

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 SURREPLY TO PETITIONER'S REPLY

Table of Contents

Table of Authorities iii

Patent Owner’s Exhibit List.....iv

I. INTRODUCTION 1

II. PATENT OWNER’S EXPERT IS A POSITA WITH EXTENSIVE
EXPERIENCE IN THE AREA OF COMPUTER SECURITY, WHICH IS
THE FOCUS OF THE ‘828 PATENT 2

III. CLAIM CONSTRUCTION 4

 A. “a sensor, which is tightly coupled to said memory” 4

 B. “monitoring the integrity of the tight coupling between said
memory and said sensor” 9

 C. “based on” 10

IV. GLASS AND RIEGER FAIL TO DISCLOSE THE LIMITATIONS OF
CLAIM 1..... 11

 A. Glass and Rieger Fail to Disclose a Sensor “Tightly Coupled” to a
Memory 11

 B. Glass and Rieger Fail to Disclose the “Monitoring” Step 16

 C. Glass Fails to Disclose “OK” and “Error” Signals 18

 D. Rieger Fails to Disclose “OK” and “Error” Signals 19

V. SERRET-AVILA COMBINED WITH GLASS OR RIEGER FAILS TO
RENDER THE CLAIMS OBVIOUS.....20

 A. Serret-Avila Is Non-Analogous Art 20

 B. A POSITA Would Not Have Been Motivated to Combine Serret-
Avila with Glass or Rieger 22

 C. Serret-Avila Does Not Disclose Generating an “OK Signal”
Indicating That the Data Stream Is Authentic.....23

VI. CONCLUSION.....24

Certificate of Service 37 C.F.R. § 42.6(e) 26

Certificate of Compliance Pursuant to 37 C.F.R. § 42.24 27

Table of Authorities

	Page(s)
Cases	
<i>ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	6
<i>Cutsforth, Inc. v. MotivePower, Inc.</i> , 636 F. App'x 575 (Fed. Cir. 2016).....	20
<i>In re Klein</i> , 647 F.3d 1343 (Fed. Cir. 2011).....	20
<i>Iridescent Networks, Inc. v. AT&T Mobility, LLC</i> , 933 F.3d 1345 (Fed. Cir. 2019)	6
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	20
<i>Liberty Ammunition, Inc. v. United States</i> , 835 F.3d 1388 (Fed. Cir. 2016)	6
<i>Ultravision Techs., LLC v. Govision, LLC</i> , 2023 WL 2182285 (Fed. Cir. Feb. 23, 2023)	5

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.
2013	Transcript of Oct. 2, 2025 Deposition of Zixiang Xiong, Ph.D.

I. INTRODUCTION

Patent Owner's Response (Paper No. 16, hereinafter "POR") provided detailed explanation for why the prior art in each of Petitioner's grounds fails to invalidate the claims of U.S. Patent No. 6,757,828 ("the '828 Patent"). In its Reply (Paper No. 16), Petitioner offers little additional argument, but instead urges the same tortured arguments presented in the Petition (Paper No. 1, hereinafter "Pet.").

First, neither Petitioner nor its expert present any evidence beyond guesswork and supposition that a sensor is physically and electrically connected to memory in Glass and Rieger, let alone connected by conductive leads and traces as Petitioner's proposed construction requires.

Second, Glass and Rieger both monitor a package or compartment surrounding a group of components including a sensor and memory rather than monitoring the coupling between the sensor and memory as the claim explicitly requires.

Third, Glass and Rieger both fail to disclose "ok" or "error" signals which are displayed to a user depending on whether the data stream is authenticated. In the case of Glass, the system only writes the result to a log file which is not necessarily ever displayed to the user. In the case of Rieger, the reference does not describe displaying such signals to a user at all, a fact which Petitioner attempts to obfuscate through pure supposition and hypothetical modification.

Finally, for Serret-Avila, Petitioner fails to show that it is appropriate to combine the reference with either Glass or Rieger and, even if it were combined, Serret-Avila fails to disclose displaying an “ok” signal to a user.

In sum, Patent Owner’s arguments are supported by detailed analysis and reasoning, while Petitioner’s arguments are conclusory and based on hypotheticals and supposition. The Board should therefore hold each challenged claim patentable.

