

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ADOBE INC.,
Petitioner,

v.

JONATHAN E. JAFFE,
Patent Owner.

IPR2024-01352
Patent 6,757,828 B1

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Patent Owner’s Expert Is Not a POSITA and Applies the Wrong Burden of Proof	1
III.	Claim Construction Issues	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”	7
	C. “based on”	9
IV.	Both Glass and Rieger Disclose the Limitations of Claim 1.....	10
	A. Glass and Rieger Disclose a Sensor “Tightly Coupled” to a Memory	10
	B. Glass and Rieger Disclose the “Monitoring” Step.....	16
	C. Glass Discloses an “OK” or “Error” Signal Indicating Whether the Data Stream Is Authentic or Not	17
	D. Rieger Discloses an “OK” or “Error” Signal Indicating Whether the Data Stream Is Authentic or Not	19
V.	Combining Serret-Avila with Glass or Rieger Renders the Claims Obvious.....	21
	A. Serret-Avila Is Analogous Prior Art	21
	B. A POSITA Would Have Been Motivated to Combine Serret-Avila with Glass or Rieger	23
	C. The Combination of Glass or Rieger with Serret-Avila Discloses Generating an “OK Signal” Indicating That the Data Stream Is Authentic	24
VI.	Conclusion	28

TABLE OF AUTHORITIES

FEDERAL CASES

<i>Apple Inc. v. Andrea Electronics Corp.</i> , 949 F.3d 697 (Fed. Cir. 2020)	2
<i>Axonics, Inc. v. Medtronic, Inc.</i> , 75 F.4th 1374 (Fed. Cir. 2023)	6
<i>In re Bigio</i> , 381 F.3d 1320 (Fed. Cir. 2004)	22
<i>Google LLC v. MindbaseHQ, LLC</i> , 2025 WL 2471511 (Fed. Cir. Aug. 28, 2025)	2
<i>Iridescent Networks, Inc. v. AT&T Mobility, LLC</i> , 933 F.3d 1345 (Fed. Cir. 2019)	4, 5
<i>In re Kuhle</i> , 526 F.2d 553 (CCPA 1975)	20
<i>Kyocera Senco Indus. Tools Inc. v. Int’l Trade Comm’n</i> , 22 F.4th 1369 (Fed. Cir. 2022)	3
<i>Liberty Ammunition, Inc. v. United States</i> , 835 F.3d 1388 (Fed. Cir. 2016)	4
<i>Recor Medical, Inc. v. Medtronic Ireland Mfg. Unlimited Co.</i> , 2025 WL 944511 (Fed. Cir. Mar. 27, 2025)	21
<i>Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.</i> , 66 F.4th 1373 (Fed. Cir. 2023)	21, 22
<i>Sierra Wireless, ULC v. Sisvel S.p.A.</i> , 130 F.4th 1019 (Fed. Cir. 2025)	3
<i>UCB, Inc. v. Actavis Labs. UT, Inc.</i> , 65 F.4th 679 (Fed. Cir. 2023)	23, 24
<i>Ultravision Techs., LLC v. Govision, LLC</i> , 2023 WL 2182285 (Fed. Cir. Feb. 23, 2023)	4, 5

ADMINISTRATIVE DECISIONS

<i>Danxiao Information Tech. v. Shenzhen Svakom Tech. Co.</i> , PGR2022-00050, Paper 36 (PTAB Jan. 19, 2024).....	22
<i>Puzhen Life USA, LLC v. ESIP Series 2, LLC</i> , IPR2017-02197, Paper 24 (PTAB Feb. 27, 2019).....	2
<i>Samsung Electronics Co. v. Google LLC</i> , IPR2024-00810, Paper 20 (PTAB Nov. 26, 2024).....	21
<i>Volkswagen Group of America, Inc. v. Michigan Motor Techs. LLC</i> , IPR2020-00446, Paper 9 (PTAB Aug. 25, 2020).....	20
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022).....	1

FEDERAL STATUTE

35 U.S.C. § 316.....	3
----------------------	---

I. INTRODUCTION

Petitioner established in the petition how the prior art, primarily Glass and Rieger, discloses and renders obvious every limitation of the challenged claims. In response, Patent Owner repeats the arguments from his Preliminary Response (Paper 7), adding only a supporting declaration by Bill Davis who parrots the same arguments. Further, Mr. Davis lacks relevant experience and applies the wrong burden of proof (clear and convincing evidence) rather than the correct preponderance standard. Patent Owner’s arguments ignore express disclosures in the prior art, impose improper claim constructions to manufacture distinctions with the prior art, and offer legally defective arguments—all based on expert testimony under the wrong burden of proof. Petitioner respectfully requests that the Board reject Patent Owner’s arguments and find the challenged claims invalid as obvious.

II. PATENT OWNER’S EXPERT IS NOT A POSITA AND APPLIES THE WRONG BURDEN OF PROOF

Patent Owner largely agrees with Petitioner’s definition of a POSITA but disagrees that such a person would have “experience involving image processing.” Paper 16 (“POR”), 4. Patent Owner’s argument is based on the declaration of his expert witness, whose testimony is entirely conclusory—he does not cite any evidence or reasoning supporting his assertion. EX2005, ¶56. Such conclusory expert testimony is due little or no weight. *See Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB Aug. 24, 2022) (finding “conclusory and

unsupported” expert testimony of “little weight”); *Puzhen Life USA, LLC v. ESIP Series 2, LLC*, IPR2017-02197, Paper 24 at 29 (PTAB Feb. 27, 2019) (finding “conclusory and unsupported” expert testimony “unhelpful and unpersuasive”).

