

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ADOBE INC.,
Petitioner

v.

JONATHAN E. JAFFE,
Patent Owner

Inter Partes Review No. IPR2024-01352
U.S. Patent No. 6,757,828

PATENT OWNER'S RESPONSE
(37 CFR § 42.120)

TABLE OF CONTENTS

PATENT OWNER’S EXHIBIT LIST	iv
I. INTRODUCTION	1
II. OVERVIEW OF THE ’828 PATENT	3
III. PERSON OF ORDINARY SKILL IN THE ART	4
IV. CLAIM CONSTRUCTION	5
A. “a sensor, which is tightly coupled to said memory” (cl. 1)	5
B. “monitoring the integrity of the tight coupling between said memory and said sensor” (cl. 1)	9
C. “based on” (cl. 1)	11
V. PETITIONER HAS FAILED TO DEMONSTRATE THAT ANY OF THE CHALLENGED CLAIMS ARE UNPATENTABLE	12
A. Ground 1: Glass Fails to Render Obvious the Challenged Claims	12
1. Claim 1	12
(a) Glass Fails to Disclose a “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter” under Petitioner’s own Proposed Claim Construction [limitation 1b]	12
(b) Glass Fails to Disclose “monitoring the integrity of the tight coupling between said memory and said sensor” under Petitioner’s own Proposed Claim Construction [limitation 1c]	20
(c) Glass Fails to Disclose “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic” [limitation 1g]	23
(d) Glass Fails to Disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic” [limitation 1g]	25
2. Claims 2-6	28
B. Ground 2: Rieger Fails to Render Obvious the Challenged Claims ...	28
1. Claim 1	28

(a) Rieger Fails to Disclose a “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter” under Petitioner’s own Proposed Claim Construction [limitation 1b].....28

(b) Rieger Fails to Disclose “monitoring the integrity of the tight coupling between said memory and said sensor” under Petitioner’s own Proposed Claim Construction [limitation 1c].....35

(c) Rieger Fails to Disclose “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic” [limitation 1g] 38

(d) Rieger Fails to Disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic” [limitation 1g] 40

2. Claims 2-6 41

C. Grounds 3-4: Exif 2.0 or Exif 2.1 Fail to Render Obvious the Challenged Claims 42

1. Claim 1 42

2. Claims 2- 6 42

D. Grounds 5-8: Serret-Avila fails to Render Obvious the Challenged Claims.....43

1. Claim 1 43

(a) Petitioner Fails to Show That It Would Have Been Obvious to Modify Glass and Rieger to add Serret-Avila.....43

(b) Serret-Avila Fails to Disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic” [limitation 1g] 47

VI. CONCLUSION.....49

Certificate of Service 37 C.F.R. § 42.6(e).....50

Certificate of Compliance Pursuant to 37 C.F.R. § 42.24 51

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Andersen Corp. v. Fiber Composites, LLC</i> , 474 F.3d 1361 (Fed. Cir. 2007)	11
<i>Cont'l Cirs. LLC v. Intel Corp.</i> , 915 F.3d 788 (Fed. Cir. 2019)	6, 7, 8
<i>In re Gurley</i> , 27 F.3d 551 (Fed. Cir. 1994)	46
<i>In re Klein</i> , 647 F.3d 1343 (Fed. Cir. 2011)	43, 44, 45
<i>Scripps Clinic & Research Found. v. Genentech, Inc.</i> , 927 F.2d 1565 (Fed. Cir. 1991)	11
<i>Thorner v. Sony Computer Ent. Am. LLC</i> , 669 F.3d 1362 (Fed. Cir. 2012)	6, 8

Other Authorities

37 C.F.R. § 42.120	1
Cambridge Dictionary	24, 26, 27

PATENT OWNER’S EXHIBIT LIST

Exhibit No.	Description
2001	IEEE, “Official IEEE 802.11 Working Group Project Timelines” (Nov. 21, 2024)
2002	Claim Construction Scheduling Order issued in in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAx) (C.D. Cal.)
2003	Docket Navigator, “How Top US Patent Courts Compare on Median Time-to-Trial Statistics” (June 27, 2022)
2004	Plaintiff’s Original Complaint filed in <i>Jaffe v. Adobe Inc.</i> , Case No. 2:23-cv-06224-JWH(MAAx) (C.D. Cal.)
2005	Declaration of Bill Davis in Support of Patent Owner’s Response
2006	Curriculum Vitae of Bill Davis
2007	US Patent No. 5,486,853
2008	US Patent No. 7,161,622
2009	US Patent No. 6,377,981
2010	Wikipedia, “Floppy Disk Drive Interface” (available at https://en.wikipedia.org/wiki/Floppy_disk_drive_interface)
2011	Cambridge Dictionary, entry for “log file” (available at https://dictionary.cambridge.org/us/dictionary/english/log-file)
2012	Transcript of May 16, 2025 Deposition of Zixiang Xiong, Ph.D.

Pursuant to 37 C.F.R. § 42.120, Patent Owner Patent Owner Jonathan E. Jaffe (“Patent Owner” or “Jaffe”) hereby submits its Patent Owner Response.

I. INTRODUCTION

The Board should hold all challenged claims patentable in the present *inter partes* review of U.S. Patent No. 6,757,828 (EX1001, hereinafter “the ’828 patent”). Petitioner presents arguments in four sets of grounds, all of which fail.

First, claim 1 of U.S. Patent No. 6,757,828 (EX1001, hereinafter “the ’828 patent”) recites “a sensor, which is tightly coupled to said memory.” Petitioner argues that this claim language should be construed as “a sensor coupled to said memory via conductive traces or leads.” However, Petitioner fails to show that any of the cited references meet Petitioner’s proposed claim construction language. In particular, the prior art structures cited against the “sensor, which is tightly coupled to said memory” limitation: (1) fail to disclose or suggest how any camera sensor is physically connected to any memory; and (2) fail to disclose or suggest that any connection is made by *conductive traces or leads*, as Petitioner’s construction includes in the claim. Accordingly, because this element is part of claim 1 of the ’828 Patent, and each challenged claim depends from claim 1, each of Petitioner’s prior art grounds fails. Alternatively, Patent Owner contends that this claim language should be construed as “a sensor that is electrically or physically coupled to memory in a device.” However, for similar reasons, the Petition fails to disclose

the physical characteristics of any specific coupling in the device described in the prior art. Consequently, for similar reasons, the Petition fails to disclose this limitation under Patent Owner's proposed construction as well.

Second, Petitioner's cited references also fail to disclose "monitoring the integrity of the tight coupling between said memory and said sensor." However, Petitioner fails to show that the references teach monitoring the coupling between the sensor and the memory specifically. Rather, the references disclose monitoring other structures, such as protective casings or compartments external to the coupling between the sensor and the memory itself identified in the claim. As such, the cited references fail to disclose this limitation because the references do not monitor the coupling between the memory and the sensor as the claim language explicitly requires.

Third, the claims require "generating an error signal" and "generating an ok signal" that are, respectively, displayed to the user depending upon whether or not the digital images have been indicated to be authentic. However, the references cited by Petitioner fail to disclose displaying such notification signals to users. Rather, the references at best merely disclose recording events to log files, but these log files are not actively displayed to users. Nor do any of the references disclose any "ok signal," even under Petitioner's tortured arguments.

II. OVERVIEW OF THE '828 PATENT

The '828 Patent generally relates to authentication of digital files by using aspects of the environment in which the digital file was created including, but not limited to, date, time, latitude, longitude, altitude, roll, pitch, yaw, and compass heading. EX1001 at 2:65-3:6. The '828 Patent was prescient in recognizing that, in the digital age, “the ability to alter images” had been brought to the “neophyte level.” *Id.* at 1:27-29. Indeed, in just the last few years the concern of digital alteration has been brought to the forefront as generative artificial intelligence and “deep fake” videos have begun to take hold.

The '828 Patent employs a method of creating and subsequently determining a digital file's authenticity. The invention uses a digital signature that is created using the file “as well as at least one parameter that is representative of at least one condition under which the digital sample was acquired.” *Id.* at 1:54-57. As described above, the parameter could be any number of things such as the date and time the file was created, or the compass heading or altitude under which the digital file was made. *Id.* at 2:65-3:6. The file is then stored in memory, and/or removable storage media, together with the parameter and digital signature. *Id.* at 1:57-59. The method then determines authenticity of the file by creating a second signature from the stored file and at least one of the parameters and then comparing the signatures. *Id.* at 1:59-62. The patented method offers several improvements over the prior art.

For example, authentication is not dependent on the identity of the device that created the digital file, such as a specific digital camera. Instead, the digital file itself contains the authentication information and the signature authenticates the file. *Id.* at 1:64-67. In addition, the invention dispenses with the need for encryption which has a number of cost savings and convenience benefits. *Id.* at 1:67-2:3.

III. PERSON OF ORDINARY SKILL IN THE ART

Petitioner argues that a person of ordinary skill in the art (“POSITA”) 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.” Pet., 13. However, the ’828 Patent is primarily directed to digital security and authentication. As such, Patent Owner asserts that a POSITA 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 digital security, authentication, or digital image authentication. EX2005 at ¶53. Patent Owner agrees that “[a] POSITA would be familiar with the design and implementation of systems and devices involving . . . image authentication, and would be familiar with authentication fundamentals, including encryption, hashing, and signature principles and techniques.” Pet. at 8. However, these are concepts primarily addressed in digital security rather than image processing. EX2005 at ¶53.

As such, Patent Owner's proposed level of ordinary skill in the art correctly relates to the actual technology identified and claimed in the '828 Patent.