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

Petitioner argues it’s definition of a POSITA is correct because Petitioner’s definition includes a requirement that a POSITA has experience in “image processing” while Patent Owner’s definition requires experience in digital security, authentication, or digital image authentication. *Compare* POR at 4-5 *with* Reply at 1-2. However, Patent Owner’s definition is the one that most accurately reflects the technology claimed in the ’828 Patent. For example, Claim 1 is not specifically limited to a camera, but instead generally requires using a “sensor” to generate a “parameter,” monitoring the “tight coupling” between the sensor and memory to ensure that the integrity of the coupling for providing the parameter is not compromised, and then utilizing the parameter in conjunction with signature protocols in order to verify the authenticity of a data stream. EX1001 at claim 1. Nothing in Claim 1 is specifically directed to image processing or image creation;

rather, the claim is directed to the process of validating and authenticating a data stream.

Patent Owner's expert, Mr. Davis, has extensive experience in the field of computer security, which is the actual focus of the '828 Patent and its claims. Mr. Davis has held the position of Principal Security Researcher at Syscall 7, LLC for the past nine years. EX2006 at 3. More specifically, Mr. Davis has developed tools that utilize data collection. *Id.* Further, Mr. Davis has performed consulting work on enterprise security specifically directed to protecting the security of documents (i.e., digital streams). *Id.* Finally, Mr. Davis has a bachelor's degree in mathematics and computer science from the University of Maryland, and a master's degree in computer science from Johns Hopkins University. *Id.* at 2. As such, Mr. Davis is well-qualified in the specific area described in the claims of the '828 Patent, namely ensuring the security of data streams which can represent samples of the environment utilizing digital signatures derived at least in part from a parameter provided from a sensor that is tightly coupled with memory, and in which the system monitors the tight coupling between the sensor and memory to ensure integrity of the parameter. EX1001 at claim 1.

In contrast, Petitioner's expert, although having experience in fields such as image processing, video processing, and image and video coding, does not identify any work or expertise specifically directed to computer security or to the

authentication of digital files or streams. EX1004 at 1. Nor is Petitioner's expert's professional experience directed to the areas of security or the authentication of digital files or streams. *Id.* at 7-8. As such, although Petitioner's expert may be knowledgeable on how digital image files are created and processed, Petitioner's expert lacks substantive experience in the specific area described in the claims of the '828 Patent, which are directed to the field of digital security generally, and to verifying the authenticity of a data stream specifically.

Petitioner notes that Mr. Davis's declaration mistakenly recites the obviousness standard applicable to District Court litigation requiring proof of obviousness by clear and convincing, rather than a preponderance, of the evidence. Reply at 3. However, as Mr. Davis makes clear, the deficiency in the Petition and in Dr. Xiong's analysis results from the failure to provide proof of the existence of the identified elements in the cited references. *See, e.g.*, EX2005 at ¶¶69-72. As such, Mr. Davis's conclusions are well-supported and based upon the underlying factual record, his analysis, and his expertise.

III. CLAIM CONSTRUCTION

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

Petitioner argues that its construction, which requires “a sensor coupled to said memory via conductive traces or leads” is a term of degree that must be based upon an objective measure. Reply at 4. However, as Patent Owner already

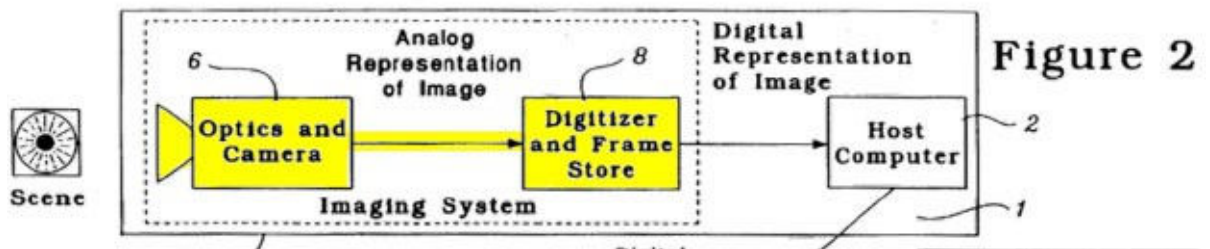
described, during prosecution the patentee explained that the purpose of being “tightly coupled” means that the processor and memory are coupled such that “there is no possibility for altering the image before the authentication information is generated.” EX1002 at 12. The specification reinforces this distinction by stating that “[t]here can be nothing that can possibly alter the recording before the authentication information is generated.” EX1001 at 3:18-20. The purpose of the tight coupling is to make it “virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor.” EX1002 at 277. As such, as previously explained, the “tightly coupled” connection is one in which the connection is secured and monitored to ensure that the information used to authenticate the data cannot be altered before the information is stored in memory. EX1001 at Claim 1.