In contrast, Petitioner’s expert, Dr. Zixiang Xiong, described his understanding of the legal framework for defining a POSITA, stated his opinion, and cited evidence and reasoning supporting his opinion. EX1003, ¶¶27-29, 81-89. Petitioner’s definition is well-supported and should be applied in this proceeding. *Id.*; EX1029, ¶¶3-9. Nevertheless, Dr. Xiong, who more than qualifies as a POSITA under Patent Owner’s proposed definition, confirms in a reply declaration that his opinions regarding the obviousness of the challenged claims would not change even if that definition were applied. EX1029, ¶11.¹

Patent Owner presumably disputes the reference to “experience involving image processing” in the definition of a POSITA because his expert witness, Mr. Davis, does not have any such experience. Mr. Davis’s *curriculum vitae* describes him as a “[s]oftware developer and cloud architect with 20 years of

¹ Petitioner appropriately provides additional argument and evidence in reply responding to Patent Owner’s arguments. *See Google LLC v. MindbaseHQ, LLC*, 2025 WL 2471511, at *5-6 (Fed. Cir. Aug. 28, 2025); *Apple Inc. v. Andrea Electronics Corp.*, 949 F.3d 697, 707 (Fed. Cir. 2020).

programming experience developing large scale distributed high-performance systems,” but makes no mention of any experience related to digital image processing, digital video or multimedia, optical sensors, or digital cameras.

EX2006; EX2005, ¶¶5-14. Because Petitioner’s definition of a POSITA is correct and because Mr. Davis does not meet it, his opinions from the perspective of such a person should be disregarded. *See Sierra Wireless, ULC v. Sisvel S.p.A.*, 130 F.4th 1019, 1025 (Fed. Cir. 2025) (abuse of discretion to credit expert testimony by a witness that did “not satisfy the requirements for an ordinarily skilled artisan”); *Kyocera Senco Indus. Tools Inc. v. Int’l Trade Comm’n*, 22 F.4th 1369, 1376-77 (Fed. Cir. 2022) (“To offer expert testimony from the perspective of a skilled artisan in a patent case—like for claim construction, validity, or infringement—a witness must at least have ordinary skill in the art.”).

The Board should disregard Mr. Davis’s opinions for the further reason that he applied the wrong burden of proof when assessing the evidence and rendering his opinions. Mr. Davis incorrectly assumed that Petitioner must establish obviousness by clear and convincing evidence (EX2005, ¶¶19, 30, 49), though Petitioner’s actual burden in this proceeding is to show that the challenged claims are obvious only by a preponderance of the evidence. 35 U.S.C. § 316(e).

III. CLAIM CONSTRUCTION ISSUES

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

Patent Owner disputes Petitioner’s proposed construction of this term as “a sensor coupled to said memory via conductive traces or leads” because the reference to traces or leads during prosecution is “exemplary only.” POR, 5. The term “tightly coupled” is a term of degree (i.e., the sensor and memory are not merely “coupled,” they are “**tightly** coupled”) and such terms must be construed based on some objective measure, which can be provided by examples in the intrinsic evidence. *See Ultravision Techs., LLC v. Govision, LLC*, 2023 WL 2182285, at *3-*4 (Fed. Cir. Feb. 23, 2023); *Iridescent Networks, Inc. v. AT&T Mobility, LLC*, 933 F.3d 1345, 1350-52 (Fed. Cir. 2019); *Liberty Ammunition, Inc. v. United States*, 835 F.3d 1388, 1395-97 (Fed. Cir. 2016). The applicants’ reference to breaking the conductive trace or lead between the memory and processor is the **only** description of any connection between components the applicants considered to be “tightly coupled.” Paper 2 (“Pet.”), 10.² Thus,

² Patent Owner notes the applicants distinguished Shipper because it involved external information provided from outside the device. POR, 7. In that discussion, the applicants identified what does not constitute “tightly coupled” components without describing what does. EX1002, 277.

Petitioner’s proposed construction appropriately incorporates the sole example in the intrinsic record (i.e., via conductive leads and traces).

Patent Owner argues the Board should disregard the applicants’ reference to “the conductive trace or lead between the memory and the processor” because “there is no clear and unmistakable disclaimer...specifically limiting the claim language to conductive traces or leads.” POR, 6. But the “prosecution history is relevant for more than an evaluation of disclaimer—it provides additional context for evaluating how the term would be understood and how it was used in the patent.” *Ultravision*, 2023 WL 2182285, at *4. As the Federal Circuit has explained, “where there is no clear ordinary and customary meaning of a coined term of degree, we may look to the prosecution history for guidance without having to first find a clear and unmistakable disavowal.” *Iridescent Networks*, 933 F.3d at 1352-53 (rejecting the argument Patent Owner makes here). The term “tightly coupled” is such a “coined term of degree” with “no clear and customary meaning.” Pet., 9; *Iridescent Networks*, 933 F.3d at 1353. Thus, the Board need not find “a clear and unmistakable disavowal” to determine that the sole example of “tightly coupled” components in the intrinsic record confirms Petitioner’s proposed construction.

While Petitioner’s proposed construction is correct, this dispute is immaterial because Patent Owner proposes a ***broader construction*** that is also

disclosed by the prior art. Patent Owner argues that “a sensor, which is tightly coupled to said memory” means “a sensor that is electrically or physically coupled to memory in a device.” POR, 9. Both Glass and Rieger meet Patent Owner’s proposed construction for the same reasons described in the petition. As Petitioner explained, Glass’s Figure 3 shows “the *sensor* (in Optics 41 and Imager & Digitizer 42) and *memory* (frame store memory 43) are ***electrically connected*** together within imaging system 4.” Pet., 26.³ Similarly, Petitioner explained that Rieger’s Figure 3 shows “the *sensor* and *memory* are ***electrically connected*** together within the protected compartment” of Rieger’s manipulation-proof digital camera. *Id.*, 44. Under either party’s construction, the prior art discloses this limitation. EX1029, ¶¶13-15; see *Axonics, Inc. v. Medtronic, Inc.*, 75 F.4th 1374, 1382-83 (Fed. Cir. 2023) (permitting reply evidence and argument in response to patent owner’s construction).

