

Adobe Inc.
Petitioner
v.
Jonathan E. Jaffe
Patent Owner

IPR2024-01352
Patent 6,757,828 B1

Oral Argument

December 9, 2025
Petitioner Adobe's Demonstratives

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

US006757828B1

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

(10) **Patent No.:** **US 6,757,828 B1**
(45) **Date of Patent:** **Jun. 29, 2004**

(54) **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**

(70) **Inventors:** **Jonathan E. Jaffe**, 1003 Bradford Blvd., Gallatin, TN (US) 37066; **Joel D. Goldfarb**, 720 Foxdale Ave., Winnetka, IL (US) 60093; **Michael A. Warot**, 532 Florence, Hammond, IN (US) 46324

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 706 days.

(21) **Appl. No.:** **09/626,044**
(22) **Filed:** **Jul. 27, 2000**

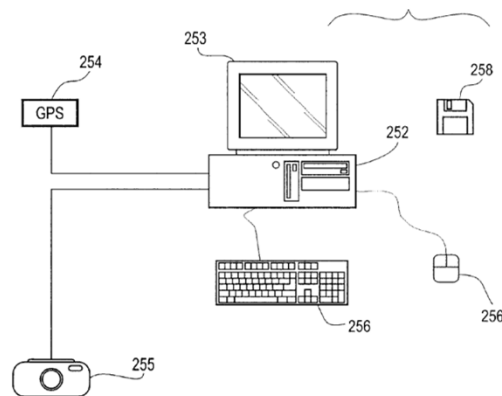
(51) **Int. CL⁷** **H04L 9/00**
(52) **U.S. CL.** **713/176; 380/200; 380/258**
(58) **Field of Search** **713/176, 168, 713/161, 200, 380/258, 229, 200, 54, 46, 348/207.99; 382/276, 312-313**

(56) **References Cited**
U.S. PATENT DOCUMENTS
5,499,294 A * 3/1996 Friedman 713/179

* cited by examiner
Primary Examiner—Kim Vu
Assistant Examiner—Hosain Song
(74) **Attorney, Agent, or Firm—Welsh & Katz, Ltd.**

(57) **ABSTRACT**
A method and system of authentication for sensor-recorders and other information capture devices is disclosed. In accordance with aspects of the current invention, a digital sample of the environment is obtained. From this sample and at least one parameter representative of at least one condition under which the sample was generated, a digital signature is created. This signature is stored in memory with the sample to be checked at a later time for authenticity. The file is checked for authenticity by generating a second signature from the file and comparing that signature to the original signature. If the two signatures are identical, the sample is considered authentic and if the two signatures are different, the sample cannot be authenticated.

6 Claims, 21 Drawing Sheets



1 INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

FIELD OF THE INVENTION

The present invention generally relates to a method and apparatus for acquiring and recording a sample of an environment and, more particularly, to a method and apparatus that allows the stored recording to be verified as an authentic, unaltered sample of the environment.

EX1001, 23

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

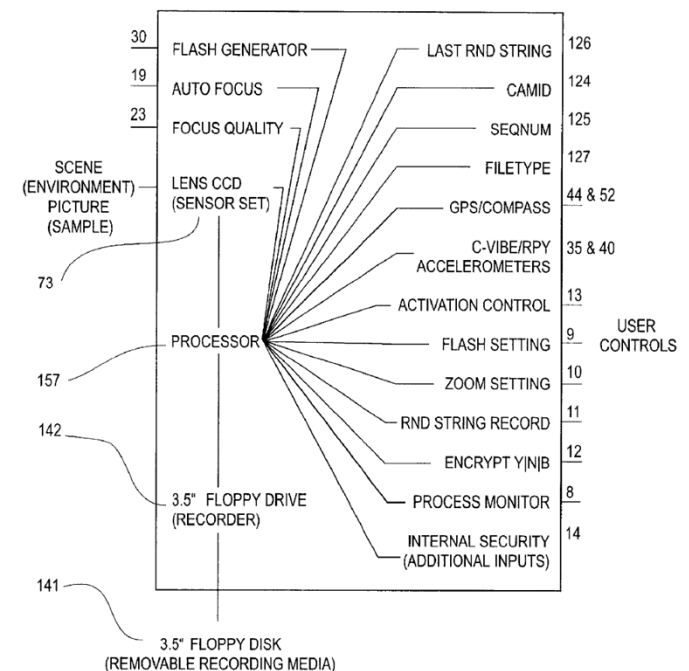
FIG. 2A is a detailed schematic diagram of a self-contained digital camera that incorporates certain aspects of the present invention.;

EX1001, 2:12-15

One aspect of the present invention is the concept and method of indigenous authentication. That is, a family of devices to create recordings with material to validate its authenticity. One embodiment of the present invention relates to digital photography where an image is authenticated as a whole. An intermediate version allows the authentication of less than the whole. An advanced version allows for recovery of damaged (altered from its original state) elements. Additional inputs including, but not limited to,

EX1001, 2:59-67

FIG. 2A



GPS IS GEOPOSITIONING SYSTEM
C-VIBE IS THE COUNTER VIBRATION UNIT
RPY IS ROLL-PITCH YAW DETECTION
CAMID IS CAMERA IDENTIFICATION
SEQNUM IS SEQUENCE NUMBER

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

Grounds	Claims	Prior Art
1	1-6	Glass
2	1-6	Rieger
3	1-6	Glass and Exif 2.0 or Exif 2.1
4	1-6	Rieger and Exif 2.0 or Exif 2.1
5	1-6	Glass and Serret-Avila
6	1-6	Rieger and Serret-Avila
7	1-6	Glass and Exif 2.0 or Exif 2.1 and Serret-Avila
8	1-6	Rieger and Exif 2.0 or Exif 2.1 and Serret-Avila

Definition of a POSITA/Burden of Proof

“A Sensor, Which Is Tightly Coupled to Said Memory”

“Monitoring the Integrity of the Tight Coupling”

“Generating an Error/OK Signal”

Glass or Rieger Combined with Serret-Avila

Definition of a POSITA

Petitioner's Reply

Patent Owner largely agrees with Petitioner's definition of a POSITA but disagrees that such a person would have "experience involving image processing."

Paper 18 at 1

Petitioner's definition is well supported.

- Expert witness Dr. Xiong provides the legal framework for his opinion. (EX1003, ¶¶27-29)
- Dr. Xiong cites evidence supporting his opinion. (EX1003, ¶¶81-89; EX1029, ¶3-9)

Patent Owner's definition is not.

- Expert witness Mr. Davis provides no legal framework for his opinion. (EX2005, ¶¶17-49)
- Mr. Davis cites no evidence supporting his conclusory opinion. (EX2005, ¶56)

Definition of a POSITA

Patent Owner makes one argument regarding the definition of a POSITA ...

Patent Owner's Sur-Reply

II. PATENT OWNER'S EXPERT IS A POSITA WITH EXTENSIVE EXPERIENCE IN THE AREA OF COMPUTER SECURITY, WHICH IS THE FOCUS OF THE '828 PATENT

Patent Owner's expert, Mr. Davis, has extensive experience in the field of computer security, which is the actual focus of the '828 Patent and its claims.

Paper 23 at 2-3

Patent Owner's Response

However, the '828 Patent is primarily directed to digital security and authentication.

However, these are concepts primarily addressed in digital security rather than image processing.

Paper 16 at 4-5

Patent Owner makes another argument regarding the prior art ...

Patent Owner's Sur-Reply

Because Serret-Avila is from the field of internet transactions or e-commerce security, while the '828 Patent, Glass, and Rieger are in the field of digital image security, a POSITA would regard them as representing separate fields.

Instead, as explained in POR, a POSITA would regard the field of digital image validation (of the '828 Patent) as a separate field of endeavor from the field of internet security (of Serret-Avila) because validation of digital images to ensure the integrity and authenticity of the images involves unique problems specific to detecting manipulation of images.

Nor would Serret-Avila be pertinent to the particular problem with which the inventor is involved because Serret-Avila is not concerned with any aspects of authenticating digital images, and it does not address any security considerations specific to digital images.