Petitioner’s argument that “tightly coupled” is a term of degree is contradicted by the lack of any attempt to measure how “tight” the coupling must be in order to be “tightly coupled.” This failure to provide criteria for evaluating any degree of tightness in the connection is clearly at odds with the cases cited by Petitioner. Reply at 4. In *Ultravision*, the Federal Circuit approved the use of ingress protection (IP) ratings of IP 65 or higher to define “waterproof.” *Ultravision Techs., LLC v. Govision, LLC*, 2023 WL 2182285, at *3-*4 (Fed. Cir. Feb. 23, 2023). In *Iridescent Networks*, the use of connection speed and packet loss measurements were used to

define a “high quality of service connection.” *Iridescent Networks, Inc. v. AT&T Mobility, LLC*, 933 F.3d 1345, 1351-52 (Fed. Cir. 2019). And in *Liberty Ammunition*, the measured area of contact in a conventional ammunition round identified in the specification was used as the basis for measuring a “reduced area of contact.” *Liberty Ammunition, Inc. v. United States*, 835 F.3d 1388, 1396-98 (Fed. Cir. 2016). In all of these cases the construction utilized measurements in order to determine whether or not a term of degree recited in the claims had been met.

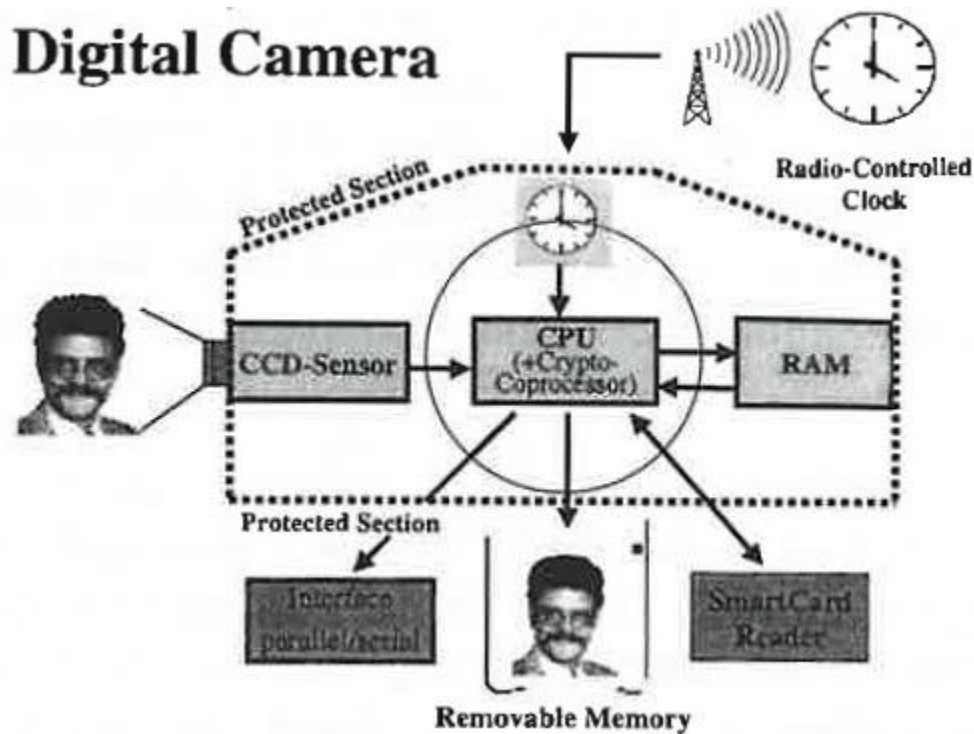
However, Petitioner proposes no measurement or standard for measurement consistent with evaluating any purported term of degree. Instead, Petitioner attempts to import structural limitations into the claim by adding unrecited structural limitations from the specification requiring a connection “via conductive traces or leads.” However, this limitation does not attempt to measure “tightness” or provide an objective standard of measurement. Instead, Petitioner improperly attempts to import structural limitations into the claim language, which is forbidden, as opposed to providing any threshold for measurement. *See ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1326 (Fed. Cir. 2012) (rejecting “proposed construction [which] erroneously reads limitations into the claims”). Rather, as the intrinsic record explains, a “tightly coupled” connection is one having “no possibility for altering the image before the authentication information is generated.” EX1002 at 12.

