

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

**DECLARATION OF ZIXIANG XIONG, PH.D. IN SUPPORT OF
PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE**

I, Zixiang Xiong, Ph.D., declare as follows:

1. I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters stated herein.

2. I have been asked by Adobe Inc. to provide my opinions in response to certain arguments and assertions made in the Patent Owner's Response (Paper 16) and accompanying declaration of Bill Davis (EX2005).

I. PERSON OF ORDINARY SKILL IN THE ART

3. Patent Owner and Mr. Davis largely agree with my definition of a person of ordinary skill in the art or POSITA. They only dispute my opinion that such a person would have experience involving image processing. Paper 16, 4; EX2005, ¶¶52-53.

4. I explained why I believe a POSITA would have such experience in my initial declaration. EX1003, ¶¶82-87. In response, Mr. Davis states "that the '828 Patent is primarily directed to digital security and authentication." EX2005, ¶53. I disagree. While the patent applies digital security and authentication concepts, it does so primarily in the context of a digital camera and digital image processing. The patent certainly does not discuss any new digital security or authentication techniques such as a new cryptographic algorithm. Rather it applies well-known techniques in order to authenticate digital images and other types of data streams.

5. The patent claims confirm that the '828 Patent is directed to individuals with experience with digital cameras and digital image processing. While claim 1 recites a “method for authenticating a data stream stored in a data file in memory,” claim 2 states that the “memory” is in “a digital camera.” EX1001, 20:59-22:2. Claim 5 recites that an “additional parameter” added to the data file can include a variety of parameters related to digital photography (e.g., zoom settings, AutoFocus status, focus quality sampling, flash status). EX1001, 22:9-14. And claim 6 states that the “data stream is a digit[al] sample of an environment” such as a digital image. EX1001, 22:15-16.

6. Similarly, the patent specification discusses the claimed invention in the context of a digital camera including an optical sensor (for capturing image data) and a processor (for processing the captured image data). EX1003, ¶85; EX1001, Figs. 2, 2A. While the patent states that the disclosed technique could be used for other types of data streams, the written description is focused almost entirely on authenticating digital image data. Indeed, every figure in the patent relates to a digital camera or processing an image captured using a digital camera. Thus, the patent’s primary focus is on processing and authenticating digital image data.

7. The specification of the '828 Patent presumes an understanding of image processing. For example, as I noted in my initial declaration, the

specification provides an extensive description of three different levels of authentication and damaged-element recovery including (1) total image authentication; (2) row/column authentication; and (3) element level authentication and damage recovery. EX1003, ¶85; EX1001, 7:1-19:62, Figs. 6B-9B4. The patent discusses techniques for authentication and damage recovery at the “pixel” level (i.e., the smallest individual element in a digital image). EX1001, 10:14-21.

8. As another example, the patent describes processing both a “Primary Image” (i.e., “the one the user can see”) and a “Backup Image,” which is the “compressed and encoded version of the image....” EX1001, 12:2-8. Image compression/decompression and encoding/decoding are fundamental concepts in image processing. That they are not discussed in any detail in the specification confirms that the inventors recognized that a POSITA would have a basic understanding of image processing.

9. In addition, the prior art cited on the face of the '828 Patent is largely focused on processing and authenticating digital image data. For instance, U.S. Patent No. 5,499,294 (“Friedman”) is entitled “Digital Camera with Apparatus for Authentication of Images Produced from an Image File” and is directed to “a digital camera equipped with apparatus for enabling an image file produced by the camera to be authenticated.” EX1015, 1:15-19. U.S. Patent No. 5,764,770 (“Schipper”) is entitled “Image Authentication Patterning” and is directed to

“identification of the circumstances under which a visual image was formed, and authentication of the image.” EX1017, 1:9-11. U.S. Patent No. 6,269,446 (“Schumacher”) is entitled “Authenticating Images from Digital Cameras” and is directed to “public key/private key authentication of images from digital cameras....” EX1019, 1:6-10.

