

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EARLY WARNING SERVICES, LLC,

Petitioner,

v.

INTELLECTUAL VENTURES, LLC,

Patent Owner.

Case No. IPR2024-01221

U.S. Patent No. 7,314,167

FIRST SUPPLEMENTAL DECLARATION OF KAI JOHNSON

TABLE OF CONTENTS

I.	Introduction.....	1
II.	UPC Barcodes.....	2
III.	Encryption.....	5
IV.	Embedding Information in an Image.....	8
V.	Analysis of Purves' Declaration	16
VI.	Conclusion	31

I. Introduction

1. I incorporate herein by reference Ex. 2001, the Declaration of Kai Johnson, in its entirety.

2. As explained in my declaration (Ex. 2001), in the context of the '167 Patent, information “embedded” in an image refers to information that is hidden in the image and used to provide security for the transaction. This is the correct construction for the reasons provided in my declaration and for the additional reasons explained below.

3. In Petitioner’s Reply to Patent Owners Preliminary Response, Petitioner argues that the term “embedded” should be accorded its plain and ordinary meaning [Pet. Rep., p. 1]. Petitioner supports this argument with the First Supplementary Declaration of Thomas Purves (Ex. 1036) and copies much of its argument from this supplementary declaration. However, as described in detail below, the First Supplementary Declaration of Thomas Purves is inaccurate in many aspects and the evidence it cites supports Patent Owner’s construction of information “embedded” in an image.

4. Petitioner’s argument in relation to the construction of the term “embedded” refers to barcodes and encryption and compares them to Patent Owner’s construction of the term. The distinctions among these concepts are clearer with an

understanding of each of the individual concepts.

II. UPC Barcodes

5. As Purves says in his declaration, “The most common well-known standard of barcodes is the UPC code which enables the representation of 12 numerical digits” [Ex. 1002, ¶134]. UPC barcodes are one-dimensional codes commonly found on retail products and used in other contexts. There are several formats for UPC barcodes, but the UPC-A format is perhaps the most familiar.



Figure 1: An example UPC barcode in the UPC-A format.

6. A UPC-A barcode is composed of several elements, highlighted in color in Fig. 2 below:

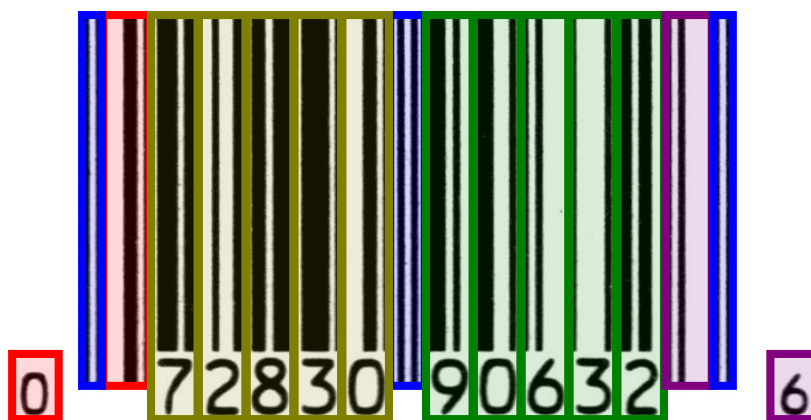


Figure 2: Components of an example UPC-A barcode highlighted in color

7. Referring to Fig. 2 above and the highlighting in color, the elements of the UPC-A barcode as described in the ISO/IEC 15420-2000 standard (Ex. 2015) are from left to right:

- a. a left quiet zone, which is the whitespace to the left of the barcode (not highlighted);
- b. a left guard pattern (in blue);
- c. six digits encoded using Number Set A (in red and yellow);
- d. a middle guard pattern (in blue);
- e. six digits encoded using Number Set C (in green and purple);
- f. a right guard pattern (in blue);
- g. a right quiet zone, which is the whitespace to the right of the barcode (not highlighted); and below
- h. a numeric interpretation of the digits printed underneath the barcode symbol (highlighted in color to match the corresponding components of the barcode)

8. Number Sets A and C define patterns of light and dark bars for each digit [Ex. 2015, Annex D, p. 26]. Fig. 3 below shows how these patterns can be interpreted as digits. The two zeros on the left side of the barcode (in red and yellow) correspond to the same pattern of light and dark bars from Number Set A. Likewise, the two sixes on the right side of the barcode (in green and purple) correspond to the same pattern of light and dark bars from Number Set C. The patterns of light and

dark bars in Number Set C are the opposite of the patterns in Number Set A, with light bars replaced by dark bars and vice versa. So, the patterns for the left zero (in yellow) and the right zero (in green) are the opposite of each other [See, Ex. 2015, Annex D, p. 26].

