

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

ADOBE INC.,  
Petitioner,

v.

JONATHAN E. JAFFE,  
Patent Owner.

---

Case IPR2024-01352  
Patent 6,757,828 B1

---

**PETITIONER'S NOTICE OF APPEAL**

Petitioner Adobe Inc. hereby provides notice of appeal to the United States Court of Appeals for the Federal Circuit pursuant to 35 U.S.C. §§ 141, 142, and 319 and 37 C.F.R. §§ 90.2 and 90.3 from the Final Written Decision of the Patent Trial and Appeal Board on March 4, 2026 (Paper 33) and from all underlying orders, decisions, rulings, and opinions in IPR2024-01352. This notice is timely filed within 63 days of the Final Written Decision (i.e., the final Board decision). 37 C.F.R. § 90.3(b)(1).

Copies of the Final Written Decision are attached.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Petitioner states that the anticipated issues on appeal may include, but are not necessarily limited to, the following:

1. Whether the Board erred in determining that claims 1-6 of U.S. Patent No. 6,757,828 (the “’828 Patent”) are not unpatentable under 35 U.S.C. § 103 over Glass;
2. Whether the Board erred in determining that claims 1-6 of the ’828 Patent are not unpatentable under 35 U.S.C. § 103 over Rieger;
3. Whether the Board erred in determining that claims 1-6 of the ’828 Patent are not unpatentable under 35 U.S.C. § 103 over Glass and Exif 2.0 or Exif 2.1;
4. Whether the Board erred in determining that claims 1-6 of the ’828

Patent are not unpatentable under 35 U.S.C. § 103 over Rieger and Exif 2.0 or Exif 2.1;

5. Whether the Board erred in determining that claims 1-6 of the '828 Patent are not unpatentable under 35 U.S.C. § 103 over Glass and Serret-Avila;

6. Whether the Board erred in determining that claims 1-6 of the '828 Patent are not unpatentable under 35 U.S.C. § 103 over Rieger and Serret-Avila;

7. Whether the Board erred in determining that claims 1-6 of the '828 Patent are not unpatentable under 35 U.S.C. § 103 over Glass and Exif 2.0 or Exif 2.1 and Serret-Avila; and

8. Whether the Board erred in determining that claims 1-6 of the '828 Patent are not unpatentable under 35 U.S.C. § 103 over Rieger and Exif 2.0 or Exif 2.1 and Serret-Avila.

9. Whether the Board erred in construing terms in claims 1-6 of the '828 Patent.

10. A copy of this Notice of Appeal is being filed with the Patent Trial and Appeal Board. In addition, this Notice of Appeal is being filed, along with the required docketing fees, with the Clerk's Office for the United States Court of Appeals for the Federal Circuit.

Dated: April 28, 2026

Respectfully submitted,

/s/ James L. Day

James L. Day

Registration No. 72,681

Farella Braun + Martel LLP

One Bush Street, Floor 9

San Francisco, CA 94104

(415) 954-4400

Attorney for the Petitioner

## **CERTIFICATE OF FILING AND SERVICE**

I hereby certify that on April 28, 2026, in addition to being filed electronically through the Patent Trial and Appeal Board's electronic filing system, the foregoing Notice of Appeal was emailed to the Director of the United States Patent and Trademark Office at the following address: [efileSO@uspto.gov](mailto:efileSO@uspto.gov)

In addition, I hereby certify that on April 28, 2026, the foregoing Notice of Appeal was electronically filed with the Clerk's Office of the United States Court of Appeals for the Federal Circuit.

In addition, I hereby certify that on April 28, 2026, the foregoing Notice of Appeal was served on the Patent Owner's counsel of record via email, as agreed to by Patent Owner, at the following email addresses:

Bryan Atkinson (batkinson@prinelobel.com)  
Micheal Saunders (msaunders@prinelobel.com)

/s/ James L. Day

James L. Day

Registration No. 72,681

April 28, 2026  
One Bush Street  
Floor 9  
San Francisco, CA

# ATTACHMENTS

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

---

Before JUSTIN T. ARBES, MITCHELL G. WEATHERLY, and  
BACH V. HOANG, *Administrative Patent Judges*.

Opinion for the Board filed by *Administrative Patent Judge* HOANG.

Opinion Dissenting filed by *Administrative Patent Judge* WEATHERLY.

HOANG, *Administrative Patent Judge*.

JUDGMENT  
Final Written Decision  
Determining No Challenged Claims Unpatentable  
*35 U.S.C. § 318(a)*

## I. INTRODUCTION

On March 7, 2025, the Board instituted an *inter partes* review of claims 1–6 of U.S. Patent No. 6,757,828 B1 (Ex. 1001, “the ’828 Patent”). Paper 8 (“Inst. Dec.”). Having considered the full record at trial, and for the reasons explained below, we determine that Petitioner has not shown that any of claims 1–6 of the ’828 Patent are unpatentable.

### A. History of this Proceeding

On August 28, 2024, Adobe Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–6 of the ’828 Patent (Paper 2 (“Pet.”)) and submitted declarations from Dr. Zixiang Xiong (Ex. 1003), Rachel J. Watters (Ex. 1007), and Kenneth Parulski (Ex. 1010). Jonathan E. Jaffe (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). On that record, the Institution Decision explained that Petitioner had demonstrated a reasonable likelihood that it would prevail in establishing the unpatentability of at least one challenged claim, and instituted an *inter partes* review of all challenged claims on all asserted grounds. Inst. Dec. 38.

During trial, Patent Owner filed a Response (Paper 16, “PO Resp.”), Petitioner filed a Reply (Paper 18, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 23, “PO Sur-reply”). With its Response, Patent Owner submitted a declaration from Bill Davis (Ex. 2005) and a deposition transcript of Dr. Xiong (Ex. 2012). With its Reply, Petitioner submitted reply declarations from Dr. Xiong (Ex. 1029) and Mr. Parulski (Ex. 1040). With its Sur-reply, Patent Owner submitted the transcript of a second deposition of Dr. Xiong (*see* Ex. 2013). There are no pending motions, and neither party moved to exclude any evidence.

An oral hearing was held on December 9, 2025, and a transcript of the hearing is included in the record. Paper 31 (“Tr.”).

*B. Related Matters*

The parties indicate that the ’828 Patent has been asserted in a district court lawsuit: *Jonathan E. Jaffe v. Adobe Inc.*, Case No. 2:23-cv-06224 (C.D. Cal.) (the “District Court proceeding”). Pet. x; Paper 6, 1.

*C. Asserted References*

Petitioner’s unpatentability challenges rely on five references:

- Glass et al., US 6,332,193 B1, filed Jan. 18, 1999, issued Dec. 18, 2001. Ex. 1005 (“Glass”).
- Bernd Rieger & Harry Rode, *Digital Image Recording for Court-Related Purposes* (IEEE 1999). Ex. 1006 (“Rieger”).
- Japan Electronic Industry Development Association, *Digital Still Camera Image File Format Standard (Exchangeable Image File Format for Digital Still Cameras: Exif) Version 2.0* (JEIDA Nov. 1997). Ex. 1008 (“Exif 2.0”).
- Japan Electronic Industry Development Association, *Digital Still Camera Image File Format Standard (Exchangeable Image File Format for Digital Still Cameras: Exif) Version 2.1* (JEIDA June 1998). Ex. 1009 (“Exif 2.1”).
- Serret-Avila, US 6,959,384 B1, issued Oct. 25, 2005. Ex. 1011 (“Serret-Avila”).

*D. Testimonial Evidence*

Petitioner submits declarations from Dr. Zixiang Xiong (Ex. 1003), Rachel J. Watters (Ex. 1007), and Kenneth Parulski (Ex. 1010).

Patent Owner submits a declaration from Bill Davis. Ex. 2005.

*E. The Petition's Asserted Grounds*

Petitioner asserts the following grounds of unpatentability (Pet. 1):

| <b>Claims Challenged</b> | <b>35 U.S.C. <sup>1</sup> §</b> | <b>Reference(s)/Basis<sup>2</sup></b> |
|--------------------------|---------------------------------|---------------------------------------|
| 1–6                      | 103(a)                          | Glass                                 |
| 1–6                      | 103(a)                          | Rieger                                |
| 1–6                      | 103(a)                          | Glass, Exif 2.0                       |
| 1–6                      | 103(a)                          | Glass, Exif 2.1                       |
| 1–6                      | 103(a)                          | Rieger, Exif 2.0                      |
| 1–6                      | 103(a)                          | Rieger, Exif 2.1                      |
| 1–6                      | 103(a)                          | Glass, Serret-Avila                   |
| 1–6                      | 103(a)                          | Rieger, Serret-Avila                  |
| 1–6                      | 103(a)                          | Glass, Exif 2.0, Serret-Avila         |
| 1–6                      | 103(a)                          | Glass, Exif 2.1, Serret-Avila         |

---

<sup>1</sup> The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011), revised 35 U.S.C. § 103 effective March 16, 2013. Because the challenged patent was filed before March 16, 2013, we refer to the pre-AIA version of § 103.

