

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ADOBE INC.

Petitioner

v.

JONATHAN E. JAFFE

Patent Owner

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

**DECLARATION OF ZIXIANG XIONG, PH.D. IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 6,757,828**

TABLE OF CONTENTS

I.	Background and Qualifications	7
II.	Materials Considered.....	11
III.	Relevant Legal Standards	14
	A. Burden of Proof.....	14
	B. Legal Standards for Prior Art.....	14
	C. Person of Ordinary Skill in the Art	15
	D. Anticipation.....	16
	E. Obviousness	17
	F. Priority/Written Description.....	22
IV.	Technical Analysis of the '828 Patent.....	23
	A. Overview of the Patent Specification.....	23
	B. The Prosecution History.....	33
	C. The Patent Claims	37
	D. Person of Ordinary Skill in the Art	39
	E. Claim Construction	42
	1. “a sensor, which is tightly coupled to said memory”	43
	2. “monitoring the integrity of the tight coupling between said memory and said sensor”	45
	3. “based on”	46
V.	Prior Art References	48
	A. Glass (EX1005).....	48
	B. Rieger (EX1006)	58
	C. Exif 2.0 (EX1008) and Exif 2.1 (EX1009)	66
	D. Serret-Avila (EX1011).....	67
VI.	The Challenged Claims Are Obvious in Light of the Prior Art	68
	A. Glass Renders the Challenged Claims Obvious.....	68
	1. Independent Claim 1	69

TABLE OF CONTENTS
(continued)

a)	[1pre] A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:.....	69
b)	[1a] storing a data stream in a data file in a memory;	70
c)	[1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;	73
d)	[1c] 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;	80
e)	[1d] 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;	83
f)	[1e] utilizing said signature protocol to generate a second signature based on said data stream;	86
g)	[1f] comparing said first signature to said second signature, ...	88
h)	[1g] 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	89
i)	[1h] 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	92
2.	Claim 2: The method of claim 1, wherein said memory form a part of a digital camera	93
3.	Claim 3: The method of claim 1, wherein said at least one parameter comprises a random number	94

TABLE OF CONTENTS
(continued)

4.	Claim 4: The method of claim 1, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.....	96
5.	Claim 5: The method of claim 4, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.....	96
6.	Claim 6: The method of claim 1 wherein said data stream is a digit sample of an environment.....	97
B.	Rieger Renders the Challenged Claims Obvious.....	98
1.	Independent Claim 1	98
a)	[1pre] A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:.....	98
b)	[1a] storing a data stream in a data file in a memory;	99
c)	[1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;	100
d)	[1c] 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;.....	107
e)	[1d] 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;	109
f)	[1e] utilizing said signature protocol to generate a second signature based on said data stream;	113

TABLE OF CONTENTS

(continued)

g)	[1f] comparing said first signature to said second signature,.....	114
h)	[1g] 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.....	115
i)	[1h] 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.....	117
2.	Claim 2: The method of claim 1, wherein said memory form a part of a digital camera.....	119
3.	Claim 3: The method of claim 1, wherein said at least one parameter comprises a random number.....	119
4.	Claim 4: The method of claim 1, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.....	120
5.	Claim 5: The method of claim 4, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.....	121
6.	Claim 6: The method of claim 1 wherein said data stream is a digit sample of an environment.....	122
C.	Exif 2.0 or Exif 2.1 Disclose Digital Camera “Parameters” Available for the Glass and Rieger Inventions	123
1.	Motivation to Combine	123
2.	Claim 1	124
3.	Claim 2	124
4.	Claim 3	124
5.	Claim 4.....	125

TABLE OF CONTENTS
(continued)

6.	Claim 5	127
D.	Serret-Avila Discloses Displaying an “Error” or “OK” Signal to the User	129
1.	Motivation to Combine Glass and Serret-Avila	130
2.	Motivation to Combine Rieger and Serret-Avila	131
3.	Serret-Avila Discloses Limitations [1f], [1g], and [1h]	132
VII.	Secondary Considerations	135
VIII.	Availability for Cross-Examination	135
IX.	Right to Supplement	135
X.	Conclusion	136

I, Dr. Zixiang Xiong, declare as follows:

1. I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters stated herein.

2. I have been asked by the petitioner Adobe Inc. to provide technical assistance in connection with the *inter partes* review of U.S. Patent No. 6,757,828 (which I will refer to as the “’828 Patent”). This declaration is a statement of my opinions on issues related to the patentability of claims 1-6 (which I will refer to as the “challenged claims”) of the ’828 Patent.

3. My compensation is not based on the content of my opinions or the resolution of this matter. I have no financial interest in this proceeding.

I. BACKGROUND AND QUALIFICATIONS

4. Currently I am a full professor in and associate head of the Electrical and Computer Engineering Department at Texas A&M University. I am also the Director of the Multimedia Laboratory at Texas A&M. I have been with Texas A&M for 25 years.

5. I have over 30 years of R&D experience on image/video processing, image data hiding and digital watermarking/fingerprinting, pattern recognition & computer vision, augmented & virtual reality. I have published 11 book chapters, 147 journal articles and 247 conference papers. I am also listed as an inventor on 23 patents, two of which are on data hiding.

6. I received a Bachelor of Science degree in Electrical Engineering from Wuhan University, China in 1987. I was an MS student at the University of the Chinese Academy of Sciences between September 1987 and December 1989. I came to the United States in January of 1990 to further my education. I received a Master of Arts degree in Mathematics from the University of Kansas in 1991, a Master of Science degree in Electrical Engineering from the Illinois Institute of Technology in 1992, and the Doctor of Philosophy (Ph.D.) degree in Electrical Engineering in 1996 from the University of Illinois at Urbana-Champaign. In the fall of 1995, I followed my Ph.D. adviser to Princeton University, first as a visiting student (1995-1996), then as a research associate (1996-1997).

7. My academic career started at the University of Hawaii at Manoa in 1997. Two years later, I moved to Texas A&M University. I teach undergraduate courses in circuit theory, signal and systems, digital signal processing, and probability theory. I also teach graduate courses in digital image processing & computer vision, advanced digital signal processing, random processes, information theory, pattern recognition, data compression, and network information theory and coding.

8. Because of my Ph.D. thesis work on the best wavelet-based image codec, I was fortunate to receive three prestigious research awards in my early career: an NSF Career Award in 1999, an ARO Young Investigator Award in

2000, and an ONR Young Investigator Award in 2001. These grants allowed me to fund graduate students and postdocs to work on distributed video coding. Prof. Bob Gray from Stanford University commented in 2005 that Prof. Kannan Ramchandran at UC Berkeley and I are the research leaders in distributed source coding.

9. In 2004, I was invited to write a feature article entitled “Distributed source coding for sensor networks” for the IEEE Signal Processing Magazine – the most cited IEEE journal according to the annual Journal Citation Report (2003 edition) published by the Institute for Scientific Information. This article subsequently received the 2006 IEEE Signal Processing Magazine best paper award. In the same year, I was elevated to an IEEE fellow for my contribution to source and channel coding. At that time, I was still an associate professor.

10. I am also co-recipient of top 10% paper awards at the 2011 and 2015 IEEE Multimedia Signal Processing (MMSP) Workshops, an IBM best student paper award at the 2016 IEEE International Conference on Pattern Recognition (ICPR), and the best demo paper award at the 2018 IEEE International Conference on Multimedia and Expo (ICME).

11. I was a visiting professor (a) in the Department of Electrical Engineering at Stanford University in Spring 2010, (b) at The Methodist Hospital Research Institute in Houston, TX during 2011-2013, and (c) in the Dept of

Electrical and Computer Systems Engineering, Monash University, Melbourne, Australia during 2016-2018.

12. I served as an associate editor for the IEEE Trans. on Circuits and Systems for Video Technology (1999-2005), the IEEE Trans. on Image Processing (2002-2005), the IEEE Trans. on Signal Processing (2002-2006), the IEEE Trans. on Systems, Man, and Cybernetics (part B) (2005-2009), the IEEE Trans. on Communications (2008-2013), and the IEEE Trans. on Multimedia (2017-2020). I also served as a guest editor for IEEE Signal Processing Magazine: Special Issue on Signal Processing for Multiterminal Communication Systems, September 2007 and IEEE Journal of Selected Topics in Signal Processing: Special Issue on MIMO-Optimized Transmission Systems for Delivering Data and Rich Content, April 2008.

13. I served as Chair of video and image processing track of IEEE ICME in 2003, Publications chair of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) in 2007, Technical program committee co-chair, of IEEE Information Theory Workshop (ITW) in 2007, Tutorial chair of IEEE International Symposium on Information Theory (ISIT) in 2010, Award chair of IEEE Global Communications Conference (Globecom) in 2014, and General co-chair of IEEE MMSP Workshop in 2017.

14. I was an invited Panelist on Distributed Video Coding: Trends and Challenges at the IEEE Picture Coding Symposium (PCS) in 2007. I also co-organized special sections on topics related to distributed source/video coding, distributed joint source-channel coding, and networked video at major conferences such as IEEE ICASSP, IEEE International Conference on Image Processing (ICIP), IEEE ICME, and IEEE/SPIE International Conference on Visual Communications and Image Processing (VCIP). I was also a tutorial presenter on these topics at ICASSP 2005, VCIP 2005, ICME 2007, Globecom 2007, and VCIP 2010.

15. I served on the IEEE Signal Processing Society Multimedia Signal Processing Technical Committee, the IEEE Communications Society Multimedia Communications Technical Committee, and the IEEE Circuits and Systems Society Multimedia Systems & Applications Technical Committee. I also served on the IEEE Trans. Circuits and Systems for Video Technology best paper award committee and was the best paper award chair for the IEEE Trans. Multimedia in 2017 and 2018. I was elected as a Distinguished Lecturer of the IEEE Circuits and Systems Society for 2008-2009.

II. MATERIALS CONSIDERED

16. In preparation of this declaration, I have considered the materials discussed in this declaration, including, for example the '828 Patent, the

prosecution history of the '828 Patent, and the prior art cited and discussed in this declaration.

17. In particular, I have reviewed and considered the following documents, among others, in connection with my analysis of the '828 Patent:

- EX1001: The '828 Patent;
- EX1002: The prosecution history of U.S. Patent Application No. 09/626,044, which led to the issuance of the '828 Patent;
- EX1005: U.S. Patent No. 6,332,193 (“Glass”);
- EX1006: Rieger and Rode, “Digital Image Recording for Court-Related Purposes” (IEEE 1999) (“Rieger”);
- EX1007: Declaration of Rachel J. Watters on Authentication of Publication;
- EX1008: “Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif) Version 2.0” (JEIDA Nov. 1997) (“Exif 2.0”);
- EX1009: “Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif) Version 2.1” (JEIDA June 1998) (“Exif 2.1”);
- EX1010: Declaration of Kenneth Parulski;
- EX1011: U.S. Patent No. 6,959,384 (“Serret-Avila”);

- EX1012: Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Chs. 8 and 18 (2d ed. 1996);
- EX1013: Rivest, Request for Comment 1321 (April 1992);
- EX1014: U.S. Patent No. 6,707,915 (“Jobst”);
- EX1015: U.S. Patent No. 5,499,294 (“Friedman”);
- EX1016: U.S. Patent No. 5,504,518 (“Ellis”);
- EX1017: U.S. Patent No. 5,764,770 (“Schipper”);
- EX1018: U.S. Patent No. 6,253,337 (“Maloney”);
- EX1019: U.S. Patent No. 6,269,446 (“Schumacher”);
- EX1020: Tentative Claim Construction Order issued in *Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.);
- EX1021: Plaintiff Jonathan E. Jaffe’s Disclosure of Asserted Claims and Infringement Contentions in *Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.);
- EX1022: Plaintiff’s Initial Claim Construction Brief in *Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.);
- EX1023: Plaintiff’s Responsive Claim Construction Brief in *Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.);

- EX1024: Plaintiff's Objections and Responses to Defendant's Claim Construction Interrogatories in *Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAx) (C.D. Cal.); and
- EX1025: Plaintiff Jonathan E. Jaffe's First Amended Complaint for Patent Infringement filed in *Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAx) (C.D. Cal.).

18. My analysis and opinions are further based on my education, training, experience, and knowledge in the relevant field.

III. RELEVANT LEGAL STANDARDS

19. I am not an attorney. For the purposes of this declaration, I have been informed by counsel for the petitioners about certain aspects of the law that are relevant to forming my opinions. My understanding of the relevant law is as follows.

A. Burden of Proof

20. I understand that the petitioner in an *inter partes* review proceeding must demonstrate unpatentability by a preponderance of the evidence. I understand preponderance means more likely than not in this context.

B. Legal Standards for Prior Art

21. I understand that a patent or other publication must first qualify as prior art before it can be used to invalidate a patent claim.

22. I understand that a U.S. or foreign patent qualifies as prior art to a challenged patent if the date of issuance of the patent is prior to the invention of the challenged patent.

23. I further understand that a printed publication, such as an article published in a magazine or trade publication, qualifies as prior art to a challenged patent if the date of publication is prior to the invention of the challenged patent.

24. I understand that a U.S. or foreign patent also qualifies as prior art to a challenged patent if the date of issuance of the patent is more than one year before the filing date of the challenged patent.

25. I further understand that a printed publication, such as an article published in a magazine or trade publication, constitutes prior art to a challenged patent if the publication occurs more than one year before the filing date of the challenged patent.

26. I also understand that a U.S. patent qualifies as prior art to the challenged patent if the application for that patent was filed in the United States before the invention of the challenged patent.

C. Person of Ordinary Skill in the Art

27. I understand that my assessment of the claims of the challenged patent and the teachings of the prior art and my analysis and opinions herein must be undertaken from the perspective of what would have been known or understood by

a person having ordinary skill in the art, reading the challenged patent on its priority date and in light of the specification and file history of the patent. I may refer to such a person as a “POSITA.”

28. I further understand that in determining the level of ordinary skill in the art, I may consider factors including:

- (a) the type of problems encountered in the art or field of invention,
- (b) prior art solutions to those problems,
- (c) the rapidity with which innovations are made,
- (d) sophistication of the technology, and
- (e) the educational level of active workers in the field.

29. I understand that a person of ordinary skill in the art, or POSITA, is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors above. This hypothetical person has knowledge of all prior art in the relevant field and takes from each reference what it would teach to a person having the skills of a POSITA.

D. Anticipation

30. I understand that a patent claim may be “anticipated” if each element of that claim is present either explicitly or inherently in a single prior art reference, and that the elements should be arranged in the reference as in the claim. I understand that for a claimed limitation to be inherently present, the prior art

reference need not expressly disclose the limitation so long as the claimed limitation necessarily flows from a disclosure in the reference.

E. Obviousness

31. I understand that a patent claim can be considered to have been obvious to a person of ordinary skill in the art at the time of the claimed invention. This means that, even if all of the requirements of a claim are not found in a single prior art reference, the claim is not patentable if the differences between the prior art and the subject matter in the claim would have been obvious to a person of ordinary skill in the art at the time of the claimed invention.

32. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious.

33. I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the asserted claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations such as commercial success, long-felt but unresolved needs, failure of others, etc.

34. I understand that an obviousness evaluation can be based on a combination of multiple prior art references.

35. I also understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but other times the nexus linking two or more prior art references is simple common sense.

36. I further understand that the obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

37. I understand that if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

38. I also understand that practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I further understand that a person of ordinary skill in the art looking to overcome a problem will often be able to fit together the teachings of multiple publications. I understand that obviousness analysis therefore takes into account the inferences and creative steps that a person of ordinary skill in the art would employ under the circumstances.

39. I understand that a particular combination may be proven obvious merely by showing that it was obvious to try the combination. For example, when

there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp because the result is likely the product not of innovation but of ordinary skill and common sense.

40. The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, the patent claim is likely obvious.

41. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill in the art, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

42. I understand that a proposed obviousness combination does not need to be the preferred, or most desirable, combination available, in order to render a claim obvious. Instead, there must be something that suggests the desirability of

the proposed combination, not necessarily something that suggests that the proposed combination is the most desirable combination available.

43. Similarly, I understand that for purposes of obviousness, when a motivating benefit comes at the expense of another benefit, that does not nullify the proposed obviousness combination or modification. Likewise, a proposed obviousness combination does not fail merely because it may be inferior to other systems used for the same use.

44. I also understand that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements between the multiple references. Likewise, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. Instead, the test is whether a claim is rendered obvious by the teachings of the prior art as a whole.

45. I understand that a claim can be obvious in light of a single reference, without the need to combine references, for example, if elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

46. I understand that in considering obviousness, I should keep in mind that a person of ordinary skill in the art has ordinary creativity and is not an automaton.

47. I understand that in considering obviousness, it is improper to determine obviousness using the benefit of hindsight derived from the patent being considered.

48. I understand that secondary indicia of non-obviousness may include: (1) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (2) commercial success of processes covered by the patent; (3) unexpected results achieved by the invention; (4) praise of the invention by others skilled in the art; (5) taking of licenses under the patent by others; (6) deliberate copying of the invention; (7) failure of others to find a solution to the long felt need; and (8) skepticism by experts.

49. I also understand that there must be a relationship between any such secondary considerations and the claimed invention. I further understand that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

50. In sum, my understanding is that prior art teachings are properly combined where a person of ordinary skill in the art having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a

reason for combining the elements of multiple prior art references in the claimed manner.

F. Priority/Written Description

51. Counsel has informed me that it is elementary patent law that a patent application is entitled to the benefit of the filing date of an earlier filed application only if the disclosure of the earlier application provides support for the full scope of the claims of the later application, as required by 35 U.S.C. § 112. Counsel has also informed me that when a priority claim involves a chain of priority documents, each application in the chain leading back to the earlier application must comply with the written description requirement of 35 U.S.C. § 112.

Petitioners' counsel has informed me that, to satisfy the written description requirement of 35 U.S.C. § 112, the disclosure of the earlier filed application must convey with reasonable clarity to those skilled in the art that, as of the filing date sought, the inventor was in possession of the invention. Petitioners' counsel has informed me that a prior application that merely renders the later-claimed invention obvious is not sufficient to meet the written description requirement—it must describe the claimed invention with all its limitations. Similarly, Petitioners' counsel has informed me that it is not sufficient for purposes of the written description requirement of § 112 that the disclosure, when combined with the

knowledge in the art, would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose.

52. Counsel has informed that even when each element may be individually described in the specification, the lack of adequate description of their combination renders those claimed combinations invalid under § 112. Petitioners' counsel has informed me that it is not enough that an applicant may show where each claimed element resides in the earliest filed application but instead must also provide support for the linkage of the claimed elements creating the embodiment. Counsel has informed me that a patent owner cannot show written description support by picking and choosing claim elements from different embodiments that are never linked together in the specification. Counsel has informed me that a description that merely renders the invention obvious does not satisfy the written description requirement.

IV. TECHNICAL ANALYSIS OF THE '828 PATENT

A. Overview of the Patent Specification

53. The '828 Patent is entitled "Indigenous Authentication for Sensor-Recorders and Other Information Capture Devices." EX1001, 1. The patent application was filed on July 27, 2000, and the patent issued on June 29, 2004. EX1001, 1.

54. The '828 Patent relates to a “method and apparatus that allows [a] stored recording to be verified as an authentic, unaltered sample of the environment.” EX1001, 1:8-12. Such “recordings” include “digital images, data files, and the more common audio recording.” EX1001, 1:17-19; *see also* EX1001, 3:41-43 (“In recording a continuous sample of a visual environment, a continuous optical recorder such as a video camera, movie film camera or a digital movie camera is used.”), 3:47-49 (“In recording a sample of an auditory environment, a continuous audio recorder such as a tape recorder or a digital recorder is used.”).

55. The '828 Patent states that “[t]he increasingly rapid transition to digital capture, analysis, storage, transmission, distribution and use of information, using increasingly sophisticated hardware and software for creation and capture tools, makes it increasingly difficult to accept any image or data file as authentic on its face.” EX1001, 4:7-12; *see also* EX1001, 1:27-29 (“Recent technological advances have brought the ability to alter images to the neophyte level.”). To address “the problem of either deliberate or inadvertent alteration of recordings,” the patent states that “[i]t is desirable to provide an improved method and system for determining the authenticity of a sample of an environment.” EX1001, 1:15-17, 1:52-54; *see also* EX1001, 4:27-31 (“One aspect of the present invention allows generally complete mitigation of the threat of undetected image alteration

and subsequent use of the altered image for purposes of deliberate or unknowing deception.”).

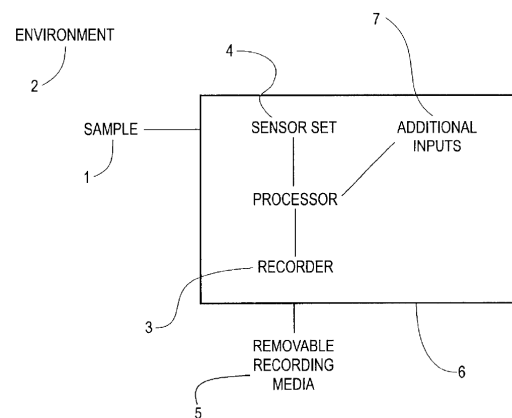
56. To this end, the ’828 Patent describes “creat[ing] an image or data file that is considered ‘trustworthy’ in any situation where proof of authenticity is necessary.” EX1001, 3:66-4:1. Specifically, the ’828 Patent describes generating “[a] digital signature...that is a function of both the sample of the environment itself, as well as at least one parameter....” EX1001, 1:54-56. “The sample is stored in memory together with the at least one parameter and the digital signature.” EX1001, 1:57-59. “Authenticity of the stored image is determined by creating a new signature from the stored image and at least one parameter, and then comparing the two signatures to determine if they are the same.” EX1001, 1:59-62.

