

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ADOBE INC.
Petitioner

v.

JONATHAN E. JAFFE
Patent Owner

Case IPR2024-01352
Patent No. 6,757,828

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

List of Exhibits.....	viii
Mandatory Notices Under 37 C.F.R. § 42.8	x
Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))	x
Related Matters (37 C.F.R. § 42.8(b)(2))	x
Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3))	x
Service Information (37 C.F.R. § 42.8(b)(4)).....	x
I. Introduction.....	1
II. Grounds for Standing.....	2
III. The Challenged Patent.....	2
A. Patent Specification.....	2
B. Prosecution History	5
C. Patent Claims.....	7
D. Person of Ordinary Skill in the Art	8
IV. Claim Construction.....	9
A. “a sensor, which is tightly coupled to said memory”.....	9
B. “monitoring the integrity of the tight coupling between said memory and said sensor”	10
C. “based on”	11
V. Prior Art References	14
A. Glass (EX1005)	14
B. Rieger (EX1006)	16
C. Exif 2.0 (EX1008).....	19

D.	Exif 2.1 (EX1009)	20
E.	Serret-Avila (EX1011)	21
VI.	Grounds of Unpatentability	22
A.	Ground 1: Glass Renders the Challenged Claims Obvious	22
1.	Claim 1	23
a.	[1pre] A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:	23
b.	[1a] storing a data stream in a data file in a memory;	24
c.	[1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;	26
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;	30
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;	32
f.	[1e] utilizing said signature protocol to generate a second signature based on said data stream;	34
g.	[1f] comparing said first signature to said second signature;	35
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	36
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.	38
2.	Claim 2: The method of claim 1, wherein said memory form a part of a digital camera.....	38
3.	Claim 3: The method of claim 1, wherein said at least one parameter comprises a random number.	39
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.	40
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.	40
6.	Claim 6: The method of claim 1 wherein said data stream is a digit sample of an environment.	41
B.	Ground 2: Rieger Renders the Challenged Claims Obvious	41
1.	Claim 1	42
a.	[1pre] A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:	42
b.	[1a] storing a data stream in a data file in a memory;	42

c.	[1b] utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;	43
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;.....	48
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;	50
f.	[1e] utilizing said signature protocol to generate a second signature based on said data stream;	52
g.	[1f] comparing said first signature to said second signature,.....	53
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	54
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.	56
2.	Claim 2	57
3.	Claim 3	58
4.	Claim 4.....	59
5.	Claim 5	60
6.	Claim 6.....	60

C.	Grounds 3-4: Exif 2.0 or Exif 2.1 Discloses Digital Camera “Parameters” Available for the Glass and Rieger Inventions	61
1.	Motivation to Combine	61
2.	Claim 1	62
3.	Claims 2-3 and 6	62
4.	Claim 4	62
5.	Claim 5	65
D.	Grounds 5-8: Serret-Avila Discloses Displaying an “Error” or “OK” Signal to the User	67
1.	Motivation to Combine	67
2.	Serret-Avila Discloses Limitations [1f], [1g], and [1h]	69
VII.	Discretionary Denial Would Be Inappropriate and Inequitable	72
A.	Institution Will Enable a Stay	72
B.	District Court Schedule	72
C.	Parallel Proceeding Considerations	72
D.	Issue Overlap	73
E.	Same Parties in Related Litigation	73
F.	Other Considerations	74
VIII.	Conclusion	74

TABLE OF AUTHORITIES

Federal Cases

<i>Apple v. Motorola</i> , 2012 WL 12537293 (N.D. Ill. Mar. 19, 2012)	12
<i>Intel v. Qualcomm</i> , 21 F.4th 801 (Fed. Cir. 2021)	13
<i>Intellectual Ventures II v. Sprint Spectrum</i> , 2018 WL 6018625 (E.D. Tex. Nov. 16, 2018).....	12
<i>Nichia Corp. v. DSS, Inc.</i> , 2023 WL 7211097 (Fed. Cir. 2023)	13
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	9, 10
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	9
<i>Samsung Elecs. Am. v. Prisia Eng'g</i> , 948 F.3d 1342 (Fed. Cir. 2020)	13
<i>Valve Corp. v. Ironburg Inventions</i> , 8 F.4th 1364 (Fed. Cir. 2021)	19, 20, 21

Federal Administrative Decisions

<i>Align Technology v. 3Shape</i> , IPR2020-01087, Paper 38 (PTAB Jan. 19, 2022)	13
<i>Apple v. Fintiv</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020).....	72, 74
<i>Cloudflare v. Sable Networks</i> , IPR2021-00909, Paper 42 (PTAB Oct. 18, 2022).....	13
<i>CrowdStrike v. Open Text</i> , IPR2023-00289, Paper 7 (PTAB July 21, 2023).....	73
<i>DJI Europe v. Daedalus Blue</i> , IPR2020-01472, Paper 31 (PTAB Feb. 14, 2022).....	13

<i>Dr. Reddy’s Laboratories v. Horizon Pharma USA</i> , IPR2018-00272, Paper 35 (PTAB Mar. 28, 2019).....	13
<i>Intel Corp. v. PACT XXP Schweiz AG</i> , IPR2020-00528, Paper 39 (PTAB Aug. 9, 2021).....	18
<i>Samsung Elecs. v. Staton Techiya</i> , IPR2022-00302, Paper 13 (PTAB July 11, 2022).....	74
<i>Sand Revolution II v. Continental Intermodal Group – Trucking</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	72
<i>Snap v. SRK Tech.</i> , IPR2020-00820, Paper 15 (PTAB Oct. 21, 2020).....	74
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	73
<i>Vizio v. Maxell</i> , IPR2022-01458, Paper 8 (PTAB Apr. 11, 2023)	74

Federal Statutes

35 U.S.C.	
§ 102.....	1, 14, 16, 19, 20
§ 103.....	1
§ 112.....	1

Federal Rules And Regulations

37 C.F.R. § 42.100(b)	9
-----------------------------	---

LIST OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 6,757,828 (the “’828 Patent”)
1002	Prosecution history of U.S. Application No. 09/626,044, which led to the issuance of the ’828 Patent
1003	Declaration of Zixiang Xiong, Ph.D. in Support of <i>Inter Partes</i> Review of U.S. Patent No. 6,757,828
1004	<i>Curriculum vitae</i> for Zixiang Xiong, Ph.D.
1005	U.S. Patent No. 6,332,193 (“Glass”)
1006	Rieger and Rode, “Digital Image Recording for Court-Related Purposes” (IEEE 1999) (“Rieger”)
1007	Declaration of Rachel J. Watters on Authentication of Publication
1008	“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”)
1009	“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”)
1010	Declaration of Kenneth Parulski in Support of <i>Inter Partes</i> Review of U.S. Patent No. 6,757,828
1011	U.S. Patent No. 6,959,384 (“Serret-Avila”)
1012	Schneier, <i>Applied Cryptography: Protocols, Algorithms, and Source Code in C</i> , Chs. 8 and 18 (2d ed. 1996)
1013	Rivest, Request for Comment 1321, “The MD5 Message-Digest Algorithm” (April 1992)
1014	U.S. Patent No. 6,707,915 (“Jobst”)
1015	U.S. Patent No. 5,499,294 (“Friedman”)

Exhibit	Description
1016	U.S. Patent No. 5,504,518 (“Ellis”)
1017	U.S. Patent No. 5,764,770 (“Schipper”)
1018	U.S. Patent No. 6,253,337 (“Maloney”)
1019	U.S. Patent No. 6,269,446 (“Schumacher”)
1020	Tentative Claim Construction Order issued in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.)
1021	Plaintiff Jonathan E. Jaffe’s Disclosure of Asserted Claims and Infringement Contentions provided in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.)
1022	Plaintiff’s Initial Claim Construction Brief filed in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.)
1023	Plaintiff’s Responsive Claim Construction Brief filed in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.)
1024	Plaintiff’s Objections and Responses to Defendant’s Claim Construction Interrogatories in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.)
1025	Plaintiff Jonathan E. Jaffe’s First Amended Complaint for Patent Infringement filed in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.)
1026	U.S. Patent No. 6,762,791
1027	U.S. Patent No. 8,102,457
1028	Declaration of Victoria C. Huang

MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))

The real party-in-interest is petitioner Adobe Inc. (“Petitioner”). No unnamed entity is funding, controlling, or directing this petition or has the ability to control or direct this petition or Petitioner’s participation in any resulting *inter partes* review. Petitioner understands based on public information that the ’828 Patent is owned by Jonathan E. Jaffe (“Patent Owner”).

Related Matters (37 C.F.R. § 42.8(b)(2))

Petitioner is aware of the following pending district court matter involving the ’828 Patent: *Jonathan E. Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224-JWH(MAAX) (C.D. Cal.).

Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3))

Petitioner appoints James L. Day (Reg. No. 72,681) of Farella Braun + Martel LLP as lead counsel and appoints Winston Liaw of Farella Braun + Martel LLP (Reg. No. 78,766) as back-up counsel.

Service Information (37 C.F.R. § 42.8(b)(4))

Service of any documents to lead and back-up counsel can be made via hand-delivery to Farella Braun + Martel LLP, One Bush Street, Suite 900, San Francisco, California, 94104. Petitioner consents to electronic service to the

following email addresses: jday@fbm.com, wliaw@fbm.com, and
calendar@fbm.com.

I. INTRODUCTION

Petitioner respectfully requests *inter partes* review of claims 1-6 (the “challenged claims”) of U.S. Patent No. 6,757,828 (the “’828 Patent”). As explained below and in the supporting declaration of Dr. Zixiang Xiong (EX1003), the challenged claims recite an invention that was obvious in light of the prior art.

The claims are unpatentable as obvious under 35 U.S.C. § 103¹ based on the following grounds:

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

¹ The pre-AIA version of Sections 102, 103, and 112 of the Patent Act apply.

Petitioner’s proposed construction of terms, evidence, and the bases for unpatentability are discussed below. A List of Exhibits is above.

II. GROUNDS FOR STANDING

Petitioner certifies that the ’828 Patent is available for *inter partes* review and that Petitioner is not barred/estopped from requesting review.

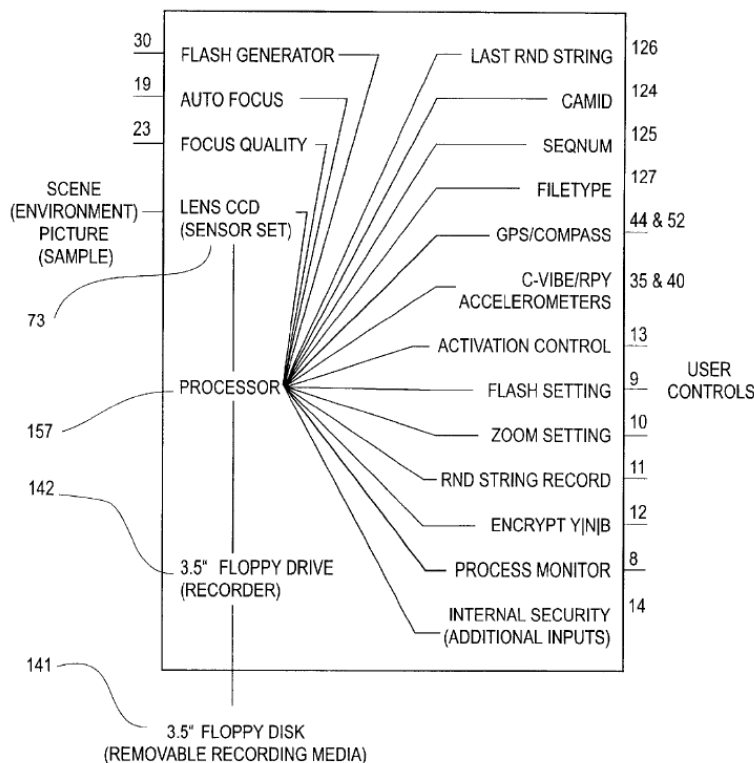
III. THE CHALLENGED PATENT

A. Patent Specification

The ’828 Patent is entitled “Indigenous Authentication for Sensor-Recorders and Other Information Capture Devices.” EX1001, 1. It relates to a “method and apparatus that allows [a] stored recording to be verified as an authentic, unaltered sample of the environment.” *Id.*, 1:8-12. Such “recordings” include “digital images, data files, and the more common audio recording.” *Id.*, 1:17-19. The patent states that “a digital signature” is created from the “sample [of the environment] and at least one parameter...” *Id.*, Abstract. The signature is stored with the sample “to be checked at a later time for authenticity.” *Id.* “The file is checked for authenticity by generating a second signature from the file and comparing [it] to the original signature.” *Id.* “If the two signatures are identical, the sample is considered authentic and if the two signatures are different, the sample cannot be authenticated.” *Id.*

The patent states that the “signature protocol” used to create the digital signature can be the “commercially available MD5.” EX1001, 7:25-27. A person of ordinary skill in the art would have known that MD5 is a one-way hash function used in cryptography and data processing. EX1003 ¶64; EX1012, 39; EX1013; EX1014, 2:38-45. A hash function is a mathematical function, or algorithm, that generates a fixed-length hash value based on the input. EX1006, 11. Such a function is useful because it always produces the same output value so long as the input is unchanged, but if even a single bit is changed to the input the resulting output value will be different. *Id.*, 11-12; EX1003, ¶65. A hash function, like MD5, is useful as a signature protocol in the context of the ’828 Patent because if the same image (or other input data) is provided to the hash function it will always produce the same output hash value. *Id.*, ¶66. But if any change is made to the image—even a single bit—the resulting output value will be different and a simple comparison between the initial hash value and the later hash value (after the modification) will show that a change has been made. *Id.*

The claimed invention is described in the context of digital photography. EX1001, 2:62-64. For instance, Figure 2A illustrates a “self-contained digital camera” incorporating aspects of the claimed invention. EX1001, 2:15-17.