10. Thus, I disagree with Patent Owner’s and Mr. Davis’s argument that a POSITA would not have experience involving image processing.

11. While I disagree with the definition of a POSITA proposed by Patent Owner and Mr. Davis, I would qualify as a person of more than ordinary skill in the art under their definition. Further, while I disagree with their definition of a POSITA, I have been asked to consider whether my opinions expressed in this matter would change if I assume their definition. I have considered my opinions, and I have concluded that they would not change even if I were to apply the definition of a POSITA proposed by Patent Owner and Mr. Davis.

II. CONSTRUCTION OF THE “TIGHTLY COUPLED” LIMITATION

12. Patent Owner and Mr. Davis argue that the claim phrase “a sensor, which is tightly coupled to said memory” means “a sensor that is electrically or physically coupled to memory in a device.” Paper 16, 9; EX2005, ¶61. I disagree, and continue to believe that a POSITA would have understood the phrase “a sensor, which is tightly coupled to said memory,” as it is used in the ’828 Patent, to

mean “a sensor coupled to said memory via conductive traces or leads” for the reasons I explained in my initial declaration. EX1003 ¶¶93-96.

13. However, I have been asked to consider whether, if I were to adopt Patent Owner’s proposed construction of the phrase, any of my opinions regarding the obviousness of the challenged claims would change. My opinions would not change because both Glass and Rieger disclose “a sensor that is electrically or physically coupled to memory in a device” for essentially the same reasons I explained in my initial declaration. Thus, both Glass and Rieger disclose “a sensor, which is tightly coupled to said memory” under Patent Owner’s proposed construction of that phrase.

14. As I explained in my initial declaration, for example, Glass’s Figure 3 shows “Optics” 41 and “Imager & Digitizer” 42 (which includes the claimed *sensor*) connected to “Frame Store” 43 (which is or includes the claimed *memory*). EX1003, ¶171. 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. A POSITA would recognize a CCD (charge-coupled device), CMOS (complementary metal-oxide semiconductor), or other two dimensional imager that creates a digital image to be integrated circuits. Integrated circuits include leads (i.e., conductive wires or balls) used to electrically connect the integrated circuit to a circuit board. EX1030, 1 (illustration of an integrated circuit

with leads); EX1031, 3:10-21, Figs. 1 and 2 (figures illustrate “solid state imaging device 2” with “leads 5a, 5b....”); EX1033, 3 (defining “lead” as a “wire to or from a circuit element”); EX1034, 3 (defining “lead” as a “term often used to denote an electric wire or cable”). The leads are connected to traces, which are conductive wires running through a circuit board to interconnect components. EX1032, 3:15-24, Fig. 1; EX1035, 3 (defining “trace” as a “conductive path on a printed circuit board”). The arrow from the *sensor* to the *memory* in Figure 3 indicates that those components are electrically connected so that image data can flow from the *sensor* to the *memory*. EX1005, 5:46-48 (“data paths are shown in solid lines”), 5:52-54 (“The digital image is sent to...a frame store memory 43.”). Thus, the arrow from optics 41/imager & digitizer 42 to frame store 43 shows “a sensor that is electrically...coupled to memory in a device” are required by Patent Owner’s proposed construction.

15. Reiger also discloses a sensor that is electrically coupled to memory in a device. Rieger’s Figure 3 shows “CCD-Sensor” (which is the claimed *sensor*) connected to “RAM” (which is the claimed *memory*) via the CPU. EX1003, ¶228. 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.

EX1030, 1; EX1031, 3:10-21, Figs. 1 and 2 ; EX1032, 3:15-24, Fig. 1. 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 were made using conductive leads and traces. The arrows from the *sensor* to the *memory* indicate that they are electrically connected so that data flows from the *sensor* to the *memory* via the CPU. EX1006, 4 (“After recording, the processor reads the image data from the CCD sensor and saves these to the RAM.”) Thus, the arrow from CCD-Sensor to RAM via the CPU show “a sensor that is electrically...coupled to memory in a device” are required by Patent Owner’s proposed construction.

