



(86) Date de dépôt PCT/PCT Filing Date: 2014/06/20
 (87) Date publication PCT/PCT Publication Date: 2015/12/23
 (45) Date de délivrance/Issue Date: 2021/07/13
 (85) Entrée phase nationale/National Entry: 2016/12/20
 (86) N° demande PCT/PCT Application No.: US 2014/043451
 (87) N° publication PCT/PCT Publication No.: 2015/195142

(51) Cl.Int./Int.Cl. *G06T 9/00* (2006.01),
H04N 5/341 (2011.01)
 (72) Inventeurs/Inventors:
POWERS, NANCY, US;
KOC SIS, PAUL, US
 (73) Propriétaire/Owner:
SIGNS & WONDERS UNLIMITED LLC, US
 (74) Agent: MARKS & CLERK

(54) Titre : SYSTEME ET PROCEDE D'ENCODAGE ET D'AUTHENTIFICATION D'UNE IMAGE NUMERIQUE
 (54) Title: SYSTEM AND METHOD FOR ENCODING AND AUTHENTICATING A DIGITAL IMAGE



(57) **Abrégé/Abstract:**

An encoding apparatus partitions a digital image into multiple regions for subsequent encoding. A first encryption code is associated with a first region, a second encryption code is associated with a second region and the first code, and a third code is associated with the first code, the second code and a third region. An authentication apparatus authenticates the digital image in an inverse process.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(10) International Publication Number
WO 2015/195142 A1

(43) International Publication Date
23 December 2015 (23.12.2015)

- (51) International Patent Classification:
H04N 1/46 (2006.01)
- (21) International Application Number:
PCT/US2014/043451
- (22) International Filing Date:
20 June 2014 (20.06.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant: **SIGNS & WONDERS UNLIMITED LLC** [US/US]; Post Office Box 489, Libertyville, Illinois 60048 (US).
- (72) Inventors: **POWERS, Nancy**; 28318 North Oak Lane, Libertyville, Illinois 60048 (US). **KOCSIS, Paul**; #102, 1809 N. 121st St., Omaha, Nebraska 68154 (US).
- (74) Agent: **THILL, Richard W.**; Pillsbury Winthrop Shaw Pittman LLP, P.O. Box 10500, McLean, Virginia 22101 (US).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

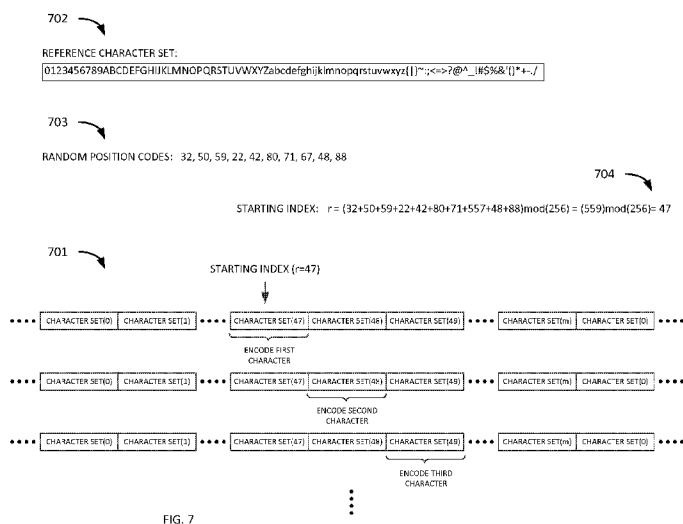
(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CL, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published: — with international search report (Art. 21(3))



WO 2015/195142 A1

(54) Title: SYSTEM AND METHOD FOR ENCODING AND AUTHENTICATING A DIGITAL IMAGE



(57) Abstract: An encoding apparatus partitions a digital image into multiple regions for subsequent encoding. A first encryption code is associated with a first region, a second encryption code is associated with a second region and the first code, and a third code is associated with the first code, the second code and a third region. An authentication apparatus authenticates the digital image in an inverse process.