Paper 23 at 21

Definition of a POSITA

Patent Owner makes one argument regarding the definition of a POSITA ...

Patent Owner's Sur-Reply

II. PATENT OWNER'S EXPERT IS A POSITA WITH EXTENSIVE EXPERIENCE IN THE AREA OF COMPUTER SECURITY, WHICH IS THE FOCUS OF THE '828 PATENT

Patent Owner's expert, Mr. Davis, has extensive experience in the field of computer security, which is the actual focus of the '828 Patent and its claims.

Paper 23 at 2-3

Patent Owner's Response

However, the '828 Patent is primarily directed to digital security and authentication.

However, these are concepts primarily addressed in digital security rather than image processing.

Paper 16 at 4-5

Patent Owner makes another argument regarding the prior art ...

Patent Owner's Response

Serret-Avila is not directed towards authenticating digital images, nor does Serret-Avila even reference authenticating digital photographs or images.

Paper 16 at 44

Patent Owner's Sur-Reply

However, Serret-Avila does not even once use the term "image."

Paper 23 at 21

Definition of a POSITA

Petitioner's Reply

Patent Owner presumably disputes the reference to “experience involving image processing” in the definition of a POSITA because his expert witness, Mr. Davis, does not have any such experience.

Because Petitioner's definition of a POSITA is correct and because Mr. Davis does not meet it, his opinions from the perspective of such a person should be disregarded.

Paper 18 at 2-3

Petitioner's expert qualifies as more than a POSITA

- Dr. Xiong exceeds the qualifications under Petitioner's definition. (EX1003, ¶88)
- Dr. Xiong also qualifies as a POSITA under Patent Owner's definition. (EX1029, ¶11; EX1003, ¶5)
- Patent Owner's argument that Dr. Xiong does not qualify as a POSITA is a new argument. (Sur-Reply at 21; POR at 4-5)

Patent Owner's expert is not qualified as a POSITA

- Patent Owner's expert is not a POSITA under Petitioner's definition. (Reply at 3)
- Patent Owner does not argue otherwise. (Sur-Reply at 3-4)

Burden of Proof

Patent Owner's Expert

19. I understand that each claim of an issued patent is presumed to be valid. A party challenging the validity of a patent claim must present clear and convincing evidence to overcome the presumption of validity.

30. I understand that invalidity must be shown by clear and convincing evidence. Furthermore, I understand that clear and convincing evidence means that it is highly probable that the fact is true.

49. For an obviousness combination, obviousness must be proven by clear and convincing evidence such that a POSITA at the time of the alleged invention would have had a reason (or reasons) for combining the teachings of those prior art references to achieve the claimed invention, and that same POSITA would have had a reasonable expectation of success from combining those teachings.

EX2005



35 U.S.C. § 316

(e) EVIDENTIARY STANDARDS.—

In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.

Definition of a POSITA/Burden of Proof

“A Sensor, Which Is Tightly Coupled to Said Memory”

“Monitoring the Integrity of the Tight Coupling”

“Generating an Error/OK Signal”

Glass or Rieger Combined with Serret-Avila

“a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

“tightly coupled”

“The term ‘tightly coupled’ is not a term of art and is not defined by the patent.”

Pet. at 9

“The term ‘tightly coupled’ is a term of degree (i.e., the sensor and memory are not merely “coupled,” they are “**tightly** coupled”)....

Reply at 4

[B]ecause the disputed term is a coined term, meaning it has no ordinary and customary meaning, the question is whether the intrinsic evidence provides objective boundaries to the scope of the term.

* * * * *

In these circumstances, where there is no clear ordinary and customary meaning of a coined term of degree, we may look to the prosecution history for guidance without having to first find a clear and unmistakable disavowal.

Iridescent Networks, Inc. v. AT&T Mobility, LLC, 933 F.3d 1345, 1353 (Fed. Cir. 2019)

“a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Remarks:

It is respectfully submitted that new claims 9-14 are not subject to rejection over U.S. Patent No. 5,764,770 to Schipper et al. (the "Schipper patent") for a number of reasons, including those set forth hereinafter. For example, the Schipper patent does not teach or suggest structure or method steps corresponding to the feature of new claims 9-14 that states,

"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.

EX1002, 277

“a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Petitioner's Construction

“a sensor coupled to said memory via conductive traces or leads”

Pet. at 10

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.

EX1002, 277

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

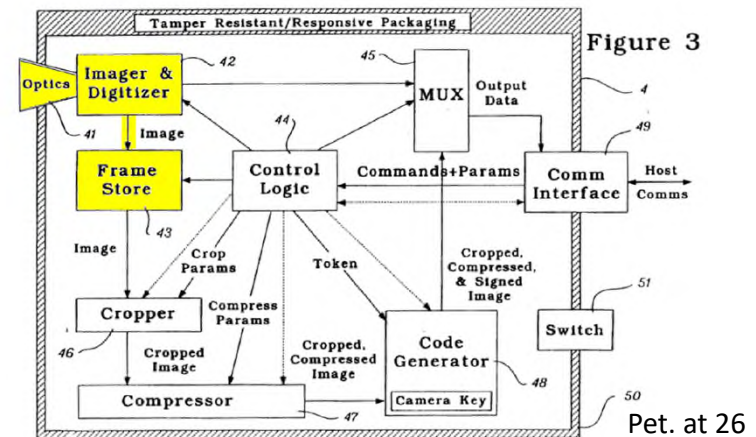
utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



A present preferred configuration of our imaging system 4 is shown in FIG. 3 wherein data paths are shown in solid lines and control signal paths are indicated by dotted lines. Optics 41 direct light from a scene to an imager which may be a CCD camera, a CMOS device or other two dimensional imager which creates a digital image. Consequently, we identify this component 42 as Imager & Digitizer. The digital image is sent to a multiplexer 45 and/or a frame store memory 43. Control logic unit 44 determines where the image is sent. The image in the frame store 43 is sent

EX1005, 5:46-55

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

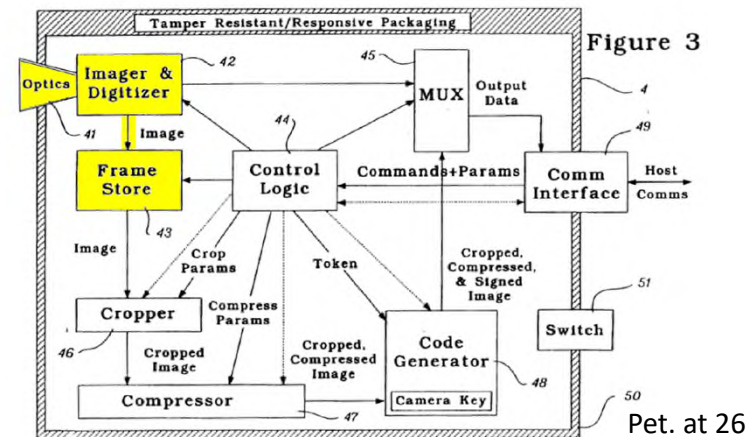
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Petitioner's Expert (Dr. Xiong)

Figure 3 shows “Optics,” “Imager & Digitizer,” and “Frame Store” electrically connected together within an “Imaging System,” which itself is contained in a “Tamper Resistant/ Responsive Packaging.” The figure illustrates a “data path” connecting the Optics/Imager/Digitizer (including a *sensor*) to Frame Store (including *memory*). EX1005, 5:46-48. The illustrated data path from the *sensor* to *memory* indicates that the components are electrically connected by conductive leads or traces within imaging system 4. Therefore, the *sensor* and *memory* are *tightly coupled* (based on the construction of that term discussed above).