16. I have also been asked to consider whether my opinions regarding the obviousness of the challenged claims would change if the definition of the phrase “a sensor, which is tightly coupled to said memory” were to be modified to require that the connections between the sensor and memory not be physically accessible to the user. My opinions would not change because both Glass and Rieger disclose that the *sensor* and *memory* are not physically accessible to the user for reasons I explained in my initial declaration.

17. As illustrated in Glass’s Figure 3, optics 41/imager & digitizer 42 and frame store 43 are both located inside “Tamper Resistant/Responsive Packaging”

in Glass's imaging system 4. EX1005, Fig. 3. Glass states that "[i]n our preferred embodiment, the imaging system 4, will be enclosed in a tamper resistant package 50 which will be used to detect unwelcome intrusion and render the system useless." EX1005, 5:20-23. Glass states that the "tamper resistant package can be passive in that any opening to the device will cause its ultimate destruction. Alternatively, the packaging could utilize at least one chassis intrusion detector or switch 51," which will "signal the control logic 44...to return to a non-functioning state similar to that found during assembly." EX1005, 5:23-30. Because the *sensor* and *memory* are contained in tamper resistant packaging in Glass's imaging system 4, the connection between the *sensor* and *memory* is not physically accessible to the user.

18. In Rieger, Figure 3 illustrates that the CCD-Sensor and the RAM are housed within a "Protected Section" in Rieger's manipulation-proof digital camera. EX1006, 4. Rieger states that "[i]n order to protect image data against manipulation from the moment they are received in the CCD sensor to generation of the signature, some of the system components, including the CCD Sensor...[and] the RAM...must be integrated into a specially protected compartment," as illustrated in Figure 3. EX1006, 4; EX1003, ¶228. Rieger further states:

The secure compartment can be protected, for example, by an

electrical “protective shield”. When this is drilled or severed, a change in potential is triggered and detected by the processor, which then automatically deletes the secret key stored in the signature chip. This ensures that image data cannot be altered without detection prior to application of the signature.

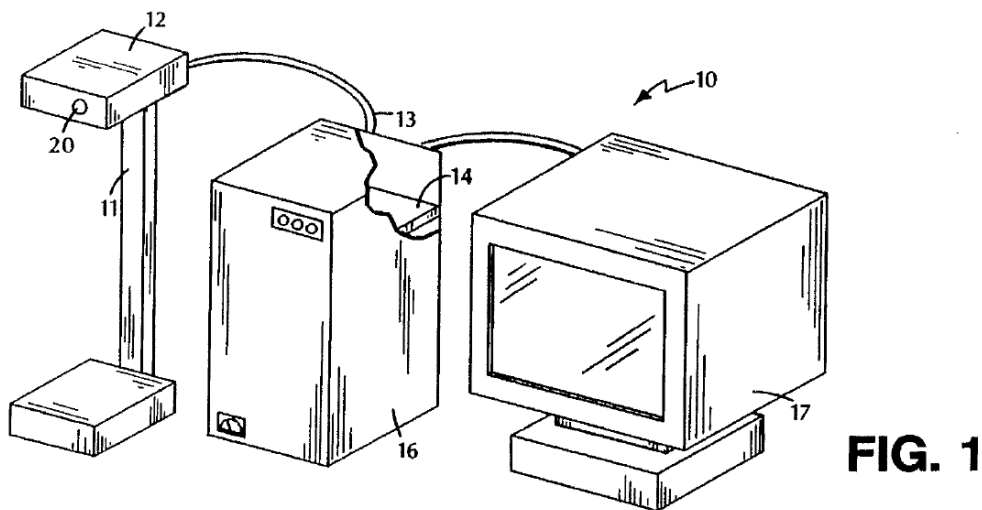
EX1006, 4. Because the CCD-Sensor and RAM are contained in a secure compartment of Rieger’s manipulation-proof digital camera, the connection between the *sensor* and *memory* is not physically accessible to the user.