IV. CLAIM CONSTRUCTION

Petitioner argues that three terms from the '828 Patent require construction. Patent Owner disagrees with Petitioner's proposed constructions for "a sensor, which is tightly coupled to said memory" and "monitoring the integrity of the tight coupling between said memory and said sensor" as being incorrect for the reasons stated below.

A. "a sensor, which is tightly coupled to said memory" (cl. 1)

Petitioner asserts that the term "a sensor, which is tightly coupled to said memory" means "a sensor coupled to said memory via conductive traces or leads." Pet. at 10. Petitioner bases this argument upon an explanation made during prosecution which added language to the claim requiring that the sensor be "tightly coupled to said memory" in response to a rejection in view of U.S. Patent No. 5,764,770 ("Schipper"). EX1002 at 277. However, full examination of the prosecution history reveals that the reference to "conductive trace or lead" in the prosecution history is exemplary only, and not limited to conductive traces or leads.

Specifically, the Patentee explained during prosecution:

Exemplary structure or method steps corresponding to this claim feature is shown in Fig. 2A of the subject application, which illustrates a processor 157 which is "**tightly coupled**" to a memory. In one *exemplary embodiment* of the present invention,

the processor 167 generates a unique random string that is used for image authentication purposes. Because the processor is “tightly coupled” to the memory, it will be virtually ***impossible for a user to supply false information*** to the memory by breaking the conductive trace or lead between the memory and the processor. This means, for example, that there is ***no possibility for altering the image before the authentication information is generated.***’

Id. (emphasis added). Here, the Patentee demonstrates that the limitation requires a coupling that ensures that false information is not capable of being injected between the image sensor and the processor in the amended claim. However, there is no clear and unmistakable disclaimer within this statement from the prosecution history specifically limiting the claim language to conductive traces or leads. Further, the mere reference to exemplary conductive traces or leads here is merely illustrative, indicating that in this exemplary embodiment the conductive traces or leads is provided in order to show one example of a tightly coupled connection that achieves the stated purpose of preventing the introduction of false information prior to storing the information in memory. *Thorner v. Sony Computer Ent. Am. LLC*, 669 F.3d 1362, 1366–67 (Fed. Cir. 2012) (“To constitute disclaimer, there must be a clear and unmistakable disclaimer”); *Cont’l Cirs. LLC v. Intel Corp.*, 915 F.3d 788, 799 (Fed. Cir. 2019) (statements relating to “one technique” during prosecution “do not clearly and unmistakably disavow any claim scope”).

The lack of any clear and unmistakable disclaimer limiting the claim to conductive traces or leads becomes further evident by the additional explanation in the prosecution history distinguishing Schipper. Specifically, the Patentee explained that Schipper involved *external* information provided from *outside* the device, specifically “comparison of *position* information, which must originate from devices external to the camera, such as satellites in orbit around the earth.” EX1002 at 277. As such, the Patentee distinguished Schipper based upon the reference providing information external to the device, not based upon whether connections are provided by conductive traces or leads specifically. The Patentee further emphasized that the method described in the patent “should always operate, irrespective of the presence or absence signals external to the device, so long as it is supplied with electric power.” *Id.*

Moreover, in a later response, the Patentee further explained that this limitation requires that the connection between the sensor and memory be tightly coupled is based upon the connection not being physically accessible to the user. Specifically, the patentee explained, “in accordance with the present invention, the claimed ‘tight coupling’ requires that the connections between the sensor and the memory not be physically accessible to a user.” *Id.* at 292. Here, again, the Patentee explained that a second reference, U.S. Patent No. 6,253,337 (“Maloney”) failed to disclose the limitation because in Maloney “the sensors can be ‘local or remote.’”

EX1002 at 292. The Patentee explained that “[i]f the sensors are, in fact, ‘remote’ from the processor, then it would be impossible to prevent physical access to the interconnections between the remote sensor and the local processor.” *Id.* Following this response, the ’828 Patent was allowed. *Id.* at 314. The prosecution history therefore shows that a POSITA would readily understand that the sensor and memory are “tightly coupled” where they are electrically or physically coupled in the device, which prevents the data stream cannot be altered before authentication information is generated. EX2005 at 60.

Petitioner’s proposed construction mirrors the District Court’s tentative claim construction, which observed that “the prosecution history discloses a ‘conductive trace or lead’ as accomplishing the coupling.” EX1002 at 10-11. However, as previously shown, there was no clear and unmistakable disclaimer limiting the physical, electrical connections within the device only to conductive traces or leads, which are merely exemplary embodiments of physical, electrical connections within the device. *Thorner*, 669 F.3d at 1366–67; *Cont’l Cirs.*, 915 F.3d at 799. In addition, Patent Owner’s proposed construction is similar to Petitioner’s proposed construction in the District Court, which asserted that the term meant “a sensor that is connected to said memory within a device.” EX1020 at 9.

For these reasons, and based upon a proper reading of the prosecution history, the Board should construe this limitation as meaning “a sensor that is electrically or physically coupled to memory in a device.”

B. “monitoring the integrity of the tight coupling between said memory and said sensor” (cl. 1)

Petitioner asserts that the term “monitoring the integrity of the tight coupling between said memory and said sensor” means “determining whether physical access has been gained to the coupling between said memory and said sensor.” Pet. at 11. However, the claim term requires “monitoring... the tight coupling” between the memory and the sensor specifically. Petitioner’s construction is improper because the claim language explicitly requires monitoring the *physical coupling* between the memory and the sensor as opposed to some third structure.

Indeed, the specification of the ’828 Patent emphasizes that the tight coupling between the sensor and the memory is specifically monitored. For example, the specification states, “During the operation of the camera, internal security 14 is monitored to detect the integrity of the tight coupling of the sensor set and the recorder 6.” EX1001 at 4:65-67. The system performs a check of internal security system 14 to determine if a violation has been recorded. *Id.* at 5:44-46. If security is compromised, a security violation is appended to the image. *Id.* at 6:64-66. As

such, security in the specification and the preferred embodiment is specifically centered upon the physical coupling between the sensor and memory.

Consistent with the specification, the claim language itself 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.” EX1001 at claim 1. Similarly, the prosecution history for the ’828 Patent is specifically focused on monitoring the specific connection between the sensor and the memory, stating, “a signal is generated if the device that prevents physical access to the *interconnections between the sensor set and memory* is broken.” EX1002 at 5 (emphasis added).

The District Court’s tentative claim construction opinion also emphasizes that it is the physical coupling between the memory and the sensor. The District Court states, “monitoring involves determining whether the *physical coupling has been accessed or disturbed*.” EX1020 at 12 (emphasis added). Although the District Court’s tentative construction utilizes the language proposed by Petitioner, the “has been gained” language in the construction injects ambiguity by making it unclear whether monitoring requires making the specific determination that the coupling between the sensor and memory has been disturbed.

Consistent with the District Court’s tentative claim construction opinion, and with the explicit claim language, a POSITA would understand that this language specifically requires monitoring the *physical coupling* between the sensor and the

memory. Accordingly, “monitoring the integrity of the tight coupling between said memory and said sensor” should be construed to mean “determining whether the physical coupling between said memory and said sensor has been accessed or disturbed.”

C. “based on” (cl. 1)

The Petition identifies the term “based on” which is in claim 1 for claim construction. Pet at 11-14. However, Petitioner never identifies a proposed construction for this term. Instead, Petitioner argues that “based on” is an open-ended term. However, “[o]pen-ended claims are not inherently improper; as for all claims their appropriateness depends on the particular facts of the invention, the disclosure, and the prior art.” *Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1376 (Fed. Cir. 2007) quoting *Scripps Clinic & Research Found. v. Genentech, Inc.*, 927 F.2d 1565, 1572 (Fed. Cir. 1991). Here, the parameters are clearly described in the specification as “representative of at least one condition under which the digital sample was acquired.” EX1001 at 1:54-57. The specification then provides several examples of a parameter such as “date, time, latitude, longitude, altitude, roll, pitch, yaw, and compass heading, [as well as] camera identification, image sequence number, flash status, lens zoom factor, counter vibration status, focus status and focus quality.” *Id.* at 2:67-3:6. A POSITA would clearly understand this term in the context of the claims and the specification,

and therefore this term is not indefinite. This is further confirmed by the district court's tentative claim construction ruling, which found this term to be not indefinite. EX1020 at 18. Because the Petition does not propose a construction for this term, however, this response presumes that it has its plain and ordinary meaning and does not otherwise require construction.

V. PETITIONER HAS FAILED TO DEMONSTRATE THAT ANY OF THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Glass Fails to Render Obvious the Challenged Claims

1. Claim 1

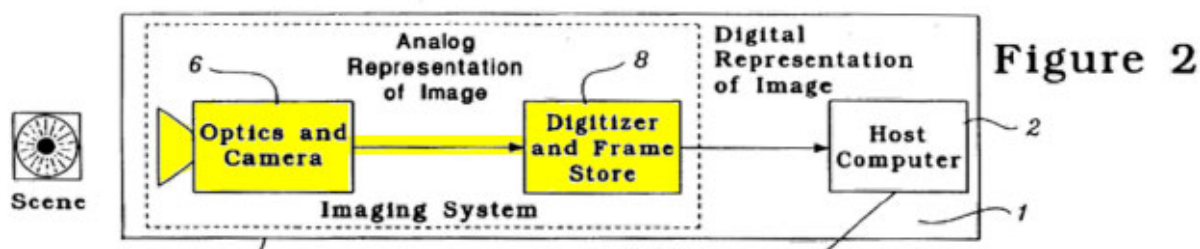
(a) Glass Fails to Disclose a “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter” under Petitioner’s own Proposed Claim Construction [limitation 1b]

As discussed above, Petitioner and Patent Owner dispute the claim construction that applies to the claim language “a sensor, which is tightly coupled to said memory.” *See supra* at IV.A. However, under either construction, Petitioner fails to show that Glass discloses this limitation.

