-1450

In response to the Notice of Non-Compliant Amendment dated June 22, 2007, applicant re-submits the amendment filed on May 14, 2007 correctly signed by applicants' attorney.

Please debit or credit Deposit Account no. 03-1231 for any overpayments, underpayments or fees. This filing includes:

(a) Response to Notice of Non-Compliant Amendment (1 pg.)
(b) Amendment Cover page - transmittal (1 pg., p. 1)
(c) Specification (8 pgs., pp. 2 - 9)
(d) Claims (33 pgs., pp. 10 - 42)
(e) Remarks (19 pgs., pp. 43 - 61)(includes Appendix Showing Support)
(f) Request for a One Month Extension of Time (1 pg.)
(g) Replacement Formal Drawings (21 pgs.)
(h) Terminal Disclaimer (3 pgs.)

Respectfully submitted,

By ____/Robert Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, FL 33316-1153
Telephone: 954-768-9002,
Facsimile: 954-768-0158

Certificate of e-Filing

I hereby certify that this correspondence is being e-filed with Commissioner for Patents, Alexandria, VA on June 27, 2007.

___/Robert Kain/_____
Robert C. Kain, Jr.
Reg. No. 30,648

\\Tiger\data share\RCK\CLIENTS\Redlich\Patents\6851-02-cip5-resp-non-comply062707.wpd

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/390,807	03/19/2003	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/14/2007**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 169	Minus	** 146	= 23	X $25 =	575	OR	X $ =	
Independent (37 CFR 1.16(h))	* 9	Minus	***8	= 1	X $100 =	100	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	675	OR	TOTAL ADD'L FEE	

AMENDMENT **06/27/2007**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 169	Minus	** 169	= 0	X $25 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 9	Minus	*** 9	= 0	X $100 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
CORALIA -. BETANCOURT

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	10/390,807	REDLICH ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 6/27/07	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
BRIAN

U.S. Patent and Trademark Office

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	738	(726/27).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/26 09:29
L2	10	L1 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:29
L3	548	(715/751).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/26 09:30
L4	7	L3 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:30
L5	1440	(715/530).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/26 09:30
L6	12	L5 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:30
L7	448	(713/166).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/26 09:30
L8	6	L7 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:30
L9	3516	(709/229).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/26 09:30
L10	39	L9 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:33
L11	1886	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:31
L12	57184	(extract$4 filter$4) with location	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:32

EAST Search History

L13	934	L12 same GPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:31
L14	3	L13 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:31
L15	59	GPS same gambling	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:31
L16	0	L15 and @ad<"20001112" and @pd>"20061207"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:31
L17	57	(REDLICH near RON) (NEMZOW nearMARTIN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:32
L18	1418	(extract$4 filter$4) same secur$4 near2 level	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:33
L19	226	18 same (location GPS)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:33
L20	56	L19 and @ad<"20001112"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:33
L21	56	20 not redlich.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:34
L22	12	(extract near (store memory database) with security adj level). clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:35

EAST Search History

L23	22	(filter$4 with security adj level).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:38
L24	16	(reconstruct$4 with security adj level).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:39
L25	0	((region location) same filter$4 same security adj level).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:41
L26	3	((region location) same extract$4 same security adj level).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 09:41

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

4897 7590 08/09/2007

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/09/2007

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	03/19/2003	Ron M. Redlich	6851-2-CIP-5	6441

TITLE OF INVENTION: DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$700	$300	$0	$1000	11/09/2007

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2007.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

4897 7590 08/09/2007

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	03/19/2003	Ron M. Redlich	6851-2-CIP-5	6441

TITLE OF INVENTION: DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$700	$300	$0	$1000	11/09/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
PYZOCHA, MICHAEL J	2137	726-027000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	03/19/2003	Ron M. Redlich	6851-2-CIP-5	6441

4897 7590 08/09/2007

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/09/2007

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 914 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 914 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	10/390,807	REDLICH ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/27/07*.

2. ☒ The allowed claim(s) is/are *1-37,39-60,62-77 and 79-146*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☒ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

1. Amendment filed 06/27/2007 has been received and considered.

2. A substitute oath is required to reflect the corrected priority data put forth in the received amendment.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment, to cancel claims 147-172 without denying the right to prosecute these claims in a continuation, was given in a telephone interview with Robert Kain on 07/25/2007.