EX1003, ¶171

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

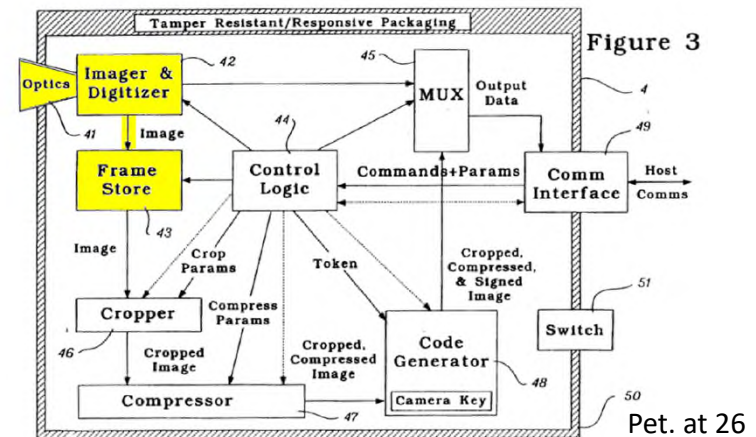
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



A present preferred configuration of our imaging system 4 is shown in FIG. 3 wherein data paths are shown in solid lines and control signal paths are indicated by dotted lines. Optics 41 direct light from a scene to an imager which may be a CCD camera, a CMOS device or other two dimensional imager which creates a digital image. Consequently, we identify this component 42 as Imager & Digitizer. The digital image is sent to a multiplexer 45 and/or a frame store memory 43. Control logic unit 44 determines where the image is sent. The image in the frame store 43 is sent

EX1005, 5:46-55

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

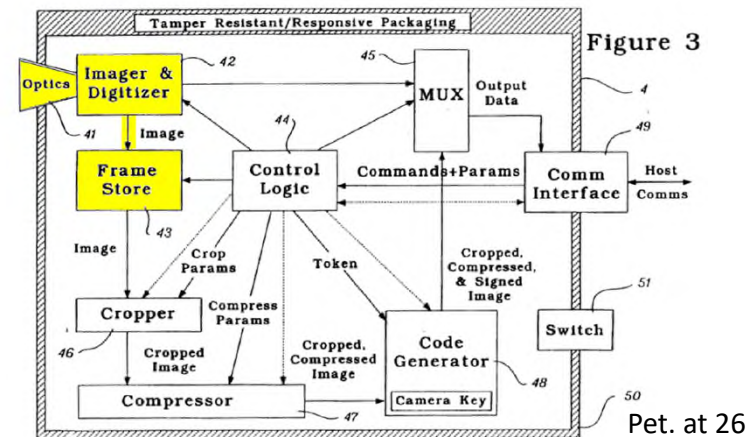
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Petitioner's Expert (Dr. Xiong)

Glass states that the optical sensor can be a “CCD camera, a CMOS device or other two dimensional imager which creates a digital image.” EX1005, 5:49-52. A POSITA would recognize a CCD (charge-coupled device), CMOS (complementary metal-oxide semiconductor), or other two dimensional imager that creates a digital image to be integrated circuits. Integrated circuits include leads (i.e., conductive wires or balls) used to electrically connect the integrated circuit to a circuit board. ... The leads are connected to traces, which are conductive wires running through a circuit board to interconnect components. ... The arrow from the *sensor* to the *memory* in Figure 3 indicates that those components are electrically connected so that image data can flow from the *sensor* to the *memory*.

EX1029, ¶14

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Petitioner's Construction

“a sensor coupled to said memory via conductive traces or leads”

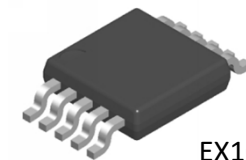
Pet. at 10

lead— 1. A wire to or from a circuit element. 2. To precede (the opposite of lag). 3. A wire, with or without terminals, that connects two points in a circuit. 4. A conductive path that is usually self-supporting.

EX1033, 3

trace 1. The visible path of a moving spot on the screen of a cathode-ray tube. 2. An extremely small quantity of a substance. 3. An interpretive diagnostic technique that provides an analysis of each executed instruction of a computer and writes it on an output device as each instruction is executed by the computer. 4. A conductive path on a printed circuit board.

EX1035, 3



EX1030, 1

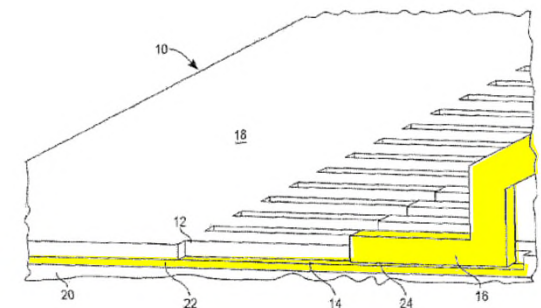


Fig. 1 EX1032

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

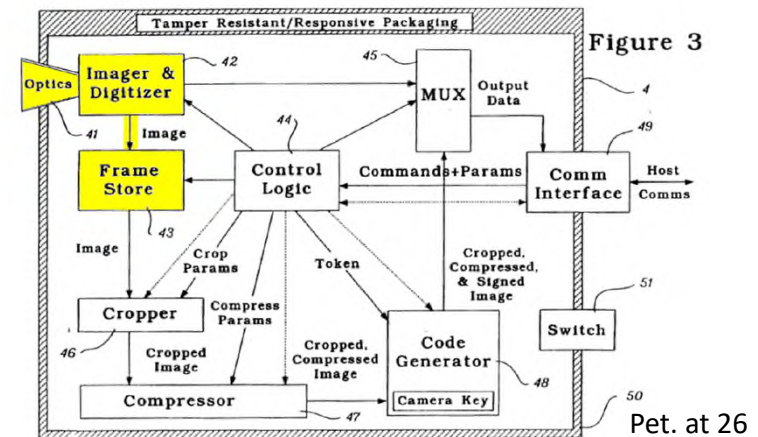
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Petitioner's Construction

“a sensor coupled to said memory via conductive traces or leads”

Pet. at 10

Glass Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

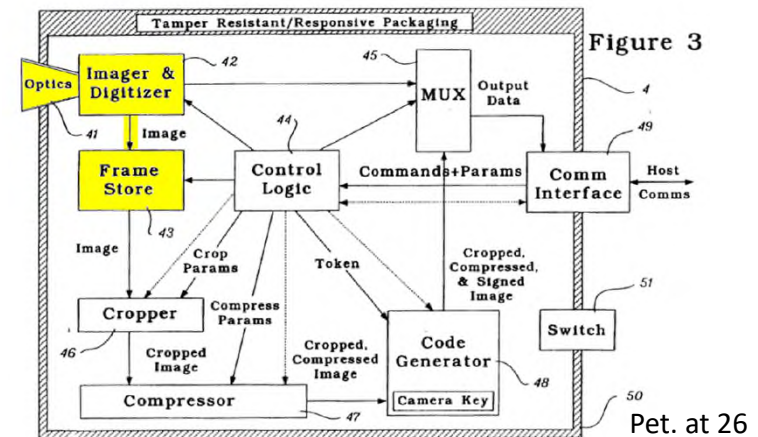
utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Patent Owner's Construction

“a sensor that is electrically or physically coupled to memory in a device”

POR at 9

Petitioner's Expert (Dr. Xiong)

Thus, the arrow from optics 41/imager & digitizer 42 to frame store 43 shows “a sensor that is electrically...coupled to memory in a device” as required by Patent Owner's proposed construction.

EX1029, ¶14

Rieger Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

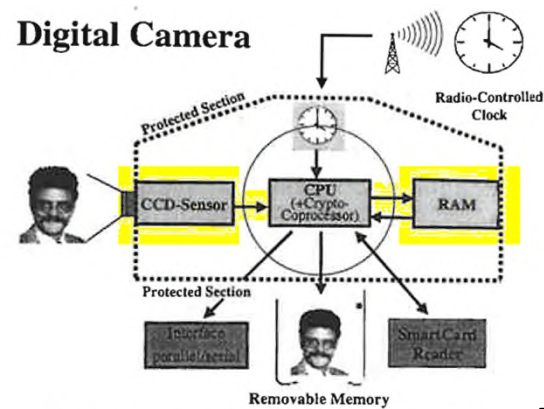


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Pet. at 43-46

Figure 3 shows the basic conceptual diagram for a digital camera of this kind. The camera processor consists essentially of a high-speed RISC processor, an interface to the CCD chip, serial or parallel ports, an interface to a RAM, a signature chip with a secret key and a data-compression block. Data transfer from the digital camera to an external computer can be effected via a removable memory medium or a suitable parallel or serial port on the camera.