57. The ’828 Patent further states that “[a] key to verifiable authenticity is to insure that the authentication information generation is tightly coupled to the sensor set and recorder.” EX1001, 3:16-18. The patent specification does not define the term “tightly coupled” but states that “[t]here can be nothing that can possibly alter the recording before the authentication information is generated.” EX1001, 3:18-20.

58. The ’828 Patent describes the purported invention largely in the context of digital photography. EX1001, 2:62-64 (“One embodiment of the

present invention relates to digital photography where an image is authenticated as a whole.”). Figure 2 of the ’828 Patent (included below) provides a “schematic diagram of a self-contained digital camera that incorporates certain aspects of the present invention....” EX1001, 2:12-14.

FIG. 2



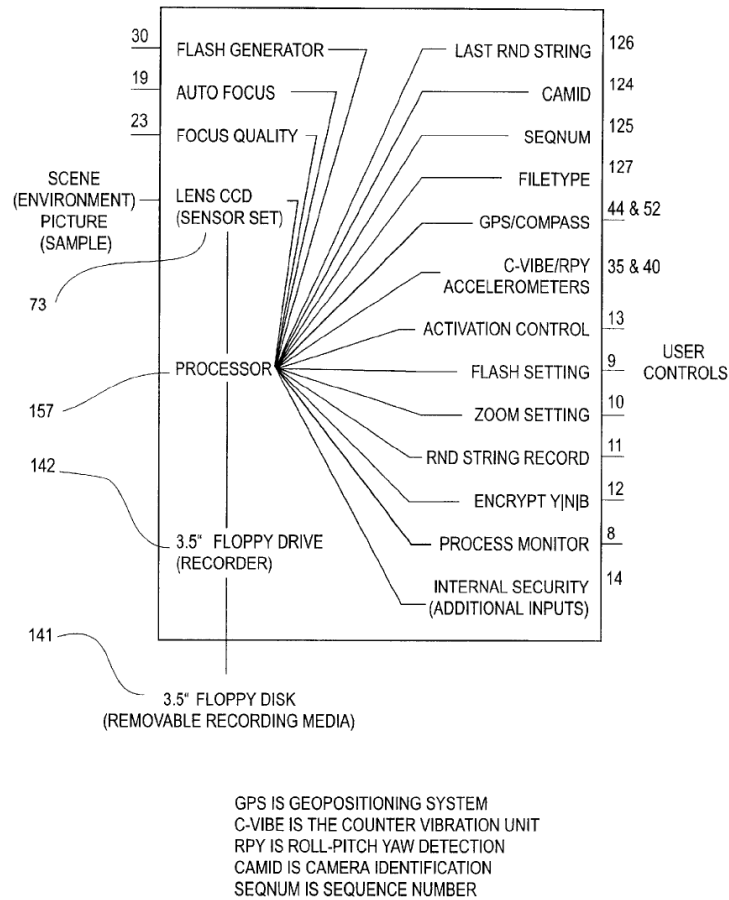
EX1001, Fig. 2.

59. In reference to Figure 2, the patent states that although “an environment 2 can be sampled 1 in a variety of formats,” “[i]n recording a single sample of a visual environment, a single frame optical recorder, generally known as a camera, is used.” EX1001, 3:32-36. “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, 4:65-67.

60. Figure 2A of the ’828 Patent (included below) is a “detailed schematic diagram of a self-contained digital camera that incorporates certain aspects of the

present invention.” EX1001, 2:15-17; *see also* 4:52-54 (“Referring to FIG. 2A, a device model for a single frame optical recorder, more commonly known as a camera, is shown.”).

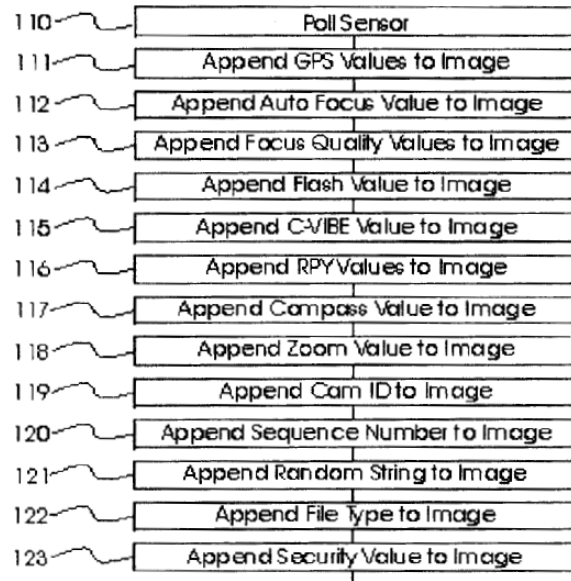
FIG. 2A



EX1001, Fig. 2A. The figure identifies the “sensor set” as a “Lens CCD.” A person of ordinary skill in the art would have readily understood “CCD” to refer to a “charge-coupled device,” which is a light-sensitive integrated circuit used to capture images in a digital camera or similar device.

61. The '828 Patent states that “[t]he sensor set 73 acquires the image 146 which is the minimum viewable information.” EX1001, 8:12-14. The patent further states that “[a]dditional data from the camera 147, viewable by the user, include: Global Positioning System (GPS) information 111; zoom settings; AutoFocus status; the results of the focus quality sampling; roll, pitch and yaw (RPY) values; the compass heading; flash status; File Type; CamID; Seq 120; and Security Value.” EX1001, 8:14-19.

62. As illustrated in Figure 6 (included below), the '828 Patent describes the post-capture processing of an image as involving “gather[ing] the image and [preparing] it for recording” and appending information about the image, such as “GPS values,” “flash value,” and “camera identifier” to the image. EX1001, 6:47-53, 6:55-67.



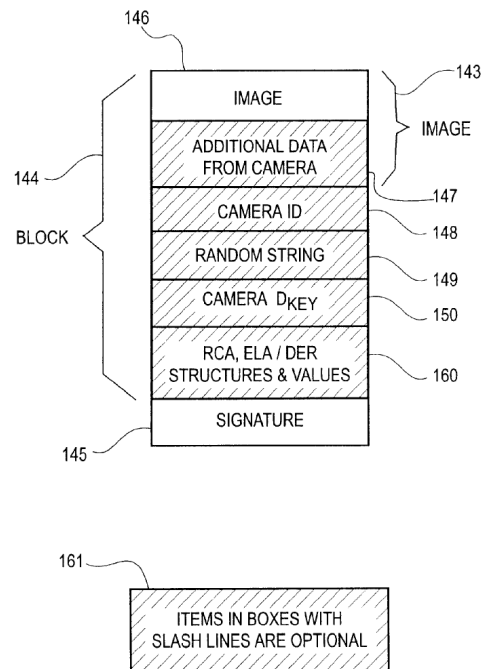
(Continued on Figure 6 B)

FIGURE 6

EX1001, Fig. 6.

63. The file produced is illustrated in Figure 7A of the '828 Patent (included below), which is a “diagram of a file format for a signed digital image.” EX1001, 2:37-38. The patent describes the illustrated file in terms of an embodiment the patent refers to as “the Signa2 process.” EX1001, 7:62-63. It states that files created by the Signa2 process are “in a format generally accepted by the industry” and that the inclusion of additional information is “in compliance with the standards for the format.” EX1001, 7:63-67.

FIG. 7A



EX1001, Fig. 7A. The digital signature is “a function of the signature protocol (SP) being used and the block” identified in Figure 7A (indicated by the bracket on the left side of the file). EX1001, 7:27-30; *see also* 8:5-8 (“The second [bracket] 144 titled ‘Block’ indicates the elements covered by the signature 145. Everything inside the ‘Block’ is what is signed.”). As illustrated, the block includes “the digital data composed of the image and optionally: additional information, the camera id, the random string, the camera decryption key, and the RCA and ELA/DER structures and values.” EX1001, 7:30-34; *see also* 8:9-10 (“Elements shaded in gray 161 are optional and not required to fulfill the basic purpose of

Signa2 devices.”). The signature is included in the file with the image and optional additional information. EX1001, 7:27-30.

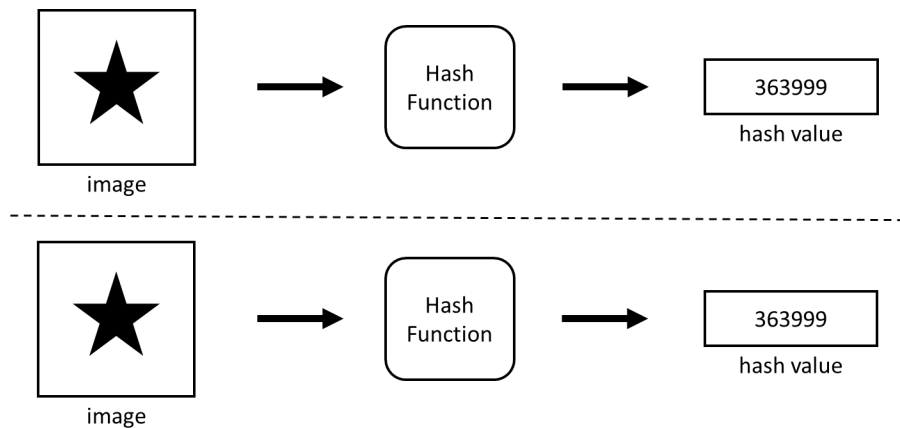
64. The digital signature is generated using a signature protocol such as “the commercially available MD5” though it is “not limited to the MD5.”

EX1001, 7:25-27. The patent does not describe MD5, but a person of ordinary skill in the art in 2000 would have known that MD5 is a one-way hash function commonly used in cryptography and data processing. EX1012, 39; EX1013; EX1014, 2:38-45; EX1006, 11.

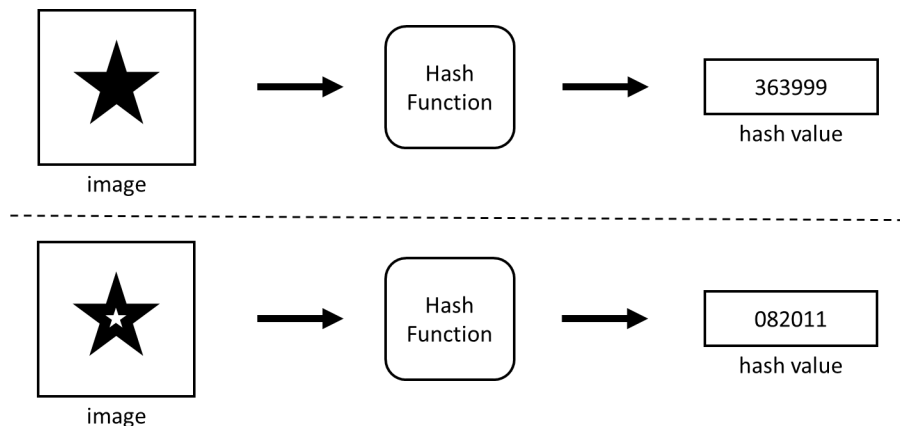
65. A one-way hash function like MD5 is a special mathematical function, or algorithm, that generates a fixed-length hash value based on the information input to the function. EX1006, 11; EX1012, 32-34. The MD5 hash function generates a 128-bit hash value regardless of the size of the input. EX1006, 11; EX1012, 39. This type of function is referred to “one-way” because it is effectively impossible to determine the input based on the output hash value. A hash function is determinative, meaning that every time the same input is used the hash function will produce exactly the same output hash value. However, if even a slight change is made to the input, the output hash value will be entirely different. EX1006, 11; EX1012, 32-34.

66. A one-way hash function, like MD5, is useful as a signature protocol in the context of the ’828 Patent because if the same image (or other type of input)

is provided to the hash function it will always produce the same output value, as illustrated below (in a simplified manner).



However, if any change is made to the image—even a single bit—the resulting output hash value will be completely different, as shown below.



Thus, a simple comparison between the initial hash value and the later hash value (after the modification) will show that a change has been made.

67. The '828 Patent discloses generating the signature using MD5, or other signature protocol, and then including it in the file with the original image and optionally other information, as illustrated in Figure 7A (discussed above).

68. The process for later authenticating the image “starts with a file believed to contain an image and the additional items (see FIG. 7A) to make the file authenticable as a Signa2 image.” EX1001, 9:13-15. The “block 144 is separated 174 from the signature 145 and the signature is recalculated 175 from the original block 144.” EX1001, 9:43-45. “If the recalculated signature (SIG_R) matches 176 the provided signature (SIG_P), the image may be viewed 248 and is marked authenticated 249 as a valid image....” EX1001, 9:45-49. However, “[i]f the two signatures do not match, and the authenticator program has been acquired from a trusted source and is free from alteration; then the image file has been damaged or altered. This is a true-negative, an image properly determined not to be authentic.” EX1001, 9:50-54.

B. The Prosecution History

69. The '828 Patent was issued based on Patent Application No. 09/626,044, which was filed on July 27, 2000. EX1002. The application contained eight claims, including two independent claims (i.e., application claims 1 and 5). Original application claim 5 read as follows:

5. A method for allowing a data stream to be authenticated comprising the steps of:
storing a data stream in a memory;

~~storing at least one parameter in said memory, said at least one parameter being generally representative of at least one condition under which said data stream was generated;~~
~~utilizing said data stream and said at least one parameter to generate a first signature that is stored in said memory with said data stream;~~
~~generating a second signature from said data stream and parameters at a point in time subsequent to computation of said first signature; and~~
~~comparing said first and second signature to see whether said first and second signatures are the same.~~

EX1002, 42-43.

70. On August 12, 2003, the examiner issued an Office Action rejecting all pending claims as anticipated by U.S. Patent No. 5,764,770 (“Schipper”).

EX1002, 151-154.

71. On December 3, 2003, the applicants responded by canceling all of the pending claims and adding new application claims 9-14. The new claim 9 (which later issued as claim 1 of the '828 Patent) read as follows:

9. (new) 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 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 image;
- 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.

EX1002, 275.

72. The applicants argued that the new claims were different from the prior art Schipper patent. EX1002, 277. They argued that Schipper does not teach the “tight coupling” required by the claim limitation “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” EX1002, 277 (emphasis in original). The applicants stated that an “[e]xemplary structure or method steps corresponding to this claim feature is shown in Fig. 2A...which illustrates a processor 157 which is ‘tightly coupled’ to a memory.” EX1002, 277. They further argued that “[b]ecause 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.” EX1002, 277. The applicants argued that “[t]he Schipper patent teaches no such ‘tight coupling.’” EX1002, 277.

73. On February 24, 2004, the examiner issued an Office Action again rejecting all pending claims. This time the rejection was based on the combination of Schipper and U.S. Patent No. 6,253,337 (“Maloney”), which rendered the claims obvious. EX1002, 282-285.

74. On March 16, 2004, the applicants responded by amending the claims and arguing that the cited prior art did not render the amended claims obvious. EX1002, 289-293. In particular, the applicants added the following step to application claim 9: “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.” EX1002, 290.

75. The applicants argued that neither of the cited prior art references taught or suggested the limitation of “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” EX1002, 292. They asserted that “the claimed ‘tight coupling’ requires that the connections between the sensor and the memory not be physically accessible to a user.” EX1002, 292. They distinguished the application claims from the Maloney prior

art reference, which referred to a “tightly coupled sensor/processor” it described as a “suite of inter operable tools,” but did not disclose that “physical access to the ‘suite of inter operable tools’ is prevented.” EX1002, 292.

76. The applicants also argued that Maloney does not teach the “monitoring” step that had been added to application claim 9. EX1002, 292-293. The applicants stated that the “monitoring” step “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.

77. On April 20, 2004, the examiner issued a Notice of Allowance. EX1002, 314-315. Application claims 9-14 were renumbered in the issued patent as claims 1-6. EX1002, 355.

78. A Certificate of Correction was issued on August 17, 2021. EX1001, 34. The correction changed the step in claim 1 of “utilizing said signature protocol to generate a second signature based on said image” to “utilizing said signature protocol to generate a second based on said data stream” (i.e., “said image” was changed to “said data stream”).

C. The Patent Claims

79. The '828 Patent contains one independent claim (i.e., claim 1) and five dependent claims (i.e., claims 2-6). I have analyzed all six claims.

80. Claim 1 reads as follows (including the modification made in a Certificate of Correction):

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

[1a] storing a data stream in a data file in a memory;

[1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

[1c] 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;

[1d] 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;

[1e] utilizing said signature protocol to generate a second signature based on said data stream;

[1f] comparing said first signature to said second signature,

[1g] 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

[1h] 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.

EX1001, 20:59-21:18 and Certificate of Correction. (I added numbering for each limitation in brackets for ease of reference.) Claims 2-6 are dependent claims that depend directly or indirectly from independent claim 1.

D. Person of Ordinary Skill in the Art

81. As discussed above, I have been informed and understand that the level of ordinary skill in the relevant art at the time of the invention is relevant to inquiries such as the meaning of claim terms, the meaning of disclosures in prior art references, and the reasons that a person of ordinary skill in the art might have combined the teachings of certain prior art references.

82. In my opinion a person of ordinary skill in the art with regard to the '828 Patent would have had an undergraduate degree (or equivalent) in electrical engineering, computer science, or a comparable subject and would have had at least two years of work experience involving image processing. Alternatively, a person of ordinary skill in the art would have had an advanced degree (or equivalent) in electrical engineering, computer science, or a comparable subject and would have had at least one year of post-graduate research or work experience involving image processing. A person of ordinary skill in the art would have been familiar with the design and implementation of systems and devices involving

image processing, including image authentication, and would have been familiar with authentication fundamentals, including encryption, signature, and hashing principles and techniques. Similar skills and knowledge could be acquired by other means.

83. In reaching this opinion, I have considered the types of problems, and techniques for addressing them, discussed in the '828 Patent and prior art references cited on the patent. The problems and technical solutions to those problems discussed in the patent and prior art support my opinion regarding the level of ordinary skill in the art.

84. The '828 Patent discusses the problem of authenticating digital images, videos, audio recordings, and other types of digital data streams. EX1001, 3:32-58. It describes a technique for addressing the problem that involves using a one-way hash functions like MD5 to generate a digital signature. EX1001, 1:51-2:3, 7:25-34. The patent does not describe MD5, presumably because the applicants knew that a person of ordinary skill in the art would have been familiar with commercially available hash functions and similar algorithms.

85. The '828 Patent also describes three different levels of authentication and damaged element recovery: (1) total image authentication; (2) row/column authentication; and (3) elemental level authentication and damage recovery. EX1001, 7:1-19:62, Fig. 6B-9B4. While the issued claims relate to total image

authentication (TIA), the description of this and the other levels of authentication presume an understanding of image processing and authentication techniques. In addition, the patent describes digital camera embodiments including hardware components like a CCD, processor, and recorder, as well as numerous user controls and other inputs to the processor. EX1001, Figs. 2, 2A.

86. The cited prior art on the face of the '828 Patent also discusses digital image processing, signature protocols, hash functions, and various other techniques to protect and authenticate digital images.

87. Further, I was teaching and conducting research in the field in the late 1990s into the 2000s. I am familiar with the pace at which innovations were being made in the area and the education level of people working and conducting research in the field. Thus, my personal experience also informs my opinion regarding the appropriate level of ordinary skill in the art in 2000.

88. In view of my educational background as well as my decades of academic and other experience discussed above, I was a person of more than the ordinary level of skill in the art in the 2000 timeframe. My opinions expressed in this declaration were formed, however, by taking into account the perspective of a person of ordinary skill in the art in 2000. I was, and am, well acquainted with the level of knowledge of a person of ordinary skill under this definition. I have taught, supervised, and conducted research with many who would meet the

definition of a person of ordinary skill in the art. As a result, I am comfortable applying this viewpoint in assessing the '828 Patent and the state of the art in the relevant timeframe, including the prior art references I discuss below.

89. I have also considered whether my opinions expressed in this declaration would change if the level of ordinary skill in the art was varied by a few years or varied somewhat with respect to subject matter. My opinions would not change in light of such minor variations.

E. Claim Construction

90. I have been advised and understand that patent claims in an *inter partes* review are interpreted by applying the same standard that applies in federal district court proceedings, which I understand is referred to as the *Phillips* standard.

91. I understand that under the *Phillips* standard, claim terms are typically given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention based on the language of the claims, the patent specification, and the prosecution history. I understand that these sources of evidence are often referred to as “intrinsic evidence” or the “intrinsic record” of the patent. I understand that under the *Phillips* standard, extrinsic evidence such as expert or inventor testimony, dictionary definitions, and

prior art publications can also be considered but are given less weight than the intrinsic evidence.

92. I have been asked to provide my opinion regarding the meaning of the following terms to a person of ordinary skill in the art at the time of the '828 Patent based on the standard that applies in this proceeding. For claim terms not listed below, I have used the plain and ordinary meaning to a POSITA.

1. “a sensor, which is tightly coupled to said memory”

93. Claim 1 recites the step of “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” EX1001, 20:62-64. The term “tightly coupled” is not a term of art in the context of claim 1. The term is also not defined in the patent specification.

94. The patent applicants described what they meant by the term “tight coupling” during prosecution. After the claims were initially rejected, the applicants canceled all claims and added new ones including the independent claim reciting the step of “utilizing a sensor, which is tightly coupled to said memory....” EX1002, 275. The applicants then argued that the cited prior does not teach or suggest the step of “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” EX1002, 277 (emphasis in original). The applicants stated that an example of this limitation is illustrated in Figure 2A showing “a processor 157 which is ‘tightly coupled’ to a memory,”

explaining that “[b]ecause 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 processor.”