<sup>2</sup> Petitioner appears to incorporate alternative references using slashes (“/”) or “or.” *See, e.g.*, Pet. 1 (“Glass and Exif 2.0 or Exif 2.1”), 62 (“the combination of Glass with Exif 2.0/2.1 or Rieger with Exif 2.0/2.1”). We understand Petitioner’s use of alternative references to be separate grounds and reproduce Petitioner’s grounds accordingly in this table.

| Claims Challenged | 35 U.S.C. <sup>1</sup> § | Reference(s)/Basis <sup>2</sup> |
|-------------------|--------------------------|---------------------------------|
| 1–6               | 103(a)                   | Rieger, Exif 2.0, Serret-Avila  |
| 1–6               | 103(a)                   | Rieger, Exif 2.1, Serret-Avila  |

*F. The '828 Patent (Ex. 1001)*

The '828 Patent describes techniques and devices to capture and create a digital photograph or image having an associated digital signature that is used to verify that the image is unaltered, i.e., authentic. Ex. 1001, 1:8–19, 1:52–62, 2:59–64. Figure 2A, reproduced in relevant part below, shows a schematic diagram of a self-contained digital camera which captures and creates an image with such a digital signature. *Id.* at 2:15–17, 4:52–54.

FIG. 2A

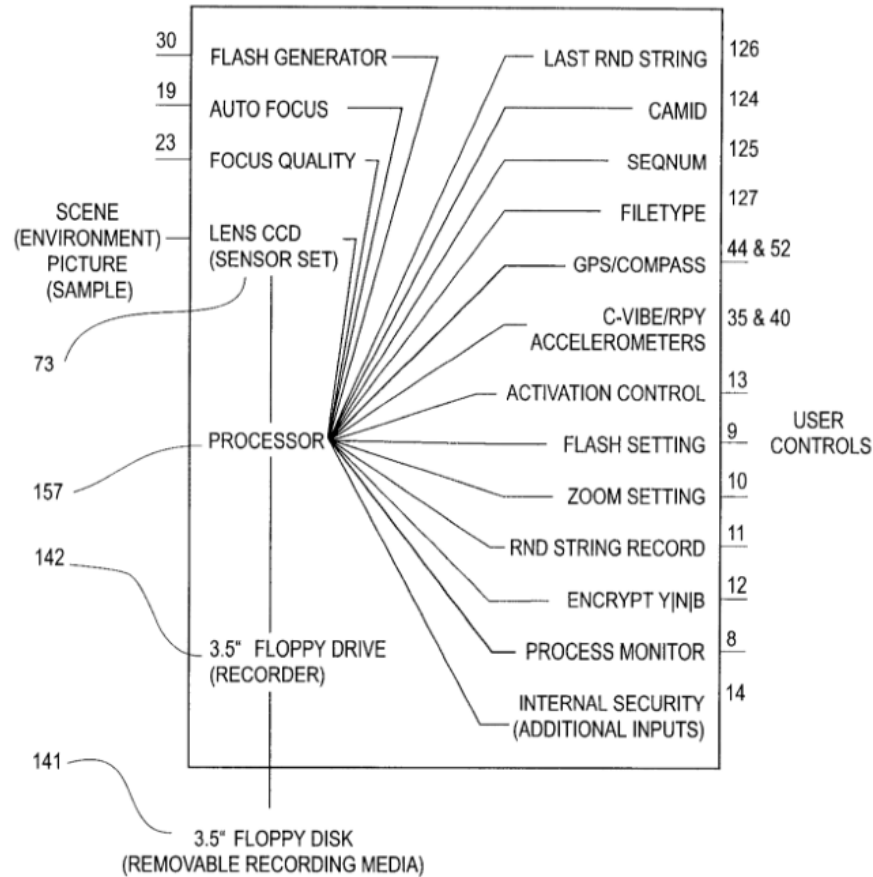


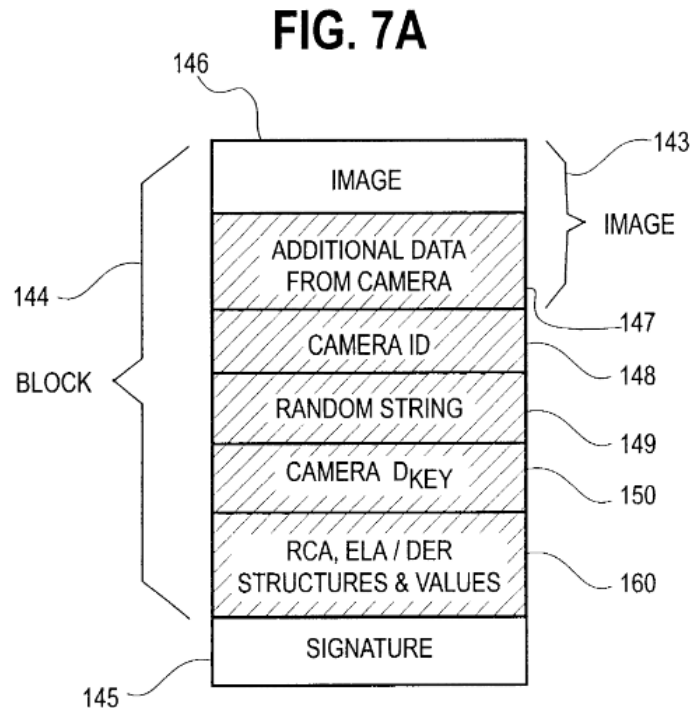
Figure 2A shows components within the self-contained digital camera including sensor set 73 (which captures an image), which is connected to processor 157 (which processes the captured image), which in turn is connected to recorder 142 (which stores the processed image). Ex. 1001, 4:52–61; *see id.* at 4:37–51, 5:1–7, 7:43–52, 8:12–14, Fig. 3. Additional components are connected to the processor and include camera identifier (CamID) 124, image sequence number 125, current random string 126, global positioning system (GPS) unit 44, and internal security system 14. *Id.* at 6:60–62; *see id.* at 4:45–51, 5:30–31.

The creation of an image having a digital signature for authentication starts with capturing an image using sensor set 73. *Id.* at 6:47–50; *see id.* Fig. 6. The captured image has information from the additional components

noted above appended to it, e.g., a camera identifier, a random string, and GPS values. *Id.* at 6:50–67, Fig. 6. The captured image also may append an indication that a security violation has occurred. *Id.*

A security violation occurs when there is a “breach of security” which compromises internal security system 14. *Id.* at 5:44–49; *see id.* Fig. 4A2. In particular, “[d]uring the operation of the camera, internal security [system] 14 is monitored to detect the integrity of the tight coupling of the sensor set and the recorder 6.” *Id.* at 4:65–67, 5:44–45. The ’828 Patent explains that “[a] key to verifiable authenticity is to [e]nsure that the authentication information generation is tightly coupled to the sensor set and recorder. There can be nothing that can possibly alter the recording before the authentication information is generated.” *Id.* at 3:16–20. But, “[i]f internal security is compromised 60 a security violation 61 [indicating the image is unverified] is appended 123 to the image.” *Id.* at 6:64–67, 8:45–49, Fig. 6.

Next, a digital signature, used for subsequently authenticating the image, is created based on the captured image and its appended information. *Id.* at 7:27–35. Figure 7A, reproduced in relevant part below, is a diagram of a file format for a “signed digital image,” which includes the captured image, appended information, and a digital signature. *Id.* at 2:37–38.



The file structure of Figure 7A shows digital signature 145 and block 144; block 144 encompasses captured image 146 and its appended information 147–160. *Id.* at 8:1–58. Digital signature 145, “which is a function of the signature protocol (SP) being used and the block, is computed and made part of the file.” *Id.* at 7:27–30. That is, “[e]verything inside the ‘Block’ is what is signed.” *Id.* at 8:7–8. The file formed by block 144 and digital signature 145 may then be used to subsequently authenticate the image. *See id.* at 7:62–8:8.

Authentication is performed, e.g., on the file of Figure 7A, by separating block 144 from the original signature 145 and then recalculating a signature using the separated block. *Id.* at 9:13–15, 9:43–45. A mismatch between the recalculated signature and the original signature indicates that the image has been damaged or altered, and the image is not authenticated. *Id.* at 9:50–59; *see id.* Fig. 9. On the other hand, if the recalculated signature matches original signature 145, the image is marked as authenticated. *Id.* at 9:45–49; *see id.* Fig. 9.

*G. Challenged Claims*

Petitioner challenges claims 1–6 of the '828 Patent. Of these, claim 1 is independent. Claim 1 is reproduced below, incorporates changes from an August 17, 2021 Certificate of Correction, and includes Petitioner's bracketed annotations for discussion purposes:

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

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

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

[1c] monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

[1d] utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

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

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

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

[1h] if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

Pet. 7–8; Ex. 1001, 20:59–21:18; *see id.* at 34 (Certificate of Correction).

## II. ANALYSIS

### A. Legal Standards

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

The legal question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness.<sup>3</sup> *Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17–18 (1966). One seeking to establish obviousness based on more than one reference also must articulate sufficient reasoning with rational underpinnings to combine teachings. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

### B. Level of Ordinary Skill in the Art

Our reviewing court has explained that “the level of skill in the art is a prism or lens through which a judge, jury, or the Board views the prior art and the claimed invention.” *Okajima v. Bourdeau*, 261 F.3d 1350, 1355

---

<sup>3</sup> The current record does not include allegations or evidence of objective indicia of nonobviousness.