'828 Patent, Fig. 2A

The figure illustrates a lens and charge-coupled device (CCD) sensor set 73 that captures an image. EX1003 ¶60. When the image is captured, a processor 157 gathers various parameters (e.g., Auto Focus, CamID, GPS/Compass, etc.) and appends them to the image. EX1001, 6:47-50, Fig. 6. The image and parameters are saved to a file using recorder 142. *Id.*, 7:44-53.

Once the image and parameters are captured, a digital signature is created based on “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.” *Id.*, 1:57-59; *see also id.*, 7:62-8:8, Fig. 7A. The authenticity of a stored image is subsequently “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.” *Id.*, 1:59-62; *see also id.*, 9:43-59.

The patent 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 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.” *Id.*, 3:18-20. The patent also states that “[d]uring 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.” *Id.*, 4:65-67.

B. Prosecution History

The ’828 Patent issued based on Patent Application No. 09/626,044, which was filed on July 27, 2000. EX1002.

On August 12, 2003, the examiner rejected all pending claims as anticipated by U.S. Patent No. 5,764,770 (“Schipper”). EX1002, 151-154. In response, the applicants canceled all pending claims and added new claims 9-14 (which later issued as claims 1-6). *Id.*, 274-276, 355. The applicants argued that the new

claims were different than Schipper because it does not teach the “tight coupling” required by the limitation “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter.” *Id.*, 277 (emphasis in original). The applicants argued that Figure 2A “illustrates a processor 157 which is ‘tightly coupled’ to a memory” and 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.” *Id.* They argued that the “Schipper patent teaches no such ‘tight coupling.’” *Id.*

On February 24, 2004, the examiner again rejected all pending claims. This time the rejection was based on the combination of Schipper and U.S. Patent No. 6,253,337 (“Maloney”). EX1002, 282-285. In response, the applicants added 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.” *Id.*, 293. They argued that neither Schipper nor Maloney discloses the required “tight coupling.” *Id.*, 292. They also argued that neither discloses the newly added “monitoring” step, which “means that, for example, a signal is generated if the device that prevents physical access to the interconnections between the sensor set and the memory is broken.” *Id.*, 292-293.

On April 20, 2004, the examiner issued a Notice of Allowance. EX1002, 314-315. A Certificate of Correction issued on August 17, 2021. EX1001, 34.

C. Patent Claims

The '828 Patent includes six claims. Claim 1 reads as follows (incorporating the change from the 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.

Dependent claims 2-6 depend directly or indirectly from claim 1. The claims are provided in the attached Claim Appendix.

D. Person of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSITA”) regarding the ’828 Patent would have an undergraduate degree (or equivalent) in electrical engineering, computer science, or a comparable subject and at least two years of work experience involving image processing. Alternatively, such a person would have an advanced degree and at least one year of post-graduate research/work experience involving image processing. EX1003 ¶82. A POSITA would be familiar with the design and implementation of systems and devices involving image processing, including image authentication, and would be familiar with authentication fundamentals, including encryption, hashing, and signature principles and techniques. *Id.*

IV. CLAIM CONSTRUCTION

The claims of the '828 Patent should be construed under the *Phillips* standard. 37 C.F.R. § 42.100(b); *see generally Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). The Board, however, only needs to construe the claims as necessary to resolve the underlying controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Aside from the following terms, Petitioner believes that no express constructions of claim terms are necessary to determine that the asserted prior art discloses the limitations of the challenged claims.

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

Claim 1 recites “utilizing a sensor, which is *tightly coupled* to said memory, to generate at least one internal and unique parameter.” EX1001, 20:62-64.² The term “tightly coupled” is not a term of art and is not defined by the patent. EX1003, ¶93. However, during prosecution, the applicants distinguished the prior art based on the “tightly coupled” claim requirement. EX1002, 277. With reference to Figure 2A, they argued:

Because the processor is “tightly coupled” to the memory, it will be virtually impossible for a user to supply false information to the memory by breaking *the conductive trace or lead* between the

² All emphasis is added unless otherwise indicated.

memory and the processor. This means, for example, that there is no possibility for altering the image before the authentication information is generated.

Id. Their 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.” EX1003, 94. A POSITA would therefore understand the term “a sensor, which is tightly coupled to said memory” to mean “a sensor coupled to said memory via conductive traces or leads.” *Id.* The district court issued a tentative claim construction ruling, and Petitioner’s construction matches that tentative construction. EX1020, 12.³

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

Claim 1 recites “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 specification explains

³ Petitioner contends in related litigation that the terms “tightly coupled”/“tight coupling” are indefinite. Petitioner does not waive that argument, which is not before the Board and does not preclude an obviousness finding. *See* Section IV.C, below.

that “[d]uring 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.” *Id.*, 4:65-67. During prosecution, the applicants added the “monitoring” step to overcome a rejection. EX1002, 290. They argued that in their “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 the newly added “monitoring” step means indicating (e.g., signaling) “if the device that prevents physical access to the interconnections between the sensor set and memory is broken.” *Id.*, 292-293. A POSITA would understand the term “monitoring the integrity of the tight coupling between said memory and said sensor” to mean “determining whether physical access has been gained to the coupling between said memory and said sensor.” EX1003, ¶99. This construction matches the court’s tentative construction. EX1020, 13.

C. “based on”

Claim 1 recites “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). The term “based on” could arguably be read as closed-ended (i.e., based exclusively on what follows) or open-ended (i.e., based at least on what follows). In light of the intrinsic evidence, a

POSITA would understand “based on” to be open-ended. EX1003 ¶102; *see also Intellectual Ventures II v. Sprint Spectrum*, 2018 WL 6018625, at *16 (E.D. Tex. Nov. 16, 2018) (“Use of ‘based on’ in the patent suggests that...the set of information following ‘based on’ is not closed.”); *Apple v. Motorola*, 2012 WL 12537293, at *9 (N.D. Ill. Mar. 19, 2012) (rejecting argument that “based on” means “based exclusively on” as “contrary to the usual usage of the phrase ‘based on,’ which does not exclude other possible bases...”).

The claim language, in light of the specification, confirms that “based on” is open-ended. Following the two “utilizing” steps, claim 1 recites “comparing said first signature to said second signature” and then (i) “generating an error signal” if they are different or (ii) “generating an ok signal” if they are the same. EX1001, 21:11-18. Thus, the data stream is authenticated if the first and second signatures match—it is not authentic if they are different. EX1003 ¶103. The only signature protocol disclosed in the patent is the MD5 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 input is the same for both signatures. *Id.* ¶104; EX1001, 7:25-27. The second signature must be generated using both the data stream *and* the same parameter(s) used in generating the first signature, though the claim recites only the data stream as input for the second signature. EX1003 ¶104; EX1001, 1:59-62, 9:43-54, Fig. 7A. Thus, “utilizing a signature protocol to generate a second

signature ***based on*** said data stream” means that the second signature is based at least on the data stream but potentially additional input data, such as the same parameter, as well (i.e., “based on” is open-ended). EX1003, ¶104; EX1001, 21:3-5.

Because “based on” is open-ended the outer bounds of the claim language is uncertain, and Petitioner has argued in the district court that this uncertainty renders the claims indefinite. The question of indefiniteness is not before the Board, however, and does not prevent Petitioner from showing that the prior art discloses all claim limitations. *See Dr. Reddy’s Laboratories v. Horizon Pharma USA*, IPR2018-00272, Paper 35 at 6 (PTAB Mar. 28, 2019) (“[W]e need not necessarily determine the outer boundaries of a claim in reaching a conclusion as to whether the asserted prior art anticipates a claim or renders it obvious.”); *see also Nichia Corp. v. DSS, Inc.*, 2023 WL 7211097, *3 (Fed. Cir. Nov. 2, 2023); *Samsung Elecs. Am. v. Prisua Eng’g Corp.*, 948 F.3d 1342, 1355 (Fed. Cir. 2020); *Cloudflare v. Sable Networks*, IPR2021-00909, Paper 42 at 23-24 (PTAB Oct. 18, 2022); *DJI Europe B.V v. Daedalus Blue*, IPR2020-01472, Paper 31 at 17, 19 (PTAB Feb. 14, 2022); *Align Technology v. 3Shape A/S*, IPR2020-01087, Paper 38 at 8, 40-41 (PTAB Jan. 19, 2022). Indeed, “[t]he indefiniteness of a limitation...precludes a patentability determination ***only*** when the indefiniteness renders it ***logically impossible*** for the Board to reach such a decision.” *Intel v.*

Qualcomm, 21 F.4th 801, 813 (Fed. Cir. 2021). Patent Owner cannot make such a showing here.

V. PRIOR ART REFERENCES

The '828 Patent claims priority to an application filed on July 27, 2000. EX1001, 1; EX1021, 8. None of the following references was cited during prosecution of the '828 Patent.

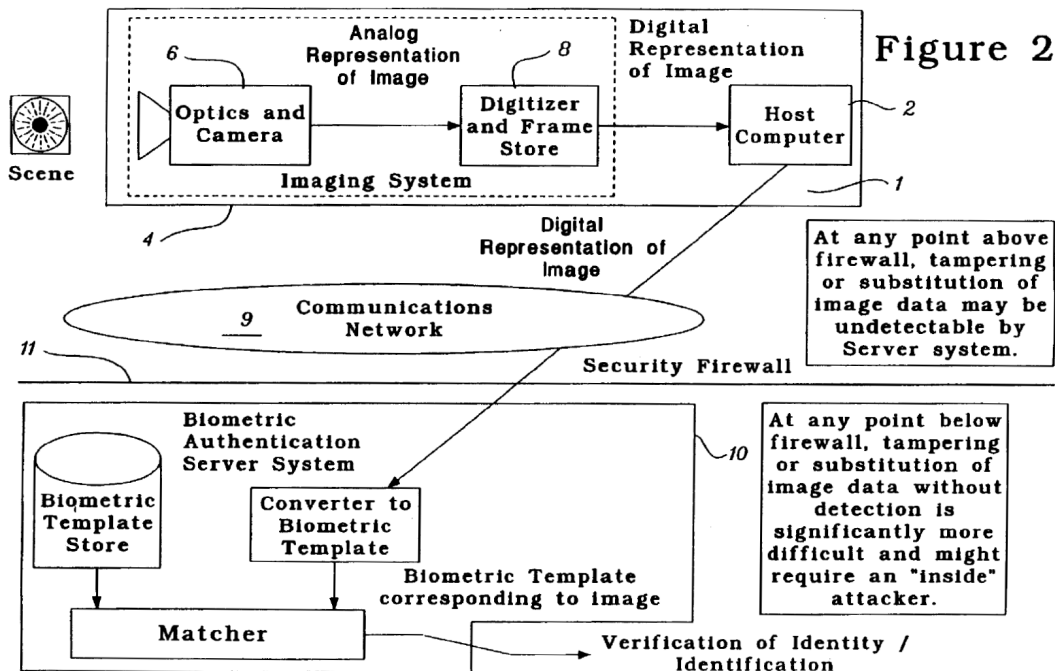
A. Glass (EX1005)

Glass is a U.S. patent that was filed on January 18, 1999, and constitutes prior under at least 35 U.S.C. § 102(e).

Glass is entitled “Method and Apparatus for Securely Transmitting and Authenticating Biometric Data Over a Network.” EX1005, 1. It describes a system providing “secure transmission and subsequent authentication of biometric data” collected by a “sensor” such as a digital camera. *Id.*, 3:45-51. The biometric data is stored in a data file along with a code, which “is computed as a function of the image, [a] token and a secret key associated with the camera.” *Id.*, 3:52-53, 4:1-8. The file is transferred 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.” *Id.*, 3:53-57.