EX1002, 277. This reference to the “conductive trace or lead” between two components is the only description of any means for coupling components that the applicants considered to be “tightly coupled.” A person of ordinary skill in the art would therefore understand the term “a sensor, which is tightly coupled to said memory” to include at least “a sensor coupled to said memory via conductive traces or leads.”

95. In addition to the patent and prosecution history, I have reviewed the tentative claim construction order of the district court in the related litigation. EX1020. In that tentative order, the judge determined that “a sensor, which is tightly coupled to said memory” means “a sensor coupled to said memory via conductive traces or leads.” EX1020, 12, 22. In light of the applicants’ statements in the prosecution history, I agree that a person of ordinary skill in the art would interpret this term as stated in the court’s tentative ruling.

96. Thus, for purposes of my analysis of the challenged claims, I understand that “a sensor, which is tightly coupled to said memory” means “a sensor coupled to said memory via conductive traces or leads.”

2. “monitoring the integrity of the tight coupling between said memory and said sensor”

97. Claim 1 recites the step of “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.” EX1001, 20:65-21:2. The term “tight coupling” is not a term of art in the context of claim 1. The term is also not defined in the patent specification.

98. The specification explains, however, that “[d]uring 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, 4:65-67. Furthermore, during prosecution, the applicants added the “monitoring” step to overcome a rejection (EX1002, 290) and then argued that the added limitation “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). They asserted that “[n]o prior art reference of record...contain[s] any disclosure of this subject matter.” EX1002, 293.

99. In the district court’s tentative claim construction order, the judge determined that “monitoring the integrity of the tight coupling between said memory and said sensor ” means “determining whether physical access has been gained to the coupling between said memory and said sensor.” EX1020, 13, 22. In

light of the specification and the applicants' statements in the prosecution history, I agree that a person of ordinary skill in the art would interpret this term as stated in the court's tentative ruling.

100. Thus, for purposes of my analysis of the challenged claims, I understand that "monitoring the integrity of the tight coupling between said memory and said sensor " means "determining whether physical access has been gained to the coupling between said memory and said sensor."

3. "based on"

101. Claim 1 recites the steps of "utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter" and "utilizing said signature protocol to generate a second signature based on said data stream." EX1001, 21:3-9 and 34 (Certificate of Correction).

102. The term "based on" is somewhat ambiguous because it could be read as closed-ended (i.e., based exclusively on what follows) or open-ended (i.e., based at least on what follows). In my opinion, considering the claim language and specification, a person of ordinary skill in the art would understand the term "based on" in claim 1 to be open-ended.

103. The claim language, in light of the specification, confirms that "based on" is open-ended. Following the two relevant "utilizing" steps, claim 1 recites "comparing said first signature to said second signature" and then (i) "generating

an error signal” if the two signatures are different or (ii) “generating an ok signal” if they are the same. EX1001, 21:11-18. The data stream is authenticated if the first and second signatures match; it is not authentic if they do not match.

104. The only signature protocol disclosed by the ’828 Patent is the MD5 one-way hash function, and the only way for MD5 to generate the same first and second signature (i.e., to authenticate the data stream) is if the same input is used to generate the first and second signatures—the inputs must be the same for both. EX1001, 7:25-27. The second signature would have to be based on the same inputs as the first signature (i.e., said data stream and said at least one parameter) even though the claim recites only the data stream as input for the second signature. EX1001, 1:59-62 (“Authenticity of the stored image is determined by creating a new signature from the stored image and at least one parameter, and then comparing the two signatures to determine if they are the same.”), 9:43-54, Fig. 7A. Thus, a person of ordinary skill in the art would understand “utilizing a signature protocol to generate a second signature based on said data stream” to mean that the second signature is based at least on the data stream but potentially other input data as well (e.g., said at least one parameter, along with the data stream, used to generate the first signature).

105. I have reviewed the district court’s tentative claim construction order, which appears to agree that “based on” is open-ended. EX1020, 16.

V. PRIOR ART REFERENCES

A. Glass (EX1005)

106. U.S. Patent No. 6,332,193 to Glass, et al. (“Glass”) was filed January 18, 1999, and issued December 18, 2001. Glass discloses “[a] method and apparatus for collecting and securely transmitting biometric data over a network contains a sensor, preferably a camera, for collecting biometric data and code generating hardware and software.” EX1005, Abstract.

107. Glass describes then-existing use of biometric data to identify a user or verify an individual’s identity. EX1005, 1:34-37. This biometric data “is obtained by a system consisting of optics, camera, and electronics which capture and digitize the scene presented to the camera.” EX1005, 1:37-40.

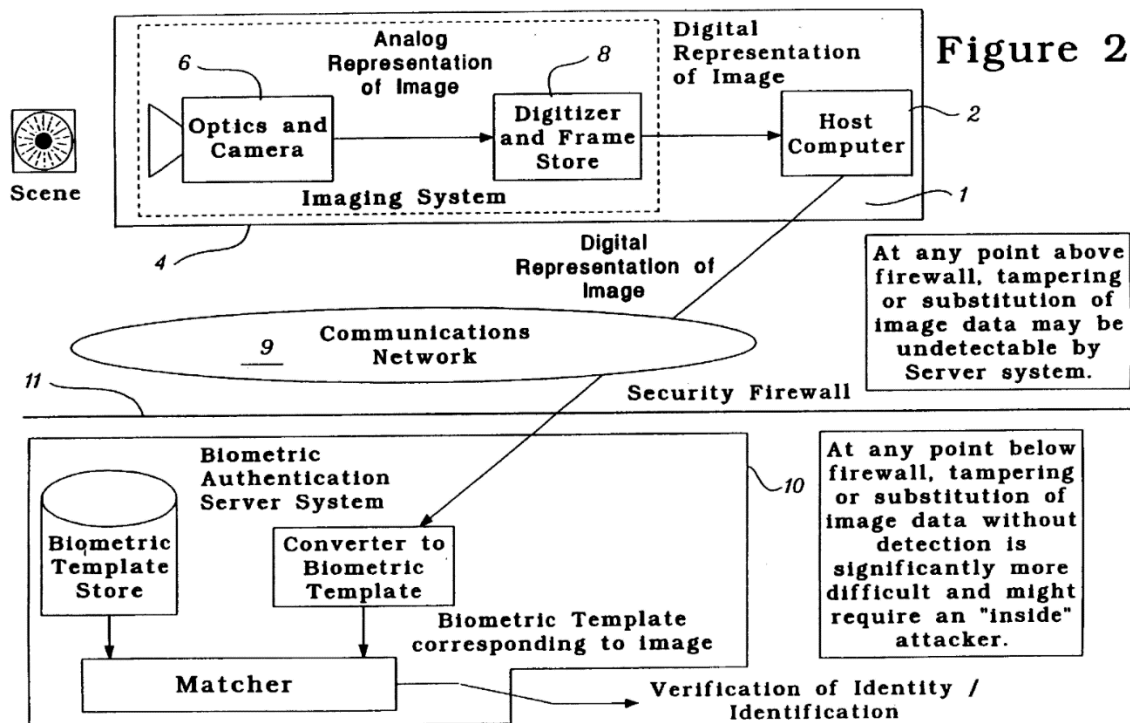
108. Glass notes, however, that “[a]ny biometric system can be defrauded if an attacker could substitute the raw image data prior to the conversion to a biometric template and subsequent matching.” EX1005, 1:60-62. An attacker, for example, “could replace the camera with a system that mimics the camera functionality thereby providing a previously stored image to the rest of the system.” EX1005, 2:13-17. An attacker could also “gain access to the inside of the client system’s host and replace the contents of the memory or frame store containing the ‘real’ image data with the memory representation of a previously stored image.” EX1005, 2:17-20. An attacker could also “gain access somewhere

along the communications path between the client system and the server system and replace the image while in transit.” EX1005, 2:21-23. Glass states a then-existing need to “prevent[] image substitution or tampering.” EX1005, 2:23-26.

109. Accordingly, Glass provides “a system and methodology which can provide secure transmission and subsequent authentication of biometric data for use in a client-server scheme in which the biometric data is transferred from one computer over an unsecured network to another computer for identification or verification of a user.” EX1005, 3:45-50. Glass “provide[s] a camera which functions as a sensor to collect the biometric data,” which “is digitized into a biometric data file.” EX1005, 3:50-52.

110. After that, “[a] code is applied to that file.” EX1005, 3:52-53. The code which is applied to the image “is computed as a function of the image, the token and a secret key associated with the camera.” EX1005, 4:1-3. The secret key “assures that an attacker with knowledge of the image, token and code generation algorithm cannot create a valid code for a substituted or tampered image” and “may be a serial number or other identification number that is unique to the camera or sensor that collects the biometric data.” EX1005, 4:3-8. “[T]he file with code is output to a network for transfer to an authentication server system,” which “validates the data by recomputing the code from its knowledge of the input data needed to generate that code.” EX1005, 3:53-57.

111. Figure 2 of Glass, shown below, “is a block diagram of a biometric identification system which transfer[s] biometric data over a network and contains our security system.” EX1005, 4:27-29; *see also* 4:45-47 (“A present preferred embodiment of our system is employed in a client server system like that illustrated in FIG. 2.”).



EX1005, Fig. 2.

112. Figure 2 shows a “separate imaging system 4” that is connected to “host computer 4.” EX1005, 4:54-55. This separate imaging system “contains a camera 6 with associated optics or other sensor for collecting the biometric data from the user.” EX1005, 4:55-58. The biometric data can be “an analog representation of an image which is then digitized and stored for later transfer.”

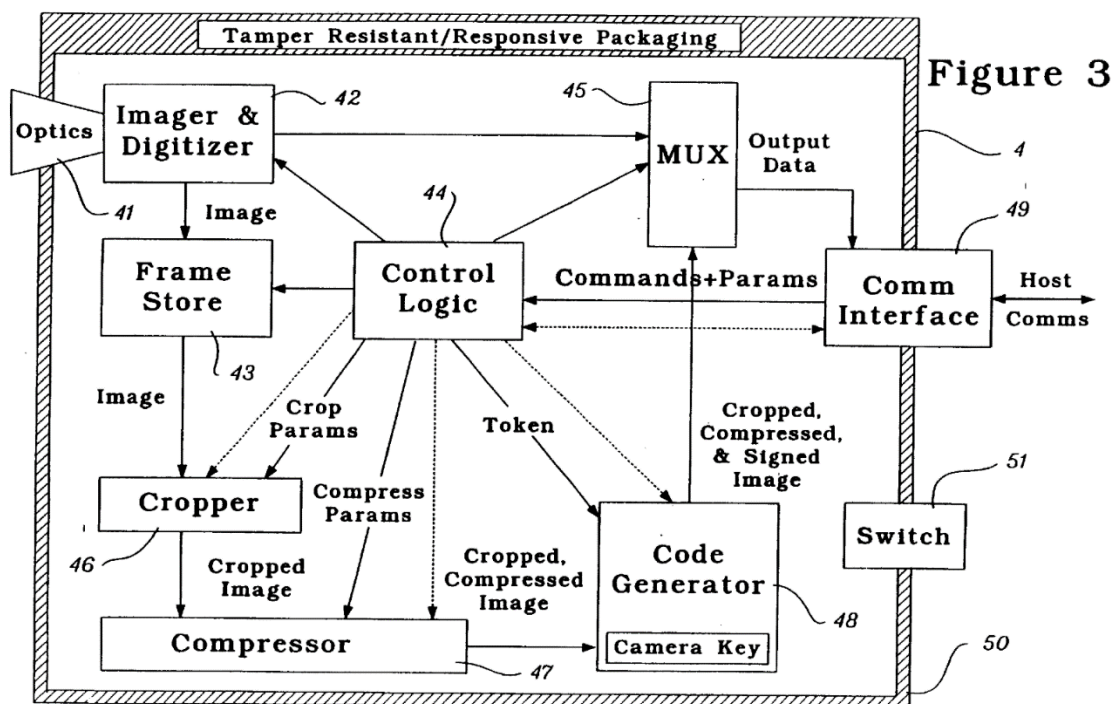
EX1005, 4:58-60. Glass “prefer[s] to provide a digitizer and memory or frame store which digitizes the image and then stores it in the imaging system 4 for later processing and transfer.” EX1005, 4:60-62.

113. Glass teaches that “[t]he 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.” EX1005, 5:13-16. This is because “[i]t is essential to ensure that the integrity of the acquired images and codes to be transmitted over the network have not been compromised.” EX1005, 5:16-19. Accordingly, Glass teaches that “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.” EX1005, 5:20-23.

114. Glass teaches both passive and active protections for the tamper resistant package. “The tamper resistant package can be passive in that any opening to the device will cause its ultimate destruction.” EX1005, 5:23-25. Or “the packaging could utilize at least one chassis intrusion detector or switch 51 shown in FIG. 3.” EX1005, 5:26-27. In this case, “[s]witch 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,” where this state “will essentially delete key software routines related to generating biometric data” and

“may also delete special battery backed up ram tables which include security or encryption information.” EX1005, 5:27-34. Thus, in Glass’s system, “if an intruder does gain access to the system he cannot inject video nor obtain codes, or even operate the system software or [firmware] thereby making his attack useless.” EX1005, 5:34-37. “Therefore, a substitution or tampering of image data after output from the secured camera will be detectable via downstream data processing, and substitution or tampering of image data prior to application of security information would be extraordinarily difficult or impossible.” EX1005, 5:37-41.

115. Figure 3, shown below, “is a functional block diagram of a present preferred imaging system which is used in the identification system” shown in Figure 2. EX1005, 4:30-32; *see also* 5:46-48 (“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.”).



EX1005, Fig. 3.

116. Figure 3 shows “Optics 41” which “direc[t]s 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,” identified as Imager & Digitizer 42 in Figure 3. EX1005, 5:49-52.

117. “The digital image is sent to a multiplexer 45 and/or a frame store memory 43.” EX1005, 5:52-54. From there, “[t]he image in the frame store 43 is sent through a cropper 46 and compressor 47 to create a cropped and compressed image that is sent to a code generator 48 which generates a code that is applied to the image.” EX1005, 5:55-58.

118. “A cryptographic technique is employed...to create a digital signature for each frame of image data acquired by the camera and optics.” EX1005, 5:62-65. The digital signature “preferably is a secure hash function which takes the following as inputs: each byte of image data in the frame; a ‘secret key’ which is stored and remains hidden inside the camera; and optionally a digital ‘token’ entered into the camera electronics by the host.” EX1005, 5:67-6:4. Alternatively, the token could have come from the authentication server. EX1005, 6:5-6. Glass notes that “[t]he ‘hidden’ or ‘secret’ key is required since an attacker, with an image plus a token plus knowledge of the digital signature algorithm could, without this secret key, mimic the authentication functionality of the camera.” EX1005, 6:6-9.

119. “The camera ‘key’ can be a small block of data contained inside the camera that is used in the digital signature algorithm.” EX1005, 6:10-12. “Optionally, the key could be a unique identifier for the camera,” which, depending on the type of scheme used, could “simply be an arbitrary value assigned to every camera, an identifier for a batch of cameras, a unique camera identifier, a unique key for a symmetric signing algorithm, or a one half of a key-pair for an asymmetric signing algorithm.” EX1005, 6:13-18.

120. Glass’s optional “token” is “a block of data generated for each and every transaction” that “is unique and is never re-used.” EX1005, 6:33-34.

“Tokens can thus be used to identify any particular transaction,” and they “provide[] an added level of security by coupling image data to a specific transaction.” EX1005, 6:35-39. Glass states that “[a]ny function which can be guaranteed to produce a unique output” can be used to generate these tokens. EX1005, 6:36-37.

121. Glass teaches using a hash function to generate the signature. EX1005, 6:40-41 (“The digital signature previously mention can be implemented as a hash function.”). Glass explains that “[t]he output of the hash function is a smaller block of data than its input elements.” EX1005, 6:41-42. “An important characteristic of a hash function is that given the same inputs, reapplication of the hash function will compute the same output.” EX1005, 6:42-45. Glass notes that “good security hash functions have the characteristic that any change in the input elements will result in a major change of the output data block” meaning that “if the hash function is computed over the image data, any change in the image data will result in a different hash function output.” EX1005, 6:45-50.

122. Given these properties, Glass states that by using hash functions, “[t]he digital signature of the data can be sent to another system (i.e. the authentication server) along with the original data; and the receiving system can, with the same or complementary token, compute a signature of the original data and check it against the signature sent with the data.” EX1005, 6:50-55. “If the

signatures match, the data can be assumed to not have been altered with an extremely high confidence level.” EX1005, 6:55-56.

123. Glass provides an example describing this authentication scheme. Glass identifies “a function $DS(x, y, z)$, where x is the image data, y is a token, and z is the secret key” that “produces an output Q .” EX1005, 6:57-61. A recipient who receives x and Q , knows y and z , and uses the same hash function “can compute $Q'=DS(x, y, z)$.” EX1005, 6:57-61. “If $Q=Q'$ then x , y , and z have not been altered, otherwise one or more of the data items have changed.” EX1005, 6:61-63.

124. Glass describes several ways the “digital signature computed by the camera can be sent back to the authenticating system.” EX1005, 7:3-5. “The most straightforward method is to append (or prepend) the signature to the data and send the complete package back to the authenticating system.” EX1005, 7:5-7. “Another technique would be to use a digital watermarking technique to embed the signature information directly into the original image data.” EX1005, 7:7-10.

125. Figures 7 and 8 of Glass, shown below, illustrate examples of “operational transaction[s]” using the disclosed system. EX1005, 4:27-41.

Figure 7

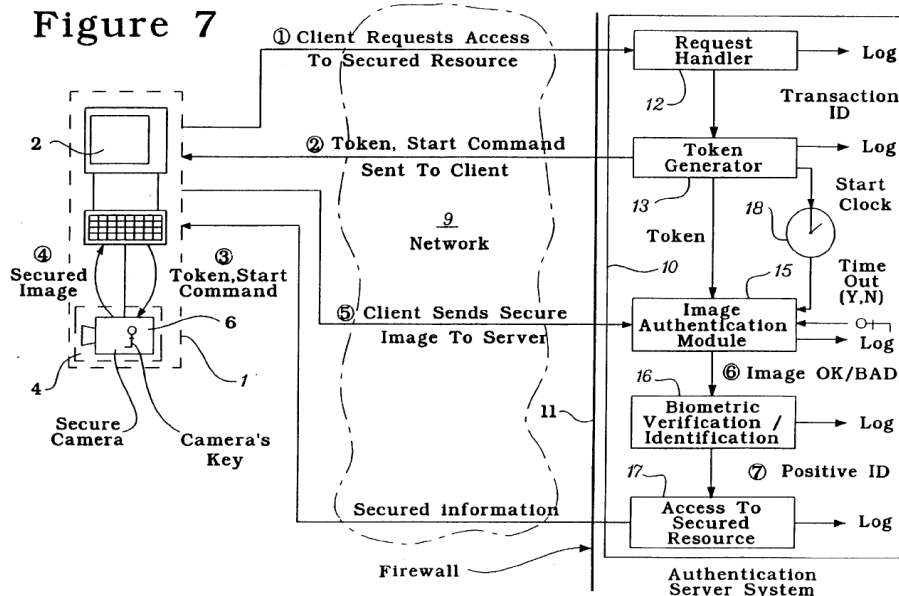
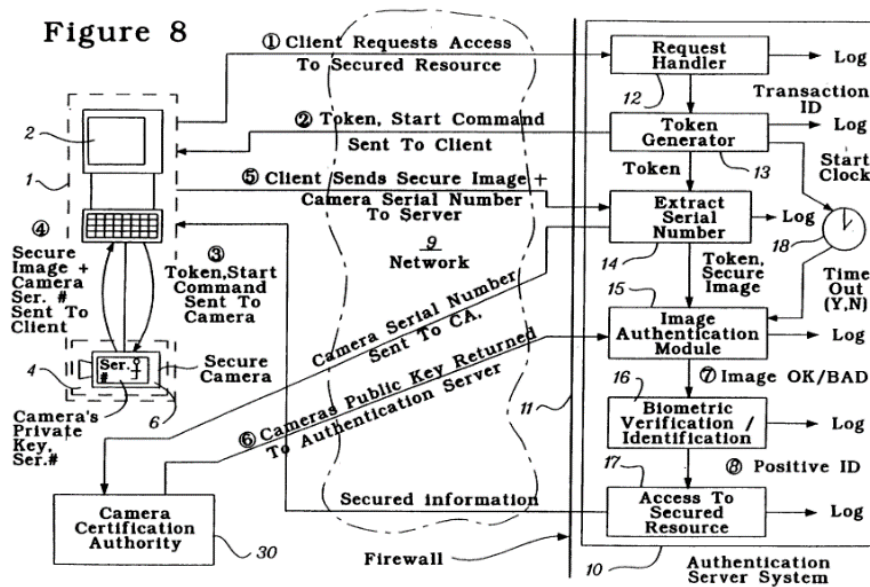


Figure 8

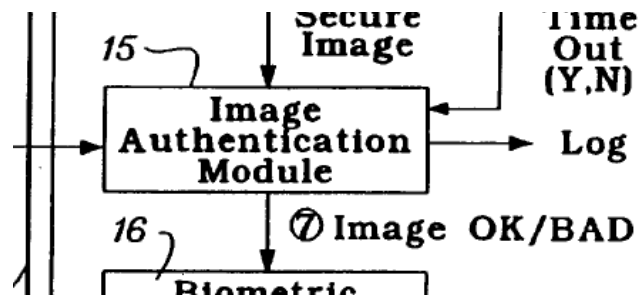


EX1005, Figs. 7 and 8.