Petitioner asserts that the claim language “a sensor, which is tightly coupled to said memory” should be construed as “a sensor coupled to said memory *via conductive traces or leads*.” Pet. at 9-10. However, neither Petitioner nor Petitioner’s expert identifies any teaching in Glass showing that the sensor (or camera) is coupled to the memory via “conductive traces or leads.” Pet. at 26-29.

Rather, Petitioner asserts that Glass teaches that the sensor and memory are coupled by “conductive leads or traces.” Pet. at 26-27. However, Petitioner cites no specific language from Glass which discusses how the sensor and the memory are coupled, whether by the specific requirement in Petitioner’s construction requiring conductive leads and traces or otherwise. Rather than citing evidence disclosing conductive traces or leads in Glass, Petitioner instead summarily cites to the declaration of its expert, Dr. Xiong. *Id.* However, Dr. Xiong likewise fails to identify anything in Glass showing that the sensor and the memory are coupled by conductive leads and traces. EX1003 at ¶¶170-176; EX2005 at ¶70.

First, Dr. Xiong cites Figure 2 of Glass, which merely illustrates a connection (via an arrow) between “Optics and Camera 6” and “Digitizer and Frame Store 8” in Glass:



EX1003, Fig. 2 (Portion, annotated by Petitioner)

Id. at ¶170. However, nothing in Figure 2 of Glass discloses that the connection between Optics and Camera 6 and Digitizer and Frame Store 8 is by conductive traces or leads. Nor is there any discussion in the specification describing any

physical aspects of the connection between Optics and Camera 6 and Digitizer and Frame Store 8. EX2005 at ¶71.

Dr. Xiong conclusorily argues, without providing any citation or evidence, that these components “are connected by electrically conductive leads or traces, most likely on a circuit board.” EX1003 at ¶170. However, Glass has no recitation identifying that the connection is by electrically conductive leads or traces, since the terms “leads” and “traces” are used nowhere in Glass. Nor does Glass have any discussion of circuit boards. Importantly, other patents from this time frame disclose connecting electronic cameras to either processors or memory by cables rather than by conductive traces or leads. *See, e.g.*, EX2007 (US Patent No. 5,486,853) (generally disclosing an electrical cable for connecting an electronic camera to a processor); EX2005 at ¶72. Because a POSITA would know that there were many ways to connect a CCD camera to either a processor or memory, Dr. Xiong has not shown that Glass teaches that the specific connection between Optics and Camera 6 and Digitizer and Frame Store 8 is by conductive traces or leads. EX2005 at ¶72.

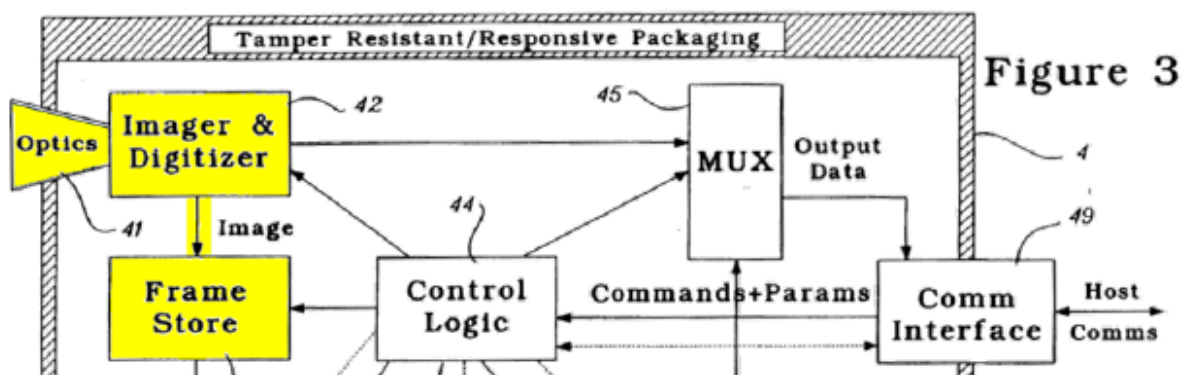
Still further, a POSITA would understand that a data path between a sensor and memory could be made without even having a physical connection. EX2005 at ¶73. For example, computing devices connected to the Internet will have a data path for share information between the computers. However, computers connected through the Internet, although having a data path to share information, are not

connected by “conductive leads or traces.” More specifically, it was known at the time of the ’828 Patent that a digital camera could include a wireless interface for wirelessly transmitting image information from the camera, with such transmission obviously not being by conductive traces or leads. *See, e.g.*, EX2008 (US Patent No. 7,161,622) (generally disclosing an electronic camera with a wireless communication interface for transmitting image information from the camera); EX2005 at ¶73. Furthermore, several Wi-Fi standards, including the 802.11a standard and the 802.11b standard, were available prior to the filing of the ’828 Patent. EX2001 at 8 (listing the approval dates for IEEE standards, including IEEE Std. P802.11a-1999 as early as September 16, 1997 and IEEE Std. P802.11b-1999 as early as December 9, 1997); EX2005 at ¶73. Communications over Wi-Fi, which are wireless, would involve the sharing of information through a data path, but a POSITA would readily appreciate that such wireless data paths would not involve “conductive traces or leads” under any meaningful interpretation of that language. EX2005 at ¶73.

To take a still further example, satellite-based internet service providers allow computers to establish data paths that are not even confined to the Earth’s atmosphere, much less an electrical connection or a connection by conductive leads or traces. *See, e.g.*, EX2009 (US Patent No. 6,377,981) (generally disclosing a system providing high-speed internet access through satellite communication links);

EX2005 at ¶74. As such, merely identifying that an *operational* data path exists between two components is not sufficient to show that the *physical* connection between the components is by “conductive leads or traces” as Petitioner’s own claim construction requires. Thus, communications by satellite, similar to communications over Wi-Fi, would readily be appreciated by a POSITA as not involving “conductive traces or leads” for similar reasons. EX2005 at ¶74.

Second, Dr. Xiong next cites Figure 3 of Glass, which merely illustrates a connection (via an arrow) between “Imager & Digitizer 42” and “Frame Store 43” in Glass:



EX1003, Fig. 3 (Portion, annotated by Petitioner)

Id. at ¶171. For the same reasons as explained above in relation to Figure 2, nothing in Figure 3 of Glass demonstrates that the connection between Imager and Digitizer 42 and Frame Store 43 is by conductive traces or leads. EX2005 at ¶75. Furthermore, the specification of Glass likewise fails to describe the specific details explaining how the connection between these components are made. Nor does the

specification of Glass disclose any further detail on the physical details of this connection. In the only discussion of the connection between the Imager and Digitizer to the Frame Store, Glass merely states, without detail, that “[t]he digital image is sent to a multiplexer 45 and/or a frame store memory 43.” EX1005 at 5:52-54. Furthermore, Dr. Xiong’s declaration concedes that Figure 3 of Glass only depicts that there is a “data path from the sensor to memory.” *Id.* at ¶171. However, the existence of a data path is not sufficient to show a connection by “conductive leads or traces” as Petitioner’s construction requires. For example, as explained above, other patents from this time frame disclose connecting electronic cameras to either processors or memory by cables rather than by conductive traces or leads. *See, e.g.,* EX2007 (US Patent No. 5,486,853) (generally disclosing an electrical cable for connecting an electronic camera to a processor); EX2005 at ¶75. Also, as explained above, data paths utilizing Wi-Fi and satellite-based communications were also known at the time of the ’828 Patent. EX2005 at ¶¶73-74.

Third, Dr. Xiong cites the prosecution history of the ’828 Patent as allegedly supporting his argument that Glass discloses this element. EX1003 at ¶¶173-175; Pet. at 27. However, nothing in the prosecution history is directed to Glass. EX2005 at ¶76. Dr. Xiong essentially makes an overly broad and untenable argument that because Figure 2A of the ’828 Patent connects the CCD Sensor through Processor 157 to 3.5” Floppy Drive Recorder using lines, and because the Patentee stated

during prosecution that Fig. 2A illustrates a tight coupling between the processor and the memory, that the lines in Glass would also disclose a tight coupling. EX 1003 at ¶¶173-175. There are at least two problems with Dr. Xiong's argument. First, Dr. Xiong cites a portion of the prosecution history where the Patentee asserts that Fig 2A discloses a tight connection, but this portion of the prosecution history does not assert that the connection between the processor and the floppy drive recorder is by conductive leads or traces. EX1003 at ¶172; EX1002 at 277; EX2005 at ¶76. Second, a POSITA would also know that floppy drives were typically connected to a processor using floppy cables to connect the floppy drive to the motherboard at the time of the '828 Patent. *See, e.g.*, EX2010 (Wikipedia entry for "floppy disk drive interface") (describing and depicting the ribbon cable typically used to connect 3.5 inch floppy drives to standard computer motherboards); EX2005 at ¶76. However, during his deposition, Dr. Xiong stated that he was unable to determine whether cables generally, nor floppy cables specifically, were connections by "conductive traces or leads"). EX2012 (Xiong Tr.) at 32:14-22; 64:22-25. As such, Petitioner's prosecution history argument is inconsistent with both the statements made during prosecution, which did not involve Glass, as well as the teachings of the '828 Patent itself, which involved cables. EX1003 at ¶¶172-175; EX2005 at ¶76.