Figure 2 illustrates an embodiment of the invention in a client-server system. EX1005, 4:45-47. The client system 1 includes a personal computer 2 (Host

Computer) and a “separate imaging system 4 which is connected to the host computer.” *Id.*, 4:47-48, 4:54-55.



Glass, Fig. 2

“The imaging system contains a camera 6 with associated optics or other sensor for collecting the biometric data from the user.” *Id.*, 4:55-58. A “digital signature” is generated using a “secure hash function” based on the image data, a “secret key,” and optionally a digital token. *Id.*, 5:62-6:3. “The 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 “compute a signature of the original data and check it against the signature sent with the data.” *Id.*, 6:50-55. “If the signatures match, the data can be assumed to not have been altered with an extremely high confidence level.” *Id.*, 60:55-56.

B. Rieger (EX1006)

Rieger is a printed publication entitled “Digital Image Recording for Court-Related Purposes” that was published no later than November 9, 1999, and constitutes prior art under at least 35 U.S.C. § 102(a).

Rieger describes “a manipulation-proof digital camera capable of meeting the stringent integrity and authenticity requirements imposed for images presented as evidence in court....” EX1006, 1. “Features built into the camera make it relatively easy to record additional characteristic parameters of the image-production process” such as “the identity of the photographer, global coordinates, date and time, to mention only a few of the most important parameters.” *Id.*, 1. These features built into the camera are “integrated into a specially protected compartment in the camera housing,” as illustrated in Figure 3. *Id.*, 4.

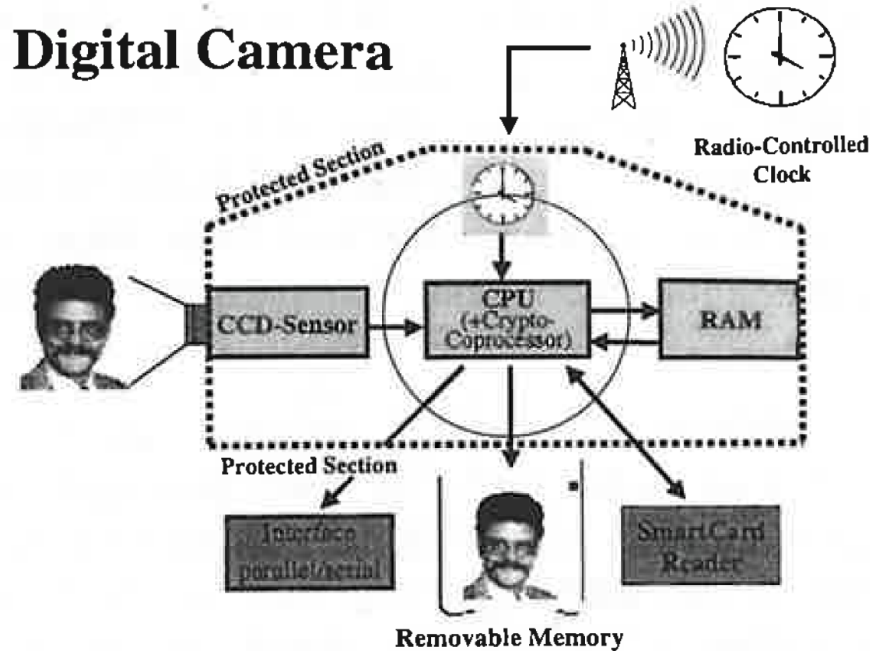


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Rieger, Fig. 3

The camera generates an “image signature” based on a hash of the image data, the camera signature (which itself is a hash of the image data), and camera parameters (e.g., GPS data, date and time, etc.). EX1006, 4-5. The image data, image signature, and parameters are saved to the camera’s removable memory. *Id.*, 5. Subsequently, the image data can be authenticated by an “integrity test” that involves recomputing a new hash value based on the image data and parameters and then comparing it to the original image signature. *Id.*, 6, 11-12. As Rieger explains:

Because 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. Thus a non-detectable manipulation of a digital image protected in this way should be impossible.

Id., 6 (footnote omitted).

The Rieger paper was presented at the IEEE’s 33rd Annual International Carnahan Conference on Security Technology held on October 5-9, 1999. As established by the declaration of Rachel J. Watters (EX1007), Rieger was published in the proceedings of that conference: Sanson, L.C. (Ed.) (1999), *33rd Annual 1999 International Carnahan Conference on Security Technology: Proceedings – The Institute of Electrical and Electronic Engineers: October 5-7, 1999, Madrid, Spain, IEEE* (the “Conference Proceedings”). *Id.*, 1.⁴ Ms. Watters is a librarian and the Head of Resource Sharing for the University of Wisconsin – Madison’s General Library System. *Id.* Exhibit A attached to the Watters declaration is a copy of the front cover, front matter, and back cover of the

⁴ Papers presented at IEEE conferences in the relevant period were commonly published at or shortly after the conference. EX1003, ¶130; EX1010, ¶10; *see also, e.g., Intel Corp. v. PACT XXP Schweiz AG*, IPR2020-00528, Paper 39 at 13-17 (PTAB Aug. 9, 2021) (finding paper published in IEEE conference proceedings to be a printed publication).

Conference Proceedings, which includes a stamp showing that the book is the property of the Kurt F. Wendt Library at the University of Wisconsin – Madison. *Id.*, 2. Exhibit B is the cataloging system record for the Conference Proceedings showing that the University of Wisconsin – Madison Libraries owned the book and had it cataloged in the system as of November 9, 1999. Exhibit C attached to the declaration is Rieger (EX1006), which was copied from pages 262 to 279 of the Conference Proceedings. *Id.* Ms. Watters also confirms that members of the interested public could locate the Conference Proceedings, including Rieger, after it was cataloged by searching the public library catalog or requesting a search, based on title, editor, or subject keywords. *Id.*, 3. Thus, Rieger qualifies as a “printed publication.” *See Valve Corp. v. Ironburg Inventions*, 8 F.4th 1364, 1373 (Fed. Cir. 2021) (“For a reference to qualify as a printed publication, before the critical date the reference must have been sufficiently accessible to the public interested in the art.”) (citations and internal quotation marks omitted).

C. Exif 2.0 (EX1008)

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, 3-4. Exif 2.0 constitutes prior art under at least 35 U.S.C. § 102(a) and (b).

Exif 2.0 was publicly accessible by November 1997, as confirmed by the Declaration of Kenneth Parulski (EX1010). Mr. Parulski worked for the Kodak Research Labs division of Eastman Kodak Company through the 1990s and early 2000s. *Id.*, ¶3. He was directly involved in the development of the Exif standard including Exif 2.0. *Id.*, ¶¶, 4-6. Indeed, Exif 2.0 (EX1008) is a copy of the Exif version 2.0 standard document that Mr. Parulski has maintained in his files since he obtained it from JEIDA in 1997. EX1010, ¶6, Exhibit B. At that time, an interested person could contact JEIDA and obtain a copy of Exif 2.0. *Id.*, ¶7. Thus, Exif 2.0 qualifies as a “printed publication” because it was “sufficiently accessible to the public interested in the art.” *See Valve Corp.*, 8 F.4th at 1373.

D. Exif 2.1 (EX1009)

Exif 2.1 is a printed publication 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 by December 1998. EX1009; EX1010, ¶¶8-9, Exhibit D. Thus, Exif 2.1 constitutes prior art under at least 35 U.S.C. § 102(a) and (b).

As confirmed by Mr. Parulski, an interested person could contact JEIDA beginning in 1998 and obtain a copy of Exif 2.1. EX1010, ¶9. Exif 2.1 qualifies as a “printed publication” because it was “sufficiently accessible to the public interested in the art.” *See Valve Corp.*, 8 F.4th at 1373.

E. Serret-Avila (EX1011)

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 issued on October 25, 2005. Serret-Avila constitutes prior art under at least 35 U.S.C. § 102(e).

Serret-Avila is entitled “Systems and Methods for Authenticating and Protecting the Integrity of Data Streams and Other Data.” EX1011, 1. Serret-Avila discloses a technique for “providing relatively fast, secure, and efficient authentication of data streams and other electronic content.” *Id.*, 2:66-3:3; *see also id.*, 3:7-9. The 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 precede it.” *Id.*, 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. *Id.*, 9:53-59.

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).” *Id.*, 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” (e.g., display an error message, log the error, etc.). *Id.*, 10:33-45.

VI. GROUNDS OF UNPATENTABILITY

A. Ground 1: Glass Renders the Challenged Claims Obvious

Like the ’828 Patent, Glass discloses an invention in the field of image processing and addresses the same problem of authenticating digital images. EX1005, Abstract, 1:7-10, 2:23-26, 2:32-35, 3:45-4:18; EX1001, Abstract. As discussed in more detail below, Glass describes an imaging system that captures biometric data in a digital image file and generates a code using the image data and a parameter (a “secret key”) that is later used to authenticate the image. Significantly, Glass also discloses a sensor that is “tightly coupled” to a memory within the imaging system and further describes “monitoring the tight coupling,” as claimed in the ’828 Patent. Thus, Glass discloses the features of the claimed invention the applicants relied on to distinguish the prior art during prosecution.

As described below, Glass discloses and renders obvious to a POSITA every element of the challenged claims. Further, Glass provides a sufficiently detailed description to permit a POSITA to practice the challenged claims with a reasonable expectation of success. EX1003, ¶155.

1. Claim 1

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

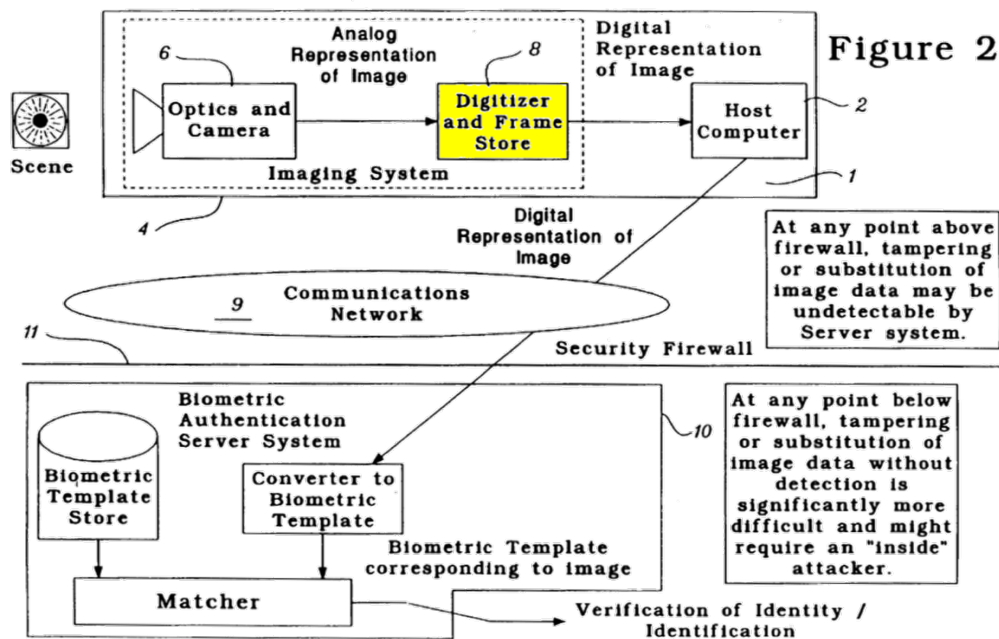
Glass discloses the preamble of claim 1. EX1003 ¶¶157-161. In particular, Glass describes a “method and apparatus for collecting and securely transmitting biometric data over a network [that] contains a sensor, preferably a camera, for collecting biometric data and code generating hardware and software.” EX1005, Abstract. The Glass system provides “secure transmission and subsequent authentication of biometric data” in the image collected by the “sensor” (e.g., camera). *Id.*, 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.” *Id.*, 3:52-53, 4:1-8, 4:58-62. The file is transferred from the imaging system to an authentication server that “validates the data by recomputing the code from its knowledge of the input data needed to generate that code.” *Id.*, 3:53-57. Thus, Glass discloses a *method for authenticating a data stream* (digital image data) that is *stored in a data file in memory*.⁵

⁵ For ease of review, claim language is in italics.