Petitioner argues that Glass and Rieger disclose “a sensor that is electrically or physically coupled to memory in a device.” Reply at 6. However, as shown in Patent Owner’s Response, the Petition fails to show that either Glass or Rieger disclose a sensor that is electrically or physically coupled to memory. POR at 12-20, 28-35. More specifically, for both references, the Petition wholly relies upon arrows in the figures. Pet. at 26-27, 44-45; POR at 19-20, 34-35. In both cases, the arrows merely depict an operational connection to convey data between the components and therefore fails to disclose how or whether any physical connection exists between the components, electrical or otherwise. POR at 19-20, 34-35. Petitioner’s conclusory assertion, devoid of evidence, that the figures depict electrical connections is similarly insufficient. Reply at 6. Nor does Petitioner’s expert declaration overcome these deficiencies. EX1029 at ¶17. For example, Fig. 2 of Glass depicts an operational connection between the Imaging System and the Host Computer using only an arrow, which is the same depiction as within the Imaging System of Fig. 2.



Glass, Fig. 2

Additionally, Rieger explicitly depicts a radio (non-electrical) connection from a transmitter to the device using the *exact same* arrow depiction which Petitioner now attempts to argue to disclose an electrical connection within the device. However, there can be no reasonable dispute that a transmission from a radio tower, which can span many miles with no intervening electrical connection from the radio tower to the camera being present. As such, there is no reasonable dispute that arrows themselves do not represent physical connections, let alone connections by conductive leads or traces.



Rieger, Figure 3

Petitioner fails to show an electrical connection in either Glass or Rieger as explained herein and in the Opposition. POR at 12-20, 28-35.

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

Petitioner erroneously attempts to avoid the explicit claim language which recites “***monitoring*** the integrity of the ***tight coupling*** between said memory and said sensor.” EX1001 at claim 1.¹ As explained, the claim language explicitly requires monitoring the *physical coupling* between the memory and the sensor as opposed to some third structure. POR at 9-11.

Petitioner concedes that the specification states that “internal security 14 is monitored to detect the integrity of the tight coupling of the sensor set and the recorder 6.” Reply at 8 (citing EX1001, 4:65-67). However, here the specification explicitly discloses that the “internal security 14” is used “to detect the integrity of the tight coupling of the sensor set and the recorder 6.” *Id.* As such, the internal security 14 reflects the integrity of the physical coupling between the sensor set (i.e., the sensor) and the recorder 6 (i.e., the memory) itself.

Petitioner further concedes that, during prosecution, the applicant stated that “a signal is generated if the device that prevents ***physical access*** to the ***interconnections*** between the sensor set and memory is broken.” Reply at 9 (quoting EX1002 at 293, emphasis added). As such, the signal generated monitors

¹ Emphasis added herein, unless otherwise noted.

the physical access to the interconnection between the sensor and the memory. Although Petitioner now attempts to expand this outward, the specific argument set forth during prosecution focused upon monitoring, and protecting, the interconnection between the sensor set and the memory.

Petitioner likewise ignores that the District Court, in construing the same term, also focused the physical coupling between the memory and the sensor. The District Court in its tentative claim construction order states, “monitoring involves determining whether the *physical coupling has been accessed or disturbed.*” EX1020 at 12 (emphasis added). Like the claim language itself, the specification, and the prosecution history, the District Court also recognized that the limitation should properly require monitoring the physical coupling in order to determine whether it has been accessed or disturbed. Therefore, “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”

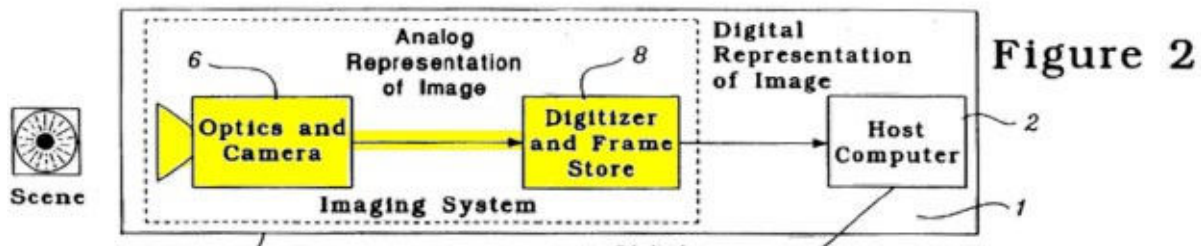
Petitioner continues to refuse to ascribe any construction to this term beyond a vague assertion that the term is “open-ended.” Reply at 9. Petitioner also provides no explanation for why the term should not be accorded its plain and meaning. *Id.* More specifically, the District Court applied this construction in the co-pending

litigation, finding the term “[n]ot indefinite. Plain and ordinary meaning.” EX1020 at 2, 18. Petitioner presents no reason to depart from the District Court’s construction.

