

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

U.S. Patent No. 11,188,998

**DECLARATION OF NATHANIEL POLISH, PH.D.,
UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION
FOR *INTER PARTES* REVIEW**

TABLE OF CONTENTS

I.	INTRODUCTION	4
II.	QUALIFICATIONS AND PROFESSIONAL EXPERIENCE	5
III.	LEVEL OF ORDINARY SKILL IN THE ART	8
IV.	RELEVANT LEGAL STANDARDS	9
V.	BACKGROUND	10
A.	Media Encryption	10
B.	Public Key Cryptography	12
VI.	OVERVIEW OF THE '998 PATENT	13
VII.	CLAIM CONSTRUCTION	17
VIII.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	17
A.	Ground 1: Claims 1-3 and 14 are obvious in view of Vataja and Cox.	18
1.	Summary of Vataja.	18
2.	Summary of Cox	22
3.	Reasons to Combine Vataja and Cox.	25
4.	Claim 1	29
5.	Claim 2	57
6.	Claim 3	58
7.	Claim 14	59
B.	Ground 2: Claims 4-13 are obvious in view of Vataja, Cox, and Hershey.....	61
8.	Summary of Hershey	61
9.	Reasons to Combine Hershey with Vataja and Cox	62
10.	Claim 4	65
11.	Claim 5	67
12.	Claim 6	69
13.	Claim 7	70
14.	Claim 8	72

Declaration of Nathaniel Polish, Ph.D.
Inter Partes Review of U.S. 11,188,998

15.	Claim 9	72
16.	Claim 10	79
17.	Claim 11	79
18.	Claim 12	80
19.	Claim 13	80
IX.	CONCLUSION.....	81

I. INTRODUCTION

1. I am making this declaration at the request of Apple Inc. in the matter of the *Inter Partes* Review of U.S. Patent No. 11,188,998 (“the ’998 patent”) to Malone *et al.*

2. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this investigation. My compensation is not contingent on the outcome of this matter or the specifics of my testimony, and I have no other interest in this case or the parties thereto.

3. I have been asked to provide my opinions regarding whether claims 1-14 (“the Challenged Claims”) of the ’998 patent are unpatentable as they would have been obvious to a person having ordinary skill in the art (“POSITA”) at the time of the alleged invention, in light of the prior art. It is my opinion that all of the limitations of the challenged claims would have been obvious to a POSITA.

4. In the preparation of this declaration, I have studied:

- Ex.1001: U.S. Patent No. 11,188,998 (“the ’998 patent”);
- Ex.1002: Prosecution History of the ’998 patent;
- Ex.1005: U.S. Patent Publication No. 2003/0120940 to Vataja (“Vataja”);
- Ex.1006: U.S. Patent No. 7,216,232 to Cox et al. (“Cox”); and
- Ex.1007: U.S. Patent No. 6,961,441 to Hershey (“Hershey”);

5. In forming the opinions expressed below, I have considered: the

documents listed above; the relevant legal standards, including the standard for obviousness; and my own knowledge and experience based upon my work in the field as described below.

- Ex.1008: RFC 2459;
- Ex.1009: RFC 2437;
- Ex.1010: Complaint, *MyPort Technologies, Inc. v. Apple, Inc.* 1-24-cv-01337 (DDE), Dec 6, 2024.

6. Unless otherwise noted, all **emphasis** in any quoted material has been added. Claim terms are *italicized*.

II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE

7. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Exhibit 1004. The following is a brief summary of my relevant qualifications and professional experience.

8. I am an independent consultant. All of my opinions stated in this declaration are based on my own personal knowledge and professional judgment. In forming my opinions, I have relied on my knowledge and experience in acoustics, signal processing, design of headsets and sound production equipment, and representations of acoustic sounds.

9. I am over 18 years of age and, if I am called upon to do so, I would be

competent to testify as to the matters set forth herein. The following provides an overview of some of my experience that is relevant to the matters set forth in this declaration.

10. I expect to testify regarding my background, qualifications, and experience relevant to the issues in this litigation. I have a Ph.D. in Computer Science from Columbia University. I hold the following four degrees from Columbia, spanning the years 1980 to 1993:

- Ph.D. in Computer Science, May 1993, Thesis: Mixed Distance Measures for the Optimization of Concatenative Vocabularies in Speech Synthesis;
- M.Phil. in Computer Science, December 1989;
- M.S. in Computer Science, December 1987; and
- B.A. in Physics, Columbia College, May 1984.

11. For over thirty years, I have run a computer technology development firm that I co-founded, called Daedalus Technology Group. My primary business activity is the development of computer-related products. This activity involves understanding the business objectives of customers, designing products to suit their needs, and supervising the building, testing, and deployment of these products. I develop hardware and software as well as supervise others who do so.

12. Also, from time to time I found other companies in order to pursue

particular product opportunities. I develop and ultimately sell these companies.

Most of my business activity, however, is as a consulting product developer. From time to time I have also served as an expert witness on computer and software related cases. I am a named inventor on twelve United States patents and am a member of several professional societies, including the IEEE and ACM.

13. I have extensive experience in several areas relevant to this case. My doctoral work was in the area of computer speech. As part of that work I developed signal processing systems and algorithms to filter and manipulate sound, especially speech. That work gave me strong practical insight into such topics as storing, retrieving, and manipulating audio and video information.

14. Much of my professional work over the past thirty years has been as a computer technology product developer. Several of those products involved technologies closely related to the topics in the patent at issue in the current matter, including digital audio systems and associated signal processing. One product in particular was for a company called IVT or burst.com in the later 1990s. That product involved developing a set of systems to record and transmit digital video and audio signals over the internet. Through this work I became very familiar with managing audio and video formats.

15. In addition to this work for IVT, I also worked with the Dun & Bradstreet Corporation in the 1980s to develop a system for interacting with

users of the credit reporting services over the telephone. It was one of the earliest interactive voice response systems that are now commonplace. This work involved the recording and manipulation of audio for use by the computer systems.

16. In 2000, I also supervised the development, design, and deployment of an industrial strength interactive voice response (IVR) system that allows users to access streaming media via their cell phones. This system supported up to 96 streams on a single chassis and was designed for a company called Savos. Under my supervision, the firm developed for this system the web-based content management system and interface for customizable user preferences.

17. Through these and other experiences, I am very familiar with the technologies at issue in this matter.

III. LEVEL OF ORDINARY SKILL IN THE ART

18. A POSITA as of the earliest possible priority date of the '998 patent (September 30, 2002) would have been someone knowledgeable and familiar with the media encryption and storage arts that are pertinent to the '998 patent. That person would have a bachelor's degree in electrical engineering, computer engineering, computer science, or equivalent training, and approximately two years of experience working in the relevant field. Lack of work experience can be remedied by additional education, and vice versa.

IV. RELEVANT LEGAL STANDARDS

19. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '998 patent, I am relying on certain basic legal principles that counsel have explained to me. These principles are discussed below.

20. I understand that prior art to the '998 patent includes patents and printed publications in the relevant art that predate the priority date of the alleged invention recited in the '998 patent.

21. I have been informed that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. I have also been informed by counsel that the obviousness analysis takes into account factual inquiries including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

22. I have been informed by counsel that the Supreme Court has recognized several rationales for combining references or modifying a reference to show obviousness of claimed subject matter. Some of these rationales include the following: (a) combining prior art elements according to known methods to yield

predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

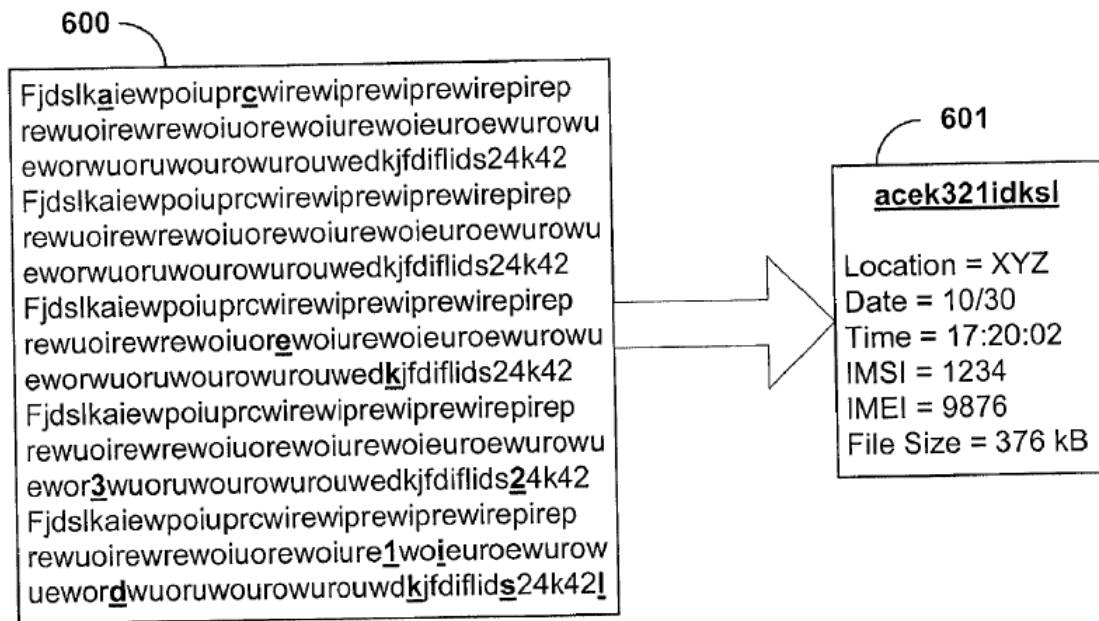
V. BACKGROUND

A. Media Encryption

23. Media files (e.g., audio/video) are often encrypted, either for authentication and verification, or for secure transfer to prevent manipulation in transit. For example, a user who takes a picture, records audio, or records a video may wish to protect their work. “Photographs, music and video are increasingly being digitally represented.” Cox, 1:14-15. “The integrity of digital images is increasingly of concern since many low cost software systems allow very sophisticated image editing capabilities that can seamlessly alter an image.” Cox, 1:30-34. To protect images, it was widely known to use “cryptography” as it was “well understood.” Cox, 1:38-40.

24. Such well-known cryptographic techniques often employ hashing.

“The basic idea behind cryptographic authentication is to pass the data through a one-way hash function resulting in an N-bit hash. The N-bit hash is then encrypted.” Cox, 1:40-43. Hashing is a technique whereby an algorithm is applied to a first set of data to produce a smaller set of data. It would be expected that any change in the data would produce a different hash result. In this way modifications can often be detected. As can be seen in the figure below, random pieces of the data 600 are reduced to a subset of data “acek321idksl” 601 as specified by the hash algorithm. See Vataja, [0022].



Vataja, Fig. 6.

25. The hash of the metadata is often encrypted using either symmetrical and/or asymmetrical encryption techniques. “Using conventional symmetrical

cryptography methods and techniques ... hashed meta-data, can be encrypted with a private key so that only the holder or holders of the private key can decrypt the meta-data.” Hershey, 8:18-22. In other words, the same key used to encrypt the metadata is the same key used to decrypt the metadata. This is distinguished from asymmetrical encryption techniques in which the decryption key is different than the encryption key.

B. Public Key Cryptography

26. One common asymmetrical encryption technique is referred to as public key cryptography. Public key cryptography is a cryptographic system that uses a pair of keys: a public key, which can be shared openly, and a private key, which is kept secret. The fundamental principle is that data encrypted with one key can only be decrypted with the other. This enables secure communication, digital signatures, and authentication without the need for both parties to share a secret key in advance.

27. An example use case involves digital signatures and authentication. For example, hashed data may be “encrypted using the private key of a public key encryption algorithm to form a digital signature. To authenticate the data, the data in question is once again hashed and ... compared with the digital signature that is decrypted using the associated public key.” Cox, 1:43-47. “In the case of digital cameras or other digital content creation devices, authentication and time stamping

require the use of a public key encryption system. The device encrypts the signature and/or time stamp using the camera's private key. The reader must then have knowledge of the corresponding public key in order to, say, authenticate the image.” Cox, 9:13-18. This means that anyone with access to the public key can verify that the data was signed by the holder of the private key, ensuring both authenticity and integrity.

28. Another use of public key cryptography is secure transfer of data. In this case, data is encrypted using the public key—not the private key. The public key is associated with the entity who will be receiving the transferred data. For example a media distributor may have a public key that is widely distributed to others. Only the distributor has the private key and thus only the distributor can decrypt files that are encrypted with its public key. For example, “the meta-data or hashed meta-data, can be encrypted using a public key so that accessors of the encrypted meta-data, or hashed meta-data, having the corresponding second key of the public key pair can decrypt, but not successfully alter, the encrypted data.” Hershey, 8:22-27.

VI. OVERVIEW OF THE '998 PATENT

29. The '998 patent describes and claims nothing more than well-known techniques for encrypting and storing media files.

30. The '998 patent describes “a capture device 102 that is operable to

capture” for example “an image of an individual” or “any type of scene.” Ex.1001, 3:49-51. “This could be a video segment, a still picture or an audio segment.” Ex.1001, 3:52-55.

31. The '998 patent also describes a “local certification” process by which location, time, and date information are collected. Ex.1001, 4:1-26. “For example, the information that is obtained will be time and date information and longitude and latitude information that is received from a GPS system (global positioning system), a conventional system.” Ex.1001, 4:9-12. “The time information, the date information and the longitude and latitude information are provided in such a manner that, when associated with the capture file 108, this provides some current validation that the file was created at that particular time and, at a later time, it could be identified by the fact that it has that information associated therewith.” Ex.1001, 4:12-18. “The result of the local certification is a locally certified captured image 120 which is illustrated with the image and a time stamp, ‘TS.’” Ex.1001, 4:50-52.