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

Glass discloses *storing a data stream in a data file in a memory*. EX1003

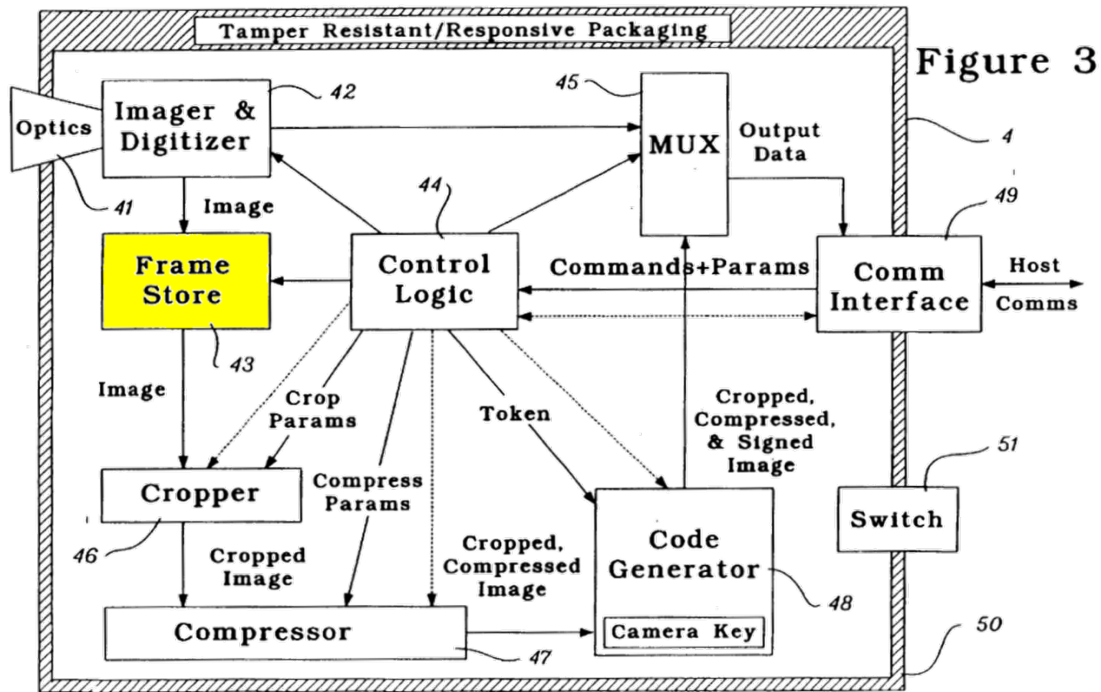
¶¶162-167. In Glass, the image (*data stream*) is stored in a “memory or frame store” (*a memory*) in the imaging system, as illustrated in Figure 2. EX1005, 4:58-62.



Glass, Fig. 2 (highlighted)

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.” *Id.*, 4:60-62; *see also id.*, 4:58-60.

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



Glass, Fig. 3 (highlighted)

In reference to Figure 3, Glass again refers to the “frame store” as *a memory*. *Id.*, 5:52-54 (“The digital image is sent to a multiplexer 45 and/or a ***frame store memory*** 43.”). Thus, Glass discloses *storing a data stream...in a memory*.

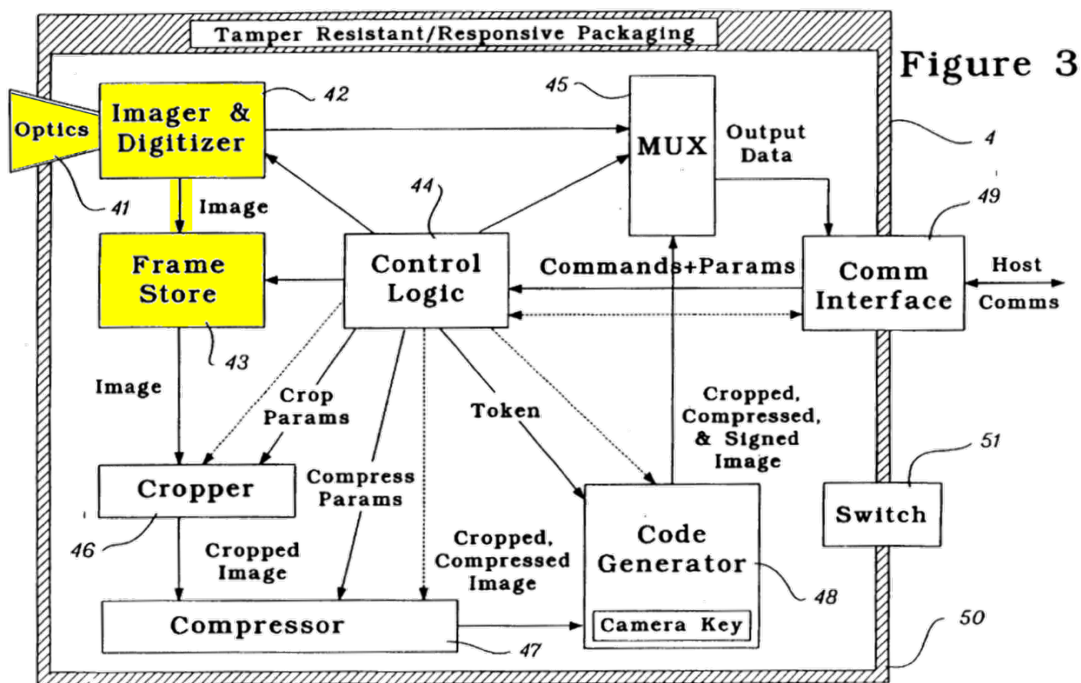
Glass also discloses storing the *data stream* (digital image) in *a data file* in the *memory*. EX1003 ¶¶165-166. Glass provides “a camera which functions as a sensor to collect the biometric data” (i.e., image data), and the “data is digitized into a biometric ***data file***.” EX1005, 3:50-52. Glass states that “[t]he camera data is digitized...[and] attached to the ***digital file***.” *Id.*, Abstract; *see also id.*, 3:62-63, 11:19-22, 12:1-3. Because the image data is digitized and stored in the imaging system (*id.*, 4:60-62), a POSITA would recognize that the file (i.e., “data file” or

“digital file”) is stored in the “frame store memory 43” (i.e., *memory* storing the image data in imaging system 4). EX1003 ¶165.

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

Glass discloses *utilizing a sensor, which is tightly coupled to said memory*.

EX1003 ¶¶168-180. As illustrated in Figure 3, the *sensor* (in Optics 41 and Imager & Digitizer 42) and *memory* (frame store memory 43) are electrically connected together within imaging system 4. *Id.*, ¶171.



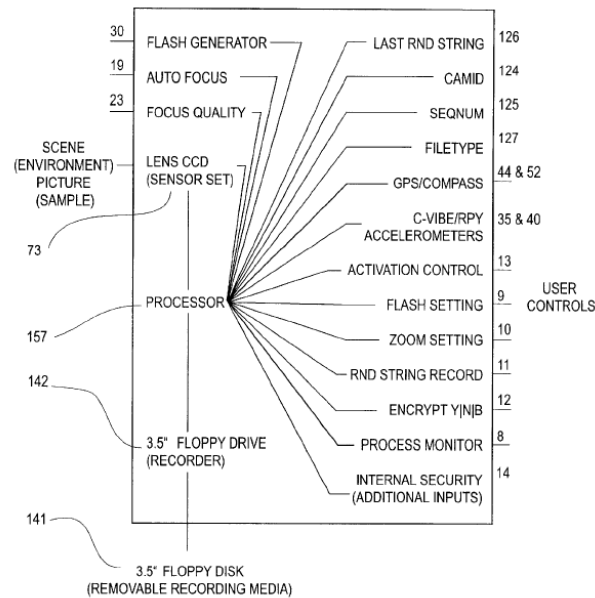
Glass, Fig. 3 (highlighted)

A POSITA would recognize that the *sensor* and *memory* are coupled “via conductive leads or traces” within the imaging system (i.e., they are *tightly*

coupled). *Id.*, ¶171; *see also* Section IV.A, above (construction of this term).

Indeed, Glass discloses *a sensor* that is *tightly coupled* to *a memory* in the same way that the patent applicants described their claimed invention during prosecution. The applicants argued that limitation [1b] is illustrated in Figure 2A, “which illustrates a processor 157 which is ‘tightly coupled’ to a memory.”

EX1002, 277.



'828 Patent, Fig. 2A (partial)

Glass’s Figures 2 and 3 show an imaging system with a *sensor* that is connected to *said memory* in a similar manner to Figure 2A. The applicants also asserted 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” (EX1002, 292), which is also true of Glass as the *sensor* and *memory* are in a

tamper resistant packaging as illustrated in Glass’s Figure 3. EX1003, ¶¶172-175.

Thus, for these further reasons, Glass discloses *a sensor, which is tightly coupled to said memory* as in [1b].

When the *sensor* captures 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*—the secret key).

EX1005, 5:49-6:4; EX1003 ¶¶176-179.⁶ In Glass, the “digital signature preferably is a secure hash function which takes 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. “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.” *Id.*, 4:6-8; *see also id.*, 6:12-13 (“Optionally, the key could be a unique identifier for the camera.”), 6:16-17. This *parameter* (secret key) is *internal* (i.e., stored inside imaging system 4) and explicitly described by Glass as *unique*. Thus, Glass’s “secret key” constitutes *at least one internal and*

⁶ According to the patent applicants, the *internal and unique parameter* need not be generated by the *sensor* itself. 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.

unique parameter.

Patent Owner has argued in the related litigation that a camera identifier (like Glass’s “secret key”) constitutes a *parameter* as recited in claim 1. In district court briefing, Patent Owner stated that “[t]he ‘at least one parameter’ [of claim 1] is described as ‘representative of at least one condition under which the digital sample was acquired’ and that “[t]he specification then provides several examples of a parameter such as ‘...camera identification....’” EX1022, 15; *see also* EX1023, 11 (same). Patent Owner further argued that Figure 7A of the ’828 Patent “describes parameters that the signature is based on” including “Camera ID.” EX1022, 15-16; *see also* EX1001, 6:60-61 (“camera identifier (CamID 124 set by the factory and unalterable by the user)”), Fig. 2A (“CAMID IS CAMERA IDENTIFICATION”).⁷ These admissions in the related litigation confirm that Glass’s “secret key”—which can be a “camera identifier”—constitutes an example of the *at least one internal and unique parameter* recited in claim 1.

Thus, Glass discloses *utilizing a sensor, which is tightly coupled to said*

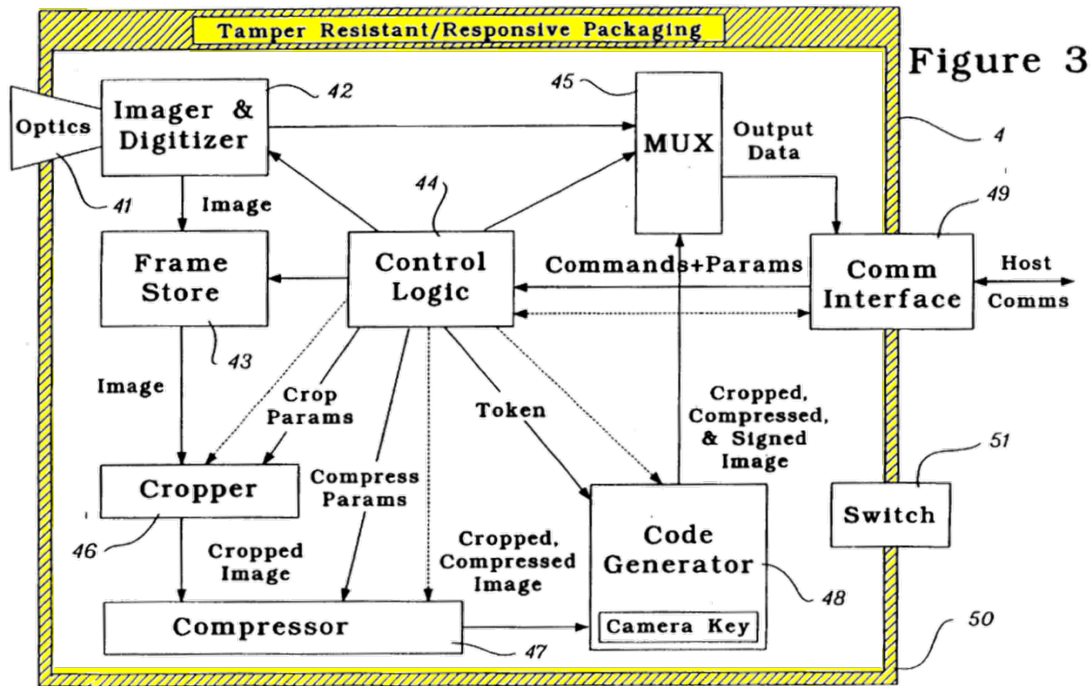
⁷ Patent Owner also contends in related litigation that the *internal and unique parameters* can include “information about the camera or device such as the maker of the camera or lens....” EX1021, 34.

memory, to generate at least one internal and unique parameter.