Finally, Dr. Xiong asserts that Glass's statement that "data paths are shown in solid lines," indicates to a POSITA that the sensor and memory in Glass are connected via conductive traces or leads. EX1003 at ¶175. However, as previously explained, merely identifying that an *operational* data path exists between two components is not sufficient to show that the *physical* connection between the components is by "conductive leads or traces." EX2005 at ¶77. Even if the arrows between the components illustrated in the Figure 3 of Rieger illustrate the capability of the components to send and receive information, these arrows do not disclose any aspects of the *physical* connection between the components, whether by "conductive leads or traces." *Id.*

Patent Owner proposes an alternative claim construction requiring "a sensor that is electrically or physically coupled to memory in a device." *Supra* at IV.A. Even under this construction, however, Petitioner and its expert fail to show that Glass teaches this limitation for reasons similar to those presented for Patent Owner's construction. First, the arrows depicted in Figs. 2 and 3 of Glass depict an *operational* connection to convey data between components. Nor is there any discussion in the specification describing any physical aspects of the connection between the sensor and memory components identified in these figures. EX2005 at ¶78. As explained above, wireless Wi-Fi connections and satellite communications represent *operational* data paths, consistent with Glass, known at the time that would

not provide a *physical* connection between the components as required in Patent Owner's proposed construction. EX2005 at ¶78. Glass therefore fails to teach this element under Patent Owner's claim construction as well for similar reasons.

Because Petitioner fails to show that Glass discloses "a sensor, which is tightly coupled to said memory" under Petitioner's own proposed claim construction, the Petition fails to show that Glass teaches limitation 1b of claim 1.

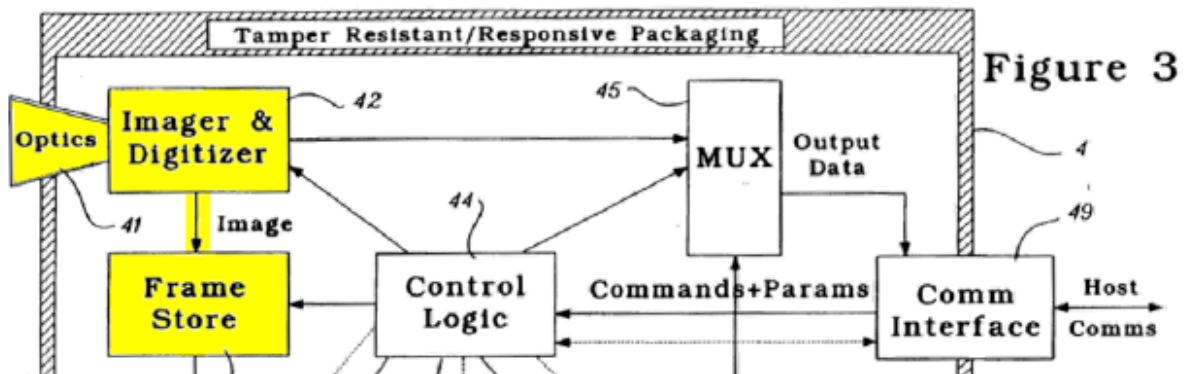
(b) Glass Fails to Disclose "monitoring the integrity of the tight coupling between said memory and said sensor" under Petitioner's own Proposed Claim Construction [limitation 1c]

As discussed above, Petitioner asserts that this limitation should be construed to mean "determining whether physical access has been gained to the coupling between said memory and said sensor." *Supra* at IV.B. Patent Owner, on the other hand, asserts that this limitation should be construed to mean "determining whether the physical coupling between said memory and said sensor has been accessed or disturbed." *Id.* However, both constructions require monitoring the specific coupling between the memory and the sensor and determining when that specific coupling has been accessed or disturbed. EX2005 at ¶79. Glass fails to teach this limitation because Glass monitors "tamper resistant package 50," but monitoring this *package* fails to teach monitoring the *coupling* between the sensor and memory specifically as the limitation requires. *Id.*

As explained above, the specification of the '828 Patent repeatedly emphasizes that the *coupling* between the sensor and the memory is *specifically monitored* in order to find a security violation. *Supra* at IV.B. For example, the specification states, “During the operation of the camera, internal security 14 is monitored to detect the *integrity of the tight coupling of the sensor set and the recorder 6.*” EX1001 at 4:65-67 (emphasis added). The system performs a check of internal security system 14 to determine if a violation has been recorded. *Id.* at 5:44-46. If security is compromised, a security violation is appended to the image. *Id.* at 6:64-66. Consequently, monitoring the specific connection between the sensor and the memory is the touchstone for this element as taught in the specification of the '828 Patent. EX2005 at ¶80.

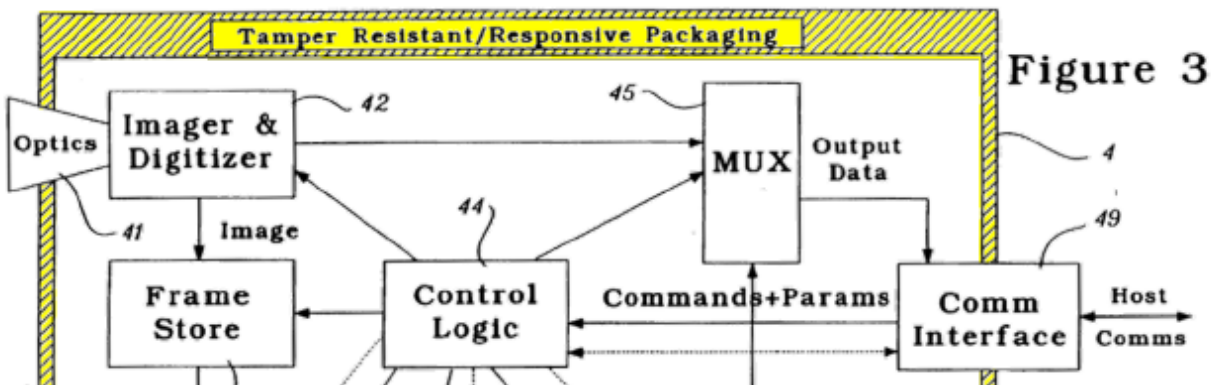
Petitioner attempts to equate monitoring the coupling itself with monitoring tamper-resistant package 50 in Glass. Pet. at 30; EX1003 at ¶181. However, the claim does not recite “monitoring the integrity of *a package that includes* the tight coupling between said memory and said sensor,” but rather “monitoring the integrity *of the tight coupling* between said memory and said sensor” as written. Glass therefore fails to disclose the claimed limitation because it discloses monitoring something other than the coupling, namely, a tamper resistant package. EX2005 at ¶81.

A comparison of different portions of Figure 3 utilized by Petitioner itself illustrates the difference. For example, Petitioner highlights the coupling between the sensor and the memory in Glass as shown below:



Glass, Fig. 3 (highlighting from Pet. at 26)

However, for this element, Petitioner explicitly does not monitor the coupling between the sensor and the memory highlighted above, as the claim recites, but rather instead monitors a tamper resistant package as illustrated below.



Glass, Fig. 3 (highlighting from Pet. at 31)

As such, the Petition itself shows that Glass does not “monitor[] the integrity of the tight coupling between said memory and said sensor” as the ’828 Patent requires.

Furthermore, the limitation is directed to the “*integrity* of the tight coupling,” but nothing in the description of the tamper-resistant package is directed to verifying the integrity of the tight coupling between the sensor and the memory specifically. EX1005 at 5:13-41. Petitioner’s expert, Dr. Xiong states that “that the intrusion detection is in effect at all times.” EX1003 at ¶244. However, this monitoring of the *packaging* is not monitoring the integrity of the *coupling* as the limitation specifically requires. EX2005 at ¶83.

Because Petitioner fails to show that Glass discloses “monitoring the integrity of the tight coupling between said memory and said sensor,” the Petition fails to show that Glass teaches limitation 1c of claim 1.

(c) Glass Fails to Disclose “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic” [limitation 1g]

Glass fails to disclose this limitation. More specifically, in the event the data stream is determined not to be authentic, the limitation requires “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic.” However, Glass fails to generate any signal that is displayed to a user *when the error is detected*. Rather, as Petitioner concedes, Glass only discloses maintaining a “record of the transaction” on the server. EX1005 at 10:54-58. Petitioner argues that this “describes maintaining a log file recording each step of the image authentication process.” Pet. at 36. However, this only means, even under

Petitioner's argument, that a *file* on the *server* is updated with the result of each transaction, not that an error signal is displayed to the user *when* the error signal is generated (i.e., when the error is detected by the system) as the claim limitation requires.