32. The '998 patent describes performing a hash operation to create a “representation” of the time-stamped image, video, or audio capture. “The document ... is converted to a ‘hash’ file.” Ex.1001, 5:34-35. “[T]he hash file is a digital representation of the actual captured file.” Ex.1001, 7:56-58. This is recited in claim 1, for example, as “*create a file comprised of a representation of the*

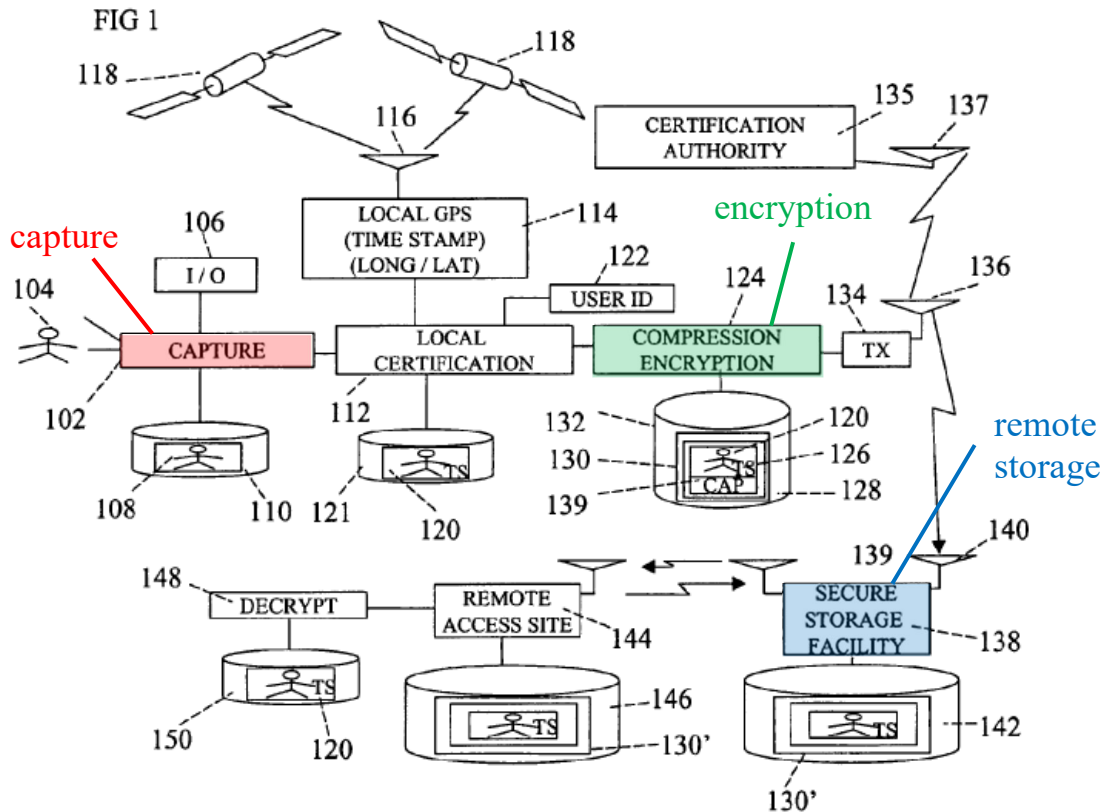
captured information associated with a representation of the date and time of the capture of the information as augmented captured information.”

33. The '998 patent additionally describes an encrypting operation. “[T]he file 120 is processed through an encryption operation wherein the file is first encrypted in accordance with predetermined encryption algorithms.” Ex.1001, 5:20-22. This is recited in claim 1, for example, as “*controlling an encryptor on the device processor to encrypt the augmented captured information as an encrypted file containing encrypted augmented captured information.*”

34. The '998 patent further describes a signing operation that adds signature information to the encrypted file. For example, claim 1 recites “*controlling the device processor to initiate a signing operation for adding signature information to the file including the encrypted augmented captured information to provide an identifiable encrypted file.*” Note that this signing operation is distinct from public or private key encryption processes, which are sometimes referred to as signing operations. Rather, this claimed signing process simply adds identifying information that is recited as “*unencrypted signature information*” that “*provides information to the receiving facility that allows identification of the party claiming to have created the captured information for later identification of the party.*” Ex.1001, claim 1.

35. The concepts of capturing, encrypting and remotely storing digital

media are illustrated in Fig. 1 below.



'998 patent, Fig. 1 (annotated).

36. In one described example, the encryption and signing process is a three-layer encryption technique. After a first layer of symmetrical encryption, “only the holder of the secret key can unlock the file.” Ex.1001, 9:47-48. Then, a second encryption process is performed: “The file is then encrypted using an asymmetrical cryptosystem under the user’s private key, effectively signing the file.” Ex.1001, 9:54-56. In a third layer, “identifying information is added to the (now doubly) encrypted file, and the file is encrypted again—this time, under the storage facility’s public key.” Ex.1001, 9:57-59.

37. In addition to the hashing, encrypting, and signing operations described above, the '998 patent describes that “the encrypted file is then passed to the transmitter 134 for transmission via the antenna 136 along a wireless path to a secure storage facility 138.” Ex.1001, 5:47-49. Upon receipt, the storage facility “performs the following steps: Remove the outer wrapper and extract an encrypted file and plain-text subscriber identification. Look up the subscriber information and recover his/her public key.” Ex.1001, 10:30-35.

38. However, the claimed concepts of hashing, encrypting, signing, and storing remotely were all known before the '998 patent was filed.

VII. CLAIM CONSTRUCTION

39. I understand that claim terms in IPRs are construed according to their “ordinary and customary meaning” to those of skill in the art. I have applied this interpretation throughout my analysis.

VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

40. The discussion in this Declaration provides a detailed analysis of how the asserted prior art references teach each limitation of the Challenged Claims.

41. As part of my analysis, I have considered, and discuss in detail, the scope and content of the prior art and any differences between the alleged invention and the prior art.

42. It is my opinion that the alleged invention recited in the Challenged

Claims would have been obvious in view of the teachings of the asserted prior art and the knowledge of a POSITA before the time of the alleged invention of the '998 patent.

A. Ground 1: Claims 1-3 and 14 are obvious in view of Vataja and Cox.

1. Summary of Vataja.

43. Vataja provides evidence that the hashing, encrypting, signing, and remotely storing media files was known. Vataja relates to “a system and method for protecting multimedia content data, such as photographs, video and audio, with location-based data.” Vataja, [0005]. Vataja’s “invention applies to content-creating devices, such as digital cameras, digital video cameras, digital audio recording devices, and any other devices that allow a user to record ... pictures 100, audio 101, and video 102.” Vataja, [0013].

44. Vataja describes protecting data by hashing and encrypting the captured media along with time and date information. Vataja, [0013]. “As the content is created alone, or in combination with other content, it is collectively transmitted to the content combination program 106” along with “time 103, location 104, and device 105 data.” Vataja, [0013]. “The time 103, location 104, and device 105 data may be incorporated as authentication data.” Vataja, [0013]. “The system then secures the authentication data to the content through content encryption 107, metadata encryption 108, and/or a ‘hash’ encryption 109, each of

which is well-known in the art.” Vataja, [0013]. Vataja illustrates these concepts generally in Fig. 1 shown below.

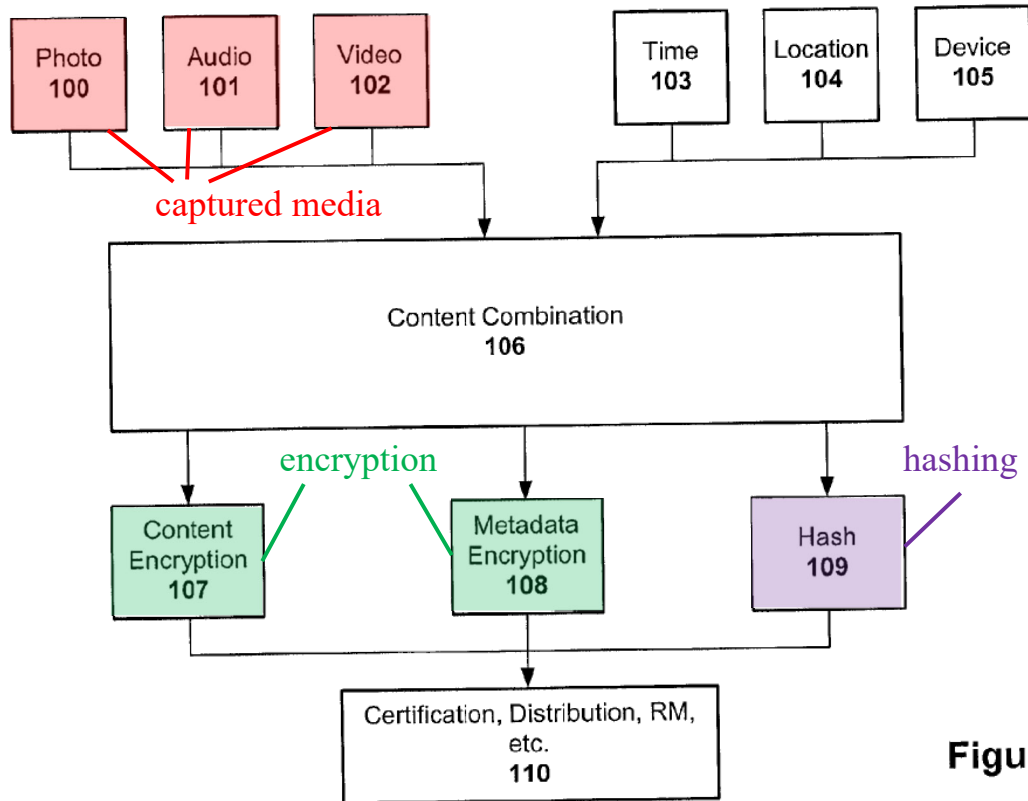
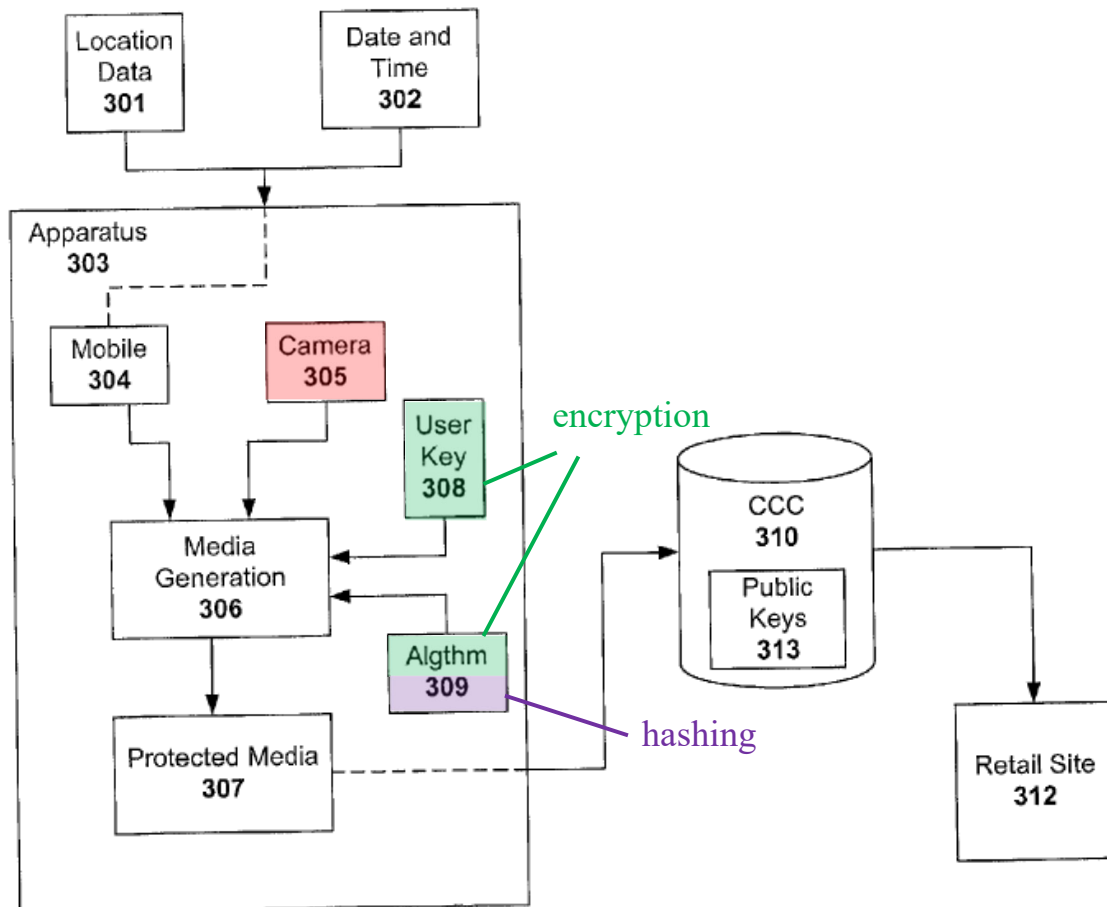


Figure 1

Vataja, Fig. 1 (annotated).

45. Vataja provides additional details of the hashing and encryption processes with respect to Fig. 3A. “Camera 305, or other multimedia audio/visual (A/V) device, initiates the creation of a multimedia file (e.g., video, audio, etc.) that is subsequently transmitted to media generation portion 306.” Vataja, [0018]. “An encrypting algorithm 309 utilizes the data from media generation portion 306 and then utilizes location data 301, date and time data 302 as well as identification information such as e.g. the IMEI and IMSI information to encrypt all the data

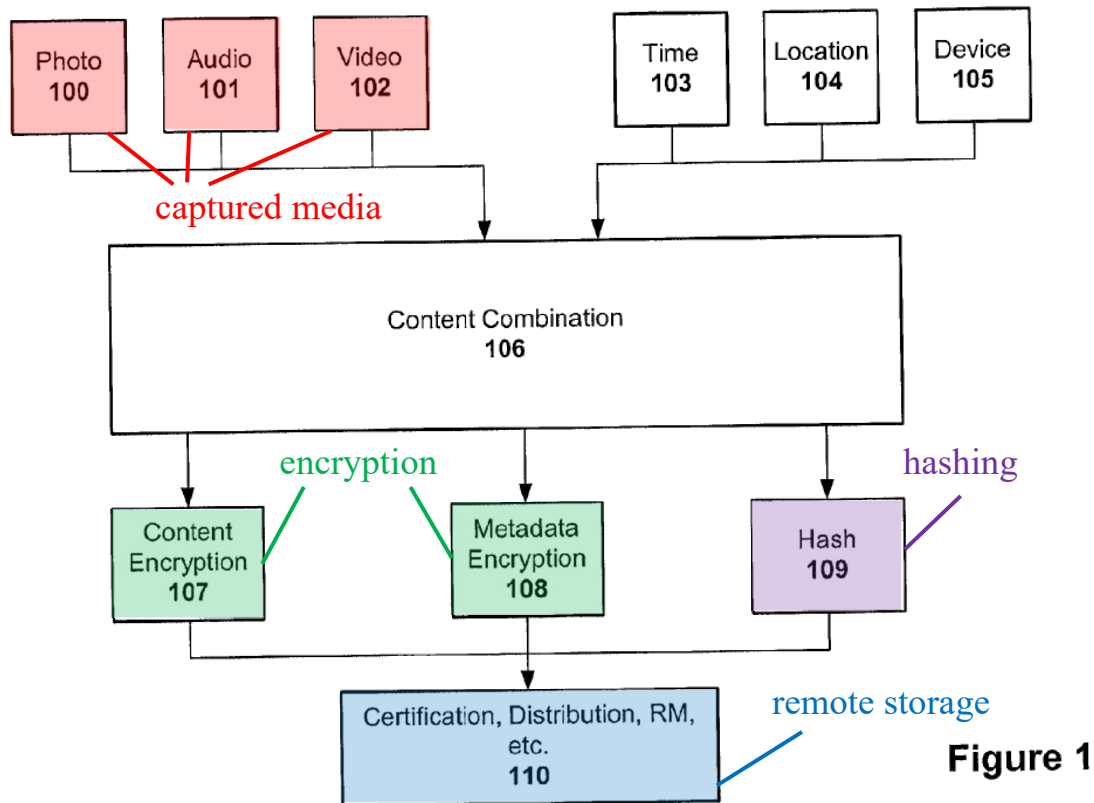
collected in the media generation portion 306.” Vataja, [0018]. “Algorithm 309 may include a ‘hash’ algorithm.” Vataja, [0018]. Fig. 3A of Vataja is shown below.