126. Glass states that “[w]e prefer to log each step of the transaction as indicated by the word Log.” EX1005, 9:61-62. This statement is in reference to the exemplary operational transaction illustrated in Figure 7, but a person of

ordinary skill in the art would recognize that it applies broadly to the example in Figure 8 as well and to the Glass system in general.

127. For example, the following excerpt from Figure 8 shows that the Glass system logs the result of the image authentication module (i.e., the determination whether the image is “OK/BAD”).



EX1005, Fig. 8 (excerpt). Figure 7 similarly shows the system logging the result of image authentication. Glass states that “[a] record of the transaction can be logged by the server system” and that logged information “can provide irrefutable evidence of the transaction if required.” EX1005, 10:54-58.

B. Rieger (EX1006)

128. Rieger is a paper entitled “Digital Image Recording for Court-Related Purposes” by Rieger and Rode of the Kriminalistisches Institut in Germany (which appears to be the German Federal police).

129. Rieger bears a 1999 copyright notice on the first page. EX1006. I understand that it was published in the Proceedings IEEE 33d Annual 1999

International Carnahan Conference on Security Technology (Cat. No. 99CH36303) in Madrid, Spain and that the conference was held on October 5-7, 1999. EX1007.

130. I attended many IEEE conferences in the late 1990s. Authors presented their papers at those conferences and attendees could obtain a compilation of the papers in the conference proceedings either at the conference or shortly afterward.

131. I have reviewed the Declaration of Rachel Watters (EX1007) showing that Rieger was published in the conference proceedings. I am familiar with conference proceedings like those identified in her declaration. I can also confirm that people working and researching in the areas of electrical engineering, computer science, and similar fields would have known that such conference proceedings were available and could be a source of papers like Rieger.

132. Rieger notes that “it is likely that the susceptibility of digital images to manipulation will lead to increasing doubt with respect to the authenticity of photographic images in the era of digital data processing.” EX1006, 1.

Accordingly, Rieger “describes an approach to ensuring the integrity and authenticity of photographic images during the image-recording phase currently favored by the Bundeskriminalamt.” EX1006, 1.

133. Rieger states that “[e]ver since the invention of the camera, photographic documents have traditionally been associated with a high degree of

authenticity and have served as convincing evidence in court time and time again.” EX1006, 1. Rieger notes, though, that “[t]he introduction of digital image processing technology has drastically diminished the traditionally high evidentiary value of photographic images virtually overnight.” EX1006, 1. But “[a]s the quality of digital image-recording devices (scanners, digital cameras, etc.) and output equipment (film and image projectors, etc.) improves, it is becoming increasingly difficult to detect and show proof of professional image manipulation aided by digital methods.” EX1006, 1. Rieger states that “[o]ne significant advantage of digital photography, namely the widespread processing of images using reasonably-priced computers and standard commercial software, will presumably become a major problem in the process.” EX1006, 3. Rieger explains that at the time, “[t]he image manipulation illustrated above can nowadays be accomplished by a practised computer user with only routine computer skills, and - even with the help of modern scientific knowledge - there is no certainty that all such changes could be detected.” EX1006, 3. Rieger concludes that “one essential prerequisite for the recognition of digital photographs as evidence in court remains to be met, namely the possibility of creating a manipulation-proof ‘original’.” EX1006, 3.

134. Rieger proposes a solution through a manipulation-proof digital camera that would perform the following high level functions:

- “generate a digital signature of the image data through a signature component in the camera processor”;
- “insert a time stamp and possibly record camera parameters”;
- “possibly insert location data (e.g. using GPS coordinates)”;
- “insert a digital signature of the photographer”; and
- “provide physical protection of the image during each stage of the image-production process, from origin in the image sensor to generation of the photographer’s signature.”

EX1006, 3-4.

135. Rieger then goes on to explain the components and functionality of a manipulation-proof camera. Rieger explains that “[i]n order to protect image data against manipulation from the moment they are received in the CCD sensor to generation of the signature, some of the system components, including the CCD sensor, the camera CPU (which also contains a signature chip with the secret key), the RAM, the internal clock, a back-up power supply and the required connector cables must be integrated into a specially protected compartment in the camera housing.” EX1006, 4. This specially protected compartment is shown in Rieger’s Figure 3, included below, which “shows the basic conceptual diagram for a digital camera of this kind.” EX1006, 4.

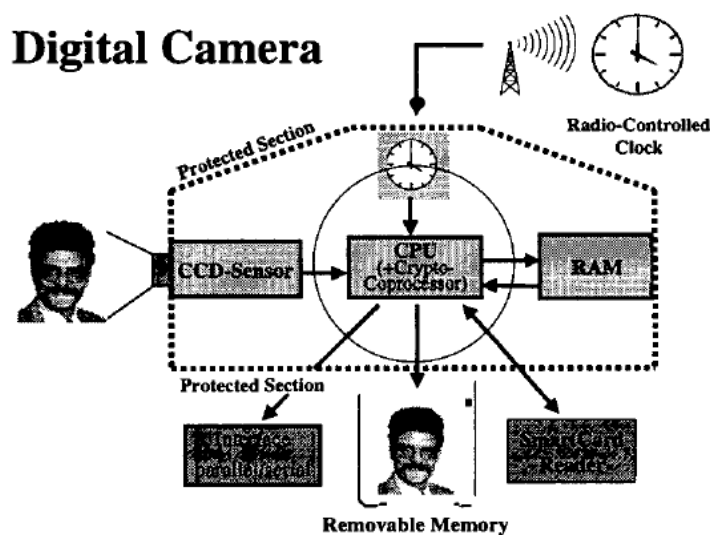


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

EX1006, Fig. 3.

136. As shown in Figure 3, Rieger’s digital camera includes a “CCD-Sensor,” “CPU (+Crypto Coprocessor),” and “RAM” (random access memory), all contained within a “Protected Section.” This secure compartment “can be protected, for example, by an electrical ‘protective shield’.” EX1006, 4. Rieger explains that when the compartment “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.” EX1006, 4. “This ensures that image data cannot be altered without detection prior to application of the signature.”

EX1006, 4.

137. Rieger explains that the CPU 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.” EX1006, 4. Figure 3 also shows “removable memory,” which Rieger says can affect “[d]ata transfer from the digital camera to an external computer.” EX1006, 4.

138. In Rieger’s camera, “[t]he signature chip has the capacity to generate a digital signature.” EX1006, 4. To do so, the signature chip contains a “secret code,” the signature algorithms, and the certifications needed for signature verification. EX1006, 4. “The matching public key for the camera is also recorded in an index on file with the issuing certification service provider.” EX1006, 4.

139. Images are saved as files in Rieger’s camera. Specifically, “[a]fter recording, the processor reads the image data from the CCD sensor and saves these to the RAM.” EX1006, 4. “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. A person of ordinary skill in the art would know that an image compressed in “the JPEG format” is stored in a file (e.g., a *.jpg file).

140. Rieger’s camera also includes a smartcard reader for use with a “signature card.” The camera is equipped with a “Smartcard reader” for use with a “signature card,” a “new multi-purpose official and installation ID card scheduled for introduction in Germany.” EX1006, 4. Before using the camera, a user

“inserts his signature card into the built-in card scanner in the camera and activates it by entering his PIN (minimum a six-place code),” after which the card and camera processor verify their compatibility. EX1006, 4. Rieger also discloses a reciprocal authentication (e.g. via the challenge-and-response method) is possible for certain applications, in which case the camera processor would be equipped with a random-number generator. EX1006, 4.

141. The image data are read out by the processor, compressed, and saved to the RAM. EX1006, 4. The compressed image data are hashed by the camera processor, and the hash total is coded with the secret key of the signature chip and linked together with the image data as the “camera signature” in the RAM. EX1006, 4.

142. A highly manipulation-proof time stamp can be obtained using a radio-controlled clock (DCF77; available throughout Central Europe) coupled with an independent, internal reference clock. EX1006, 5. Rieger states that the reference clock, at least, must be integrated into the “secure compartment” of the camera. EX1006, 5.

143. Rieger explains that the addition of a GPS receiver makes it possible to record both the exact time and the precise location of the camera along with the image data. EX1006, 5. Rieger also explains that “all camera parameters,” including focus values, aperture settings, and exposure times can be recorded and

signed. EX1006, 5. This also applies to physical data on environmental conditions (e.g. temperature, humidity, etc.). EX1006, 5.

144. In Rieger, before the entire package of image data is saved to the removable camera memory medium, “the data are hashed once again by the camera processor.” EX1006, 5. This hash value (based on image, camera signature, and camera parameters) is then “encrypted along with the secret key of the photographer’s signature card.” EX1006, 5. This encrypted hash value is returned to the RAM, where it is “linked with the image data already recorded there.” EX1006, 5.

145. Rieger describes a number of potential security-related attacks on the manipulation-proof camera. Among other scenarios, Rieger describes how the camera would handle “[a]lteration of image data.” EX1006, 6-7. Rieger discloses the use of an “integrity test,” explaining that in such a test, “[b]ecause every alteration of image data, regardless of how minor (one bit is enough!), produces a totally different result in the computed check sum (hash total), an integrity test will immediately detect any alteration of the data.” EX1006, 6 (footnote omitted). The integrity test is described in Appendix II of Rieger. EX1006, 6 fn. 11.

146. In Rieger’s integrity test, “hash functions are used to verify the integrity of texts (or data).” EX1006, 11. First, “[t]he hash value is computed for a given text for this purpose.” EX1006, 11. “The hash value is then stored, either

separately or together with the text (in which case it is given special security protection).” EX1006, 11. “If subsequent recomputation of the hash value for what is presumed to be the identical text produces a different hash value, the text is presumed to have been falsified.” EX1006, 11-12. “Conversely, identical hash values confirm the identity of the data tested and thus the integrity of the text.” EX1006, 12.

C. Exif 2.0 (EX1008) and Exif 2.1 (EX1009)

147. Exif 2.0 is a printed publication entitled “Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif) Version 2.0” that was made publicly available in November 1997 by the Japan Electronic Industry Development Association (JEIDA). EX1008, 3; EX1010, ¶6. This document sets out version 2.0 of the Exif standard describing available metadata fields for digital cameras adopted by many camera makers by the late 1990s.

148. Exif 2.1 is the next version of the Exif standard. It is a document entitled “Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif) Version 2.1” that was made publicly available in 1998 by the Japan Electronic Industry Development Association (JEIDA). EX1009, 1; EX1010, ¶¶8-9.

149. I was familiar with the Exif standard in the late 1990s and early 2000s. I was also familiar with JEIDA. I taught Exif. I have often used Phil Harvey's ExifTool to extract metadata from JPEG photos. In a research project involving segmentation of FLIR (i.e., forward looking infrared) images, I wrote Matlab code to extract camera properties and GPS measurements in the Exif metadata together with the raw heatmap data embedded in the TIFF files.

D. Serret-Avila (EX1011)

150. Serret-Avila is a U.S. Patent that was filed on April 5, 2000, claiming priority to a provisional application filed on December 14, 1999, and that issued on October 25, 2005. Serret-Avila is entitled "Systems and Methods for Authenticating and Protecting the Integrity of Data Streams and Other Data." EX1011, 1.

151. Serret-Avila discloses a system and method for "providing relatively fast, secure, and efficient authentication of data streams and other electronic content." EX1011, 2:66-3:3; *see also* 3:7-9 ("The present invention provides systems and methods for securely verifying and protecting the integrity of electronic data streams and other types of electronic data."). The disclosed technique involves breaking the streaming data into multiple sub-blocks that are each hashed in a manner that creates a "chain or progression of verification values, each verification value in the chain being partially derived from the verification

values that preceded it.” EX1011, 8:32-40, Fig. 3. The encoding system sends each sub-block and its related hash value in succession to a recipient until the entire file has been transmitted. EX1011, 9:53-59.

152. As each sub-block in the file is received, “the hash of the sub-block is calculated using the same hashing function used by the encoding system” and in the same manner that the original hash values were generated. EX1011, 10:16-24. The calculated hash value is compared to the received hash value, and if the two values are equal the sub-block is “deemed to be authentic, and the sub-block can be released for use (518).” EX1011, 10:24-31, Fig. 5. If the two values are not equal, the sub-block “is judged to be unauthentic” and the decoding system can “take appropriate defensive action 516” such as displaying a warning or error message. EX1011, 10:33-45.

VI. THE CHALLENGED CLAIMS ARE OBVIOUS IN LIGHT OF THE PRIOR ART

153. It is my opinion that claims 1-6 of the '828 Patent are obvious in light of at least the prior art discussed below.

A. Glass Renders the Challenged Claims Obvious

154. While Glass discloses a particular implementation involving biometric data, Glass and '828 Patent disclose purported inventions in the same field of image processing and address the same problem of authenticating digital images. EX1005, Abstract, 1:7-10, 2:23-26, 2:32-35, 3:45-4:18; EX1001, Abstract.

155. Glass provides a sufficiently detailed description to permit a person of ordinary skill in the art to implement the aspects of Glass's system discussed below in regard to the challenged claims with a reasonable expectation of success. It would have been within the skill level of a person of ordinary skill in the art to implement Glass's system based on the disclosure.

1. Independent Claim 1

156. As I discuss further below, Glass discloses to a person of ordinary skill in the art every limitation of claim 1.

a) [1pre] A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

157. Glass discloses a *method for authenticating a data stream stored in a data file in memory*, as recited in the preamble of claim 1. (I will put claim language in italics for ease of reference throughout my analysis.)

158. Glass describes a “method and apparatus for collecting and securely transmitting biometric data over a network [that] contains a sensor, preferably a camera, for collecting biometric data and code generating hardware and software.” EX1005, Abstract. Glass uses a camera to capture biometric data to determine if the user is authorized. EX1005, 2:32-35 (“Rather the present invention is aimed at maintaining the integrity of an image containing biometric data and preventing image tampering or substitution.”).

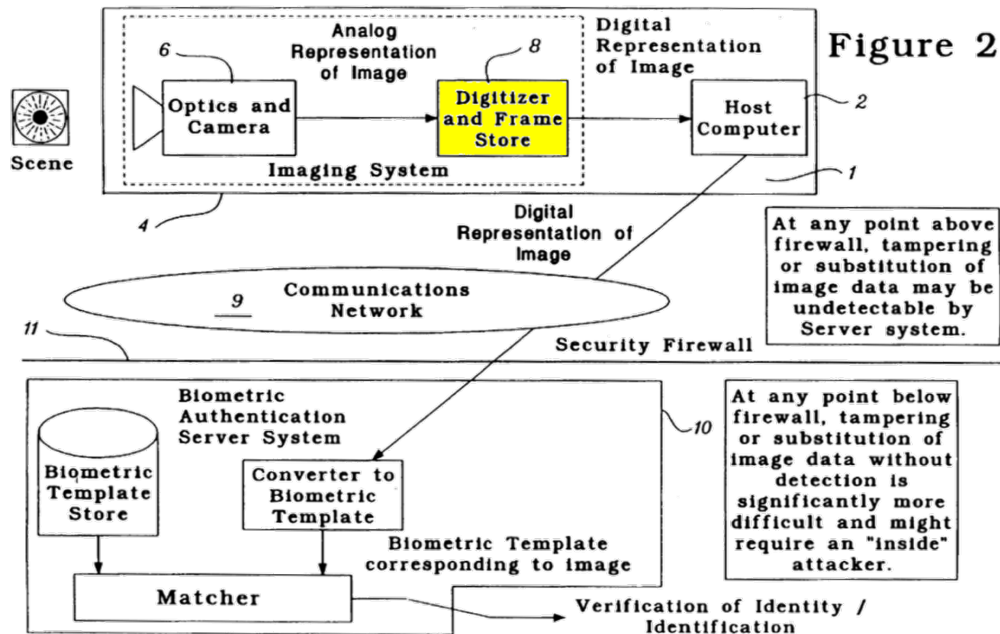
159. Glass's system provides "secure transmission and subsequent authentication of biometric data" in the image collected by the "sensor" (e.g., camera). EX1005, 3:45-51. The imaging system stores the digital image in a "memory" along with a code, which "is computed as a function of the image, [a] token and a secret key associated with the camera." EX1005, 3:52-53, 4:1-8, 4:58-62.

160. The file containing the image and code is transferred from the imaging system to an authentication server system that "validates the data by recomputing the code from its knowledge of the input data needed to generate that code." EX1005, 3:53-57.

161. Thus, Glass discloses a *method for authenticating a data stream* (digital image data) that is *stored in a data file in memory* as recited in claim 1.

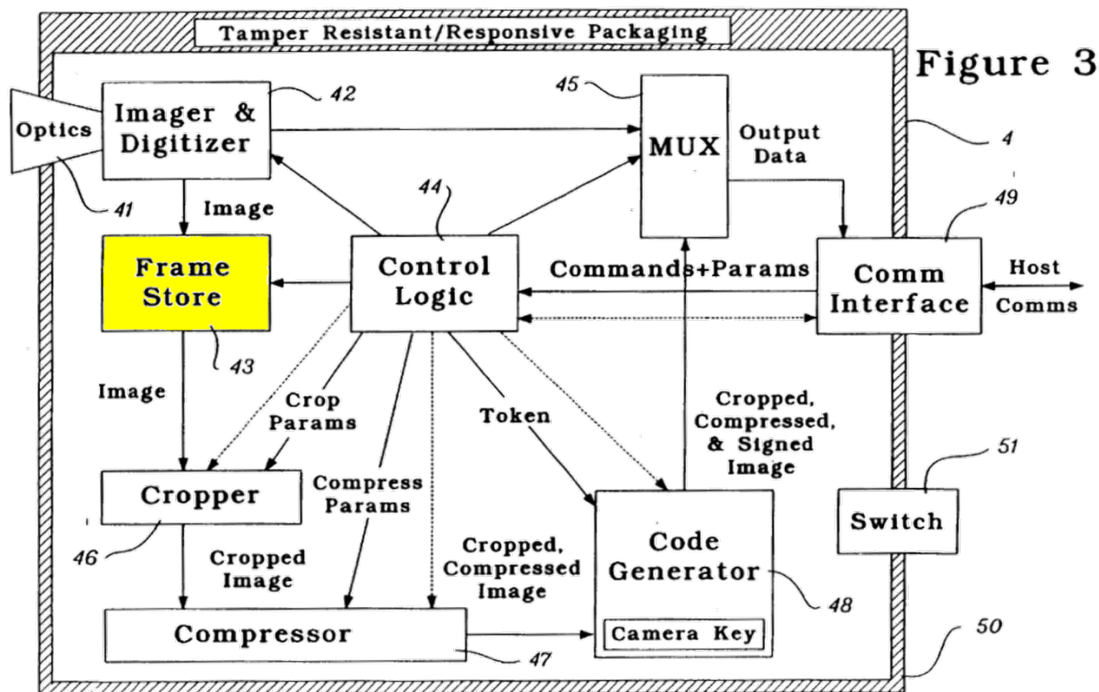
b) [1a] storing a data stream in a data file in a memory;

162. Glass discloses storing *a data stream in a data file in a memory*. In Glass, the image containing biometric data (*data stream*) is stored in a "memory or frame store" (*a memory*) in the imaging system portion of the overall system, as illustrated in Figure 2 included below. EX1005, 4:58-62.



EX1005, Fig. 2 (highlighted). As Glass explains, “[t]ypically, the biometric data will be an analog representation of an image which is then digitized and stored for later transfer.” EX1005, 4:58-60. The system uses “a digitizer and memory or frame store which digitizes the image and then stores it in the imaging system 4 for later processing and transfer.” EX1005, 4:60-62.

163. Glass’s Figure 3 also illustrates the “frame store” within imaging system 4. EX1005, 4:30-32, 5:46-48.



EX1005, Fig. 3 (highlighted). Regarding Figure 3, Glass again refers to the “frame store” as *a memory* stating that “[t]he digital image is sent to a multiplexer 45 and/or a frame store memory 43.” EX1005, 5:52-54.

164. Thus, Glass discloses *storing a data stream...in a memory* such as frame store 43 in Figure 3 (or digitizer and frame store 8 in Figure 2).

165. Glass also discloses storing the *data stream* (digital image) in a *data file* in the imaging system as recited in [1a]. In Glass, the camera data is “digitized” into a “digital file.” EX1005, Abstract (“The camera data is digitized and a unique code...is attached to the digital file.”), 3:62-63 (“That token is applied to the digital file before it is transferred to the authentication server.”), 11:19-22 (claim 1 reciting “a digitizer coupled to the sensor, the digitizer

converting the biometric data collected by the sensor into a digital file”). A person of ordinary skill in the art would understand from Glass’s disclosure that (1) the camera data is digitized into a digital file, and (2) stored in the frame store. Because the image data is digitized and stored in the imaging system (EX1005, 4:60-62), a person of ordinary skill in the art would recognize that the file (i.e., “data file” or “digital file”) is stored in the “frame store memory 43,” which is the *memory* storing the image data in imaging system 4.

166. Furthermore, a person of ordinary skill in the art would know that digital image data is almost always stored in a file in memory so that the image can be processed using standard image processing functions and tools.