IV. GLASS AND RIEGER FAIL TO DISCLOSE THE LIMITATIONS OF CLAIM 1

A. Glass and Rieger Fail to Disclose a Sensor “Tightly Coupled” to a Memory

Petitioner fails to show that either Glass or Rieger disclose a sensor that is “tightly coupled” to memory under either Petitioner’s own construction or under Patent Owner’s proposed construction. First, as previously explained, Petitioner fails to show any teaching in Glass disclosing that the sensor (or camera) is coupled to the memory via “conductive traces or leads.” POR at 13-14. However, the only evidence in Glass relied upon by Petitioner and its expert is an illustration in Figure 2 showing a connection by an arrow between “Optics and Camera 6” and “Digitizer and Frame Store 8.”

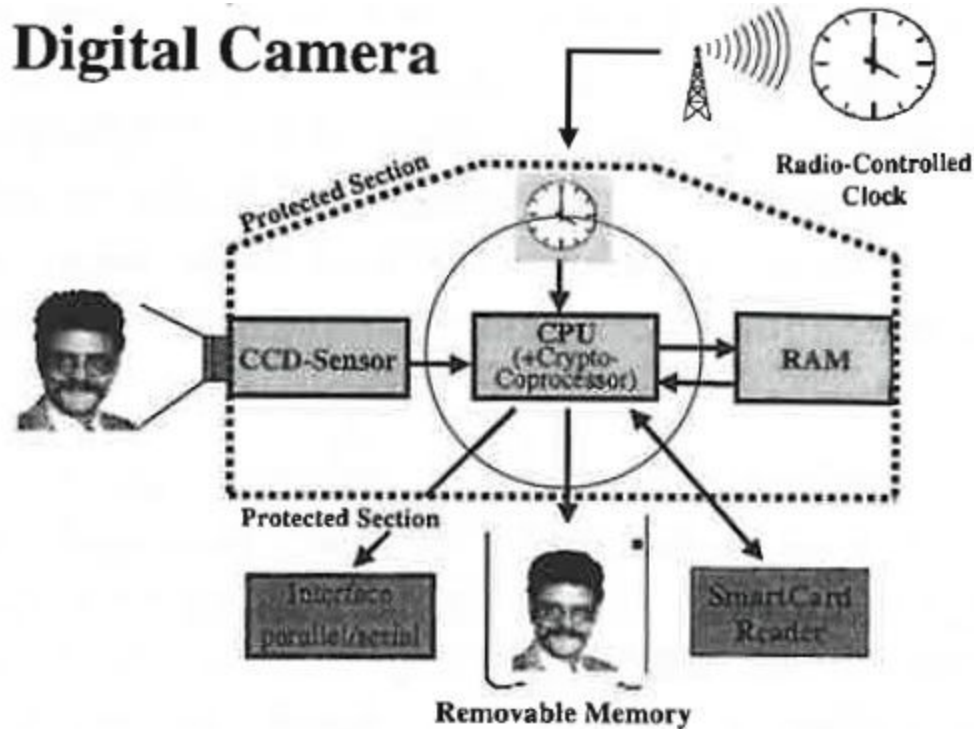


EX1003, Fig. 2 (annotated)

Petitioner’s Reply argues that Glass describes and depicts “an integrated circuit... is connected to a circuit board by leads... that are soldered or otherwise

connected to traces.” Reply at 11. However, there are several deficiencies in Petitioner’s supposition. First, there is no disclosure in Glass that the camera sensor and the frame store memory are implemented as integrated circuits, nor does Petitioner cite to any. *Id.* Second, there is no showing that, even if they were implemented as integrated circuits, they are located on the same circuit board. *Id.* And, finally, the assertion that the arrow represents a physical as opposed to an operational data path is entirely conclusory in the context of Glass. The arrow merely identifies that an *operational* data path exists, but this is not sufficient to show that the *physical* connection between the components as required under both Petitioner’s and Patent Owner’s proposed constructions for “tightly coupled.” POR at 14-20.

Petitioner fails to show that Rieger discloses this limitation for similar reasons. Petitioner fails to show any teaching in Rieger disclosing that the sensor is coupled to the memory via “conductive traces or leads.” POR at 28-35. But the only actual evidence in Rieger cited by Petitioner and its expert is Figure 3, merely depicting arrows between “CCD-Sensor,” “CPU” and “RAM.”