Finally, as the Board noted in its Institution Decision, the applicants stated during prosecution that, “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.” Paper 8, 18-19 n.6 (citing EX1002, 292). Petitioner cited the passage as support for its proposed construction of claim 1’s

³ All emphasis using bold and italics is added.

“monitoring” step because applicants’ statement refers to the term “tight coupling,” which appears in the “monitoring” step. Pet., 11; EX1002, 292-293. Should the Board conclude, however, the claim limitation reciting “a sensor, which is tightly coupled to said memory” further requires that “the connections between the sensor and the memory not be physically accessible to the user,” it would be disclosed nevertheless by both Glass and Rieger. EX1029, ¶¶16-18. Glass states that the optical sensor and memory are enclosed in “a tamper resistant package 50” in imaging system 4. Pet., 30-31. The tamper resistant package prevents access to the components and interconnections inside. EX1005, 5:13-41, Fig. 3. Similarly, Rieger’s optical sensor and memory are enclosed in a “secure compartment” within the digital camera. Pet., 48-50. The secure compartment prevents access to the internal components/interconnections. EX1006, 4, Fig. 3. Thus, in both references, the connections between the sensor and the memory are not physically accessible to the user. EX1003, ¶¶175, 232.

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

Patent Owner argues the “monitoring” step of claim 1 means “determining whether the physical coupling between said memory and said sensor has been accessed or disturbed.” POR, 11. He further argues that his proposed construction requires “monitoring the specific coupling between the memory and the sensor and determining when that specific coupling has been accessed or disturbed.” *Id.*, 20.

His proposed construction—and further explanation of it—is apparently intended to exclude the security features disclosed by Glass and Rieger that determine whether access has been gained to the secure device’s internal components and interconnections including the connection between sensor and memory. But Patent Owner’s narrow construction is not supported by the claim language, which does not require “specifically” monitoring the tight coupling, and is contradicted by the specification and file history.

Contrary to Patent Owner’s argument, the specification does not describe “specifically” monitoring the physical connection between sensor and memory. Instead, 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.” EX1001, 4:65-67. The patent explains that, during the camera’s pre-capture processing, “a check 59 of the internal security system 14” is performed and “[i]f there is a breach of security 60 the violation is recorded 61.” *Id.*, 5:44-46; *see also id.*, 6:64-66 (“If internal security is compromised 60 a security violation 61 is appended 123 to the image.”), Fig. 4A2 (step 59: “Internal Security Compromised?”). Thus, the specification describes monitoring “the integrity of the tight coupling” by checking the “internal security system” to determine if “internal security” of the camera has been compromised (just as in Glass and Reiger).

The ’828 Patent’s file history also contradicts Patent Owner’s narrow reading of the “monitoring” step. During prosecution, the applicants amended claim 1 to add the “monitoring” step and argued that it was not disclosed by the cited prior art. EX1002, 290, 292-293. They described the “monitoring” step with reference to Figure 4A (step 59) and argued that “a signal is generated if the device that prevents physical access to the interconnections between the sensor set and memory is broken.” *Id.*, 293. In other words, the “monitoring” step is performed by determining whether “the device” preventing access to the tight coupling “is broken” (just as in Glass and Reiger); the claim is not narrowly limited to determining whether the tight coupling itself is broken. Thus, the applicants’ own argument distinguishing the prior art confirms that the “monitoring” step means “determining whether physical access has been gained to the coupling between said memory and said sensor.” Pet., 10-11.

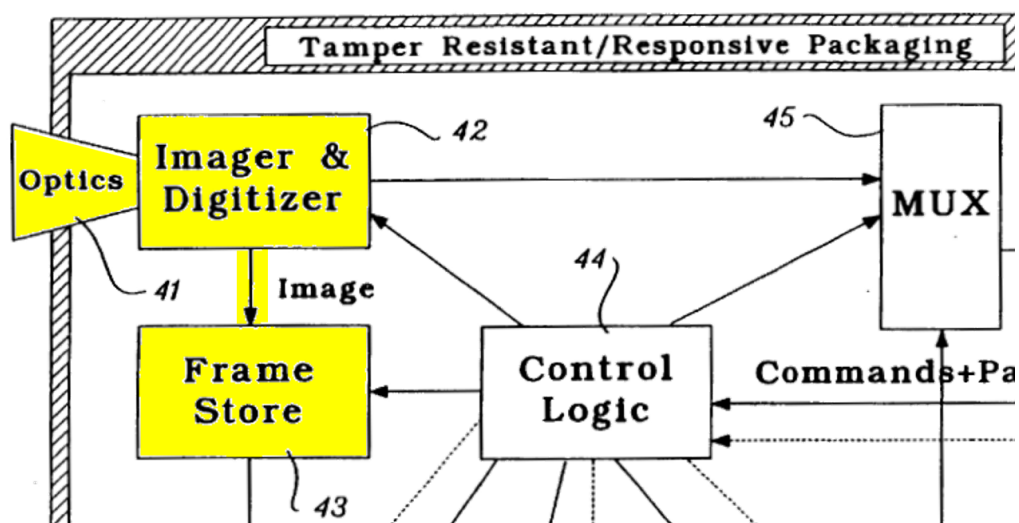
C. “based on”

Contrary to Patent Owner’s argument, Petitioner provided a proposed construction for the term “based on” in claim 1: “based on” is open-ended (i.e., based at least on what follows). Pet., 11-13. It is undisputed.