EX1006, 4

After recording, the processor reads the image data from the CCD sensor and saves these to the RAM. The image file is then compressed (e.g. in the JPEG format), signed and saved to a removable memory medium (floppy disc, semiconductor memory, etc.) or transmitted directly to an external computer.

EX1006, 4

Rieger Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

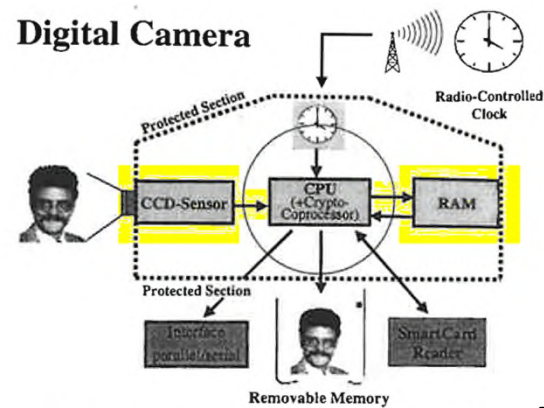


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Pet. at 43-46

Petitioner's Expert (Dr. Xiong)

The arrows in Figure 3 illustrating a data path from the sensor to memory indicate that the components are electrically connected by conductive leads or traces within the protected section of Rieger's manipulation-proof camera.

EX1003, ¶1228

A person of ordinary skill in the art would understand that these connections would be made using conductive traces and leads, including to transmit information between those components.

EX1003, ¶1232

Rieger Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

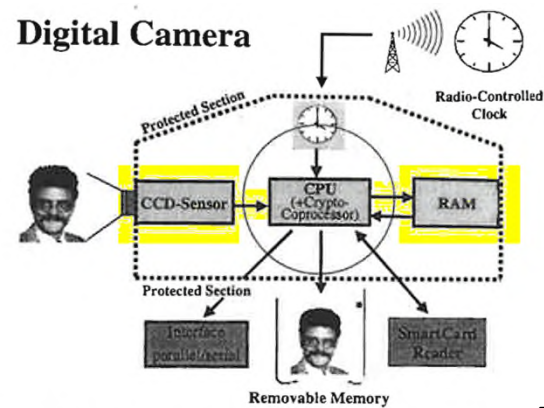


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Pet. at 43-46

Petitioner's Expert (Dr. Xiong)

Rieger states that “[t]he camera processor consists essentially of a high-speed RISC processor, an interface to the CCD chip,...[and] an interface to a RAM....” EX1006, 4. A “high-speed RISC processor” (CPU), “CCD chip, and “RAM” are integrated circuits commonly interconnected by leads and traces on a circuit board. [citations omitted] Further, Rieger states that the CCD-Sensor, CPU, and RAM are inside a “Protected Section” of the digital camera (EX1006, 4), suggesting to a POSITA that the connection between those components should be secure, as it would be if the connections were made using conductive leads and traces.

EX1029, ¶15

Rieger Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

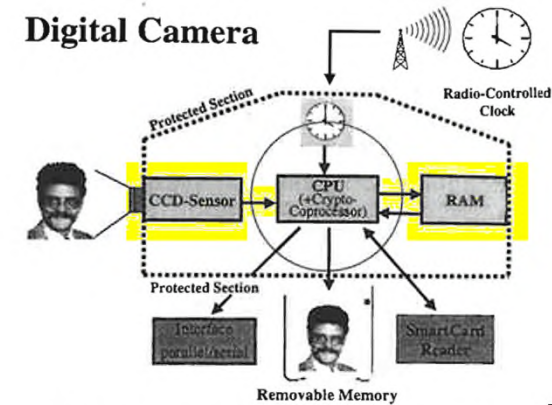


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Pet. at 43-46

Petitioner's Construction

“a sensor coupled to said memory via conductive traces or leads”

Pet. at 10

Rieger Discloses “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

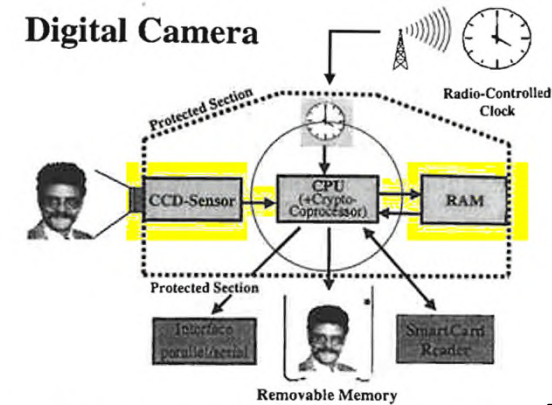


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Pet. at 43-46

Patent Owner's Construction

“a sensor that is electrically or physically coupled to memory in a device”

POR at 9

Petitioner's Expert (Dr. Xiong)

Thus, the arrow from CCD-Sensor to RAM via the CPU shows “a sensor that is electrically...coupled to memory in a device” as required by Patent Owner's proposed construction.

EX1029, ¶15

Glass/Rieger Disclose “a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Patent Owner's Response

Because a POSITA would know that there were many ways to connect a CCD camera to either a processor or memory, Dr. Xiong has not shown that Glass teaches that the specific connection between Optics and Camera 6 and Digitizer and Frame Store 8 is by conductive traces or leads. EX2005 at ¶72.

Paper 16 at 14; *see also id.* at 31

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

- storing a data stream in a data file in a memory;
- utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

comparing said first signature to said second signature,

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

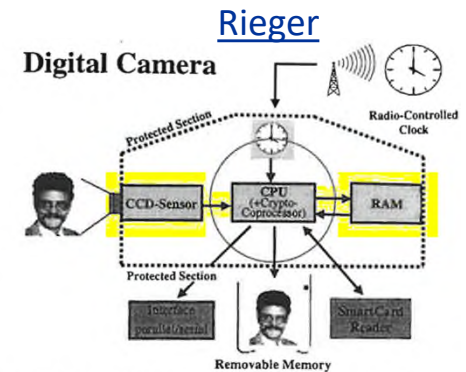
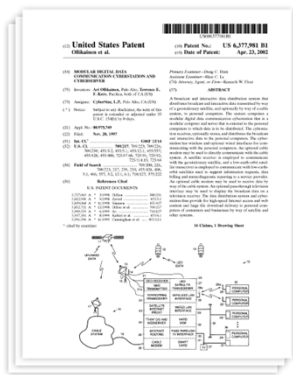


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Satellite



EX2009

“a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Institution Decision

Applicant's March 16, 2004 Preliminary Amendment asserted “in accordance with the present invention, the claimed ‘tight coupling’ requires that the connections between the sensor and the memory not be physically accessible to a user.” Ex. 1002, 292. Should the construction of “tight coupling” continue to be an issue during trial, we invite the parties to address its construction in consideration of the intrinsic evidence in the manner asserted in the March 16, 2004 Preliminary Amendment.

Paper 8 at 18 n.6

Exemplary support for this claim feature is disclosed, for example, at page 5, lines 22-24, which state, to “ensure authentication, additional inputs 7 other than the sensor set 4 are not accessible to the user without detection as shown in Fig. 2.” Thus, in accordance with the present invention, the claimed “tight coupling” requires that the connections between the sensor and the memory not be physically accessible to a user.

