



Patent Owner's Demonstratives

Adobe Inc. (Petitioner)

v.

Jonathan E. Jaffe (Patent Owner)

Case IPR2024-01352 - Patent 6,757,828

Prince Lobel Tye LLP

www.princelobel.com



Agenda

I. US Patent No. 6,757,828

II. Claim Construction

- “a sensor, which is tightly coupled to said memory”
- “monitoring the integrity of the tight coupling between said memory and said sensor”

III. Glass and Rieger References

- Neither Disclose a Sensor “Tightly Coupled” to a Memory
- Neither Disclose “Monitoring the Integrity of the Tight Coupling”
- Neither Disclose “OK” and “Error” Signals

IV. Serret-Avila Reference

- Non-Analogous Art
- POSITA Would Not Have Been Motivated to Combine
- Does Not Disclose “OK” Signal



I. U.S. Patent No. 6,757,828

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

3

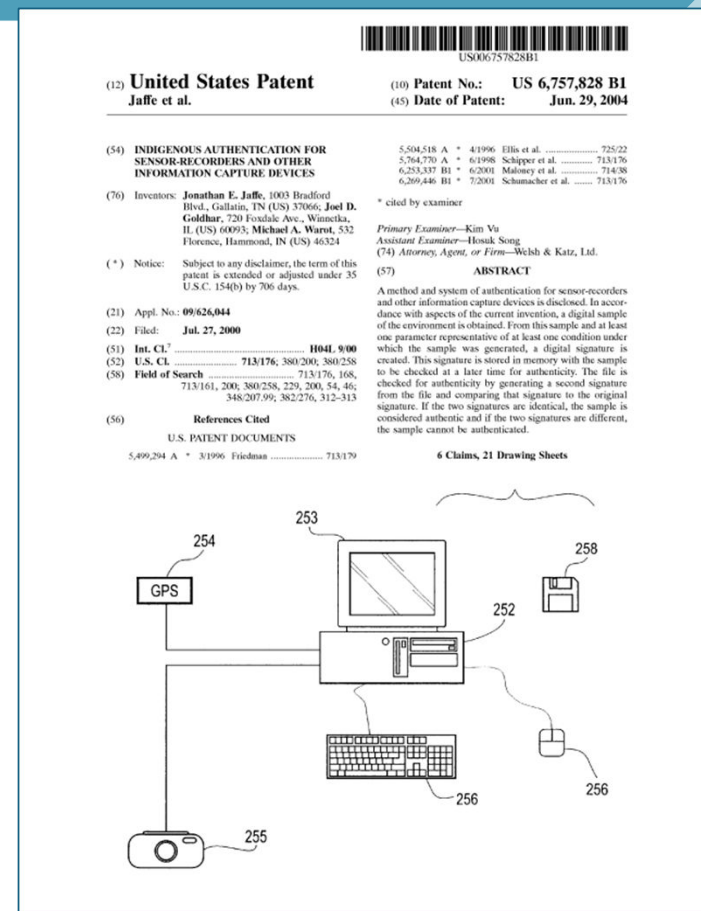
U.S. Patent No. 6,757,828

- Authenticates digital files
- Uses a digital signature that is created using the file “as well as at least one parameter that is representative of at least one condition under which the digital sample was acquired.”

EX1001, 1:54-57

- The parameter can be information such as:
 - Date & Time file created
 - Compass Heading
 - Altitude

EX1001, 2:65-3:6



POR at 3

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

4

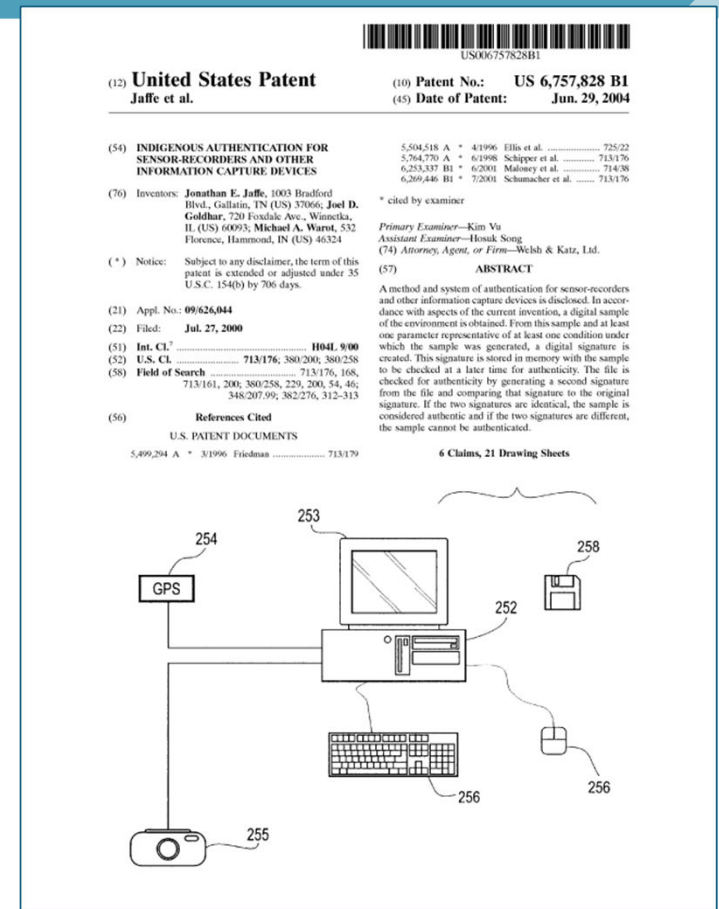
U.S. Patent No. 6,757,828

- Authenticity determined by creating a second signature from the stored file and at least one of the parameters, and then comparing the signatures.

EX1001, 1:59-62

- Digital file contains the authentication information
- Signature authenticates the file
- Avoids the need for encryption

EX1001, 1:64-2:3



POR at 3-4

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

5



II. Claim Construction

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

6

Claim Construction: “a sensor, which is tightly coupled to said memory”

- **Petitioner’s Proposed Construction:** a sensor coupled to said memory via conductive traces or leads. Pet. at 10.
- **Patent Owner’s Proposed Construction:** a sensor that is electrically or physically coupled to memory in a device. POR at 9.
- **Prosecution History:** “conductive trace or lead” language was *exemplary* only.