IV. BOTH GLASS AND RIEGER DISCLOSE THE LIMITATIONS OF CLAIM 1

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

As explained in the petition, Glass’s Figure 3 illustrates a *sensor* (in Optics 41 and Imager & Digitizer 42) and *memory* (frame store memory 43) that are electrically connected via leads and traces within imaging system 4. Pet., 26. Patent Owner criticizes Petitioner’s expert testimony on this point as “conclusory,” but it is well supported by Glass. For instance, Glass states that the optical sensor can be a “CCD camera, a CMOS device or other two dimensional imager which creates a digital image.” EX1005, 5:49-52. “The digital image is sent to...a frame store memory 43” using the “data path” indicated by the arrow from Optics 41/Imager & Digitizer 42 to Frame Store 43 in Figure 3. *Id.*, 5:46-48, 5:52-54.



Glass, Figure 3 (excerpt, highlighted)

A POSITA would have known that an integrated circuit (e.g., CCD, CMOS, two dimensional imager) is connected to a circuit board by leads (i.e., conductive wires or balls) that are soldered or otherwise connected to traces (i.e., wires running through circuit boards). EX1003, ¶¶170-171, 175; EX1029, ¶14.

Similarly, Rieger’s Figure 3 illustrates a *sensor* (CCD-Sensor) and *memory* (RAM) that are electrically connected, via the CPU, by conductive leads and traces in Rieger’s manipulation-proof digital camera. Pet., 26; EX1003, ¶¶228-233.

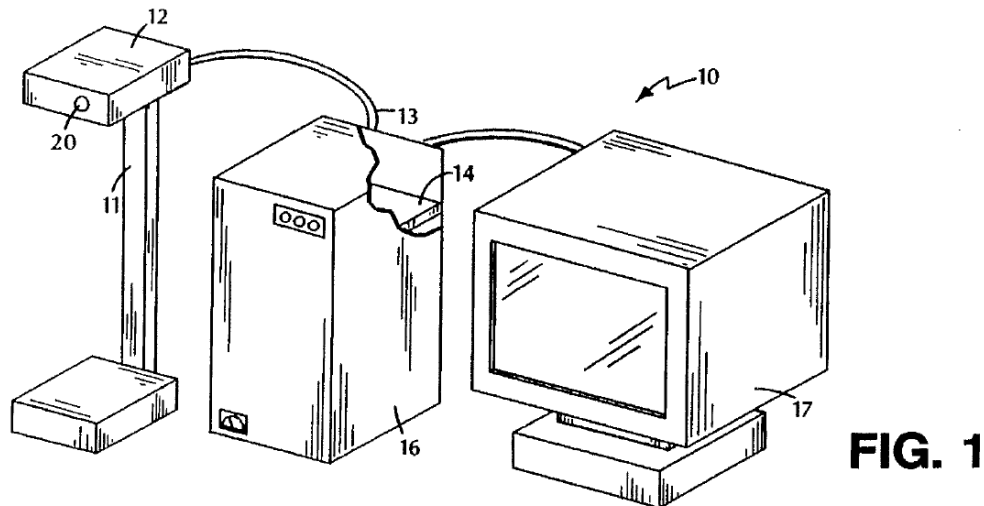
Again, Petitioner’s expert testimony is well supported. Rieger states that “[t]he camera processor consists essentially of a high-speed RISC processor, an interface to the CCD chip,...[and] an interface to a RAM....” EX1006, 4. A high-speed RISC processor (CPU), CCD chip, and RAM are integrated circuits commonly interconnected by leads and traces on a circuit board. EX1029, ¶15. Further, Rieger states that the CCD-Sensor, CPU, and RAM are inside a “Protected Section” of the digital camera (EX1006, 4), suggesting to a POSITA that the connection between those components should be secure, as it would be if the connections are made using leads and traces. EX1029, ¶15.⁴

⁴ Glass and Rieger each disclose “a sensor that is electrically...coupled to memory in a device,” meeting Patent Owner’s proposed construction of this limitation. Pet. 26, 44; EX1003, ¶¶171, 228; EX1029, ¶13-15.

Patent Owner criticizes Petitioner’s expert testimony regarding the similarity between the Glass and Rieger figures and the applicants’ description of a “tightly coupled” connection in the prosecution history. POR, 17-18, 33-34. During prosecution, the applicants stated that the “tightly coupled” limitation was illustrated in Figure 2A because it shows “a processor 157 which is ‘tightly coupled’ to a memory” meaning that “it will be virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor.” EX1002, 277. The applicants’ explanation is relevant because there is no express reference of conductive traces or leads in the ’828 Patent. The applicants and examiner simply understood that Figure 2A—illustrating a digital camera with solid lines connecting internal components—shows connections via leads and traces (just as in Glass and Rieger).

Patent Owner also argues that “[b]ecause a POSITA would know that there were many ways to connect a CCD [camera/sensor] to either a processor or memory,” Petitioner has not shown that the sensor and memory in Glass/Rieger are connected by conductive leads and traces. POR, 14, 31. Rather than citing anything in Glass or Rieger to suggest a connection other than by leads and traces, Patent Owner instead argues in the abstract that there are other ways to transfer data. But none of Patent Owner’s theoretical alternatives has any relation to Glass or Rieger.

First, Patent Owner cites U.S. Patent No. 5,486,853 (EX2007) disclosing “an electrical cable for connecting an electronic camera to a processor.” POR, 14, 30-31. But that patent does not disclose an optical sensor and processor/memory connected ***within a single device*** as illustrated in Glass and Rieger. Instead, as shown in Figure 1 below, the ’853 Patent discloses “an electric cable 13” connecting “a video electronic camera head 12” to “a video processor card 14, inserted within personal computer 16....” EX2007, 5:17-23.



