

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

**DECLARATION OF BILL DAVIS
IN SUPPORT OF PATENT OWNER'S RESPONSE**

Table of Contents

I. INTRODUCTION 4

II. BACKGROUND AND QUALIFICATIONS 5

III. COMPENSATION 8

IV. MATERIALS CONSIDERED 8

V. UNDERSTANDING OF LEGAL PRINCIPLES 9

 A. Claim Construction 9

 B. Invalidity Based on Prior Art 10

 1. Prior Art 10

 2. Anticipation.....13

 3. Obviousness 15

VI. LEVEL OF ORDINARY SKILL IN THE ART 20

VII. OVERVIEW OF THE '828 PATENT 21

VIII. CLAIM CONSTRUCTION 22

 A. “a sensor, which is tightly coupled to said memory” (cl. 1).....22

 B. “monitoring the integrity of the tight coupling between said memory and said sensor” (cl. 1).....25

 C. “based on” (cl. 1).....27

IX. PETITIONER HAS FAILED TO DEMONSTRATE THAT ANY OF THE CHALLENGED CLAIMS ARE UNPATENTABLE 28

 A. Ground 1: Glass Fails to Render Obvious the Challenged Claims.....28

 1. Claim 1 28

 (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].....28

 (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]	36
(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]	40
(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]	42
B.	Ground 2: Rieger Fails to Render Obvious the Challenged Claims ...	44
1.	Claim 1	44
(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].....	44
(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].....	51
(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]	54
(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]	55
C.	Grounds 3-4: Exif 2.0 or Exif 2.1 Fail to Render Obvious the Challenged Claims	57
1.	Claim 1	57
D.	Grounds 5-8: Serret-Avila fails to Render Obvious the Challenged Claims.....	58
1.	Claim 1	58
(a)	Petitioner Fails to Show That It Would Have Been Obvious to Modify Glass and Rieger to add Serret- Avila.....	58

	(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]	61
X.	CONCLUSION.....	63

I. INTRODUCTION

1. I have been retained by Patent Owner Force Jonathan E. Jaffe (“Patent Owner” or “Jaffe”) in this *inter partes* review proceeding number IPR2024-01352 (“IPR”), filed by Petitioner Adobe Inc. (“Adobe” or “Petitioner”). I understand that this IPR proceeding involves U.S. Patent No. 6,757,828 (the ’828 patent) and that the challenged claims are claims 1-6 (the “Challenged Claims”).

2. I have been asked to provide my objective, independent analysis of the ’828 patent in view of the asserted prior art references cited in the Petition and to provide my opinion regarding the allegations in the Petition, as well as the supporting opinions of Dr. Zixiang Xiong.

3. I have based my opinions on the information available to me as of the date of this declaration. I understand that additional information may become available after this declaration is submitted. If I become aware of additional information following my submission of this declaration I may, if I am permitted, offer additional opinions (including by amending and/or supplementing this declaration) taking into account such new information.

4. I am not currently, nor have I ever been, an employee of Patent Owner. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent working on this IPR. I will not

receive any added compensation based on the outcome of this IPR, any other IPR, or any other proceeding involving the '828 patent.

II. BACKGROUND AND QUALIFICATIONS

5. I am currently a Partner and Lead Engineer at Syscall 7. My work focuses on computer information security, distributed analytical systems for network detection and response platforms, and enterprise dataflow management for indexing and search. I have over 20 years of experience building software for defense and industry applications.

6. In 1997, I received a Bachelor of Science with a double major in Mathematics and Computer Science from the University of Maryland, graduating as part of the Gemstone Honors Program. In 2006, I received my Master of Science in Computer Science from Johns Hopkins University. Since 2011, I have been a member of the Association for Computing Machinery.

7. I have been involved in research and technology in the area of embedded systems since 2002, building gunfire control systems and cutting-edge analytic systems for defense intelligence analysts. This included developing and deploying many software applications to embedded device platforms. My experience involves designing and implementing embedded device systems using various languages like C/C++, Java, Scala, and Python, and I have also designed and

implemented a number of embedded applications targeting network equipment like router and switches. These applications integrated with software signing mechanisms to establish chain of trust using hardware components. Analytics systems I have built are capable of running software across databases holding billions of events. Most recently I have been responsible for the design and implementation of an analytic architecture which operates over computer network metadata. The analytics are designed to detect and classify anomalous or malicious network activity without the use of signature-based detections. These systems rely heavily on Kafka, Hadoop HDFS, Postgres, and Apache Spark for scalable and efficient operations. I designed and coded a framework and testing architecture to migrate these workflows to Kubernetes-based cluster deployments.

8. I have additionally been the technical lead on small teams of 5 to 10 engineers in the area of search engine technologies since 2008. I designed and built search engines and data ingest pipelines to support large scale collections of intelligence reports for the purposes of user free text and structured search queries. I have built both backend processing systems and front-end user facing applications, which included designing custom query languages to facilitate user queries. I have authored several internal papers related to graph search engines as applied to document search and network community analytics.

9. I have developed applications for the purposes of reverse engineering and software analysis. For example, since 2012, I have built, run and maintained disassembler.io, which is the leading web application for reverse engineering binaries for over 50 CPU architectures.

10. From 2018 to the present, I have also assisted multiple companies transition their enterprise Hadoop/Spark based workflows from on-premise data center deployments to modern cloud service architectures utilizing both AWS and Microsoft Azure.

11. Since 2021, supported information security programs at Fortune 500 companies, including managing document security settings and configuring cloud applications to align with security standards.

12. In 2024-2025 I conducted security analysis on signed PDF files to verify signature integrity and establish chain of custody. This includes metadata analysis on cryptographic signatures to determine their authenticity.

13. I have conducted independent security analysis of third-party custom encryption algorithms, ensuring compliance with NIST standards and evaluating against established cryptographic benchmarks.

