

## 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 unscrutable audit logs --that is, they cannot be erased by client-side intruders -- security personnel 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 dispersal. 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)).