Vataja, Fig. 3A (annotated).

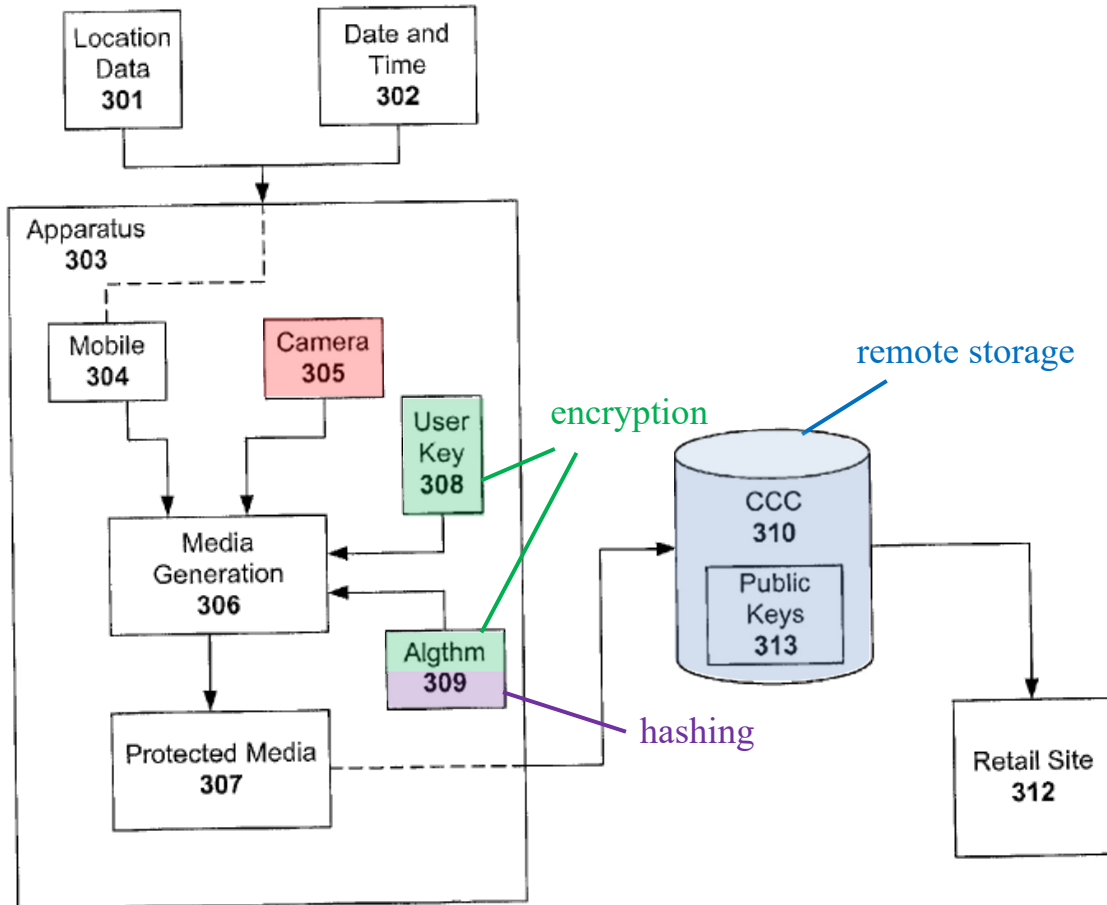
46. In addition to the hashing, encrypting, and signing operations, Vataja describes transmitting the protected media file to a remote facility. “Once an encrypted signature based on the authentication data 103,104, and 105 is integrated into the content file, the file is then transmitted to a Content Certification Company (CCC) 110, or other distributor or Rights Management (RM) provider.” Vataja,

[0014]. “The integrated signature then identifies the content owner, along with the location and time in which the content was created. Once the provider 110 stores the content, it can subsequently be made available for trusted distribution.” Vataja, [0014].



Vataja, Fig. 1 (annotated).

47. “A CCC may be set up so that each user sending multimedia data must be pre-registered as a subscriber. Under this embodiment, the CCC confirm’s [sic] the user as a subscriber 504, either through a password, or through automatic identification of the user’s IMEI/IMSI.” Vataja, [0021].



Vataja, Fig. 3A (annotated).

48. Vataja thus describes the same hashing, encrypting, signing and remote storing concepts that are recited in the '998 patent.

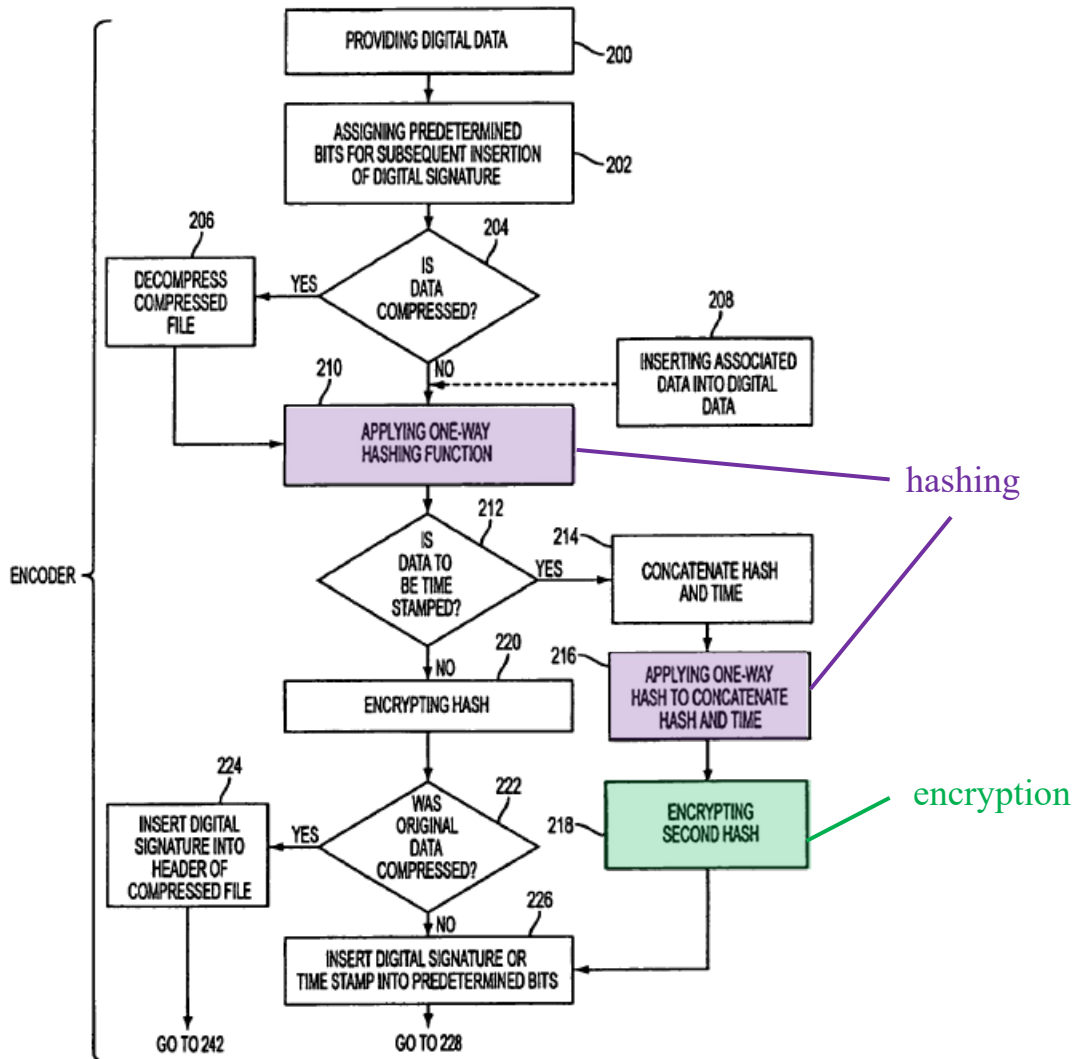
2. Summary of Cox

49. Like Vataja and the '998 patent, Cox describes techniques for hashing, encrypting, and signing captured media content. Cox “relates generally to methods and devices for inserting and authenticating a digital signature in digital data and, more particularly, encoders and decoders for inserting and authenticating a digital signature and associated data in digital image, video, and audio data.”

Cox, 1:8-12.

50. Cox describes performing a hashing operation on a “digital image (or alternatively, digital video or audio).” Cox, 5:34-35. Cox’s system “appl[ies] a one-way hashing function to the digital data ... resulting in a hash (or hash value).” Cox, 5:50-52. Cox also describes processing the “current time/date (time data) through another round of one-way hashing at step 216.” Cox, 8:17-18.

51. Cox also describes encrypting the hash values. The hash of the captured image “is then encrypted at step 220.” Cox, 5:53. The time stamp information “is then encrypted at step 218 using a public key encryption method.” Cox, 8:19-20. The hashing and encrypting steps are shown in Fig. 2A below.



Cox, Fig. 2A (annotated).

52. Cox also describes adding identifying information to the media file.

“The photographer’s name, say Adam, and public key may be placed in the clear in a field within the LSB’s of the image (digital data) that are also authenticated.”

Cox, 9:30-32.

53. Cox thus provides additional implementation details of known hashing and encrypting techniques.

3. Reasons to Combine Vataja and Cox.

54. A POSITA would have found it obvious for Vataja’s apparatus—which provides an encryption process—to utilize known encryption techniques such as those taught by Cox.

55. As an initial matter, both Vataja and Cox are analogous art to the ’998 patent. Like the ’998 patent, Vataja and Cox both relate to encrypting captured media. *See e.g.* Vataja, [0002] (“The invention disclosed broadly relates to methods for providing location-based content protection, and to encoding content with location-based authenticating data for secure distribution.”); Cox, 1:7-12 (“The present invention relates generally to methods and devices for inserting and authenticating a digital signature in digital data and, more particularly, encoders and decoders for inserting and authenticating a digital signature and associated data in digital image, video, and audio data.”). Vataja and Cox are also pertinent to the problem that is purportedly solved by the ’998 patent. The ’998 patent states that “it has become increasingly easy to copy, counterfeit, falsify and misuse digital information of all kinds.” Ex.1001, 2:30-32. Vataja and Cox address these concerns through the encryption and authentication techniques that they disclose. *See* Vataja, [0002], Cox, 1:7-12.

56. Vataja describes a multimedia capture device (e.g., a video camera)

that when media is captured, “time 103, location 104, and device 105 data may be incorporated as authentication data.” Vataja, [0013]. “Sample code of the content along with the authentication data. The system then secures the authentication data to the content through content encryption 107, metadata encryption 108, and/or a ‘hash’ encryption 109, each of which is well-known in the art.” Vataja, [0014]. Vataja explains that “Encryption algorithm 309 is provided to encrypt the information ... and may be further integrated into a Public Key Infrastructure (PKI) system. Through PKI, user public keys can be managed on a secure basis for distribution system.” Vataja, [0019]. Vataja further explains that “the public/private key arrangements may be implemented in various ways and combinations under the disclosure of the present invention to allow the encryption/decryption of data.” Vataja, [0019]. Accordingly, because Vataja explicitly encourages the use of known encryption techniques in the context of its system, a POSITA would have found it obvious to look to known encryption techniques for multimedia systems such as those described in Cox.

57. Cox describes known encryption techniques. Like Vataja and the ’998 patent, Cox “relates generally to methods and devices for inserting and authenticating a digital signature in digital data and, more particularly, encoders and decoders for inserting and authenticating a digital signature and associated data in digital image, video, and audio data.” Cox, 1:8-12.

58. In one example, Cox describes a multilevel encryption technique:

“Several levels of signing¹ are possible. This allows the image to be **signed by the camera** (indicating that the data has not been processed subsequent to its recording from the CCD array), **the photographer** (identifying the person responsible for the image), **the distributor**, etc.” Cox, 9:37-41. In this multilevel technique, “[t]he device encrypts the signature and/or time stamp using the camera’s private key.” Cox, 9:15-17. “Next this signature is encrypted using the photographer’s private key.” Cox, 9:32-36. The next iteration of encryption may then be performed using a distributor’s key. *See* Cox, 9:37-60.

59. A POSITA implementing Vataja’s encryption process would have been motivated to use Cox’s three-level encryption technique to sign the captured media. Indeed, Cox’s multilevel encryption technique provides various benefits. Cox explains that when an image is encrypted using only the camera’s key, “all that can be confirmed is that a specific camera captured the image” but the “viewer does not know who took the photograph.” Cox, 9:23-25. However, “this knowledge [who took the photograph] can also be provided by allowing the

¹ In Cox, “signing” refers to encryption: “**signing** (creating the digital signature by hashing and **encrypting**).” Cox, 2:62-63.

photographer (user) to program his/her camera (image generation device) with his/her name and public and private keys.” Cox, 9:27-29. Thus, the image encrypted with the camera’s key can then “encrypted using the photographer’s private key” as well—allowing authentication of the photographer. Cox, 9:35-36.

60. By encrypting the image with the photographer’s private key, anyone with the public key can “decrypt[] the signature using the photographer’s public key” and “determine the authenticity of the whole.” Cox, 10:44-50. A hypothetical impersonator “would also be aware of [the photographer’s] public key.” But without the “private key, it is impossible for him to correctly encrypt the signature. This is the great strength of public key encryption systems.” Cox, 11:1-2. Accordingly, a POSITA would have found it beneficial to implement Cox’s multi-level encryption technique into Vataja’s encryption process.

61. A POSITA would have had a reasonable expectation of success because Vataja’s camera provides the functionality required to perform Cox’s technique. Vataja’s camera includes “content combination 106” capabilities that receive time 103, location, 104, and device 105 data. *See* Vataja, Fig. 1, [0013]. Vataja’s camera also includes the functionality for “content encryption 107, metadata encryption 108, and/or a ‘hash’ encryption 109, each of which is well-known in the art.” Vataja, [0014]. As such, Vataja’s device is capable of performing the multi-level encryption techniques of Cox, which perform

encryption on both the image and the metadata (e.g., time and location data).

Indeed, Vataja explicitly encourages the use of these known encryption techniques, as noted above.

62. The results of the combination of Vataja and Cox would have been predictable because public key cryptography techniques referenced by both Vataja and Cox were well-known, standardized encryption techniques. *See* Vataja, [0019] (“Through PKI, user public keys can be managed on a secure basis for distribution systems (e.g., IETF X.509 standard).” Cox, 5:46-50 (“Any signing method known in the art can be used without departing from the scope or spirit of the present invention.”); *See* Ex.1008 (RFC defining the X.509 standard).