SYSTEM AND METHOD FOR ENCODING AND AUTHENTICATING A DIGITAL IMAGE

TECHNICAL FIELD

[0001] The present invention relates generally to the field of digital image processing and, more particularly to protective encoding and authentication of digital images.

BACKGROUND

[0002] This section is intended to provide a background or context to the disclosed embodiments. The description herein may include concepts that could be pursued, but are not necessarily ones that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the description and claims in this application and is not admitted to be prior art by inclusion in this section.

[0003] The proliferation of digital cameras and camera-equipped smartphones, along with sophisticated image processing software such as Adobe Photoshop® have made it extremely easy to alter digital photographs, and such doctored photographs are appearing with increasing frequency. Conventional digital forensic techniques use variations of statistical analysis to detect alterations due to cloning, resampling, splicing and the like. While useful in many different contexts, these techniques are not capable of authenticating every individual pixel in a digital image.

SUMMARY

[0004] Embodiments of the present invention are directed to encoding digital images at the time of their creation so that any alteration to even a single pixel can later be detected. In one

embodiment, a method for encoding a digital image includes: capturing a digital image comprising a plurality of pixel rows; partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row; generating a first code from the first plurality of pixel rows; overlaying the second plurality of pixel rows with an image representing the first code; generating a second code from the second plurality of pixel rows; generating a third code based on the first code and the second code; and encoding the first code, the second code and the third code into the remaining row of pixels.

[0005] In one embodiment, generating the first code includes: extracting first pixel data from the first plurality of pixel rows; and hashing the first pixel data using a first hashing function to generate a first hash code.

[0006] In one embodiment, the encoding method further includes: selecting a first character of the first hash code; randomly selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets, wherein each character in the first randomly-ordered character set is assigned a position code; matching the first character of the first hash code to a corresponding character in the first randomly ordered character set; and replacing the first character of the first hash code with a character from a reference character set at the position code of the corresponding character in the first randomly-ordered character set.

[0007] In one embodiment, the encoding method further includes: selecting a next character of the first hash code; matching the next character of the first hash code to a corresponding character in a next randomly ordered character set; replacing the next character of the first hash code with a character from the reference character set at the position code of the corresponding character in the next randomly ordered character set; and repeating the operations until the first hash code is exhausted, wherein the first code is generated.

[0008] In one embodiment, overlaying the second plurality of pixel rows with an image representing the first code includes: initializing each pixel in the second plurality of pixel rows; partitioning the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows; and mapping an image of the first code to the first subset of pixels.

[0009] In one embodiment, the encoding method further includes collecting metadata and encoding the metadata into the second subset of pixel rows, where encoding the metadata includes: selecting a first character of the metadata for encoding; selecting a first randomly-ordered character set from the ordered plurality of randomly ordered-character sets, wherein each character in the randomly ordered character set is assigned a position code; matching the first character of the metadata to a corresponding character in the next randomly-ordered character set; converting the position code of the corresponding character in the next randomly-ordered character set into a three-digit base-n number; and encoding a first pixel in the second subset of pixel rows with an RGB color code comprising the three-digit base-n number.

[0010] In one embodiment, encoding the metadata further includes: selecting a next character of the metadata for encoding; selecting a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets; matching the next character of the metadata to a corresponding character in the next randomly-ordered character set; converting the position code of the corresponding character in the next randomly-ordered character set into a next three-digit base-n number; encoding a next pixel in the second subset of pixel rows with an RGB color code comprising the next three-digit base-n number; and repeating the operations until the metadata is exhausted. In one embodiment, any remaining pixels in the second plurality of pixel rows with random RGB color codes based on random 3-digit base-n numbers.

[0011] In one embodiment, generating the second code includes extracting second pixel data from the second plurality of pixel rows and hashing the second pixel data using a second hashing function to generate the second code.