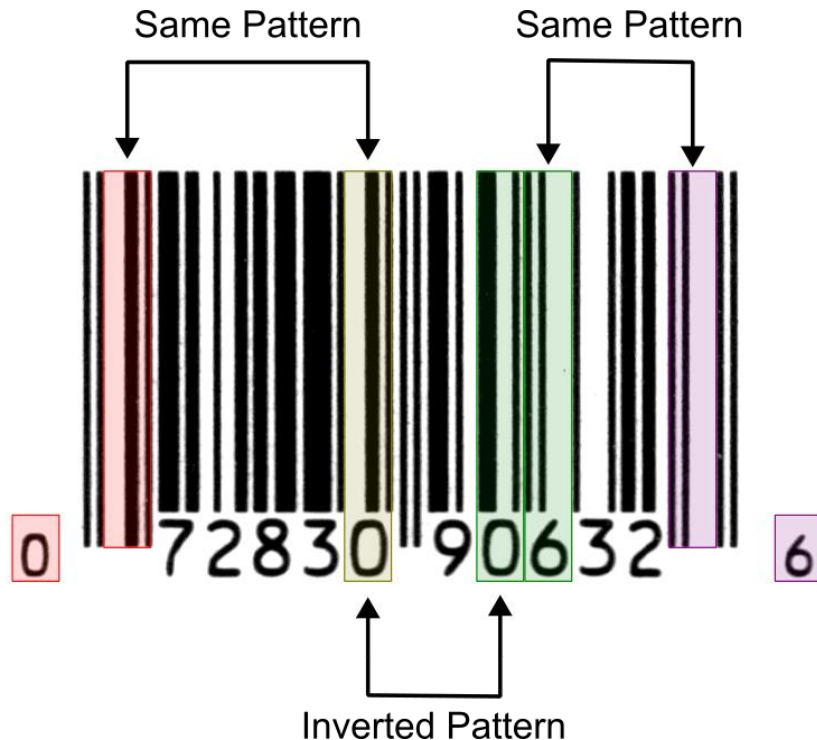


Fig. 3: UPC-A barcode with numeric symbols highlighted

9. Interpreting a UPC barcode is as simple as interpreting the symbols in the components of the barcode as the corresponding digits. And since the UPC format mandates that a human-readable representation of the barcode data is printed next to the barcode [Ex. 2015, p. 23], no special equipment or knowledge is needed to read the barcode. In addition, the patterns of light and dark bars are in plain view and can be interpreted by a human, so no barcode scanner is necessary to read a UPC

barcode. There is no hidden information in a UPC barcode. Everything is as simple and straightforward as it appears.

III. Encryption

10. The *Encyclopedia of Computer Science, Third Edition* provides a good description of cryptography: “Cryptography is the science of transforming messages for the purpose of making the message unintelligible to all but the intended receiver of the message.” [Ex. 2016]

11. NIST published the Advanced Encryption Standard (AES) in 2001 [Ex. 2017]. As a practitioner in the field, I recall that AES was commonly used at the time of the patent. Cryptographic methods such as AES use “key” data to control the operation of a cipher that transforms an original message (“plaintext”) into an encrypted message (“ciphertext”). In addition to the key, AES uses an “initialization vector” of random data to start the encryption process.

12. For example, AES could be used to encrypt the data from the UPC barcode above. This encryption process is shown below in Fig. 4.

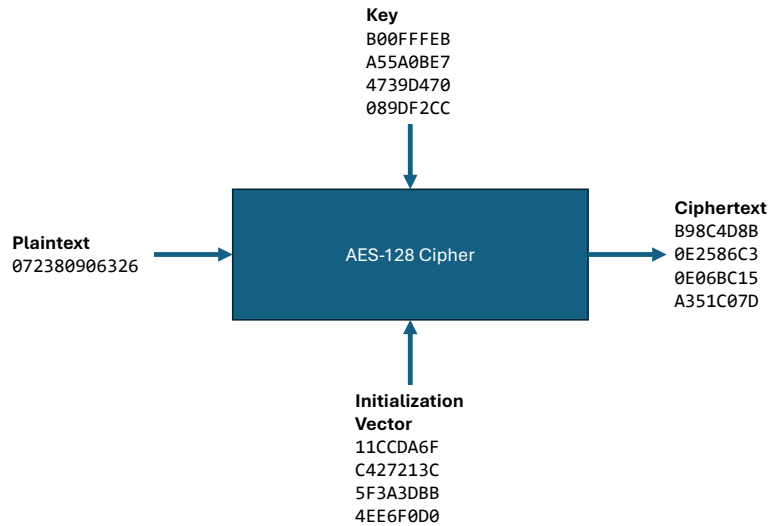


Figure 4: AES encryption of the UPC barcode data

13. While the initial plaintext is meaningful, the resulting ciphertext appears to be random data without any apparent meaning. The meaning of the ciphertext can only be determined by reversing the process and decrypting the data using the same key and initialization vector to recover the original plaintext. This is the purpose of the encryption, to transform the message for the purpose of making it unintelligible to all but the intended receiver.

14. Notably, the ciphertext is not the same length or format as the plaintext. The plaintext in this example was 12 decimal digits while the ciphertext is 32 hexadecimal digits (or 128 bits). This makes it impractical to use the ciphertext in place of the plaintext, so for example, it would not be possible to represent the ciphertext in a UPC-A barcode.

15. In addition, the initialization vector is necessary for both encryption and

decryption and so it is normally delivered along with the ciphertext while the key remains secret. In a practical implementation, that would mean that 64 hexadecimal digits (or 256 bits) would need to be delivered to include both the initialization vector and the ciphertext for the recipient to be able to recover the plaintext using the secret key. That is substantially more data than the original 12 digits from the UPC barcode.

16. The *Encyclopedia of Computer Science, Third Edition* mentions a classical encryption method that would preserve the format of the original data: “Classical encryption techniques involve such operations as substituting for each message letter a substitute letter; in this case, the key is the correspondence between message (plaintext) letters and the enciphered message (ciphertext) letters” [Ex. 2016].

17. For example, a classical substitution cipher could be used to encrypt the data from the UPC barcode above. This encryption process is shown below in Fig. 5.