The application has been amended as follows:

Claims 147-172 (Canceled)

Allowable Subject Matter

4. Claims 1-37, 39-60, 62-77, and 79-146 are allowed.

5. The following is an examiner's statement of reasons for allowance: The prior art teaches filtering data based on security levels and storing the data and allowing full or partial reconstruction of data based on a respective security clearance. The prior art fails to teach storing only the extracted data for each security level at an extract store for each security level and storing the remainder data at a separate remainder store. The terminal disclaimer filed 06/27/2007 has overcome all double patenting rejections.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Fletcher and Tachibana teach methods of filtering data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael

Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

PTO/SB/42 (10-96)

Sheet 1 of 3

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number 10/390807
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

31032 U.S. PTO 10/390807 03/19/03

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mmp	6,192,472 B1	2/20/2001	Garay et al.	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al.	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al.	707	1	
	5,832,212	11/3/1998	Cragun et al.	395	188.01	
mmp	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
mmp	WO 00/75779 A2		WIPO			

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mmp	Ingrom i100, Content Security Appliance (2 pages) printed 6/25/01	mmp
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	printed 6/25/01 mmp
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)	August 2000 mmp
	ZD Net Interactive iWeek - IBS, SAP: XML to Boost Security Integration (1 page)	May 3, 1999 mmp
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	
mmp	Cisco Systems' Intrusion Detection System (IDS) Host Sensor 2.0 product data sheet and technical overview, 10 pgs., July 3, 2000, www.cisco.com	

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number 10/390 807
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mp	5,892,908	4/6/1999	Hughes et al.	395	200.8	
	5,423,032	6/6/1995	Byrd et al.	395	600	
	6,044,375	3/28/2000	Shmueli et al.	707	101	
	5,715,399	2/3/1998	Bezos	395	227	
	5,982,897	11/9/99	Clark	380	21	
	6,370,629B1	4/9/02	Hastings et al.	711	163	
mp	6,154,172	11/28/00	Piccionelli et al.	342	357.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mp	"Protecting Privacy using the Decentralized Label Model" A. Myers, Cornell Univ. 1/1/2000	
	Mimesweeper Product Data sheet, Resoft Int'l LLC., Nov. 12, 2001 re-soft.com/product/mimeswep.	
	Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July 2000.	
	Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys., Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.	
	Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001.	
mp	Intelligence Community System for Information Sharing (ICSIS) Relationship to the Global Information Grid (GIG), White Paper, 27 March 2001	

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-2 CIP-5	Application Number 10/190807
	Applicant(s) Ron Redlich	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
MWP	5,887,269	3/23/99	Brunts et al.	701	208	
	5,842,023	11/24/98	Tsumura	395	712	
	5,778,304	7/7/98	Grube et al.	455	33.1	
	5,757,916	5/26/98	MacDoran et al.	380	25	
	5,933,498	8/3/99	Schneck et al	380	4	
	6,078,907	6/20/00	Lamm	705	40	
	5,581,682	12/3/96	Anderson et al.	395	792	
MWP	0073313 A1	6/13/02	Brown et al.	713	165	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
MMP	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
MMP	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

MMP	MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
MMP	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER [signature] DATE CONSIDERED 12/7/04

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mm	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
mm	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mm	Ingrian i100, Content Security Appliance (1 pages)	printed 4/25/01 mm
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	printed 4/25/01 mm
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigrigg, John D. Strunk, Gregory R. Ganger, Han Kiloccote Pradeep K. Khosla (8 pages)	August 2000 mm
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)	May 3, 1999 mm
mm	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	

EXAMINER [signature] DATE CONSIDERED 12/7/06

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mp	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
mp	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

mp	The 1996 book, Applied Cryptography, by Schneier	1996 mp
	The Uniform Resource Locator article "FOLD OC"	2/17/2000 mp
mp	Microsoft Word "Learning Microsoft Word 7.0"	7/9/97 mp