(Fed. Cir. 2001) (citing *Al-Site Corp. v. VSI Int'l, Inc.*, 174 F.3d 1308, 1324 (Fed. Cir. 1999)). “This reference point prevents these factfinders from using their own insight or, worse yet, hindsight, to gauge obviousness.” *Id.* In finding the level of ordinary skill in the art, we may consider various factors, including: “(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field.” *Best Med. Int'l, Inc. v. Elekta Inc.*, 46 F.4th 1346, 1353 (Fed. Cir. 2022) (quoting *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007)). “The patent’s purpose can also be informative.” *Id.* (citation omitted).

Petitioner asserts a person of ordinary skill in the art (“POSITA”) at the time of the ’828 Patent (July 2000) “would have [had] an undergraduate degree (or equivalent) in electrical engineering, computer science, or a comparable subject and at least two years of work experience involving image processing. Alternatively, such a person would have [had] an advanced degree and at least one year of post-graduate research/work experience involving image processing.” Pet. 8 (citing Ex. 1003 ¶ 82). Petitioner further asserts the POSITA would have been “familiar with the design and implementation of systems and devices involving image processing, including image authentication,” and would have been “familiar with authentication fundamentals, including encryption, hashing, and signature principles and techniques.” *Id.* (citing Ex. 1003 ¶ 82).

The Institution Decision adopted and applied Petitioner’s proposed level of ordinary skill because Petitioner’s “definition generally comports with the level of skill necessary to understand and implement the teachings

of the '828 Patent and the asserted prior art.” Inst. Dec. 15–16 (citing Ex. 1002 ¶¶ 81–83).

Offering a different level of ordinary skill, Patent Owner asserts a POSITA would have had “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,” and agrees with Petitioner in part that a POSITA would have been “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.” PO Resp. 4 (citing Ex. 2005 ¶ 53).

Having considered the full record at trial, we maintain the preliminary finding regarding the level of ordinary skill in the art. *See* Inst. Dec. 15–16. In particular, based on the teachings of the '828 Patent and the asserted prior art, we are persuaded that an ordinarily skilled artisan would have had a working knowledge of digital imaging processing generally. Patent Owner at least appears to agree that the skilled artisan would have had experience in a particular type of digital image processing, digital image authentication. PO Resp. 4. Moreover, our decision would be the same under either proposed level of skill. Indeed, in their respective arguments, the parties do not assert or explain how their proposed level of ordinary skill in the art affects any findings or conclusions. *See* PO Resp.; Pet. Reply; PO Sur-reply.

### *C. Claim Construction*

We interpret claim terms using “the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C.

282(b).” 37 C.F.R. § 42.100(b) (2024). Under the principles set forth by our reviewing court, the “words of a claim ‘are generally given their ordinary and customary meaning,’” as would be understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)).

The parties present various claim construction arguments, disputing the meaning of three limitations recited in claim 1: “a sensor, which is tightly coupled to said memory”; “monitoring the integrity of the tight coupling between said memory and said sensor”; and “based on.” See Pet. 9–14; PO Resp. 5–12; Pet. Reply 4–9; PO Sur-reply 4–11. For purposes of this Decision, we do not need to discuss the construction of “based on.” See *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). As explained below, this Decision turns on whether Glass or Rieger discloses limitation [1c] reciting “monitoring the integrity of the tight coupling between said memory and said sensor.” Ex. 1001, 20:65–66; see *infra* §§ II.C.2, II.E.1, II.F. That limitation recites an element which overlaps with the earlier-recited limitation “a sensor, which is tightly coupled to said memory.” To reach our decision, we need only provide a limited discussion of two of the parties’ claim construction arguments. Our analysis follows.

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

Limitation [1b] recites, in relevant part, “a sensor, which is tightly coupled to said memory.” Ex. 1001, 20:62–63. Petitioner proposes that the limitation means “a sensor coupled to said memory via conductive traces or leads.” Pet. 10. Patent Owner argues for a *broad*er construction, proposing that the limitation means “a sensor that is electrically or physically coupled to memory in a device.” PO Resp. 9; *see id.* at 5. That is, the parties’ dispute regarding this limitation focuses on the meaning of “tightly,” specifically whether “tightly coupled” requires a coupling to have conductive traces or leads.

For the purposes of this Decision, we need not resolve the meaning of “tightly coupled,”<sup>4</sup> but we determine that the limitation at least requires some kind of coupling from the sensor to the memory. The parties do not dispute that the claim requires some kind of coupling from the sensor to the memory; in fact, the competing constructions both require that a sensor is “coupled to” a memory. *Compare* Pet. 10 *with* PO Resp. 9. Indeed, the claim language plainly reads that there is some kind of coupling from the sensor to the memory. Ex. 1001, 20:62–63.

Accordingly, we agree with the parties that this limitation at least requires some kind of coupling from the sensor to the memory. The existence of some kind of coupling is relevant to the construction of dispositive limitation [1c], which relatedly recites “the tight coupling.” However, our decision is not contingent on whether the recited coupling

---

<sup>4</sup> Petitioner states “this dispute is immaterial.” Pet. Reply 5–6.

must have conductive traces or leads and, so, we do not opine on that issue.<sup>5</sup> *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” and “we need not construe [claim limitations] ‘where the construction is not ‘material to the [obviousness] dispute’” (alteration in original) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

2. “*monitoring the integrity of the tight coupling*”

Limitation [1c] recites, in relevant part, “monitoring the integrity of the tight coupling between said memory and said sensor.” Ex. 1001, 20:65–66. The Institution Decision did not expressly construe this limitation (*see* Inst. Dec. 16–20), but the Board’s analysis of Petitioner’s unpatentability challenge stated that the claim did not “specify any particular manner of ‘monitoring the integrity of the tight coupling’” (*id.* at 30). As noted, the Board did not have the benefit of full briefing on this issue by Patent Owner (*id.*) and the Preliminary Response’s claim construction section did not address this particular issue (*see* Prelim. Resp. 8–9). Patent Owner’s Response now includes such arguments and explanations. *See* PO Resp. 9–

---

<sup>5</sup> In the District Court proceeding, the District Court “issued a tentative order before the claim construction hearing” (Ex. 1020) and conducted the hearing (Ex. 1042 (transcript)), but did not issue a final ruling because the District Court proceeding was stayed. Tr. 10:16–25. The District Court tentatively construed “a sensor, which is tightly coupled to said memory,” to mean “a sensor coupled to said memory via conductive traces or leads.” Ex. 1020, 9–12.

11. This full record counsels us to construe this limitation in Patent Owner’s favor.

Patent Owner proposes that this limitation means “determining whether the physical coupling between said memory and said sensor has been accessed or disturbed” which “specifically requires monitoring the *physical coupling* between the sensor and the memory.” PO Resp. 10–11; PO Sur-reply 9–10. Petitioner proposes we construe the limitation to mean “determining whether physical access has been gained to the coupling between said memory and said sensor.” Pet. 11 (citing Ex. 1003 ¶ 99); Pet. Reply 7–9. Moreover, Petitioner disagrees with Patent Owner’s requirement that the tight coupling is specifically monitored and takes the position that the limitation includes monitoring the integrity of something other than the tight coupling, e.g., by monitoring a camera or packaging that houses the tight coupling. *See* Pet. Reply 8–9, 16–17.

We agree with Patent Owner’s construction that this limitation “specifically requires monitoring the *physical coupling* between the sensor and the memory.” PO Resp. 10–11. We initially note that, although we do not construe “tightly coupled” as recited in limitation [1b] (*see* § II.C.2.), Patent Owner’s construction in this limitation expressly states that the recited “tight coupling” is a “*physical coupling*” as opposed to any electrical coupling. *See id.*; PO Sur-reply 9. As we adopt Patent Owner’s construction in this limitation, this construction also follows Patent Owner’s requirement that the tight coupling is a physical coupling. Our detailed analysis is provided below.

We begin with the express claim language, which better supports Patent Owner’s construction. The full claim limitation recites “monitoring the integrity of the tight coupling between said memory and said sensor

when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity.” Ex. 1001, 20:65–21:2. Although Petitioner points out that the limitation does not expressly recite “‘specifically’ monitoring the tight coupling” (Pet. Reply 8), the structure of the clause suggests that the tight coupling is specifically monitored. At a high level, the limitation is straightforward in its recitation that the integrity being monitored is “*of the tight coupling*” (Ex. 1001, 20:65–66 (emphasis added)), plainly suggesting that the tight coupling is specifically monitored. More granularly, breaking the relevant clause down to its grammatical parts, the clause recites a gerund (“monitoring”) acting on a direct object (“the integrity”) which is modified by a prepositional phrase (“of the tight coupling”). Notably, the object of the preposition (“of”) is “the tight coupling.” Altogether, this reads that the integrity being monitored is specifically of the tight coupling. Also, the claim recites that “if said integrity is compromised, then also providing an indication of said compromised integrity.” Therefore, from the claim language we know that the “integrity” of the tight coupling is something that may be “compromised,” which is consistent with Patent Owner’s proposed construction of determining whether the physical coupling has been “accessed or disturbed.”