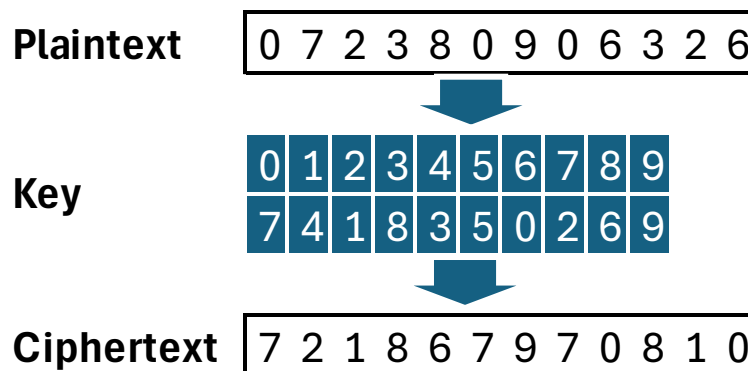


Figure 5: A classical substitution cipher

18. Although the ciphertext appears to have the same format as the plaintext, the digits appear random and are no longer meaningful. With knowledge of the substitution key, the plaintext can be recovered by reversing the substitution.

19. However, as the encyclopedia notes: “These [substitution] techniques are insecure in general” [Ex. 2016], meaning that it is relatively easy for someone other than the intended recipient to determine the substitution key and thus decrypt the messages.

IV. Embedding Information in an Image

20. The exhibits cited by both Patent Owner and Petitioner contain many examples of embedding information in images. These examples all use a common method of starting with an original or base image, encoding the information to be embedded in the image as required by the method, then modifying the base image to embed the data.

21. The examples of embedding information in images in Petitioner’s exhibits are discussed in further detail below. But to illustrate the concept of embedding information in an image, I have produced an example of the method using the 2003 article, “Graphical Indicia,” which is Petitioner’s Exhibit 1037.

22. The “Graphical Indicia” article describes a method of embedding data in an image where the image is partitioned into a rectangular array of “blocks” each

of which may be “dark” or “light” to represent a component of the image. Then the method chooses a halftone pattern based on whether the color of the block and the information to be encoded in the image and substitutes the halftone pattern for the block of the image [Ex. 1037, 2-3]. The article illustrates the selection of halftone patterns in its Fig. 3, reproduced below.

Message Block Bits Color		00	01	10	11
Light					
Dark					

Figure 3: A simplistic graphical modulation scheme.

[Ex. 1037, Figure 3]

23. This method is relatively straightforward and easy to understand, so I have chosen to use this method to produce an example of information embedded in an image. As with the other methods of embedding information in an image, this method starts with a base image. To illustrate the method, I have chosen a very small and simple base image which is eight pixels on a side with dark pixels in the upper left quadrant and light pixels in the remaining quadrants.

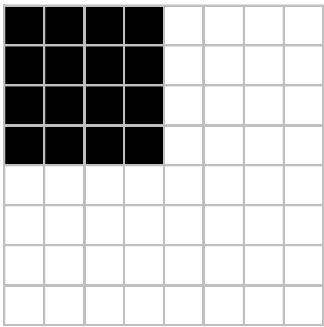


Figure 6: A base image of 8 by 8 pixels in which information will be embedded

24. Since this image is small, only a small amount of information can be embedded in the image. I have chosen a short phrase which when encoded is suitable to be embedded in the image: “DATA IS EMBEDDED.” The encoding of this phrase as binary digits using ASCII encoding [See, Ex. 2019] is shown below. The short phrase is plaintext and the conversion to binary digits based on ASCII encoding is not encryption, so the data remains as plaintext.

Text	D	A	T	A		I	S	
Hexadecimal	44	41	54	41	20	49	53	20
Binary	0100 0100	0100 0001	0101 0100	0100 0001	0010 0000	0100 1001	0101 0011	0010 0000
Text	E	M	B	E	D	D	E	D
Hexadecimal	45	4D	42	45	44	44	45	44
Binary	0100 0101	0100 1101	0100 0010	0100 0101	0100 0100	0100 0100	0100 0101	0100 0100

Figure 7: Data to be embedded, encoded as required by the embedding method

25. As described in the article, each pixel in the base image will be replaced by a halftone pattern selected based on the color of the pixel and the information to be embedded in the image. This selection process is illustrated below.