EX1002, ¶292

“a Sensor, Which Is Tightly Coupled to Said Memory”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

- The statement supports Petitioner’s construction of “monitoring the integrity of the tight coupling between said memory and said sensor....” (Pet. at 11)
- The description of the “present invention” is also true of Glass and Reiger, which is a further evidence they disclose the “utilizing” and “monitoring” limitations. (Pet. at 27-28, 46)
- If the construction of “a sensor, which is tightly coupled to said memory” is modified to require that they “are not physically accessible to the user,” Glass and Rieger still disclose the limitation. (Reply at 7)

Exemplary support for this claim feature is disclosed, for example, at page 5, lines 22-24, which state, to “ensure authentication, additional inputs 7 other than the sensor set 4 are not accessible to the user without detection as shown in Fig. 2.” Thus, in accordance with the present invention, the claimed “tight coupling” requires that the connections between the sensor and the memory not be physically accessible to a user.

EX1002, 292

Definition of a POSITA/Burden of Proof

“A Sensor, Which Is Tightly Coupled to Said Memory”

“Monitoring the Integrity of the Tight Coupling”

“Generating an Error/OK Signal”

Glass or Rieger Combined with Serret-Avila

“Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Operators may aim the device, activate the device, and set user controls, including but not limited to, flash 9 zoom 10 random string recording (RSR) 11 or optional encryption 12. 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, 4:62-67

Independent of the compass status, processing continues 58 with a check 59 of the internal security system 14. If there is a breach of security 60 the violation is recorded 61. Otherwise 62 the value “ImageGuard” is recorded 63 and the process monitor 8 is updated 64 with the violation or “ImageGuard”

EX1001, 5:44-49

are all appended to the image. If internal security is compromised 60 a security violation 61 is appended 123 to the image. Otherwise the “ImageGuard” value is appended 123 to the image.

EX1001, 6:64-67

“Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Second, the Maloney patent does not teach or the following feature of the amended claims, which states,

"monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;"

Exemplary disclosure corresponding to this claim feature is shown, for example, in Figure 4A, step 59, which is a flow chart decision block in which it is determined whether 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, 292-293

“Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Exemplary support for this claim feature is disclosed, for example, at page 5, lines 22-24, which state, to "ensure authentication, additional inputs 7 other than the sensor set 4 are not accessible to the user without detection as shown in Fig. 2." Thus, in accordance with the present invention, the claimed "tight coupling" requires that the connections between the sensor and the memory not be physically accessible to a user.

EX1002, 292

“Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Petitioner's Construction

“determining whether physical access has been gained to the coupling between said memory and said sensor”

Pet. at 11

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, 293

accessible to the user without detection as shown in Fig. 2.” Thus, in accordance with the present invention, the claimed “tight coupling” requires that the connections between the sensor and the memory not be physically accessible to a user.

EX1002, 292

Glass Discloses “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

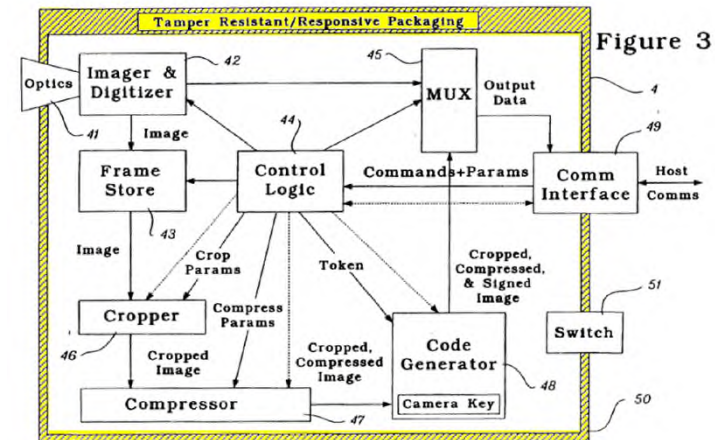
monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



The entire package which contains the imaging system 4, must be tamper-resistant so that it is extremely difficult to access the internal elements of the package without detection or actual destruction of the device. It is essential to ensure that the integrity of the acquired images and codes to be transmitted over the network have not been compromised. This is especially important in applications where large value transactions might occur. Thus, in our preferred

EX1005, 5:13-20

Glass Discloses “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

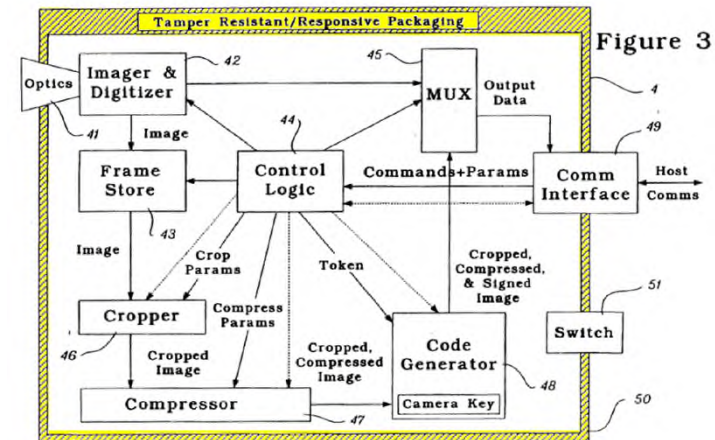
monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



large value transactions might occur. Thus, in our preferred embodiment, the imaging system 4, will be enclosed in a tamper resistant package 50 which will be used to detect unwelcome intrusion and render the system useless. The tamper resistant package can be passive in that any opening to the device will cause its ultimate destruction.

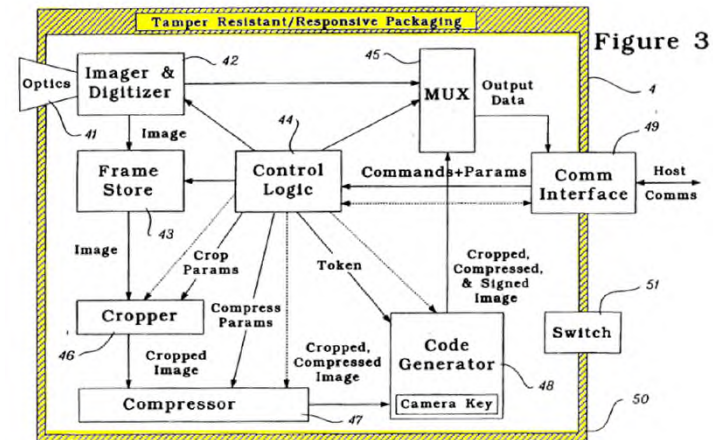
EX1005, 5:20-25

Glass Discloses “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
utilizing said signature protocol to generate a second signature based on said data stream;
comparing said first signature to said second signature,
if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and
if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Alternatively, the packaging could utilize at least one chassis intrusion detector or switch 51 shown in FIG. 3. Switch 51 will signal the control logic 44 (which could be implemented by a microcontroller) to return to a non-functioning state similar to that found during assembly. This non-functioning state will essentially delete key software routines related to generating biometric data. It may also delete special battery backed up ram tables which include security or encryption information. Thus, if an intruder does gain access to the

EX1005, 5:25-34

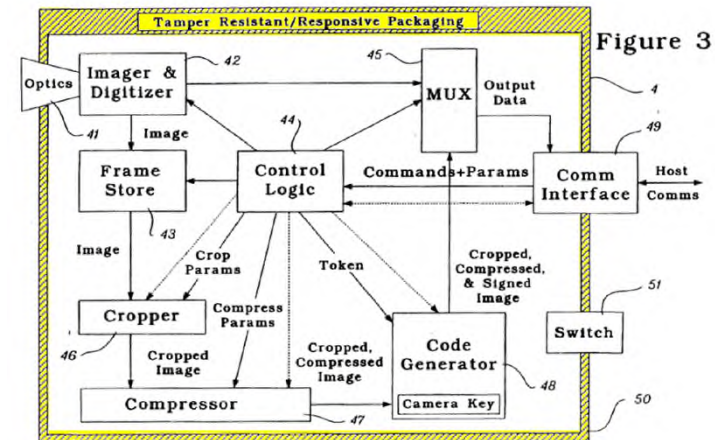
Glass Discloses “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Exemplary disclosure corresponding to this claim feature is shown, for example, in Figure 4A, step 59, which is a flow chart decision block in which it is determined whether 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, 293

Rieger Discloses “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
utilizing said signature protocol to generate a second signature based on said data stream;
comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

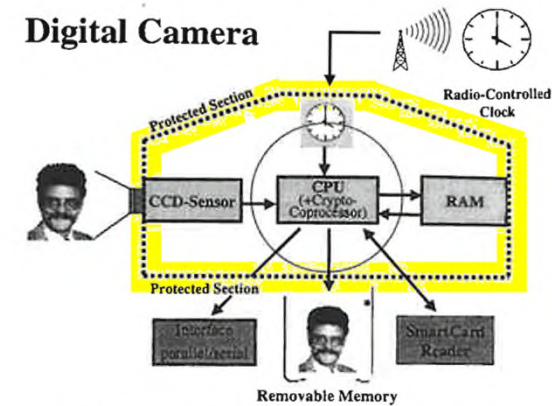


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

The secure compartment can be protected, for example, by an electrical “protective shield”. When this is drilled or severed, a change in potential is triggered and detected by the processor, which then automatically deletes the secret key stored in the signature chip. This ensures that image data cannot be altered without detection prior to application of the signature.