POR at 5-9



Claim Construction: “a sensor, which is tightly coupled to said memory”

- **Prosecution History:** “exemplary” only, no clear and unmistakable disclaimer. EX1002 at 277:

Exemplary structure or method steps corresponding to this claim feature is shown in Fig. 2A of the subject application, which illustrates a processor 157 which is “tightly coupled” to a memory. In one exemplary embodiment of the present invention, the processor 157 generates a unique random string that is used for image authentication purposes. Because the processor is “tightly coupled” to the memory, it will be virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor. This means, for example, that there is no possibility for altering the image before the authentication information is generated.

- Functional emphasis in prosecution was that “there is no possibility for altering the image before the authentication information is generated.” EX1002 at 12.

POR at 5-6; Sur-Reply at 5



Claim Construction: “a sensor, which is tightly coupled to said memory”

- **Prosecution History:** Cited Schipper reference distinguished because it involved external information, not because of conductive leads or traces

The Schipper patent teaches no such “tight coupling.” In direct contrast to this, the relevant portion of the Schipper patent cited by the Examiner in the Office Action relating to this issue (column 15, lines 30-45 and 59-67) teach that authentication is accomplished by comparison of *position* information, which must originate from devices *external* to the camera, such as satellites in orbit around the earth. The Schipper system can be fooled by supplying false position signals to the recording device, which is not the case with the claimed invention. For this reason alone, new claims 9-14 should be found to be allowable over the Schipper patent.

- No “clear and unmistakable disclaimer.”

EX1002 at 277; POR at 10



Claim Construction: “monitoring the integrity of the tight coupling between said memory and said sensor”

- **Petitioner’s Proposed Construction:** “determining whether physical access has been gained to the coupling between said memory and said sensor.” Pet. at 11.
- **Patent Owner’s Proposed Construction:** “determining whether the physical coupling between said memory and said sensor has been accessed or disturbed.” POR at 11.
- **Specification:** Shows that the claim language is directed to monitoring the tight coupling between the sensor and the memory.

POR at 9-11

Claim Construction: “monitoring the integrity of the tight coupling between said memory and said sensor”

- **Specification:**

During the operation of the camera, internal security **14** is monitored to detect the integrity of the tight coupling of the sensor set and the recorder **6**.

EX1001 at 4:65-67

- Spec describes the system checking internal security system 14 to determine if a violation has been recorded. EX1001 at 5:44-46. If security is compromised, a security violation is appended to the image. EX1001 at 6:64-66.
- Specification and claim language centers on the physical coupling between the sensor and memory, and identifying whether the coupling itself has been disturbed.

POR at 9-10; Sur-Reply at 9



Claim Construction: “monitoring the integrity of the tight coupling between said memory and said sensor”

- **Prosecution History:**

internal security has been compromised. This means that, for example, a signal is generated if the device that prevents physical access to the interconnections between the sensor set and memory is broken.

EX1002 at 293

- Emphasis on ***monitoring*** the “***physical access***” to the “***interconnections***” between the sensor and memory

Sur-Reply at 10



III. Glass and Rieger References (Grounds 1-4)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

13

Glass - U.S. Patent No. 6,332,193

- Collects biometric data from a sensor
- Unique code that is a function of camera data attached to digitized biometric data file
- Data and code transmitted over network to a server
- Server authenticates data using a secret key and the transaction token

EX1005, Abstract

US006332193B1

(12) **United States Patent**
Glass et al.

(10) Patent No.: **US 6,332,193 B1**
(45) Date of Patent: **Dec. 18, 2001**

(54) **METHOD AND APPARATUS FOR SECURELY TRANSMITTING AND AUTHENTICATING BIOMETRIC DATA OVER A NETWORK**

(75) Inventors: **Randal Glass**, Hockessin, DE (US); **Marcos Salgunkoff**, Ulf Cahn von Seelen, both of Philadelphia, PA (US)

(73) Assignee: **Sensar, Inc.**, Moorestown, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/232,538**
(22) Filed: **Jan. 18, 1999**

(51) Int. Cl.⁷ **H04K 1/00**
(52) U.S. Cl. **713/170**
(58) Field of Search **713/170**

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,641,349	2/1987	Flom et al.	
5,131,058	* 7/1992	Pohl et al.	380/23
5,280,527	1/1994	Gullman et al.	
5,291,560	3/1994	Dugman	
5,613,004	3/1997	Cooperman et al.	
5,706,349	* 1/1998	Adrian et al.	380/25
5,768,426	6/1998	Rhodes	
5,809,139	9/1998	Gind et al.	
5,822,432	10/1998	Moskowitz et al.	
5,825,892	10/1998	Bradaway et al.	

FOREIGN PATENT DOCUMENTS

0 863 491 A1	5/1998	(EP)	
--------------	--------	------	--

0 426 432 A2 8/1991 (EP)
WO 94/19770 1/1994 (WO)
WO 96/36934 2/1996 (WO)
WO 98/50875 12/1998 (WO)

* cited by examiner

Primary Examiner—Gail Hayes
Assistant Examiner—James Scal
(74) *Attorney, Agent, or Firm*—Woodcock Washburn LLP

(57) **ABSTRACT**

A method and apparatus for collecting and securely transmitting biometric data over a network contains a sensor, preferably a camera, for collecting biometric data and code generating hardware and software. The camera data is digitized and a unique code which is a function of the digitized camera data, a secret key and a transaction token is attached to the digital file. The code may identify the sensor which acquired the biometric information, a time at which the biometric information was acquired, or a time interval during which the data is considered to be valid, and a unique transaction code. The data and code are transmitted over a network to a server which authenticates that the data has not been altered by recomputing the code using its own knowledge of the secret key and transaction token needed to generate the code. If the data is authentic the server then computes a biometric template using the data. This biometric template is then compared to a previously defined biometric template to identify the user and give the user access to a secured resource. The system can be used for online banking and Internet commerce transactions.