EX2007, Fig. 1

The patent states that cable 13 is a “coaxial cable” including multiple conductive wires. EX2007, 6:39-42, 648-55, Figs. 7A, 7B.

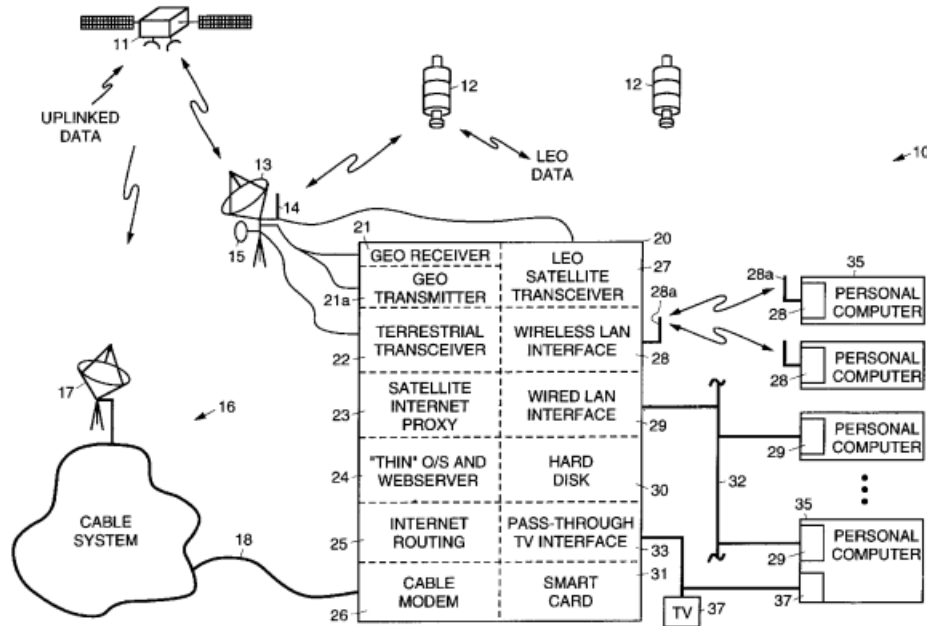
A POSITA would not understand the figures in Glass and Rieger to illustrate an optical sensor connected to a memory using coaxial cable. EX1029, ¶21. Using such cables would require unnecessary additional space and increase the component cost for no offsetting benefit. *Id.* By comparison, connecting the

internal components in the standard manner by soldering leads to traces on circuit boards would require far less space and would be far less expensive. *Id.* Thus, a POSITA would **not** understand the connection from a *sensor* to *memory* in Glass’s imaging system or Rieger’s camera to be via coaxial cable. *Id.*; EX1040, ¶¶18-22.

Second, Patent Owner cites U.S. Patent 7,161,622 (EX2008) disclosing “an electronic camera with a wireless communication interface for transmitting image information from the camera.” POR, 15, 31-32. Again, this patent discloses a first device (digital camera 1) communicating with a second, separate device such as a personal computer. EX2008, 2:64-3:1, 4:24-32. It does not disclose a sensor and memory wirelessly connected ***within a single device***.

A POSITA would not have considered implementing Glass’s imaging system or Rieger’s camera with a connection from the sensor to a wireless transmitter inside the device to send a wireless signal to a receiver connected to memory in the same device. EX1029, ¶23. A POSITA would have realized that one could instead connect the optical sensor to memory using leads and traces, eliminating the wireless transmitter and receiver, reducing the component cost and overall size, and improving performance and security. *Id.* Thus, a POSITA would **not** understand Glass or Rieger to illustrate a wireless connection from optical sensor to memory. *Id.*; EX1040, ¶¶23-28.

Third, Patent Owner cites U.S. Patent 6,377,981 (EX2009) disclosing “a system providing high-speed internet access through satellite communication links.” POR, 15-16, 32. The figure below from the cited patent depicts personal computers in different locations communicating via satellite. EX2009, 2:43-3:10.



EX2009, Figure (at 2)

It does not show, or even suggest, using a satellite to transmit information between two components inside a device, such as a personal computer 35. EX1029, ¶24. A POSITA would certainly **not** understand the connection from *sensor* to *memory* in Glass’s imaging system or Rieger’s camera to be via satellite transmission as Patent Owner seems to suggest. *Id.*, ¶25; EX1040, ¶¶29-33.

B. Glass and Rieger Disclose the “Monitoring” Step

As Petitioner explained in the petition, Glass describes locating the *sensor* and *memory* in tamper resistant package 50, which is “used to detect unwelcome intrusion and render the system useless.” Pet., 30. By monitoring Glass’s tamper resistant package 50, Glass discloses monitoring the integrity of the components and interconnections contained in that packaging including the *tight coupling* between *sensor* and *memory*. *Id.*, 30-32. Similarly, Rieger describes locating the *sensor* and *memory* in a “secure compartment” in Rieger’s manipulation-proof camera. *Id.*, 48-49. Like Glass, Rieger monitors the “secure compartment” to ensure the integrity of the components and interconnections inside including the *tight coupling* between *sensor* and *memory*. *Id.*, 49-50.

In response, Patent Owner argues that the “monitoring” step requires “specifically” monitoring the tight coupling itself. POR, 21, 35-36. But the claim does not recite such a limitation or specify any particular manner of monitoring the integrity of the tight coupling. EX1001, 20:65-21:2. Moreover, Glass and Rieger disclose an approach to monitoring the integrity of internal components/interconnections consistent with the ’828 Patent specification, which describes “a check 59 of the internal security system 14” to determine “[i]f there is a breach of security 60....” EX1001, 5:44-46. Glass and Rieger both disclose monitoring

internal security systems to determine if there has been a breach of security. Pet., 30-32, 49-50.