EX1006, 4

Rieger Discloses “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

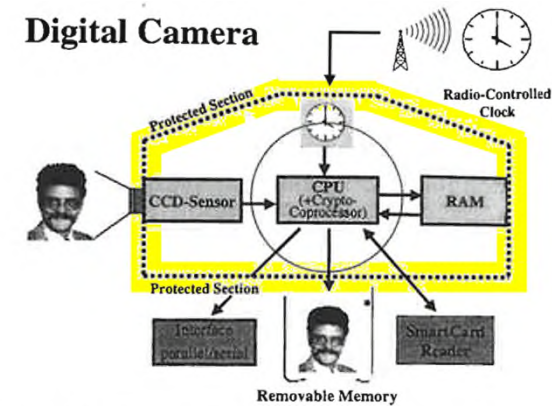


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Exemplary disclosure corresponding to this claim feature is shown, for example, in Figure 4A, step 59, which is a flow chart decision block in which it is determined whether 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, 293

Glass/Rieger Disclose “Monitoring the Integrity of the Tight Coupling”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:
storing a data stream in a data file in a memory;
utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Patent Owner's Response

However, the claim term requires “monitoring ... the tight coupling” between the memory and the sensor specifically.

Paper 16 at 9

Definition of a POSITA/Burden of Proof

“A Sensor, Which Is Tightly Coupled to Said Memory”

“Monitoring the Integrity of the Tight Coupling”

“Generating an Error/OK Signal”

Glass or Rieger Combined with Serret-Avila

Glass Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

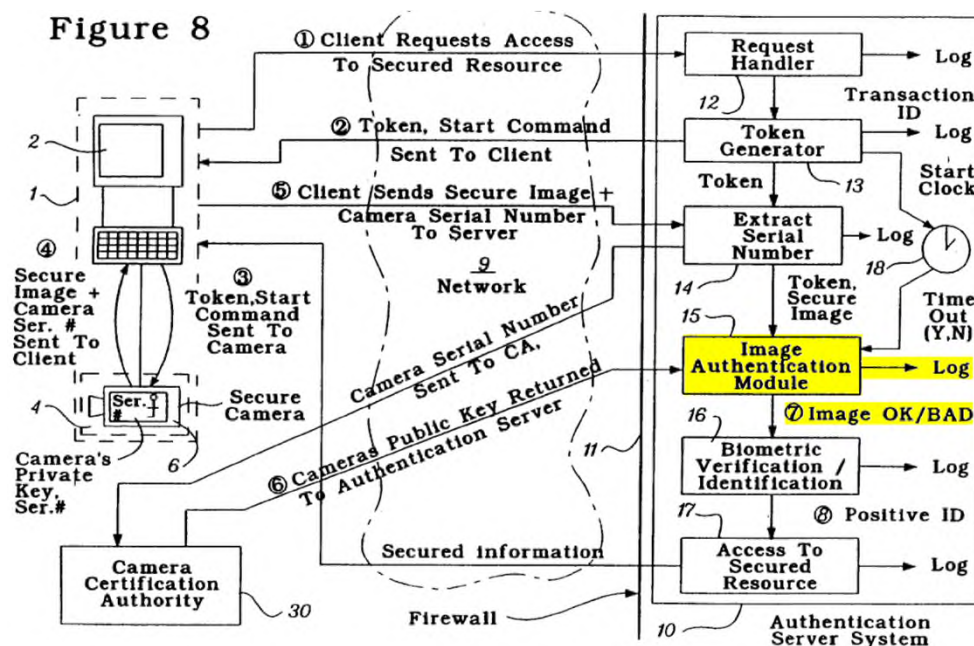
utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.



Glass Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

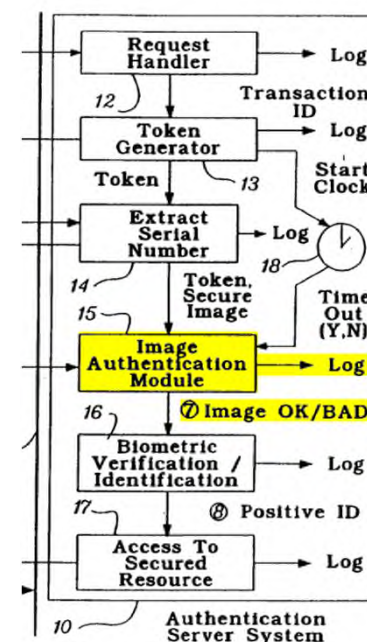
if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

We prefer to log each step of the transaction as indicated by the word Log. We also prefer to provide a clock 18 which is used in checking time-stamped data as well as recording the time of each transaction.

EX1005, 9:61-64

resource 17. A record of the transaction can be logged by the server system, which could contain, among other things, the original, secured image data sent by the client and the unique camera identification or key. This data can provide irrefutable evidence of the transaction if required.

EX1005, 10:54-58



Glass Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Patent Owner’s Sur-Reply

The mere possibility of display is therefore insufficient.

In short, the issue is not temporality but rather certainty, as required by the claim language.

Paper 23 at 18-19

- This is a new argument. (See POR at 23-25)
- The argument is legally invalid because “combinations of prior art that sometimes meet the claim elements are sufficient to show obviousness.” *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 995, 1002 (Fed. Cir. 2016)
- There is no dispute that log files will at least “sometimes” be displayed to a user (e.g., as evidence).

Glass Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Patent Owner’s Sur-Reply

Because the information is recorded on the server, the user may not have access to the log files. For example, system log files are routinely available only to administrators of a server.

Paper 23 at 18-19

- This is a new argument. (See POR at 23-25)
- Patent Owner is implicitly construing the term “a user” to exclude an administrator—with no support.
- The plain meaning of “a user” includes whoever is evaluating the authenticity of the image (e.g., an administrator).

Rieger Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

- storing a data stream in a data file in a memory;
- utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;
- monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;
- utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
- utilizing said signature protocol to generate a second signature based on said data stream;
- comparing said first signature to said second signature,
- if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and
- if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