41 Claims, 7 Drawing Sheets

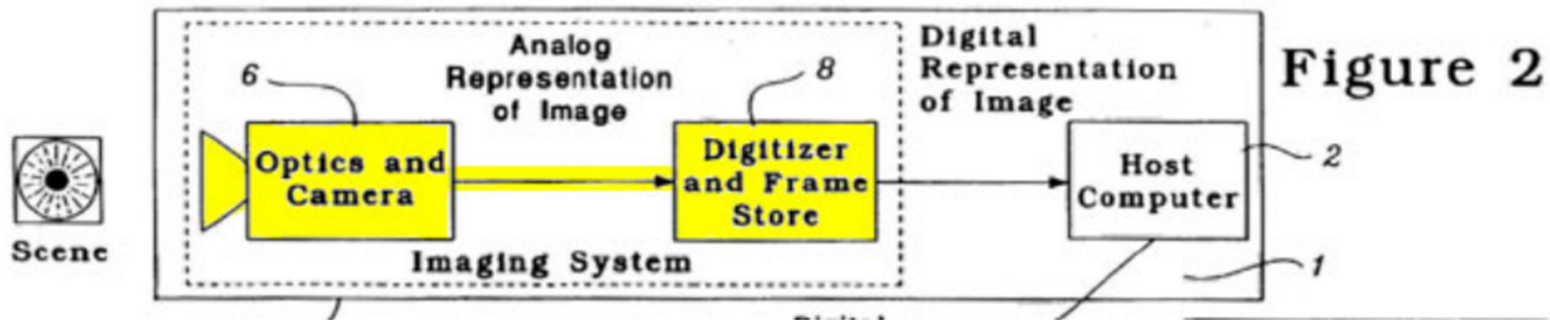
EX1005

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

14

Glass: No “sensor, which is tightly coupled to said memory”

- Petitioner’s proposed construction for “tightly coupled” requires that the connection be by “conductive leads or traces.”
- Glass discloses only an operational data path connecting the sensor (Optics and Camera 6) to memory (Digitizer and Frame Store 8); there are no details on how a data path would be implemented physically (by “conductive leads or traces” or otherwise)

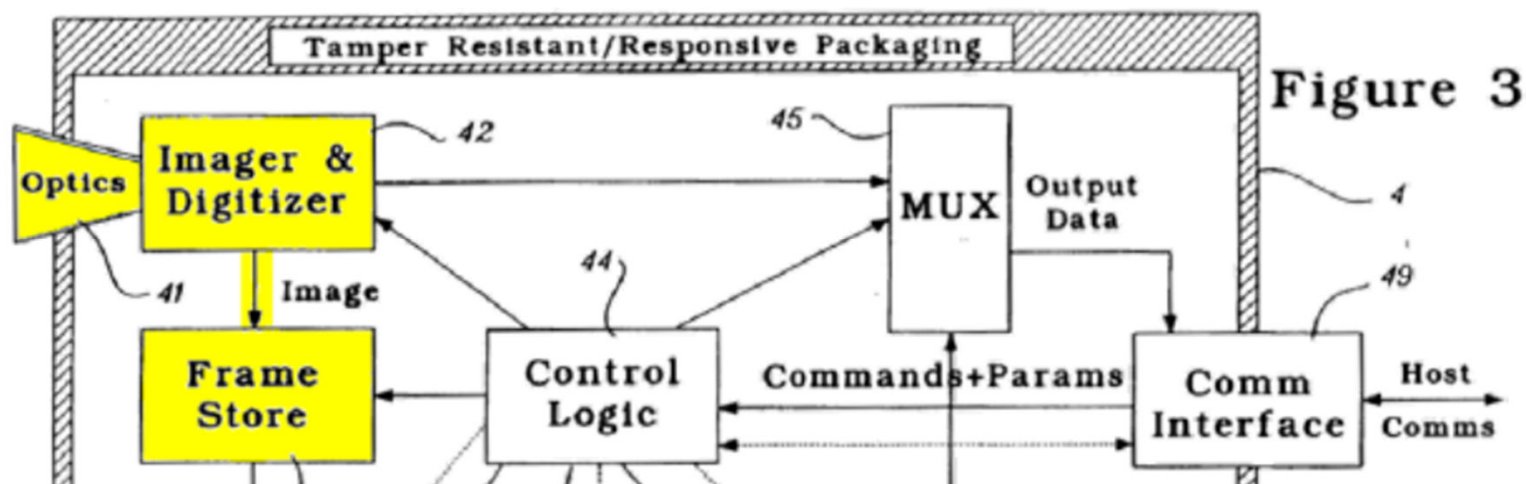


EX1003 (Glass), Fig. 2

POR at 12-14

Glass: No “sensor, which is tightly coupled to said memory”

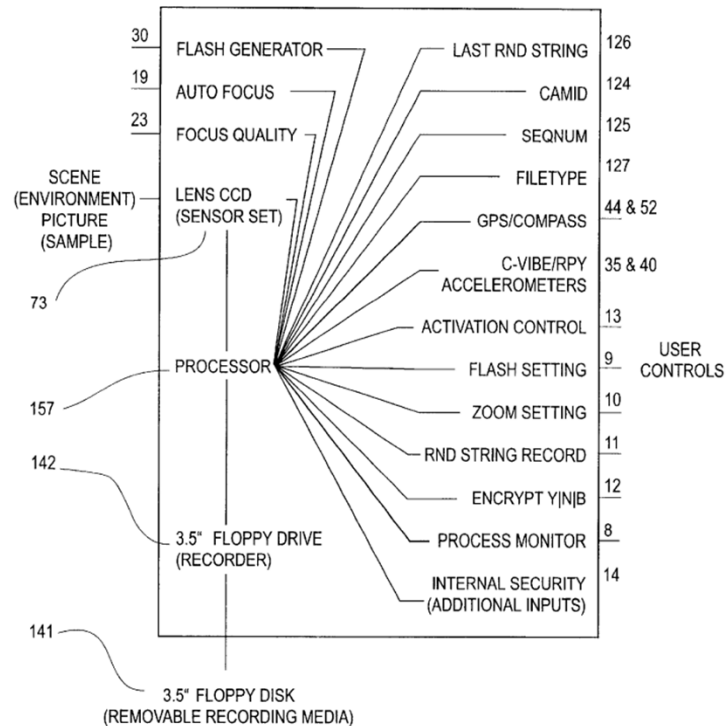
- Fig. 3 of Glass is cumulative of Fig. 2 regarding the structure of the interconnection, only disclosing an operational data path shown by an arrow.