14. My curriculum vitae, which is attached as Appendix A also includes list of all other cases in which, during at least the previous 4 years, the I have served as an expert.

III. COMPENSATION

15. I am being compensated as an expert witness in this case at my standard hourly rate in addition to out-of-pocket expenses. I have received no additional compensation for my work on this matter and my compensation does not depend, and has not ever depended in any way, on my opinion as expressed in this matter, in any testimony that I may give, or on the outcome of this matter. I am not and have never been employed by Patent Owner. I have no financial stake in the '828 Patent, the outcome of this IPR, or any other matter involving the '828 Patent.

IV. MATERIALS CONSIDERED

16. In formulating my opinions, I have relied upon my training, knowledge and experience that are relevant to the '828 Patent. I have also considered the '828 Patent and its file history, Petition ("Pet.") and attached exhibits, the Patent Owner's preliminary response, the Board's decision on institution, the asserted prior art references, and the declaration of Dr. Xiong and the materials cited therein. In addition to the materials cited elsewhere in this declaration, I have also considered the following:

Exhibit No.	Description
2007	US Patent No. 5,486,853
2008	US Patent No. 7,161,622
2009	US Patent No. 6,377,981
2010	US Patent No. 5,486,853
2011	Wikipedia, “Floppy Disk Drive Interface” (available at https://en.wikipedia.org/wiki/Floppy_disk_drive_interface)
2012	Cambridge Dictionary, entry for “log file” (available at https://dictionary.cambridge.org/us/dictionary/english/log-file)
2013	Transcript of May 16, 2025 Deposition of Zixiang Xiong, Ph.D.

V. UNDERSTANDING OF LEGAL PRINCIPLES

17. I am not an attorney. I have been asked to provide opinions on the validity of the Asserted Claims of the Patents-in-Suit from the perspective of a person of ordinary skill in the art (“POSITA”).

A. Claim Construction

18. I have been provided certain legal principles relating to the construction of patent claims. I understand that “claim construction” is the interpretation of the meaning of patent claims. I understand that words of a claim are generally given their ordinary and customary meaning, which is the meaning the term or phrase would have to a person of ordinary skill in the art at the time of the invention. I understand that both intrinsic and extrinsic evidence can be used to assist in understanding the meaning of a claim. Intrinsic evidence includes the claim language, language in other claims of the patent, the specification, and the prosecution record. I further understand that, unless required by the claim language

or specification, claims should generally not be limited to embodiments in the specification, including preferred embodiments. I understand that extrinsic evidence, which consists of all evidence external to the patent and prosecution history including expert and inventor testimony, dictionaries, and learned treatises, may also be relevant to claim construction.

B. Invalidity Based on Prior Art

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

1. Prior Art

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

21. I understand that a U.S. or foreign patent qualifies as prior art to an asserted patent if the date of issuance of the patent is prior to the invention of the asserted patent. I further understand that a printed publication, such as an article published in a magazine, academic journal, conference proceedings, or trade publication, or U.S. or foreign published patent application qualifies as prior art to an asserted patent if the date of publication is prior to the invention of the asserted patent.

22. I understand that a U.S. or foreign patent qualifies as prior art to an asserted patent if the date of issuance of the patent is more than one year before the priority date of the asserted patent. I further understand that a printed publication, such as an article published in a magazine, academic journal, conference proceedings, or trade publication, or U.S. or foreign published patent application constitutes prior art to an asserted patent if the publication occurs more than one year before the priority date of the asserted patent.

23. I understand that, absent an assertion by the patentee otherwise, the date of invention is the filing date of the patent. I understand that a U.S. patent qualifies as prior art to the asserted patent if the application for that patent was filed in the United States before the invention of the asserted patent.

24. I understand that a system or device qualifies as prior art to the asserted patent if it was known or used in the United States prior to the invention of the asserted patent. I further understand that a system or device qualifies as prior art to the asserted patent if it was in public use or on sale in the United States more than one year prior to the priority date of the asserted patent.

25. I understand that if a device was used by others in this country before the date of the invention, or if it was in public use in this country more than one year before the effective date of application, the device qualifies as prior art. I understand

that, under either scenario, for a non-patentee's use to qualify as prior art, the purported use must have been available to the public. I understand that the following factors may be helpful in analyzing whether there was a public use: (1) the nature of the activity that occurred in public; (2) the public access to and knowledge of the public use; and (3) whether there was any confidentiality obligation imposed on persons who observed the use. I further understand that where a non-patentee's public use puts all the claimed features of an invention in the public's possession, this cannot be negated by evidence that other, unclaimed aspects of the non-patentee's device were not publicly available. Conversely, I understand that for a non-patentee's uses to constitute prior art, that use must have placed each of the claimed features of an invention in the public's possession. And, I understand that a non-patentee's secret or confidential uses do not invalidate later-filed patents.

26. I understand that a patent claim may be anticipated where, before the invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. I further understand that when the non-patentee's invention's "inner workings" are the essence of the invention, it is those "inner workings" that must not be suppressed or concealed in order for the invention to constitute prior art.

27. I also understand that prior art can include work by a prior inventor if that prior inventor: (1) conceived of the claimed invention before the conception date of the patentee, (2) was reasonably diligent in reducing the invention to practice from just prior to the conception date of the patentee, and (3) has not abandoned, suppressed or concealed the invention.

28. I understand that to qualify as prior art, a reference must contain an enabling disclosure that allows one of ordinary skill to practice the claims without undue experimentation.

29. I understand that documents and materials that qualify as prior art can be used to invalidate a patent claim as anticipated or as obvious.

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

2. Anticipation

31. I understand that, pursuant to 35 U.S.C. § 102, a claim of a patent is invalid for anticipation if, among other things, any of the following is true: (i) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, (ii) the invention was patented or described in a printed

publication in this or a foreign country or in public use or on sale in this country more than one year prior to the date of the application for patent in the United States, or (iii) the invention was described in another's United States patent or published patent application which issued from a patent application filed in the United States before the invention by the applicant for patent.

32. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

33. I understand that a prior art reference "anticipates" an asserted claim, and thus renders the claim invalid, if all elements of the claim are disclosed in that prior art reference, either expressly or inherently (i.e., necessarily present), arranged in the same way as in the claim. I understand that, for inherent anticipation, it is required that the missing descriptive material is necessarily present in the prior art reference.

34. I understand that to anticipate an asserted claim, an allegedly anticipatory prior art reference has to have an enabling disclosure. I understand an enabling disclosure describes the claimed invention in sufficient detail to enable a person of ordinary skill in the art to carry out the claimed invention.

35. I understand that a patent is anticipated if, before such invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it.

36. A patent claim is also anticipated if there is clear and convincing proof that, more than one year before the priority date of the patent, the claimed invention was: in public use or on sale in the United States; patented anywhere in the world; or described in a printed publication anywhere in the world. This is called a statutory bar.

37. I have written this declaration with the understanding that anticipation must be shown by clear and convincing evidence. I understand that clear and convincing evidence means that it is highly probable that the fact is true.

3. Obviousness

38. I understand that even if a patent is not anticipated, it is still invalid pursuant to 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the pertinent art (henceforth, a “POSITA”).

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

40. I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the Asserted Claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations (also called objective indicia of non-obviousness).

41. I understand that the test of obviousness is whether the claimed invention, as a whole, would have been obvious to one of ordinary skill in the art as of the date of the invention in light of the prior art.

42. I understand that a claim is not proved obvious merely by demonstrating that each of the elements was independently known in the prior art. I understand that most, if not all, inventions rely on building blocks long since uncovered, and claimed discoveries, almost of necessity, will likely be combinations of what is already known. I understand that it is important to identify whether a reason existed at the time of the invention that would have prompted a person of ordinary skill in the art in the relevant field to combine the known elements in the way the claimed invention does. I understand that the use of hindsight must be

avoided when considering whether the alleged invention would have been obvious to the person of ordinary skill in the art. In assessing obviousness, I have been instructed to consider the distortion caused by hindsight bias, guard against slipping into the use of hindsight, be cautious of arguments that rely upon after-the-fact reasoning, and avoid the temptation to read into the prior art the teachings of the invention in issue.

43. I understand that secondary considerations of non-obviousness (also known as objective indicia of non-obviousness) may include: (1) a long felt but unsolved need; (2) commercial success; (3) unexpected results; (4) industry praise; (5) licensing; and (6) copying by others. I also understand that there must be a relationship or nexus between any such secondary considerations and the claimed invention. I further understand that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

44. I understand that any secondary consideration must bear a nexus to the claimed invention. Where the offered secondary consideration actually results from something other than what is both claimed and novel in the claim, there is no nexus to the merits of the claimed invention. I further understand that the patentee bears the burden of demonstrating that the relevant secondary indicia is attributable to the claimed invention, as opposed to other economic and commercial factors unrelated

to the technical quality of the patented subject matter. I understand that a nexus is presumed where the secondary considerations are tied to a particular product which: (i) embodies the claimed invention and (ii) is coextensive with the claimed invention. In analyzing whether a product is coextensive with the claimed invention, I understand that there is no requirement for a perfect correspondence between the claims and the product, and that the presumption of a nexus can still apply when unclaimed features present in the product amount to nothing more than additional insignificant features.

45. I further understand that, as a safeguard against hindsight bias, all secondary considerations of non-obviousness must be considered prior to reaching an obviousness conclusion.

46. I understand that an obviousness evaluation can be based on a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but other times the nexus linking two or more prior art references can be based on the ordinary understandings available to a POSITA. I further understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

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

48. I understand that whether a prior art reference “teaches away” from the claimed invention is a fact to be considered in determining obviousness. I understand that it is improper to combine references where the references teach away from their combination. However, I understand that the nature of the teaching is highly relevant and must be weighed in substance – a known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use. Furthermore, I understand that the prior art’s mere disclosure of more than one alternative does not constitute a teaching away from any of those alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed.

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

references to achieve the claimed invention, and that same POSITA would have had a reasonable expectation of success from combining those teachings.

VI. LEVEL OF ORDINARY SKILL IN THE ART

50. My opinions herein are based from my standpoint of a person of ordinary skill in the art at the time of invention of the '828 Patent, *i.e.*, POSITA.

51. I understand that, for the purposes of proceeding, the '828 Patent is entitled to a priority date no later than July 27, 2000, the filing date of the application leading to the '828 Patent (U.S. Pat. Appl. No. 11/633,366).

52. I understand that Petitioner and its expert Dr. Xiong have proposed 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 image processing.” Pet., 13.

53. Having reviewed the '828 Patent specification and claims, it is my opinion that the '828 Patent is primarily directed to digital security and authentication. It is therefore my opinion 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. I agree with Petitioner and Dr. Xiong 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, in my opinion these are concepts primarily addressed in digital security rather than image processing.

VII. OVERVIEW OF THE '828 PATENT

54. 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.

55. The '828 Patent employs a method of creating and later 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.

VIII. CLAIM CONSTRUCTION

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

56. 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, having examined the prosecution history, it is my opinion that the reference to “conductive trace or lead”

in the prosecution history is exemplary only, and not exclusively limited to conductive traces or leads.

57. 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). It is my opinion that the Patentee here 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. I find no clear and unmistakable disclaimer within this statement specifically limiting the claim language to conductive traces or leads specifically. It is my opinion that the reference to exemplary conductive traces or leads here is illustrative, indicating that in this exemplary embodiment the conductive traces or leads are 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.