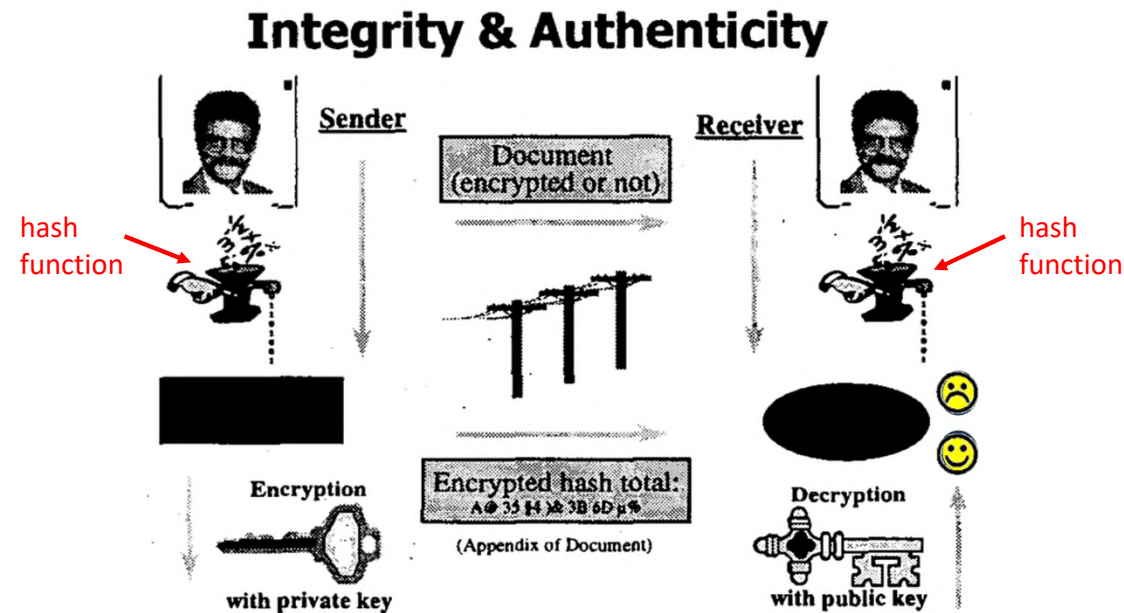


Figure 7: Principles of the integrity and authenticity test

Rieger Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

- storing a data stream in a data file in a memory;
- utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;
- monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;
- utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
- utilizing said signature protocol to generate a second signature based on said data stream;
- comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

THE INTEGRITY TEST

The advantage of this process lies in the fact that only a (relatively) short hash value must be stored or transmitted in a secure manner – and not the entire text. If such a hash process is openly disclosed and described to every user, any user can compute the hash value himself on the basis of the original plain text and determine, through comparison, whether the value transmitted by the sender is identical with his own result. In this way every user can check to determine whether a given hash result can actually be assigned to a specific message.

EX1006, 11-12

Rieger Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Digital Image Recording for Court-Related Purposes

Reflections regarding the basic configuration of a manipulation-proof digital camera capable of meeting the stringent integrity and authenticity requirements imposed for images presented as evidence in court will be discussed. We propose the use of a suitable digital signature, a method

EX1006, 1

Requirements for digital photographs in police work

Prior to introduction of digital photo and video technology for police use on broad basis, the following requirements must be imposed upon that technology for the purpose of ensuring the integrity and authenticity of images presented as evidence in court:

EX1006, 3

- It must be possible to verify image integrity in order to ensure effective protection of digital image data against unauthorized alteration.
- Necessary or useful image-processing techniques (format conversion, scaling, contrast enhancement, compression, etc.) applied must be identifiable.

Simple, published techniques must be available to ensure that the integrity and authenticity of images and supplementary data can be verified by third parties.

EX1006, 3

Rieger Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said data stream;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Petitioner's Expert

The frowning face image indicates to a person of ordinary skill in the art that *if said first and second signatures are not the same*, Rieger's integrity test generates *an error signal* (like a frowning face) *that is displayed to a user to indicate that said stored data stream is not authentic.* Such a person would recognize that the integrity test would have little or no use if it did not provide such an indication to the user when an image is not authentic.

EX1003, ¶257

The smiling face image indicates to a POSITA that *if said first and second signatures are the same*, Rieger's integrity test generates *an ok signal* (like a smiling face) *that is displayed to a user to indicate that said stored data stream is authentic.*

Displaying such a message to the user would be an obvious design choice for a person of ordinary skill in the art. It would require little effort and provide the user with a clear indication that the document/image has been validated.

EX1003, ¶260

Definition of a POSITA/Burden of Proof

“A Sensor, Which Is Tightly Coupled to Said Memory”

“Monitoring the Integrity of the Tight Coupling”

“Generating an Error/OK Signal”

Glass or Rieger Combined with Serret-Avila

Serret-Avila Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

- storing a data stream in a data file in a memory;
- utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;
- monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;
- utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
- utilizing said signature protocol to generate a second signature based on said data stream;
- comparing said first signature to said second signature,
- if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and
- if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

304 of FIG. 3. Next, the calculated check value $H(C_i')$ is compared with the check value that was received, $H(C_1)'$ (514), which in the case of the first sub-block, P_1 , is the unsigned value $H(C_1)'$ obtained in block 504.

EX1011, 10:24-27

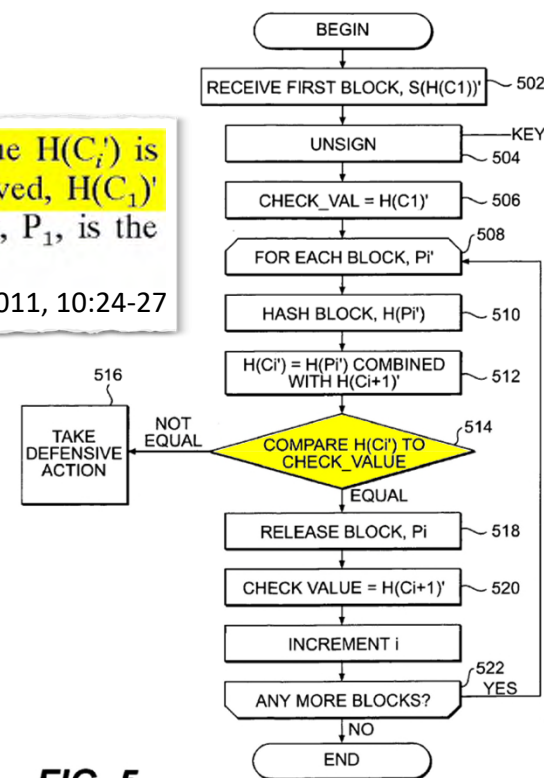


FIG. 5

Serret-Avila Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

- storing a data stream in a data file in a memory;
- utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;
- monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;
- utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
- utilizing said signature protocol to generate a second signature based on said data stream;
- comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

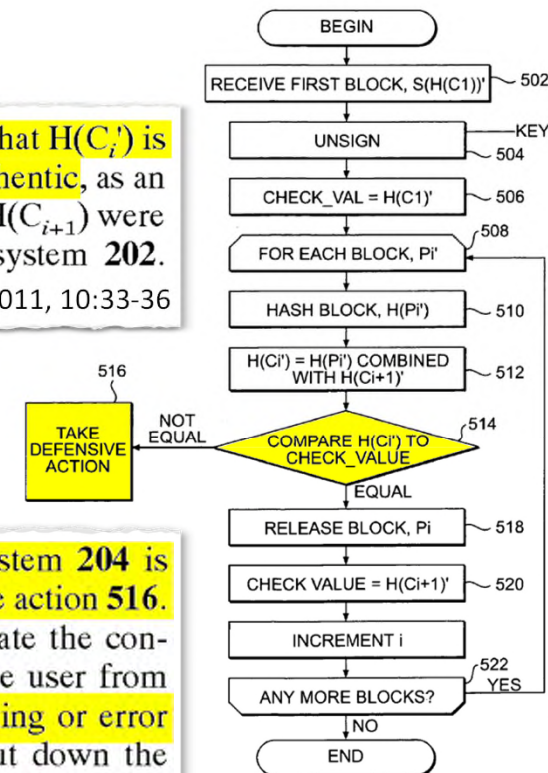
if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

However, if comparison block 514 indicates that $H(C_i')$ is not equal to $H(C_i)$, then P_i is judged to be unauthentic, as an inequality at block 514 indicates that P_i and/or $H(C_{i+1})$ were modified after being processed by encoding system 202.