- 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;**

Glass discloses this limitation. EX1003 ¶¶181-186. 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.” *Id.*, 5:13-16.

Figure 3 illustrates tamper-resistant package 50 containing the components of the imaging system, including the *sensor* and *memory*. EX1005, 5:13-45; EX1003 ¶182.



Glass, Fig. 3 (highlighted)

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.” *Id.*, 5: 26-30. Thus, Glass discloses “determining whether physical access has been gained to the coupling between said memory and said sensor” (i.e., *monitoring the integrity of the tight coupling between said memory and said sensor*). *Id.*, 5:16-19 (“It is essential to ensure that the **integrity** of the acquired image and codes to be transmitted over the network have not been

compromised.”); *see also* Section IV.B, above (construction of this term).

The Glass system monitors the *integrity of the tight coupling...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 hidden secret key).

EX1003 ¶184. Glass confirms that the tamper-resistant packaging is in effect at all times “after system software is loaded and enabled” and “until intrusion is detected or the system software is reloaded using a special protocol,” including *when said...parameter is generated*. EX1005, 5:42-45.

Further, Glass discloses that *if said integrity is compromised, then also providing an indication of said compromised integrity*. EX1003 ¶185. Glass states that if an intrusion is detected, switch 51 signals control logic 44 “to return to a non-functioning state....” EX1005, 5:27-30. “This non-functioning state will essentially delete key software routines” and “may also delete special battery backed up ram tables which include security or encryption information.” *Id.*, 5:30-34. Thus, when *integrity is compromised*, the imaging system is put in a “non-functioning state,” which *provid[es] an indication of said compromised integrity*.

- 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;**

Glass discloses this limitation. EX1003, ¶¶187-193. 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’” *Id.*, 5:67-6:3; *see also id.*, 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).*

A POSITA would recognize that generating the digital signature using a secure hash function, as in Glass, does not involve altering the image data (*said first signature being generated without altering said data stream*). EX1003 ¶191. In addition, Glass describes the *first signature (digital signature) being appended to said data file in said memory*. *Id.*, ¶192. Glass expressly 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 id.*, 9:37-40, 11:47-49

(“codes prepended to the digital file and codes *appended to the digital file*”).⁸

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

Glass discloses *utilizing the same signature protocol to generate a second signature based on said data stream*. EX1003 ¶¶194-198. Glass states: “The 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...compute a signature of the original data and check it against the signature sent with the data. If the signatures match, the data can be assumed to not have been altered with an extremely high confidence level.” EX1005, 6:40-56. The signature computed by the authentication server is the *second signature*. EX1003 ¶195.

Glass describes the signature matching technique in more detail as follows:

[I]f 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

⁸ Glass distinguishes the “most straightforward” technique of appending/prepending the signature to the image data without altering it from “[a]nother technique” involving digital watermarking. EX1005, 7:7-10. Petitioner’s arguments do not relate to Glass’s discussion of the alternative technique of watermarking.

both original values y , z , as well as the hashing function $DS()$, a recipient can compute $Q'=DS(x, y, z)$. If $Q=Q'$ then x , y , and z have not been altered, otherwise one or more of the data items have changed.

EX1005, 6:57-65. In this description, the claimed *signature protocol* is $DS()$, the *first signature* is Q , and the *second signature* is Q' . EX1003 ¶196; *see also id.*, ¶198 (discussing example in Figure 8). This disclosure confirms that the *second signature* (Q') is based on said data stream because $Q'=DS(x, y, z)$ “where x is the image data.” EX1005, 6:57-61. Because the claim term “based on” is open-ended, it is immaterial that the *second signature* is computed using other inputs in addition to the *data stream*. EX1003, ¶196; *see* Section IV.C, above (construction of “based on”).⁹

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

Glass discloses this limitation. EX1003 ¶¶200-202. As discussed for [1e],

⁹ Patent Owner contends 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 (z). EX1003 ¶197.

Glass expressly describes *comparing said first signature to said second signature*:

“If $Q=Q'$ then x, y, and z have not been altered, otherwise one or more of the data items have changed.” *Id.*, 6:61-63; *see also id.*, 6:50-56 (“[T]he receiving system can ...*compute a signature of the original data and check it against the signature sent with the data.*”), 9:40-47 (“The server checks that the image has not been tampered with by computing the same or complementary digital signature...[which is] *compared to* the digital signature from the client.”).

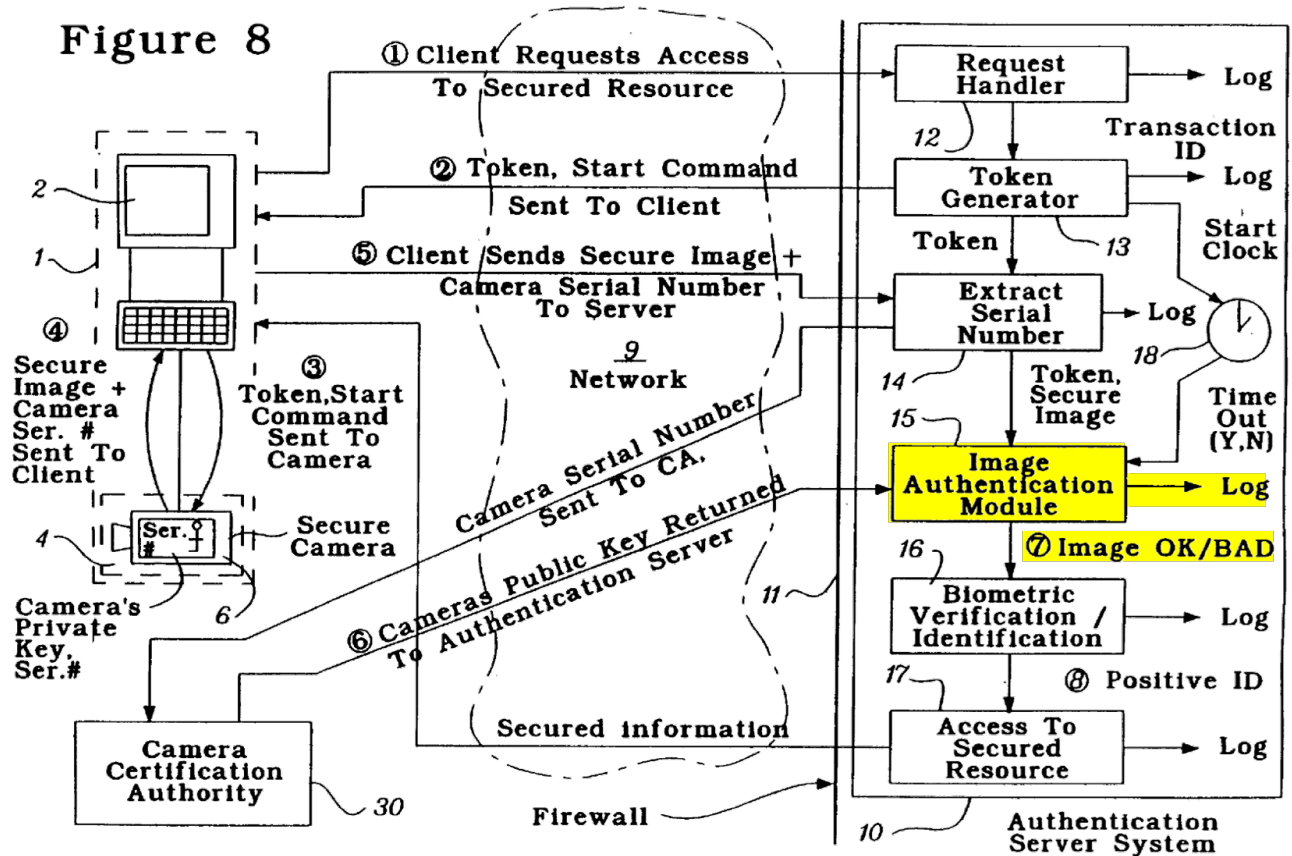
- h. [1g] if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and**

Glass discloses this limitation. EX1003 ¶¶203-206. As discussed for [1e]-[1f], Glass discloses that *if said first and second signatures are not the same, then...said stored data stream is not authentic.* EX1005, 6:61-63, 6:50-56, 9:40-47.

Glass also discloses *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic.* Glass describes maintaining a log file recording each step of the image authentication process. EX1005, 9:56-62 (“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.

Figures 7 and 8 show that Image Authentication Module 15 in Authentication Server System 10 determines if the image is authenticated (“Image OK/BAD”) and

that this determination is added to a “Log.” EX1003 ¶204; EX1005, 9:60-62 (“We prefer to log each step of the transaction as indicated by the word Log.”).



Glass, Fig. 8 (highlighted)

Thus, Glass discloses *generating an error signal (“BAD”) indicating that said stored data stream is not authentic.* EX1003 ¶205. A POSITA would know that a primary reason for storing the *error signal* in a “Log” is to present a record of the error to a system administrator or other *user* (i.e., *an error signal that is displayed to a user to indicate that said stored data stream is not authentic*). *Id.* Indeed, Glass’s statement that the log data “can provide irrefutable evidence of the

transaction” (EX1005, 9:58-60) confirms that the log data (including any *error signal*) is intended to be *displayed to a user*. EX1003, ¶205.

- 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.**

Glass discloses this limitation. EX1003 ¶207-210. As discussed for [1e]-[1f], Glass discloses that *if said first and second signatures are the same, then...said stored data stream is authentic*. EX1005, 6:61-63, 6:50-56, 9:40-47. Further, as discussed for [1g], Glass describes logging each step of the authentication process. *Id.*, 9:56-62. Figures 8-7 show the Authentication Module determining if the image is “OK” (“Image OK/BAD”) and adding the determination to the “Log.” EX1003 ¶208. A POSITA would know that a primary reason for storing an *ok signal* in a “Log” is to present a record of the authenticated image to a system administrator or other *user* (i.e., *an ok signal that is displayed to a user to indicate that said stored data stream is authentic*). *Id.*, ¶209. Glass’s statement that the log data “can provide irrefutable evidence of the transaction” (EX1005, 9:58-60) confirms that the log data (including any *ok signal*) is intended to be *displayed to a user*. EX1003 ¶209.

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

Glass discloses that the *memory* is *part of a digital camera*. EX1003, ¶¶211-

213; 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. Figure 3 illustrates the *memory* (frame store memory 43) housed in a *digital camera*. EX1003, ¶212.

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

Glass discloses that the *at least one parameter* can include a *random number*. EX1003 ¶¶214-215. As discussed for [1b], Glass’s “secret key” constitutes the *at least one parameter* recited in claim 1. According to Glass, “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 POSITA would know that a simple and effective means for assigning the secret key an “arbitrary value” would be to use a *random number*. EX1003 ¶214. 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 POSITA would know that such a key should be a *random number* to prevent an attacker from simply guessing the key value. EX1003 ¶215; EX1012, 17 (“Good keys are random-bit strings generated by some automatic process.”).

- 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.**

Glass discloses claim 4. EX1003 ¶216. Glass states 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, Abstract, 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*. EX1003 ¶216. And both time and location information constitute an *additional parameter* that is *generally representative of a condition under which said data stream was generated*. *Id.*

- 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.**

Glass discloses claim 5. EX1003 ¶217. As discussed 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, 12:66-13:3. A POSITA would know that by 2000 digital image metadata commonly included location information in the form

of *GPS coordinates*. EX1003 ¶217; EX1008, 64; EX1009, 62.

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

A POSITA would understand that claim 6 requires that the “data stream is a digit[al] sample of an environment.” EX1003 ¶¶218-219; EX1002, 276. In Glass, the imaging system captures an image to obtain biometric data (e.g., the user’s eye) and digitizes it. EX1005, Abstract, 1:19-22, 3:50-52, Fig. 2. The *data stream* (image data) is therefore *a digital sample of an environment*, including the user. *Id.*, Fig. 2 (illustrating the image being captured as an iris and referring to it as the “scene”). Thus, Glass discloses that the *data stream* being authenticated is a *digit[al] sample of an environment*.

B. Ground 2: Rieger Renders the Challenged Claims Obvious

Like the ’828 Patent, Rieger discloses an invention in the field of image processing and addresses the same problem of authenticating digital images. EX1006, 1 (Abstract); EX1001, Abstract. As discussed below, Rieger describes a manipulation-proof camera that captures digital images and generates digital signatures from the image data and other parameters (e.g., date, time, location, etc.). Rieger also describes an “integrity test” that is later used to verify the integrity of the image. Significantly, Rieger discloses a sensor that is *tightly coupled* to a memory within the camera and further describes *monitoring the tight coupling*, as claimed in ’828 Patent. Thus, Rieger discloses the features of the

claimed invention the applicants relied on to distinguish the prior art during prosecution.