[0012] In one embodiment, encoding the first code, the second code and the third code into the remaining row of pixels includes: encoding each pixel of the remaining row of pixels with RGB color codes based on random 3-digit base-n numbers; reserving a first subset of pixels of the remaining row of pixels for the third code; encoding the first code, the second code and the position codes as 3-digit base-n RGB color codes into predetermined pixel locations in the remaining row of pixels; excluding the first subset of pixels, hashing the pixel data of the remaining line using a third hashing function to generate the third code; and encoding the third code into the first subset of pixels as 3-digit base-n RGB color codes.

[0013] In one embodiment, a method for authenticating a digital image includes: receiving a digital image comprising a plurality of pixel rows; partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining row of pixels; extracting a first code from a first subset of pixel locations in the remaining row of pixels; excluding the first subset of pixel locations, extracting first pixel data from all other pixels in the remaining row of pixels; hashing the first pixel data using a first hashing function to generate a first comparison code; and comparing the first code to the first comparison code to determine if the remaining row of pixels has been altered.

[0014] In one embodiment, the authentication method further includes extracting a second code from a second subset of pixels in the remaining row of pixels; extracting second pixel data from the second plurality of pixel rows; hashing the second pixel data using a second hashing

function to generate a second comparison code; and comparing the second code to the second comparison code to determine if the second plurality of pixel rows has been altered.

[0015] In one embodiment, the authentication method further includes: extracting a third code from a third subset of pixels in the remaining row of pixels; extracting third pixel data from the first plurality of pixel rows; hashing the third pixel data using a third hashing function to generate a third comparison code; and comparing the third code to the third comparison code to determine if the first plurality of pixel rows has been altered.

[0016] In one embodiment, the authentication method further includes: extracting position codes from a fourth subset of pixels in the remaining row of pixels; decoding the position codes to obtain an index to a first randomly-ordered character set in an ordered plurality of randomly-ordered character sets, wherein each character in the randomly ordered character sets is assigned a position code; partitioning the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows; extracting pixel data from the second subset of pixel rows; and decoding metadata from the second subset of pixel rows.

[0017] In one embodiment, decoding the metadata may include: decoding a first pixel of the second subset of pixel rows to obtain a first position code; selecting the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets based on the index; selecting a character in the first randomly-ordered character set at the first position code; decoding a next pixel of the second subset of pixel rows to obtain a next position code; selecting a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets; selecting a character in the next randomly-ordered character set at the next position code; and repeating the operations until the metadata is exhausted.

[0018] Other disclosed embodiments include apparatus and computer program products for performing the encoding and authentication methods.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] Various disclosed embodiments are illustrated by way of example, and not of limitation, by referring to the accompanying drawings, in which:

[0020] FIG. 1 illustrates an exemplary image encoding apparatus;

[0021] FIG. 2 illustrates an exemplary image authentication apparatus

[0022] FIG. 3 illustrates an exemplary processor and memory system that can be configured to implement elements of the exemplary image encoding apparatus of FIG. 1 and the exemplary image authentication apparatus of FIG. 2;

[0023] FIG. 4 illustrates an exemplary digital image and its associated metadata;

[0024] FIG. 5 is a flowchart illustrating an exemplary method for encoding a digital image;

[0025] FIG. 6 is a flowchart illustrating an exemplary method for generating a code;

[0026] FIG. 7 illustrates a method for selecting character sets for encoding image data;

[0027] FIG. 8 further illustrates an exemplary method for encoding image data;

[0028] FIG. 9 illustrates an exemplary encoded image;

[0029] FIG. 10 is a flowchart further illustrating an exemplary method for encoding image data;

[0030] FIG. 11 illustrates an exemplary segment of an encoded image;

[0031] FIG. 12 is a flowchart illustrating an exemplary method for encoding metadata;

[0032] FIG. 13 is a flowchart illustrating an exemplary method for further encoding a digital image;

[0033] FIGS. 14A and 14B illustrate another exemplary segment of an encoded image;

[0034] FIG. 15 is a flowchart illustrating an exemplary method for authenticating an encoded digital image;

[0035] FIG 16 is a flowchart further illustrating the exemplary method for authenticating an encoded digital image;

[0036] FIG. 17 is flowchart further illustrating the exemplary method for authenticating an encoded digital image;

[0037] FIG. 18 is a flowchart further illustrating the exemplary method for authenticating an encoded digital image; and

[0038] FIG. 19 is a flowchart illustrating an exemplary method for verifying metadata.