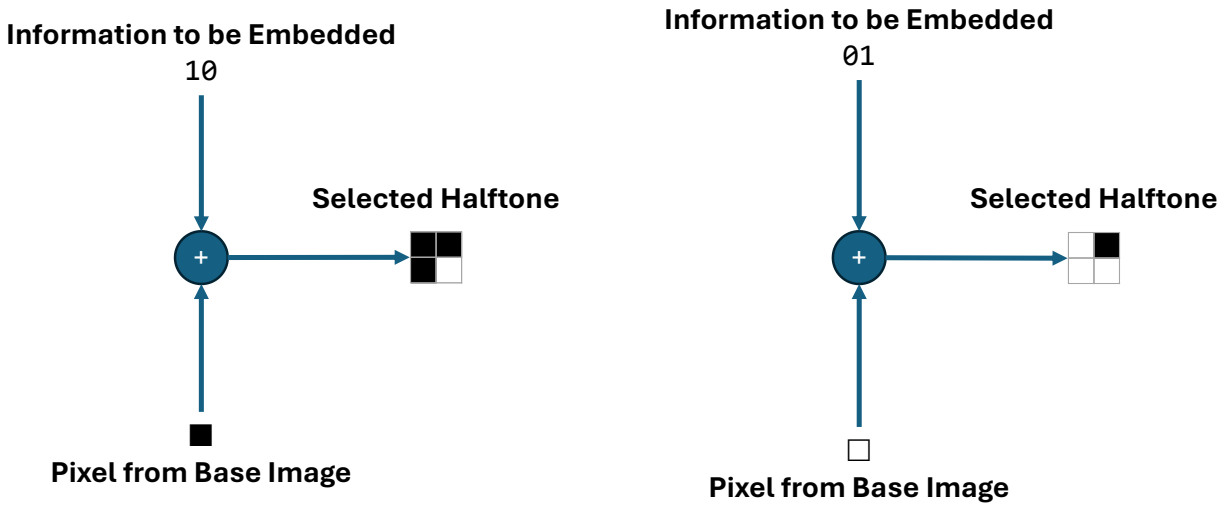


Figure 7: Examples of selecting halftones to embed information in an image

26. Applying the process of selecting a halftone image based on each pixel in the base image and the information to be embedded in the image, then replacing the pixel with the halftone produces an image with information embedded therein.

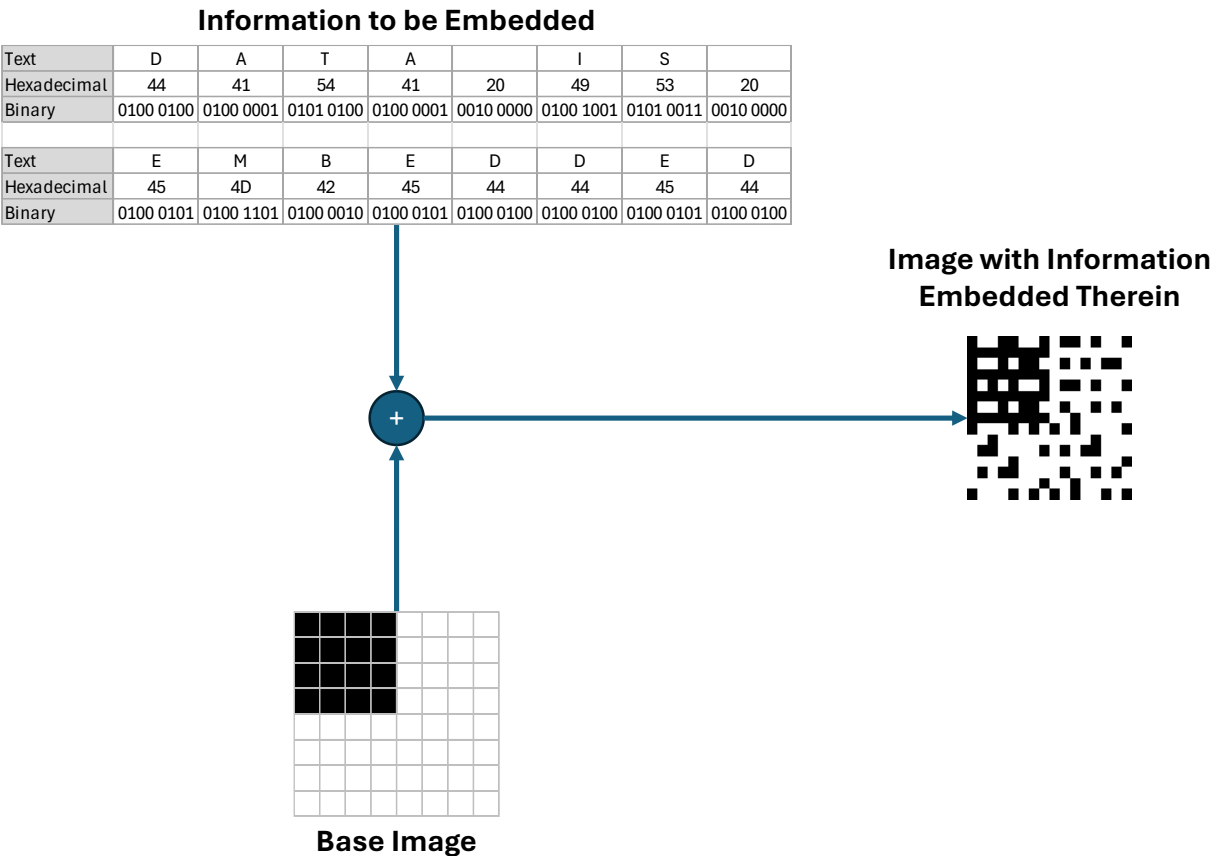
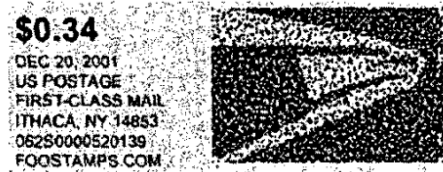


Figure 8: Information embedded in an image

27. As described above, I have chosen the method of embedding information in the image, the information to be embedded in the image, and the base image to be small and simple for the benefit of this explanation. Although the original character of the base image is retained with the dark square in the upper left quadrant, the choices I have made for the sake of this example result in significant distortion of the base image. In a real-world implementation of embedding information in an image, one would make better choices that result in less distortion of the original image. The “Graphical Indicia” article provides a better example of

an image having information therein as a postmark with information embedded in the halftone pattern.