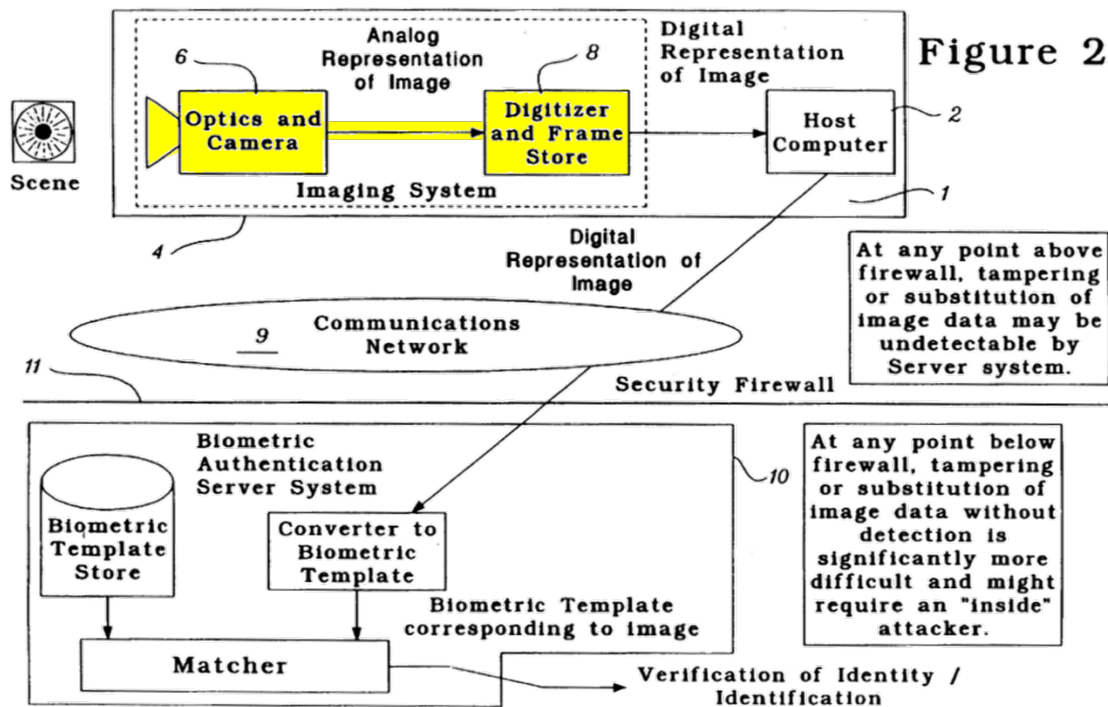
167. For these reasons, Glass discloses the step of *storing a data stream in a data file in a memory* as recited in [1a].

c) [1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

168. Glass discloses *utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter* as recited in claim 1.

169. Glass discloses a *sensor* and a *memory*. In the summary of the invention, Glass “provide[s] a camera which functions as a sensor to collect the biometric data,” such as an image (a *data stream*). EX1005, 3:50-51.

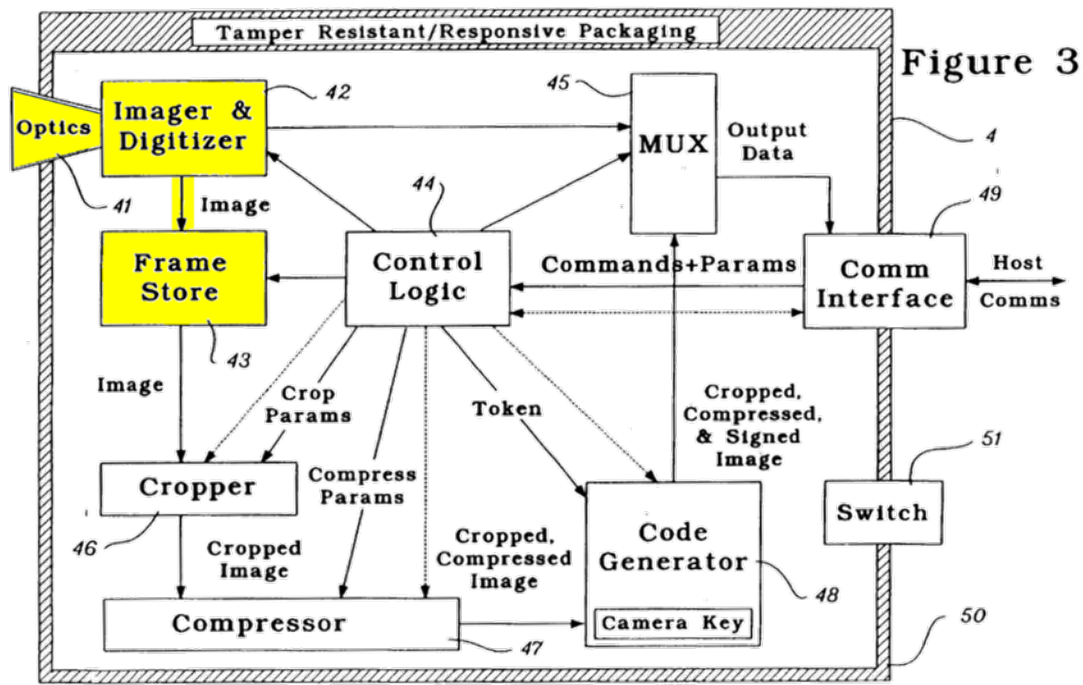
170. Figure 2, shown below, illustrates Glass's imaging system 4 including "Optics and Camera" 6 (which includes a *sensor*) and "Digitizer and Frame Store" 8 (which includes *memory*).



EX1005, Fig. 2 (highlighted). An arrow from optics and camera 6 to digitizer and frame store 8 indicates that they are connected by electrically conductive leads or traces, most likely on a circuit board, inside imaging system 4. Therefore, the *sensor* and *memory* are *tightly coupled* (based on the construction of that term discussed above).

171. Figure 3, shown below, illustrates in more detail imaging system 4 from Figure 2. EX1005, 4:30-32. The figure shows "Optics" 41 and "Imager &

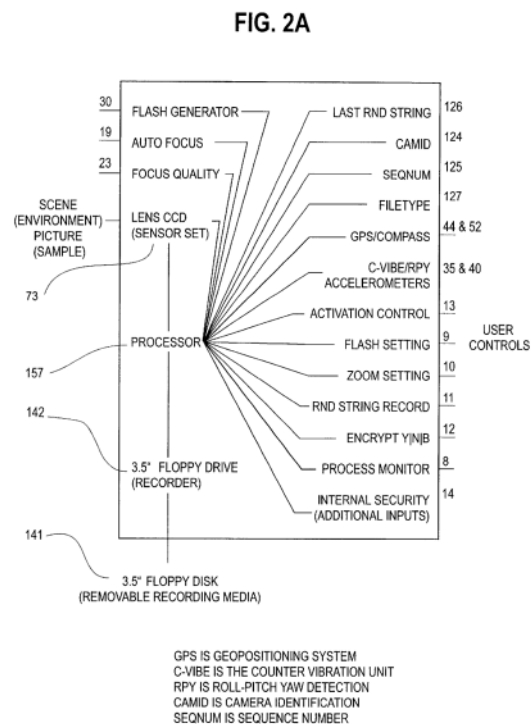
Digitizer” 42 (which includes a *sensor*) and “Frame Store” (which is or includes *memory*).



EX1005, Fig. 3 (highlighted). 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).

172. My opinion that Glass discloses *utilizing a sensor, which is tightly coupled to said memory* is further supported by the prosecution history of the '828 Patent. As discussed above, the applicants argued during prosecution that the cited prior art did not disclose “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” EX1002, 277. They then stated that “this claim feature is shown in Fig. 2A of the subject application, which illustrates a processor 157 which is ‘tightly coupled’ to a memory.” EX1002, 277.

173. Figure 2A, shown below, shows a Sensor Set that is connected through a Processor to a Recorder.



EX1001, Fig. 2A. Glass discloses the same arrangement with the same characteristics. Figures 2 and 3 in Glass show an imaging system that includes a *sensor* (i.e., optics and imager & digitizer) that is connected to *said memory* (i.e., frame store) as in Figure 2A of the '828 Patent. The similarity between this figure from the '828 Patent and Figures 2 and 3 in Glass further shows that Glass discloses a *sensor* that is *tightly coupled* to a *memory*.

174. Further, the applicants went on to explain that in Figure 2A, “[b]ecause 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” and that “[t]his means, for example, that there is no possibility for altering the image before the authentication information is generated.” EX1002, 277. They later explained that in the “present invention,” “the claimed ‘tight coupling’ requires that the connections between the sensor and the memory not be physically accessible to a user” and that “[i]f the sensors are, in fact, ‘remote’ from the processor, then it would be impossible to prevent physical access to the interconnections between the remote sensor and the local processor.” EX1002, 292. The applicants’ descriptions of *tightly coupled* components apply equally to the *memory* and *sensor* in Glass and therefore further confirm that Glass discloses a *sensor* that is *tightly coupled* to a *memory*.

175. For instance, Glass discloses connections between the *sensor* and *memory* where the connections (conductive traces or leads) are not accessible to the user. Figures 2 and 3 in Glass shows the optics/imager/digitizer and frame store connected to each other. Glass also explains that “data paths are shown in solid lines,” which indicates to a person of ordinary skill in the art that the optics/imager/digitizer and frame store are connected via conductive traces or leads. EX1005, 5:46-48. Figure 3 also shows the connected sensor, processor, and RAM within a “tamper resistant/responsive packaging,” and Glass explains that “[t]he tamper resistant package can be passive in that any opening to the device will cause its ultimate destruction” or that “the packaging could utilize at least one chassis intrusion detector or switch 51 shown in FIG. 3.” EX1005, 5:23-27. Thus, Glass discloses a *sensor* coupled to *memory* where the connection is not accessible to the user as asserted by the applicants during prosecution.

176. For all these reasons, Glass discloses *utilizing a sensor, which is tightly coupled to said memory*. In addition, as I will explain next, Glass discloses *utilizing a sensor...to generate at least one internal and unique parameter*.

177. For example, when the *sensor* obtains an image, the imaging system retrieves a “secret key” that is used by the code generator to create a “digital signature” for the image (i.e., *utilizing a sensor...to generate at least one...parameter*). EX1005, 5:49-6:4. In Glass, the “digital signature preferably is

a secure hash function which takes the following as inputs: each byte of image data in the frame; a ‘secret key’ which is stored and remains hidden inside the camera; and optionally a digital ‘token’....” EX1005, 5:67-6:4; *see also* 6:10-12 (“The camera ‘key’ can be a small block of data contained inside the camera....”). The “secret key” is therefore an *internal...parameter*.

178. The secret key is a “small block of data” maintained in the camera that “could be a unique identifier for the camera.” EX1005, 6:12-13. “Depending on the type of scheme used, the camera ‘key’ may simply be an arbitrary value assigned to every camera, an identifier for a batch of cameras, a unique camera identifier, a unique key for a symmetric signing algorithm, or a one half of a key-pair for an asymmetric signing algorithm.” EX1005, 6:13-18; *see also* 4:6-8 (“The secret key may be a serial number or other identification number that is unique to the camera or sensor that collects the biometric data.”). Thus, Glass explicitly describes the secret key as *unique* (i.e., a *unique parameter*).

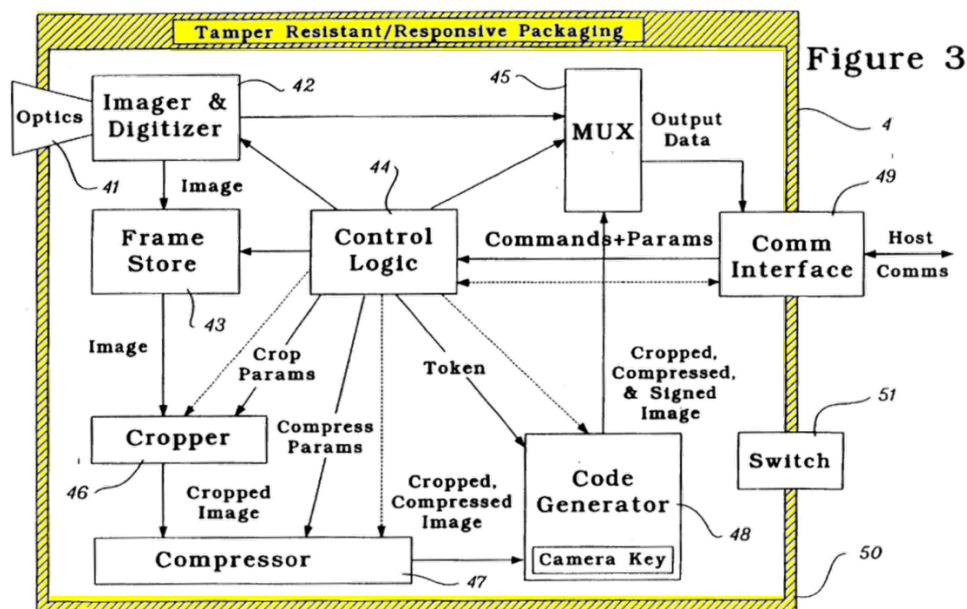
179. Glass also states that the “secret key” can be “a unique key for a symmetric signing algorithm.” EX1005, 6:16-17. A “secret key” of this type also constitutes an *internal and unique parameter*.

180. For these reasons, Glass discloses to a person of ordinary skill in the art *utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter* as recited in [1b].

- d) **[1c] 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;**

181. Glass discloses this limitation. In particular, Glass describes an imaging system, including the *sensor* and *memory*, “enclosed in a tamper-resistant package 50 which will be used to detect unwelcome intrusion and render the system useless.” EX1005, 5:13-41. Glass explains that “[t]he 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.” EX1005, 5:13-16.

182. Figure 3, shown below, illustrates tamper-resistant package 50 containing the components of the imaging system, including the *sensor* and *memory*. EX1005, 5:13-45.



EX1005, Fig. 3 (highlighted).

183. Glass states that “[t]he tamper resistant package can be passive in that any opening to the device will cause its ultimate destruction.” EX1005, 5:23-24. Glass also describes an alternative design in which “the packaging could utilize at least one chassis intrusion detector or switch 51” (in Figure 3 above), and “[s]witch 51 will signal the control logic 44...to return to a non-functioning state similar to that found during assembly.” EX1005, 5: 26-30. Glass explains that “[i]t is essential to ensure that the integrity of the acquired image and codes to be transmitted over the network have not been compromised.” EX1005, 5:16-19. Thus, Glass discloses *monitoring the integrity of the tight coupling between said memory and said sensor* (which means “determining whether physical access has

been gained to the coupling between said memory and said sensor” as discussed above).

184. Further, the Glass system monitors the *integrity of the tight coupling* between the *memory* and *sensor* at the point *when said at least one internal and unique parameter is generated* (i.e., when the imaging system utilizes the sensor to capture the image and retrieve the secret key hidden in the camera). Glass teaches that the intrusion detection is in effect at all times, from “after system software is loaded and enabled” until “intrusion is detected or the system software is reloaded using a special protocol.” EX1005, 5:42-45. Because this *monitoring* is in effect at all times, the *tight coupling* is monitored *when said at least one internal and unique parameter is generated*.

185. Glass also discloses that *if said integrity is compromised, then also providing an indication of said compromised integrity*. Glass states that if a chassis intrusion is detected, “[s]witch 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,” and that this state “will essentially delete key software routines related to generating biometric data” and “may also delete special battery backed up ram tables which include security or encryption information.” EX1005, 5:27-34. Thus, when *integrity is compromised*, the

imaging system is put in a “non-functioning state,” which *provid[es] an indication of said compromised integrity.*

186. For these reasons, Glass discloses *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* as recited in [1c].

- e) **[1d] 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;**

187. Glass discloses this limitation. In the summary of the invention, Glass states that after the image is “digitized into a biometric data file,” a “code is applied to that file.” EX1005, 3:51-53. “The code which is applied to the image for transfer is computed as a function of the image, the token and a secret key associated with the camera.” EX1005, 4:1-3. “Then the file with code is output to a network for transfer to an authentication server system.” EX1005, 3:53-54.

188. More specifically, Glass states that “[a] cryptographic technique is employed inside the code generator to create a digital signature for each frame of image data acquired by the camera and optics.” EX1005, 5:62-65. “The digital signature preferably is a secure hash function which takes the following as inputs: each byte of image data in the frame; a ‘secret key’ which is stored and remains

hidden inside the camera; and optionally a digital ‘token’....” EX1005, 5:67-6:3; *see also* 6:57-65. Thus, Glass discloses *utilizing a signature protocol* (secure hash function) *to generate a first signature* (digital signature) *based on said data stream* (image data) *and said at least one parameter* (secret key).

189. Glass provides an example (in the context of Figure 3) where a function with three inputs “DS(x, y, z), where x is the image data, y is a token, and z is the secret key, produces an output Q.” EX1005, 6:57-58. Then, “given x, and Q via some data exchange means and with knowledge of both original values y, z, as well as the hashing function DS(), a recipient can compute Q'=DS(x, y, z).” EX1005, 6:58-61. In this example, DS() is the *signature protocol*, and Q is the *first signature*, which takes x (the *data stream*), y, and z (the *internal and unique parameter*) as input. Because the *first signature* is generated based at least on the *data stream* and *at least one parameter* but potentially other input data as well (i.e., “based on” is open-ended as discussed above), it does not matter that Q also takes y as input.

190. Glass provides another example in Figure 8, which illustrates an “example operational transaction.” EX1005, 4:40-41. In this example, a camera is instructed by a client computer “to generate a secure image.” EX1005, 10:22-24. The camera “captures an image” and “uses a digital signature algorithm” (*signature protocol*), which takes the image (the *data stream*), the camera’s unique

private key (*said at least one parameter*), and a token “to provide a digital signature of the particular image.” EX1005, 10:24-28. This digital signature is another example of a *first signature* as in claim 1.

191. A person of ordinary skill in the art would have understood that applying a hash function would not alter the image data. Such a person would know and understand that hash functions, such as the MD5 hash function, do not modify their inputs; rather, they perform operations or computations based on those inputs while leaving the actual input unchanged. A person of ordinary skill in the art would recognize that generating Glass’s digital signature using a secure hash function, as described in Glass, does not involve altering the image data (*said first signature being generated without altering said data stream*).

192. In addition, Glass describes the *first signature* (digital signature) *being appended to said data file in said memory*. Glass states that “[t]here are a number of ways the digital signature computed by the camera can be sent back to the authenticating system” and that “[t]he most straightforward method is to append (or prepend) the signature to the data and send the complete package back to the authenticating system.” EX1005, 7:3-7; *see also* 9:37-40 (“Transmitted along with the image is the digital signature, either embedded directly into the image or alongside the image in the data package sent to the server.”), 11:47-49 (“codes prepended to the digital file and codes appended to the digital file”).

193. Glass also notes an alternate means of storing and transmitting the signature by using a “digital watermarking technique to embed signature information directly into the original image data.” EX1005, 7:7-10. This alternative technique would involve modifying the image data and is not part of my analysis of Glass.

f) [1e] utilizing said signature protocol to generate a second signature based on said data stream;

194. Glass discloses *utilizing said signature protocol* (a hash function) *to generate a second signature based on said data stream* (subsequent computation of the signature that is checked against the *first signature* generated in [1d]). In the summary of the invention, Glass teaches sending the file with code (*first signature*) “to an authentication server system.” EX1005, 3:53-54. After receiving the file with code, “[t]he authentication server system validates the data by recomputing the code from its knowledge of the input data needed to generate that code.” EX1005, 3:54-57.

195. More specifically, after computing the first signature as discussed in element [1d], Glass states that “[t]he digital signature of the data can be sent to another system (i.e. the authentication server) along with the original data; and the receiving system can, with the same or complementary token, compute a signature of the original data and check it against the signature sent with the data.” EX1005,

6:50-55. This “comput[ation] of the original data” that is checked “against the signature sent with the data” is the *second signature*.

196. As discussed above, Glass explains that if a function “DS(x, y, z), where x is the image data, y is a token, and z is the secret key, produces an output Q, then given x, and Q via some data exchange means and with knowledge of both original values y, z, as well as the hashing function DS(), a recipient can compute Q'=DS(x, y, z).” EX1005, 6:57-61. In this example, DS() is the *signature protocol*, Q is the *first signature*, and Q' is the *second signature*, which takes x (the *data stream*) as input. Because the *second signature* is generated based at least on the *data stream* but potentially other input data as well (i.e., “based on” is open-ended as discussed above), it does not matter that Q also takes y and z as input data.

197. I understand that the patent owner has asserted in the related district court litigation that “the ‘second signature’ is based on the said data stream and said at least one parameter.” EX1024, 4. Glass discloses the *second signature* under that proposed construction because the *second signature* (Q') is computed using a function (DS) with inputs including the *data stream*/image data (x) and *parameter*/secret key (y).

198. Glass provides another example illustrated in Figure 8. Continuing the discussion from [1d], after generating the digital signature, Glass’s camera

“outputs the secured image to the client.” EX1005, 10:28-29. “[A]long with the image is the digital signature and the camera’s unique serial number, either embedded directly into the image or alongside the image in the data package sent to the [authentication] server.” EX1005, 10:32-35. “Using module 15 the server checks that the image has not been tampered with by computing the same or complimentary digital signature algorithm on the data, using the token or complimentary token respectively, along with the camera’s public key provided by the Camera Certification Authority 30.” EX1005, 10:40-45. The server’s computation using the same digital signature algorithm on the data is *generat[ing] a second signature based on said data stream*.

199. Thus, in multiple ways, Glass discloses *utilizing said signature protocol to generate a second signature based on said data stream* as recited in [1e].

g) [1f] comparing said first signature to said second signature,

200. Glass discloses *comparing said first signature to said second signature*. In the summary of the invention, Glass states that the “authentication server system validates the data by recomputing the code from its knowledge of the input data needed to generate that code.” EX1005, 3:54-57. After re-computing the signature, as discussed in element [1e], Glass teaches to “check it against the signature sent with the data” (compare the *first signature* with the *second*

signature). EX1005, 6:50-55. “If the signatures match, the data can be assumed to not have been altered with an extremely high confidence level.” EX1005, 6:55-56.