DETAILED DESCRIPTION

[0039] In the following description, for purposes of explanation and not limitation, details and descriptions are set forth in order to provide a thorough understanding of the various disclosed embodiments. However, it will be apparent to those skilled in the art that the various embodiments may be practiced in other embodiments that depart from these details and descriptions.

[0040] As used herein, the terms “component,” “module,” “system” and the like are intended to refer to a computer-related entity, either hardware, firmware, a combination of hardware and software, software, or software in execution. For example, a component may be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program and/or a computer. By way of illustration, both an application running on a computing device and the computing device can be a component. One or more components can reside within a process and/or thread of execution and a component may be localized on one

computer and/or distributed between two or more computers. In addition, these components can execute from various computer readable media having various data structures stored thereon.

The components may communicate by way of local and/or remote processes such as in accordance with a signal having one or more data packets (e.g., data from one component interacting with another component in a local system, distributed system, and/or across a network such as the Internet with other systems by way of the signal).

[0041] Various aspects, embodiments or features will be presented in terms of systems that may include a number of devices, components, modules, and the like. It is to be understood and appreciated that the various systems may include additional devices, components, modules, and so on, and/or may not include all of the devices, components, modules and so on, discussed in connection with the figures. A combination of these approaches may also be used.

[0042] Additionally, in the subject description, the word “exemplary” is used to mean serving as an example, instance or illustration. Any embodiment or design described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments or designs. Rather, use of the word exemplary is intended to present concepts in a concrete manner.

[0043] It will be appreciated that for ease of explanation, digital image processing operations are described herein as operating “on” or “in” a digital image (e.g., encoding or decoding pixels, replacing rows of pixels, etc.). It will be understood by a person of ordinary skill in the art that such operations may be performed as file operations using data representations of the digital images that may be stored in memory and various data structures, image buffers, registers and the like.

[0044] Additionally, terms such as “random,” “random-selected,” “randomly-ordered” and the like are used throughout the following description. It will be appreciated that such terms may refer to random processes or pseudorandom processes, which are random-like but nevertheless deterministic. A process for selecting numbers or values may rely on a truly random physical phenomenon such as sampled electrical noise. Additionally, it is known in the art that a pseudorandom sequence of any arbitrary length, using any arbitrary set of numbers or characters, can be generated using registers, adders and feedback.

[0045] FIG. 1 is a block diagram of an exemplary digital image encoding apparatus 100. Apparatus 100 includes an image capture module 101, an image processing module 102 and an image storage module 103. Image capture module 101 may be any type of digital imaging device or system such as, for example, a digital camera or a smartphone or cellphone equipped with a digital camera. In certain embodiments, image capture module 101 may also include a GPS receiver to provide location information and wireless connectivity to time servers and or reverse geocode servers to provide GPS to address translation. Image processing module 102 may include hardware, software and firmware to manipulate a digital image from the image capture module 101 to encode the digital image according to the methods described herein. Image storage module 103 may be any type of digital storage device or medium capable of storing a digital image file. Image storage module 103 may also be wirelessly connected to other systems, such as remote file servers, so that encoded digital images may be transmitted to other locations for authentication.

[0046] FIG. 2 is a block diagram of an exemplary image authentication apparatus 200. Image authentication apparatus 200 includes an image receiving module 201 and an image authentication module 202. Image receiving module 201 may be any system or apparatus capable

of receiving a digital image file on a digital storage medium or via a wired or wireless connection, and providing the digital image file to image authentication module 202 for subsequent processing, including the image authentication methods described herein.