63. Accordingly, the combination of Vataja and Cox is merely the use of a known technique (Cox’s multi-level encryption) to improve similar methods (Vataja’s encryption process) in the same way. The combination is also applying a known technique (Cox’s multi-level encryption) to a known method (Vataja’s encryption process) ready for improvement to yield predictable results.

4. Claim 1

[1.0] *A method for interfacing with a device and acquiring information with the device from an environment external to the device to be transmitted to a receiving facility and for transmitting the acquired information thereto, comprising:*

64. To the extent the preamble is limiting, it is rendered obvious by

Vataja.

65. **First**, Vataja describes a “system and **method** for protecting multimedia content data” in which a “user creates content on a multimedia device” and thus interfaces with the device (a “*method for interfacing with a device*”).

Vataja, [0005].

66. **Second**, Vataja describes records visual or audio images.

The invention applies to **content-creating devices, such as digital cameras, digital video cameras, digital audio recording devices, and any other devices that allow a user to record visual or audio images, including text and other communicative indicia**. These devices may be stand-alone devices, or may be integrated into wireless telephone or PDA devices. FIG. 1 illustrates a system view of content authentication under an embodiment of the invention and how content data is gathered and encrypted. The content data is shown in the format of one or more of the following: photographic pictures 100, audio 101, and video 102. As the content is created alone, or in combination with other content, it is collectively transmitted to the content combination program 106. Time 103, location 104, and device 105 data is also sent to the content combination program 106. The time 103, location 104, and device 105 data may be incorporated as authentication data, provided from trusted sources. The

trusted source may be based on identification protocols
such as an identified content device and/or user.

Vataja, [0013].

67. These images or recordings may include “a wide spectrum of location based content, from wildlife pictures to news reporting and entertainment.” Vataja, [0024]. By recording images, video, or audio from the real world, Vataja’s device “*acquir[es] information with the device from an environment external to the device.*”

68. **Third**, Vataja explains that the captured media “file is then transmitted to a Content Certification Company (CCC) 110, or other distributor or Rights Management (RM) provider” (“*to be transmitted to a receiving facility and for transmitting the acquired information thereto*”). Vataja, [0014].

Once the content and authentication data is collected in the content combination program 106, the system will now have a sample code of the content along with the authentication data. The system then secures the authentication data to the content through content encryption 107, metadata encryption 108, and/or a “hash” encryption 109, each of which is well-known in the art.

Once an encrypted signature based on the authentication data 103, 104, and 105 is integrated into the content file, the file is then transmitted to a Content Certification Company (CCC) 110, or other

distributor or Rights Management (RM) provider. The integrated signature then identifies the content owner, along with the location and time in which the content was created. Once the provider 110 stores the content, it can subsequently be made available for trusted distribution.

Vataja, [0014].

69. “Once encrypted, the protected media file 307 is then sent to CCC 310, where it will be stored and subsequently transferred to a requesting retail site 312.” Vataja, [0018].

70. Thus, Vataja describes a method by which a user records image, video, or audio data from the real world using a digital video camera, and sending the recordings to a content certification company for storage, which renders obvious a “*method for interfacing with a device and acquiring information with the device from an environment external to the device to be transmitted to a receiving facility and for transmitting the acquired information thereto.*”

[1.1] *the device including a capture device and the capture device controlled to capture the information from the external environment where the information is selected from the group consisting of a video segment, a still image and an audio segment, each of which varies in real time in the external environment and relative to time in the external environment prior to capture by the capture device, and*

71. First, Vataja teaches a “*device including a capture device*” because it describes a “multimedia apparatus 303” with a “camera 305, or other multimedia

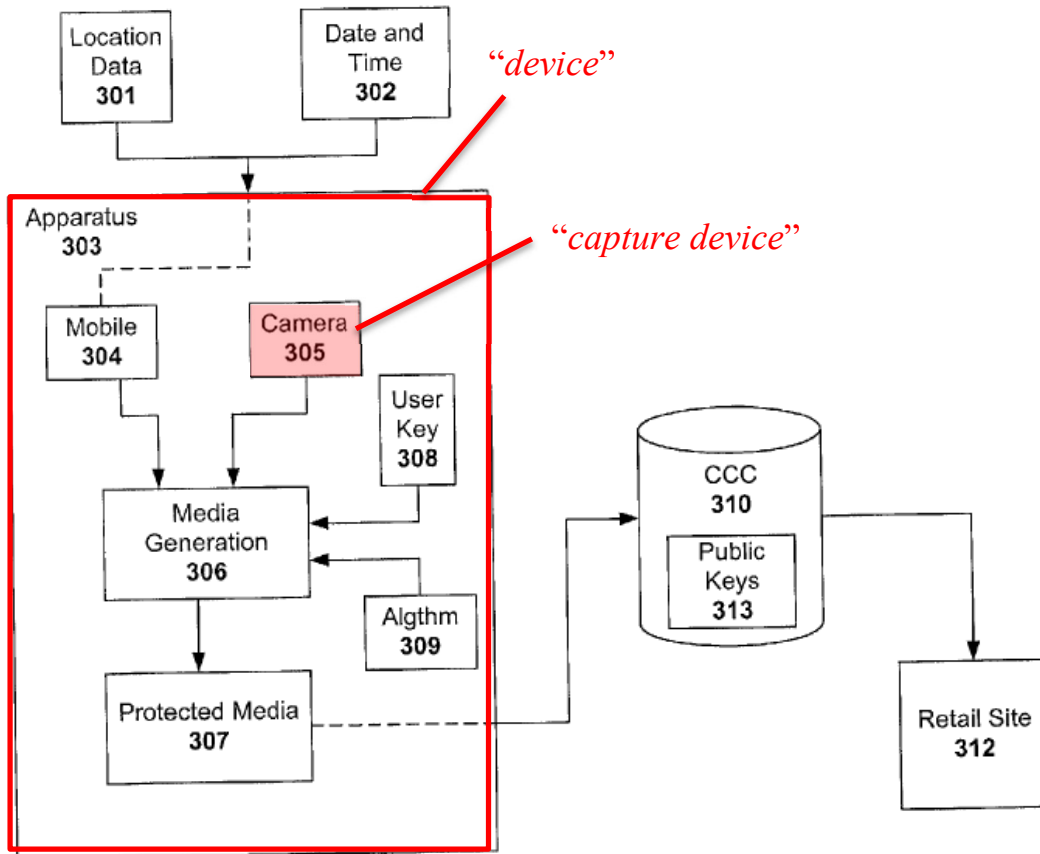
audio/visual (A/V) device.” Vataja, [0018].

Another embodiment of the present invention is shown in FIG. 3A. Location data 301 and the date and time 302 are transmitted to multimedia apparatus 303, and is sent to mobile portion or unit 304. The location data 301 and the date and time 302 may be generated from external sources (such as a GPS unit), or may be integrated as a single unit into apparatus 303, with internal location and date/time protocols. Camera 305, or other multimedia audio/visual (A/V) device, initiates the creation of a multimedia file (e.g., video, audio, etc.) that is subsequently transmitted to media generation portion 306 of apparatus 303. Media generation portion 306 algorithmically processes the data into a digital media format, such as JPEG, WAV, AVI, MPEG or other similar formats.

Vataja, [0018].

72. Indeed, Vataja’s “invention applies to content-creating devices, such as digital cameras, digital video cameras, digital audio recording devices, and any other devices that allow a user to record visual or audio images.” Vataja, [0013].

Vataja’s apparatus 303 (“*device*”) and camera 305 (“*capture device*”) are illustrated in Fig. 3A below.



Vataja, Fig. 3A (annotated).

73. **Second**, Vataja’s camera (“*capture device*”) is “*controlled to capture the information from the external environment*” because it “*initiates the creation of a multimedia file (e.g., video, audio, etc.)*.” Vataja, [0018]. These images or recordings may include “*a wide spectrum of location based content, from wildlife pictures to news reporting and entertainment*” and thus are recordings of the “*external environment.*” Vataja, [0024].

74. **Third**, Vataja’s camera records “*multimedia content data, such as photographs, video and audio*” and thus “*the information is selected from the group*

consisting of a video segment, a still image and an audio segment.” Vataja, [0005].

75. Fourth, Vataja’s video camera captures audio and video information from the real world (*“each of which varies in real time in the external environment and relative to time in the external environment prior to capture by the capture device”*).² The recordings may include “a wide spectrum of location based content, from wildlife pictures to news reporting and entertainment,” “accident photographs,” and “photographs taken at traffic intersections or speed traps.” Vataja, [0024].

76. It is generally understood by POSITAs that audio and video data is stored as time samples. *See e.g.,* Cox, 4:62-5:8 (*“each of the samples being defined by a plurality of bits, wherein the samples are pixels for image data, time samples for audio data, and spatial temporal samples for video data.”*). Moreover, it is generally understood that when taking a picture or video of something, that thing existed before its picture was taken (*“relative to time in the external environment prior to capture by the capture device”*). For example, if one were to record a video of a car passing through an intersection, it is understood that the car existed

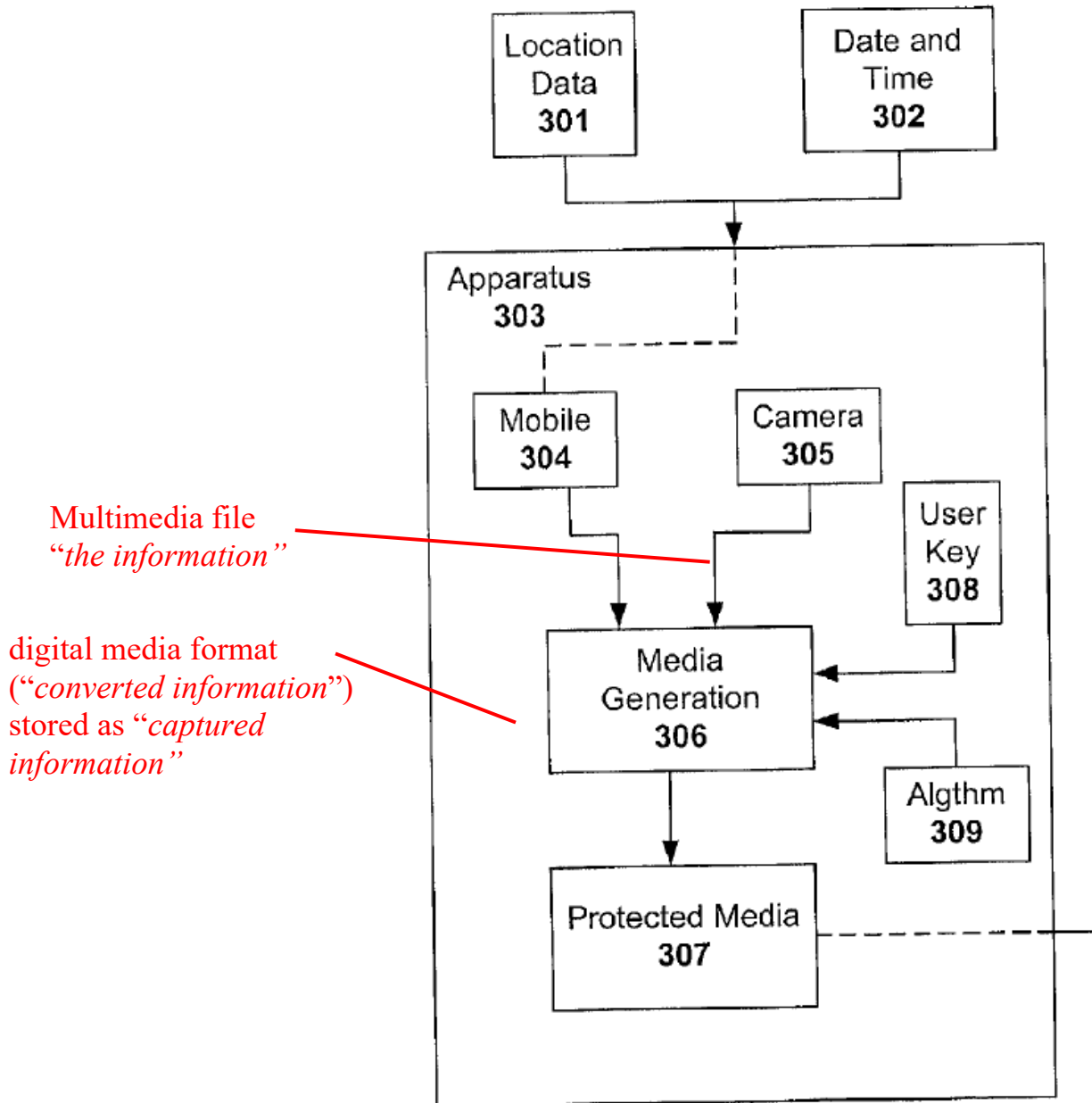
² I note that the prior art teaches this limitation at least under Patent Owner’s interpretation, which is that this limitation is met by “captur[ing] still image, video, and audio information from the surrounding environment.” Ex.1010 (Complaint).

in real time prior to being recorded with the video camera.

77. Thus, Vataja's device includes a camera or other capture device that records video, images, or audio from the real environment and thus renders obvious "*the device including a capture device and the capture device controlled to capture the information from the external environment where the information is selected from the group consisting of a video segment, a still image and an audio segment.*"

[1.2] converting the information to converted information for storage in a storage area as captured information;

78. First, Vataja's camera "*convert[s] the information to converted information*" because it "initiates the creation of a multimedia file (e.g., video, audio, etc.)" that is "algorithmically processe[d] ... into a digital media format, such as JPEG, WAV, AVI, MPEG or other similar format[]." Vataja, [0018]. Specifically, the multimedia file ("*the information*") "is subsequently transmitted to media generation portion 306 of apparatus 303" which "algorithmically processes the data into a digital media format" ("*converted information*"). Vataja, [0018].



Vataja, Fig. 3A (partial, annotated).

79. **Second**, to the extent it is not intended use, Vataja’s multimedia file is “for storage in a storage area as captured information.” Vataja explains that its apparatus includes “at least one storage medium for storing data.” Vataja, claim 14.

Because the digital media format file (e.g., JPEG, WAV, AVI, MPEG) represents recorded image, audio, or video data, it stored “*captured information*” as claimed.

80. Additionally, Vataja’s digital media format file is “*for storage in a storage area*” because after undergoing additional processes, it is ultimately stored at a remote storage facility: “Once encrypted, the protected media file 307 is then sent to CCC 310, where it will be stored.” Vataja, [0018].

81. Thus, because Vataja’s camera converts captured image, audio, or video data into a digital media format that is stored in a storage medium, Vataja renders obvious “*converting the information to converted information for storage in a storage area as captured information*.”