III. GLASS AND RIEGER DISCLOSE A SENSOR CONNECTED TO MEMORY BY CONDUCTIVE LEADS AND TRACES

19. Patent Owner and Mr. Davis argued that Glass and Rieger do not disclose “a sensor, which is tightly coupled to said memory” because the connection between the components could be made in some way other than conductive leads and traces. Paper 16, 12, 28; EX2005, ¶¶70, 92. A POSITA would not understand Glass or Rieger to disclose a connection between the claimed *sensor* and *memory* in any of the ways they suggest.

20. First, Patent Owner and Mr. Davis cite U.S. Patent No. 5,486,853 (EX2007), which they state discloses “an electrical cable for connecting an electronic camera to a processor.” Paper 16, 14, 30-31; EX2005, ¶72, 94. But the cited patent does not disclose an electrical cable connecting two components within the same device, let alone an optical sensor connected to a processor/memory within the same device as is illustrated in Glass (Figures 2 and

3) and Rieger (Figure 3). Instead, as shown in the figure below, the '853 Patent discloses “an electrical cable 13” that connects “a video electronic camera head 12” to “a video processor card 14, inserted within personal computer 16, where the signals are digitally processed before being displayed on a monitor 17.” EX2007, 5:17-23.



EX2007, Fig. 1. The '853 Patent states that cable 13 is a “coaxial cable” including multiple conductive wires. EX2007, 6:39-42, 6:48-55, Figs. 7A, 7B.

21. A POSITA would not understand the figures in Glass or Rieger to illustrate an optical sensor connected to memory using a cable like the one disclosed in the '853 Patent. Using coaxial cable would require unnecessary additional space, would increase the cost, and would introduce additional points of potential failure where the coaxial cable connects to the circuit board or digital components, and it would not provide any added benefit. In comparison, connecting the internal digital components in the standard manner by soldering

leads to traces on circuit boards would require far less space, would be cheaper, and would be less likely to fail. Further, there would be no reason to connect components inside Glass's imaging system 4 or Rieger's camera with a cable like the one in the '853 Patent because there would be no reason for anyone to disconnect and reconnect the internal components (as they do with separate devices). This is particularly true because the sensor and memory are a tamper resistant packaging (Glass) or secure compartment (Rieger) intended to prevent access to the internal components and connections. I do not believe that using a cable as in the '853 Patent would have even occurred to a POSITA as a viable option for connecting the *sensor* and *memory* in Glass's imaging system 4 or Rieger's manipulation-proof digital camera.