58. My opinion that the prosecution history does not contain any clear and unmistakable disclaimer limiting the claim to conductive traces or leads is further supported by the additional explanation in the prosecution history distinguishing Schipper. 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. 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 stated 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.*

59. In a later response, the Patentee further explained that this limitation requiring that the connection between the sensor and memory be tightly coupled is based upon the connection not being physically accessible to the user. 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. 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.

60. It is my opinion that the prosecution history 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 from being altered before authentication information is generated.

61. For these reasons, it is my opinion that this limitation should be construed to mean “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)

62. 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. It is my opinion that Petitioner’s construction is not correct

because the claim term requires “monitoring... the tight coupling” between the memory and the sensor specifically. It is my opinion that Petitioner’s construction is not correct because the claim language explicitly requires monitoring the *physical coupling* between the memory and the sensor as opposed to some third structure.

63. It is my opinion that 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.

64. Consistent with the specification, the claim language 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. It is my opinion that the prosecution history for the ’828 Patent is also 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).

65. It is my opinion that the “has been gained” language in the construction proposed by Petitioner injects ambiguity by making it unclear whether monitoring requires making the specific determination that the coupling between the sensor and memory has been disturbed.

66. For these reasons, it is my opinion that a POSITA would understand that this language specifically requires monitoring the *physical coupling* between the sensor and the memory. It is my opinion that “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)

67. The Petition identifies the term “based on” which is in claim 1 for claim construction. Pet at 11-14. However, Petitioner does not identify a proposed construction for this term. Instead, Petitioner argues that “based on” is an open-ended term. 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. It is my opinion that a POSITA would understand this term in the context of the claims and the specification, and therefore it is my opinion that this term is not indefinite. I also note that the District Court’s tentative claim construction ruling found this term to be not indefinite. EX1020 at 18. Because the Petition does not propose a construction for this term, however, I have applied plain and ordinary meaning and do not otherwise apply any special construction.

IX. 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

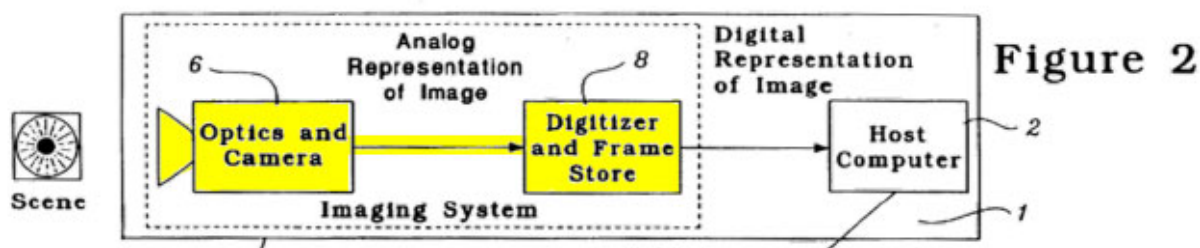
(a) Glass Fails to Disclose a “utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter” under Petitioner’s own Proposed Claim Construction [limitation 1b]

68. As I discuss 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 VIII.A. However, under either construction, it is my opinion that Petitioner fails to show that Glass discloses this limitation.

69. 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 Dr. Xiong identify any teaching in Glass showing that the sensor (or camera) is coupled to the memory via “conductive traces or leads.” Pet. at 26-29; EX1003 at ¶¶170-176.

70. 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 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.

71. 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.

72. Dr. Xiong argues, without providing 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. I have reviewed one patent from this time frame that discloses connecting electronic cameras to either processors or memory by cables rather than by conductive traces or leads. EX2007 (US Patent No. 5,486,853) (generally disclosing an electrical cable for connecting an electronic camera to a processor).

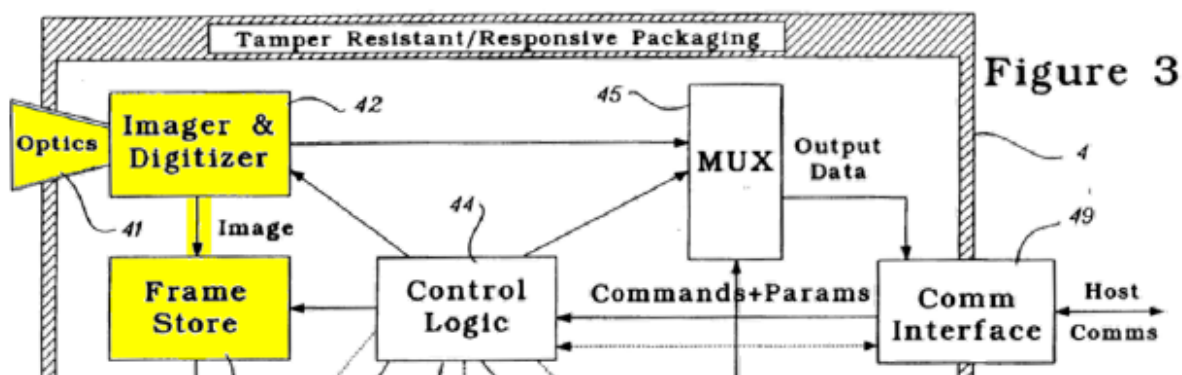
Additionally, I am familiar with computing equipment in this time frame, and it is my opinion from my experience that connecting components by cable was generally known. Because a POSITA would know that there were many ways to connect a CCD camera to either a processor or memory, it is my opinion that 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.

73. It is my opinion that a POSITA would understand that a data path between a sensor and memory could be made without even having a physical connection. 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). 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). Communications over Wi-Fi, which are wireless, would involve the sharing of information through a data path, but a POSITA would appreciate that such wireless data paths would not involve “conductive traces or leads” under any meaningful interpretation of that language.

74. As a further example, satellite-based internet service providers allow computers to establish data paths that are not even confined to the Earth’s atmosphere, nor to 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). It is my opinion that 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 claim construction requires. Communications by satellite, similar to communications over WiFi, would be appreciated by a POSITA as not involving “conductive traces or leads” for similar reasons.