[1.3] controlling a device processor to create a file comprised of a representation of the captured information associated with a representation of the date and time of the capture of the information as augmented captured information, wherein the representation of the date and time information in association with the representation of the captured information forms the file containing the augmented captured information

82. First, Vataja’s media generation portion 306 performs hashing, encrypting, and signing processes and is thus a “*device processor*” itself or includes a “*device processor*” for performing such tasks. See Vataja, [0018]. Further, Vataja’s claims recite that encryption processes are performed by a processor: “a processor ...configured to ... execute an encryption algorithm.” Vataja, claim 39.

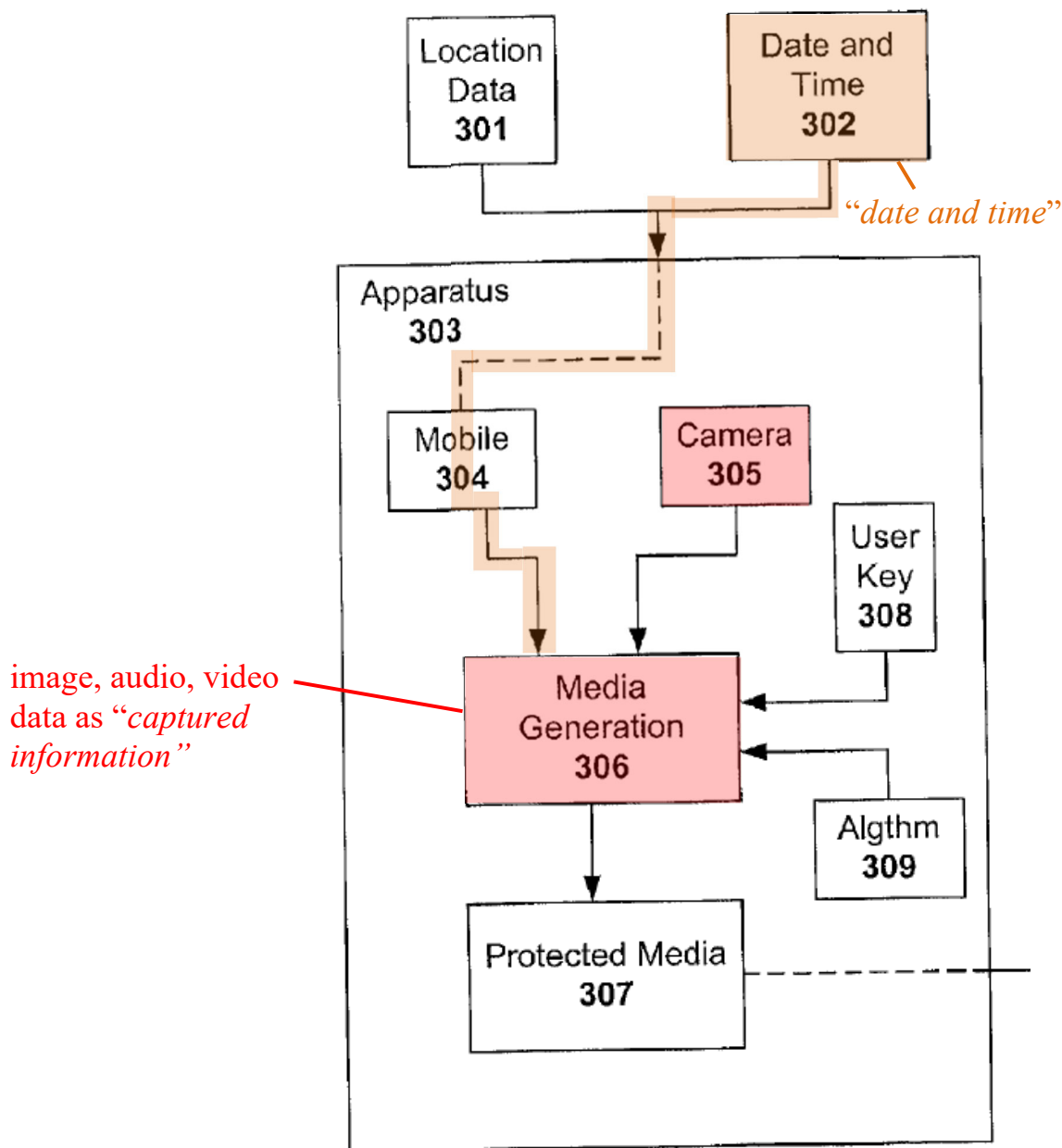
83. Second, Vataja's media generation portion 306 creates a media file that includes "date and time data 302," which teaches "*a file comprised of ... the captured information associated with ... the date and time of the capture of the information as augmented captured information.*" Vataja, [0018].

Another embodiment of the present invention is shown in FIG. 3A. Location data 301 and the date and time 302 are transmitted to multimedia apparatus 303, and is sent to mobile portion or unit 304. The location data 301 and the date and time 302 may be generated from external sources (such as a GPS unit), or may be integrated as a single unit into apparatus 303, with internal location and date/time protocols. Camera 305, or other multimedia audio/visual (A/V) device, initiates the creation of **a multimedia file (e.g., video, audio, etc.) that is subsequently transmitted to media generation portion 306 of apparatus 303. Media generation portion 306 algorithmically processes the data into a digital media format, such as JPEG, WAV, AVI, MPEG or other similar formats. At the same time the digital media is being formatted, mobile unit 304 prepares location data 301, date and time data 302, as well as IMEI, IMSI, Memory Card ID or other similar identification information to be encoded to media generation portion 306.** A user private key 308 may also be transmitted and encoded to the media for additional encryption protection.

An encrypting algorithm 309 utilizes the data from media generation portion 306 and then utilizes location data 301, date and time data 302, as well as identification information such as e.g. the IMEI and IMSI information to encrypt all the data collected in the media generation portion 306. Algorithm 309 may include a “hash” algorithm that is offered by the CCC. Once encrypted, the protected media file 307 is then sent to CCC 310, where it will be stored and subsequently transferred to a requesting retail site 312. CCC 313 may also contain user public keys 313 to decode any users keys 308 that are transmitted with the file.

Vataja, [0018].

84. Describing its invention more generally, Vataja explains that “[t]he time 103, location 104, and device 105 data may be incorporated as authentication data.” Vataja, [0013]. The date and time data 302 is shown being combined with the captured information from the camera in Fig. 3A below.



Vataja, Fig. 3A (partial, annotated).

See also Vataja, Fig. 1 (illustrating time and date information 103 being combined with photo 100, audio 101, or video 102 information).

85. Third, Vataja’s media generation portion 306 creates a

“representation of the captured information” and a *“representation of the time and date information”* by performing a hash function to create a hash value. Vataja, [0018]. The “hash” of the captured data and time and date data is a *“representation”* of that data consistent with how the ’998 patent uses the term *“representation.”* The ’998 patent states that “the document 130, in its encrypted form, is converted to a ‘hash’ file and this hash file, which is a **representation** of the encrypted file...” Ex.1001, 5:34-36. “Hashing refers to a practice of creating a short dataset that **represents** a larger dataset.” Ex.1001, 9:24-26.

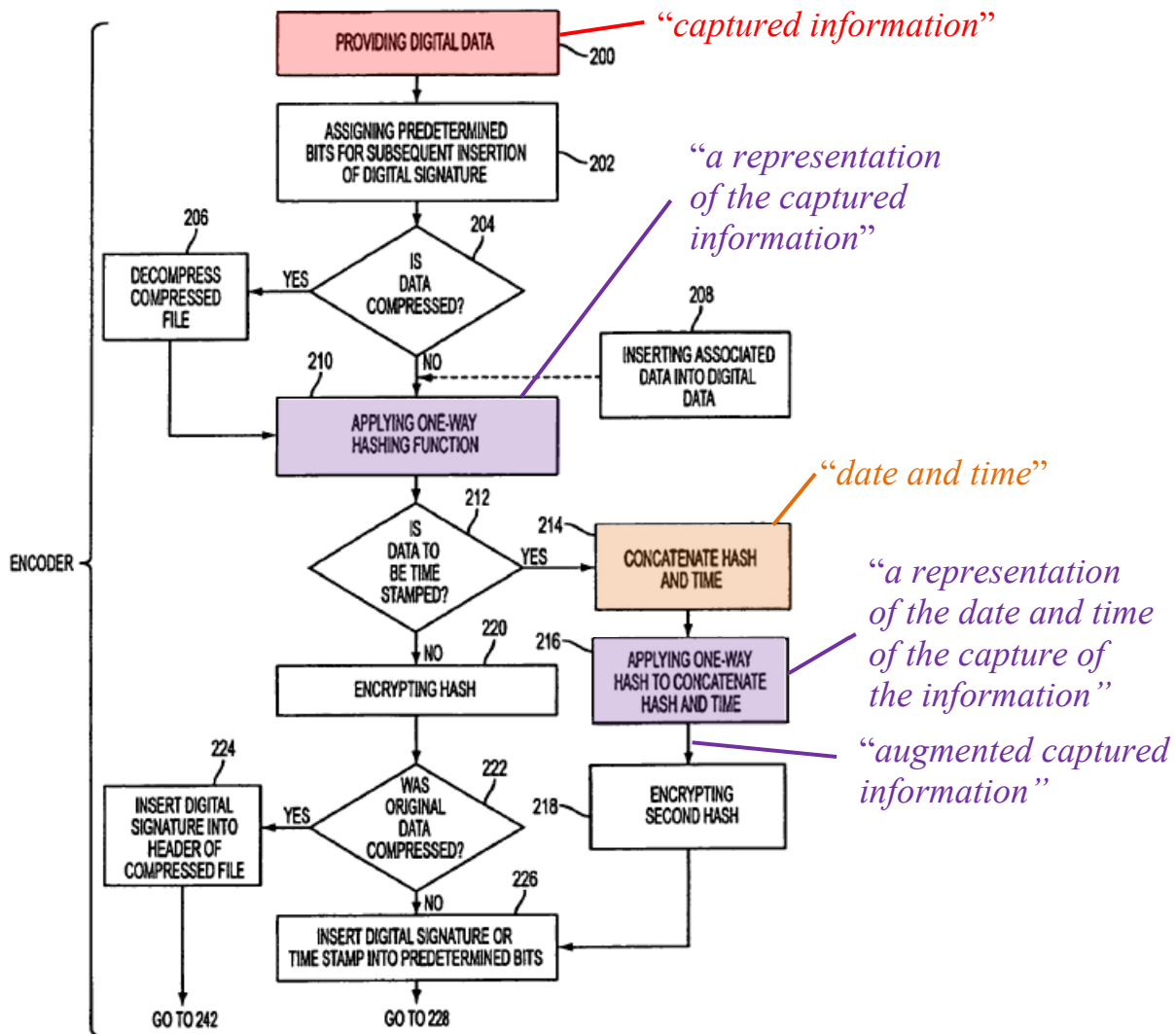
86. Vataja explains that “[a]n encrypting algorithm 309 utilizes the data from media generation portion 306 and then utilizes ... date and time data 302 ... to encrypt all the data collected in the media generation portion 306.” Vataja, [0018]. The encryption “[a]lgorithm 309 may include **a ‘hash’ algorithm**.” Vataja, [0018]. Referring to its invention more generally, Vataja states that “[t]he system then secures the authentication data to the content through content encryption 107, metadata encryption 108, **and/or a ‘hash’ encryption 109**, each of which is well-known in the art.” Vataja, [0014]. Vataja thus generally describes using well-known encryption techniques that utilize hash functions.

87. A POSITA would have thus found it obvious for Vataja’s encryption and hashing techniques to be implemented according to the well-known techniques in the art. Cox provides an example technique for hashing and encrypting and

specifically teaches hashing captured data (e.g., image, audio, or video) as well as hashing time and date data. *See generally* Cox.

88. In particular, Cox describes “*captured information*” in the form of “digital data” that “defines the digital image (or alternatively, digital video or audio).” Cox, 5:34-35. Cox then describes “applying a one-way hashing function to the digital data ... resulting in a hash (or hash value). This is shown at step 210.” Cox, 5:49-51. Cox’s hash value is thus “*a representation of the captured information.*”

89. Cox additionally describes concatenating time/date data and hashing the concatenated time/date data, which teaches “*a representation of the date and time of the capture of the information.*” “If the digital data is to be time stamped (step 212, Yes Decision), the [concatenated hash] and the current time/date (time data)” are passed “through another round of one-way hashing at step 216.” Cox, 8:13-18. Creating a hash of the captured information and time and date information is illustrated below in Fig. 2A below.



Cox, Fig. 2A (annotated).

90. Accordingly, Vataja’s media generation portion 306—performing well-known hashing/encrypting techniques such as those described by Cox—creates a hash (“representation”) of both the captured information and the time and date information.

91. **Fourth**, because Vataja’s media generation portion 306 operates on a media “file,” to perform the hash function, the result of the hash is similarly a file

that comprises/contains the augmented captured information along with the captured media itself.

92. Vataja thus teaches “**a file comprised of** a representation of the captured information associated with a representation of the date and time of the capture of the information **as augmented captured information.**” For similar reasons, Vataja and Cox teach the similarly recited “wherein the representation of the date and time information in association with the representation of the captured information **forms the file containing the augmented captured information.**”

93. Thus, because Vataja describes creating a file through a process that involves hashing and encrypting time and location data, and Cox provides implementation examples of hashing time and location data before encrypting, Cox and Vataja render obvious “controlling a device processor to create a file comprised of a representation of the captured information associated with a representation of the date and time of the capture of the information as augmented captured information.”