Rieger, Figure 3

Petitioner's Reply argues that the CPU, CCD, and RAM "are integrated are integrated circuits commonly interconnected by leads and traces on a circuit board." Reply at 11. But, even if these components were integrated circuits, there is no showing beyond that they are located on the same circuit board. *Id.* Specifically, in many digital devices, including digital cameras and computing devices generally, these components are often implemented on different circuit boards, which can be connected by interfaces and cables. And, like in Glass, the assertion that the arrows between represent a physical as opposed to an operational data paths is entirely conclusory. Specifically, as depicted in Figure 3, a radio transmitter is connected by the same arrow depiction to the protected section, but because any information from

the transmitter is by radio waves, these would not be physical connections. Like Glass, the arrow in Rieger identifies that an *operational* data path exists but does not depict a *physical* connection as required under both Petitioner's and Patent Owner's proposed constructions for "tightly coupled." POR at 28-35. As such, Rieger indisputably depicts *non-physical, operational* connections with an arrow.

Petitioner argues that, in the prosecution history of the '828 Patent, the applicant referred to it being "virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor." EX1002 at 277, Reply at 12. Petitioner appears to contend that the lines depicted in Figure 2A of the '828 Patent disclose connections by conductive leads and traces. This reasoning is incorrect for several reasons. First, lines in Figure 2A do not represent physical connections by conductive leads and traces because one connection is to a 3.5" Floppy Disk which would not be connected by leads and traces due to the nature of the medium. EX1001 at Fig. 2A. Second, many other items are merely items of data that is provided to the processor and are not physical components that could be connected by conductive leads and traces. *Id.* Finally, the applicant never represents to the examiner that lines in Figure 2A represent conductive leads and traces. EX1002 at 277.

Petitioner makes the irrelevant observation that U.S. Patent No. 5,486,853 (EX2007), which discloses the use of a cable for transferring data, is not applicable

because the system described there was not contained within a single device. Reply at 13. However, Patent Owner did not identify this reference to show that it met the claims of the '828 Patent, but rather to show that it was known at that time that a cable could transfer data from a camera sensor to memory. Nor do the claims include a single device limitation. As such, Petitioner's single device argument is irrelevant in the context of the '828 Patent claims. Substantively, it is undisputed that a POSITA would know that a data path could be created using a cable at the time of the '828 Patent. Petitioner also argues that using a coaxial cable would require additional space and cost. Reply at 13-14. However, Petitioner presents no objective evidence showing that cable connections would add additional cost or expense. *Id.* Further, Petitioner's expert does not dispute that it was known to connect components within digital devices using cables at this time. EX2013 at 52:13-54:5. Petitioner also fails to present any argument for limiting connections by cable only to coaxial cable connections. Reply at 13-14.

Petitioner makes the same argument that U.S. Patent 7,161,622, which utilizes wireless transmissions for conveying data from a camera, was not within a single device. Reply at 14. However, as above, there is no requirement in the '828 Patent that data transfers be within a single device, and Petitioner does not dispute that transmissions by wireless data paths were known at the time of the '828 Patent and of the Glass and Rieger references. The same deficiencies also apply to Petitioner's

argument relating to U.S. Patent 6,377,981 (EX2009), which utilizes satellite to transfer information because there is no single device requirement in the '828 Patent, and Petitioner does not dispute that transmissions by wireless satellite data paths were known at the time of the '828 Patent and of the Glass and Rieger references.

B. Glass and Rieger Fail to Disclose the “Monitoring” Step

Claim 1 explicitly requires “*monitoring* the integrity of the tight *coupling* between said memory and said sensor.” EX1001 at Claim 1. As such, the claim explicitly requires monitoring the coupling between the memory and the sensor to ensure that the integrity of the coupling itself is not disturbed. However, for the Glass and Rieger references, Petitioner fails to show “*monitoring* the integrity of the tight *coupling* between said memory and said sensor” in both.

In Glass, Petitioner argues that monitoring tamper-resistant package 50 is the same as monitoring the integrity of the coupling between memory and a sensor within the package. Reply at 16. However, Petitioner concedes that Glass does not actually monitor the integrity of the coupling between the sensor and the memory in Glass. *Id.* Petitioner instead argues that because these, and other, components are located within a tamper resistant package that Glass discloses the monitoring step. *Id.* Similarly, Rieger does not monitor the coupling between the sensor and memory, but instead monitors a “secure compartment” containing several components, including a sensor and memory. *Id.*, EX1006 at 4.

However, the specification of the '828 Patent does not disclose monitoring a container for multiple components, but rather it monitors the integrity of the coupling between the sensor and memory. Specifically, 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. Internal security system 14 is monitored to determine whether 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.

Petitioner argues that, in the prosecution history, the applicant stated “a signal is generated if the device that prevents physical access to the interconnections between the sensor set and memory is broken.” Reply at 17. However, as shown above, this reference is to “internal security 14” which monitors the tight coupling between the sensor set and the recorder. EX1001 at 4:65-67. As such, the focus of “internal security 14” is upon the connection between the memory and the sensor; there is no description in either the specification of monitoring a container with multiple components such as the “tamper resistant package” of Glass or the “secure compartment” of Rieger. As such, the '828 Patent, which monitors the interconnection between the sensor and the memory, is readily distinguishable from both Glass and Rieger.