75. Dr. Xiong next cites Figure 3 of Glass, which 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 I have 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. The specification of Glass also 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 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. Dr. Xiong’s declaration also states 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 does not show a connection by “conductive leads or traces” as Petitioner’s construction requires. For example, as I explain above, 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.*, EX2010 (US Patent No. 5,486,853) (generally disclosing an electrical cable for connecting an electronic camera to a processor). Also, as I explain above, data paths utilizing WiFi and satellite-based communications were also known at the time of the '828 Patent.

76. Dr. Xiong cites the prosecution history of the '828 Patent as supporting his argument that Glass discloses this element. EX1003 at ¶¶173-175. However, nothing in the prosecution history is directed to Glass. Dr. Xiong essentially argues 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. However, it is my opinion that 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. 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). However, Dr. Xiong stated in his deposition that he was unable to determine whether cables generally, nor floppy cables specifically, were connections by “conductive traces or leads”). EX2013 (Xiong Tr.) at 32:14-22; 64:22-25. As such, it is my opinion that 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. EX1003 at ¶¶172-175.

77. 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 I 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.” Even if the arrow between the components illustrated in the Figures 2 and 3 of Glass 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.”

78. Patent Owner proposes, to which I agree for the reasons I explain above, an alternative claim construction requiring “a sensor that is electrically or physically coupled to memory in a device.” *Supra* at VIII.A. However, even under this construction, Petitioner and Dr. Xiong fail to show that Glass teaches this limitation for similar reasons. It is my opinion that the arrows depicted in Figs. 2 and 3 of Glass depict an operational connection to convey data between components. There is no discussion in the specification describing any physical aspects of the connection between the sensor and memory components identified in these figures. As I explain above, wireless WiFi connections and satellite communications represent *operational* data paths, consistent with Glass, known at the time that would not inherently provide a *physical* connection between the components as required in Patent Owner’s proposed construction. It is my opinion that Glass fails to teach this element under Patent Owner’s claim construction as well for similar reasons.

(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]

79. As I have discussed above, Petitioner asserts that this limitation should be construed to mean “determining whether physical access has been gained to the

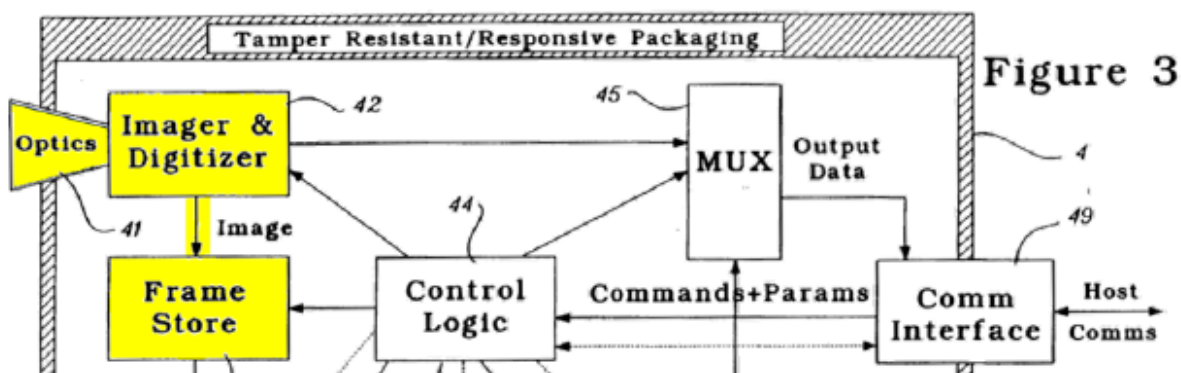
coupling between said memory and said sensor.” *Supra* at VIII.B. Patent Owner, on the other hand, asserts that this limitation should be construed to mean “determining whether the physical coupling between said memory and said sensor has been accessed or disturbed.” *Id.* It is my opinion that both constructions require monitoring the specific coupling between the memory and the sensor and determining when that specific coupling has been accessed or disturbed. 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.*

80. As I explain 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 VIII.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, it is my opinion that 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.

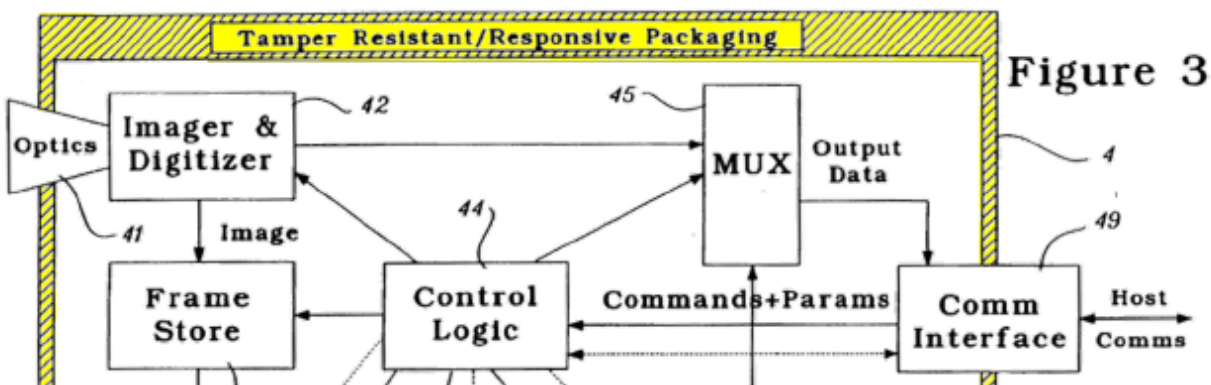
81. Petitioner and Dr. Xiong attempt to equate monitoring the coupling itself with monitoring tamper-resistant package 50 in Glass. Pet. at 30; EX1003 at ¶181. However, the claim does not recite “monitoring the integrity of *a package that includes* the tight coupling between said memory and said sensor,”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

82. A comparison of different portions of Figure 3 utilized by Petitioner 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, Glass 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, it is my opinion that Glass does not “monitor[] the integrity of the tight coupling between said memory and said sensor” as the ’828 Patent requires.