[1.4] controlling an encryptor on the device processor to encrypt the augmented captured information as an encrypted file containing encrypted augmented captured information,

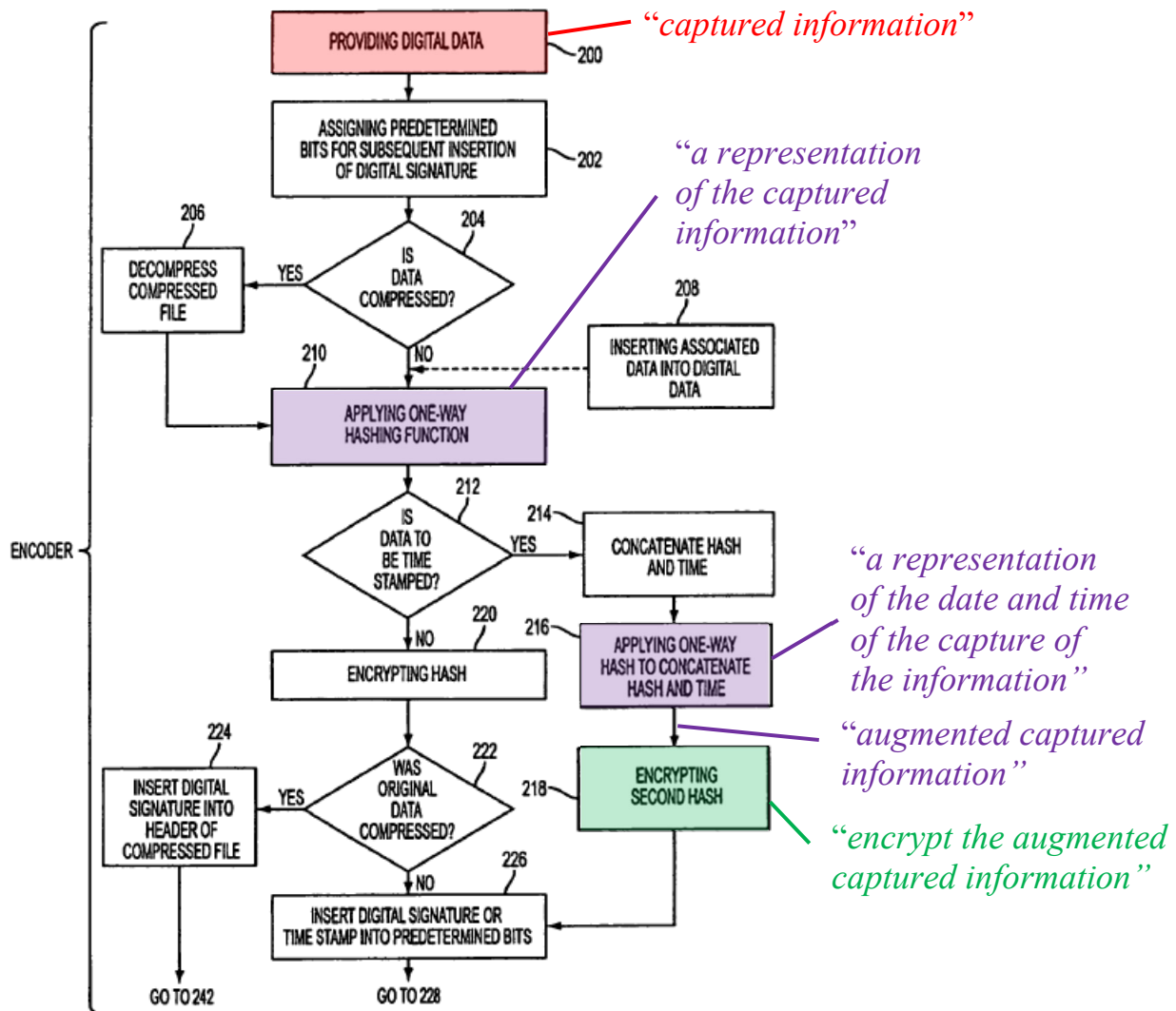
94. First, Vataja’s multimedia apparatus includes an encryption algorithm 309 (“an encryptor”) that “utilizes the data from media generation portion 306 ...

to encrypt all the data collected in the media generation portion 306.” Vataja, [0018].

An encrypting algorithm 309 utilizes the data from media generation portion 306 and then utilizes location data 301, date and time data 302, as well as identification information such as e.g. the IMEI and IMSI information to encrypt all the data collected in the media generation portion 306. Algorithm 309 may include a “hash” algorithm that is offered by the CCC. Once encrypted, the protected media file 307 is then sent to CCC 310, where it will be stored and subsequently transferred to a requesting retail site 312. CCC 313 may also contain user public keys 313 to decode any users keys 308 that are transmitted with the file.

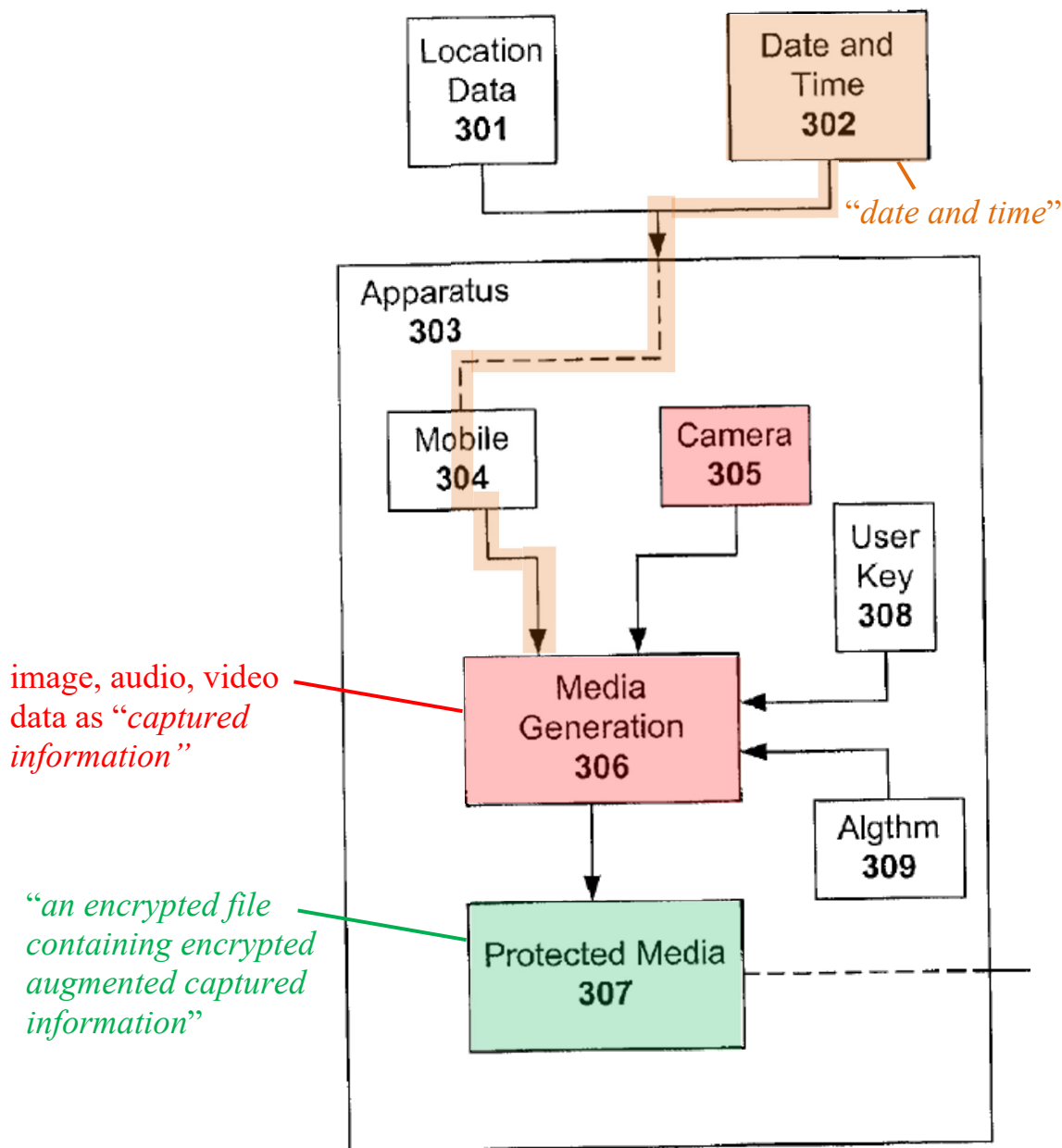
Vataja, [0018].

95. Second, Vataja’s media generation portion 306 and encryption algorithm 309—implemented according to Cox’s teachings—encrypt the concatenated hash results (“*augmented captured information*”). “This hash is then encrypted at step 218 using a public key encryption method.” Cox, 8:18-20.



Cox, Fig. 2A (annotated).

96. The output of the encryption process creates a protected media file 307 (“an encrypted file containing encrypted augmented captured information”). “Media generation portion 306 algorithmically processes the data into a digital media format, such as JPEG, WAV, AVI, MPEG or other similar formats.” Vataja, [0018]. “Once encrypted, the protected media file 307 is then ...” Vataja, [0018].



Vataja, Fig. 3A (partial, annotated).

97. Thus, Vataja’s apparatus, implementing the teachings of Cox, uses an encryption algorithm to encrypt the hashed media and time stamp data to create a protected media file, which renders obvious “controlling an encryptor on the

device processor to encrypt the augmented captured information as an encrypted file containing encrypted augmented captured information.”

[1.5] controlling the device processor to initiate a signing operation for adding signature information to the file including the encrypted augmented captured information to provide an identifiable encrypted file,

98. Vataja and Cox teach “*a signing operation for adding signature information to the file*” as claimed. Notably, the claimed signing operation does not refer to an encryption process as sometimes used in the art. Rather, the claimed signing operation merely adds “*signature information*” that remains “*unencrypted signature information*” that “*allows identification of the party claiming to have created the captured information*” as will be discussed in further detail below at [1.6] and [1.7].

99. First, as explained above at [1.3], Vataja’s functions are performed by a processor (“*controlling the device processor*”).

100. Second, it would have been obvious for Vataja’s identification information to include a photographer’s name and/or public key as taught by Cox. Vataja explains that “identification information such as e.g. the IMEI and IMSI” is added to the protected media file 307. Vataja, [0018]. Cox describes a process by which a photographer’s name and public key (“*signature information*”) may be added to the image data:

In an alternative version of the methods of the prior art, this knowledge can also be provided by allowing the photographer (user) to program his/her camera (image generation device) with his/her name and public and private keys. **The photographer's name, say Adam, and public key may be placed in the clear in a field within the LSB's of the image (digital data) that are also authenticated.** The image, together with all the LSB's except those that are used to store the signature are then first signed by the camera using its private key. Next this signature is encrypted using the photographer's private key.

Cox, 9:26-36.

101. Accordingly, it would have been obvious to similarly add the photographer's name and public key to Vataja's protected media file 307 (*"the file including the encrypted augmented captured information"*). Because the user's name and public key (which identify the photographer) are placed within the image, the image file becomes an *"identifiable encrypted file"* as claimed.

102. Thus, because Vataja describes adding identification information to the protected media file, which may be the user's name and public key as described by Cox, Vataja and Cox render obvious *"controlling the device processor to initiate a signing operation for adding signature information to the file including the encrypted augmented captured information to provide an identifiable encrypted*

file.”

[1.6] *wherein the signature information provides information to the receiving facility that allows identification of the party claiming to have created the captured information for later identification of the party,*

103. First, consistent with the discussion above at [1.5], Cox teaches that the user may place his or her name and public key within the file as signature information.

104. Second, Vataja teaches that the CCC (“*receiving facility*”) may use such signature information to identify a user. “Once an encrypted signature based on the authentication data 103, 104, and 105 is integrated into the content file, the file is then transmitted to a Content Certification Company (CCC) 110 ... The integrated signature then identifies the content owner, along with the location and time in which the content was created.” Vataja, [0014]. That signature information may include the photographer’s name as described by Cox. Cox, 9:30-32. The signature information thus “*allows identification of the party claiming to have created the captured information for later identification of the party.*”

105. Thus, because Vataja teaches that the CCC receiving the protected media file uses the signature information to identify the content owner, and that signature information may include the photographer’s name as described by Cox, Vataja and Cox render obvious “*wherein the signature information provides information to the receiving facility that allows identification of the party claiming*

to have created the captured information for later identification of the party.”

[1.7] controlling the device processor to place the identifiable encrypted file including both the encrypted augmented captured information and the unencrypted signature information in association with subscriber information

106. First, as shown above at [1.5], Vataja and Cox teach signing and encrypting operations in which the protected media file 307 includes encrypted hashes (“*the encrypted augmented captured information*”) and the user’s name and public key (“*signature information*”).

107. Second, Cox explains that the signature information “may be placed in the clear.” Cox, 9:30-31. Because the information is in the clear, it is “*unencrypted signature information*” as claimed. Cox, 6:55-56 (“The content owner may choose to leave some of this information in the **clear, i.e. unencrypted** while other fields may be encoded.”).

108. Third, Vataja explains that a user’s International Mobile Subscriber Identifier (IMSI) (“*subscriber information*”) may be added to the protected media file. “At the same time the digital media is being formatted, mobile unit 304 prepares location data 301, date and time data 302, as well as IMEI, **IMSI**, Memory Card ID or other similar identification information to be encoded to media generation portion 306.” Vataja, [0018]. Because the IMSI becomes part of the protected media file 307, the information in the protected media file such as the hashed date and time (“*encrypted augmented captured information*”) is “in

association with” the IMSI.

109. Thus, because Vataja’s protected media file includes an IMSI, along with the encrypted hashes of the captured image and date and time, Vataja renders obvious “controlling the device processor to place the identifiable encrypted file including both the encrypted augmented captured information and the unencrypted signature information in association with subscriber information.”

[1.8] as a transmission file for transmission to a receiving facility requiring the subscriber information, the subscriber information required at the receiving facility for a lookup operation to obtain additional information to allow further processing of the augmented captured information at the receiving facility;

110. First, the protected media file 307 is transmitted to the CCC and thus becomes “a transmission file for transmission to a receiving facility.” “Once encrypted, the protected media file 307 is then sent to CCC 310, where it will be stored.” Vataja, [0018].

111. Second, the CCC (“receiving facility”) uses the IMSI for identification of the user as a subscriber and thus the CCC “require[es] the subscriber information.” “A CCC may be set up so that each user sending multimedia data must be pre-registered **as a subscriber**. Under this embodiment, the CCC confirm’s [sic] the user as a subscriber 504, either through a password, or through automatic identification of the user’s IMEI/**IMSI**.” Vataja, [0021].

112. Third, Vataja explains that upon receipt, the CCC obtains “additional

information” in the form of the user keys transmitted with the file. “CCC 313 may also contain user public keys 313 to decode any user keys 308 that are transmitted with the file.” Vataja, [0018]. The process of matching the appropriate public keys to 313 to the transmitted media file is “*a lookup operation*.” Because the public keys are used to decode the encrypted media file 307, Vataja thus teaches “*a lookup operation to obtain additional information to allow further processing of the augmented captured information at the receiving facility*.” Notably, Vataja describes the lookup operation at the same level of specificity as the ’998 patent: “The storage facility can look up the public key of the party claiming to be the author of the file.” ’998 patent, 19:1-7.

113. Decrypting the user keys (“*additional information*”) allows for further processing of the protected media file for distribution. “Once the provider 110 stores the content, it can subsequently be made available for trusted distribution.” Vataja, [0014]. After decrypting the file, the “CCC would then run encoding algorithm 505 to protect the content under a location-based content protection (LBCP) protocol. Once encoded, the protected media would be ready for secure transmission and distribution to requesting users.” Vataja, [0021].

114. Thus, because Vataja’s protected media file, which includes the IMSI, is transmitted to the CCC which then obtains the matching public keys to decode the private key encrypted media file, Vataja renders obvious “*as a transmission file*

for transmission to a receiving facility requiring the subscriber information, the subscriber information required at the receiving facility for a lookup operation to obtain additional information to allow further processing of the augmented captured information at the receiving facility.”