[Ex. 1037, Figure 4]

28. Although the halftone pattern in this image is noticeable, there are methods of embedding information in images that are much more subtle, such as the method described in Petitioner's Exhibit 1040: which is "'invisible' digital watermarking [...]" as small as a person can hardly visibly perceive" [Ex. 1040, 9:27-29] and subtle enough that the embedded information is intentionally lost if the image is photocopied [Ex. 1040, 5:51-55].

29. Several aspects of the process of embedding information in an image are notable. First, the original character of the base image is preserved (albeit with some distortion in my simplified example). Second, although the information embedded in the image is encoded as required by the embedding method, it is not encrypted. Unlike an encrypted message, any party that implements the method of extracting the embedded information from the image can recover the original information. Third, depending on the size of the image and method of embedding information in the image, substantial amounts of data can be embedded. The simple

example above embeds 128 bits (16 characters with 8 bits per character) of information in a very small image. That is enough to embed the entire output of the AES encryption described above, much more data than could be encoded in a UPC-A barcode. While in the example above, the information embedded in the image was plaintext, it would also be possible to encrypt the data first and then embed the ciphertext in the image. It is possible to combine the techniques of encrypting information, rendering the information unintelligible to all but the intended receiver, with embedding information in an image, hiding the information by making it imperceptible.

30. As described in my declaration, in the context of the '167 Patent, the information “embedded” in the image is used to provide security for the transaction. This is possible even if the information embedded in the image is not encrypted. For example, the information embedded in the image could contain a nonce used to derive the authentication code to provide security for the transaction: “the image or video captured by the secure device 100 may include a unique number, nonce, a transaction number or a random number, a number that the secure device 100 will use to derive the authentication code” [Ex. 1001, 7:55-69].

31. In the context of the '167 Patent, the base image in which information is to be embedded can be a barcode: “The image or video 340, such as a linear barcode, [...] contain[s] certain embedded information” [Ex. 1001, 6:49-51].

Conventional barcodes such as the UPC-A format discussed above do not hide information. Indeed, the UPC format requires that the information in the barcode is printed in human-readable form.

32. However, at the time of the '167 Patent there were methods of embedding information in barcode images so that the base image of the barcode is preserved, and the additional information is hidden in the barcode. The article titled “Embedding biometric identifiers in 2D barcodes for improved security” cited in my declaration as Exhibit 2007 describes a method where information is “embedded into the black bar of the 2D barcode image” where “[t]he embedding process replaces the intensity value of the selected barcode pixels with the L, I and M bits” of the embedded information [Ex. 2007, p. 3]. As described in the article, “This technique does not affect the original utility and storage capacity of the 2D barcode” [Ex. 2007, p. 7]. So, the resulting image retains the unhidden barcode symbols representing the original barcode data. In addition, the information embedded in the barcode “is also imperceptible and not readily apparent to a person who wants to tamper [with the embedded information]” [Ex. 2007, p. 7]. So, the resulting image also contains embedded information hidden in selected pixels of the black bars of the barcode.

V. Analysis of Purves' Declaration

33. Purves argues that “PO’s construction of ‘embedded’ reads on conventional barcodes, which contain hidden information that require barcode readers to decode, thereby providing a level of security” [Ex. 1036, ¶4, emphasis added]. However, as discussed above, a conventional barcode does not contain hidden information. With an understanding of how the barcode symbols are used to represent data, as shown in the example of the UPC-A barcode above, decoding the information in a barcode is straightforward. Although it is inconvenient to do so, even a 2D barcode can easily be decoded by hand using nothing more than an understanding of the barcode format and a pencil and paper [Ex. 2018].

34. Further, Purves conflates the alleged security of information in the barcode with the concept of providing security for a transaction in Patent Owner’s construction of information “embedded” in an image. The correct construction of information “embedded” in an image in the context of the ’167 Patent is that the information that is embedded (hidden) in the image is used to provide security for the transaction, not that a barcode itself provides “a level of security.”

35. Even so, a conventional barcode does not provide “a level of security” as Purves implies. A conventional barcode does not ensure the confidentiality of the information in the barcode since anyone can decode the barcode (as described

above). A conventional barcode does not ensure the integrity of the information in the barcode, since anyone could modify or replace the barcode with another barcode without being detected. (For example, someone could peel the barcode off conventional produce and place it on organic produce to buy the organic produce at a lower price.) A conventional barcode does not ensure the authenticity of the information encoded in the barcode since even if the data in the barcode identifies the source of the barcode, this information could easily be changed if the barcode itself is modified or replaced. A conventional barcode does not prevent the barcode's producer from repudiating the information in the barcode because the barcode could have been modified or replaced by another party. The '167 Patent compensates for this lack of security by encrypting the information embedded in the image: "The information embedded in the image or stream of images may be created using any one of a number of well-known decryption/encryption algorithms, such as, a symmetric system using shared keys an asymmetric system using public/private key pairs" [Ex. 1001, 5:57-61].

36. Purves says that "For purposes of this declaration, however, I have interpreted PO's position to be that the term 'hidden' requires some level of encryption" [Ex. 1036, ¶4]. However, Patent Owner's construction does not require that the term "hidden" requires "some level of encryption." As discussed in detail below, several of the references that Purves cites contradict this interpretation and

confirm that the use of information “embedded” in an image in the context of the ’167 Patent refers to “hidden” information.