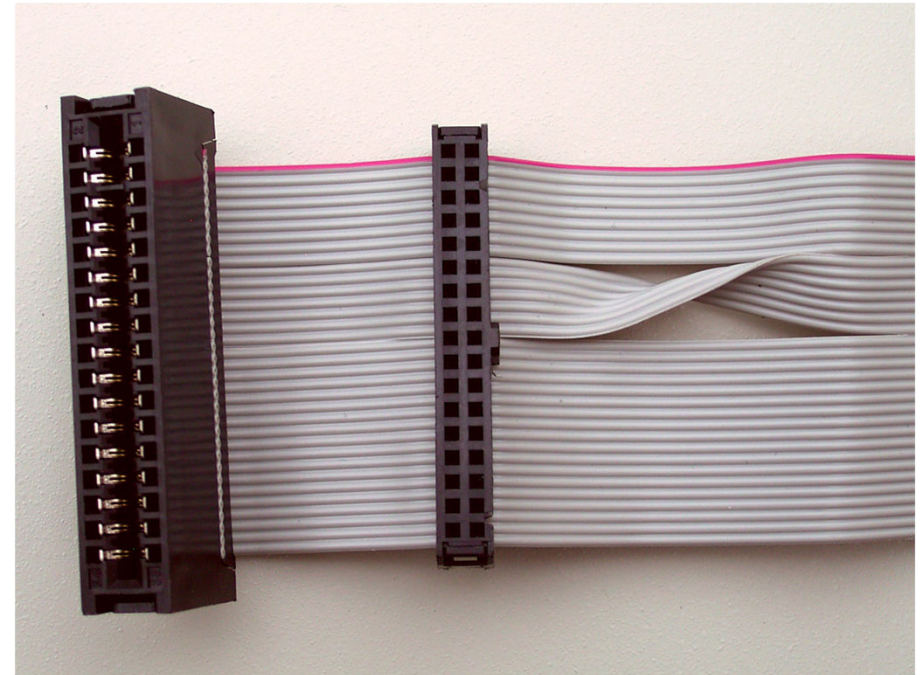
EX1003 (Glass), Fig. 3

POR at 16-17

The '828 Patent and Prosecution History do not use lines as meaning “conductive leads or traces”



EX2001, Fig. 2A



EX2010, Photo of Floppy Drive Ribbon Cable

POR at 17-18; Sur-Reply at 14

The '828 Patent and Prosecution History Do Not Use Lines as Meaning Conductive Leads or Traces

- The portion of the Prosecution History cited by Petitioner indicates only that the processor is “tightly coupled” to the memory
- No discussion that the lines in Fig. 2A depict conductive leads or traces

“utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter ” (emphasis added).

Exemplary structure or method steps corresponding to this claim feature is shown in Fig. 2A of the subject application, which illustrates a processor 157 which is “tightly coupled” to a memory.

In one exemplary embodiment of the present invention, the processor 157 generates a unique random string that is used for image authentication purposes. Because the processor is “tightly coupled” to the memory, it will be virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor. This means, for example, that there is no possibility for altering the image before the authentication information is generated.

EX2002, 277

POR at 17-18; Sur-Reply at 14

Exemplary Known Data Paths Not Using Conductive Leads or Traces

- Cables
- E.g., U.S. Patent 5,486,853 (EX2007)