Petitioner’s interpretation effectively inserts additional language into the limitation such that the limitation includes monitoring the integrity of a device containing or surrounding the tight coupling, such as a camera (or camera housing), e.g., “monitoring the integrity of *a camera that includes the tight coupling*.” But, because the plain reading and the structure of the limitation reads that it is specifically the tight coupling’s integrity—not another physical structure, like a camera—which is being monitored, a

construction in which only the integrity of the camera or its housing is being monitored is not consistent with the language of the claim. *See* PO Resp. 9 (arguing that “Petitioner’s construction is improper because the claim language explicitly requires monitoring the physical coupling between the memory and the sensor as opposed to some third structure” (emphasis omitted)).

We next look to the Specification for guidance on the construction of this term. Both parties agree that column 4, lines 65–67 of the ’828 Patent describe this feature. *See* Pet. 10–11; PO Resp. 9; Pet. Reply 8; PO Sur-reply 9. That description, referring to Figure 2A, states: “[d]uring the operation of the camera, internal security 14 is monitored to detect the integrity of the tight coupling of the sensor set and the recorder 6.”<sup>6</sup> Ex. 1001, 4:65–67. Figure 2A is a “detailed schematic diagram[s] of a self-contained digital camera” (*id.* at 2:12–17) and is reproduced below:

---

<sup>6</sup> Although this portion of the Specification discussing Figure 2A references recorder 6, we read this portion as referencing element 142 because Figure 2A does not show recorder 6 and the only recorder shown in that figure is 3.5” FLOPPY DRIVE (RECODER) 142. *See* Ex. 1001, Fig. 2A. Somewhat confusingly, Figure 2 shows a RECORDER, but, that recorder is enumerated as element 3, not element 6. *See id.* at Fig. 2. Further confusingly, Figure 2 shows element 6 as a box encompassing other elements, but the portions of the Specification discussing Figure 2 do not reference element 6. *See id.* 3:32–40, 3:60–65, Fig. 2.

FIG. 2A

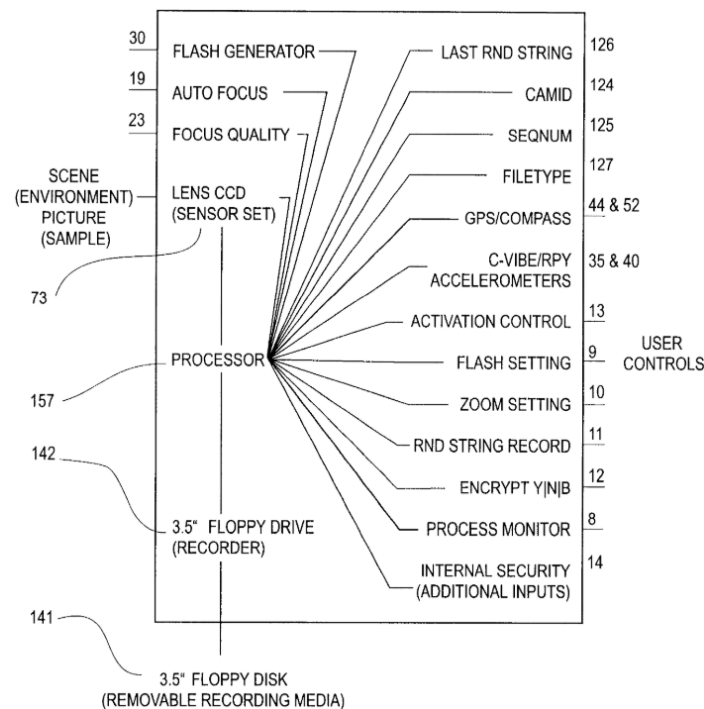


Figure 2A shows a box encompassing a number of text components connected by lines, e.g., LED CCD (SENSOR SET) 73 linked by a line to PROCESSOR 157 which is in turn linked by a line to 3.5" FLOPPY DRIVE (RECORDER) 142. *See id.* at 4:52–61.

Regarding internal security, the Specification describes checking an “internal security system” for security breaches: “processing continues 58 with a check 59 of the internal security system 14. If there is a breach of security 60 the violation is recorded 61.” Ex. 1001, 5:44–49; *see id.* at 6:64–66 (“If internal security is compromised 60 a security violation 61 is appended 123 to the image.”). The Specification does not further discuss “internal security.” *See id.*

The above-cited portions of the Specification describe the act of “monitoring the integrity of the tight coupling between said memory and said sensor,” but are limited in describing how that act is accomplished. In

particular, we do not readily find any description or example showing that the tight coupling is monitored in Petitioner's suggested manner, namely, by monitoring the camera housing the tight coupling. Petitioner points out 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" (Pet. Reply 8 (citing Ex. 1001, 4:65–67)), but that statement does not disclose that the internal security system is the camera or that it monitors the camera to indirectly monitor the integrity of the tight coupling. To the contrary, the only function of "internal security system 14" is to monitor the integrity "of the tight coupling" between the sensor and recorder. *See* Ex. 1001, 4:65–67, 5:44–45. Indeed, Petitioner acknowledges that the Specification does not describe the internal security system monitoring the camera or the camera housing. Tr. 54:19–55:1 ("JUDGE ARBES: But there's also no disclosure of assessing the internal security of the device as a whole, in your view, right? [PETITIONER]: Well, I think that's true, there's no detail. The words internal security to me mean assess the security of the internals of the camera. So I think -- I don't completely agree with you, except that I completely agree there's no detailed description of any internal security system."). If anything, the relevant disclosure only discusses the integrity of the tight coupling, rather than the integrity of some other component such as the camera or its housing. Accordingly, the Specification better aligns with Patent Owner's construction which requires specifically monitoring the integrity of the tight coupling.

Next, we examine the prosecution history. This limitation was added in a March 11, 2004 Amendment ("Amendment") and the claim was thereafter allowed. *See* Ex. 1002, 289–293, 314–315. In the Amendment's remarks, the then-Applicant stated,

[e]xemplary 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.

*Id.* at 293.

Petitioner argues that, because Applicant stated “the device” that prevents access to the tight coupling is broken, “the claim is not narrowly limited to determining whether the tight coupling itself is broken.” Pet. Reply 9. Petitioner asserts that “the device” referenced by Applicant is the camera itself, or the camera housing. Tr. 19:14–21 (“JUDGE ARBES: What, in your view, is ‘the device’ referring to . . . [PETITIONER]: It’s a digital camera.”), 22:6–8 (“[T]he device that is broken is the camera.”); *see* Pet. Reply 9 (“the ‘monitoring’ step is performed by determining whether ‘the device’ preventing access to the tight coupling ‘is broken’ (just as in Glass and Rieger)” which describe camera housings). Petitioner states that Applicant “told the examiner what this limitation means is a signal is generated if the device is broken and the device is the camera.” Tr. 20:14–18. Petitioner also argues the Applicant’s discussion of a “device” refers to a camera because the Specification describes the operation of a camera and because the “only device” described by the Specification is a camera. *Id.* at 20:5–6, 21:17–22, 22:6–21.

As an initial matter, we note that the paragraph of the prosecution history discussing the “monitoring the integrity of the tight coupling” amendment merely refers to “exemplary disclosure” and an “example” for the newly added limitation. Ex. 1002, 293. Even so, we do not agree with Petitioner’s reading. Petitioner’s arguments interpret Applicant’s use of a

generic term, “device,” to specifically mean a camera. However, we do not readily see where Applicant’s remarks stated that “the device” preventing physical access to interconnections is a camera, contrary to Petitioner’s assertion otherwise. *See* Ex. 1002, 292–293. In fact, Applicant’s remarks did not mention a camera at all; instead, Applicant only discussed the interconnections between the sensor and the memory, better supporting Patent Owner’s construction that the claimed monitoring is specific to those interconnections. *See id.* Also, Petitioner proposes a construction of determining “whether physical access [to the coupling] has been gained,” but Applicant’s statement above referenced the device preventing physical access being “broken.” *See id.* Furthermore, Applicant’s discussion of the “broken” device is in the immediate context of its statement explaining that the monitoring step “determine[s] whether internal security has been compromised” (*id.*), suggesting that the device referenced is an “internal security” device specific to the physical coupling between the sensor and memory. Indeed, Applicant cites as “[e]xemplary disclosure” step 59 of Figure 4A, which, as explained above, the Specification describes as “a check . . . of the internal security *system* 14.” *See* Ex. 1001, 4:65–67, 5:44–45 (emphasis added); Ex. 1002, 293. As such, we understand Applicant’s remarks to have generically referenced a device, namely, an internal security device, preventing physical access to the specific interconnections between the sensor and memory, rather than asserting that the device preventing physical access is a camera. *See* PO Sur-reply 17.

Further, although the Specification uses both terms, “camera” and “device,” the Specification does not expressly define a “device” as a camera. Without some explicit disclosure or admission that a “device” is specifically

a camera, we decline to read Applicant's reference to a "device" so narrowly.