Log files are generally understood to be “computer file[s] that contains a record of all actions that have been done on a computer.” EX2011 (Cambridge Dictionary). Because the log file only records events, these events are not displayed to the user at the time that the event occurs. EX2005 at ¶85. Instead, a user is only informed of the events recorded in the file when the user opens the file, which can occur long after the time the event takes place. This is confirmed in Glass, which notes that the log file includes a time stamp to show when the event occurred because the user viewing the log file would only see events in the past. EX1005 at 9:61-64 (“We prefer to log *each step* of the transaction as indicated by the word Log. We also prefer to provide a clock 18 which is used in checking time-stamped data as well as recording the time of *each transaction*.”). Additionally, there is no disclosure in Glass describing that it would be “displayed to the user” as opposed to merely being logged in the file with the results of all other transactions. *Id.*

Nor does Petitioner's expert dispute that the log files present historic events that have already occurred as opposed to presenting the signal to the user *when the signal is generated*. Specifically, Dr. Xiong states that “one primary reason for

storing an indication of an unauthenticated image in a ‘Log’ file would be to present a record of the error to a system administrator or other user.” EX1003 at ¶205. However, presenting a *record* of events necessarily means that the record provides only historical information on events that have already occurred. The claim language itself requires “generating an error signal that *is displayed* to a user to indicate that said stored data stream is not authentic.” This requires displaying the error signal *when* the error signal is generated. EX2005 at ¶86. Petitioner and its expert attempt to improperly rewrite to limitation to require “generating an error signal that *will be displayed* to a user to indicate that said stored data stream is not authentic.” However, Glass’s log files do not display the error signal to the user when the error signal is generated as the limitation, as written, explicitly requires.

Because Petitioner fails to show that Glass discloses “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic,” the Petition fails to show that Glass teaches limitation 1g of claim 1.

(d) Glass Fails to Disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic” [limitation 1g]

Glass fails to disclose this limitation for the same reasons as for limitation 1g. *See supra* at V.A.1.c. More specifically, this limitation requires “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.” However, Glass fails to generate any signal that is displayed to a user *when the data*

is authenticated. Glass only discloses maintaining a “record of the transaction” on the server. EX1005 at 10:54-58. Petitioner argues that this “describes maintaining a log file recording each step of the image authentication process.” Pet. at 38. However, as above, this only means, even under Petitioner’s argument, that a *file* on the *server* is updated with the result of each transaction, not that an error signal is displayed to the user *when* the signal representing the authentication determination is generated (i.e., when the image is authenticated by the system) as the claim limitation requires.

Log files are generally understood to be “computer file[s] that contains a record of all actions that have been done on a computer.” EX2011 (Cambridge Dictionary). Because the log file only records events, these events are not displayed to the user at the time that the event occurs. EX2005 at ¶88. Instead, a user is only informed of the events recorded in the file when the user opens the file, which can occur long after the time the event takes place. This is confirmed in Glass, which notes that the log file includes a time stamp to show when the event occurred because the user viewing the log file would only see events in the past. EX1005 at 9:61-64 (“We prefer to log *each step* of the transaction as indicated by the word Log. We also prefer to provide a clock 18 which is used in checking time-stamped data as well as recording the time of *each transaction*.”). Additionally, there is no

disclosure in Glass describing that it would be “displayed to the user” as opposed to merely being logged in the file with the results of all other transactions. *Id.*

Nor does Petitioner’s expert dispute that the log files present historic events that have already occurred as opposed to presenting the signal to the user ***when the signal is generated***. Specifically, Dr. Xiong states that “one primary reason for storing an indication of an unauthenticated image in a ‘Log’ file would be to present a record of the error to a system administrator or other user.” EX1003 at ¶209. However, presenting a ***record*** of events necessarily means that the record provides only historical information on events that have already occurred. The claim language itself requires “generating an ok signal that ***is displayed*** to a user to indicate that said stored data stream is authentic.” This requires displaying the ok signal ***when*** the ok signal is generated. Ex2005 at ¶89. Petitioner and its expert attempt to improperly rewrite to limitation to require “generating an ok signal that ***will be displayed*** to a user to indicate that said stored data stream is authentic.” However, Glass’s log files do not display the ok signal to the user when the ok signal is generated as the limitation, as written, explicitly requires.

Because Petitioner fails to show that Glass discloses “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic,” the Petition fails to show that Glass teaches limitation 1h of claim 1.

2. Claims 2-6

Claims 2 through 6 depend from claim 1. Ex. 1001, cls. 2-6. Petitioner's arguments in Ground 1 for claims 2 through 6 are therefore based on Petitioner's arguments for Ground 1, claim 1, from which they depend, which fail as discussed above. Pet. at 38-41; *supra*, V.A.1.a-V.A.1.d. Thus, Petitioner has not demonstrated that claims 2 through 6 are invalid.

B. Ground 2: Rieger Fails to Render Obvious the Challenged Claims

1. Claim 1

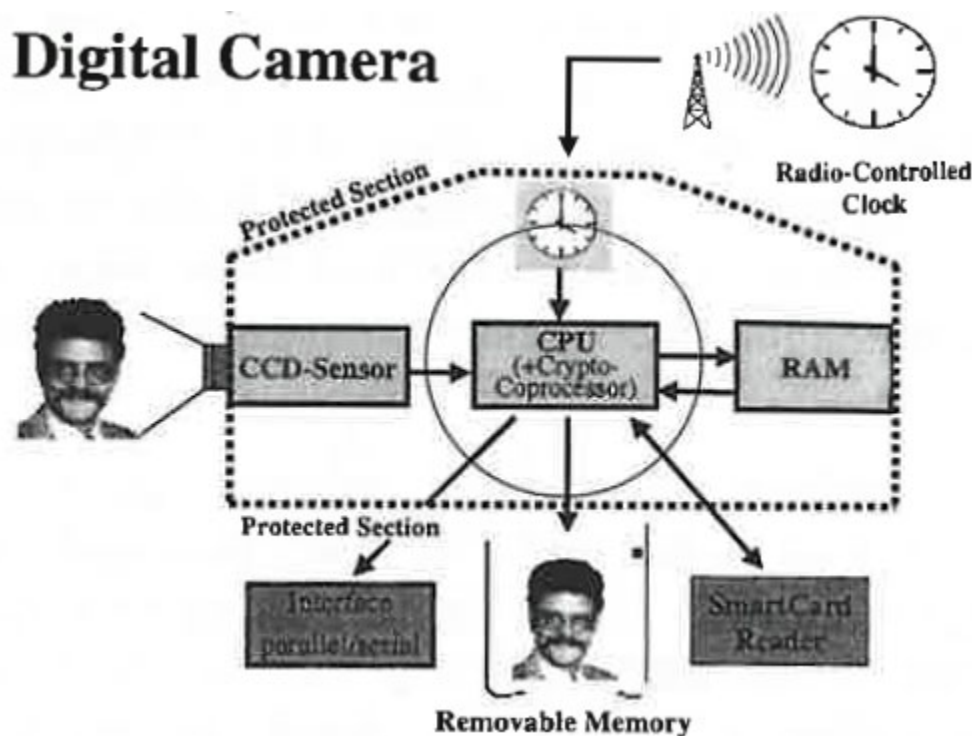
- (a) **Rieger Fails to Disclose a “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter” under Petitioner’s own Proposed Claim Construction [limitation 1b]**

Rieger fails to meet this limitation for similar reasons as Glass. *See supra*. at V.A.1.a. As discussed above, Petitioner and Patent Owner dispute the claim construction that applies to the claim language “a sensor, which is tightly coupled to said memory.” *See supra* at IV.A. However, under either construction, Petitioner fails to show that Rieger discloses this limitation.

Petitioner asserts that the claim language “a sensor, which is tightly coupled to said memory” should be construed as “a sensor coupled to said memory *via conductive traces or leads*.” Pet. at 9-10. However, neither Petitioner nor Petitioner's expert identifies any teaching in Rieger showing that the sensor (or camera) is coupled to the memory via “conductive traces or leads.” Pet. at 43-46.

Rather, Petitioner asserts, conclusorily, that Rieger teaches that the sensor and memory are coupled by “conductive leads or traces.” Pet. at 44. However, Petitioner cites no specific language from Rieger which discusses how the sensor and the memory are coupled, whether by the specific requirement in Petitioner’s construction requiring conductive traces or leads, or otherwise. Rather than citing evidence disclosing conductive traces or leads in Rieger, Petitioner instead summarily cites to the declaration of its expert, Dr. Xiong. *Id.* However, Dr. Xiong likewise fails to identify anything in Rieger showing that the sensor and the memory are coupled by conductive traces or leads. EX1003 at ¶¶228-234; EX2005 at ¶92.

First, Dr. Xiong cites Figure 3 of Rieger, which merely illustrates a connection (via an arrow) between several components including a CCD sensor, a CPU, RAM, and an internal clock in Rieger:



Rieger, Figure 3

See EX1003 at ¶228. However, nothing in Figure 3 of Rieger discloses that the connection between the CCD sensor, the CPU, or the RAM is by conductive traces or leads. Nor is there any discussion in the Rieger describing any physical aspects of the connection between the CCD sensor, the CPU, or the RAM. EX2005 at ¶93.

Dr. Xiong conclusorily argues, without providing any citation or evidence, that these components “are electrically connected by conductive leads or traces within the protected section of Rieger’s manipulation-proof camera.” EX1003 at ¶228. However, Rieger has no recitation identifying that the connection is by electrically conductive leads or traces, since the terms “leads” and “traces” are used nowhere in Rieger. Importantly, other patents from this time frame disclose

connecting electronic cameras to either processors or memory by cables rather than by conductive traces or leads. *See, e.g.*, EX2007 (US Patent No. 5,486,853) (generally disclosing an electrical cable for connecting an electronic camera to a processor); EX2005 at ¶94. Because a POSITA would know that there were many ways to connect a CCD sensor to either a processor or memory, Dr. Xiong has not shown that Rieger teaches that the specific connection between the CCD Sensor and the RAM illustrated in Figure 3 is by conductive traces or leads. EX2005 at ¶94.