83. 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, it is my opinion this monitoring of the *packaging* is not monitoring the integrity of the *coupling* as the limitation specifically requires for the reasons presented above.

(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]

84. It is my opinion that 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, 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.

85. Log files are generally understood to be “computer file[s] that contain[] a record of all actions that have been done on a computer.” EX2012 (Cambridge Dictionary). Because the log file only records events, these events are not displayed to the user at the time that the event occurs. 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.*

86. Nor does Dr. Xiong 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*. 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 implies that the record provides only historical information on events that have already occurred. The claim language requires “generating an error signal that *is displayed* to a user to indicate that said stored data stream is not authentic.” A POSITA would recognize that this requires displaying the error signal *when* the error signal is generated. Petitioner and Dr. Xiong’s argument would essentially 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, it is my opinion that Glass’s log files do not display the error signal to the user when the error signal is generated as the limitation requires as written.

(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]

87. It is my opinion that Glass fails to disclose this limitation for the same reasons as for limitation 1g. *See supra* at IX.A.1.d. 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.

88. Log files are generally understood to be “computer file[s] that contain[] a record of all actions that have been done on a computer.” EX2012 (Cambridge

Dictionary). Because the log file only records events, these events are not displayed to the user at the time that the event occurs. 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.*

89. Nor does Dr. Xiong 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*. 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 concedes that the record provides only historical information on events that have already occurred. The claim language requires “generating an ok signal that *is displayed* to a user to indicate that said stored data stream is authentic.”

A POSITA would recognize that this requires displaying the ok signal *when* the ok signal is generated. Petitioner and Dr. Xiong’s argument would essentially 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, it is my opinion that Glass’s log files do not display the ok signal to the user when the ok signal is generated as the limitation explicitly requires.

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]

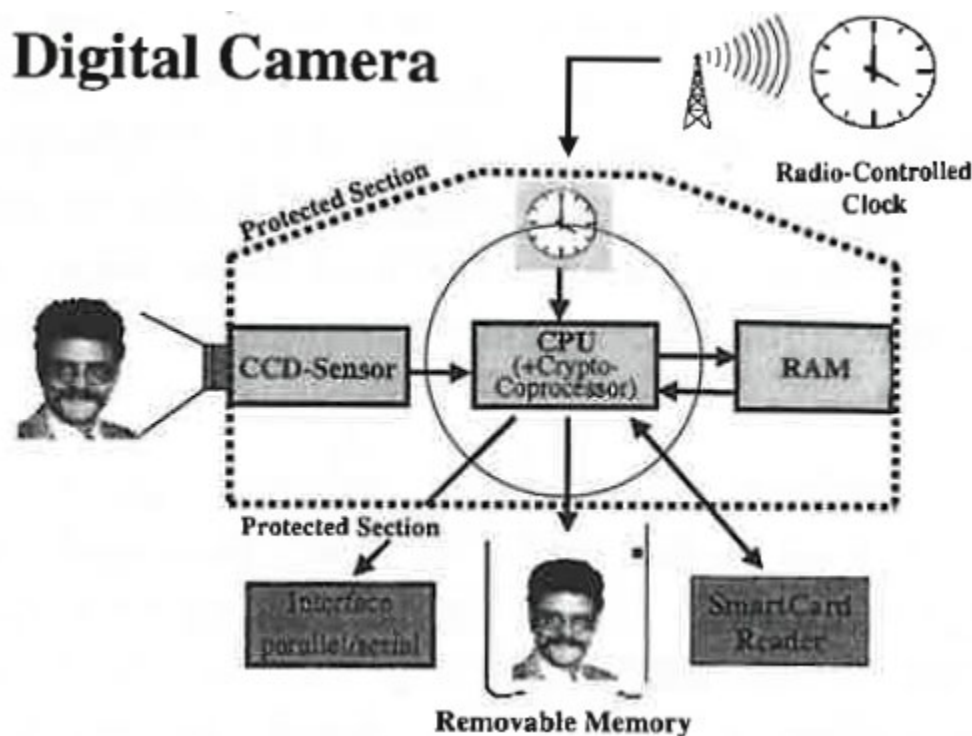
90. It is my opinion that Rieger fails to meet this limitation for similar reasons as Glass. *See supra* at IX.A.1.a. As discussed above, Petitioner and Patent Owner dispute the claim construction that applies to the claim language “a sensor, which is tightly coupled to said memory.” *See supra* at VIII.A.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

91. 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 Dr.

Xiong identify any teaching in Rieger showing that the sensor (or camera) is coupled to the memory via “conductive traces or leads.” Pet. at 43-46; EX1003 at ¶¶228-234.

92. Petitioner asserts 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 leads and traces 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 leads and traces. EX1003 at ¶¶228-234.

93. 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.

94. Dr. Xiong argues, without providing 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. I have reviewed one patent from this time frame that discloses 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). Additionally, I am familiar with computing equipment in this time frame, and it is my opinion from my experience that connecting components by cable was generally known. Because a POSITA would know that there were many ways to connect a CCD sensor to either a processor or memory, it is my opinion that 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.

95. It is my opinion that a POSITA would understand that a data path between a sensor and memory could be made without even having a physical connection. 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). 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). Communications over Wi-Fi, which are wireless, would involve the sharing of information through a data path, but a POSITA would appreciate that such wireless data paths would not involve “conductive traces or leads” under any meaningful interpretation of that language.

96. As a further example, satellite-based internet service providers allow computers to establish data paths that are not even confined to the Earth’s atmosphere, nor to 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). It is my opinion that 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. Communications by satellite, similar to communications over WiFi, would

readily be appreciated by a POSITA as not involving “conductive traces or leads” for similar reasons.