Additionally, dependent claim 2's express recitation that the claimed memory is housed in "a digital camera" (Ex. 1001, 22:1–2) suggests that, during prosecution, Applicant could—but chose not to—have included such language itself and drafted the claim in a manner stating that the integrity of a digital camera is monitored, rather than the integrity of a tight coupling between two particular components. Therefore, the prosecution history does not show that monitoring the integrity of the tight coupling should be read to include monitoring a camera, as Petitioner contends.

Accordingly, the intrinsic evidence—the claim language, Specification, and prosecution history—consistently describes the claimed monitoring as specific to the tight coupling. There is no intrinsic evidence describing monitoring a camera housing the tight coupling.

We have also reviewed the proffered extrinsic evidence supporting the parties' claim constructions, i.e., the declarations from Dr. Xiong (Ex. 1003; Ex. 1029) and Mr. Davis (Ex. 2005). Dr. Xiong's first declaration cites the same portions of the Specification and prosecution history we have already discussed and agrees with the District Court's tentative claim construction, but does not offer any further explanation or evidence in support of Petitioner's arguments. *See* Ex. 1003 ¶¶ 97–100. Dr. Xiong's reply declaration does not address this limitation. *See* Ex. 1029. Mr. Davis's declaration, similarly, cites already reviewed portions of the Specification and prosecution history but does not offer any further explanation or evidence in support of Patent Owner's arguments. Ex. 2005 ¶¶ 62–66. As such, the extrinsic evidence does little to inform claim construction.

We also note that Patent Owner’s construction is consistent with the District Court’s tentative claim construction. Ex. 1020, 12–13. The District Court tentatively construed the limitation to mean “determining whether physical access has been gained to the coupling between said memory and said sensor.” *Id.* at 13. The District Court, however, stated that, “*as Adobe argues*, monitoring involves determining whether the physical coupling has been accessed or disturbed.” *Id.* at 12 (emphasis added). Thus, the District Court tentatively agreed with Petitioner’s position in that proceeding that the claimed monitoring is with respect to the physical coupling between the memory and sensor (not a different structure or device, like a camera). Patent Owner’s construction (“determining whether the physical coupling between said memory and said sensor has been accessed or disturbed”) mirrors the language in the District Court’s tentative order.

For the foregoing reasons, we construe “monitoring the integrity of the tight coupling between said memory and said sensor” to mean determining whether the physical coupling between said memory and said sensor has been accessed or disturbed, which specifically requires monitoring the physical coupling between the sensor and the memory.

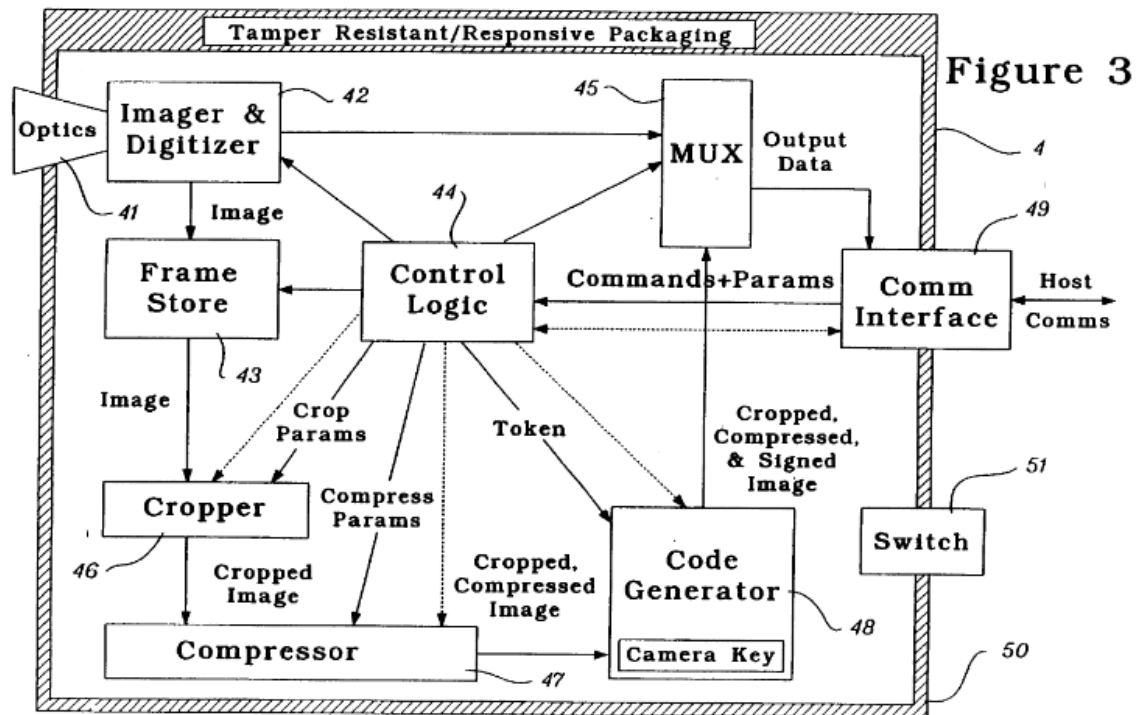
#### *D. Summary of Asserted Prior Art References*

Below we summarize the asserted references. We discuss any additional pertinent details of the references in our patentability analysis.

##### *1. Glass (Ex. 1005)*

Glass describes techniques to provide secure transmission and subsequent authentication of biometric data, e.g., image data. Ex. 1005, 3:45–53, 4:58–60. In one example, Glass describes an “imaging system”

that uses a camera to collect biometric data. *Id.* at 4:54–60. The imaging system embeds information into the image such that the image can be subsequently authenticated. *Id.* at 4:60–5:3. Figure 3, reproduced below, is a functional block diagram of such an imaging system. *Id.* at 4:30–32.



As shown in Figure 3, tamper resistant package 50 encloses imaging system 4 which includes Image & Digitizer 42 connected to frame store memory 43 via a data path shown in a solid line. *Id.* at 5:13–22, 5:46–53. Image & Digitizer 42 creates a digital image that is stored in frame store memory 43. *Id.* at 5:49–55. Glass then applies a cryptographic technique to create a digital signature for the image data. *Id.* at 5:62–65. The digital signature is created using image data and a key which may be hidden in the imaging system. *Id.* at 5:67–6:3.

Further, according to Glass, tamper resistant package 50 enclosing imaging system 4 makes it “extremely difficult to access the internal elements of the package without detection or actual destruction of the

device.” *Id.* at 5:13–16. In one embodiment, an intrusion detector or switch 51 sends a signal that places the imaging system in a non-functioning state. *Id.* at 5:25–30. Glass explains that “tampering of image data prior to application of security information would be extraordinarily difficult or impossible.” *Id.* at 5:37–41.

Furthermore, Glass describes techniques where the previously generated digital signature and image are subsequently used to authenticate the image. *Id.* at 3:53–57, 4:65–5:7. In one embodiment, the system authenticating the image receives the image, the imaging system’s key, and the previously generated digital signature. *Id.* at 7:3–7, 9:35–40, 10:30–35. The authenticating system then recomputes a digital signature for the image. *Id.* at 9:40–47, 10:40–45. If the previously generated digital signature matches the recomputed digital signature, the image is authenticated. *Id.* at 9:47–51, 10:45–50. Glass also states that it “log[s] each step of the transaction.” *Id.* at 9:61–10:34, 10:54–58; *see id.* Fig. 8.

## 2. *Rieger (Ex. 1006)*

Rieger describes techniques to “ensure the integrity and authenticity of the images produced” by a digital camera. Ex. 1006, 3. Figure 3, reproduced below, shows a “basic conceptual diagram” of such a digital camera (*id.* at 4).

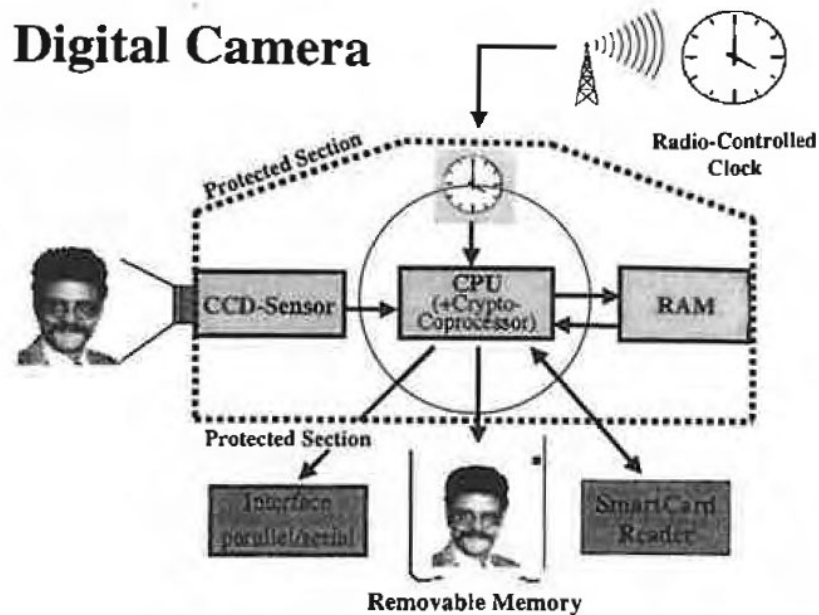


Figure 3 shows a digital camera having a “specially protected compartment in the camera housing” which encloses a CCD sensor, which is connected to a processor, which is connected to RAM. Ex. 1006, 4. Rieger explains the processor includes a signature chip with a secret key. *Id.* A verifiable image is created by hashing data to create a digital signature of the image. *Id.* at 3–4; *see id.* at 11.