37. According to the ’167 Patent, the “hidden” information can optionally have a further layer of protection based on the use of encryption. For example, the ’167 Patent says, “The Secure device 100 then derives the authentication code 350 and other relevant information 360 based on the embedded information stored in the scanned image or video [...] The derivation process may be performed using an encryption, a decryption or a message authentication algorithm” [Ex. 1001 6:60-7:1]. The information embedded in the image would be hidden, as described in the explanation of embedding information in an image above. However, the derivation process could use a message authentication code, which ensures the integrity and/or authenticity of the information but does not encrypt the information. The ’167 Patent continues: “If the image 340 has been generated using an encryption or decryption algorithm, the derivation process may correspond to the encryption or decryption algorithm used to create the information embedded in the image or video 340” [Ex. 1001, 7:2-5]. So, the use of encryption is optional and separate from embedding information in the image.

38. Purves says that “[I]nformation itself decoded from the barcode is hidden in that you need a barcode scanner to decode it. Further, product information pulled up from a lookup table using decoded barcode information is further hidden

in that you require a lookup table” [Ex. 1036, ¶5]. It is not clear how to reconcile this with Purves’ assertion that “‘hidden’ requires some level of encryption” [Ex. 1036, ¶4] because as described above, barcodes merely encode data, not encrypt it. In addition, as described above in the explanation of barcodes, the information in a barcode is not hidden but readily apparent. It is also not clear how Purves’ reference to a lookup table is relevant since there is no mention of a lookup table in the ’167 Patent and the UPC lookup tables that Purves refers to are public information that is not hidden.

39. Purves says, “It is unclear to me how much security is required to satisfy PO’s construction of the term ‘embedded’” [Ex. 1036, ¶5]. Purves could have considered conventional barcodes in the context of confidentiality, integrity, authenticity, or non-repudiation, as discussed above. But, as also discussed above, if he had chosen to do so he would have found that conventional barcodes do not provide these attributes commonly associated with security.¹

40. Here, Purves seems to have confused the concept of securing information in a barcode (in his terms) with Patent Owner’s construction which is

¹ Some barcodes include error detecting or error correcting codes that ensure a certain level of integrity. However, these codes are merely intended to improve reading accuracy do not protect the barcodes against intentional modification or tampering. The purpose of error detecting and error correcting codes is to ensure that the data can be properly decoded, so error detecting and error correcting codes cannot be used to provide confidentiality.

that “information ‘embedded’ in an image refers to information that is hidden in the image and used to provide security for the transaction” [Ex. 2001, ¶81, emphasis added]. The ’167 Patent makes it clear that the information embedded in the image is used to secure the transaction, e.g., “the transaction server 600 may then use the transaction number to identify the session and check the generated confirmation signature or authorization code relative to the information embedded in the image or stream of images and, if appropriate, effect the transaction” [Ex. 1001, 10:7-12, emphasis added].

41. Purves says that “the plain and ordinary meaning [of a term] reflects how a POSA would interpret the term in light of the specification and prosecution history” [Ex. 1036, ¶7]. As a POSITA and having read the claims, specification, and prosecution history of the ’167 Patent, I understand that information “embedded” in an image refers to information that is hidden in the image and used to provide security for the transaction in the context of the ’167 Patent. The reasoning for my understating of this term is provided in my declaration [Ex. 2001, Section X.B.].

42. Purves argues that since the ’167 Patent mentions 1D and 2D barcodes, “the plain and ordinary meaning of ‘embedded’ includes information contained in any barcode” [Ex. 1036, ¶8]. However, the ’167 Patent makes a clear and unmistakable distinction between decoding the information from a barcode and extracting the embedded information:

the processor 110 decodes the captured image or video and extracts the relevant embedded information. [Ex. 1001, 6:8-10, emphasis added]

43. Therefore, the invention disclosed in the '167 Patent is distinct from a conventional barcode reader that simply decodes the information in a single step rather than being processed using “decoding” followed by “extracting.”

44. Purves argues that since “The '167 patent [...] mentions the optional use of encryption [...] the intrinsic evidence ('167 patent and its prosecution history) supports a plain and ordinary meaning of “embedded” that reads on any information derived from barcodes—whether encrypted, unencrypted, hidden, or unhidden” [Ex. 1036, ¶9]. Here, Purves has again conflated encrypting information with hiding it. However, Patent Owner’s construction does not require that “hidden” requires “some level of encryption.”

45. Purves argues that “blocks 1010 and 1110 of the '167 patent, the transaction information derived from the barcode involves only information that, in my view, a POSA would recognize as being readily known by both parties of the transaction: a merchant name, the sender’s identifier, and a transaction amount” [Ex. 1036, ¶10]. The implication that it matters whether the information is “readily known by both parties” seems to have been based on the confusion between encryption and embedding information in an image. As described above, encryption and embedding information in an image are separate and distinct concepts. Embedding information

in an image hides the information but does not ensure its confidentiality. If confidentiality were required, the information would need to be encrypted before it is embedded in the image. In addition, the '167 Patent makes clear that the barcodes in 1010 and 1110 contain embedded information using the exact same language in both cases: “The image or stream of images includes embedded information relating to the transaction” [Ex. 1001, 13:43-45 and 14:8-9]. And as described above, information “embedded” in an image refers to information that is hidden in the image in the context of the '167 Patent.

46. Purves refers to a “doctrine of claim differentiation” to show that “this doctrine appears to contradict PO’s position that ‘embedded’ refers to hidden, i.e., encrypted, information, provided for security purposes” [Ex. 1036, ¶11]. However, Purves has again conflated encrypting information with hiding information. Patent Owner’s construction of information “embedded” in an image does not require that hiding information means encrypting it, and so there is no contradiction between the dependent claims and independent claims of the '167 Patent.