As described below, Rieger discloses and renders obvious to a POSITA every element of the challenged claims. Further, Rieger provides a sufficiently detailed description to permit a POSITA to practice the challenged claims with a reasonable expectation of success. EX1003, ¶221.

1. Claim 1

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

Rieger discloses a *method for authenticating a data stream* (digital image) *stored in a data file in memory*. EX1003, ¶222. Rieger describes “the basic configuration of a manipulation-proof digital camera....” EX1006, 1. In particular, Rieger “describes an approach to ensuring the integrity and authenticity of photographic images during the image-recording phase” that involves “the use of a suitable digital signature...as an effective means of protecting digital images against manipulation.” *Id.* The *data stream* (image) being authenticated is *stored in a data file in memory* as explained below for [1a].

- b. [1a] storing a data stream in a data file in a memory;**

Rieger discloses this limitation. EX1003, ¶¶223-226. Rieger’s manipulation-proof camera records an image and, “[a]fter recording, the processor reads the image data from the CCD sensor and saves these to the RAM.”

EX1006, 4. The CCD (charge-couple device) sensor and RAM (random access memory) are shown in Figure 3, which illustrates Rieger's camera.

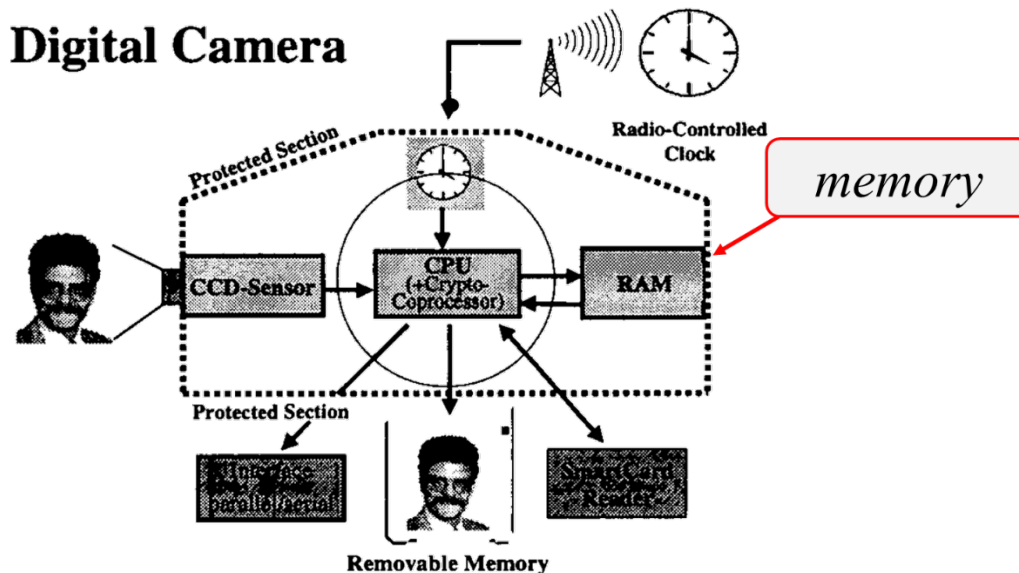


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Rieger, Fig. 3 (annotated)

The image data in RAM “is then compressed (e.g., in the JPEG format)...”

EX1006, 4; *see also id.* (“The image data are read out by the processor, compressed and saved to the RAM.”). A POSITA would understand that the image data is stored in a JPEG file in the camera’s RAM. EX1003, ¶¶225-226.

Thus, Rieger discloses *storing a data stream* (image data) *in a data file* (JPEG file) *in a memory* (RAM).

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

Rieger discloses this limitation. EX1003, ¶¶227-241. 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 Figure 3.

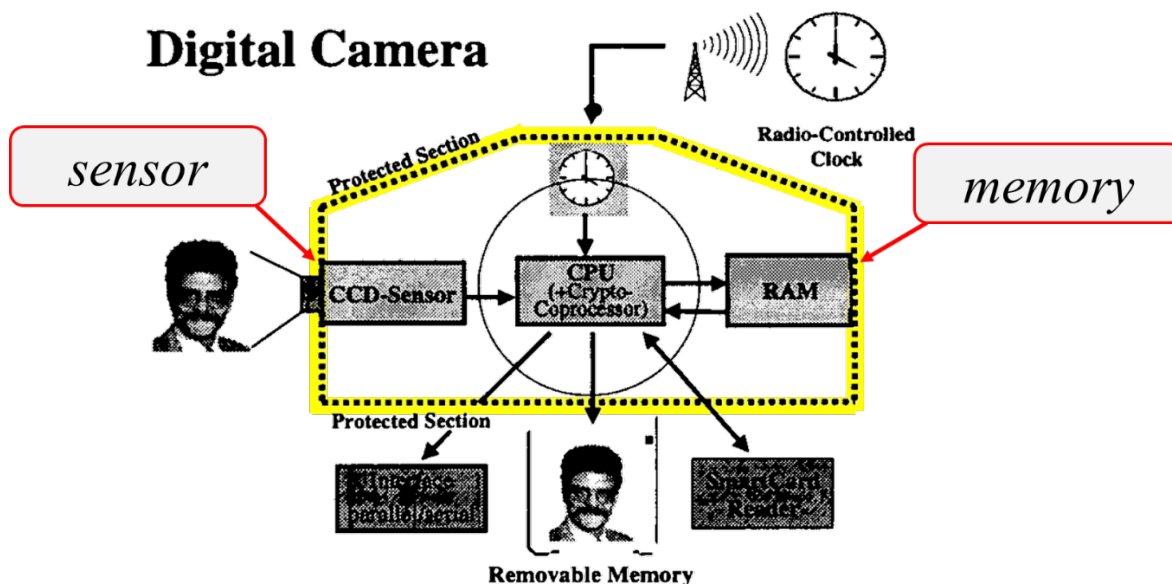
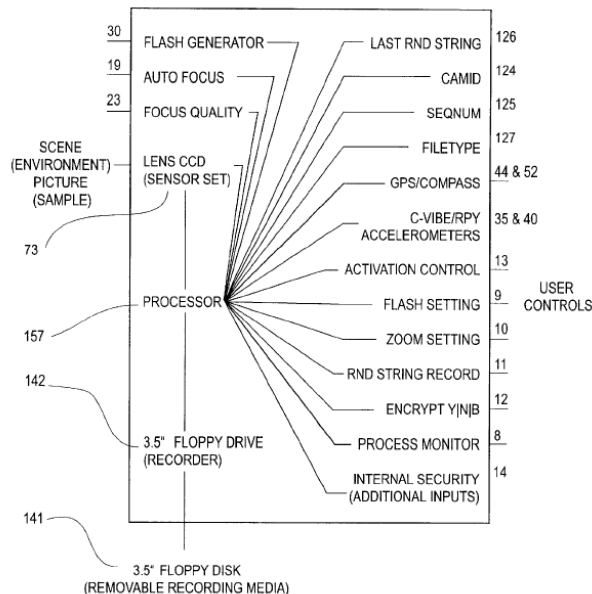


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Rieger, Fig. 3 (annotated, highlighted)

As illustrated, the *sensor* and *memory* are electrically connected together within the protected compartment. A POSITA would recognize that the *sensor* and *memory* are coupled “via conductive leads or traces” within the camera (i.e., they are *tightly coupled*). EX1003, ¶228; see also Section IV.A, above.

Indeed, Rieger discloses *a sensor* that is *tightly coupled* to *a memory* in the same way that the patent applicants described their claimed invention during prosecution. The applicants argued that limitation [1b] is illustrated in Figure 2A of the '828 Patent. EX1002, 277.



'828 Patent, Fig. 2A (partial)

Just as in Rieger's Figure 3, the '828 Patent's Figure 2A illustrates a *sensor* (Sensor Set) connected through a processor to a *memory* (Recorder). EX1003, ¶¶229-230. Further, the applicants argued that because the components are tightly coupled, "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. Rieger discloses that the components within the secure compartment are electrically connected, and a POSITA would understand that in

practice those connections would be made by conductive leads and traces used to transmit information between the components. EX1006, 4; EX1003, ¶232. The applicants also argued that “the claimed ‘tight coupling’ requires that the connection between the sensor and the memory not be physically accessible to the user” (EX1002, 292), which is also true of the *sensor* and *memory* in Rieger’s secure compartment (EX1006, 4). EX1003, ¶233. Thus, for these further reasons, Rieger discloses *a sensor, which is tightly coupled to said memory* as recited in [1b].

Rieger also discloses *utilizing a sensor...to generate at least one internal and unique parameter*. When Rieger’s manipulation-proof camera captures an image, multiple 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*. EX1003, ¶235.¹⁰ The parameters include several that constitute *at least one internal and unique parameter*. *Id.*, ¶¶236-241.

Date and Time: Rieger describes recording “additional characteristic

¹⁰ See fn. 6, above.

parameters of the image-production process” including “date and time.”

EX1006, 1; *see also id.*, 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.” *Id.*, 5; EX1003, ¶237. Date and time provide a *unique parameter* because it will be different for each image taken by Rieger’s camera. EX1003, ¶237. Further, Patent Owner has alleged in litigation that the *internal and unique parameter[s]* of claim 1 “include elements such as...the date and time of the image....” EX1025, ¶39; *see also* EX1022, 15; EX1023, 11.¹¹

Global Coordinates: Rieger describes recording “additional characteristic parameters of the image-production process” including “global coordinates.” EX1006, 1; *see also id.*, 3 fn. 3 (“supplementary information” including “GPS coordinates for the recording location”). The global coordinates for an image constitute an *internal...parameter* because it is provided by a “GPS receiver” in the manipulation-proof camera. *Id.*, 5; EX1003, ¶239. The global coordinates are a *unique parameter* because images taken by different cameras will not be in

¹¹ Patent Owner also asserts that a digital camera capturing date/time information for an image constitutes *utilizing a sensor* as in [1b]. EX1025, ¶33.

precisely the same location. EX1003, ¶239. Further, Patent Owner has alleged in the related litigation that the *internal and unique parameter[s]* of claim 1 “include elements such as GPS (latitude and longitude). . . .” EX1025, ¶39; *see also* EX1022, 15; EX1023, 11.¹²

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 in the preceding two paragraphs. The combination provides a *unique parameter* because “the exact time and the precise location of the camera” (*id.*) will be different for every image taken by that camera (or any other camera). EX1003, ¶241.

- 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;**

Rieger discloses this limitation. EX1003, ¶¶242-245. Rieger describes a

¹² Patent Owner also asserts that a digital camera capturing “location” information for an image constitutes *utilizing a sensor* as in [1b]. EX1025, ¶33.

manipulation-proof camera including a “secure compartment” surrounding internal components including the *sensor* and *memory*. EX1006, 4, Fig. 3. Rieger explains:

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

EX1006, 4. Thus, Rieger’s camera uses a “protective shield” for “determining whether physical access has been gained to the coupling between said memory and said sensor” (i.e., *monitoring the integrity of the tight coupling between said memory and said sensor*). EX1003, ¶243; *see also* Section IV.B, above. The secure compartment is monitored at all times (EX1006, 4), including *when said at least one internal and unique parameter is generated*. EX1003, ¶244.

If the secure compartment is compromised—for example if someone opens or drills into the camera body—the processor will detect a change in potential of the protective shield and automatically delete the camera’s secret key. EX1006, 4. In this way, Rieger’s camera determines *if said integrity is compromised* (i.e., has someone drilled into or otherwise accessed the secure compartment) and, if so, the camera *then also provid[es] an indication of said compromised integrity* by

“automatically delet[ing] the secret key stored in the signature chip.” *Id.*; EX1003, ¶245.

- 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;**

Rieger discloses this limitation. EX1003, ¶¶246-251. Rieger’s camera generates a “digital signature” for each image so that it can be subsequently authenticated. EX1006, 3. When an image is captured, the camera saves the image data to RAM and “[t]he compressed image data are hashed by the camera processor.” *Id.*, 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.” *Id.* As discussed above, the camera also captures various parameters related to the image including date, time, and location. *Id.*, 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.” *Id.* This time, the input to the hash function includes the “image, camera signature, and camera parameters” (e.g., date, time, location). *Id.*; EX1003, ¶246. This hash value constitutes the claimed *first signature*—it 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).