EXAMINER [signature] DATE CONSIDERED 12/7/06

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
mmp	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
mmp	6,662,189	12/9/03	Oyanagi	707	102	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER mmp DATE CONSIDERED 12/7/06

Notice of References Cited	Application/Control No. 10/390,807	Applicant(s)/Patent Under Reexamination REDLICH ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,010,681 B1	03-2006	Fletcher et al.	713/154
*	B	US-6,480,963 B1	11-2002	Tachibana et al.	726/4
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
10390807	REDLICH ET AL.
Examiner	**Art Unit**
Pyzocha, Michael	2137

ORIGINAL	
CLASS	SUBCLASS
726	27

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
713	166	193			
715	751	530			
709	229				

INTERNATIONAL CLASSIFICATION										
CLAIMED					NON-CLAIMED				
G	0	6	F	12 / 14 (2006.0)	G	0	6	F	12 / 14 (2006.0)
G	0	6	F	17 / 30 (2006.0)	G	0	6	F	17 / 30 (2006.0)

Pyzocha, Michael (Assistant Examiner)	7/26/07 (Date)	EMMANUEL L. MOISE SUPERVISORY PATENT EXAMINER	Total Claims Allowed: 143
(Legal Instruments Examiner) (Date)		(Primary Examiner) (Date) 07-26-07	O.G. Print Claim(s): 1 / O.G. Print Figure: 1

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007	07/26/2007							
1	1	✓	=							
2	2	✓	=							
6	3	✓	=							
25	4	✓	=							
26	5	✓	=							
27	6	✓	=							
28	7	✓	=							
29	8	✓	=							
30	9	✓	=							
31	10	✓	=							
32	11	✓	=							
33	12	✓	=							
34	13	✓	=							
35	14	✓	=							
36	15	✓	=							
37	16	✓	=							
38	17	✓	=							
39	18	✓	=							
40	19	✓	=							
41	20	✓	=							
42	21	✓	=							
43	22	✓	=							
44	23	✓	=							
45	24	✓	=							
3	25	✓	=							
4	26	✓	=							
5	27	✓	=							
8	28	✓	=							
9	29	✓	=							
10	30	✓	=							
11	31	✓	=							
7	32	✓	=							
12	33	✓	=							
13	34	✓	=							
14	35	✓	=							
15	36	✓	=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007	07/26/2007							
16	37	✓	=							
	38	✓	-							
17	39	✓	=							
18	40	✓	=							
19	41	✓	=							
20	42	✓	=							
21	43	✓	=							
22	44	✓	=							
23	45	✓	=							
24	46	✓	=							
46	47	✓	=							
47	48	✓	=							
48	49	✓	=							
65	50	✓	=							
66	51	✓	=							
67	52	✓	=							
68	53	✓	=							
69	54	✓	=							
70	55	✓	=							
71	56	✓	=							
72	57	✓	=							
73	58	✓	=							
74	59	✓	=							
75	60	✓	=							
	61	✓	-							
76	62	✓	=							
77	63	✓	=							
78	64	✓	=							
79	65	✓	=							
80	66	✓	=							
49	67	✓	=							
50	68	✓	=							
51	69	✓	=							
52	70	✓	=							
53	71	✓	=							
54	72	✓	=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007	07/26/2007							
55	73	✓	=							
56	74	✓	=							
57	75	✓	=							
58	76	✓	=							
59	77	✓	=							
	78	✓	-							
60	79	✓	=							
61	80	✓	=							
62	81	✓	=							
63	82	✓	=							
64	83	✓	=							
81	84	✓	=							
82	85	✓	=							
83	86	✓	=							
84	87	✓	=							
85	88	✓	=							
86	89	✓	=							
87	90	✓	=							
88	91	✓	=							
89	92	✓	=							
90	93	✓	=							
91	94	✓	=							
92	95	✓	=							
93	96	✓	=							
94	97	✓	=							
95	98	✓	=							
96	99	✓	=							
97	100	✓	=							
98	101	✓	=							
99	102	✓	=							
100	103	✓	=							
101	104	✓	=							
102	105	✓	=							
103	106	✓	=							
104	107	✓	=							
105	108	✓	=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007	07/26/2007							
106	109	✓	=							
107	110	✓	=							
108	111	✓	=							
109	112	✓	=							
110	113	✓	=							
111	114	✓	=							
112	115	✓	=							
113	116	✓	=							
114	117	✓	=							
115	118	✓	=							
116	119	✓	=							
117	120	✓	=							
118	121	✓	=							
119	122	✓	=							
120	123	✓	=							
121	124	✓	=							
122	125	✓	=							
123	126	✓	=							
124	127	✓	=							
125	128	✓	=							
126	129	✓	=							
127	130	✓	=							
128	131	✓	=							
129	132	✓	=							
130	133	✓	=							
131	134	✓	=							
132	135	✓	=							
133	136	✓	=							
134	137	✓	=							
135	138	✓	=							
136	139	✓	=							
137	140	✓	=							
138	141	✓	=							
139	142	✓	=							
140	143	✓	=							
141	144	✓	=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/16/2007	07/26/2007							
142	145	✓	=							
143	146	✓	=							
	147		-							
	148		-							
	149		-							
	150		-							
	151		-							
	152		-							
	153		-							
	154		-							
	155		-							
	156		-							
	157		-							
	158		-							
	159		-							
	160		-							
	161		-							
	162		-							
	163		-							
	164		-							
	165		-							
	166		-							
	167		-							
	168		-							
	169		-							
	170		-							
	171		-							
	172		-							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10390807	REDLICH ET AL.
	Examiner	Art Unit
	Pyzocha, Michael	2137