Subsequently, a receiver of the image and associated signature can verify the integrity and authenticity of the image. *Id.* at 11–12. Verification is provided by re-hashing the image data. *Id.* If the resultant hash value matches the received digital signature, the integrity and authenticity of the image is verified. *Id.* at 12.

### 3. Exif 2.0 (Ex. 1008)

Exif 2.0 describes a standard file format for the image data recorded by digital still cameras to ensure data compatibility and exchangeability. Ex. 1008, 10.

4. *Exif 2.1 (Ex. 1009)*

Exif 2.1 describes a standard file format for the image data recorded by digital still cameras to ensure data compatibility and exchangeability. Ex. 1009, 7.

5. *Serret-Avila (Ex. 1011)*

Serret-Avila describes systems and methods for enabling a recipient of a cryptographically signed electronic communication to verify the authenticity of the communication. Ex. 1011, code (57). Serret-Avila authenticates data by comparing computed hash values from a received hash value and a calculated hash value. *Id.* at 10:16–27. Where the hashes match, data is “deemed to be authentic” and “can be released for use.” *Id.* at 10:28–30. On the other hand, where data is judged to be unauthentic due to a mismatch in computed hashes, an “appropriate defensive action” is taken. *Id.* at 10:33–38. For example, the system may “display a warning or error message on [a] display.” *Id.* at 10:39–45.

*E. Obviousness Based on Glass*

Petitioner contends that the subject matter of claims 1–6 would have been obvious over Glass. Pet. 1, 22–41. Patent Owner opposes, contending Petitioner insufficiently shows that Glass teaches certain limitations recited in claim 1. PO Resp. 12–28.

For the reasons explained below, we determine that Petitioner fails to show that any of the challenged claims would have been obvious over Glass. For clarity and simplicity, we address only one dispositive limitation in independent claim 1, which all the remaining challenged claims depend on.

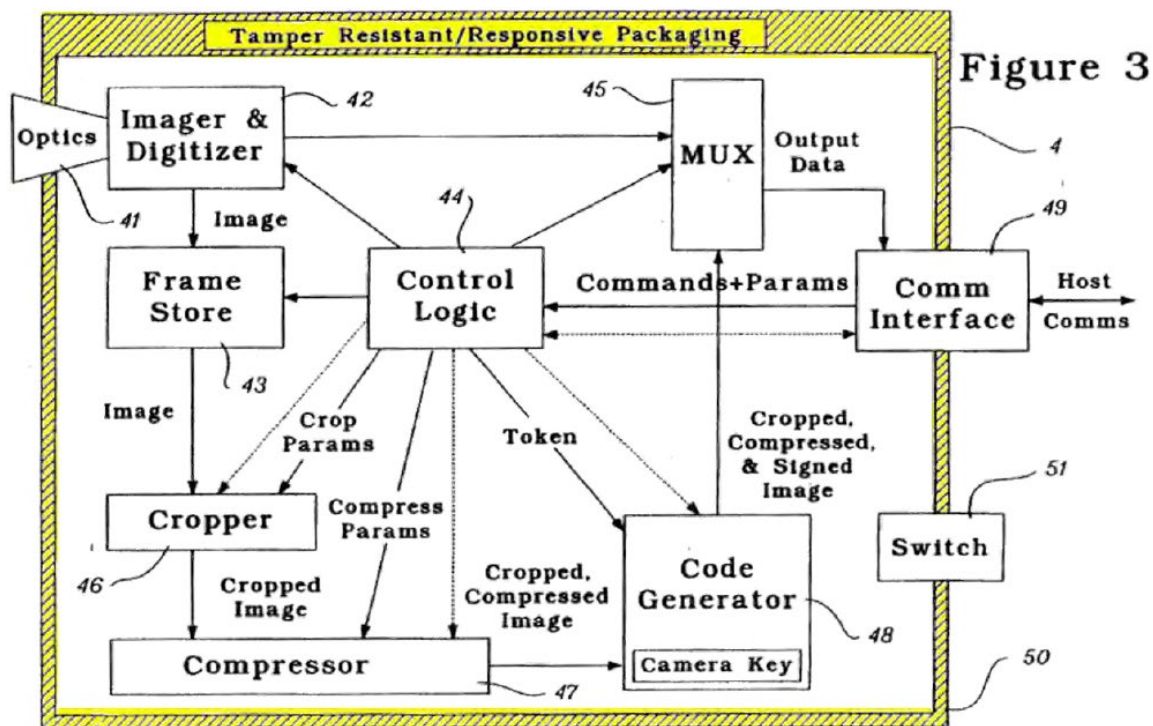
1. Independent Claim 1

Claim 1 recites in relevant-part:

[1c] monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity.

Ex. 1001, 20:65–21:2.

Petitioner contends Glass discloses this limitation. Pet. 30–32 (citing Ex. 1003 ¶¶ 181–186; Ex. 1005, 5:13–45, Fig. 3). Of particular relevance, Petitioner provides a highlighted version of Glass’s Figure 3, reproduced below. *Id.* at 31.



Petitioner’s annotation of Figure 3 shows Glass’s imaging system 4, containing imager & digitizer 42 (a “sensor”) and frame store 43 (a “memory”), enclosed, along with numerous other components, in highlighted tamper resistant/responsive packaging 50. Pet. 30–31; see Ex. 1005, 5:13–45, Fig. 3. Petitioner explains that if Glass’s tamper resistant

package 50 is compromised, a “chassis intrusion detector or switch 51” causes Glass’s imaging system to be placed in a non-functioning state. *Id.* at 31–32 (citing Ex. 1005, 5:16–19, 5:26–34, Fig. 3). That is, Petitioner’s position is “[b]y monitoring Glass’s tamper resistant package 50, Glass discloses monitoring the integrity of [all] components and interconnections contained in that packaging including the *tight coupling* between *sensor* and *memory*.”<sup>7</sup> Pet. Reply 16.

Patent Owner argues that, according to its asserted claim construction, “monitoring [Glass’s] *package* fails to teach monitoring the *coupling* between the sensor and memory specifically as the limitation requires.” PO Resp. 20; PO Sur-reply 16. According to Patent Owner, Glass does not teach limitation [1c] because “it discloses monitoring something other than the coupling, namely, a tamper resistant package.” PO Resp. 21.

Petitioner acknowledges that monitoring Glass’s tamper resistant package 50 does not specifically monitor the integrity of the coupling between Glass’s sensor and the memory and, instead, argues that Glass detects tampering of all “the components and interconnections contained in that packaging,” e.g., control logic 44, cropper 46, compressor 47, MUX 45, code generator 48, and the various interconnections between those components. *See* Pet. Reply 16; Ex. 1005, 5:13–41. As explained above, we construe “monitoring the integrity of the tight coupling between said memory and said sensor” to mean determining whether the physical

---

<sup>7</sup> Petitioner does not assert that a person of ordinary skill in the art would have been motivated to modify Glass’s device in any way; Petitioner solely argues that Glass teaches limitation [1c], based on Petitioner’s proposed claim construction. *See* Pet. 30–32 (“Glass discloses this limitation.”); Pet. Reply 16–17 (“Glass and Rieger disclose the ‘monitoring’ step.”).

coupling between said memory and said sensor has been accessed or disturbed, which specifically requires monitoring the physical coupling between the sensor and the memory. *See supra* § II.C.2. As we agree with Patent Owner that this limitation requires monitoring the physical coupling between the sensor and the memory, monitoring Glass’s tamper resistant package 50 does not teach or disclose “monitoring the integrity of the tight coupling between said memory and said sensor.”

Accordingly, we determine that Petitioner fails to show that Glass teaches or suggests

[1c] monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity,

as required by claim 1. Consequently, we determine that Petitioner has not shown, by a preponderance of the evidence, that the subject matter of claim 1 would have been obvious over Glass.<sup>8</sup>

## *2. Dependent Claims 2–6*

Claims 2–6 depend from independent claim 1. Ex. 1001, 22:1–16. Each of these dependent claims include all the limitations of the respective independent claim. Petitioner’s reliance on and application of Glass to these dependent claims does not cure the above-noted deficiency of independent claim 1. *See* Pet. 38–41.

---

<sup>8</sup> For clarity, given our determination herein regarding limitation [1c], we need not decide Patent Owner’s other arguments regarding limitations [1b] and [1g]. *See* PO Resp. 12–20, 23–27.

Accordingly, we determine that Petitioner has not shown, by a preponderance of the evidence, that the subject matter of any of dependent claims 2–6 would have been obvious over Glass.