In addition, Glass and Rieger disclose *monitoring the integrity of the tight coupling* in the same way the applicants described it during prosecution.

Responding to a rejection, the applicants amended claim 1 to include the “monitoring” step and argued that it distinguished the prior art as follows:

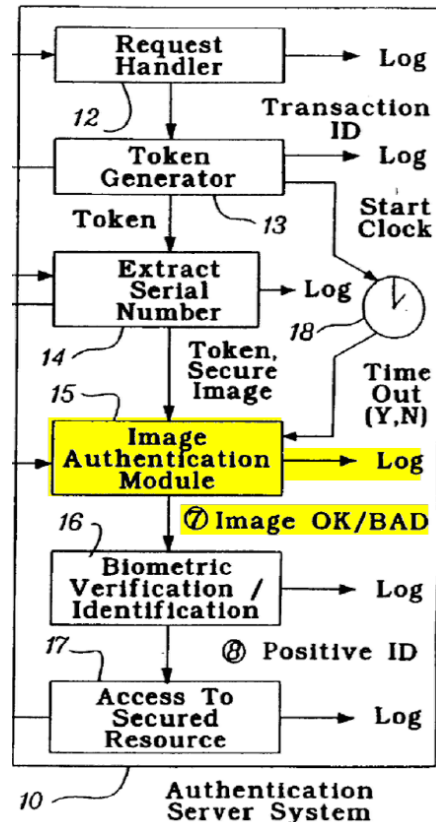
Exemplary disclosure corresponding to this claim feature is shown, for example, in Figure 4A, step 59, which is a flow chart decision block in which it is determined whether internal security has been compromised. This means that, for example, a signal is generated ***if the device that prevents physical access*** to the interconnections between the sensor set and memory ***is broken***.

EX1002, 290, 292-293. The examiner then allowed the patent. *Id.*, 315. Glass and Rieger both disclose internal security systems that monitor the *tight coupling* by determining if the device that prevents physical access to the interconnections between *sensor* and *memory* is broken. Pet., 30-32, 49-50. Thus, Glass and Rieger disclose the “monitoring” step in the very same way the applicants described it in prosecution to gain allowance.

C. Glass Discloses an “OK” or “Error” Signal Indicating Whether the Data Stream Is Authentic or Not

As explained in the petition, Glass discloses *generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic or*

generating an ok signal that is displayed to the user to indicate that said stored data stream is authentic. Pet., 36-38. In particular, Glass’s Figure 8 shows that the result of the image authentication module (i.e., “Image OK/BAD”) is saved in a “Log.”



Glass, Fig. 8 (excerpt, highlighted)

Glass “log[s] each step of the transaction” and “[t]his data can provide irrefutable evidence of the transaction.” EX1005, 9:58-60. Maintaining a record of “evidence” (i.e., the logged authentication result) confirms that the log is meant to be reviewed by a user. Thus, a POSITA would understand that Glass’s image

authentication result, whether an error (“BAD”) or not (“OK”), is logged and displayed to a user. EX1003, ¶205.

In response, Patent Owner argues that “Glass fails to generate any signal that is displayed to a user *when the error is detected*.” POR, 23. But the claim does not state that an error signal is displayed “when the error is detected”; it requires instead only that the error signal “is displayed to a user.” EX1001, 21:12-14. The specification and file history similarly do not impose such a temporal limitation on the claim, and Patent Owner does not argue otherwise. Patent Owner’s only support for this improper temporal limitation is the conclusory assertion of Mr. Davis, who simply repeats the same argument without explanation or citation to evidence. POR, 25; EX2005, ¶86.

Patent Owner repeats the same unsupported temporal argument regarding the “OK signal” limitation. POR, 25-27, 40-41. Again, neither the claim language nor anything in the intrinsic record requires the OK signal to be displayed to the user “when the signal is generated” as Patent Owner argues.

D. Rieger Discloses an “OK” or “Error” Signal Indicating Whether the Data Stream Is Authentic or Not

As explained in the petition, Rieger’s Figure 7 illustrates an integrity test used to authenticate images based on a comparison of hash values. Pet., 54-57. If the hash values are not the same, the data is not authenticated as indicated by a frowning face image in the figure. Petitioner’s expert witness Dr. Xiong explained

that “[t]he frowning face image indicates to a person of ordinary skill in the art that *if said first and second signatures are not the same*, Rieger’s integrity test generates *an error signal* (like a frowning face) *that is displayed to a user to indicate that said stored data stream is authentic.*” EX1003, ¶257. He further explained that “[s]uch a person would recognize that the integrity test would have little or no use if it did not provide such an indication to the *user* when an image is not authentic.” *Id.* Dr. Xiong also explained that the smiling face image in Figure 7 “indicates to a POSITA that *if said first and second signatures are the same*, Rieger’s integrity test generates *an ok signal* (like a smiling face) *that is displayed to a user to indicate that said stored data stream is authentic.* *Id.*, ¶260.

As he explained:

Displaying such a message to the user would be an obvious design choice for a person of ordinary skill in the art. It would require little effort and provide the *user* with a clear indication that the document/image has been validated.

Id.; see also *Volkswagen Group of America, Inc. v. Michigan Motor Techs. LLC*, IPR2020-00446, Paper 9 at 28 (PTAB Aug. 25, 2020) (citing *In re Kuhle*, 526 F.2d 553, 555 (CCPA 1975) finding that the use of a claimed feature “would be an obvious matter of design choice” when it “solves no stated problem” and “presents no novel or unexpected result”).