Still further, a POSITA would understand that a data path between a sensor and memory could be made without even having a physical connection. EX2005 at ¶95. For example, computing devices connected to the Internet will have a data path for share information between the computers. However, computers connected through the Internet, although having a data path to share information, are not connected by “conductive leads or traces.” More specifically, it was known at the time of the ’828 Patent that a digital camera could include a wireless interface for wirelessly transmitting image information from the camera, with such transmission obviously not being by conductive traces or leads. *See, e.g.*, EX2008 (US Patent No. 7,161,622) (generally disclosing an electronic camera with a wireless communication interface for transmitting image information from the camera); EX2005 at ¶95. Furthermore, several Wi-Fi standards, including the 802.11a standard and the 802.11b standard, were available prior to the filing of the ’828

Patent. EX2001 at 8 (listing the approval dates for IEEE standards, including IEEE Std. P802.11a-1999 as early as September 16, 1997 and IEEE Std. P802.11b-1999 as early as December 9, 1997); EX2005 at ¶95. Communications over Wi-Fi, which are wireless, would involve the sharing of information through a data path, but a POSITA would readily appreciate that such wireless data paths would not involve “conductive traces or leads” under any meaningful interpretation of that language. EX2005 at ¶95.

To take a still further example, satellite-based internet service providers allow computers to establish data paths that are not even confined to the Earth’s atmosphere, much less an electrical connection or a connection by conductive leads or traces. *See, e.g.*, EX2009 (US Patent No. 6,377,981) (generally disclosing a system providing high-speed internet access through satellite communication links); EX2005 at ¶96. As such, merely identifying that an *operational* data path exists between two components is not sufficient to show that the *physical* connection between the components is by “conductive leads or traces” as Petitioner’s own claim construction requires. Thus, communications by satellite, similar to communications over Wi-Fi, would readily be appreciated by a POSITA as not involving “conductive traces or leads” for similar reasons. EX2005 at ¶96.

Second, Dr. Xiong cites the prosecution history of the ’828 Patent as allegedly supporting his argument that Rieger discloses this element. EX1003 at ¶¶229-232;

Pet. at 45-46. However, nothing in the prosecution history is directed to Rieger. EX2005 at ¶97. Dr. Xiong essentially makes an overly broad and untenable argument that because Figure 2A of the '828 Patent connects the CCD Sensor through Processor 157 to 3.5" Floppy Drive Recorder using lines, and because the Patentee stated during prosecution that Fig. 2A illustrates a tight coupling between the processor and the memory, that the arrows in Rieger would also disclose a tight coupling. EX 1003 at ¶¶229-232. However, there are at least two problems with Dr. Xiong's argument. First, Dr. Xiong cites a portion of the prosecution history where the Patentee asserts that Fig 2A discloses a tight connection, but this portion of the prosecution history does not assert that the connection between the processor and the floppy drive recorder is by conductive leads or traces. EX1003 at ¶229; EX1002 at 277; EX2005 at ¶97. Second, a POSITA would also know that floppy drives were typically connected to a processor using floppy cables to connect the floppy drive to the motherboard at the time of the '828 Patent. *See, e.g.*, EX2010 (Wikipedia entry for "floppy disk drive interface") (describing and depicting the ribbon cable typically used to connect 3.5 inch floppy drives to standard computer motherboards); EX2005 at ¶97. However, Dr. Xiong stated that he was unable to determine whether cables generally, nor floppy cables specifically, were connections by "conductive traces or leads"). EX2012 (Xiong Tr.) at 32:14-22; 64:22-25. As such, Petitioner's prosecution history argument is inconsistent with both the

statements made during prosecution, which did not involve Rieger, as well as the teachings of the '828 Patent itself. EX1003 at ¶¶229-232; EX2005 at ¶97.

Finally, Dr. Xiong asserts that because Rieger's Figure 3 and Figure 2A of the '828 Patent "disclose[] the same arrangement with the same characteristics" the (unexplained) similarity in the figures that the sensor is tightly coupled to the memory in Rieger. EX1003 at ¶175. However, as previously explained, merely identifying that an *operational* data path exists between two components is not sufficient to show that the *physical* connection between the components is by "conductive leads or traces." EX2005 at ¶98. Even if the arrow between the components in Figure 3 of Rieger illustrate the capability of the components to send and receive information, these arrows do not disclose any aspects of the *physical* connection between the components, whether by "conductive leads or traces." *Id.*

Patent Owner proposes an alternative claim construction requiring "a sensor that is electrically or physically coupled to memory in a device." *Supra* at IV.A. However, even under this construction, Petitioner and its expert fail to show that Rieger teaches this limitation for reasons similar to those presented for Patent Owner's construction. First, the arrows in Figure 3 of Rieger depict an operational connection to convey data between components. Nor is there any discussion in Rieger describing any physical aspects of the connection between the sensor and memory components identified in these figures. EX2005 at ¶99. As explained

above, wireless Wi-Fi connections and satellite communications represent *operational* data paths, consistent with Rieger, known at the time that would not provide a *physical* connection between the components as required in Patent Owner's proposed construction. EX2005 at ¶99. Rieger therefore fails to teach this element under Patent Owner's claim construction as well for similar reasons.

Because Petitioner fails to show that Rieger discloses "a sensor, which is tightly coupled to said memory" under Petitioner's own proposed claim construction, the Petition fails to show that Rieger teaches limitation 1b of claim 1.

(b) Rieger Fails to Disclose "monitoring the integrity of the tight coupling between said memory and said sensor" under Petitioner's own Proposed Claim Construction [limitation 1c]

As discussed above, Petitioner asserts that this limitation should be construed to mean "determining whether physical access has been gained to the coupling between said memory and said sensor." *Supra* at IV.B. Patent Owner, on the other hand, asserts that this limitation should be construed to mean "determining whether the physical coupling between said memory and said sensor has been accessed or disturbed." *Id.* However, both constructions require monitoring the specific coupling between the memory and the sensor and determining when that specific coupling has been accessed or disturbed. EX2005 at ¶100. Rieger fails to teach this limitation because Rieger monitors a "protected compartment" located within the

camera, but monitoring this *compartment* fails to teach monitoring the *coupling* between the sensor and memory specifically as the limitation requires. *Id.*

As explained above, the specification of the '828 Patent repeatedly emphasizes that the *coupling* between the sensor and the memory is *specifically monitored* in order to find a security violation. *Supra* at IV.B. For example, the specification states, “During the operation of the camera, internal security 14 is monitored to detect the *integrity of the tight coupling of the sensor set and the recorder 6.*” EX1001 at 4:65-67 (emphasis added). The system performs a check of internal security system 14 to determine if a violation has been recorded. *Id.* at 5:44-46. If security is compromised, a security violation is appended to the image. *Id.* at 6:64-66. Consequently, monitoring the specific connection between the sensor and the memory is the touchstone for this element as taught in the specification of the '828 Patent. EX2005 at ¶101.

Petitioner attempts to equate monitoring the coupling itself with monitoring the so-called “secure compartment” in Rieger. Pet. at 48-49; EX1003 at ¶243. However, the claim does not recite “monitoring the integrity of *a compartment that includes* the tight coupling between said memory and said sensor,” but rather “monitoring the integrity of the tight coupling between said memory and said sensor” as written. Rieger therefore fails to disclose the claimed limitation because

it discloses monitoring something other than the coupling, namely, a secure compartment. EX2005 at ¶102.

Figure 3 of Rieger itself illustrates the difference between the claim limitation and Rieger. For this element, Petitioner relies upon a “secure compartment” (labeled as “Protected Section” in Figure 3) as illustrated below.

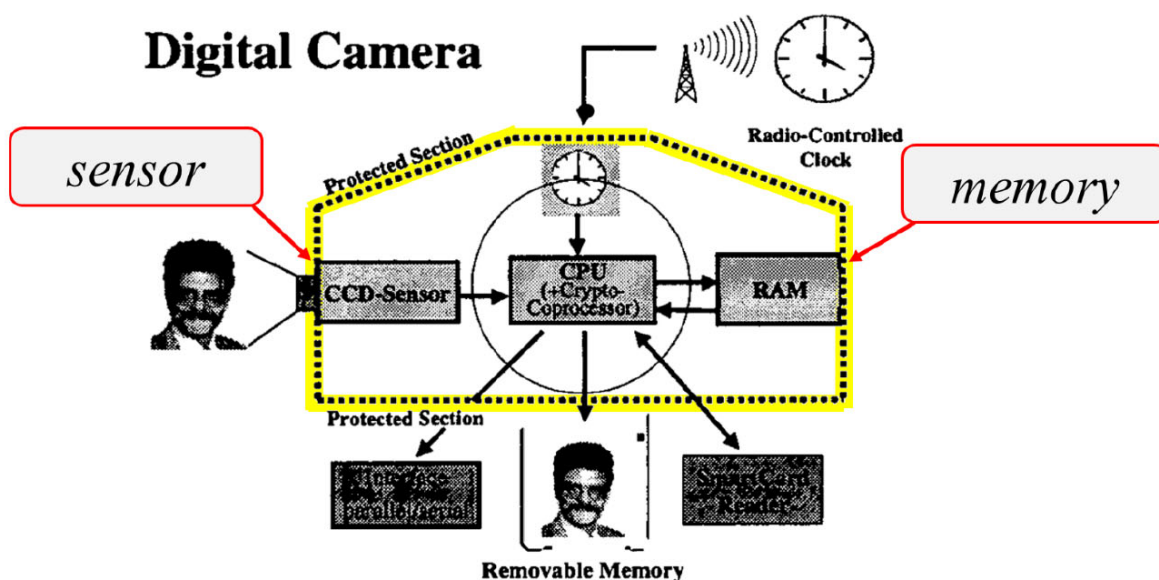


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

Rieger, Fig. 3 (highlighting and annotations from Pet. at 44)

As such, the Petition itself shows that Rieger does not “monitor[] the integrity of the tight coupling between said memory and said sensor” as the ’828 Patent requires. EX2005 at ¶103.