*F. Obviousness Based on Rieger*

Petitioner contends claim 1 would have been obvious over Rieger. Pet. 1, 41–61. Petitioner cites disclosures in Rieger which are similar to disclosures in Glass. *Compare* Pet. 22–38, *with id.* at 41–57 (citations omitted). Like its challenge based on Glass, Petitioner argues that Rieger discloses

[1c] monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity,

because Rieger describes a “protected section” or “‘secure compartment’ surrounding internal components including [Rieger’s] *sensor* and *memory*.” Pet. 48–49 (citing Ex. 1006, 4, Fig. 3); Pet. Reply 16. As shown below in Petitioner’s annotation of Figure 3 of Rieger, a digital camera, containing a CCD-Sensor (a “sensor”) and RAM (a “memory”), is enclosed, along with numerous other components, in a highlighted “protected section.” Pet. 44; *see* Ex. 1006, 4 (disclosing that the protected section includes “the CCD sensor, the camera CPU (which also contains a signature chip with the secret key), the RAM, the internal clock, a back-up power supply and the required connector cables”), Fig. 3.<sup>9</sup>

---

<sup>9</sup> Similar to its asserted ground based on Glass, Petitioner does not argue that a person of ordinary skill in the art would have been motivated to modify Rieger’s device in any way; Petitioner solely argues that Rieger teaches

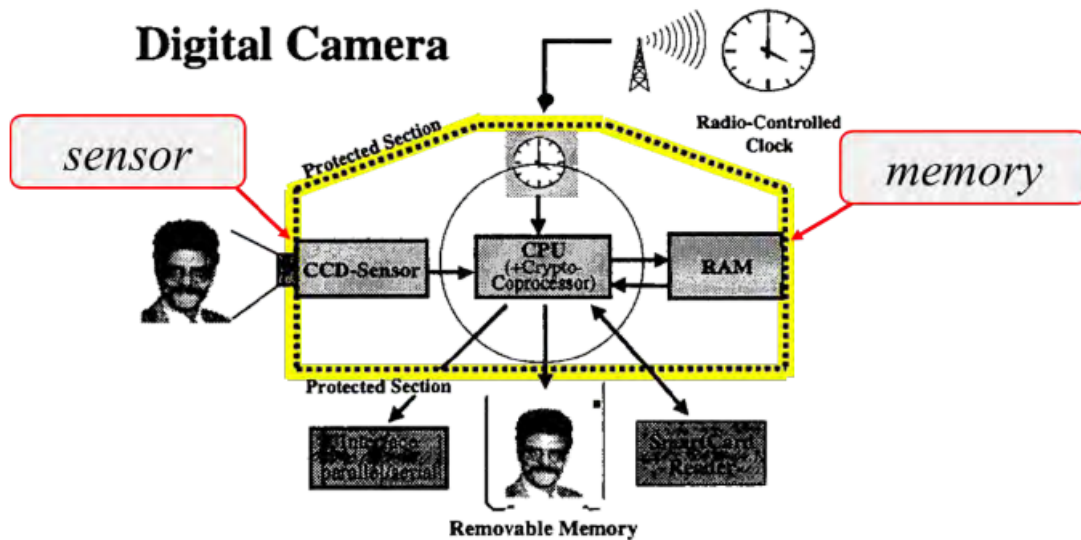


Figure 3: Basic conceptual diagram of a digital camera involving digital signature methods.

**Rieger, Fig. 3 (annotated, highlighted)**

Patent Owner argues, like its arguments in the challenge based on Glass, that Rieger monitors a “protected section” housing multiple components and interconnections, rather than monitoring the integrity of the coupling between Rieger’s sensor and memory. PO Resp. 35–38.

Petitioner acknowledges that, rather than specifically monitoring the integrity of the coupling between the sensor and memory, “Rieger monitors the ‘secure compartment’” as a whole. Pet. Reply 16. As we explained in our discussion of Petitioner’s challenge based on Glass (*see* §§ II.C.2, II.E.1), the claim requires specifically monitoring the physical coupling between the sensor and memory. Therefore, we determine that monitoring Rieger’s “protected section” or “secure compartment” does not teach or suggest “monitoring the integrity of the tight coupling between said memory

---

limitation [1c], based on Petitioner’s proposed claim construction. *See* Pet. 48–50 (“Rieger discloses this limitation.”); Pet. Reply 16–17 (“Glass and Rieger disclose the ‘monitoring’ step.”).

and said sensor.” Consequently, we determine that Petitioner has not shown, by a preponderance of the evidence, that the subject matter of claim 1 would have been obvious over Rieger.<sup>10</sup>

Claims 2–6 depend from independent claim 1. Ex. 1001, 22:1–16. Each of these dependent claims include all the limitations of the respective independent claim. Petitioner’s reliance on and application of Rieger to these dependent claims does not cure the above-noted deficiency of independent claim 1. *See* Pet. 57–61. Accordingly, we also determine that Petitioner has not shown, by a preponderance of the evidence, that the subject matter of any of dependent claims 2–6 would have been obvious over Rieger.

#### *G. Remaining Grounds*

Petitioner’s remaining grounds each challenge claims 1–6 based on Glass or Rieger in various combinations with Exif 2.0, Exif 2.1, and Serret-Avila. Pet. 1. Petitioner’s reliance on Exif 2.0, Exif 2.1, and Serret-Avila does not cure the above noted deficiencies with regards to Glass or Rieger. *See id.* at 61–72. Specifically, Petitioner does not assert Exif 2.0, Exif 2.1, or Serret-Avila, alone or in combination with Glass or Rieger, teach or suggest limitation [1c]. *See id.* Accordingly, Petitioner has not shown, by a preponderance of the evidence, that the subject matter of any of claims 1–6 would have been obvious over Glass or Rieger in combination with Exif 2.0, Exif 2.1, or Serret-Avila.

---

<sup>10</sup> For clarity, given our determination herein regarding limitation [1c], we need not decide Patent Owner’s other arguments regarding limitations [1b] and [1g]. *See* PO Resp. 28–35, 38–41.

### III. CONCLUSION

Based on the evidence presented with the Petition, the evidence introduced during the trial, and the parties' respective arguments, Petitioner has not shown by a preponderance of the evidence that any of claims 1–6 are unpatentable.

In summary:

| <b>Claim(s)</b> | <b>35<br/>U.S.C.<br/>§</b> | <b>Reference(s)/<br/>Basis</b>    | <b>Claim(s)<br/>Shown<br/>Unpatentable</b> | <b>Claim(s) Not<br/>Shown<br/>Unpatentable</b> |
|-----------------|----------------------------|-----------------------------------|--------------------------------------------|------------------------------------------------|
| 1–6             | 103(a)                     | Glass                             |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Rieger                            |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Glass, Exif 2.0                   |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Glass, Exif 2.1                   |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Rieger, Exif 2.0                  |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Rieger, Exif 2.1                  |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Glass, Serret-<br>Avila           |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Rieger, Serret-<br>Avila          |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Glass, Exif 2.0,<br>Serret-Avila  |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Glass, Exif 2.1,<br>Serret-Avila  |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Rieger, Exif 2.0,<br>Serret-Avila |                                            | 1–6                                            |
| 1–6             | 103(a)                     | Rieger, Exif 2.1,<br>Serret-Avila |                                            | 1–6                                            |

#### IV. ORDER

It is:

ORDERED that claims 1–6 of U.S. Patent No. 6,757,828 B2 are not determined to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

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

---

WEATHERLY, *Administrative Patent Judge, dissenting.*

I. INTRODUCTION

The majority finds that Petitioner has failed to demonstrate that the challenged claims are unpatentable because Petitioner has failed to prove by a preponderance of evidence that the prior art teaches or suggests an aspect of limitation 1c within independent claim 1. Dec. 28–34. More specifically, the majority concludes that Petitioner has failed to prove that the prior art forming the basis of Petitioner’s challenges teaches the step of “monitoring the integrity of the tight coupling between said memory.” *Id.* The majority agrees with Patent Owner’s contention that this phrase means “determining whether the physical coupling between said memory and said sensor has been accessed or disturbed, which specifically requires monitoring the physical coupling between the sensor and the memory.” *Id.* at 24. Although I agree with this aspect of the majority’s interpretation of the “monitoring”

step, I disagree with the majority's conclusion that the "monitoring" step also "*specifically* requires monitoring the physical coupling between the sensor and the memory." *Id.* at 16 (emphasis added). Because I disagree on this aspect of the majority's interpretation of limitation 1c, I also disagree with the majority's finding that Glass does not teach limitation 1c. *Id.* at 31. For these reasons, I respectfully dissent.

## II. ANALYSIS

Patent Owner argued that in limitation 1c when "determining whether the physical coupling between said memory and said sensor has been accessed or disturbed," the claimed method also "specifically requires monitoring the physical coupling between the sensor and the memory." PO Resp. 10–11; Sur-reply 9–10. The majority agrees with this additional requirement, and in finding that Glass fails to teach it, implicitly finds that "specifically" monitoring the tight coupling refers to more than monitoring whether the "tight coupling" has been "accessed or disturbed." I would conclude that this narrow reading of limitation 1c is inconsistent with the plain language, the Specification, and the prosecution history support.