Patent Owner ignores Dr. Xiong’s explanation for his opinions and instead argues that Rieger does not expressly describe displaying an error/ok signal to the user. POR, 38-41. But prior art is not limited to its express textual descriptions; instead, it “must be considered for everything it teaches” a POSITA. *Recor Medical, Inc. v. Medtronic Ireland Mfg. Unlimited Co.*, 2025 WL 944511, *2 (Fed. Cir. Mar. 27, 2025) (citation omitted). For the understanding of a POSITA, Patent Owner relies on the testimony of Mr. Davis who does not qualify as a POSITA and who analyzed Rieger under the improperly stringent clear and convincing evidentiary burden of proof. Thus, Dr. Xiong’s explanation is unrefuted by any relevant evidence.

**V. COMBINING SERRET-AVILA WITH GLASS OR RIEGER
RENDERS THE CLAIMS OBVIOUS**

A. Serret-Avila Is Analogous Prior Art

Patent Owner argues that Serret-Avila is “non-analogous art” and therefore cannot be used to show obviousness. POR, 43-46. Patent Owner’s argument is fundamentally flawed, however, because he does not compare Serret-Avila to the challenged ’828 Patent—rather he argues only that Serret-Avila is “not analogous art with Glass nor Rieger.” *Id.*, 46. Yet the Federal Circuit has “consistently held” that the analysis “must compare the reference to the challenged patent.” *Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1377 (Fed. Cir. 2023); *see also Samsung Electronics Co. v. Google LLC*, IPR2024-00810, Paper

20 at 22-23 (PTAB Nov. 26, 2024) (“[W]hen more than one prior art reference is used as the basis of an obviousness assertion, it is not required that the references be analogous art to each other.”); *Danxiao Information Tech. v. Shenzhen Svakom Tech. Co.*, PGR2022-00050, Paper 36 at 13 (PTAB Jan. 19, 2024) (“The correct inquiry is whether [the prior art reference] is analogous to the [challenged] patent.”).

Moreover, Serret-Avila **is analogous** to the ’828 Patent. They are both in the same field of endeavor involving data streams including digital images. Pet., 67; EX1003, ¶¶286, 289; EX1029, ¶28.⁵ And they both address the same problem of authenticating data streams including digital images. Pet., 67; EX1003, ¶¶286, 289; EX1029, ¶29. Thus, Serret-Avila is (i) in the same field of endeavor and (ii) addresses the same problem as the ’828 Patent, either of which is independently sufficient to establish that Serret-Avila is analogous prior art. *See In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004).

⁵ Petitioner appropriately supplements on reply its argument and evidence showing that Serret-Avila is analogous prior art. *See Sanofi-Aventis*, 66 F.4th at 1379.

B. A POSITA Would Have Been Motivated to Combine Serret-Avila with Glass or Rieger

As shown in the petition, a POSITA would have been motivated to combine Serret-Avila with Glass to provide in Glass’s imaging system an indication to a user that the image is either authentic or not as taught by Serret-Avila. Pet., 68. A POSITA also would have been motivated to combine Serret-Avila with Rieger to provide in Rieger’s image “integrity test” an indication to the user that the image is authentic or not as taught by Serret-Avila. *Id.*, 68-69. Aside from its erroneous analogous art argument, Patent Owner does not dispute Petitioner’s argument and evidence establishing a motivation to combine.

At most, Patent Owner asserts that the references “teach away” from each other. POR, 46. But a prior art reference only “teaches away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken.” *UCB, Inc. v. Actavis Labs. UT, Inc.*, 65 F.4th 679, 692 (Fed. Cir. 2023) (citation modified). A prior art “reference does not teach away if it merely expresses a general preference for an alternative invention but does not criticize, discredit or otherwise discourage investigation into the invention claimed.” *Id.* (citation modified). Patent Owner offers nothing to meet the standard for “teaching away.”

Instead, Patent Owner asserts that Glass utilizes “an off-line system where a camera provides information to a remote server” (POR, 46) but does not even attempt to show that Glass criticizes, discredits, or otherwise discourages adding an indication to the user that the image is authentic or not as taught by Serret-Avila. Similarly, Patent Owner asserts that Rieger “fails to disclose any means for informing users of the result of any authentication determination at all” (*id.*) but again offers nothing to suggest that Rieger criticizes, discredits, or otherwise discourages a POSITA from combining with Serret-Avila as described. Thus, Patent Owner’s “teaching away” argument fails.

C. The Combination of Glass or Rieger with Serret-Avila Discloses Generating an “OK Signal” Indicating That the Data Stream Is Authentic

Patent Owner argues that Serret-Avila does not disclose *generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic*. POR, 47.⁶ Patent Owner largely ignores Petitioner’s explanation regarding this limitation, which is based on citations to Serret-Avila and the well-supported testimony of its expert Dr. Xiong. Instead, Patent Owner relies entirely

⁶ Patent Owner does not dispute that Serret-Avila discloses the “error signal” limitation of claim 1.

on unsupported assertions about Serret-Avila by his expert Mr. Davis (who is not a POSITA and applied an inappropriately high burden of proof).

As explained in the petition, Serret-Avila discloses a technique in which a data stream (e.g., video, audio, or multimedia) is broken into sub-blocks for authentication by comparing in turn each sub-block’s received hash value to its calculated hash value. Pet., 69; EX1011, 8:32-40, 9:53-59, 10:16-45, Figs. 3, 5. By authenticating successive sub-blocks of the data stream (e.g., streaming video), there is no need to wait for the entire file to download. EX1011, 2:36-49, 3:46-58, 6:31-45. The hash value comparison is illustrated as step 514 in Figure 5.