SEARCHED

Class	Subclass	Date	Examiner
726	27	12/8/06	MJP
715	751, 530	12/8/06	MJP
713	166	12/8/06	MJP
709	229	12/8/06	MJP
updated	search	7/26/07	MJP
713	193	7/26/07	MJP

SEARCH NOTES

Search Notes	Date	Examiner
BRS search USPAT, USPGPUB, EPO, JPO, IBM, DERWENT see attached search history	12/8/06	MJP
all claims have been reviewed for 35 USC non-statutroy subject matter	12/8/06	MJP
new and updated BRS search, see attached search history	7/26/07	MJP

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	27	7/26/07	MJP
715	751, 530	7/26/07	MJP
713	166, 193	7/26/07	MJP
709	226	7/26/07	MJP

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 6441

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/390,807	03/19/2003	709	2137	6851-2-cip-5

APPLICANTS

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;

OK mpp 7/24/07

**** CONTINUING DATA ***************************

This application is a CIP of 10/277,196 12/31/2002 *
and is a CIP of 10/115,192 04/02/2002 *
and is a CIP of 10/155,525 05/23/2002 PAT 7,191,252
and claims benefit of 60/400,062 08/02/2002
and claims benefit of 60/400,112 08/02/2002
and claims benefit of 60/400,406 08/02/2002
and claims benefit of 60/400,407 08/02/2002
and is a CIP of 10/008,209 12/06/2001 PAT 7,140,044
and is a CIP of 10/008,218 12/06/2001 PAT 7,146,644
and is a CIP of 09/916,397 07/27/2001 PAT 7,103,915
which claims benefit of 60/260,398 01/09/2001 *
and claims benefit of 60/287,813 05/02/2001
and claims benefit of 60/267,944 02/12/2001
and claims benefit of 60/247,242 11/13/2000
and claims benefit of 60/247,232 11/13/2000
(*)Data provided by applicant is not consistent with PTO records.

OK mpp 7/24/07

**** FOREIGN APPLICATIONS ***************************

NONE mpp 7/24/07

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ****
06/19/2003

Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		FL	20	146	8

ADDRESS

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

TITLE

Data security system and method for portable device

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
2394	No._____ to charge/credit DEPOSIT ACCOUNT	☐ 1.16 Fees (Filing)
	No._____ for following:	☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)

BIB (Rev. 05/07).