[1.9] controlling a transmitter on the device for transmitting the transmission file to the receiving facility in order to further process the augmented captured information at the receiving facility; and

115. First, Vataja’s device includes a “*transmitter*” at least because it is connected through “a digital wireless wide area network (WAN), based on architectures such as Global System for Mobile Communication (GSM), IS-136 TDMA-based Digital Advanced Mobile Phone Services (DAMPS).” Vataja, [0015]. Vataja also explains that connections may be made using Bluetooth or 802.11 (i.e., Wifi). Vataja, [0013]; *see also* Vataja, Fig. 5 (illustrating the step of **transmitting** content to the CCC). It also would have been obvious for Vataja’s device to use wired connections as described by Cox. Cox, 9:11-12 (describing a “cable interface 412 connected to the personal computer 408.”).

116. Second, Vataja’s device transmits the protected media file to the CCC (“*receiving facility*”). “Once encrypted, the protected media file 307 is then sent to CCC 310.” Vataja, [0018]. “Once an encrypted signature based on the authentication data 103, 104, and 105 is integrated into the content file, **the file is then transmitted** to a Content Certification Company (CCC) 110.” Vataja, [0014].

117. Third, as explained above at [1.8], Vataja teaches “*further processing of the augmented captured information at the receiving facility*,” which happens after the CCC receives the protected media file. Accordingly, the file is transmitted “*in order to further process*” the file.

118. Thus, because Vataja’s apparatus transmits the protected media file to the CCC for further processing, Vataja renders obvious “*controlling a transmitter on the device for transmitting the transmission file to the receiving facility in order to further process the augmented captured information at the receiving facility*.”

[1.10] receiving the transmission file and accepting the identifiable encrypted file after verification of the subscriber information.

119. First, as explained above at [1.9], the protected media file is transmitted to the CCC and thus the CCC “*receiv[es] the transmission file*.”

120. Second, the CCC accepts the protected media file 307 (“identifiable encrypted file”) after verification: “Under this embodiment, the CCC confirm's the user as a **subscriber 504**, either through a password, or through automatic identification of the user's IMEI/**IMSI**.” Vataja, [0021]. “Also, the CCC could be configured to **accept** only certified user apparatus and application data, so that fraudulent location/content combinations would not be accepted.” Vataja, [0023].

121. Thus, because the CCC accepts the protected media file after verifying the user as a subscriber, Vataja renders obvious “*receiving the*

transmission file and accepting the identifiable encrypted file after verification of the subscriber information.”

5. Claim 2

[2.1] *The method of claim 1, wherein the step of controlling the device processor to create a file associates the captured information with a representation of location information representing the location of the capture device at the completion of the time of the capture of the information as augmented captured information.*

122. First, as explained above at [1.3], Vataja and Cox teach creating a file that includes a hash of (“*representation of*”) time and date data along with the image data (“*captured information*”).

123. Second, Vataja and Cox also teach that the file may include a hash of location data (“*a representation of location information*”). In Vataja, “**location data 301** and the date and time 302 are transmitted to multimedia apparatus 303.” Vataja, [0018]. “At the same time the digital media is being formatted, mobile unit 304 prepares **location data 301**, date and time data 302, ... to be encoded to media generation portion 306.” Vataja, [0018]. “An encrypting algorithm 309 utilizes the data from media generation portion 306 and then utilizes **location data 301**, ... to encrypt all the data collected in the media generation portion 306.” Vataja, [0018]. Accordingly, Vataja describes adding location data along with the time and date data to the protected media file 307.

124. Third, Cox describes “inserting time data into the digital data **for**

identifying the time the digital data was created.” Cox, 8:8-10. This time data

includes location data: “A further refinement of this system is to time stamp the image with both time **and place** of the image generation device.” Cox, 3:15-20.

Accordingly, Vataja and Cox teach adding location information “*representing the location of the capture device at the completion of the time of the capture of the information.*”

125. Thus, because Vataja and Cox describe creating a hash of time stamp data, along with location data at the time and place of capture, Vataja and Cox render obvious “*wherein the step of controlling the device processor to create a file associates the captured information with a representation of location information representing the location of the capture device at the completion of the time of the capture of the information as augmented captured information.*”

6. Claim 3

[3.1] The method of claim 1, wherein the processor includes a geographical position and time-of-day determination (GPS) receiver for providing such location information.

126. Vataja explains that “ “[t]he location data 301 and the date and time 302 may be generated from external sources (such as **a GPS unit**), or may be integrated as a single unit into apparatus 303, **with internal location and date/time protocols.**” Vataja, [0018]; *see also* Vataja, [0013] (“The location data includes Global Positioning System (GPS) coordinates.”).

127. Thus, because Vataja's location data may be obtained using a GPS integrated with date/time protocols, Vataja renders obvious "*wherein the processor includes a geographical position and time-of-day determination (GPS) receiver for providing such location information.*"

7. Claim 14

[14.0] *A method for acquiring information with a device from an environment external to the device to be transmitted to a receiving facility and for transmitting the acquired information thereto, comprising:*

128. See [1.0].

[14.1] *the device including a capture device for capturing the information from the external environment where the information is selected from the group consisting of a video segment, a still image and an audio segment, each of which varies in real time in the external environment and relative to time in the external environment prior to capture by the capture device, and*

129. See [1.1].

[14.2] *converting the information to converted information for storage in a storage area as captured information;*

130. See [1.2].

[14.3] *creating a file comprised of the captured information associated with a representation of the date and time of the capture of the information as augmented captured information, wherein the representation of the date and time information in association with the captured information forms the file containing the augmented captured information;*

131. See [1.3].

[14.4] *encrypting with an encryptor the augmented captured information as an encrypted file containing encrypted augmented captured information,*

132. See [1.4].

[14.5] *in a signing operation, adding signature information to the file including the encrypted augmented captured information to provide an identifiable encrypted file,*

133. See [1.5].

[14.6] *wherein the signature information provides information to the receiving facility that allows identification of the party claiming to have created the captured information for later identification of the party,*

134. See [1.6].

[14.7] *placing the identifiable encrypted file including both the encrypted augmented captured information and the unencrypted signature information in a transmission file for transmission to a receiving facility;*

135. See [1.7]-[1.8].

[14.8] *transmitting with a transmitter the transmission file to the receiving facility in order to further process the augmented captured information at the receiving facility; and*

136. See [1.9].

[14.9] *receiving at the receiving facility the transmission file and accepting the identifiable encrypted file and identifying the encrypted file with the signature information for processing of the encrypted file without removing the encryption therefrom.*

137. First, for the reasons explained above at [1.10], Vataja and Cox render obvious “*receiving at the receiving facility the transmission file and accepting the identifiable encrypted file.*”

138. Second, because the signature information is placed “in the clear” as described above at [1.5]-[1.7], the receiving facility is able to identify the file without having to decode the file (“*identifying the encrypted file with the signature*

information ... without removing the encryption therefrom.”

139. Third, for the reasons explained above at [1.9], the media file is sent to the receiving facility *“for processing of the encrypted file.”*

B. Ground 2: Claims 4-13 are obvious in view of Vataja, Cox, and Hershey.

1. Summary of Hershey

140. Like Vataja, Cox, and the '998 patent, Hershey relates to “a digital camera that generates meta-data related to an electro-optical image and steganographically combines the meta-data and the image. This camera can ... and hash or encrypt the acquired meta-data before performing the data combining.” Hershey, 2:20-26. The encrypted data can then be transmitted “to remote locations.” Hershey, 2:24-25.

141. In particular, Hershey explains that when encrypting metadata, “[e]ither symmetrical encryption techniques or asymmetrical encryption techniques can be used.” Hershey, 8:30-32. When using symmetrical encryption, the metadata is “encrypted with a private key so that only the holder or holders of the private key can decrypt the meta-data.” Hershey, 8:20-22. When encrypting with asymmetrical encryption, “the meta-data or hashed meta-data, can be encrypted using a public key so that accessors of the encrypted meta-data, or hashed meta-data, having the corresponding second key of the public key pair can decrypt, but

not successfully alter, the encrypted data.” Hershey, 8:22-27.

142. Hershey thus provides evidence that it was known to use either symmetrical or asymmetrical encryption techniques when encrypting media data for transfer to a remote site.

2. Reasons to Combine Hershey with Vataja and Cox

143. A POSITA would have found it obvious to use either symmetrical or asymmetrical encryption for certain levels of the Vataja/Cox multilevel encryption techniques, as taught by Hershey. *See* Hershey, 8:30-32

144. As an initial matter, Hershey is analogous art to the ’998 patent. Hershey relates to the same field of endeavor, namely protecting media files. *See* Hershey, abstract (“An electronic device, such as a digital camera, includes sensors to acquire subject data, such as ... date and time”); *see also* Hershey, 2:25 (describing “hash[ing] or encrypt[ing] the acquired meta-data.”). Hershey also seeks to solve the same technical problem that the ’998 patent purports to solve. Hershey states that a “need, therefore, exists for electronic devices that acquire subject, or cover, data to also acquire meta-data corresponding with the subject data and to associate the subject data and the meta-data in an error-free and efficient manner that reduces the resources needed for the storage and management of the subject data.” Hershey, 1:52-58; *compare with* Ex.1001, 2:41-46 (“An attendant problem is that of secure storage. While a flash memory card within

these digital recording devices (in any of its currently popular forms) can hold hundreds of pictures, images, video and audio, the problem with securely storing, indexing and retrieving thousands of media files has still not been solved.”).

145. As described above at VIII.B.3, it would have been obvious to implement Vataja’s encryption process according to Cox’s multilevel encryption technique. Cox’s multilevel encryption technique includes a first level for the camera, a second level for the photographer, and a third level for the distributor. *See* Cox, 9:37-41. Cox explains that the encryption technique for the photographer uses public and private keys, thus indicating an asymmetrical encryption technique. For the camera layer, Cox mentions only a private key, thus suggesting a symmetrical encryption technique. Cox, 9:35-36; *See also infra*, V.A. Cox is also silent as to the type of encryption used for the third layer (e.g., a distributor). Cox, 9:37-41. A POSITA would have thus found it obvious to look to known encryption options the third layer (distributor layer).

146. Hershey explains that in the context of encrypting image metadata, “[e]ither symmetrical encryption techniques or asymmetrical encryption techniques can be used.” Hershey, 8:30-32. When using asymmetrical encryption, metadata “can be encrypted using a public key so that accessors of the encrypted meta-data, or hashed meta-data, having the corresponding second key of the public key pair can decrypt, but not successfully alter, the encrypted data.” Hershey, 8:23-27.

Indeed, Vataja explains that “public/private key arrangements may be implemented in various ways and combinations under the disclosure of the present invention to allow the encryption/decryption of data.” Vataja, [0019].

147. Accordingly, a POSITA would have found it beneficial that when sending a protected media file to a distributor, such as Vataja’s CCC, one would seek to use the public key of the CCC for encryption of the final layer. Indeed, Vataja describes using an encryption algorithm from the CCC. Vataja, [0018]. That way, if the file were to be intercepted in transit, it could not be decrypted without the CCC’s private key. Only the CCC—the intended recipient—may decrypt the file.

148. A POSITA would have had a reasonable expectation of success because Vataja suggests that known public key techniques can be used in various ways: “It is understood that the public/private key arrangements may be implemented in various ways and combinations under the disclosure of the present invention to allow the encryption/decryption of data.” Vataja, [0019]. Such known public/private key arrangements include Hershey’s technique of encrypting the data with a public encryption key. *See* Hershey, Hershey, 8:30-32. And because such techniques were known and standardized (e.g., IETF RFC 2437), using them would have been predictable. *See* Ex.1009.

149. Additionally, Hershey is representative of the background knowledge

of a POSITA with respect to symmetrical/asymmetrical encryption. A POSITA would have recognized that encrypting and decrypting with the same key is a symmetrical encryption technique. *See* Hershey, 8:18-22. And decrypting with a different key than what was used for encryption (e.g., public/private keys) is an asymmetrical encryption technique. *See* Hershey, 8:23-27.

150. Accordingly, the combination of Hershey with Vataja and Cox is merely the use of a known technique (Hershey's asymmetrical encryption with a public key) to improve similar methods (the Vataja/Cox encryption process) in the same way. The combination is also applying a known technique (Hershey's symmetrical/asymmetrical encryption techniques) to a known method (Vataja's encryption process) ready for improvement to yield predictable results.

3. Claim 4

[4.1] *The method of claim 1, wherein the step of controlling the encryptor encrypts the augmented captured information with a symmetrical encryption algorithm in a first layer to provide the encrypted augmented captured information which is included in the transmission with the signature information and the subscriber information transmitted by the step of controlling the transmitter.*

151. First, for the reasons described above at [1.4], Vataja and Cox teach “the step of controlling the encryptor encrypts the augmented captured information.”

152. Second, Cox explains that the encryption process may be a multilevel

encryption process—at least one level for the camera and one level for the photographer: “The image, together with all the LSB’s except those that are used to store the signature are then **first signed by the camera using its private key.** Next this signature is encrypted **using the photographer’s private key.**” Cox, 9:32-36. “Several levels of signing are possible. This allows the image to be signed by the camera (indicating that the data has not been processed subsequent to its recording from the CCD array), the photographer (identifying the person responsible for the image), the distributor, etc..” Cox, 9:37-41. Accordingly, encryption with the *camera’s* private key is encryption “*in a first layer*” as claimed.

153. Third, it would have been obvious for encryption with the camera’s private key to be a symmetrical encryption process as taught by Hershey. As explained above at Section V, symmetrical encryption techniques use the same key for encryption as for decryption. Cox describes only a single private key for the camera layer encryption, thus indicating a symmetrical encryption technique. And Hershey explains that when encrypting hash values or other metadata for a captured image, “[e]ither symmetrical encryption techniques or asymmetrical encryption techniques can be used.” Hershey, 8:31-33. Accordingly, Cox alone and also considering the background knowledge of a POSITA—as well as Cox in combination with Hershey—teach “*a symmetrical encryption algorithm.*”

154. Fourth, for the reasons explained above at [1.7]-[1.9], Vataja and Cox teach “*provide the encrypted augmented captured information which is included in the transmission with the signature information and the subscriber information transmitted by the step of controlling the transmitter*” as claimed.

155. Thus, because Vataja and Cox describe an encryption process that may involve multiple levels, including one level using the camera’s private key, which is a symmetrical encryption process as evidenced by Hershey, Vataja, Cox and Hershey render obvious “*wherein the step of controlling the encryptor encrypts the augmented captured information with a symmetrical encryption algorithm in a first layer to provide the encrypted augmented captured information which is included in the transmission with the signature information and the subscriber information transmitted by the step of controlling the transmitter.*”

4. Claim 5

[5.1] *The method of claim 4, and wherein the step of controlling the encryptor further encrypts the first layer encrypted augmented captured information with a second layer of encryption utilizing an asymmetrical encryption algorithm to provide a two layer encrypted file, which two layered encrypted file has the signature information added thereto to provide the identifiable encrypted file.*

156. First, for the reasons explained at [4.1], Vataja and Cox teach encrypting the augmented captured information first with the camera’s private key (“*the first layer encrypted augmented captured information.*”).