C. Glass Fails to Disclose “OK” and “Error” Signals

As explained previously. Glass does not “generat[e] an error signal that is displayed to a user to indicate that said stored data stream is not authentic.” POR at 23-25. However, Glass does not display error signals to users when a data stream is determined not to be authentic. Instead, Glass discloses maintaining a “record of the transaction” on the server. EX1005 at 10:54-58. Petitioner argues that, because the result of an authentication determination is saved to a log file on the server, this limitation is met. Reply at 18. Petitioner’s argument is deficient in at least three respects.

First, Petitioner concedes that a user would not receive any display of an error signal because the contents of the log file would not be displayed unless and until the user reviewed the log file. *Id.* However, Claim 1 does not recite “generating an error signal that *may be displayed* to a user;” the claim recites “generating an error signal *that is displayed* to a user.” The mere possibility of display is therefore insufficient.

Second, there is no reason to assume that the user would have access to the log file described in Glass. By its terms, Glass records authentication determinations to a log file on a server, not the user’s local device. EX1005 at 10:54-58. Because the information is recorded on the server, the user may not have access to the log files. For example, system log files are routinely available only to administrators of

a server.

Third, as explained in POR, Glass fails to generate any signal that is displayed to a user when the error is detected. POR at 23-24. Petitioner misconstrues this as inserting a strict temporal requirement into the claim. Reply at 19. However, the issue is not immediacy, the issue is certainty. Because the claim recites “generating an error signal that is displayed to a user,” the claim requires assurance that signal is actually displayed to the user. As such, the issue is not temporal, the issue is that records in a log file are potentially *never* displayed to a user. In short, the issue is not temporality but rather certainty, as required by the claim language.

For these reasons, Petitioner fails to show that Glass discloses “generating an error signal that is displayed to a user.” For the similar reasons, Petitioner also fails to show “generating an ok signal that is displayed to a user.”

D. Rieger Fails to Disclose “OK” and “Error” Signals

Petitioner essentially concedes that Rieger does not actually disclose generating an error signal (nor an ok signal) that is displayed to the user. Reply at 19-20. Petitioner attempts to overcome the fact that Rieger does not actually disclose displaying such signals to a user by arguing that Figure 7 of Rieger includes smiling and frowning faces in the figure and by making the supposition that displaying similar faces to a user would be a “design choice.” *Id.* However, merely stating that an element is a design choice does not make it obvious; there must be explanation

for *why* a POSITA would have made the specific design choice. *Cutsforth, Inc. v. MotivePower, Inc.*, 636 F. App'x 575, 578 (Fed. Cir. 2016). This is not a situation where one type of indication is substituted for another; rather, there is no disclosure in Rieger regarding the display of *any* indication of the success or failure of any authentication determination. As such, because no indication to the user is described in Rieger, it does not represent “the mere substitution of one element for another known in the field.” *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Instead, Petitioner attempts to add an element that is entirely absent in Rieger. Because the element is completely absent, it would not be a mere design choice to add the omitted element.

V. SERRET-AVILA COMBINED WITH GLASS OR RIEGER FAILS TO RENDER THE CLAIMS OBVIOUS

A. Serret-Avila Is Non-Analogous Art

Serret-Avila is non-analogous art to the '828 Patent as well as to the Glass and Rieger. 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.” *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011). As explained in POR, Serret-Avila relates to a “verify[ing] the authenticity of [a] communication” by using “check values... constructed from the original content of the communication.” POR at 44; EX1011 at Abstract. In contrast, Glass and Rieger (like the '828 Patent) are generally directed to authenticating image

data from an imaging sensor (such as a camera). POR at 44. Because Serret-Avila is from the field of internet transactions or e-commerce security, while the '828 Patent, Glass, and Rieger are in the field of digital image security, a POSITA would regard them as representing separate fields.

In its reply, Petitioner argues that Serret-Avila is analogous art to the '828 because they allegedly “involve data streams including digital images” and allegedly “address the same problem of authenticating data streams including digital images.” Reply at 22. However, Serret-Avila does not even once use the term “image.” EX1011. Instead, as explained in POR, A POSITA would regard the field of digital image validation (of the '828 Patent) as a separate field of endeavor from the field of internet security (of Serret-Avila) because validation of digital images to ensure the integrity and authenticity of the images involves unique problems specific to detecting manipulation of images. POR at 44-45; EX1006 at 1 (“it is becoming increasingly difficult to detect and show proof of professional image manipulation aided by digital methods”). Nor would Serret-Avila be pertinent to the particular problem with which the inventor is involved because Serret-Avila is not concerned with any aspects of authenticating digital images, and it does not address any security considerations specific to digital images. POR at 45. As such, Petitioner has failed to establish that Serret-Avila is analogous art.