EX1011, 10:33-36

Upon detecting such a condition, decoding system 204 is preferably operable to take appropriate defensive action 516. For example, decoding system 204 can terminate the connection with the source of the data, prevent the user from making further use of the data, display a warning or error message on display 262, shut itself down, shut down the application that was receiving or using the file, or simply

EX1011, 10:37-43



Serret-Avila Discloses “Generating an Error/OK Signal”

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

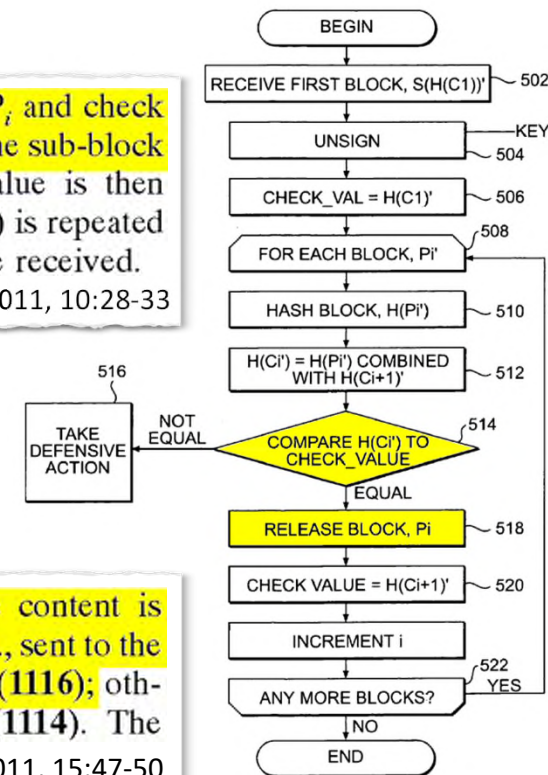
- storing a data stream in a data file in a memory;
- utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;
- monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;
- utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;
- utilizing said signature protocol to generate a second signature based on said data stream;
- comparing said first signature to said second signature, if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

If the two values are equal, then sub-block P_i and check value $H(C_{i+1})$ are deemed to be authentic, and the sub-block can be released for use (518). The check value is then updated (520), and the entire process (508–522) is repeated for the next sub-block and check value that are received.

EX1011, 10:28-33

ously-authenticated hash values (1112). If the content is deemed to be authentic, it is released for use (e.g., sent to the system's speakers, display screen, printer, etc.) (1116); otherwise, an error handling routine is called (1114). The

EX1011, 15:47-50



Analogous Prior Art

Patent Owner's Response

Consequently, Serret-Avila is not analogous art with Glass and Rieger.

Paper 16 at 46

In evaluating whether a reference is analogous, we have consistently held that a patent challenger must compare the reference to the challenged patent.

Sanofi-Aventis Deutschland GmbH v. Mylan Pharmaceuticals Inc.,
66 F.4th 1373, 1377 (Fed. Cir. 2023)



Analogous Prior Art

Patent Owner's Sur-Reply

Serret-Avila is non-analogous art to the '828 Patent as well as to the Glass and Rieger.

Because Serret-Avila is from the field of internet transactions or e-commerce security, while the '828 Patent, Glass, and Rieger are in the field of digital image security, a POSITA would regard them as representing separate fields.

Paper 23 at 20-21

Patent Owner's Sur-Reply

II. PATENT OWNER'S EXPERT IS A POSITA WITH EXTENSIVE EXPERIENCE IN THE AREA OF COMPUTER SECURITY, WHICH IS THE FOCUS OF THE '828 PATENT

Patent Owner's expert, Mr. Davis, has extensive experience in the field of computer security, which is the actual focus of the '828 Patent and its claims.

Paper 23 at 2-3

Patent Owner's Response

However, the '828 Patent is primarily directed to digital security and authentication.

However, these are concepts primarily addressed in digital security rather than image processing.

Paper 16 at 4-5

Analogous Prior Art

Patent Owner's Sur-Reply

Serret-Avila is non-analogous art to the '828 Patent as well as to the Glass and Rieger.

Because Serret-Avila is from the field of internet transactions or e-commerce security, while the '828 Patent, Glass, and Rieger are in the field of digital image security, a POSITA would regard them as representing separate fields.

Paper 23 at 20-21

tives, modifications and equivalents. For example, while several embodiments are described in the context of a system and method for viewing or playing video, audio, or multimedia data, those skilled in the art will recognize that the disclosed systems and methods are readily adaptable for broader application. For example, without limitation, the

EX1011, 6:13-18

other suitable format. Data 400 may additionally (or alternatively) include video, textual, or multimedia information, a computer program or applet, or any other type of data or executable.

EX1011, 9:8-11

16. A method as in claim 15, in which the at least one use of the first block of data includes one of: sending the first block of data to a speaker system; displaying the first block of data on a viewing device; printing the first block of data; and storing the first block of data on a computer readable medium.

EX1011, 23:6-11

Analogous Prior Art

Patent Owner's Sur-Reply

Serret-Avila is non-analogous art to the '828 Patent as well as to the Glass and Rieger.

Because Serret-Avila is from the field of internet transactions or e-commerce security, while the '828 Patent, Glass, and Rieger are in the field of digital image security, a POSITA would regard them as representing separate fields.

Paper 23 at 20-21

Petitioner's Expert

Serret-Avila discloses a technique for authenticating data streams that is described largely in the context of video, audio, and other multimedia data.

Thus, Serret-Avila, like the '828 Patent, is in the field of endeavor involving processing data streams including digital images.

EX1029, ¶128

Petitioner's Expert

In addition, Serret-Avila and the '828 Patent both address the problem of authenticating data streams including digital images.

Thus, Serret-Avila, like the '828 Patent, addresses the problem of authenticating data streams including digital images.

EX1029, ¶129

Motivation to Combine

Petitioner's Expert

A person of ordinary skill in the art would have been motivated to provide in Glass's system an indication to a user that the image is either authentic or not as taught by Serret-Avila. Indeed, Glass suggests this by stating that each step of the authentication process is logged, which would permit subsequent user review. EX1005, 9:61-62, 10:54-58, Figs. 7, 8. Failing to indicate the results of the authentication process to a user would frustrate the purpose of the invention. Serret-Avila teaches employing defensive measures such as displaying a "warning or error message" when an image is deemed unauthentic. EX1011, 10:39-45. In Glass's system, such a warning or error message would alert a user attempting to access sensitive information that their biometric data had been corrupted or fraudulently modified and would permit the user to respond appropriately (e.g., by discontinuing use of the system). Similarly, a user monitoring Glass's system (e.g., a system administrator) would be alerted to any fraudulent attempt to access sensitive information so that he or she could take immediate remedial action. Similarly, a message indicating that the biometric image data is authentic would reassure a user that the system is operating as intended and is free of fraudulent activity.

EX1003, ¶287

Petitioner's Expert

A person of ordinary skill in the art would have been motivated to combine Glass with Serret-Avila and would have been able to do so with a reasonable expectation of success. It would have been a simple matter for such a person to program Glass's system to provide an error or ok message to a system user.

EX1003, ¶288

Motivation to Combine

Petitioner's Expert

A person of ordinary skill in the art would have been motivated to provide in Rieger's "integrity test" an indication to a user that the image is either authentic or not as taught by Serret-Avila. Rieger suggests as much by illustrating in Figure 7 either a smiling or frowning face icon to indicate whether the image is authentic or not authentic. EX1006, 12. Serret-Avila teaches employing defensive measures such as displaying a "warning or error message" when an image is deemed unauthentic. EX1011, 10:39-45. In Rieger's integrity test, such a warning or error message would provide an unequivocal indication to the user whether the image is authentic or not. A message indicating the image is authentic, would allow the user to rely on the image. This is the entire point of Rieger's integrity test. EX1006, 11-12. Failing to indicate the results of authentication to the user would frustrate the purpose of the invention.

EX1003, ¶290

Petitioner's Expert

A person of ordinary skill in the art would have been motivated to combine Rieger with Serret-Avila and would have been able to do so with a reasonable expectation of success. It would have been a simple matter for such a person to program Rieger's integrity test to provide an error or ok message to a user attempting to authenticate an image captured by Rieger's manipulation-proof camera.

EX1003, ¶291

Adobe Inc.
Petitioner
v.
Jonathan E. Jaffe
Patent Owner

IPR2024-01350
Patent 6,757,828 B1

Oral Argument

December 9, 2025
Petitioner Adobe's Demonstratives