157. Second, consistent with the discussion above at [4.1], Cox’s

encryption “using the **photographer’s** private key” teaches encrypting “*with a second layer of encryption.*” Cox, 9:35-36.

158. Third, Cox explains that the encryption using the photographer’s private key has a corresponding public key and is thus “*an asymmetrical encryption algorithm.*” Cox’s system allows “the photographer (user) to program his/her camera (image generation device) with his/her name and **public and private keys**. The photographer’s name, say Adam, and public key may be placed in the clear.” Cox, 9:27-31. Because the photographer encryption layer uses public and private keys, it is an asymmetrical encryption technique. See Hershey, 8:23-26; *supra* V. With this second level of encryption, a “*two layer encrypted file*” is produced.

159. Fourth, for the reasons explained above at [1.5]-[1.6], Vataja and Cox teach “*which two layered encrypted file has the signature information added thereto to provide the identifiable encrypted file*” as claimed.

160. Thus, because Cox describes a second encryption layer in which the photographer’s key is used to encrypt the previously encrypted file using a public/private key technique, Cox renders obvious “*wherein the step of controlling the encryptor further encrypts the first layer encrypted augmented captured information with a second layer of encryption utilizing an asymmetrical encryption algorithm to provide a two layer encrypted file, which two layered encrypted file*

has the signature information added thereto to provide the identifiable encrypted file.”

5. Claim 6

[6.1] *The method of claim 5, wherein the asymmetrical encryption algorithm utilizes a public key for encryption and a private key is required for decryption.*

161. Asymmetrical encryption algorithms were capable of encrypting with the public key, as taught by Hershey: “[T]he meta-data or hashed meta-data, can be encrypted using a public key so that accessors of the encrypted meta-data, or hashed meta-data, having the corresponding second key of the public key pair can decrypt ... the encrypted data.” Hershey, 8:22-27. Regardless of whether the second layer encryption of the Vataja/Cox encryption scheme uses a public or private key for encryption³, asymmetrical algorithms can “*utilize[] a public key for*

³ Notably, the ’998 patent only discloses that the third layer (discussed below in claim 7) is encrypted using a public key, while the second layer is encrypted using a private key: “Now the file is encrypted [**first layer**], and only the holder of the secret key can unlock the file.” Ex.1001, 9:47-49. “The file is then encrypted using an asymmetrical cryptosystem under the **user’s private key** [**second layer**], effectively signing the file.” Ex.1001, 9:54-56. “Finally, identifying information is added to the (now doubly) encrypted file, and the file is encrypted again—this time, under the storage **facility’s public key** [**third layer**].” Ex.1001, 9:57-59.

encryption and a private key is required for decryption.”

162. Thus, because the encryption techniques described by Vataja and Cox use asymmetrical encryption algorithms, which can encrypt using a public key and decrypt with the private key as taught by Hershey, Vataja, Cox, and Hershey render obvious “*wherein the asymmetrical encryption algorithm utilizes a public key for encryption and a private key is required for decryption.*”

6. Claim 7

[7.1] *The method of claim 5, wherein the step of controlling the encryptor further encrypts the identifiable encrypted file including the first and second layer encrypted augmented information with the added signature information with a third layer of encryption with an asymmetrical encryption algorithm to provide a three layer encrypted file that provides a combined encrypted file having encrypted therein the encrypted augmented information and the unencrypted signature information for transmission in the transmission with the subscriber information.*

163. First, for the reasons described above at [5.1], Vataja, Cox, and Hershey teach “*the identifiable encrypted file including the first and second layer encrypted augmented information with the added signature information.*”

164. Second, Cox teaches at least three levels of encryption: “Several levels of signing are possible. This allows the image to be signed by the **camera** (indicating that the data has not been processed subsequent to its recording from the CCD array), the **photographer** (identifying the person responsible for the image), the **distributor, etc.**” Cox, 9:37-41. The third layer of encryption on behalf

of the distributor teaches “*further encrypts the identifiable encrypted file ... with a third layer of encryption.*”

165. Third, it would have been obvious to for the distributor’s encryption to use “*an asymmetrical encryption algorithm.*” In Vataja, the CCC (i.e., distributor) provides the encryption algorithm: “Algorithm 309 may include a “hash” algorithm that is offered by the CCC.” Vataja, [0018]. It would have thus been obvious for Algorithm 309 to encrypt the third layer (on behalf of the CCC/distributor) “using a public key so that accessors of the encrypted meta-data, or hashed meta-data, having the corresponding second key of the public key pair can decrypt ... the encrypted data.” Hershey, 8:23-27. Accordingly, by encrypting the protected media file 307 using the CCC’s public key, only the CCC (which has the corresponding private key) can decrypt the third encryption layer of the transmitted file. The first two encryption layers remain encrypted with the photographer and camera keys.

166. Fourth, for the reasons described above at [1.7]-[1.9], the final protected media file—as encrypted with three layers—is “*a three layer encrypted file that provides a combined encrypted file having encrypted therein the encrypted augmented information and the unencrypted signature information for transmission in the transmission with the subscriber information.*”

167. Thus, because Vataja teaches an encryption algorithm that may

include an algorithm from the CCC, Cox teaches a three layer encryption algorithm, which may include a third layer public/private key pair as taught by Hershey, Vataja, Cox, and Hershey render obvious “*wherein the step of controlling the encryptor further encrypts the identifiable encrypted file including the first and second layer encrypted augmented information with the added signature information with a third layer of encryption with an asymmetrical encryption algorithm to provide a three layer encrypted file that provides a combined encrypted file having encrypted therein the encrypted augmented information and the unencrypted signature information for transmission in the transmission with the subscriber information.*”

7. Claim 8

[8.1] *The method of claim 7, wherein the third layer asymmetrical encryption algorithm utilizes a public key of a third party.*

168. Consistent with the discussion above at [7.1], the third level of encryption uses the CCC’s public key, which renders obvious “*wherein the third layer asymmetrical encryption algorithm utilizes a public key of a third party.*”

8. Claim 9

[9.0] *A method for acquiring information with a device from an environment external to the device to be transmitted to a receiving facility and for transmitting the acquired information thereto, comprising:*

169. See [1.0].

[9.1] *the device including a capture device for capturing the information from*

the external environment where the information is selected from the group consisting of a video segment, a still image and an audio segment, each of which varies in real time in the external environment and relative to time in the external environment prior to capture, and

170. See [1.1].

[9.2] converting the information to converted information for storage in a storage area as captured information;

171. See [1.2].

[9.3] associating with the captured information a representation of the date and time of the capture of the information, wherein the representation of the date and time information in association with the captured information forms a file containing the augmented captured information;

172. See [1.3]. For the reasons explained above at [1.2], in which the hash of the time and date (“*representation of the date and time*”) is concatenated with the media file (“*captured information*”), Vataja and Cox teach “*associating with the captured information a representation of the date and time of the capture of the information.*”

[9.4] encrypting with an encryptor the augmented captured information with a bottom layer of encryption as a bottom layer encrypted file that provides a first level of encryption of the augmented captured information that is only accessible by a secret key of a party,

173. First, for the reasons explained above at [1.4] Vataja and Cox teach “*encrypting with an encryptor the augmented captured information with a ... layer of encryption as [an] encrypted file that provides ... encryption of the augmented captured information.*”

174. Second, for the reasons described above at [4.1], Vataja and Cox teach encrypting with a multilevel process starting with a first layer for the camera (*“bottom layer of encryption”*). Thus, encrypting the augmented captured information with the camera’s private key creates a *“bottom layer encrypted file that provides a first level of encryption of the augmented captured information.”*

175. Third, because the first level/bottom level of encryption uses a private key for a symmetrical encryption technique as described at [4.1], Vataja, Cox, and Hershey teach that the first level encrypted file *“is only accessible by a secret key of a party.”*

176. Thus, because Cox describes a multilevel encryption process in which the first level uses only a private key, which indicates a symmetrical encryption technique as taught by Hershey, Vataja, Cox, and Hershey render obvious *“encrypting with an encryptor the augmented captured information with a bottom layer of encryption as a bottom layer encrypted file that provides a first level of encryption of the augmented captured information that is only accessible by a secret key of a party.”*

[9.5] in a signing operation, adding signature information to the encrypted file at the bottom layer, wherein the signature information provides information to the receiving facility that allows identification of the party claiming to have created the bottom layer encrypted augmented captured information for later identification of the party,

177. For the reasons explained above at [1.5] and [1.6], Vataja and Cox

teach “*adding signature information to the encrypted file at the bottom layer, wherein the signature information provides information to the receiving facility that allows identification of the party claiming to have created the bottom layer encrypted augmented captured information for later identification of the party.*”

[9.6] *encrypting with the encryptor the combined encrypted file containing the encrypted augmented captured information and previously unencrypted signature information with a top layer of encryption comprising a second level of encryption different from the first level of encryption as an identifiable encrypted file*

178. First, for the reasons explained above at [7.1], Vataja and Cox teach a three-level encryption technique in which the third layer (“*top layer*”) is encrypted using the public key of the distributor/CCC.

179. Second, as also described at [7.1], the third layer may use the public key of the distributor/CCC and is thus an asymmetrical encryption technique. The third-level *asymmetrical* encryption technique is thus different from the symmetrical technique of the first layer (“*a second level of encryption different from the first level of encryption*”).

180. Third, for the reasons explained above at [1.5]-[1.6] because Vataja’s protected media file 307—encrypted according to Cox’s multilevel technique—includes the photographer’s name and public keys, it is “*an identifiable encrypted file.*”

181. Thus, because the encryption process of Vataja and Cox uses a three-

level encryption technique using both symmetrical and asymmetrical encryption as taught by Hershey, Vataja, Cox, and Hershey render obvious “*encrypting with the encryptor the combined encrypted file containing the encrypted augmented captured information and previously unencrypted signature information with a top layer of encryption comprising a second level of encryption different from the first level of encryption as an identifiable encrypted file.*”

[9.7] wherein at least the first level of encryption utilizes a symmetrical encryption algorithm different from the second level of encryption and not associated with the secret key of a party associated with the first level of encryption,

182. As explained above at [4.1], the camera level encryption (“*first level*”) is a symmetrical encryption algorithm (“*utilizes a symmetrical encryption algorithm*”) this is different than the public key encryption used for the top layer (“*second level of encryption*”), which uses an asymmetrical encryption technique. Moreover, the asymmetrical encryption layer uses a public key of the distributor/CCC as discussed at [7.1]. Therefore, the second level encryption is not associated with the private key of the first level of encryption (“*not associated with the secret key of a party associated with the first level of encryption⁴*”).

⁴ The claim limitation’s use of the word “and” makes the claim read as “*wherein at least the first level of encryption utilizes a symmetrical encryption algorithm ... not associated with the secret key of a party associated with the first level of*

[9.8] *placing the identifiable encrypted file including both the bottom layer encrypted file at the first layer of encryption and the encrypted signature information at the second level of encryption in association with subscriber information as a transmission file for transmission of the identifiable encrypted file to a receiving facility requiring such subscriber information,*

183. First, as explained above at [9.4] and [9.6], Vataja and Cox teach a multilevel encryption technique that includes a bottom layer/first level for the camera and a top layer/second level of encryption for the distributor (“*the identifiable encrypted file including both the bottom layer encrypted file at the first layer of encryption and the encrypted signature information at the second level of encryption.*”)

184. Second, for the reasons explained above at [1.7] and [1.8], Vataja and Cox teach “*placing the identifiable encrypted file ... in association with subscriber information as a transmission file for transmission of the identifiable encrypted file*

encryption” which is nonsensical given the claim previously recites “*a first level of encryption of the augmented captured information that is only accessible by a secret key of a party.*” An encryption level cannot make the data only accessible by a private key and yet somehow “*not associated with*” that secret key. For purposes of this proceeding, I treat this term to mean the “*second level of encryption*” is “*not associated with the secret key of a party associated with the first level of encryption ...*”

to a receiving facility requiring such subscriber information.”

[9.9] *the subscriber information not encrypted at either the first or second levels of encryption, which subscriber information is required at the receiving facility for a lookup operation to obtain additional information;*

185. First, as described above at [1.5]-[1.7], Cox describes placing identification information such as the user’s name and public key “in the clear.” Cox, 9:31. Vataja also describes “identification information such as e.g. the IMEI and IMSI [*‘subscriber information’*].” Vataja, [0018]. Thus, when implementing Vataja’s encryption technique according to Cox, it would have been obvious to similarly include the disclosed types of identification information such as the IMSI “in the clear.” Thus, the IMSI (*“subscriber information”*) is “*not encrypted at either the first or second levels of encryption.*”

186. Second, for the reasons described above at [1.8], the “*subscriber information is required at the receiving facility for a lookup operation to obtain additional information.*”

[9.10] *transmitting with a transmitter the augmented captured information formatted for transmission including the identifiable encrypted file and the subscriber information to the receiving facility; and*

187. For the reasons explained above at [1.9], Vataja and Cox teach “*transmitting with a transmitter the augmented captured information formatted for transmission including the identifiable encrypted file and the subscriber information to the receiving facility.*”

[9.11] *receiving at a receiving facility the transmission file and accepting the identifiable encrypted file after verification of the subscriber information.*

188. For the reasons explained above at [1.10], Vataja's CCC ("*receiving facility*") receives the protected media file 307, which teaches "*receiving at a receiving facility the transmission file and accepting the identifiable encrypted file after verification of the subscriber information.*"

9. Claim 10

[10.1] *The method of claim 9, and wherein the step of encrypting further encrypts the encrypted augmented captured information with a middle layer of encryption utilizing an asymmetrical encryption algorithm to provide a two layer encrypted file, which has the signature information added thereto after encryption to provide the identifiable encrypted file.*

189. First, for the reasons explained at [5.1], Vataja, Cox, and Hershey teach encrypting with the photographer's private key, which teaches "*wherein the step of encrypting further encrypts the encrypted augmented captured information with a middle layer of encryption utilizing an asymmetrical encryption algorithm to provide a two layer encrypted file.*"

190. Second, for the reasons explained above at [1.5]-[1.7], the user's name and public key ("*signature information*") are placed "in the clear" and are thus "*added thereto after encryption to provide the identifiable encrypted file.*"

10. Claim 11

[11.1] *The method of claim 10, wherein the asymmetrical encryption algorithm utilizes a public key for encryption and a private key is required for decryption.*

191. See [6.1].

11. Claim 12

[12.1] *The method of claim 10, wherein top layer of encryption utilizes an asymmetrical encryption algorithm to provide a three layer encrypted file for transmission in the transmission with the subscriber information.*

192. See [7.1].

12. Claim 13

[13.1] *The method of claim 12, wherein the top layer asymmetrical encryption algorithm utilizes a public key of a third party.*

193. See [8.1].

IX. CONCLUSION

194. 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 that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Dated: 8/26/25



Nathaniel Polish, Ph.D.