[0047] FIG. 3 is a block diagram of a system 300 that may be used to implement any of modules 101, 102, 103, 201 and 202. System 300 includes a processor 301 and a memory 302. Memory 302 may include stored instructions for performing any of the operations for encoding and authenticating digital images described herein, and processor 301 may be configured to execute the stored instructions.

[0048] In one embodiment, a method for encoding a digital image begins by capturing the image with, for example, a smartphone. The image may have any preset resolution, but for the purpose of the present description, it is assumed that the image is a 600 pixel by 800 pixel RGB encoded image. That is, the image is 600 pixels wide and contains 800 rows of pixels. As is known in the art, each pixel may be encoded using three 8-bit bytes of data, one byte each for RED, GREEN and BLUE luminosity. This system provides for 256^3 or 16, 777,216 combinations. Conventionally, an RGB color code of (0,0,0) represents pure black (zero luminosity) while an RGB color code of (255,255,255) represents pure white of the highest luminosity. That convention will be used throughout the following description.

[0049] As will be described in greater detail below, embodiments of the encoding methodology employed herein uses a limited number of RGB color codes to embed a corresponding limited number of characters into a digital image. In particular, the limited number of characters may be encoded into the “lowest” RGB color codes. For example, if the character set is a standard 128 character ASCII character set, then all 128 characters could be coded with RGB color codes from (0,0,1) through (0,0,128) in base 10. However this coding

scheme would produce pixels with no RED or BLUE luminosity and steadily increasing GREEN luminosity (up to 50% of maximum) with higher numbered character codes. Such coding could easily be visually perceived by a human observer, revealing an aspect of the encoding scheme.

[0050] Alternatively, the decimal character codes can be expressed in a lower base numbering system. For example, a three-digit base-n numbering system is capable of coding n^3 codes. For $n=5$, it is possible to uniquely code up to 125 characters in base-5 RGB color codes from $(0,0,0)_5$ to $(4,4,4)_5$, or 124 codes from $(0,0,1)_5$ through $(4,4,4)_5$ where the subscript 5 indicates the base. Accordingly, all but 4 of the standard ASCII characters can be encoded into RGB color codes in a base 5 numbering system and, advantageously, will be indistinguishable from black to the naked eye at such low intensities. It will be appreciated that lower or higher base number may be used to accommodate lower or higher numbers of characters.

[0051] As will be described in greater detail below, embodiments of the encoding methodology employed herein also use hashing functions operating on image data to generate multiple hash codes. Hash functions are known in the art and accordingly are not described in detail. A hash function is any function that can be used to map data of arbitrary size to data of fixed size, with slight differences in input data producing very big differences in output data. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. Hash values are commonly used to differentiate between data.

[0052] A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or simply digest. The ideal cryptographic hash function has four main properties: (1) it is easy to compute

the hash value for any given message, (2) it is infeasible to find a message that has a given hash, (3) it is infeasible to modify a message without changing its hash, and (4) it is infeasible to find two different messages with the same hash.

[0053] It is also known in the art that any “message” may be “salted” before it is hashed in order to provide additional security. A salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. The salt may be prepended, appended or interspersed within the message.

[0054] FIG. 4 is a simple representation of a captured digital image 400 having a width of W pixels and a height of H pixel rows, where the actual content of the image is not shown. As illustrated in FIG. 4, digital image 401 may be divided into three “working” areas: a first plurality of pixel rows, a second plurality of pixel rows, and a remaining row of pixels. While FIG. 4 illustrates the three working areas in an exemplary physical order, the arrangement is arbitrary. For example, the second plurality of pixel rows could be located at the top of the image and the remaining row of pixels could be located between the first plurality of pixel rows and the second plurality of pixel rows. Additionally, the remaining row could be more than one row. By way of example for the present description, it will be assumed that the width of the image W is 600 pixels, the height H of the image is 800 rows of pixels, the first plurality of pixel rows is 768 rows and the second plurality of pixel rows is 31 rows (leaving one remaining row).