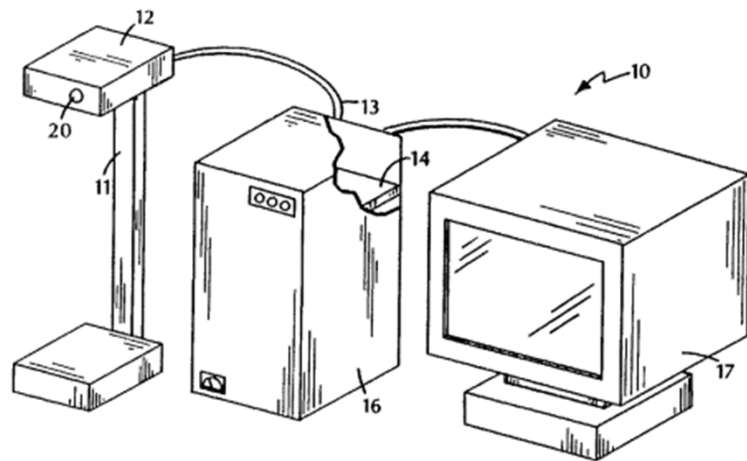


FIG. 1

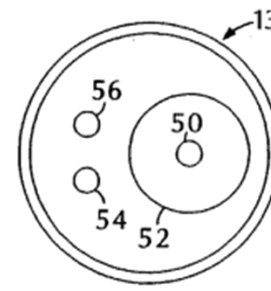


FIG. 7A

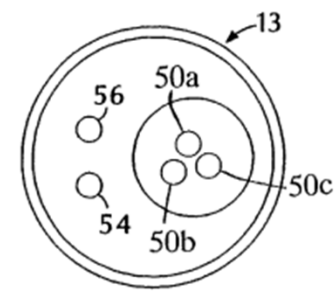


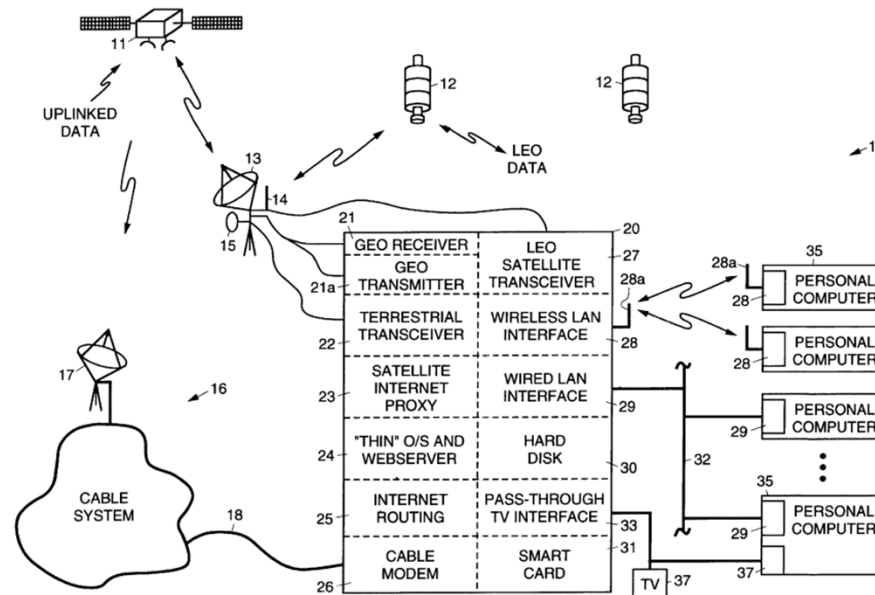
FIG. 7B

EX2007, Figs. 1, 7A, 7B

POR at 14; Sur-Reply at 14-15

Exemplary Known Data Paths Not Using Conductive Leads or Traces

- Wireless connections (including by wireless LAN, or Wi-Fi, or by satellite)
- E.g., U.S. Patent 6,377,981 (EX2009)

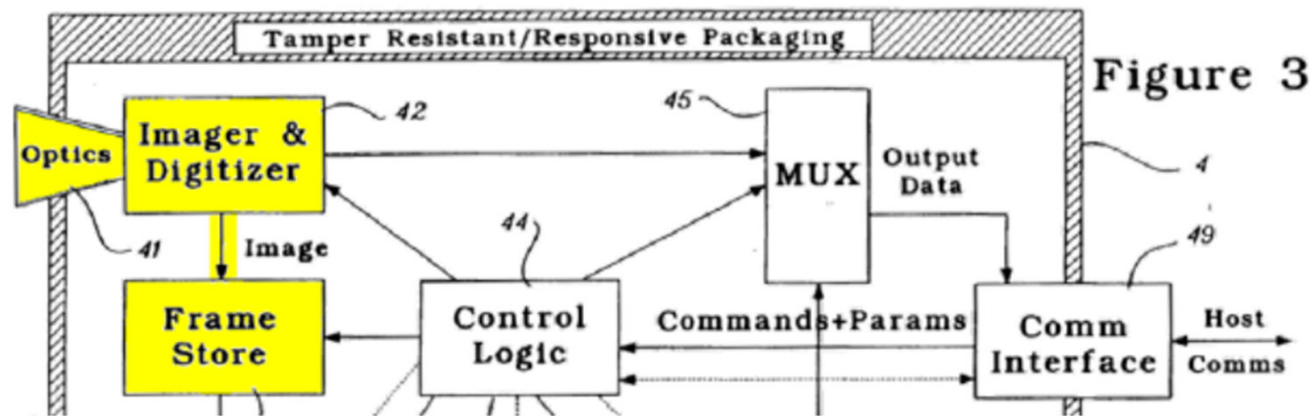


EX2009, Fig.

POR at 15-16; Sur-Reply at 15-16

Glass: No “sensor, which is tightly coupled to said memory”

- Glass does not discuss the design details of how, if at all, the sensor is connected to memory; no “conductive leads or traces” under Petitioner’s construction
- Arrows only disclose an operational connection, but fail to identify whether there is a physical or electrical connection, and therefore fails to teach limitation under POs construction as well



EX1003 (Glass), Fig. 3

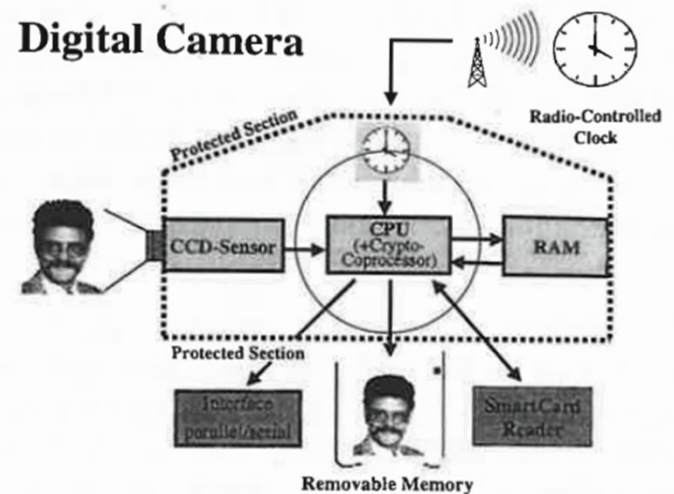
POR at 16-17, 19

Rieger – “Digital Image Recording for Court-Related Purposes”

- Depicts a camera which creates image data from a CCD sensor and saves to RAM
- Some components, including the CCD sensor, CPU, and RAM, as well as connector cables, are in a specially protected compartment
- Compartment utilizes an “electrical ‘protective shield’” that automatically deletes a key used to authenticate images when the compartment is “drilled or severed”

EX1006 at 265

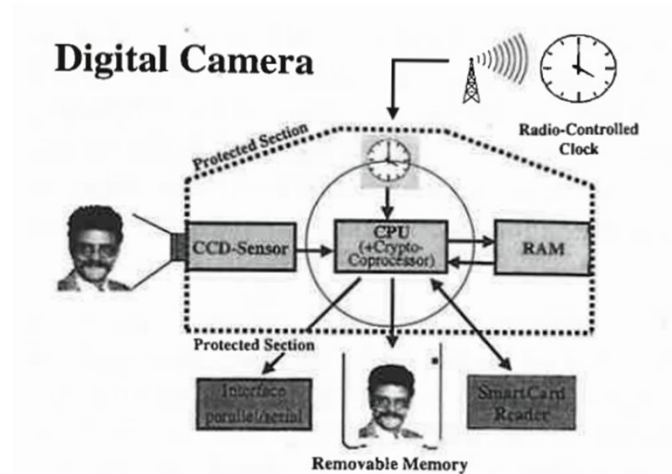
Digital Camera



EX1006 at Fig. 3

Reiger: No “sensor, which is tightly coupled to said memory”

- Like Glass, Rieger does not discuss the design details of how the sensor is connected to memory; no “conductive leads or traces” under Petitioner’s construction
- Arrows only disclose an operational connection, but fail to identify whether there is a physical or electrical connection, and therefore fail to teach limitation under POs construction as well