201. Continuing with the discussion of Figure 3 in Glass discussed above, Glass teaches that “[i]f $Q=Q'$ then x, y, and z have not been altered, otherwise one or more of the data items have changed,” i.e., it teaches comparing Q, the *first signature*, and Q', the *second signature*. EX1005, 6:61-65.

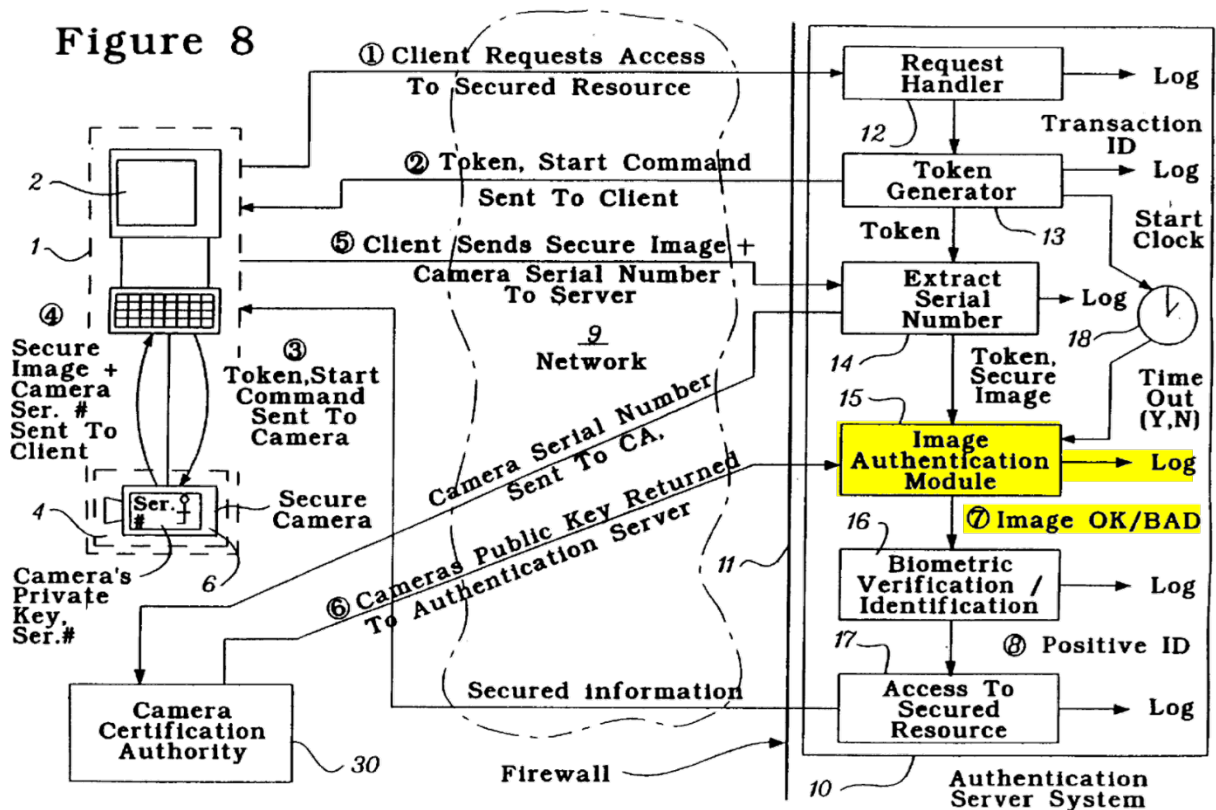
202. Glass provides another example, shown in Figure 8. Continuing the discussion from elements [1d] and [1e], Glass teaches that after “computing the same or complementary digital signature algorithm on the data,” “[t]he output of the algorithm is checked against the digital signature from the client,” i.e., the two signatures are compared. EX1005, 10:45-47.

h) [1g] 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

203. Glass discloses this limitation. As discussed for [1d]-[1f], Glass discloses that *if said first and second signatures are not the same, then...said stored data stream is not authentic. See, e.g.,* EX1005, 6:61-63 (“If $Q=Q'$ then x, y, and z have not been altered, otherwise one or more of the data items have changed.”).

204. Glass discloses *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic* when the signatures do not

match. In particular, Glass teaches maintaining a log that contains all transactions, including “each step” of a transaction. EX1005 9:56-60 (“A record of the transaction can be logged by the server system.... This data can provide irrefutable evidence of the transaction is required.”); 10:54-58 (same). Figure 8, shown below, illustrates that “Image Authentication Module” 15 determines whether the image is “OK” or “BAD” and writes an indication of this to the “Log.” EX1005, 9:61-62 (“We prefer to log each step of the transaction as indicated by the word Log.”).



EX1005, Fig. 8 (highlighted). Figure 7 illustrates another example “operational transaction” and also illustrates the system logging an indication that the image is “OK/BAD.” EX1005, 4:37-38, Fig. 7.

205. It would be immediately apparent to a person of ordinary skill in the art that “BAD” (in Figures 7 and 8) indicates that the image is not authentic (*said first and second signatures are not the same*). A person of ordinary skill in the art would also understand that “Log” files are intended to be viewed and read by users, and thus one primary reason for storing an indication of an unauthenticated image in a “Log” file would be to present a record of the error to a system administrator or other *user*. Glass further states that the log data “can provide irrefutable evidence of the transaction” (EX1005, 9:59-60, 10:57-58), which confirms that the log data (including any *error signal* such as “BAD”) is intended to be displayed to, and examined by, a *user*. Thus, Glass’s disclosure of storing an indication that an image is “BAD” in a log file constitutes *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic*.

206. Thus, Glass discloses that *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* as recited in [1g].

- i) **[1h] 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.**

207. Glass discloses this limitation. As discussed for [1d]-[1f], Glass discloses that *if said first and second signatures are the same, then...said stored data stream is authentic. See, e.g., EX1005, 6:61-63* (“If Q=Q’ then x, y, and z have not been altered, otherwise one or more of the data items have changed.”).

208. Glass also discloses *generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic* when the signatures match. As discussed for [1g], Glass teaches maintaining a log that contains all transactions, including “each step” of a transaction. EX1005 9:56-60 (“A record of the transaction can be logged by the server system.... This data can provide irrefutable evidence of the transaction if required.”); 10:54-58 (same). As discussed for [1g], both Figures 7 and 8 show that the “Image Authentication Module” 15 determines whether the image is “OK” or “BAD” and writes an indication of this to the “Log.” EX1005, 9:61-62 (“We prefer to log each step of the transaction as indicated by the word Log.”), Fig. 7-8.

209. It would be immediately apparent to a person of ordinary skill in the art that “OK” (in Figures 7 and 8) indicates that the image is authentic (*said first and second signatures are the same*). A person of ordinary skill in the art would also understand that “Log” files are intended to be viewed and read by users, and

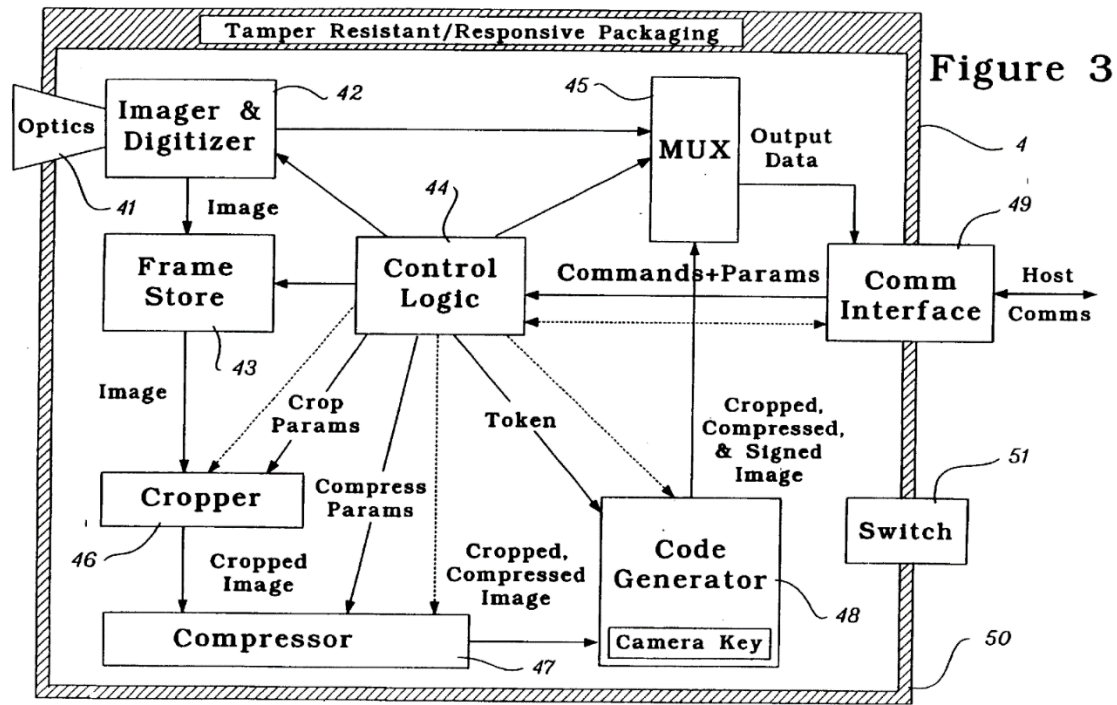
thus one primary reason for storing an indication of an unauthenticated image in a “Log” file would be to present a record of the error to a *user* such as a system administrator. Glass further states that the log data “can provide irrefutable evidence of the transaction” (EX1005, 9:59-60, 10:57-58), which confirms that the log data (including any *ok signal* such as “OK”) is intended to be displayed to, and examined by, a *user*. Thus, Glass’s disclosure of storing an indication that an image is “OK” in a log file constitutes *generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic*.

210. Thus, Glass discloses that *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* as recited in [1h].

2. Claim 2: The method of claim 1, wherein said memory form a part of a digital camera.

211. Glass discloses the method of claim 1 as I discussed above. In addition, Glass discloses that the *memory is part of a digital camera*. EX1005, Abstract (“A method and apparatus for collecting and securely transmitting biometric data over a network contains a sensor, preferably a camera, for collecting biometric data and code generating hardware and software. The camera data is digitized....”), 4:62-65 (“To secure the raw image data, additional electronic hardware and software are included in either the digital camera package or the image system.”).

212. In Glass, “[t]he camera’s tamper resistant/responsive packaging protects the secret key embedded inside.” EX1005, 3:25-26. Figure 3, shown below, illustrates the *memory* (i.e., Frame Store 43), housed in the tamper resistant packaging of Glass’s imaging system:



EX1005, Fig. 3.

213. Glass therefore discloses *memory* that is *part of a digital camera*.

3. Claim 3: The method of claim 1, wherein said at least one parameter comprises a random number.

214. Glass discloses the method of claim 1 as I discussed above. In addition, Glass discloses *said at least one parameter* (which is the *at least one internal and unique parameter* of claim 1) that is *a random number*. As discussed for [1b], Glass’s “secret key” constitutes *said at least one parameter* recited in

claim 1. Glass states that “the key could be a unique identifier for the camera” and “[d]epending on the type of scheme used...may simply be an arbitrary value....” EX1005, 6:12-14. A person of ordinary skill in the art would understand that using a random number would be a simple, straightforward, and effective way to provide “an arbitrary value assigned to every camera.” Indeed, Glass’s use of the term “arbitrary value” would suggest *a random number* to a person of ordinary skill in the art.

215. In addition, Glass states that the “secret key” can be “a unique key for a symmetric signing algorithm, or a one half of a key-pair for an asymmetric signing algorithm.” EX1005, 6:13-18. A person of ordinary skill in the art would understand that such a key ideally should be *a random number* as it would increase security by helping to prevent an attacker from simply guessing or reverse engineering the key value. EX1012, 17 (“Good keys are random-bit strings generated by some automatic process.”). For example, if an incremental numbering system—not a random number—was used to assign these “unique keys” during the time of manufacture, an attacker would be more likely to determine the unique key if he or she knew, for example, the manufacture date of the camera.

- 4. Claim 4: The method of claim 1, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.**

216. Glass discloses the method of claim 1 as I discussed above. In addition, Glass discloses the additional limitation of claim 4. In particular, Glass discloses that the “signed data package” (*said data file in said memory*) transmitted to the authentication server can contain “a time at which the biometric information was acquired” or “a location at which the biometric information was acquired.” EX1005, 12:66-13:3. By adding either time or location data to the “signed data package,” the Glass system *append[s] at least one additional parameter to said data file in said memory*. Further, both time and location information constitute an *additional parameter* that is *generally representative of a condition under which said data stream was generated*.

- 5. Claim 5: The method of claim 4, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.**

217. Glass discloses the additional limitation of claim 5. As discussed above for claim 4, Glass discloses that the “signed data package” (*said data file in said memory*) transmitted to the authentication server can contain “a location at which the biometric information was acquired.” EX1005, 12:65-13:3. A person of

ordinary skill in the art would know that by 2000, digital image metadata commonly included location information in the form of *GPS coordinates*.

EX1008, 64; EX1009, 62.

6. Claim 6: The method of claim 1 wherein said data stream is a digit sample of an environment.

218. A person of ordinary skill in the art would understand the reference in claim 6 to “digit sample” to be a typographical or clerical error, including in view of the prosecution history. EX1002, (application claim 14, which issued as claim 6, referred to “a digital sample of an environment”). A person of ordinary skill then, in light of the patent including its reference to digital cameras, would understand claim 6 to mean “wherein said data stream is a digital sample of an environment.”

219. Glass discloses a data stream that is a digital sample of an environment. In the summary of the invention, Glass “provide[s] a camera which functions as a sensor to collect the biometric data,” such as an image of the human eye, i.e., a *sample of an environment*. EX1005, 3:50-51; 1:17-22. “That data is digitized into a biometric data file.” EX1005, 3:51-52; *see also* Abstract (“The camera data is digitized and a unique code...is attached to the digital file.”). Figure 2 illustrates the image being captured by Glass’s system as an iris and refers to it as the “scene.” Thus, Glass discloses that *said data stream is a digit[al] sample of an environment*.

B. Rieger Renders the Challenged Claims Obvious

220. The '828 Patent and Rieger disclose purported inventions in the field of image processing and address the same problem of authenticating digital images. EX1006, 1 (Abstract); EX1001, Abstract.

221. Rieger provides a sufficiently detailed description to permit a person of ordinary skill in the art to implement the aspects of Rieger's manipulation-proof camera and associated integrity test discussed below in regard to the challenged claims with a reasonable expectation of success. It would have been within the skill level of a person of ordinary skill in the art to implement Rieger's manipulation-proof camera and associated integrity test based on the disclosure.

1. Independent Claim 1

- a) [1pre] A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:**

222. Rieger discloses a *method for authenticating a data stream* (digital image) *stored in a data file in memory*. Rieger “describes an approach to ensuring the integrity and authenticity of photographic images during the image-recording phase....” EX1006, 1. In particular, Rieger describes “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....” EX1006, 1. Rieger's approach involves “the use of a suitable digital signature, a method that is also used in other cases for the purpose of establishing the binding

legal character of a digital expression of intent, as an effective means of protecting digital images against manipulation.” EX1006, 1. The *data stream* being authenticated is *stored in a data file in memory* as explained below for limitation [1a].

b) [1a] storing a data stream in a data file in a memory;

223. Rieger discloses storing *a data stream in a data file in a memory*.

Rieger states that “[a]fter recording, the processor reads the image data from the CCD sensor and saves these to the RAM.” EX1006, 4.

224. The CCD (charge-couple device) sensor and RAM (random access memory) are shown in Figure 3, which illustrates Rieger’s manipulation-proof camera.

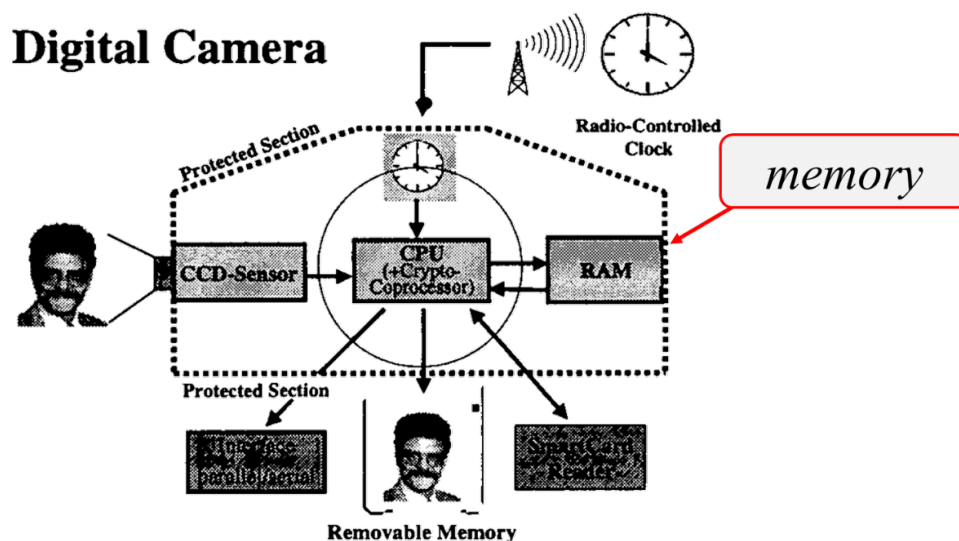


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

EX1006, Fig. 3 (annotated).

225. The image file data in RAM “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. A person of ordinary skill would understand the “JPEG format” to refer to applying JPEG compression and storing the image in standard JPEG file format (*.jpg) and would further understand from Rieger that the image is stored in a file in RAM before subsequently being saved to a removable memory medium or transmitted to an external computer.

226. Furthermore, a person of ordinary skill in the art would know that digital image data is almost always stored in a file in memory so that the image can be processed using standard image processing functions and tools.

c) [1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

227. Rieger discloses *utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter* as recited in claim 1.

228. Rieger discloses a *sensor* and a *memory*. Rieger explains that, “[i]n order to protect image data against manipulation from the moment they are received in the CCD sensor to generation of the signature, some of the system components, including the CCD sensor, the camera CPU (which also contains a

signature chip with the secret key), the RAM, the internal clock, a back-up power supply and the required connector cables must be integrated into a specially protected compartment in the camera housing.” EX1006, 4. The protected compartment is illustrated in Rieger’s Figure 3.

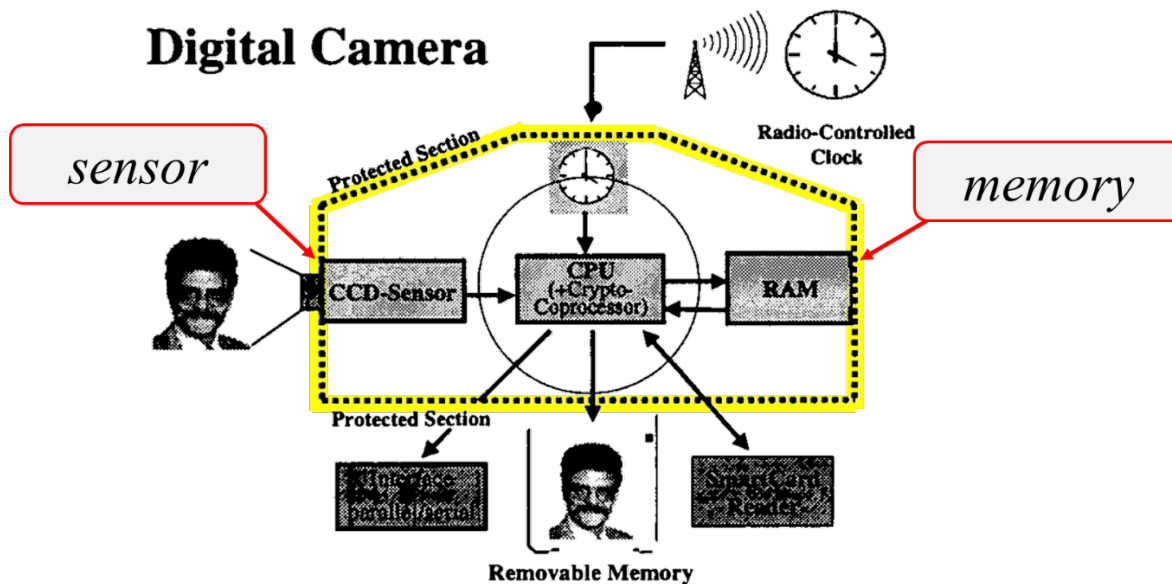


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

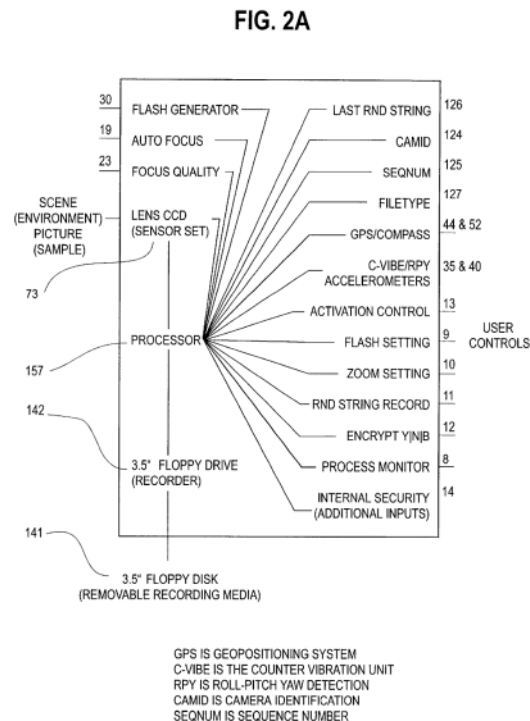
EX1006, Fig. 3 (annotated and highlighted). The arrows in Figure 3 illustrating a data path from the *sensor* to *memory* indicate that the components are electrically connected by conductive leads or traces within the protected section of Rieger’s manipulation-proof camera. Therefore, the *sensor* and *memory* are *tightly coupled* (based on the construction of that term discussed above).