Because Petitioner fails to show that Rieger discloses “monitoring the integrity of the tight coupling between said memory and said sensor,” the Petition fails to show that Rieger teaches limitation 1c of claim 1.

(c) Rieger Fails to Disclose “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic” [limitation 1g]

Rieger fails to disclose this limitation. More specifically, in the event that the data stream is determined not to be authentic, the limitation requires “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic.” However, Rieger fails to disclose generating an error signal that is displayed to a user. Rather, Rieger only discloses comparing hash values, but there is no discussion in Rieger that describes actually generating an error signal that is displayed to the user based on the result of this comparison. EX1006 at 11-12. Instead, Rieger only describes comparing hash values in order to verify integrity of data; the disclosure in Rieger is silent as to whether, or if, that information is presented to users. *Id.* However, the actual communication to the user of an error is precisely the subject of this limitation. EX2005 at ¶104.

Petitioner and Petitioner’s expert rely upon a “frowning face image” shown in Figure 7 of Rieger as disclosing this limitation. Pet. at 55; EX1003 at ¶257. However, nothing in Figure 7 of Rieger, or in the text describing the Figure, indicates that the “frowning face image” is displayed to the user. EX2005 at ¶105. Figure 7

of Rieger illustrates the authentication process, but it does not address how, or even if, the user is notified of the result of the authentication process. *Id.* For example, Figure 7 also has “key” images, but there is no indication in Rieger that the “key” images are displayed to the user. *Id.* A POSITA would therefore understand that Figure 7 illustrates the authentication process, but it does not illustrate how the results of that process are communicated, if any.

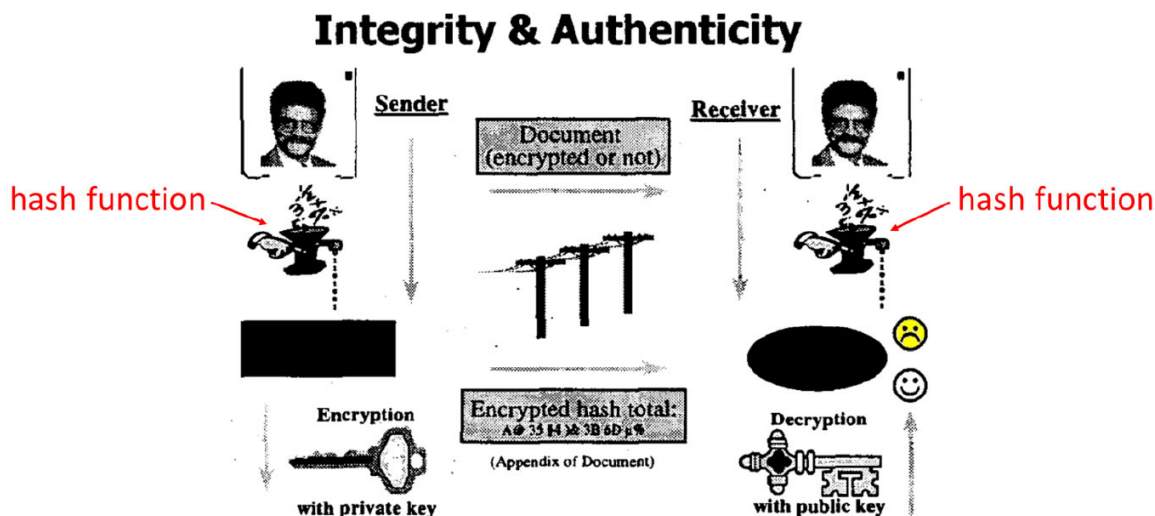


Figure 7: Principles of the integrity and authenticity test

Rieger, Fig. 7 (highlighting and annotations from Pet. at 55)

Because Petitioner fails to show that Rieger discloses “generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic,” the Petition fails to show that Rieger teaches limitation 1g of claim 1.

(d) Rieger Fails to Disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic” [limitation 1g]

Rieger fails to disclose this limitation for the same reasons as for limitation 1g. *See supra* at V.B.1.c. More specifically, in the event that the data stream is determined to be authentic, the limitation requires “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.” However, Rieger fails to disclose generating an ok signal that is displayed to a user. Rather, Rieger only discloses comparing hash values, but there is no discussion in Rieger that describes actually generating an ok signal that is displayed to the user. EX1006 at 11-12. Instead, the disclosure only describes comparing hash values in order to verify integrity of data; the disclosure in Rieger is silent as to whether, or if, that information is presented to users. *Id.* However, this *communication to the user* of an ok indication is precisely the subject of this limitation. EX2005 at ¶106.

Petitioner and Petitioner’s expert rely upon a “smiling face image” shown in Figure 7 of Rieger as disclosing this limitation. Pet. at 57; EX1003 at ¶260. However, nothing in Figure 7 of Rieger, or in the text describing the Figure, indicates that the “smiling face image” is displayed to the user. EX2005 at ¶107. Figure 7 of Rieger illustrates the authentication process, but it does not address how, or even if, the user is notified of the result of the authentication process. *Id.* For example, Figure 7 also depicts “key” images, but there is no indication in Rieger that the “key”

images are displayed to the user. *Id.* A POSITA would therefore understand that Figure 7 illustrates the authentication process, but it does not illustrate how the results of that process are communicated, if any.

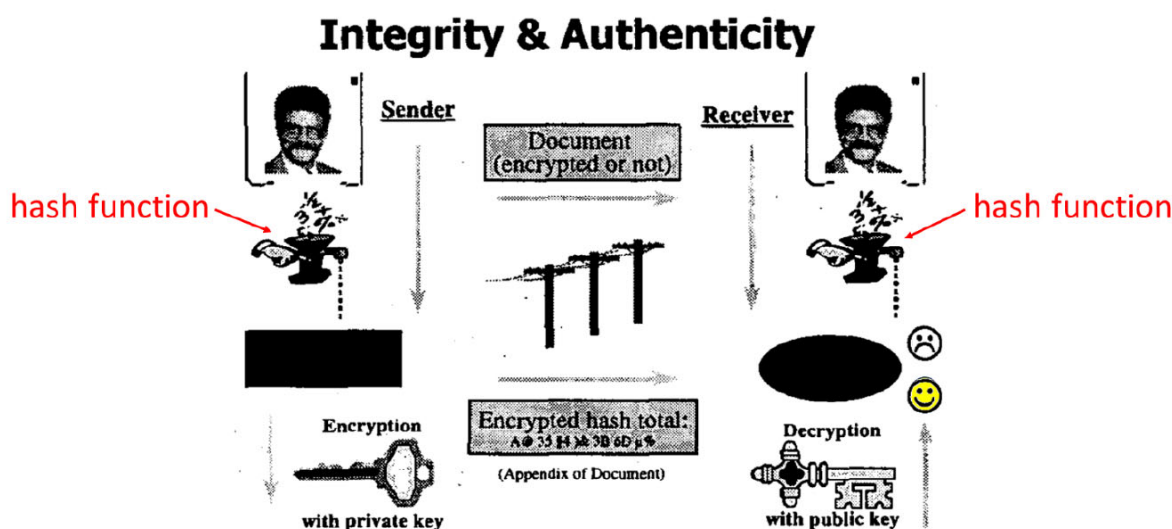


Figure 7: Principles of the integrity and authenticity test

Rieger, Fig. 7 (highlighting and annotations from Pet. at 57)

Because Petitioner fails to show that Rieger discloses “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic,” the Petition fails to show that Rieger teaches limitation 1h of claim 1.

2. Claims 2-6

Claims 2 through 6 depend from claim 1. Ex. 1001, cls. 2-6. Petitioner’s arguments in Ground 2 for claims 2 through 6 are therefore based on Petitioner’s arguments for Ground 1, claim 1, from which they depend, which fail as discussed

above. Pet. at 57-61; *supra*, V.B.1.a-V.B.1.d. Thus, Petitioner has not demonstrated that claims 2 through 6 are invalid.

C. Grounds 3-4: Exif 2.0 or Exif 2.1 Fail to Render Obvious the Challenged Claims

1. Claim 1

Petitioner's obviousness arguments in Grounds 3-4 for alleged obviousness of claim 1 are based on Petitioner's arguments that the Glass and Rieger references, discussed above relating to Grounds 1-2, respectively, invalidate claim 1. Pet. at 62. In fact, Petitioner advances no additional invalidity arguments relating to claim 1 based upon Exif 2.0 and Exif 2.1, merely citing to Petitioner's previous arguments and conclusorily stating that the references "provide more detail about the specific metadata fields available for digital cameras." *Id.* Petitioner's arguments fail as discussed above. *See supra* at V.A.1, V.B.1. More specifically, because Petitioner has failed to demonstrate that Glass and Rieger discloses each limitation of claim 1, Petitioner's arguments in Grounds 3-4 for claim 1 fail for the same reasons discussed above. *Id.*

2. Claims 2- 6

Claims 2 through 6 depend from claim 1. EX1001, cls. 2-6. Petitioner's arguments in Grounds 3-4 for claims 2 through 6 are therefore based on Petitioner's arguments for claim 1, from which they depend, which fail as discussed above. Pet.

at 62-67; *supra*, IV.A.1, IV.B.1. Thus, Petitioner has not demonstrated that claims 2 through 6 are invalid.