		☐ Other _____
		☐ Credit

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Robert C. Kain, Jr.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, FL 333161153

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Robert C. Kain, Jr.	(Depositor's name)
/rck/	(Signature)
08/31/2007	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	03/19/2003	Ron M. Redlich	6851-02-cip-5	6441

TITLE OF INVENTION:

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	yes	$700	$300	$1000	11/09/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Robert C. Kain, Jr.
2 Fleit Kain
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Digital Doors, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Miami Beach, Florida

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. The following fee(s) are enclosed:
☑ Issue Fee
☑ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):
☐ A check in the amount of the fee(s) is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☑ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number 031231 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.
NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /rck/ Date 08/31/2007

Typed or printed name Robert C. Kain, Jr. Registration No. 30648

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	10390807
Filing Date:	19-Mar-2003
Title of Invention:	DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-2-CIP-5

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	700	700
Publication fee for republication	1505	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt

EFS ID:	2147488
Application Number:	10390807
International Application Number:	
Confirmation Number:	6441
Title of Invention:	DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-2-CIP-5
Receipt Date:	31-AUG-2007
Filing Date:	19-MAR-2003
Time Stamp:	13:34:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$1000
RAM confirmation Number	9184
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)

1	Oath or Declaration filed	6851-02-cip5-dec-signed-082107.pdf	59758 805e504ebb6751057d419667913042bd29e83664	no	2
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	6851-02-cip5-Issue-Fee-Form-083107.pdf	46824 adc61169c65855b40a1483187555921f73d95a76	no	1
Warnings:					
Information:					
3	Fee Worksheet (PTO-06)	fee-info.pdf	8266 84205ac58804398f4d81d995f895ea8f0dcd065a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	114848		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SUPPLEMENTAL DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled Data Security System and Method For Portable Device the specification of which

(check one) ☐ is attached hereto.

☐ was filed on March 19, 2003

as Application Serial No. 10/390,807

and was amended on 06/27/2007 (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	☐ Yes	☐ No
(Number)	(Country)	(Day/Month/Year Filed)	☐ Yes	☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status)
10/277,196	12/31/02	pending
09/916,397	07/27/01	patented
10/008,209	12/6/01	patented
10/008,218	12/6/01	patented
10/155,192	05/23/02	pending
10/155,525	05/23/02	patented

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

60/260,398, filed Jan. 9, 2001 (Provisional Application No.) 60/287,813, filed May 2, 2001 (Provisional Application No.) 60/267,944, filed February 12, 2001 (Provisional Application No.)

60/247,242, filed November 13, 2000 (Provisional Application No.) 60/247,232, filed November 13, 2000 (Provisional Application No.) 60/400,062, filed August 2,2002 (Provisional Application No.)

60,400,112, filed August 2, 2002 (Provisional Application No.) 60/400,406, filed August 2, 2002 (Provisional Application No.) 60/400,407, filed August 2, 2002 (Provisional Application No.)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon. **POWER OF ATTORNEY**: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. Robert C. Kain, Jr., Reg. No. 30,648; Martin Fleit, Reg. No. 16,900; Jon A. Gibbons, Reg. No. 37,333; Jose Gutman, Reg. No. 35,171; Steve Bongini, Reg. No. 40,917; and Paul D. Bianco, Reg. 43,5000.

Send Correspondence to: Robert C. Kain, Jr., **Customer Number 004897**
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153

Direct Telephone Calls to: Robert C. Kain, Jr., (954) 768-9002

Ron M. Redlich
Full name of sole or first inventor

Inventor's signature 8.21.07 Date

Miami Beach, FL
Residence

U.S.
Citizenship

4201 Collins Avenue, Apt. 2103
Post Office Address

Miami Beach, FL 33140

Martin A. Nemzow
Full name of second joint inventor, if any

Inventor's signature 08-21-07 Date

Miami Beach, FL
Residence

U.S.
Citizenship

2915 Flamingo Drive
Post Office Address

Miami Beach, FL 33140

(Supply similar information and signature for third and subsequent joint inventors.)