229. My opinion that Rieger discloses *utilizing a sensor, which is tightly coupled to said memory* is further supported by the prosecution history of the ’828 Patent. As discussed above, the applicants argued during prosecution that the

cited prior art does not disclose “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” EX1002, 277.

They then stated that “this claim feature is shown in Fig. 2A of the subject application, which illustrates a processor 157 which is ‘tightly coupled’ to a memory.” EX1002, 277.

230. Figure 2A, shown below, shows a Sensor Set that is connected through a Processor to a Recorder:



EX1001, Fig. 2A. Rieger discloses the same arrangement with the same characteristics. Figure 3 in Rieger shows a protected section in the camera that includes a *sensor* (CCD-sensor) that is connected through a processor to *said memory* (RAM) in the same arrangement as in Figure 2A of the '828 Patent. The

similarity between this figure from the '828 Patent and Figure 3 in Rieger further shows that Rieger discloses a *sensor* that is *tightly coupled* to a *memory*.

231. Further, the applicants went on to explain that in Figure 2A, “[b]ecause 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” and that “[t]his means, for example, that there is no possibility for altering the image before the authentication information is generated.” EX1002, 277. They later explained that in the “present invention,” “the claimed ‘tight coupling’ requires that the connections between the sensor and the memory not be physically accessible to a user” and that “[i]f the sensors are, in fact, ‘remote’ from the processor, then it would be impossible to prevent physical access to the interconnections between the remote sensor and the local processor.” EX1002, 292. The applicants’ descriptions of *tightly coupled* components apply equally to the *memory* and *sensor* in Rieger and therefore further confirm that Rieger discloses a *sensor* that is *tightly coupled* to a *memory*.

232. For instance, Rieger discloses connections between the *sensor* and *memory* where the connections (conductive traces or leads) are not accessible to the user. Figure 3 shows the CCD-sensor, processor, and RAM connected to each other with “required connector cables.” EX1006, 4. A person of ordinary skill in

the art would understand that these connections would be made using conductive traces or leads, including to transmit information between those components.

233. Rieger explains that “[i]n order to protect image data against manipulation from the moment they are received in the CCD sensor to generation of the signature, some of the system components, including the CCD sensor, the camera CPU (which also contains a signature chip with the secret key), the RAM, the internal clock, a back-up power supply and the required connector cables must be integrated into a specially protected compartment in the camera housing.”

EX1006, 4. Rieger goes on to explain that “[t]he secure compartment can be protected, for example, by an electrical ‘protective shield’.” EX1006, 4. “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.” EX1006, 4. “This ensures that image data cannot be altered without detection prior to application of the signature.” EX1006, 4. Thus, Rieger discloses a sensor and memory where the connections are not accessible to the user, just as the applicants explained about their claimed invention.

234. For all these reasons, Rieger discloses *utilizing a sensor, which is tightly coupled to said memory*. In addition, as I will explain next, Rieger discloses *utilizing a sensor...to generate at least one internal and unique parameter*.

235. When Rieger’s manipulation-proof camera captures an image, multiple different parameters related to that image are collected. EX1006, 1 (“Features built into the camera make it relatively easy to record additional characteristic parameters of the image-production process.”), 3 (referring to “integrating supplementary information into the image file...relat[ing] specifically to the recording situation”). Thus, the camera is *utilizing a sensor...to generate...at least one...parameter*. According to the patent applicants, the *internal and unique parameter* need not be generated by the sensor itself. For instance, they argued during prosecution that [1b] is met when “the processor 157 generates a unique random string that is used for image authentication purposes.” EX1002, 277 (emphasis added).

236. The parameters collected by Rieger’s camera include several that constitute *at least one internal and unique parameter*.

237. Date and Time: Rieger describes recording “additional characteristic parameters of the image-production process” including “date and time.” EX1006, 1; *see also* 3 fn. 3 (referring to “supplementary information” including “date, time”). The date and time of an image is an *internal...parameter* because it can be provided or verified by a “reference clock” that “must be integrated into the ‘secure compartment’ of the camera.” EX1006, 5. Date and time provide a *unique*

parameter because no two digital images captured by the camera can have the exact same date and time.

238. My opinion that Rieger’s data and time parameters constitute the claimed *at least one internal and unique parameter* is supported by statements by the patent owner in the related litigation. I have reviewed a brief that I understand was filed on his behalf stating that the *internal and unique parameter[s]* of claim 1 “include elements such as...the date and time of the image....” EX1025, ¶39. I have reviewed similar assertions in other papers filed by the patent owner. EX1022, 15; EX1023, 11.

239. Global Coordinates: Rieger describes recording “additional characteristic parameters of the image-production process” including “global coordinates.” EX1006, 1; *see also* 3 fn. 3 (referring to “supplementary information” including “GPS coordinates for the recording location”). The global coordinates for an image constitute an *internal...parameter* because it can be provided by a “GPS receiver” in the manipulation-proof camera. EX1006, 5. The global coordinates are a *unique parameter* because images taken by different cameras will not be in precisely the same location.

240. My opinion that Rieger’s GPS parameters constitute the claimed *at least one internal and unique parameter* is supported by statements by the patent owner in the related litigation. I have reviewed a brief that I understand was filed

on his behalf stating that the *internal and unique parameter[s]* of claim 1 “include elements such as GPS (latitude and longitude). . . .” EX1025, ¶39 I have reviewed similar assertions in other papers filed by the patent owner. EX1022, 15; EX1023, 11.

241. Date/Time and Global Coordinates: Rieger states that, in addition to an internal clock, “[t]he addition of a GPS receiver makes it possible to record both the exact time and the precise location of the camera along with the image data.” EX1006, 5. Date, time, and global coordinates are all *internal...parameter[s]* as discussed immediately above. The combination provides a *unique parameter* because “the exact time and the precise location of the camera” will be different for every image taken by that camera or any other camera.

- d) **[1c] 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;**

242. Rieger discloses this limitation. As discussed above, Rieger describes a manipulation-proof camera including a “secure compartment” surrounding internal components including the *sensor* and *memory*. EX1006, 4, Fig. 3.

243. Rieger discloses *monitoring the integrity of the tight coupling between said memory and said sensor* (which means “determining whether physical access has been gained to the coupling between said memory and said sensor” as

discussed above). Rieger states that the “secure compartment can be protected, for example, by an electrical ‘protective shield’.” EX1006, 4. When the secure compartment “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.” EX1006, 4. According to Rieger, this mechanism “ensures that image data cannot be altered without detection prior to application of the signature.” EX1006, 4. By determining whether the secure compartment has been drilled or severed, the Rieger system “determin[es] whether physical access has been gained to the coupling between said memory and said sensor” (as this term is construed).

244. Rieger also discloses *monitoring the integrity of the tight coupling...when said at least one internal and unique parameter is generated* because the system is always monitoring the secure compartment to determine whether physical access has been gained to the connection between *memory* and *sensor*, including when camera parameters are generated. Indeed, Rieger states that the camera “provide[s] physical protection of the image during each stage of the image-production process, from origin in the image sensor to generation of the photographer’s signature” (i.e., at all times). EX1006, 4. Because Rieger’s *monitoring* is in effect at all times, the *tight coupling* is monitored *when said at least one internal and unique parameter is generated*.

245. Rieger also discloses that *if said integrity is compromised, then also providing an indication of said compromised integrity*. In Rieger, if the integrity of the secure compartment is compromised (i.e., if someone gains access to the connections between the internal components) then “a change in potential is triggered and detected by the processor, which then automatically deletes the secret key stored in the signature chip.” EX1006, 4. Thus, when the processor deletes the secret key in response to a change in potential, that is an *indication of said compromised integrity*.

- e) **[1d] 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;**

246. Rieger discloses this limitation. Rieger’s manipulation-proof camera generates a “digital signature” for each image so that the image can be subsequently authenticated. EX1006, 3. When an image is captured, the camera saves the image data to RAM and “the compressed image data are hashed by the camera processor.” EX1006, 4. The hash value is encoded using a secret key and then “linked together with the image data as the camera signature in the RAM.” EX1006, 4. The camera also captures various parameters related to the image including date, time, and location. EX1006, 5. “Before the entire package of image data is saved to the removeable camera memory medium, the data are

hashed once again by the camera processor....” EX1006, 5. This time, the input to the hash function includes the “image, camera signature, [and] camera parameters” (e.g., date, time, location). EX1006, 5. Rieger refers here to the “hash value (image, camera signature, camera parameters),” which a person of ordinary skill in the art would recognize to mean that the image, camera signature, and camera parameters are inputs to a hash function used to generate the hash value. This hash value is the claimed *first signature* and includes the hash of (i) the image; (ii) the image signature (which includes a hash of the image); and (iii) the camera parameters (including time, date, location, etc.). Thus, this hash value constituted the *first signature* and is generated *utilizing a signature protocol* (hash function) *based on said data stream* (image data) *and said at least one parameter* (e.g., date, time, location).

247. The *first signature* in Rieger is generated *without altering said data stream*. Rieger teaches using a hash function to generate a signature, as discussed above. A person of ordinary skill in the art would know and understand that hash functions do not modify their inputs; rather, they perform operations or computations based on those inputs, while leaving the actual input untouched. For example, Rieger discloses MD5 as a possible hash function. EX1006, 11. A person of ordinary skill in the art would know that MD5, when provided with a data stream as input, does not modify that data stream. A person of ordinary skill

in the art when presented with Rieger would further understand that there would be no reason or benefit to modifying the data stream itself; in fact, if the Rieger system modified the data stream as a result of, or during the process of, generating the signature, the integrity test disclosed by Rieger would fail when the two signatures were compared and the data stream would always be flagged as inauthentic. This is confirmed by Rieger itself, which notes that “[t]he characteristics of the check sum are such that any change in the original text (no matter how slight) will produce a totally different hash value.” EX1006, 11.

248. Rieger states that once the hash value (*first signature*) is encrypted, it “is returned to the RAM, where it is linked with the image data already recorded there.” EX1006, 5. The final package transferred off the camera includes signatures, parameters, and “the compressed image file.” EX1006, 5. Thus, the image data is transferred without alteration; indeed, that is a fundamental point of Rieger’s camera (i.e., preventing image alteration before signatures can be generated). EX1006, 4 (the camera’s secure compartment “protect[s] image data against manipulation from the moment they are received in the CCD sensor to generation of the signature”).

249. Rieger also discloses *append[ing]* the signature *to said data file in said memory*. Indeed, Rieger states that the hash value based on the image, camera signature, and camera parameters (*first signature*) is encrypted and “is returned to

the RAM, where it is linked with the image data already recorded there” (i.e., *appended to said data file in said memory*). EX1006, 5.

250. In addition, Rieger includes an Appendix discussing various relevant topics including a section entitled “The Digital Signature.” EX1006, 11. In that section, Rieger discusses hash functions such as the claimed *signature protocol*. EX1006, 11. Rieger explains a hash function as follows:

Following a predefined process, it generates a check sum (hash total, also hash value, the document ‘fingerprint’) from a plaintext passage of any length. The characteristics of the check sum are such that any change in the original text (no matter how slight) will produce a totally different hash value.

EX1006, 11. This description further suggests and teaches *utilizing a signature protocol* (hash function) *to generate a first signature..., said first signature being generated without altering said data stream*.

251. In addition, Rieger states that the hash value is stored “either separately or together with the text (in which case it is given special security protection).” EX1006, 11. Rieger’s reference to storing the hash value “together with the text” further suggests and teaches *utilizing a signature protocol* (hash function) *to generate a first signature..., said first signature...being appended to said data file in said memory* (image data in RAM).

f) [1e] utilizing said signature protocol to generate a second signature based on said data stream;

252. Rieger discloses *utilizing said signature protocol to generate a second signature based on said data stream*. Rieger explains that “[b]ecause every alteration of image data, regardless of how minor (one bit is enough!), produces a totally different result in the computed check sum (hash total), an integrity test^[fn] will immediately detect any alteration of the data.” EX1006, 6. In a footnote, Rieger states that the “integrity test” is described in Appendix. *Id.*, 6 fn.11.

253. In the Appendix, Rieger describes the integrity test (in a section entitled “Integrity Test”).

Generally speaking, hash functions are used to verify the integrity of texts (or data). The hash value is computed for a given text for this purpose. The hash value is then stored, either separately or together with the text (in which case it is given special security protection). If subsequent recomputation of the hash value for what is presumed to be the identical text produces a different hash value, the text is presumed to have been falsified. Conversely, identical hash values confirm the identity of the data tested and thus the integrity of the text.

EX1006, 11-12. The “subsequent recomputation” referred to here by Rieger is the *second signature*. A person of ordinary skill in the art would understand that Rieger’s instruction to perform a “subsequent recomputation” of the hash value would mean using the same inputs as the first computation of a hash value, i.e., the

image, camera signature, and camera parameters as disclosed by Rieger, and thus this *second signature* would be based on the image (*said data stream*).

g) [1f] comparing said first signature to said second signature,

254. Rieger discloses this limitation. As discussed for [1d] and [1e], Rieger's manipulation-proof camera employs a hash function to generate a *first signature* based on the image data, camera signature, and camera parameters (e.g., date, time, location). EX1006, 5. Rieger also explains that "[b]ecause every alteration of image data...produces a totally different result in the computed check sum (hash total), an integrity test^[fn] will immediately detect any alteration of the data." EX1006, 6. In Rieger's integrity test, "[i]f subsequent recomputation of the hash value for what is presumed to be the identical text produces a different hash value, the text is presumed to have been falsified." EX1006, 11-12. Using this integrity test, "any user can compute the hash value himself and determine, through comparison, whether the value transmitted by the sender is identical with his own result" (i.e., whether "the text is presumed falsified"). A person of ordinary skill in the art would understand from Rieger that the image data is verified by comparing the computed hash value generated on the camera (*first signature*) to a "subsequent recomputation of the hash value" (*second signature*). Thus, Rieger discloses *comparing said first signature to said second signature*.

- h) [1g] 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**

255. Rieger discloses this limitation. Rieger states that “every alteration of image data, regardless of how minor...produces a totally different result in the computed check sum (hash total)” and further that “[i]f subsequent recomputation of the hash value for what is presumed to be the identical text produces a different hash value, the text is presumed to have been falsified.” EX1006, 6, 11-12. Thus, Rieger’s integrity test shows that *if said first and second signatures are not the same, then said stored data stream is not authentic.*

256. Rieger also suggests and teaches *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic.*

Rieger’s Figure 7, shown below, illustrates principles of the integrity and a related authenticity test that is also described by Rieger.

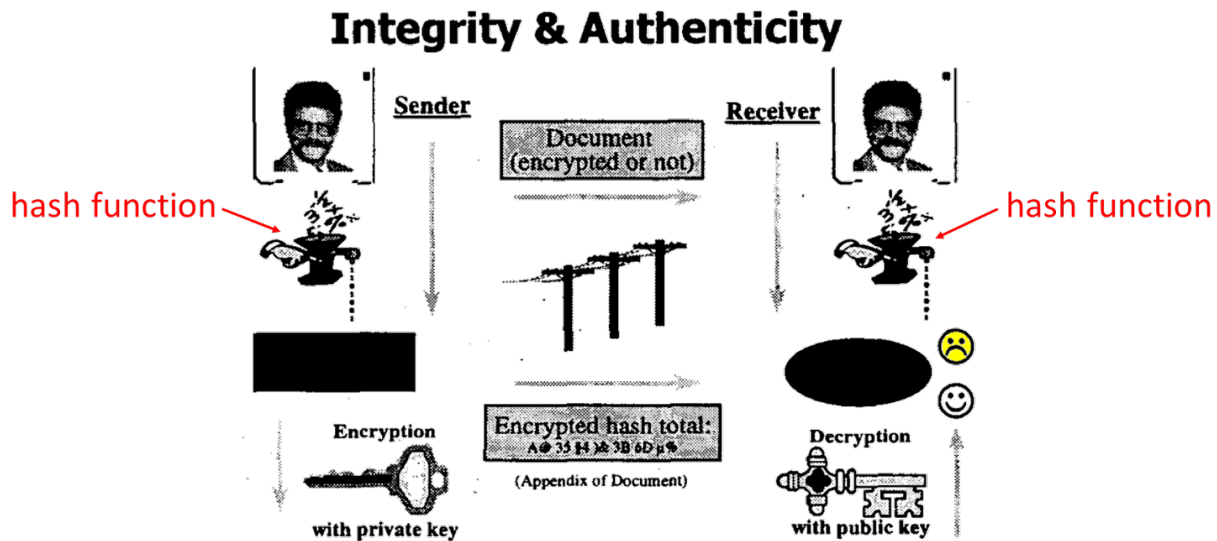


Figure 7: Principles of the integrity and authenticity test

EX1006, Fig. 7 (annotated and highlighted).

257. In the figure, on the left side, a “Sender” is shown (i) computing the hash total for a document using a hash function, and (ii) sending both the document and the hash total to a “Receiver.” On the right side, the figure illustrates a “Receiver” using the same hash function to recompute the hash total based on the document as it was received. If the transmitted hash total and the recomputed hash total are different, the document has been falsified as indicated by the frowning face image (highlighted in the image above). 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 not use if it did not provide such an indication to the *user* when an image is not authentic.

- i) **[1h] 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.**

258. Rieger discloses this limitation. Rieger states that “every alteration of image data, regardless of how minor...produces a totally different result in the computed check sum (hash total)” and further that “identical hash values confirm the identity of the data tested and thus the integrity of the text.” EX1006, 6, 12; *see also* 12 (“any user can compute the hash value himself on the basis of the original plan text and determine, through comparison, whether the value transmitted by the sender is identical with his own result”). Thus, Rieger’s integrity test shows that *if said first and second signatures are the same, then said stored data stream is authentic.*

259. Rieger also suggests and teaches *generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.* As discussed for [1g], Figure 7 shows how a “Receiver” utilizing Rieger’s integrity test can compare the hash total received from a “Sender” with the recomputed hash total to validate the received document.

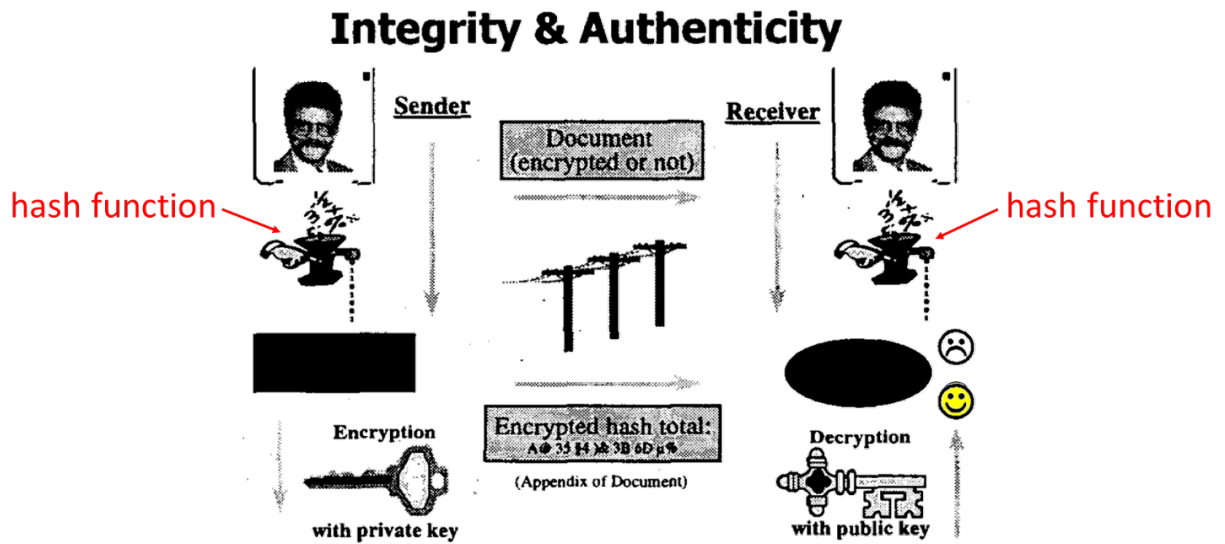


Figure 7: Principles of the integrity and authenticity test

EX1006, Fig. 7 (annotated and highlighted).

260. As illustrated in Figure 7, if the transmitted hash total and the recomputed hash total are identical, the integrity of the document is verified as indicated by the smiling face image (highlighted above). 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.

2. Claim 2: The method of claim 1, wherein said memory form a part of a digital camera.

261. Rieger discloses the method of claim 1 as I discussed above. In addition, Rieger discloses that *said memory form[s] part of a digital camera*. For example, Rieger's "Figure 3 shows the basic conceptual diagram for a digital camera...." EX1006, 4; *see also* 1 ("Reflections regarding the basis configuration of a manipulation-proof digital camera...will be discussed.").