Rieger's camera generates *said first signature...without altering said data stream*. EX1003, ¶¶247-248. The hash function (*signature protocol*) does not alter the image (*data stream*) that is input to the function. *Id.* 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 are generated). *Id.*, 4.

Rieger also discloses that the *first signature is appended to said data file in said memory*. EX1003, ¶¶249-251. 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” (*appended to said data file in said memory*). EX1006, 5.

In addition, Rieger refers to and includes an Appendix providing further details regarding aspects of the disclosed invention, including a section entitled “The Digital Signature.” EX1006, 11. In that section, Rieger discusses hash functions such as the claimed *signature protocol*. *Id.* 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 that the *first signature* is *generated without altering said data stream*. EX1003, ¶250. Rieger also 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* (i.e., image data in RAM). EX1003, ¶251.

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

Rieger discloses this limitation. EX1003, ¶¶252-253. 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 an “integrity test” is described in the Appendix. *Id.*, fn. 11. There, Rieger explains (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.

Id., 11-12. The “subsequent recomputation of the hash value” referred to by Rieger is the *second signature* of [1e]. EX1003, ¶253. It is generated *utilizing said signature protocol* (hash function) *based on said data stream* (i.e., “what is presumed to be the identical text”).

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

Rieger discloses this limitation. EX1003, ¶254. As discussed for [1d]-[1e], 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 POSITA 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*). EX1003, ¶254.

- 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**

Rieger discloses this limitation. EX1003, ¶¶255-257. 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. 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.*

Rieger also discloses or at least suggests *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic.*

EX1003, ¶256. Rieger’s Figure 7 illustrates the integrity test (and a related authenticity test also described by Rieger).

- 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.**

Rieger discloses this limitation. EX1003, ¶¶258-260. 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, 11; *see also id.*, 11 (“any user can compute the hash value himself on the basis of the original plain text and determine, through comparison, whether the value transmitted by the sender is identical with his own result”). Thus, Rieger’s integrity test shows that *if said first and second signatures are the same, then said stored data stream is authentic.*

Rieger also discloses or at least suggests *generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.* EX1003, ¶259. 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.

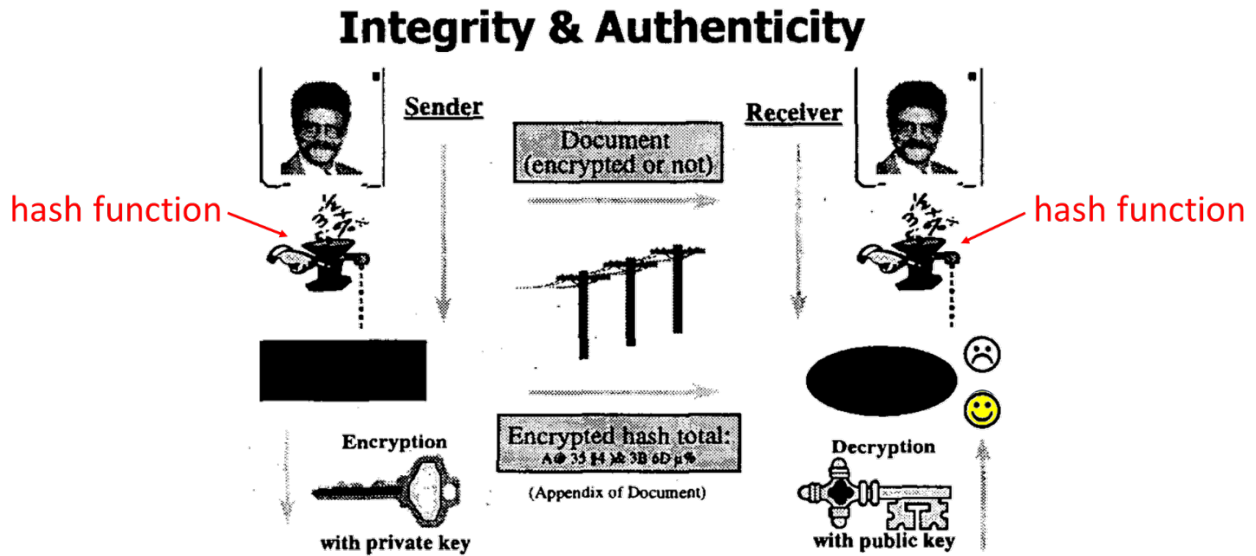


Figure 7: Principles of the integrity and authenticity test

Rieger, Fig. 7 (annotated, highlighted)

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. *Id.*, ¶260. The smiling face 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*. *Id.* Displaying such a message to the user would be an obvious design choice for a POSITA that, with little effort, would provide the user with a clear indication that the document/image has been validated. *Id.*

2. Claim 2

Rieger discloses that *said memory form[s] part of a digital camera*.

EX1003, ¶261. Rieger’s “Figure 3 shows the basic conceptual diagram for a *digital camera*....” EX1006, 4; *see also id.*, 1 (“Reflections regarding the basic

configuration of a manipulation-proof *digital camera*...will be discussed.”)

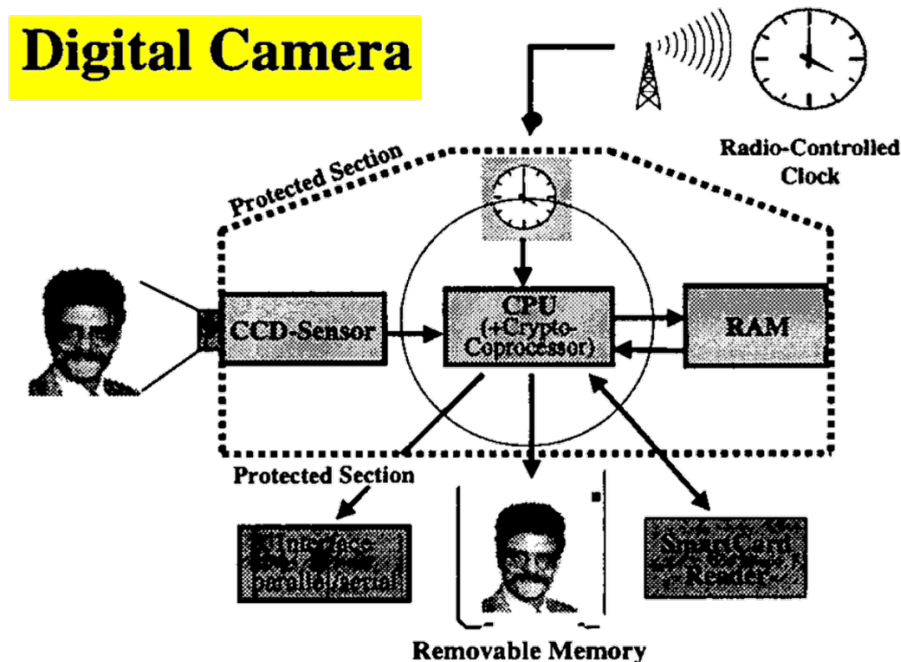


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Rieger, Fig. 3 (highlighted)

As illustrated, the *digital camera* includes RAM, which is the claimed *memory*.

3. Claim 3

Rieger discloses that the *at least one parameter* can include a *random number*. EX1003 ¶262. Rieger states that the “hash value (image, camera signature, camera parameters)” is encrypted using a “secret key.” EX1006, 5. A POSITA would know that using a *random number* for the key would enhance security. EX1003, ¶262; 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” (*id.*, 4).

4. Claim 4

Rieger discloses claim 4. EX1003, ¶¶263-265. 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*. EX1003, ¶263. According to Rieger, the supplementary 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. Rieger indicates that this type of supplementary information can include “a CPU serial number” and “date, time and GPS coordinates for the recording location.” *Id.*, 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*.

In addition, Rieger states:

In principle, all camera parameters, including focus values, aperture settings and exposure times, can be recorded and signed. This 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.” *Id.*

Rieger’s discussion 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.* EX1003, ¶265.

5. Claim 5

Rieger discloses claim 5. EX1003, ¶¶266-269. As discussed for claim 4, Rieger states that “supplementary information” (*at least one additional parameter*) “should...provide reliable identification of ...the camera and include other relevant data as well.” EX1006, 3 (footnotes omitted). An *additional parameter* that “provide[s] reliable identification of...the camera” constitutes a *CamID* (i.e., camera identifier). EX1003, ¶266; EX1001, 6:60-61, Fig. 2A. The “other relevant data” can include “GPS coordinates for the recording location.” EX1006, 3 fn. 3. Such a parameter constitutes *GPS coordinates*. EX1003, ¶267. Further, Rieger describes recording “aperture settings” (EX1006, 5), which constitute *zoom settings*. EX1003, ¶268.

6. Claim 6

Rieger discloses that the *data stream is a digit[al] sample of an environment.* EX1003, ¶¶270-271. Figure 3 illustrates Rieger’s digital camera taking a picture of a person’s face. EX1006, Fig. 3. Because the person is part of

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

C. Grounds 3-4: Exif 2.0 or Exif 2.1 Discloses Digital Camera “Parameters” Available for the Glass and Rieger Inventions

1. Motivation to Combine

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 were widely adopted and would have been a natural approach for implementing Glass’s system or Rieger’s manipulation-proof camera. EX1003, ¶272. Rieger refers to “camera parameters,” which a POSITA would have understood to include Exif metadata. *Id.*; EX1006, 5. Such a person would have been well-aware of Exif and the metadata tags specified by it for inclusion with compressed JPEG image data. EX1003, ¶272. Indeed, the ’828 Patent 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. EX1003 ¶272.

A POSITA would have been motivated to implement the Glass system or the Rieger camera in compliance with the Exif/JPEG standards. EX1003 ¶273. It would have allowed an implementer to use widely available, off-the-shelf image

processing algorithms and tools. *Id.* A POSITA 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 Exif was well-known and commonly used in digital cameras by 2000. *Id.*

2. Claim 1

Glass and Rieger each disclose the limitations of claim 1, including the *at least one internal and unique parameter* identified in [1b]. *See* Sections VI.A.1 and VI.B.1, above. The Exif 2.0 and Exif 2.1 standard documents provide more detail about the specific metadata fields available for digital cameras by 2000. EX1003, ¶274. 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. *Id.*

3. Claims 2-3 and 6

Glass and Rieger each disclose claims 2, 3, and 6 whether combined with Exif 2.0/2.1 or not. *See* Sections VI.A.2-VI.A.3, VI.A.6, VI.B.2-VI.B.3, VI.B.6 above.

4. Claim 4

Glass and Rieger each disclose 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* as recited in claim 4. *See* Sections VI.A.4 and VI.B.4, above. Should

Patent Owner argue otherwise, both Exif 2.0 and Exif 2.1 disclose this additional limitation as well. EX1003, ¶¶277-279.

The Exif standards describe a file format including Exif tags (or metadata fields) in the same file with compressed JPEG image data. EX1003, ¶278. 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, 20.¹³

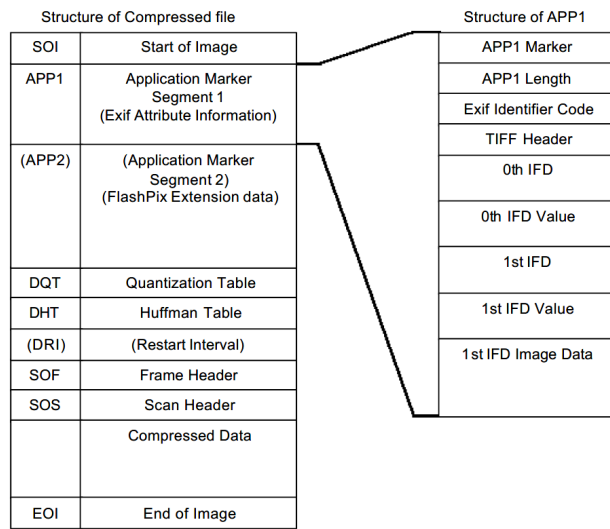


Fig. 6 Basic Structure of Compressed Data Files

Exif 2.1, 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).*

¹³ Petitioner relies on parallel disclosures in Exif 2.0 and Exif 2.1 should Patent Owner challenge the prior art status of either.

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	

Exif 2.1, Table 5 (highlighted)

These include tags for the exposure time, shutter speed, light source, scene type, and many others that a POSITA would have recognized as parameters *generally representative of a condition under which said data stream was generated*.

EX1003 ¶279. Thus, the combination of Exif 2.0 or Exif 2.1 with Glass or Rieger discloses claim 4.

5. Claim 5

Glass and Rieger each disclose claim 5. *See* Sections VI.A.5 and VI.B.5, above. Should Patent Owner argue otherwise, both Exif 2.0 and Exif 2.1 disclose *at least one additional parameter* identified in the list in claim 5. EX1003 ¶¶280-284. 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 the claim. Thus, the combination of Exif 2.0 or Exif 2.1 with Glass or Rieger discloses claim 5.