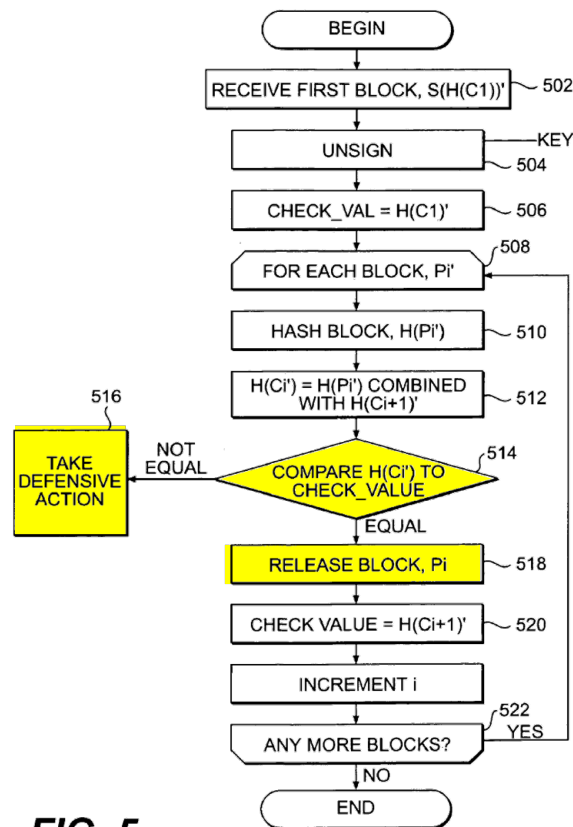


FIG. 5

Serret-Avila, Fig. 5 (highlighted)

When a sub-block is determined to be “unauthentic” based on the comparison, the embodiment illustrated in Figure 5 takes defensive action (516) and does not continue processing additional sub-blocks. On the other hand, if the sub-block is determined to be authentic, it is “released for use (518).” EX1011, 10:28-30. Thus, when the data stream of sub-blocks is presented to the user, the user is informed that it is “ok” (i.e., it is an *ok signal* indicating that the *data stream is authentic*).

In response, Patent Owner argues that “the release of the sub-block of data for use would not normally be displayed to the user.” POR, 47. Patent Owner’s assertion is based on the testimony of Mr. Davis who cites nothing for support. EX2005, ¶115. And contrary to his conclusory assertion, Serret-Avila expressly discloses that authenticated sub-blocks are displayed to the user. For example, Serret-Avila states that “[i]f the content is deemed to be authentic, it is **released for use** (e.g., sent to the system’s speakers, **display screen**, printer, etc.)....” EX1011, 15:47-50. Serret-Avila also states, in a dependent claim, that “at least one use” of an authenticated “first block of data” is “**displaying** the first block of data on **a viewing device**.” *Id.*, 23:6-11.

Patent Owner also argues that Serret-Avila does not disclose the “ok signal” limitation because Serret-Avila “is not directed towards authenticating digital images....” POR, 48. Patent Owner’s argument is again based only on the

conclusory assertion of Mr. Davis (EX2005, ¶115) and is simply incorrect because Serret-Avila in fact discloses techniques for authenticating data streams including digital images. Indeed, Serret-Avila describes embodiments largely in the context of video, audio, or multimedia data. EX1011, 2:36-49, 6:13-18 (“several embodiments are described in the context of a system and method for viewing or playing video, audio, or multimedia data”), 6:46-52, 9:8-11 (“Data 400 may additionally (or alternatively) include video, textual, or multimedia information....”). A POSITA would know “multimedia” data includes digital images. EX1029, ¶28. Additionally, streamed video is composed of a series of frames (e.g., MPEG frames) including many that are essentially individual digital images. *Id.*

Patent Owner also argues that because the data stream is composed of multiple sub-blocks “there would be no indication associated with each sub-block comprising the image.” POR, 47-48. This argument is wrong and beside the point—if the sub-blocks in a data stream are determined to be authentic, then the sub-blocks will be released for use (i.e., presented to the user); otherwise, if a sub-block is determined to be unauthentic, the user will see an error message instead. EX1011, 10:28-45, Fig. 5. Thus, when the user sees the video or other multimedia data stream—which is composed of multiple, individually

authenticated sub-blocks—it *indicate[s]* to the user that *said stored data stream is authentic* as claimed.

Additionally, Patent Owner does not even acknowledge Petitioner’s citation to the “data flow diagram” in Serret-Avila’s Figure 14. That figure shows multiple comparisons between stored and computed hash values to authenticate data, with each comparison indicating either an “Err” (error) or “OK.” Pet., 71. Patent Owner ignores this additional evidence showing that Serret-Avila discloses and suggests to a POSITA *generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.*

VI. CONCLUSION

The challenged claims of the ’828 Patent are invalid and should be canceled.

Date: September 5, 2025

Respectfully submitted,

/James L. Day/

James L. Day (Reg. No. 72,681)
Lead Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

This reply complies with the word count limit of 5,600 words under 37 C.F.R. § 42.24(c)(1). The reply contains 5,578 words, excluding the parts exempted by 37 C.F.R. § 42.24(c) (i.e., table of contents, table of authorities, certificate of service or word count, and appendix of evidence), as determined by the word count feature of Microsoft Word, which was used to prepare this reply.

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

CERTIFICATE OF SERVICE

I hereby certify that on September 5, 2025, the foregoing document entitled **PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE** along with all supporting exhibits was served on Patent Owner's counsel of record via email, as agreed to by Patent Owner, at the following email addresses:

batkinson@dickinsonwright.com
msaunders@dickinsonwright.com

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