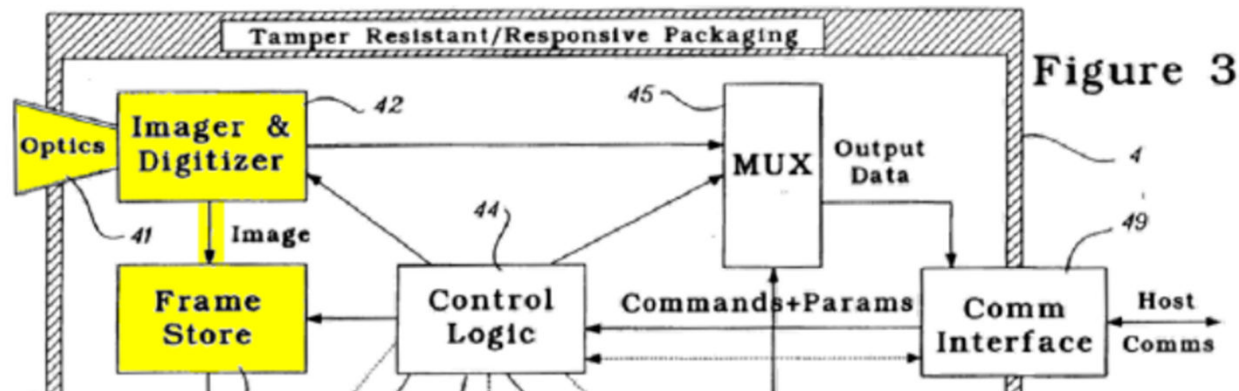


EX1006 (Rieger), Fig. 3

POR at 28-29, 34-35

Glass: No “monitoring the integrity of the tight coupling”

- Both proposed constructions require monitoring the coupling between the sensor and the memory
- Glass does not monitor the interconnection between the sensor and the memory
- Glass monitors the tamper resistant package surrounding the components, not the connection itself.



EX1003 (Glass), Fig. 3

POR at 20-23



Glass: No “monitoring the integrity of the tight coupling”

- As explained, specification discloses monitoring the integrity of the coupling, not merely a package or compartment surrounding the coupling

During the operation of the camera, internal security 14 is monitored to detect the integrity of the tight coupling of the sensor set and the recorder 6.

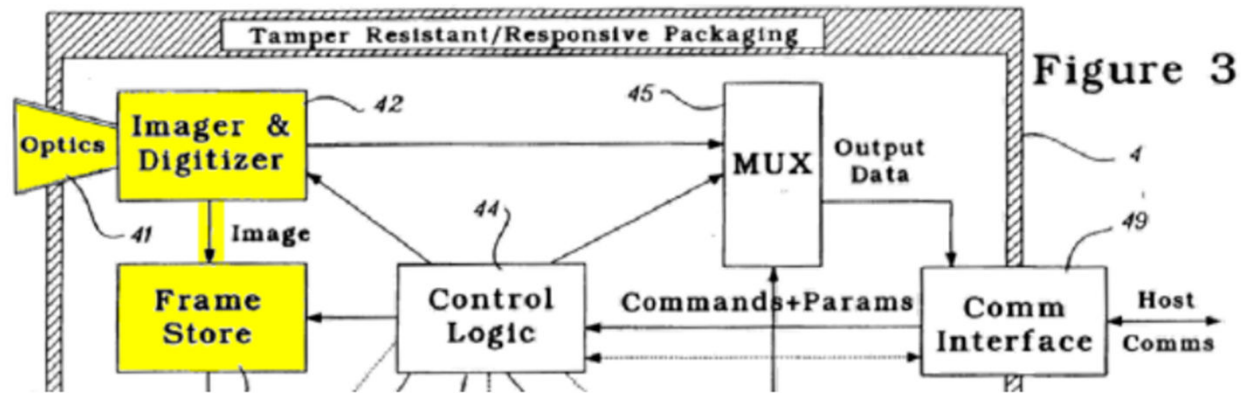
EX1001 at 4:65-67

- The system checks internal security system 14 to determine if a violation has been recorded. EX1001 at 5:44-46.
- If security is compromised, a security violation is appended to the image. EX1001 at 6:64-66.
- Specification monitors the sensor and the memory

POR at 21

Glass: No “monitoring the integrity of the tight coupling”

- Glass monitors the tamper resistant package, not the connection between the sensor and the memory.

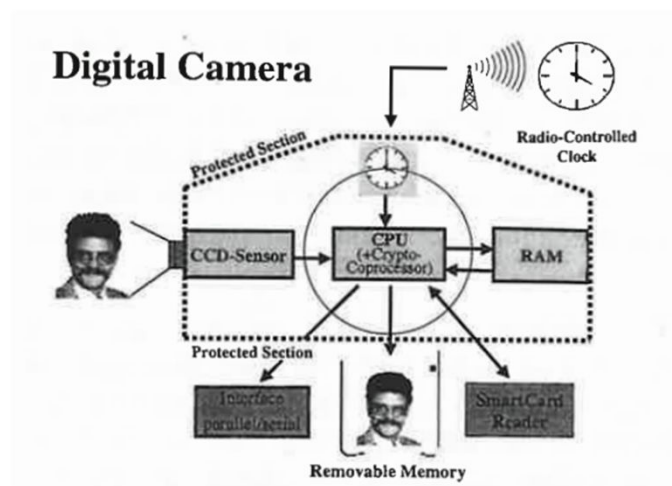


EX1003 (Glass), Fig. 3

POR at 22

Rieger: No “monitoring the integrity of the tight coupling”

- Similar to Glass, Rieger monitors a “secure compartment,” not the connection between the sensor and the memory.
- Rieger’s compartment utilizes an “electrical ‘protective shield’” (shown as “Protected Section” in the Figure) that automatically deletes a key used to authenticate images when the compartment is “drilled or severed.”