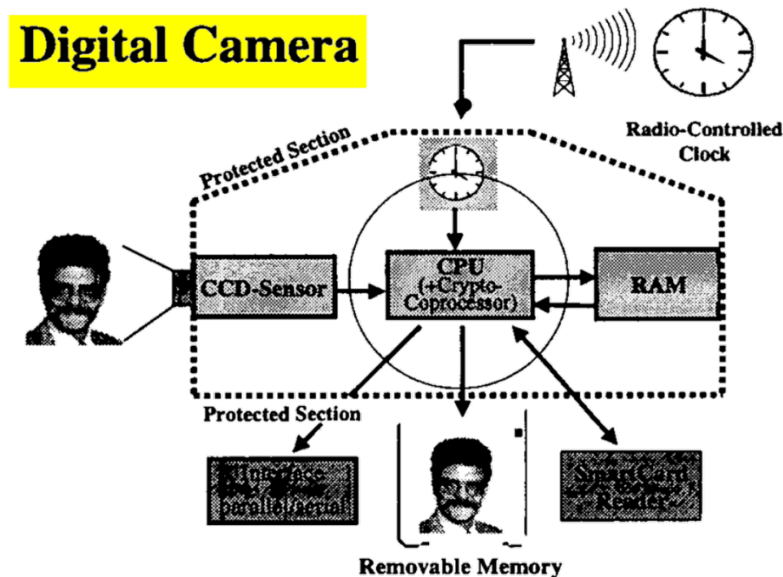


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

EX1006, Fig. 3 (highlighted). As shown in the figure, the *digital camera* includes RAM, which is the claimed *memory*.

3. Claim 3: The method of claim 1, wherein said at least one parameter comprises a random number.

262. Rieger discloses the method of claim 1 as I discussed above. In addition, Rieger discloses that the *at least one parameter* can include a *random*

number. Rieger state that the “hash value (image, camera signature, camera parameters)” is encrypted using a “secret key.” EX1006, 5. As I explained above in paragraph 215, a person of ordinary skill in the art would know that using an encryption key based on *a random number* would enhance security. EX1012, 17. Indeed, Rieger discusses generating a key using “a random generator” (EX1006, 10) and further discloses that the “camera processor [is] equipped with a random-number generator” EX1006, 4).

4. Claim 4: The method of claim 1, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.

263. Rieger discloses the additional limitations of claim 4. For instance, Rieger states that “[t]he evidentiary value of digital images for court-related purposes must be enhanced by integrating supplementary information into the image file.” EX1006, 3. The “supplementary information” integrated “into the image file” constitutes *appending at least one additional parameter to said data file in said memory*.

264. Rieger further states that the supplemental information “should relate specifically to the recording situation, provide reliable identification of the photographer^[fn] and the camera^[fn] and include other relevant data^[fn] as well.” EX1006, 3. In the related footnotes, Rieger indicates that this type of supplemental

information can include “a CPU serial number” and “date, time and GPS coordinates for the recording location.” EX1006, 3, fn. 2-3. Supplementary information relating “specifically to the recording situation” constitutes *at least one additional parameter being generally representative of a condition under which said data stream was generated.*

265. In addition, Rieger states that “[i]n principle, all camera parameters, including focus values, aperture settings and exposure times, can be recorded and signed” and that “[t]his also applies to physical data on environmental conditions (e.g., temperature, humidity, etc.).” EX1006, 5. These “recorded camera parameters” can be transferred off Rieger’s camera using removeable memory along with the “compressed image file.” EX1006, 5. This discussion by Rieger of “recorded camera parameters” further discloses *appending at least one additional parameter to said data file in said memory where the at least one additional parameter is generally representative of a condition under which said data stream was generated.*

- 5. Claim 5: The method of claim 4, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.**

266. Rieger discloses the additional limitations of claim 5. As I discussed for claim 4, Rieger states that “supplemental information” (*at least one additional*

parameter) “should...provide reliable identification of ...the camera and include other relevant data as well.” EX1006, 3. An *additional parameter* that “provide[s] reliable identification of...the camera” constitutes a *CamID* (i.e., a camera identifier) as recited in claim 5 and as that term is used in the ’828 Patent. EX1001, 6:60-61, Fig. 2A.

267. The “other relevant data” can include “GPS coordinates for the recording location.” EX1006, 3 fn. 3. Such an *additional parameter* would constitute *GPS coordinates* as recited in claim 5.

268. Further, Rieger describes recording “aperture settings” (EX1006, 5), which a person of ordinary skill in the art would know constitute *zoom settings* as recited in claim 5.

269. Any one of these parameters constitutes *at least one additional parameter...selected from [the] group* of parameters recited in claim 5.

6. Claim 6: The method of claim 1 wherein said data stream is a digit sample of an environment.

270. A person of ordinary skill in the art would understand that claim 6 requires that the “data stream is a digit[al] sample of an environment” as I explained above in paragraph 218.

271. Rieger discloses that the *data stream is a digit[al] sample of an environment*. For example, Figure 3 illustrates the manipulation-proof digital camera taking a picture of a person’s face. EX1006, Fig. 3. Because the person is

part of the environment around the camera, the figure shows that the *data stream* (image of the person) *is a digit[al] sample of an environment*.

C. Exif 2.0 or Exif 2.1 Disclose Digital Camera “Parameters” Available for the Glass and Rieger Inventions

1. Motivation to Combine

272. Both Glass and Rieger describe inventions incorporating digital cameras. EX1005, Abstract, 4:62-65, Figs. 2-3; EX1006, 1, 4, Fig. 3. By 2000, the JPEG image compression and Exif metadata standards had been widely adopted and would have been a natural approach for a person of ordinary skill in the art implementing Glass’s system or Rieger’s manipulation-proof camera. Indeed, Rieger explicitly refers to “camera parameters,” which a person of ordinary skill in the art would have recognized as a reference to Exif metadata. EX1006, 5. Such a person would have been well-aware of the Exif standard and the metadata tags specified by that standard for inclusion with compressed JPEG image data. The ’828 Patent itself describes an embodiment storing image data and parameters in files “in a format generally accepted by the industry” and “in compliance with the standards for the format.” EX1001, 7:62-67. By 2000, the generally accepted industry standard for digital cameras was the Exif/JPEG image format.

273. A person of ordinary skill in the art would have been motivated to implement the Glass system or the Rieger camera in compliance with the Exif/JPEG image standards. It would have allowed an implementer to use widely

available (i.e., off-the-shelf) image processing algorithms and tools designed for such files. Further, a person of ordinary skill in the art would have been able to implement Glass's system or Rieger's camera with image files containing Exif metadata with a reasonable expectation of success because the Exif standard was well-known and commonly used in digital cameras by 2000. Such an implementation would have been well within the skill level of a person of ordinary skill in the art by that time.

2. Claim 1

274. As discussed above, Glass and Rieger each disclose the limitations of claim 1, including the *at least one internal and unique parameter* identified in [1b]. The Exif 2.0 and Exif 2.1 standard documents provide more detail about the specific metadata fields available for digital cameras by 2000. Thus, the combination of Glass with Exif 2.0/2.1 or Rieger with Exif 2.0/2.1 discloses all limitations, specifically including the *parameter* limitations, of claim 1.

3. Claim 2

275. Glass and Rieger each disclose the additional limitation of claim 2 whether or not combined with Exif 2.0/Exif 2.1.

4. Claim 3

276. Glass and Rieger each disclose the additional limitation of claim 3 whether or not combined with Exif 2.0/Exif 2.1.

5. Claim 4

277. Claim 4 recites the additional *step of appending at least one additional parameter to said data file* where the *at least one additional parameter is generally representative of a condition under which said data stream was generated*. Both Exif 2.0 and Exif 2.1 disclose this additional limitation as I will explain.

278. The Exif standard documents describe a file format including Exif tags (or metadata fields) in the same file with compressed JPEG image data. For instance, Figure 6 in Exif 2.0 and Exif 2.1 illustrates the basic structure of JPEG compressed data including Exif attribute information (i.e., Exif tags). EX1008, 23; EX1009, 20.

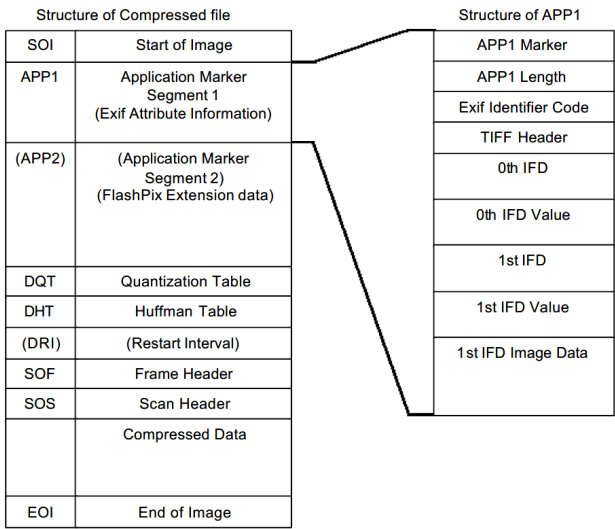


Fig. 6 Basic Structure of Compressed Data Files

EX1009, Fig. 6; *see also* EX1008, Fig. 6. Thus, Exif 2.0 and Exif 2.1 disclose *the step of appending at least one additional parameter (Exif tags) to said data file in said memory (JPEG image file).*

279. Both Exif 2.0 and Exif 2.1 also disclose *at least one additional parameter that is generally representative of a condition under which said data stream was generated.* Indeed, Exif 2.0 and Exif 2.1 each include a table-full of such parameters referred to as “Tags Relating to Picture-Taking Conditions.”

EX1008, 43 (Table 5); EX1009, 41 (Table 5).

Table 5 Exif IFD Attribute Information (2)

G. Tags Relating to Picture-Taking Conditions					
Exposure time	ExposureTime	33434	829A	RATIONAL	1
F number	FNumber	33437	829D	RATIONAL	1
Exposure program	ExposureProgram	34850	8822	SHORT	1
Spectral sensitivity	SpectralSensitivity	34852	8824	ASCII	Any
ISO speed rating	ISOSpeedRatings	34855	8827	SHORT	Any
Optoelectric conversion factor	OECF	34856	8828	UNDEFINED	Any
Shutter speed	ShutterSpeedValue	37377	9201	SRATIONAL	1
Aperture	ApertureValue	37378	9202	RATIONAL	1
Brightness	BrightnessValue	37379	9203	SRATIONAL	1
Exposure bias	ExposureBiasValue	37380	9204	SRATIONAL	1
Maximum lens aperture	MaxApertureValue	37381	9205	RATIONAL	1
Subject distance	SubjectDistance	37382	9206	RATIONAL	1
Metering mode	MeteringMode	37383	9207	SHORT	1
Light source	LightSource	37384	9208	SHORT	1
Flash	Flash	37385	9209	SHORT	1
Lens focal length	FocalLength	37386	920A	RATIONAL	1
Flash energy	FlashEnergy	41483	A20B	RATIONAL	1
Spatial frequency response	SpatialFrequencyResponse	41484	A20C	UNDEFINED	Any
Focal plane X resolution	FocalPlaneXResolution	41486	A20E	RATIONAL	1
Focal plane Y resolution	FocalPlaneYResolution	41487	A20F	RATIONAL	1
Focal plane resolution unit	FocalPlaneResolutionUnit	41488	A210	SHORT	1
Subject location	SubjectLocation	41492	A214	SHORT	2
Exposure index	ExposureIndex	41493	A215	RATIONAL	1
Sensing method	SensingMethod	41495	A217	SHORT	1
File source	FileSource	41728	A300	UNDEFINED	1
Scene type	SceneType	41729	A301	UNDEFINED	1
CFA pattern	CFAPattern	41730	A302	UNDEFINED	Any

EX1009, 41 (highlighted); *see also* EX1008, 43. These include tags for the exposure time, shutter speed, light source, scene type, and many others relating to the picture-taking conditions. A person of ordinary skill in the art would have

recognized these as parameters *generally representative of a condition under which said data stream was generated*. Thus, the combination of Exif 2.0 or Exif 2.1 with Glass or Rieger discloses claim 4 of the '828 Patent.

6. Claim 5

280. Exif 2.0 and Exif 2.1 disclose *at least one additional parameter* identified in the list of parameters recited in claim 5. Indeed, Exif 2.0 and Exif 2.1 recite several of the listed parameters (*zoom settings, flash status, GPS coordinates, and compass headings*), any one of which constitutes *at least one additional parameter* as recited in claim 5. Thus, the combination of Exif 2.0 or Exif 2.1 with Glass or Rieger discloses claim 5 of the '828 Patent.

281. Zoom settings: One of the tags disclosed in Table 5 of Exif 2.0 and Exif 2.1 is called “Lens focal length” (or “FocalLength”). EX1008, 43; EX1009, 41. The FocalLength field provides “[t]he actual focal length of the lens, in mm.” EX1008, 57; EX1009, 55. A person of ordinary skill in the art would recognize that the Exif lens focal length tag is a parameter providing *zoom settings*.

282. Flash status: Another tag disclosed in Table 5 of Exif 2.0 and Exif 2.1 is called “Flash.” EX1008, 43; EX1009, 41. This “tag is recorded when an image is taken using a strobe light (flash)” and indicates whether “Flash fired” or “Flash did not fire.” EX1008, 56; EX1009, 54. A person of ordinary skill in the art

would recognize that the Exif flash tag is a parameter included in the JPEG file indicating *flash status*.

283. GPS coordinates: The Exif standard documents include Table 12 entitled “GPS Attribute Information” identifying a number of tags relating to GPS. EX1008, 64; EX1009, 62.

Table 12 GPS Attribute Information

Tag Name	Field Name	Tag ID		Type	Count
		Dec	Hex		
A. Tags Relating to GPS					
GPS tag version	GPSTagVersionID	0	0	BYTE	4
North or South Latitude	GPSLatitudeRef	1	1	ASCII	2
Latitude	GPSLatitude	2	2	RATIONAL	3
East or West Longitude	GPSLongitudeRef	3	3	ASCII	2
Longitude	GPSLongitude	4	4	RATIONAL	3
Altitude reference	GPSAltitudeRef	5	5	BYTE	1
Altitude	GPSAltitude	6	6	RATIONAL	1
GPS time (atomic clock)	GPSTimeStamp	7	7	RATIONAL	3
GPS satellites used for measurement	GPSSatellites	8	8	ASCII	Any
GPS receiver status	GPSStatus	9	9	ASCII	2
GPS measurement mode	GPSMeasureMode	10	A	ASCII	2
Measurement precision	GPSDOP	11	B	RATIONAL	1
Speed unit	GPSSpeedRef	12	C	ASCII	2
Speed of GPS receiver	GPSSpeed	13	D	RATIONAL	1
Reference for direction of movement	GPSTrackRef	14	E	ASCII	2
Direction of movement	GPSTrack	15	F	RATIONAL	1
Reference for direction of image	GPSImgDirectionRef	16	10	ASCII	2
Direction of image	GPSImgDirection	17	11	RATIONAL	1
Geodetic survey data used	GPSMapDatum	18	12	ASCII	Any
Reference for latitude of destination	GPSDestLatitudeRef	19	13	ASCII	2
Latitude of destination	GPSDestLatitude	20	14	RATIONAL	3
Reference for longitude of destination	GPSDestLongitudeRef	21	15	ASCII	2
Longitude of destination	GPSDestLongitude	22	16	RATIONAL	3
Reference for bearing of destination	GPSDestBearingRef	23	17	ASCII	2
Bearing of destination	GPSDestBearing	24	18	RATIONAL	1
Reference for distance to destination	GPSDestDistanceRef	25	19	ASCII	2
Distance to destination	GPSDestDistance	26	1A	RATIONAL	1

EX1009, 62; *see also* EX1008, 64. The Exif tags in these tables include “Latitude” and “Longitude.” EX1008, 65-66 (describing “GPSLatitude” and “GPSLongitude”); EX1009, 63-64 (same). Other Exif tags indicate “whether the latitude is north or south latitude” and “whether the longitude is east or west longitude.” EX1008, 65-66; EX1009, 63-64. A person of ordinary skill in the art would recognize that at least the Exif tags for latitude and longitude are parameters indicating the *GPS coordinates* of the image.

284. Compass heading: Table 12 also lists a tag for “Direction of image” (“GPSImgDirection”). EX1008, 64; EX1009, 62. This tag “[i]ndicates the direction of the image when it was captured” and can have a range of values “from 0.00 to 359.99.” EX1008, 69; EX1009, 67. Another field (GPSImgDirectionRef) provides “the reference for giving the direction of the image when it is captured” where “T” indicates the “true direction” and “M” indicates “magnetic direction.” EX1008, 69; EX1009, 67. A person of ordinary skill in the art would recognize that GPSImgDirection is a parameter providing the *compass heading* for the image.

D. Serret-Avila Discloses Displaying an “Error” or “OK” Signal to the User

285. As I explained above, Glass (either alone or with Exif 2.0/2.1) and Rieger (either alone or with Exif 2.0/2.1) disclose every limitation of claim 1. To the extent that the patent owner may argue that Glass or Rieger does not disclose the limitations of claim 1 requiring either *generating an error signal that is displayed to a user* or *generating an ok signal that is displayed to a user* (EX1001, 21:11-18), such functionality is disclosed by Serret-Avila. Thus, the combination of Glass and Serret-Avila or Rieger and Serret-Avila discloses these limitations of the challenged claims.

1. Motivation to Combine Glass and Serret-Avila

286. The '828 Patent, Glass, and Serret-Avila all disclose inventions in the field of image processing and address the same problem of authenticating images and other data streams. EX1001, Abstract, 1:7-12, 1:15-38, 1:52-61; EX1005, Abstract, 1:7-23, 1:34-37, 2:23-26, 2:32-35, 2:58-61, 3:50-57; EX1011, Abstract, 1:32-35, 1:51-55, 2:66-3:3, 3:7-9. A person of ordinary skill in the art would have naturally considered prior art references such as Glass and Serret-Avila.

287. 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.

288. 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.

2. Motivation to Combine Rieger and Serret-Avila

289. The '828 Patent, Rieger, and Serret-Avila all disclose inventions in the field of image processing and address the same problem of authenticating images and other data streams. EX1001, Abstract, 1:7-12, 1:15-38, 1:52-61; EX1006, 1 (Abstract); EX1011, Abstract, 1:32-35, 1:51-55, 2:66-3:3, 3:7-9. A person of ordinary skill in the art would have naturally considered prior art references such as Rieger and Serret-Avila.

290. 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.

291. 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.

3. Serret-Avila Discloses Limitations [1f], [1g], and [1h]

292. Serret-Avila discloses *generating an error signal that is displayed to a user* or *generating an ok signal that is displayed to a user* as recited in limitations [1f], [1g], and [1h]. As in [1f], Serret-Avila discloses *comparing* a sub-block’s received hash value (*first signature*) to the calculated hash value, which Serret-Avila also refers to as the “check value” (*second signature*). EX1011, 10:24-27.

Figure 5 is a flow-chart that illustrates this comparison. EX1011, 5:39-40, 9:66-10:1.

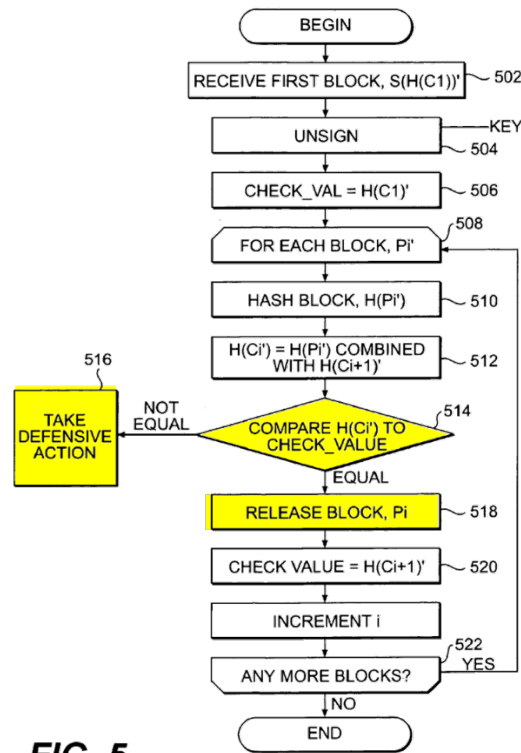


FIG. 5

EX1011, Fig. 5 (highlighted).

293. Serret-Avila explains that if the hash values are not equal, the sub-block “is judged to be unauthentic” and the system can take “defensive action” by, for example, “display[ing] a warning or error message” or “simply record[ing] the occurrence of this condition for later reporting or action.” EX1011, 10:33-45. In either case, Serret-Avila discloses *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic* as recited in [1g]. Alternatively, if the hash values are equal, the sub-block is “deemed to be

and suggests to a person of ordinary skill in the art *generating an [error/ok] signal that is displayed to a user* as recited in [1f], [1g], and [1h].

VII. SECONDARY CONSIDERATIONS

295. While I have considered the impact of secondary considerations of obviousness, I am not aware of any relevant information related to secondary considerations of obviousness that would impact my opinions at this time. To the extent the patent owner may present any such information, I will consider it.

VIII. AVAILABILITY FOR CROSS-EXAMINATION

296. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during a time as mutually agreed between the parties.

IX. RIGHT TO SUPPLEMENT

297. I reserve the right to supplement my opinions in the future to respond to any arguments that the patent owner raises. This declaration represents only those opinions that I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information that becomes available to me and on my continuing analysis of the materials already provided.

X. CONCLUSION

298. For the reasons discussed in this declaration, it is my opinion that the challenged claims of the '828 Patent are unpatentable in view of the prior art I have discussed above.

Acknowledgement of Oath

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1101 of Title 18 of the United States Code.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "Zixiang Xiong".

Zixiang Xiong, Ph.D.

Dated: August 27, 2024