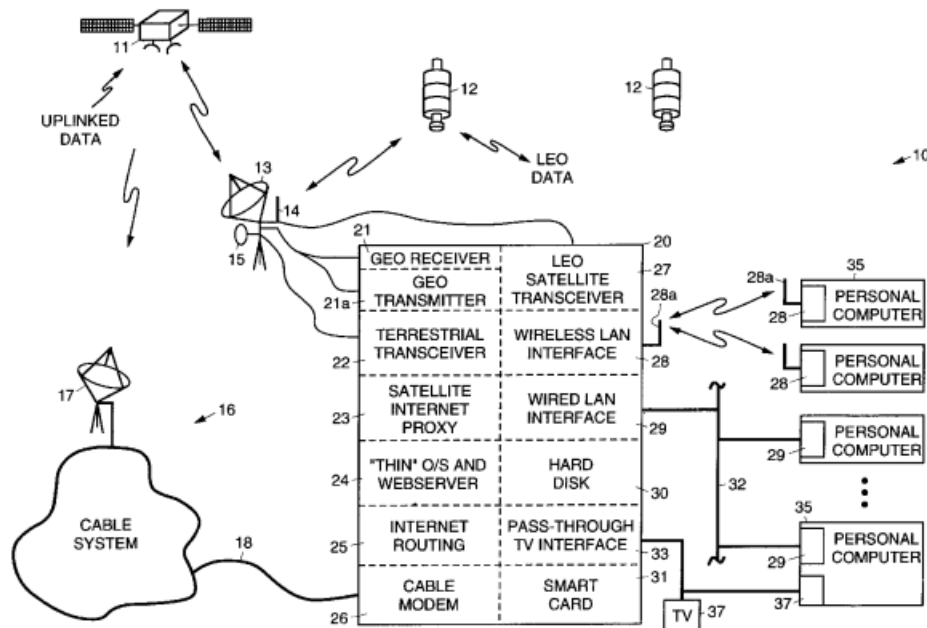
22. Next, Patent Owner and Mr. Davis cite U.S. Patent 7,161,622 (EX2008), which they state discloses "an electronic camera with a wireless communication interface for transmitting image information from the camera." Paper 16, 15, 31; EX2005, ¶73, 95. Again, this patent discloses one device communicating with another separate device. Specifically, it describes digital camera 1 with attached communication unit 2 that permits wireless transmission of image data off the camera to a separate device such as a personal computer. EX2008, 2:64-3:1 ("the recorded image file is automatically transferred to, for example, the personal computer in one's own house, the laboratory which is

contracted beforehand, or the server of the computer network joined beforehand”), 4:24-32 (“the image data file received from electronic camera 1 is transferred to the personal computer of own house, the laboratory which is contracted beforehand or, and the data server of the computer network service joined beforehand”). The ’622 Patent does not disclose two components wirelessly connected within the same device, let alone a sensor and memory wirelessly connected within the same device as is illustrated in Glass and Rieger.

23. Patent Owner and Mr. Davis seem to suggest that a POSITA would have considered implementing Glass’s imaging system 4 and Rieger’s camera with a connection from the optical sensor going to a wireless transmitter inside the device so that it could send a wireless signal to a receiver connected to the memory in the same device. A POSITA would not understand the figures in Glass or Rieger to illustrate a wireless connection between the optical sensor and memory. A POSITA would have realized that one would instead simply connect the optical sensor and memory using leads and traces to eliminate the wireless transmitter and the wireless receiver to reduce the component cost and overall size while improving performance. Moreover, both Glass and Rieger are concerned with maintaining security of image data. A POSITA would have known that a wireless connection between the optical sensor and memory would be much less secure than the standard manner of connecting components via leads and traces. I do not

believe that a wireless connection would have even occurred to a POSITA as a viable option for implementing Glass's imaging system 4 or Rieger's manipulation-proof camera.

24. Next, Patent Owner and Mr. Davis cite U.S. Patent 6,377,981 (EX2009), which they state discloses “a system providing high-speed internet access through satellite communication links.” Paper 16, 15-16, 32; EX2005, ¶¶74, 96. The figure below from the '981 Patent depicts satellite communication between personal computers at different locations.



EX2009, 2. It does not show or even suggest using a satellite to transmit information from one component inside a computer to another component inside the same computer.

25. While I find it somewhat hard to believe, Patent Owner and Mr. Davis seem to suggest that a POSITA would have considered implementing Glass's imaging system 4 and Rieger's camera with a connection from the optical sensor to a satellite transmitter so that it could send a signal to a satellite to be bounced back to a satellite receiver connected to the memory in the same device. A POSITA would **not** understand Glass or Rieger to illustrate a satellite connection between the optical sensor and memory. For one thing, it would require connecting the device to a satellite antenna, which would have been a foot or more in diameter at the time. A POSITA would have realized that one could instead connect the sensor and memory using leads and traces to eliminate the satellite transmitter/receiver/antenna to reduce the component cost and overall size while improving performance. Moreover, Glass and Rieger are concerned with maintaining the security of image data, and a POSITA would know that a satellite connection between the optical sensor and memory would be far less secure than the standard manner of connecting components via leads and traces entirely inside the device. I do not believe that it would have even occurred to a POSITA as a viable option for implementing Glass's disclosed imaging system 4 or Rieger's manipulation-proof camera.