EX1006 (Rieger), Fig. 3

POR at 35-37



Glass: No “error signal that is displayed to a user ”

- Claim 1 requires “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic”
- Glass does not display error signals to the user
- Transaction results are written to a log file on the server, but this is not displayed to the user when any error is detected
- A log file is potentially never viewed unless the user opens it; no certainty that the error will actually be displayed to the user
- Because the log file is on a server, some users may have no access

POR at 23-25; Sur-Reply at 18-19



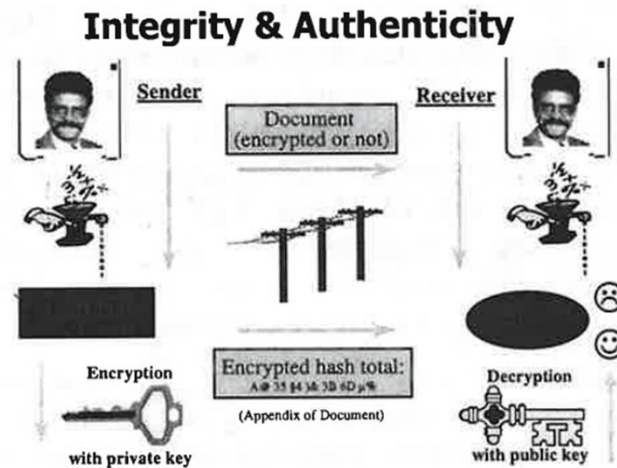
Glass: No “ok signal that is displayed to a user”

- For the same reasons as for the “error signal” limitation, Glass fails to disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic”
 - Transaction results, including successful transactions, written to a log file are not displayed to the user when any error is detected
 - Unless the user opens the log file, the results will never be displayed
 - Log file is on a server, and some users may have no access

POR at 25-27; Sur-Reply at 18-19

Rieger: No “error signal that is displayed to a user ”

- Rieger does not depict or describe generating an error signal
- Petitioner relies upon a frowning face image in a figure, but the figure depicts how authentication is performed, not what, if anything, is presented to the user
- The text of Rieger discuss hashing, but there is no discussion regarding how, or if, results are provided to users



EX1006 (Rieger), Fig. 7

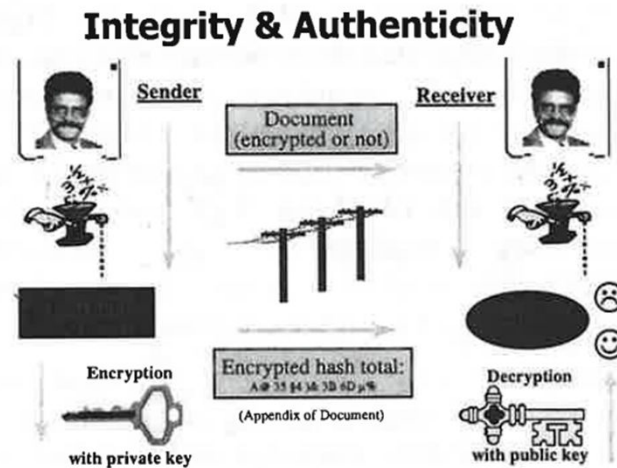
POR at 38-39; Sur-Reply at 19-20

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

30

Rieger: No “error signal that is displayed to a user ”

- For the same reasons as for the “error signal” limitation, Rieger fails to disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic”
 - The “smiling face” in Rieger Figure 7 is not described as being displayed to users
 - Figure 7 is directed to describing the hashing/authentication process, not how results of the process are communicated to users



EX1006 (Rieger), Fig. 7

POR at 40-41; Sur-Reply at 19-20

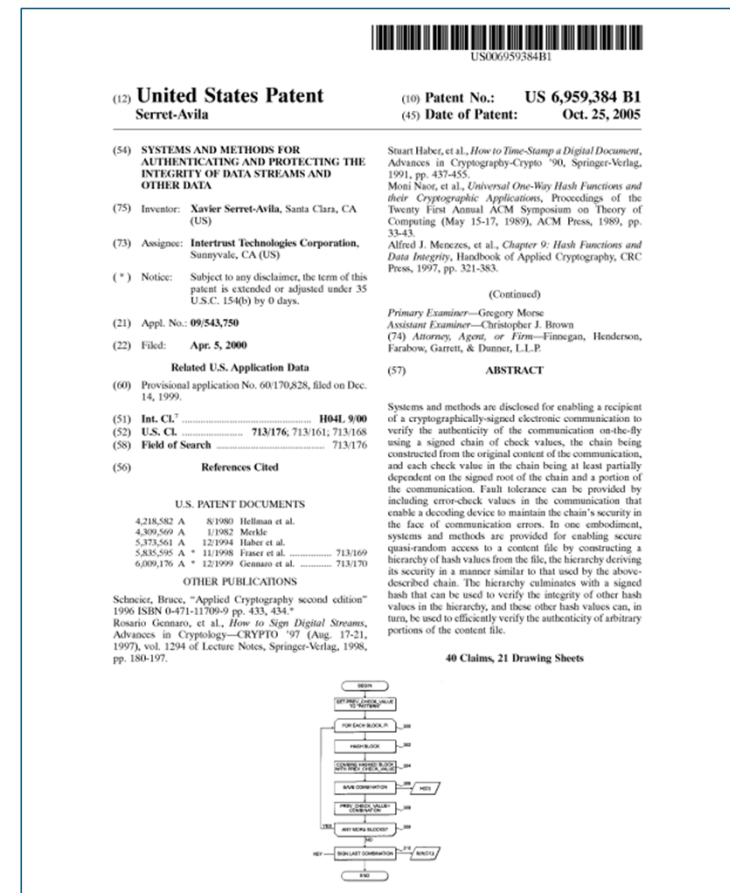


IV. Serret-Avila Reference (Grounds 5-8)

Serret-Avila - U.S. Patent No. 6,959,384

- Allows a recipient of data to verify authenticity on-the-fly
- Utilizes a chain of check values
- A signed hash is used to verify other hash values in the hierarchy
- As blocks of data are verified, they may be released for use by the receiving system

EX1011, Abstract, 7:31-34



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

33

Serret-Avila - U.S. Patent No. 6,959,384

- When a hash value check fails, the system takes defensive action, which can include displaying a warning or error message on a display. EX1011, 10:37-45.
- When a hash value check succeeds, the relevant sub-block may be released for use. EX1011, 10:28-30.