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip5-dec-062007.wpd

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 6441

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/390,807	03/19/2003 RULE	726	2137	6851-2-CIP-5

APPLICANTS

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;

TMN 10-12-07

**** CONTINUING DATA ***************************

This application is a CIP of 10/277,196 12/31/2002 *
and is a CIP of 10/155,192 05/23/2002
and is a CIP of 10/155,525 05/23/2002 PAT 7,191,252
and claims benefit of 60/400,062 08/02/2002
and claims benefit of 60/400,112 08/02/2002
and claims benefit of 60/400,406 08/02/2002
and claims benefit of 60/400,407 08/02/2002
and is a CIP of 10/008,209 12/06/2001 PAT 7,140,044
and is a CIP of 10/008,218 12/06/2001 PAT 7,146,644
and is a CIP of 09/916,397 07/27/2001 PAT 7,103,915
which claims benefit of 60/260,398 01/09/2001 *
and claims benefit of 60/287,813 05/02/2001
and claims benefit of 60/267,944 02/12/2001
and claims benefit of 60/247,242 11/13/2000
and claims benefit of 60/247,232 11/13/2000
(*)Data provided by applicant is not consistent with PTO records.

**** FOREIGN APPLICATIONS *********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** SMALL ENTITY **
** 06/19/2003

Foreign Priority claimed ☐ yes ☐ no 35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance Verified and Acknowledged Examiner's Signature Initials	STATE OR COUNTRY FL	SHEETS DRAWING 20	TOTAL CLAIMS 146	INDEPENDENT CLAIMS 8

ADDRESS
4897

TITLE
DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE

FILING FEE RECEIVED	FEES: Authority has been given in Paper
2394	No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:

☐ All Fees
☐ 1.16 Fees (Filing)
☐ 1.17 Fees (Processing Ext. of time)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/390,807	12/25/2007	7313825	6851-2-CIP-5	6441

4897 7590 12/05/2007

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 797 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 10/390,807

Confirmation No.: 6441 Group Art 2137

Filed: March 19, 2003

For: Data Security System and Method for Portable Device

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97. Applicant's related cases are listed below.

The examiner in Serial No. 11/465309 cited the following references:

U.S. Patent No. 6,845,448 to Chaganti (Jan. 2005; 713/166)
U.S. Patent No. 6,941,459 to Hind (Sept., 2005; 713/167)
U.S. Patent No. 7,010,681 to Fletcher (Mar. 2006; 713/154)

The examiner in Serial No. 10/396,088 cited the following references:

U.S. Patent No. 6,922,696 to Lincoln
U.S. Patent No. 7,031,961 to Pitkow
U.S. Patent No. 7,089,428 to Farley
U.S. Patent No. 7,188,107 to Moon

Related Cases

Our Ref.	Serial No.	Filed
-02-div1	11/465309	08.17.2006
-02-div2	11/465350	08.17.2006
-02-con	11/465388	08.17.2006
-02-cip4-con	11/682941	03.07.2007
-02-cip5	10/390,807	March 19, 2004
-02-cip7	10/998,366	Nov. 26, 2003
-02-cip8	10/998,365	Nov. 26, 2004
-02-cip9	10/998,363	Nov. 26, 2004
-02-cip10	11/829207	09.06.2007
-03	10/396,088	Mar. 25, 2003

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By_____

Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-cip5-IDS-020409-update-pendng-IDS.wpd

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-02-CIP5	Application Number 10/390,807
Title: Data Security System and Method for Portable Device	Applicant(s) Ron M. Redlich	
	Filing Date March 19, 2003	Group Art Unit 2143

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,845,448	01/2005	Chaganti	713	166	
	6,941,459	09/2005	Hind	713	167	
	7,010,681	03/2006	Fletcher	713	154	
	6,922,696	07/2005	Lincoln	707	101	
	7,031,961	04/2006	Pitkow	707	4	
	7,089,428	05/2006	Farley	370	231	
	7,188,107	03/2007	Moon	707	5	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER DATE CONSIDERED

G:\RCK\CLIENTS\Redlich\6851-02-cip5-Form-PTO-1449-Master.wpd

Electronic Acknowledgement Receipt

EFS ID:	4738891
Application Number:	10390807
International Application Number:	
Confirmation Number:	6441
Title of Invention:	DATA SECURITY SYSTEM AND METHOD FOR PORTABLE DEVICE
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-2-CIP-5
Receipt Date:	05-FEB-2009
Filing Date:	19-MAR-2003
Time Stamp:	11:49:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	6851-02-cip5-IDS-020409-update-pendng-IDS.pdf	78331 e8f32712fecb53fccfc2efb519a44e5a5a704e42	no	3

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	78331

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.