47. Purves cites additional extrinsic evidence in an attempt to support his arguments. However, this additional extrinsic evidence does not show what Purves claims it does.

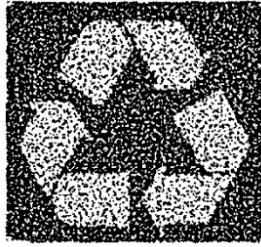
48. As shown in the example of embedding information in an image above,

the 2003 article, “Graphical Indicia” (Ex. 1037) describes a method of generating “graphical barcodes” by modifying a base image to embed additional data in the image, and a further “graphical indicium” which is a “graphical barcode” with additional security attributes:

The graphical barcode is generated by modulating halftone patterns according to the message to be embedded in the barcode during the rendering of a base image. The generated barcode has the appearance of the base image, and when it is printed and scanned back in, the message can be retrieved. A graphical indicium is a graphical barcode embedded with a digitally signed message such that the integrity and authenticity of the message can be verified. [Ex. 1037, Abstract, p. 485]

49. The article describes the use of “graphical indicia” for secure transactions: “There are a wide variety of potential applications for graphical indicia. Any e-commerce transaction that requires payment evidence such as concert tickets and electronic stamps, for instance, can leverage this technology” [Ex. 1037, p. 485, emphasis added].

50. In addition, the article provides examples of its “graphical barcodes” such as a recycling logo embedded with additional information in the halftone pattern. In this example, clusters of dots in the halftone pattern would be chosen to embed the additional information. These clusters of dots would be interpreted to extract the embedded information from the image.



[Ex. 1037, Figure 1, excerpt]

51. As discussed above, the article proposes a simple scheme by which the clusters of dots could be chosen to embed data when producing an image or extracting the embedded data from an image.

Message Block Bits Color	00	01	10	11
Light				
Dark				

Figure 3: A simplistic graphical modulation scheme.

[Ex. 1037, Figure 3]

52. That is, at a glance, the image appears to be ordinary and unremarkable, as in Figure 1. But the embedded information is hidden in the image by using clusters of dot patterns to represent the data, as in Figure 3. This data is “hidden” because it would not be detected except by someone using the proper method of extracting the data.

53. As Purves says, “In one embodiment, the ‘**embedded**’ information includes a digital signature that can be used to verify the integrity and authenticity.”

[Ex. 1036, ¶13, emphasis in original]. Integrity and authenticity are aspects of security, and so the information **embedded** in an image is clearly being used to provide security.

54. Purves suggests that “A person of ordinary skill in the art would understand that this exhibit does not require that the embedded information is hidden or provided for security purposes.” However, the 2003 article, “Graphical Indicia” (Ex. 1037) unambiguously contradicts this conclusion by providing a clear example of embedding information by hiding it in an image and using the information to provide security.

55. The 2003 article, “Practical Guide to Bar Coding for Patient Medication Safety” (Ex. 1038), discusses “Bar coding for the medication administration step of the drug-use process.” Purves attempts to use this document to provide an alternate definition of “data embedded within the bar code” [Ex. 1036, ¶14]. However, this article was written for practitioners in health care and only provides a basic overview of barcode technology. A POSITA would not look to an article from outside the field to understand the use of “embedded” as a term of art.

56. The 1993 article, “Bridging the Paper and Electronic Worlds: The Paper User Interface” (Exhibit 1039), describes “a new technology for bridging the paper and the electronic worlds. In the new technology, the user interface moves beyond

the workstation and onto paper itself” [Ex. 1039, Abstract, p. 507].

57. This article is not directed toward embedding information in images at all, but instead focuses on allowing users to interact with computer applications by marking up paper forms that are scanned and interpreted by the application: “A form is a paper interface to a computer application just as a dialog box is a screen interface to a computer application. Forms combine the simple paper syntax and infrastructure support of paper with the functionality of computer applications.” [Ex. 1039, p. 508]. Since the article is not directed toward embedding information in images, a POSITA would not look to this article to understand the use of “embedded” as a term of art.

58. In passing, the article mentions some other contemporary work on embedding information in images. Purves does not cite this other work, nor is it clear that there are any published articles on this subject. There is no further mention of this other work in the article, nor would there be as this is not the subject of the article. The single paragraph referring to embedding information in images reads:

Recent work at Xerox PARC, led by Dan Bloomberg and David Hecht, has seeded the development of an end-run around these problems in document recognition. The basic technology is a method for embedding digital data in documents as diagonal marks on paper, and reading back this data from images of the documents. These marks, which Bloomberg has labeled simply “glyphs,” are robust in the face of the range of distortions introduced in printing, copying, faxing, and scanning. Furthermore, they are scalable, and thus useful for encoding information in documents scanned or printed at very low and very high

resolutions. Finally, their simple, regular pattern fails to catch the eye, so they are not visually distracting when embedded in a paper document. [Ex. 1039, p. 508, emphasis added]

59. As this reference says, the data is “embedded” in a document as diagonal marks that fail to catch the eye (i.e., are hidden) and are preserved in spite of distortions introduced in printing, copying, faxing, and scanning and therefore provide some integrity (i.e., security) to the document.

60. Purves says that “A person of ordinary skill in the art would understand that this exhibit does not require that the embedded information is hidden or provided for security purposes” [Ex. 1036, ¶15] However, as described above, this passing mention clearly supports the conclusion that information “embedded” in an image refers to information that is hidden in the image and used to provide security.