I agree with the majority that grammatically, "monitoring the integrity of the tight coupling," means that "the integrity of the tight coupling" is "monitored." Dec. 17. I also agree with the majority that "monitoring" involves "determining whether the physical coupling has been 'accessed or disturbed.'" *Id.* However, the claim does not expressly limit any such "monitoring" to "specifically" the tight coupling. Additionally, I do not agree that adding a requirement of "specifically monitoring" to limitation 1c clarifies the meaning of the limitation unless it is interpreted to mean that when "monitoring the integrity of the tight coupling," no other integrity may

simultaneously be “monitored,” a sort of negative limitation. I find such a negative limitation to be inconsistent with determining whether the tight coupling has been “accessed or disturbed” because I read “accessed” more broadly than “disturbed.” That is, a physical “coupling” may be “accessed” without the coupling being “disturbed.”

The Specification as a whole is directed to a “method of indigenous authentication.” Ex. 1001, 2:59–60. The only time the Specification expressly refers to any aspect of “monitoring the integrity of a tight coupling” is when it 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.” *Id.* at 4:65–67.

The Specification never provides details about what constitutes a “tight coupling,” and never explains whether a “coupling” refers to a physical connection between two physical structures or also refers more broadly to a functional relationship between two items. The only explanation for what the inventor considers to define two or more items being “tightly coupled” appears when explaining the concept of “indigenous authentication” and reads as follows:

A key to verifiable authenticity is to insure [sic] that the authentication information generation is *tightly coupled* to the sensor set and recorder. There can be nothing that can possibly alter the recording before the authentication information is generated. Authentication using this method requires neither comparison files, nor conventional or reverse encryption. . . . The absence of required conventional encryption or reverse encryption eliminates the need for a public registrar or record keeping relating to the management of decryption keys. As the authentication is indigenous there is no requirement to identify which recorder was used.

*Id.* at 3:16–31 (emphasis added). This passage broadly refers to a tight coupling in a functional sense, that is, in the sense that the relationship between the signal generated by a sensor and the data stored in memory reflecting that signal must be “tightly coupled” so that “nothing can possibly alter the recording.” No details are provided regarding how such alterations in the recording of sensor data are prevented.

During prosecution of the application that resulted in the ’828 patent, the applicants attempted to distinguish Schipper<sup>11</sup> by amending claim 1 to require that the claimed method use “a sensor, which is tightly coupled to said memory to generate at least one internal and unique parameter.” Ex. 1002, 151–154, 274–276, 277, 355. The applicants argued that “[b]ecause processor is ‘tightly coupled’ to the memory, it will be virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor.” *Id.* at 277. The applicants argued that Schipper did not teach the claimed “tight coupling” between sensor and memory. *Id.*

The Examiner again rejected claim 1, this time over the combined teachings of Schipper and Maloney.<sup>12</sup> The applicants further amended claim 1 by adding limitation 1c. *Id.* at 293. The applicants argued that neither Schipper nor Maloney taught “monitoring the integrity of the tight coupling between said memory and said sensor when at least one internal and unique parameter is generated.” *Id.* The applicants explained that the “monitoring” step “means that, for example, a signal is generated if the device that prevents *physical access* to the interconnections between the

---

<sup>11</sup> U.S. Patent No. 5,764,770 (“Schipper”). Ex. 1002, 151–154.

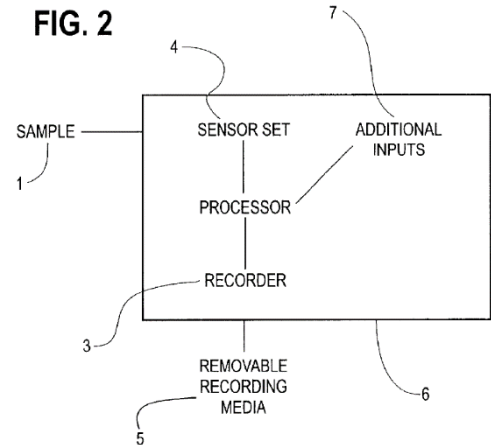
<sup>12</sup> U.S. Patent No. 6,253,337 (“Maloney”). Ex. 1002, 282–285.

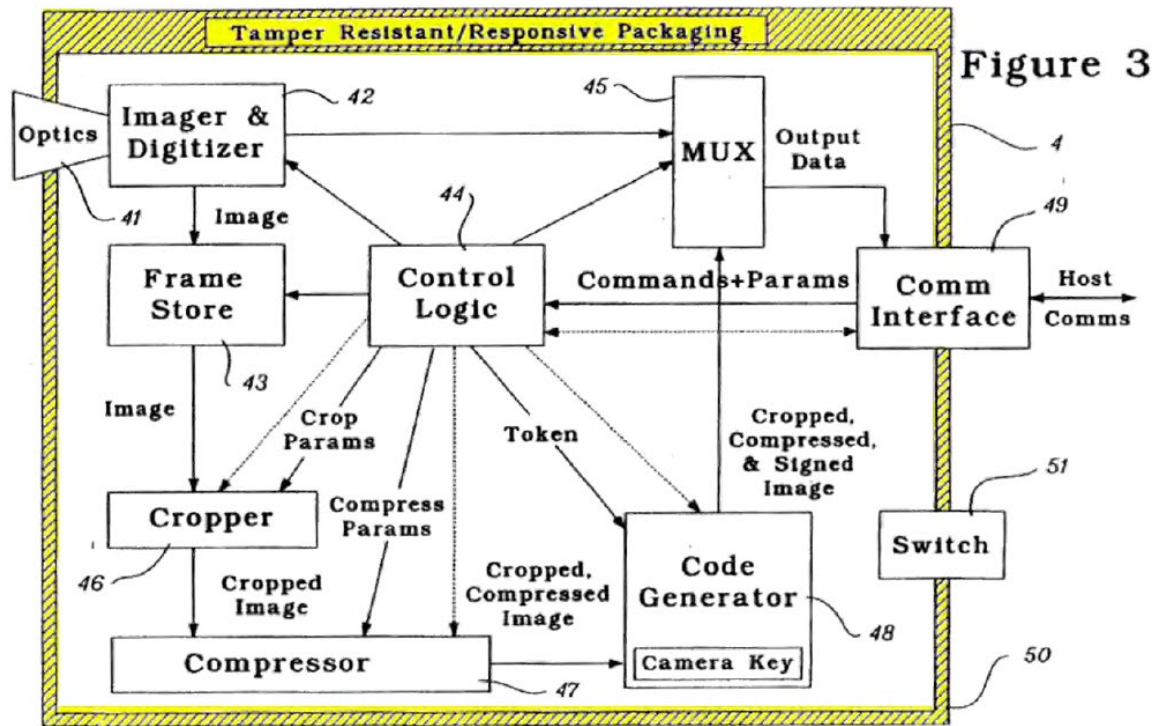
sensor set and the memory is broken.” *Id.* at 292–293 (emphasis added). Thus, applicants explained that “monitoring” encompasses generating a signal when a device that prevents physical access to the sensor and memory is “broken.”

I find that the Specification refers to such a device as “a self-contained camera” as schematically illustrated in Figures 2 and 2A.

Ex. 1001, 2:12–17. Figure 2, the relevant portion of which is reproduced at right, illustrates the “self-contained camera” with a sensor set 4 and recorder 3 “inside the physical device boundary” such that they “are not accessible to the user without detection.” *Id.* at 3:60–64. Crossing the “physical device boundary” would provide “access” to the tight coupling between the sensor set 4 and recorder 3. Thus, the Specification describes using the “physical device boundary” of a “self-contained camera” as the method of preventing access to the tight coupling of the sensor and memory.

Petitioner persuades me that Glass describes the same sort of “device” in the form of the tamper resistant package 50 (a physical device boundary of a self-contained camera) containing imager 42 (sensor) and frame store 43 (memory). Petitioner addresses whether Glass discloses limitation 1c in its analysis of an annotated version of Glass’s Figure 4, reproduced below.





Pet. 31; Ex. 1005, Fig. 4. In Fig. 4, Glass describes imaging system 4 in which imager & digitizer 42 (a sensor) and frame store 43 (a memory) is enclosed within tamper-resistant packaging 50 (highlighted yellow).

Pet. 30–31; *see* Ex. 1005, 5:13–45, Fig. 3. Petitioner explains that if Glass’s package 50 is compromised, a “chassis intrusion detector or switch 51” causes Glass’s imaging system to be placed in a non-functioning state. *Id.* at 31–32 (citing Ex. 1005, 5:16–19, 5:26–34, Fig. 3). Petitioner thus contends that “[b]y monitoring Glass’s tamper resistant package 50, Glass discloses monitoring the integrity of [all] components and interconnections contained in that packaging including the *tight coupling* between *sensor* and *memory*.” Pet. Reply 16.

Accordingly, I dissent from the majority’s decision finding that Petitioner has failed to prove by a preponderance of evidence that Glass teaches limitation 1c.

IPR2024-01352  
Patent 6,757,828 B1

FOR PETITIONER:

James Day  
Winston Liaw  
FARELLA BRAUN & MARTEL LLP  
jday@fbm.com  
wliaw@fbm.com

FOR PATENT OWNER:

Bryan Atkinson  
Micheal Saunders  
PRINCE LOBEL TYE LLP  
batkinson@princelobel.com  
msaunders@princelobel.com