97. Dr. Xiong cites the prosecution history of the '828 Patent as 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. Dr. Xiong essentially argues 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. 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). However, Dr. Xiong stated in his deposition that he was unable to determine whether cables generally, nor floppy cables specifically, were connections by “conductive traces or leads”). EX2013 (Xiong Tr.) at 32:14-22; 64:22-25. As such, it is my opinion that 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.

98. 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 means that the sensor is tightly coupled to the memory in Rieger. EX1003 at ¶175. However, as I 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.” 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.”

99. Patent Owner proposes, to which I agree for the reasons I explain above, an alternative claim construction requiring “a sensor that is electrically or

physically coupled to memory in a device.” *Supra* at VIII.A. However, even under this construction, Petitioner and Dr. Xiong fail to show that Rieger teaches this limitation for similar reasons. 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. As I explain above, wireless WiFi connections and satellite communications represent *operational* data paths, consistent with Rieger, known at the time that would not necessarily provide a *physical* connection between the components as required in Patent Owner’s proposed construction. It is my opinion that Rieger fails to teach this element under Patent Owner’s claim construction as well for similar reasons.

(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]

100. As I have 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 VIII.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.* It is my opinion that both constructions require

monitoring the specific coupling between the memory and the sensor and determining when that specific coupling has been accessed or disturbed. Rieger fails to teach this limitation because Rieger monitors a “protected compartment” within the housing of the camera, but monitoring this *compartment* fails to teach monitoring the *coupling* between the sensor and memory specifically as the limitation requires. *Id.*

101. As I explain 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 VIII.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, it is my opinion that 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.

102. Petitioner and Dr. Xiong attempt to equate monitoring the coupling itself with monitoring a 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. It is my opinion that Rieger fails to disclose the claimed limitation because it discloses monitoring something other than the coupling, namely, a tamper resistant package.

103. 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.

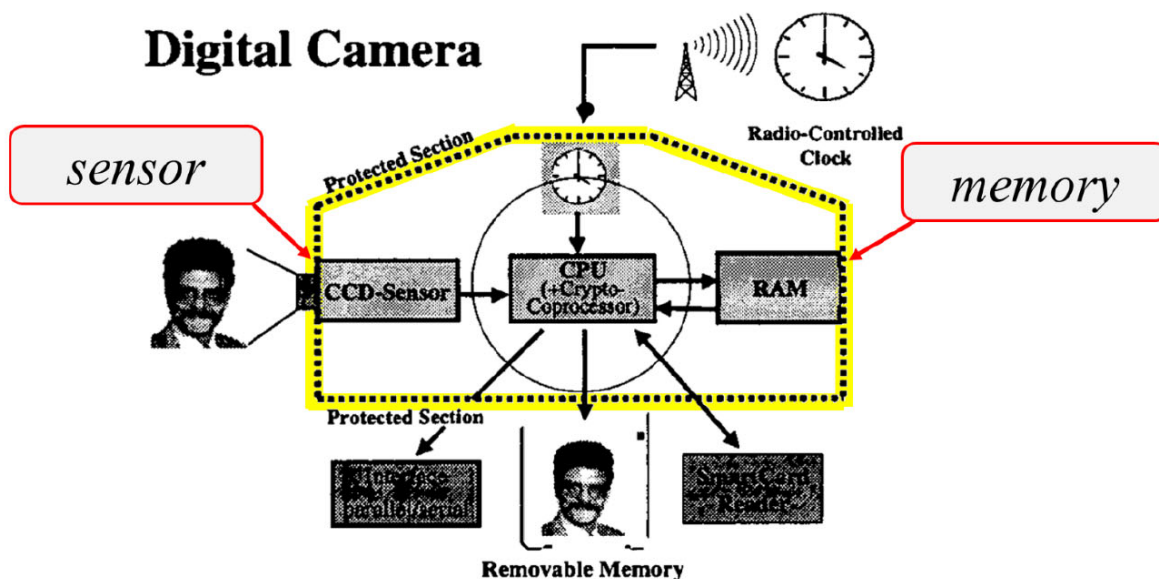


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

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

As such, it is my opinion that Rieger does not “monitor[] the integrity of the tight coupling between said memory and said sensor” as the ’828 Patent requires.

(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]

104. It is my opinion that Rieger 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, 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 the subject of this limitation.

105. Petitioner and Dr. Xiong rely upon a “frowning face image” shown in Figure 7 of Rieger as purportedly 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. 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. EX1006 at 12. 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.* It is my opinion that 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 to a user, if any.