61. U.S. Patent No. 7,287,284 (Ex. 1040) is directed to “verifying the relationship between given document data and a master (original)” [Ex. 1040, 1:9-10]. The object of the invention is “to provide an information processing method and apparatus, which embed a plurality of types of different information, verify and check each embedded information, and verify if target document data corresponds to an original or copy,” [Ex. 1040, 1:45-49].

62. Claim 1 of Ex. 1040 reads:

1. An information processing method for embedding additional information in document data, comprising:

- a document data input step of inputting document data that includes a character string;
- an additional information input step of inputting additional information;
- an image data input step of inputting image data as a background image:
- a first embedding step of embedding the additional information in the input background image data, using a first digital watermark method and a parameter defining a robustness, wherein the first digital watermark method embeds information in an image by changing a pixel value using the parameter defining the robustness, and wherein the parameter is determined so that, in a case where an original document, in which information has been embedded using the first digital watermark method, is copied by a copying machine, the embedded information cannot be detected in the copied document output from the copying machine;
- a second embedding step of embedding the additional information in the input document data, using a second digital watermark method, wherein the second digital watermark method embeds information in an image by changing a distance between characters in the image so that, in a case where an original document, in which information has been embedded using the second digital watermark method, is copied by a copying machine, the embedded information can be detected in the copied document output from the copying machine;
- a composition step of compositing the document data in which the additional information has been embedded in the second embedding step, as a foreground image, and the background image in which the additional information has been embedded in the first embedding step; and

an output step of outputting the document data composed with the image data in the composition step. [Ex. 1040, 31:22-59, emphasis added.]

63. As described in independent claim 1, the invention uses two methods to embed information in an input image. The first method modifies individual pixels of the input image, and the second method modifies the space between characters in the input image. Both methods are subtle and are not intended to be detected by someone reading the document. The first method is so subtle that the modifications to the document are lost when it is reproduced in a copying machine [Ex. 1040, 9:35-38]. That is, both methods hide information in the image of the document.

64. Independent claim 3 [Ex. 1040, 31:65-32:35] describes “An information processing method for verifying whether or not document data matches an original.” This method uses the embedded information described in claim 1 to determine whether “the input document data corresponds to the original.” That is, the embedded information is used to ensure the integrity (*i.e.*, security) of the document.

65. Purves says that “A person of ordinary skill in the art would understand that this exhibit does not require that the embedded information is hidden or provided for security purposes” [Ex. 1036, ¶16]. However, U.S. Patent No. 7,287,284, (Ex. 1040) directly contradicts this conclusion and shows that information “embedded” in an image refers to information that is hidden in the image

and used to provide security.

66. U.S. Patent Application 10/698,162 (Ex. 1041) is directed to “a method and apparatus for encoding and/or decoding embedded instructions” [Ex. 1041, ¶0001]. Having reviewed the claims and specifications of the patent application, the patent application clearly uses “embedded” not as a term of art but colloquially to mean “incorporated.” In addition, the invention described in the patent application is merely an application of conventional barcode technology. A POSITA would not look to Ex. 1041 to understand “embedded” as a term of art in the context of information embedded in images.

67. The 1998 instruction manual, “DataMax Programmers Manual” (Ex. 1042), “explains in detail the Datamax Programming Language (DPL), how to write programs that will enable Datamax label printers to create label formats (designs), and allow the user to control the operation of the printer” [Ex. 1042-2].

68. Purves cites Appendix G of Ex. 1042: “Under Appendix G are provided a list of available barcodes to print including UPA-A and EAN-13, which are ‘used when the price or weight of an item is embedded into the barcode data (this is commonly used in the food industry.)’ Id. at 181” [Ex. 1036, ¶18].

69. However, Purves’ omits the context of the quote: “The EAN/UPC standard allows for an additional checksum to be generated in the middle of the

barcode based on the data. This is used when the price or weight of an item is embedded into the barcode data (this is commonly used in the food industry)” [Ex. 1036, ¶18, emphasis added]. In context, this is clearly a checksum to be embedded in the barcode data, or data to be embedded in data. This is not an image having information embedded therein as required by the ’167 Patent.

70. Appendix G provides an example of what Datamax means by “embedding”:

1B110000200020012345V01199

Prints a UPC-A barcode with the variable price checksum in the 6th position. [Ex. 1041-181, emphasis added]

71. In this case, the letter “V” would be replaced by a checksum digit calculated from the other digits in the input. Contrary to Purves’ suggestion, this exhibit is not related to an “image having information embedded therein” as required by the ’167 Patent since it merely refers to substituting a checksum digit for the “V” character in the input data. With this understanding of the context, a POSITA would not look to the “DataMax Programmers Manual” to understand the use of the term “embedded” in the ’167 Patent.

VI. Conclusion

72. As described in my declaration, in the context of the ’167 Patent, information “embedded” in an image refers to information that is hidden in the image

First Supplemental Declaration of Kai Johnson

and used to provide security for the transaction [Ex. 2001, Section X.B.]. Purves does not correctly construe the term “embedded” in the context of the claims, specification, and prosecution history of the ’167 Patent. And the additional extrinsic evidence that Purves cites either supports Patent Owner’s construction of the term or is not relevant to the construction of the term.

73. This declaration represents the opinions that I have formed up to date based on the material currently available to me. I reserve the right to revise, supplement, and/or amend my opinions stated in this declaration based on new information that becomes available to me and on my continuing analysis of the materials available to me.

74. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine, imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: December 19, 2024



Kai Johnson