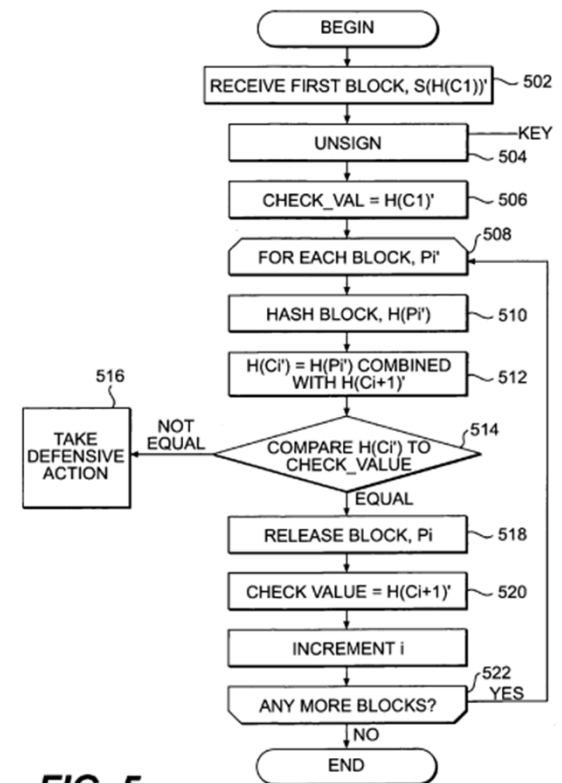


FIG. 5

EX1011, Fig. 5



Serret-Avila: Non-Analogous Art

- Grounds 4-8 attempt to combine Serret-Avila with Glass/Rieger
- Glass and Rieger (like the '828 Patent) are generally directed to authenticating images, while Serret-Avila is directed to data generally, but not to images specifically
- Serret-Avila is not directed towards authenticating digital images
- Rieger: “it is becoming increasingly difficult to detect and show proof of professional image manipulation aided by digital methods” (EX1006 at 1)
 - Different fields – Serret-Avila is not in the field of image authentication
 - Not reasonably pertinent because using parameters associated with images would not be applicable to general data, including non-image data

POR at 44-45; Sur-Reply at 20-21



Serret-Avila: No Motivation to Combine

- Glass – Offline system recording authentication determinations in a log file on a server
- Rieger – No discussion of how authentication determinations would be communicated to users
- Serret-Avila – utilizes an online system where sub-blocks are available for use as they are authenticated
- All three references involve differing, and incongruent, ways of communicating determinations to users due to the divergent online/offline natures of the systems

POR at 46; Sur-Reply at 21-22

Serret-Avila: No “ok signal that is displayed to a user”

- Claim 1 requires “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic”
- Hash value check failures result in defensive actions, including a warning message on the display screen. EX1011 at 10:39-45
- BUT there is no opposite (i.e., an ok) message to the user when the value check passes
- The sub-block may be released for use. EX1011, 10:28-30. But no actual “ok” signal is discussed in Serret-Avila

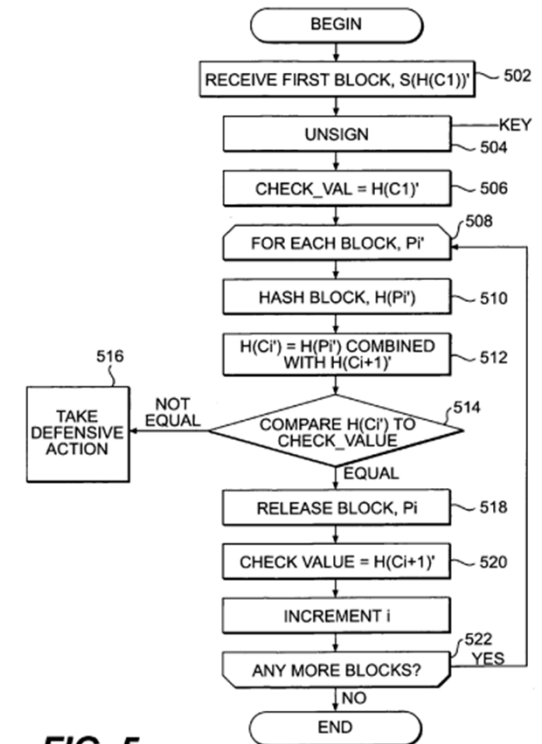


FIG. 5

EX1011, Fig. 5

POR at 47-49; Sur-Reply at 23-24

Serret-Avila: No “ok signal that is displayed to a user”

- Petitioner argues that releasing the block for use is an OK signal. But, there is no ok signal; whatever activity the block relates to merely continues
 - Analogy: A car that keeps running is not displaying a signal to the driver; it is only operating normally
 - Some data streams described in Serret-Avila are not visual; e.g., audio data that would be played on speaker. EX1011 at 15:47-50
 - Even for images, one image may be composed of multiple blocks, and there is no way to know whether any particular block is “ok” or if it has an error based upon whether an image is displayed

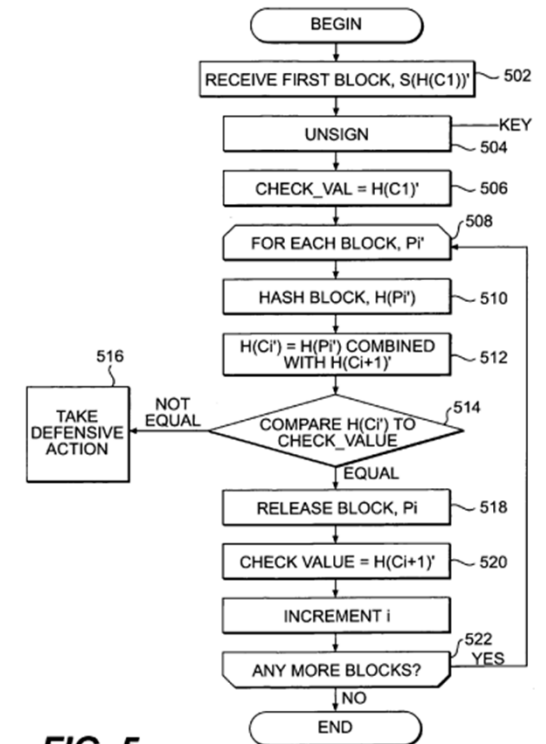


FIG. 5

EX1011, Fig. 5

POR at 47-49; Sur-Reply at 23-24

END