B. A POSITA Would Not Have Been Motivated to Combine Serret-Avila with Glass or Rieger

A POSITA would not be motivated to combine Serret-Avila with Glass or Rieger. As explained in POR, the three references use incompatible approaches to informing users whether or not information has been authenticated. POR at 45-46. Glass is an offline system the records authentication determinations to a server, and a user would therefore not receive the result of any authentication determination when it was made. *Id.*, EX1005 at 1:7-9, 9:61-64. Serret-Avila, which uses an online system, provides warnings to users which, unlike Glass, requires the user to be online. *Id.*, EX1011 at 10:39-45. And Rieger fails to disclose any method for disclosing any authentication determination to users. *Id.*, EX2006 at 12. As explained in POR, because the offline, online, and silent systems represented by the three systems are incompatible with each other, a POSITA would be discouraged from combining the references. POR at 46.

Petitioner makes conclusory assertions that a POSITA would be motivated to combine the systems, but makes no effort to explain *how* a POSITA would make the combination of incompatible systems. Reply at 23. For example, Petitioner does not explain how the online system of Serret-Avila could be combined with Glass, which makes determinations offline and therefore could not present online notifications since the user may not be present at the time the determination is made.

Id. Nor does Petitioner explain how the online notifications of Serret-Avila could be combined with Rieger, which provides neither online nor offline notifications.

Id.

C. Serret-Avila Does Not Disclose Generating an “OK Signal” Indicating That the Data Stream Is Authentic

Serret-Avila fails to disclose an “ok signal” because it only displays notification messages when hash values are determined to be unauthentic. POR at 47-48; EX1011 at 10:39-45. Serret-Avila discloses displaying “a warning or error message” when hash values show that a sub-block in a data stream is not authenticated. EX1011 at 10:39-45. However, Serret-Avila displays no corresponding message to the user when hash values show that a data stream has been authenticated.

Petitioner attempts to overcome this deficiency by arguing that, when a sub-block is authenticated, it is “released for use (518)” and that presentation of a sub-block to the user is an “ok signal.” Reply at 18. However, there are multiple deficiencies in Petitioner’s theory. First, the fact that a car continues running is not a signal displayed to the user that a car has gasoline; it is only the regular consequence of the car having gasoline. In the same way, that the sub-block is released for use by the system is not a visual “ok signal” displayed to the user; it is only the regular consequence of each successive block being available. Second, the

very portion of Serret-Avila relied upon by Petitioner shows that making a sub-block available for use will not necessarily result in any visual indication being presented to the user on the display in multiple situations, such as when the data stream is an audio stream provided to speakers or when it is a document provided to a printer. Reply at 26, EX1011 at 15:47-50 (“If the content is deemed to be authentic, it is released for use (e.g., sent to the *system’s speakers*, display screen, *printer*, etc.)”). Content intended for the system’s speakers or the printer would indisputably not be presented to the user on the display and would thereby provide no “ok signal” as recited in Claim 1, even under Petitioner’s tortured application of the claim language. Petitioner fails to show that this limitation is disclosed in Serret-Avila.

VI. CONCLUSION

For the above reasons, the Board should hold that all challenged claims are patentable.

Date: October 10, 2025

Respectfully submitted,

/ Bryan D. Atkinson /
Bryan D. Atkinson (Reg. No. 52,574)
batkinson@princelobel.com
PRINCE LOBEL TYE LLP
500 W. 2nd Street, Suite 1900
Austin, Texas 78701
Telephone: (512) 737-2403
Fax: (617) 456-8100
Counsel for Patent Owner

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

The undersigned certifies that on October 10, 2025, I will cause true and correct copies of the foregoing Patent Owner's Surreply to Petitioner's Reply, 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@princelobel.com
PRINCE LOBEL TYE LLP
500 W. 2nd Street, Suite 1900
Austin, Texas 78701
Telephone: (512) 737-2403
Fax: (617) 456-8100

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 5,248 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: October 10, 2025

Respectfully submitted,

/ Bryan D. Atkinson /

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

batkinson@princelobel.com

PRINCE LOBEL TYE LLP

500 W. 2nd Street, Suite 1900

Austin, Texas 78701

Telephone: (512) 737-2403

Fax: (617) 456-8100

Counsel for Patent Owner