D. Grounds 5-8: Serret-Avila fails to Render Obvious the Challenged Claims

1. Claim 1

(a) Petitioner Fails to Show That It Would Have Been Obvious to Modify Glass and Rieger to add Serret-Avila

Petitioner argues it would have been obvious to modify Glass and Rieger to add Serret-Avila. Pet. at 67. However, Petitioner's obviousness theory suffers from several fatal flaws, none of which are addressed in Petitioner's purported motivation to combine.

First, Serret-Avila is non-analogous art and therefore does not "qualif[y] as prior art for an obviousness determination under § 103." *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011). A prior art reference is analogous prior art if: (1) "the art is from the same field of endeavor" or (2) "the reference [] is reasonably pertinent to the particular problem with which the inventor is involved." *Id.* A reference satisfies the "reasonably pertinent" test if "because of the matter with which it deals, [it] logically would have commended itself to an inventor's attention in considering his problem." *Id.* Petitioner makes no effort to show that Serret-Avila is analogous art under either prong of the test.

As to the first prong of the analogous art test, Serret-Avila clearly fails. Serret-Avila relates to a “verify[ing] the authenticity of [a] communication” by using “check values... constructed from the original content of the communication.” EX1011 at Abstract. Serret-Avila is not directed towards authenticating digital images, nor does Serret-Avila even reference authenticating digital photographs or images. *Id.*; EX2005 at ¶110. Glass, on the other hand, focuses on “securely transmitting biometric data over a network contains a sensor, preferably a camera.” EX1005 at Abstract; EX2005 at ¶110. Rieger focuses on “ensuring the integrity and authenticity of photographic images during the image-recording phase.” EX1006 at 1; EX2005 at ¶110.

A POSITA would therefore recognize that Serret-Avila is generally in the field of internet transaction or e-commerce security. EX2005 at ¶111. By contrast, a POSITA would recognize that Glass and Rieger are generally in the field of endeavor of digital imaging security. EX2005 at ¶111. A POSITA would regard the field of digital image validation as a separate field of endeavor from the field of internet security because validation of digital images to ensure the integrity and authenticity of the images involves unique problems specific to detecting manipulation of images. *See, e.g.*, EX1006 at 1 (“it is becoming increasingly difficult to detect and show proof of professional image manipulation aided by

digital methods.”). EX2005 at ¶111. A POSITA would therefore regard such fields as separate. EX2005 at ¶111.

As to the second prong of the analogous art test, regarding whether the reference “is reasonably pertinent to the particular problem with which the inventor is involved” Serret-Avila also fails. *In re Klein*, 647 F.3d at 1348. In the specification of the ’828 patent, the purpose of the “error signal” recited in limitation 1g and of the “ok signal” recited in limitation 1h is to inform the user whether or not the images include either errors or if security has been compromised. EX1001 at 8:45-50 (“ImageGuard appears if no internal errors are detected and the security is not compromised. NONVERIFIED (or other indication of compromise) appears if security is compromised within the system.”); EX2005 at ¶112. On the other hand, because Serret-Avila is not directed, and does not even discuss, authenticating digital images nor any aspects of security relating to digital images. *See, e.g.*, EX1006 at Abstract. EX2005 at ¶112. In light of these significant differences in field of use, purpose, problems solved, and manner of solution, Serret-Avila would not “have commended itself to an inventor’s attention in considering” the problems solved by the ’828 Patent.

In the Board’s Institution Decision (Paper No. 8, “DI”), the Board states that “informing users whether data has been compromised due to mis-matched hashes is the same problem Petitioner asserts Serret-Avila addresses.” *Id.* at 37. However,

the three references apply fundamentally different approaches to informing users as to how, or whether, they are informed of authentication determinations. Glass, utilizes an off-line system where a camera provides information to a remote server. EX1005 at 1:7-9. However, because the information is only provided to the remote server, a user is not necessarily able to receive notifications at the time any determination is made and recorded. *See* EX1005 at 9:61-64; EX2005 at ¶113. Serret-Avila, on the other hand, uses a warning display system, requiring online presence by a user to receive the warning display. EX1011 at 10:39-45; EX2005 at ¶113. And, finally, Rieger fails to disclose any means for informing users of the result of any authentication determination at all, whether by active, by record-based, or by any other possibility. EX2006 at 12. EX2005 at ¶113. As such, each reference follows divergent, and incongruent, paths for informing users of results (if any). EX2005 at ¶113. *See, e.g., In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994) (“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant [t]he degree of teaching away will of course depend on the particular facts”).

Consequently, Serret-Avila is not analogous art with Glass nor Rieger.

(b) Serret-Avila Fails to Disclose “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic” [limitation 1g]

Serret-Avila fails to disclose this limitation. More specifically, in the event that the data stream is determined to be authentic, the limitation requires “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.” However, Serret-Avila fails to disclose generating an ok signal that is displayed to a user. Petitioner asserts that when hash values are determined to be unauthentic that the system may display “a warning or error message” on a display. EX1011 at 10:39-45. However, there is no opposite message made to the user by the system in Serret-Avila when hash values are determined to be authentic. Nor does Petitioner or Petitioner’s expert identify any messaging to users when hash values are determined to be authentic. Rather, Petitioner and its expert acknowledge that, in the event that a sub-block of data is determined to be authentic, “the sub-block can be released for use.” Pet. at 70; EX1003 at ¶293. However, the release of the sub-block of data for use would not normally be displayed to the user. EX2005 at ¶115. Petitioner and its expert assert that “[b]y releasing the sub-block for use, the user is permitted to see or hear the authenticated sub-block, which is the equivalent of displaying an ok signal to the user.” Pet. at 71; EX1003 at ¶293. However, releasing the sub-block is not equivalent to an “ok” signal for at least three reasons. First, an image file, even if it utilized the system disclosed in Serret-Avila,

could be composed of multiple sub-blocks and, therefore, there would be no indication associated with each sub-block comprising the image. EX1006 at 8:36-38 (stating that the process of Fig. 3 “is repeated for each sub-block P_i of a data file (300), starting with the last sub-block of the file,” indicating that each file is composed of multiple sub-blocks). A POSITA would recognize that an image file would not be displayed when each sub-block is authenticated because the image itself is composed of multiple sub-blocks, each of which would be authenticated individually. EX2005 at ¶115. Second, as previously stated, Serret-Avila is not directed towards authenticating digital images, nor it even mention digital photographs or images. EX1011; EX2005 at ¶115. Third, Serret-Avila does not state that any data associated with a sub-block is actually provided to the user, either visually or otherwise. Rather, the sub-block is “released for use,” indicating that the sub-block may potentially be accessed by a user in the future but not that it is actually displayed or otherwise perceptible to the user at the time the sub-block is authenticated. EX1011 at 10:28-30; EX2005 at ¶115.

Rather, Serret-Avila only discloses comparing hash values, but there is no discussion in Rieger that describes actually generating an ok signal that is displayed to the user. EX1006 at 11-12. Instead, the disclosure only describes comparing hash values in order to verify integrity of data; the disclosure in Rieger is silent as to whether, or if, that information is presented to users. *Id.* However, this

communication to the user of an ok indication is precisely the subject of this limitation. EX2005 at ¶116.

Because Petitioner fails to show that Rieger discloses “generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic,” the Petition fails to show that Rieger teaches limitation 1h of claim 1.

VI. CONCLUSION

For the above reasons, Patent Owner requests that Board hold that all challenged claims are patentable.

Date: June 13, 2025

Respectfully submitted,

By: / Bryan D. Atkinson /
Bryan D. Atkinson (Reg. No. 52,574)
batkinson@dickinsonwright.com
DICKINSON WRIGHT PLLC
607 W. 3rd Street, Suite 2500
Austin, Texas 78701
Telephone: (512) 770-4208
Fax: (844) 670-6009
Counsel for Patent Owner

Certificate of Service 37 C.F.R. § 42.6(e)

The undersigned certifies that on June 13, 2025, I will cause true and correct copies of the foregoing Patent Owner's Response, and all associated exhibits or appendices referred to therein, to be served electronically upon the following attorneys who have consented to service via email. Pet. at 2-3.

James L. Day (Registration No. 72,681)
jday@fbm.com
Winston Liaw (Registration No. 78,766)
wliaw@fbm.com
Farella Braun + Martel LLP
One Bush Street, Suite 900
San Francisco, California 94104
Telephone: (415) 954-4400
Facsimile: (415) 954-4480

/ Bryan D. Atkinson /
Bryan D. Atkinson (Reg. No. 52,574)
batkinson@dickinsonwright.com
DICKINSON WRIGHT PLLC
607 W. 3rd Street, Suite 2500
Austin, Texas 78701
Telephone: (512) 582-6889
Fax: (844) 670-6009

Counsel for Patent Owner

Certificate of Compliance Pursuant to 37 C.F.R. § 42.24

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24.

This paper contains 10,717 words, excluding the parts of the paper exempted by 37 C.F.R. § 42.24(a).

This paper also complies with the typeface requirements of 37 C.F.R. § 42.6(a)(ii) and the type style requirements of 37 C.F.R. § 42.6(a)(iii)&(iv).

Dated: June 13, 2025

Respectfully submitted,

/ Bryan D. Atkinson /

Bryan D. Atkinson (Reg. No. 52,574)

batkinson@dickinsonwright.com

DICKINSON WRIGHT PLLC

607 W. 3rd Street, Suite 2500

Austin, Texas 78701

Telephone: (512) 582-6889

Fax: (844) 670-6009

Counsel for Patent Owner