Zoom settings: One tag disclosed in Table 5 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 POSITA would recognize that this tag is a *parameter* providing *zoom settings*. EX1003 ¶281.

Flash status: Another tag disclosed in Table 5 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 POSITA would recognize that this tag is a *parameter* indicating *flash status*. EX1003 ¶282.

GPS coordinates: Exif 2.0 and Exif 2.1 include Table 12 entitled “GPS Attribute Information” identifying a number of GPS-related tags. 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	GPSVersionID	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

Exif 2.1, Table 12

Among others, the Exif tags include “Latitude” and “Longitude.” EX1003, ¶283; *see also* 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 POSITA would recognize at least the latitude-related and longitude-related tags are parameters indicating *GPS coordinates*. EX1003 ¶283.

Compass heading: Table 12 also lists a tag for “Direction of image” (“GPSImgDirection”), which “[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, 64, 69; EX1009 62, 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 POSITA would recognize that GPSImgDirection is a parameter providing the *compass heading* for the image. EX1003 ¶284.

D. Grounds 5-8: Serret-Avila Discloses Displaying an “Error” or “OK” Signal to the User

As discussed above, Glass alone or with Exif 2.0/2.1 renders obvious every limitation of the challenged claims. *See* Sections VI.A and VI.C, above. Similarly, Rieger alone or with Exif 2.0/2.1 renders obvious the limitations of the challenged claims. *See* Sections VI.B and VI.C, above. To the extent Patent Owner argues that Glass or Rieger does not disclose the limitations of claim 1 that require *generating* either an *error signal* or 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 the challenged claims (whether further combined with Exif 2.0/2.1 or not).

1. Motivation to Combine

Like the ’828 Patent, Glass, Rieger, and Serret-Avila disclose inventions in the field of image processing and address the same problem of authenticating images. 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; EX1006, 1 (Abstract); EX1011, Abstract, 1:32-35, 1:51-55, 2:66-3:3, 3:7-9. A POSITA would have naturally considered these prior art references. EX1003, ¶¶286, 289.

A POSITA 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. EX1003, ¶287. Indeed, Glass suggests as much by stating that each step of the authentication process is logged, which permits subsequent user review. EX1005, 9:61-62, 10:54-58, Figs. 7, 8. 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/error message would alert a user accessing 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). EX1003, ¶287. A user monitoring Glass’s system, such as a system administrator, would be alerted to any fraudulent attempt to access sensitive information so that he or she could take immediate remedial action. *Id.* 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. *Id.* Failing to indicate the results of the authentication process to a user would frustrate the purpose of the invention. *Id.*

Similarly, a POSITA would have been motivated to provide in Rieger’s image “integrity test” an indication to a user that the image is either authentic or not as taught by Serret-Avila. EX1003, ¶290. Indeed, Rieger suggests as much by illustrating in Figure 7 smiling and frowning face icons to indicate whether the

image is authentic or not. 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/error message would provide an unequivocal indication to the user whether the image is authentic. EX1003, ¶290. This is the point of Rieger’s integrity test. *Id.*; EX1006, 11-12. Failing to indicate the results of authentication to the user would frustrate the purpose of the invention. *Id.*, ¶290.

A POSITA would have been able to combine the references as described with a reasonable expectation of success. EX1003, ¶288, 291. It would have been a simple matter for such a person to program Glass’s system or Rieger’s integrity test to provide an error or ok message to a system user. *Id.*

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

Serret-Avila discloses *generating an [error/ok] signal that is displayed to a user* as recited in [1f]-[1h]. EX1003, ¶292-294. 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. *Id.*, 5:39-40, 9:66-10:1.

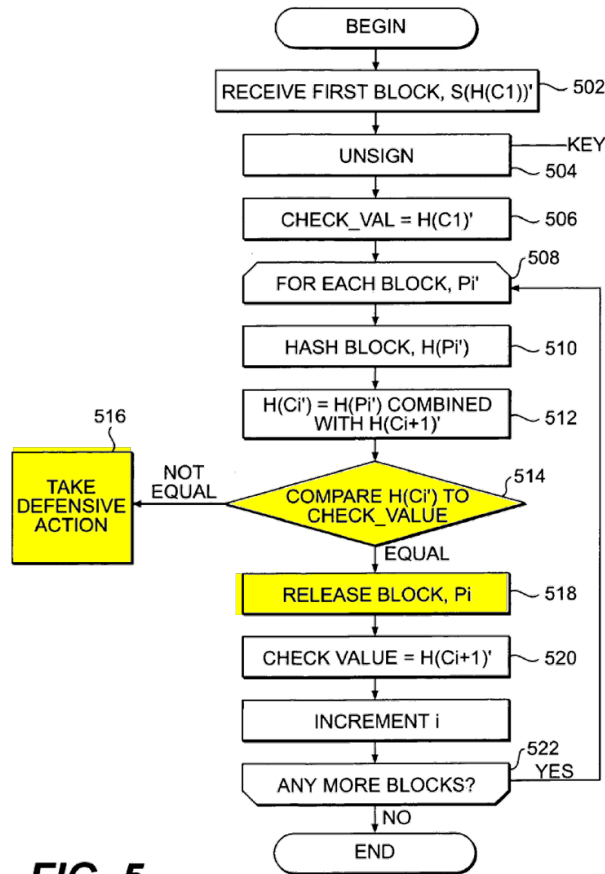
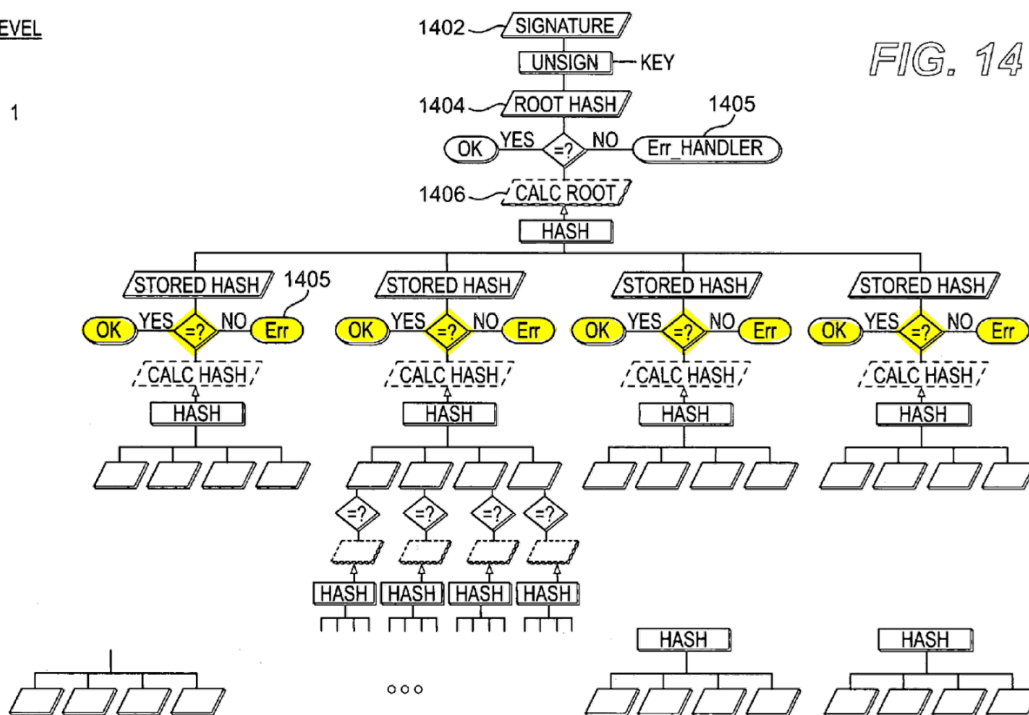


FIG. 5

Serret-Avila, Fig. 5 (highlighted)

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 in [1g]. EX1003, ¶293. If the hash values are equal, the sub-block is “deemed to be authentic, and the sub-block can be released for use (518).” EX1011, 10:28-30. By releasing the

In addition, Serret-Avila’s Figure 14 illustrates “a data flow diagram” of an embodiment that shows multiple comparisons of stored hash values to computed hash values to authenticate the stored data. EX1011, 5:64-67, 17:35-53.



Serret-Avila, Fig. 14 (highlighted)

[error/ok] signal that is displayed to a user as in [1g]-[1h]. EX1003, ¶294.

VII. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE AND INEQUITABLE

Under *Apple, Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020), the Board considers several factors—none of which supports a discretionary denial here.

A. Institution Will Enable a Stay

Neither party has requested a stay in the related litigation. This factor is neutral because the Board “will not attempt to predict” how the district court will proceed under such circumstances. *Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020).

B. District Court Schedule

The district court has not yet scheduled trial. Given the filing of this petition, Petitioner anticipates that either no trial date will be set or it will be scheduled after the deadline for Final Written Decision in this proceeding. The absence of a competing trial date weighs heavily against discretionary denial.

C. Parallel Proceeding Considerations

In the related litigation, the parties have briefed and argued claim construction but little else has been done. The court issued a tentative claim construction order but no final order as yet. Virtually no discovery has been

conducted, and the little that has was focused solely on claim construction. The parties have not yet exchanged final infringement or invalidity contentions, full fact discovery has not begun, expert discovery is far in the future, and there is no scheduling order setting a trial date or any post-claim-construction deadlines. This factor weighs against discretionary denial.

D. Issue Overlap

Petitioner stipulates that if the requested review is instituted, Petitioner will not pursue in the related litigation the grounds raised or that could have been raised in this petition. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020). This stipulation alone should preclude discretionary denial. *See* “Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation” at 3 (June 21, 2022) (“Consistent with *Sotera Wireless, Inc.*, the PTAB will not discretionarily deny institution in view of parallel district court litigation where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any grounds that could have reasonably been raised before the PTAB.”).

E. Same Parties in Related Litigation

Because Petitioner and Patent Owner are parties in the related litigation, and because the Board is likely to reach the merits before the district court, this factor weighs against discretionary denial. *CrowdStrike v. Open Text*, IPR2023-00289,

Paper 7 at 16 (PTAB July 21, 2023); *Samsung Elecs. v. Staton Techiya*, IPR2022-00302, Paper 13 at 18-19 (PTAB July 11, 2022). At worst, this factor should be considered neutral. *Snap v. SRK Tech.*, IPR2020-00820, Paper 15 at 16 (PTAB Oct. 21, 2020).

F. Other Considerations

Other considerations weigh strongly against discretionary denial. The challenged claims are clearly invalid as demonstrated herein, and Petitioner has not previously challenged the '828 Patent.

In summary, the *Fintiv* factors weigh against discretionary denial. Were that not so, institution would be appropriate nevertheless because the petition satisfies the compelling merits standard. Interim Guidance, 4; *Vizio v. Maxell*, IPR2022-01458, Paper 8 at 62 (PTAB Apr. 11, 2023).

VIII. CONCLUSION

Petitioner respectfully requests institution of review and cancellation of the challenged claims.

Respectfully submitted,

/James L. Day/

James L. Day
Registration No. 72,681
FARELLA BRAUN + MARTEL LLP
One Bush Street, Suite 900
San Francisco, California 94104
jday@fbm.com

CLAIM APPENDIX

(The claim language here has been modified according to the Certificate of Correction attached to the '828 Patent.)

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

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

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

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

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

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

comparing said first signature to said second signature,

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

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

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

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

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.

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.

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

CERTIFICATE OF COMPLIANCE

This petition complies with the 14,000 word-count limit under 37 C.F.R. § 42.24(a)(1)(i). The petition contains 13,995 words, excluding the parts exempted by 37 C.F.R. § 42.24(a)(1) (i.e., table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, word count certificate, and appendix of exhibits), as determined by the word count feature of Microsoft Word, which was used to prepare this petition.

/James L. Day/

James L. Day
Registration No. 72,681
Farella Braun + Martel LLP
235 Montgomery Street; 17th Floor
San Francisco, CA 94104

CERTIFICATE OF SERVICE

I hereby certify that on August 28, 2024, I caused a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits to be served by express mail, or means at least as fast and reliable as express mail, on the following counsel of record identified through the USPTO Patent Center.

Husch Blackwell Sanders Welsh & Katz
c/o Mark Murphy
120 S. Riverside Plaza, 22nd Floor
Chicago, IL 60606

In addition, courtesy copies were sent by electronic means to Patent Owner's litigation counsel at the following addresses:

chanba@dickinson-wright.com
jjones@dickinson-wright.com
eschiffer@schifferapc.com

/James L. Day/
James L. Day
Registration No. 72,681