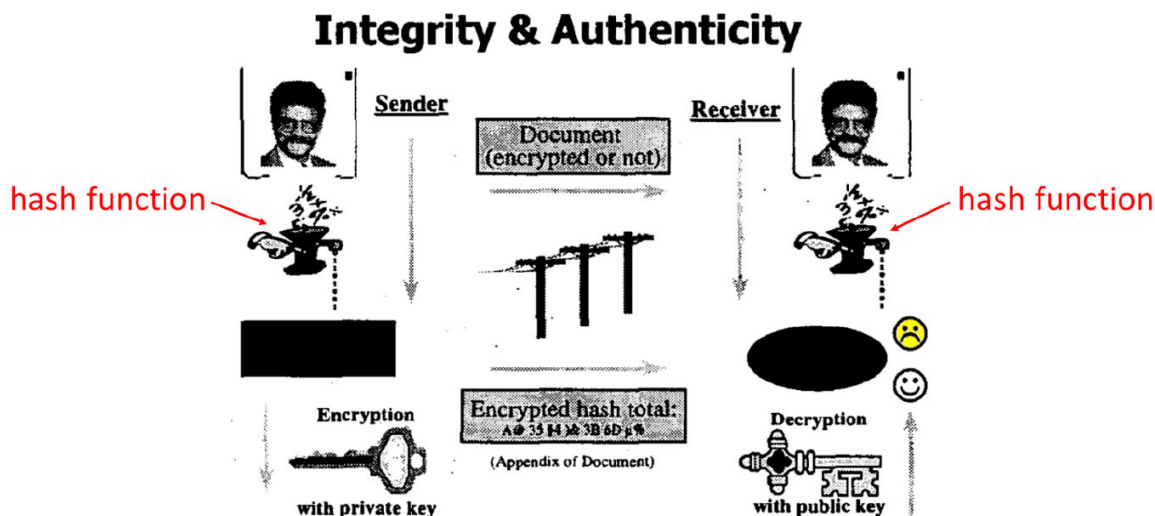


Figure 7: Principles of the integrity and authenticity test

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

- (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]**

106. It is my opinion that Rieger fails to disclose this limitation for the same reasons as for limitation 1g. *See supra* at IX.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, the actual communication to the user of an ok indication is the subject of this limitation.

107. Petitioner and Dr. Xiong 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. 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.* It is my opinion that 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.

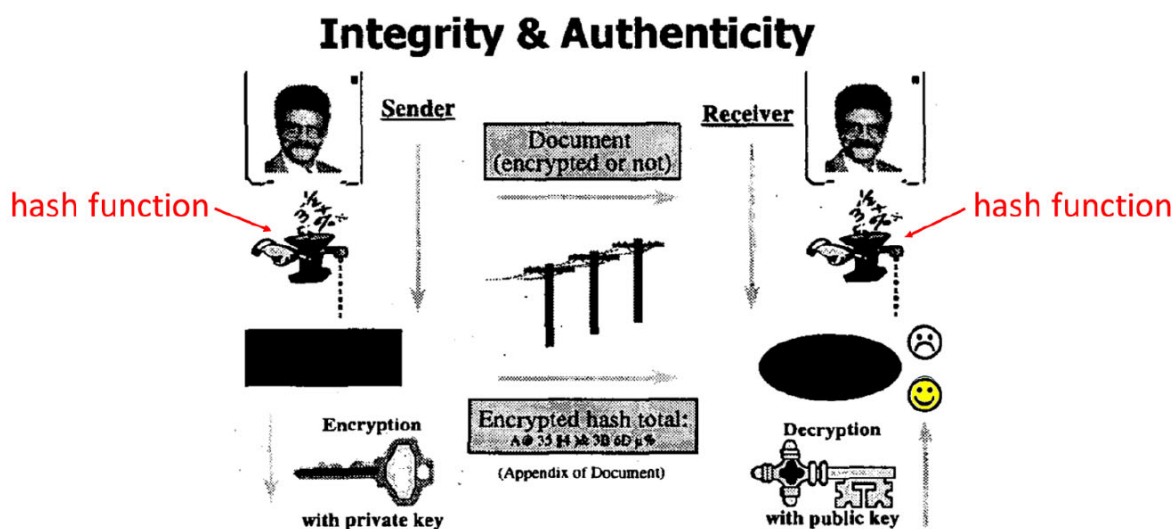


Figure 7: Principles of the integrity and authenticity test

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

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

1. Claim 1

108. 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. 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 stating that the references "provide more detail about the specific metadata fields available for digital cameras." *Id.* Petitioner's arguments fail for the reasons I have as discussed above. *See supra* at IX.A.1, IX.B.1. 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 I have discussed above. *Id.*

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

109. Petitioner argues it would have been obvious to modify Glass and Rieger to add Serret-Avila. Pet. at 67. It is my opinion that Petitioner fails to show motivation to combine these references for several reasons.

110. It is my opinion that Serret-Avila is non-analogous art. 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.* Glass, on the other hand, focuses on “securely transmitting biometric data over a network contains a sensor, preferably a camera.” EX1005 at Abstract. Rieger focuses on “ensuring the integrity and authenticity of photographic images during the image-recording phase.” EX1006 at 1.

111. For this reason, it is my opinion that a POSITA would therefore recognize that Serret-Avila is generally in the field of internet transaction or e-commerce security. By contrast, a POSITA would recognize that Glass and Rieger are generally in the field of digital imaging security. It is my opinion that 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.”).

112. It is also my opinion that Serret-Avila is not reasonably pertinent to the particular problem with which the inventor was involved. 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.”). On the other hand, Serret-Avila is not directed to, nor does it discuss, authenticating digital images, nor aspects of security

specifically relating to digital images. *See, e.g.*, EX1006 at Abstract. In light of these significant differences in field of use, purpose, problems solved, and manner of solution, it is my opinion that Serret-Avila would not “have commended itself to an inventor’s attention in considering” the problems solved by the ’828 Patent.

113. I have reviewed the Board’s Institution Decision (Paper No. 8, “DI”), where 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, it is my opinion that 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. Serret-Avila, on the other hand, uses a warning display system, requiring online presence by a user to receive the warning display. EX2011 at 10:39-45. 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. As such, each

reference follows divergent, and incongruent, paths for informing users of results (if any).

114. For these reasons, it is my opinion that 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]

115. It is my opinion that 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. 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. Second, as previously stated, Serret-Avila is not directed towards authenticating digital images, nor it even mention digital photographs or images. EX2011. 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. EX2011 at 10:28-30.

116. 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 the subject of this limitation.

X. CONCLUSION

117. I currently hold the opinions that I have expressed in this declaration. However, my analysis may continue, and I may acquire or receive additional information or insights that may result in revised or supplemental observations or opinions.

118. I understand this declaration will be used as evidence in a contested case before the PTAB.

119. I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 or Title 18 of the United State Code, and that such willful false statements may jeopardize the validity of the '828 Patent.

I declare under penalty of perjury that the foregoing is true and correct.

Executed: June 13, 2025



Bill Davis