IV. SERRET-AVILA IS ANALOGOUS PRIOR ART

26. Patent Owner and Mr. Davis argue that Serret-Avila is not

“analogous” prior art. Paper 16, 43-46; EX2005, ¶¶110-114. I disagree.

27. I have been informed that a prior art reference is “analogous” to the challenged patent when (1) the reference is from the same field of endeavor as the challenged patent regardless of the problem addressed, or (2) the reference is not in the same field of endeavor but it is reasonably pertinent to the particular problem addressed by the challenged patent. As I stated in my initial declaration in this matter, Serret-Avila and the ’828 Patent disclose inventions in the same field of endeavor (i.e., image processing) and also address the same problem (i.e., authenticating images). EX1003, ¶¶286, 289.

28. Mr. Davis argues that “Serret-Avila is generally in the field of internet transaction or e-commerce security.” EX2005, ¶111. I disagree. Serret-Avila discloses a technique for authenticating data streams that is described largely in the context of video, audio, and other multimedia data. EX1011, 6:13-18 (“several embodiments are described in the context of a system and method for viewing or playing video, audio, or multimedia data”). Serret-Avila specifically discusses problems with authenticating streaming video. EX1011, 2:36-49. Serret-Avila also describes various embodiments that apply the disclosed authentication technique to video and multimedia streams. EX1011, 6:13-18, 6:46-52 (embodiment can be a “television set-top box” or “video player”), 7:27-31 (same), 9:8-11 (data stream can be “video” or “multimedia information”), 23:6-11.

Multimedia includes digital images. EX1036, 3 (definition of “multimedia” including “still images (photographs)”); EX1037, 3 (definition of “multimedia” including “still or video images”); EX1038, 3 (definition of “multimedia” including “images”). And streamed video is composed of a series of frames (e.g., MPEG frames), many of which are essentially individual digital images. EX1039, 7-8. Thus, Serret-Avila, like the ’828 Patent, is in a field of endeavor involving processing data streams including digital images.

29. In addition, Serret-Avila and the ’828 Patent both address the problem of authenticating data streams including digital images. Claim 1 of the ’828 Patent recites a “method for authenticating a data stream,” and Serret-Avila is entitled “Systems and Methods for Authenticating and Protecting the Integrity of Data Streams and Other Data.” EX1001, 20:59-60; EX1011, 1. The ’828 Patent specification describes the claimed invention in the context of a digital camera but states that an embodiment can record “a continuous sample of a visual environment” using “a continuous optical recorder such as a video camera, movie film camera or a digital movie camera....” EX1001, 3:41-45. Similarly, Serret-Avila discloses a technique for authenticating a data stream including digital video. EX1011, 2:36-49, 6:13-18, 6:46-52, 7:27-31. Both patents also state that the disclosed authentication techniques can be used for other types of data streams as well. EX1001, 3:8-15, 3:32-39, 3:47-59; EX1011, 6:13-22. And both patents

describe the same problem to be addressed (i.e., the problem presented by intentional or inadvertent manipulation of such data streams). EX1001, 1:15-19; EX1011, 1:51-55. Further, both patents describe techniques for authenticating data and informing users that data has been compromised based on a comparison of hash values calculated before and after transmission. EX1001, 7:25-27, 9:13-15, 9:43-54; EX1011, 8:32-40, 9:53-59, 10:16-45, Figs. 3, 5. Thus, Serret-Avila, like the '828 Patent, addresses the problem of authenticating data streams including digital images.

Acknowledgement of Oath

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1101 of Title 18 of the United States Code.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Zixiang Xiong". The signature is written in a cursive, flowing style.

Zixiang Xiong, Ph.D.

Dated: September 5, 2025