[0055] The digital image 401 may be accompanied by metadata 402. For example, if the image encoding apparatus 100 includes GPS capability, the metadata 402 may include the GPS coordinates where the digital image was captured. The metadata 402 may also include a GPS accuracy (e.g., if an enhanced GPS service is available), a date and time from a time server or a local clock, a date and time source name if the date and time data is obtained from a server, a

device ID, a device operating system and version, a user ID, an organization ID, an assigned group name, and a reverse geocoded address if such a service is available to the image encoding apparatus via a wireless connection such as a cellular connection or a WiFi connection.

[0056] In one embodiment, some or all of the metadata may be used to overwrite portions of the first plurality of pixel rows as illustrated in FIG. 9 (which also illustrates the second plurality of pixels and the remaining row of pixels after encoding as described below).

[0057] FIG. 5 is a flowchart 500 illustrating an exemplary method for encoding a digital image. In operation 501, a digital image is captured, for example a 600x800 pixel image as described above. In operation 502, the digital image is partitioned into three working areas; a first plurality of pixels (e.g., 768 rows), a second plurality of pixel rows (e.g., 31 rows) and a remaining row of pixels (e.g., 1 row). In operation 503, a first code is generated from the first plurality of pixels as illustrated in FIG. 6.

[0058] FIG. 6 is a flowchart 600 illustrating an exemplary method for generating the first code. In operation 601, pixel data (first pixel data) is extracted from the first plurality of pixels. For example, the 3-byte RGB data from each pixel may be extracted to a data buffer for subsequent operations. In operation 602, the first pixel data is hashed using a first hashing function to generate a first hash code. In operation 603, a first character of the first hash code is selected for encoding.

[0059] Aspects of character encoding include the use of a rotating buffer structure as illustrated in FIGS. 7 and 8. The rotating buffer 701 illustrated in FIG. 7 consists of m randomly-ordered character sets, each containing the same N number of characters (i.e., each character set includes the same set of characters in a random order). In one embodiment, each character set may contain $N=88$ randomly-ordered characters based on a reference character set and m may be

256. Each character in the reference character set has a position code from 1 to N and each character in each of the m randomly-ordered character sets also has a position code from 1 to N. It will be appreciated that because the character sets are randomized, the same character in two different character sets will typically have different position codes. An exemplary 88 character reference character set 702 is illustrated in FIG. 7. As a first encoding step, an index is calculated to select one of the m randomly-ordered character sets for encoding the first character of the first hash code. In one embodiment, R position codes (703) from 1 to N may be randomly selected as illustrated in FIG. 7. In the example illustrated, R=10 and the randomly selected position codes are {32, 50, 59, 22, 42, 80, 71, 67, 48, 88}. These position codes may be summed modulo m to obtain an index (704) to the character set that will be used to encode the first character of the first hash code. In the example illustrated in FIG. 7, m=256 and the summation modulo m = 47. Accordingly, the index r=47 and the 47th character set in the rotating buffer is selected to encode the first character in the first hash code. As each subsequent character in the first hash code is selected for encoding, the index is increased by 1 to select the next character set in the buffer. This sequence is illustrated in FIG. 7 for the first three characters of the first hash code.

[0060] An exemplary encoding process is illustrated in FIG. 8. For the example illustrated in FIG. 8, the first hash code is assumed to be a 7-character hash code consisting of the characters {h, A, i, L, X, g, A}. The encoding process proceeds as follows. The first character in the first hash code (h) is located in the starting character set S(47) at position k=57. In the reference character set, position 57 is occupied by the character (u). Accordingly, the (h) is encoded as a (u), which can subsequently be encoded as a base-5 RGB color code of (2,1,2). The second character in the first hash code (A) is located in the next character set S(48) at position k=23. In

the reference character set, position 23 is occupied by the character (M). Accordingly, the (A) is encoded as an (M), which can subsequently be encoded as a base-5 RGB color code of (0,4,3). The third character in the first hash code (i) is located in the next character set S(49) at position k=72. In the reference character set, position 72 is occupied by the character (?). Accordingly, the (i) is encoded as a (?), which can subsequently be encoded as a base-5 RGB color code of (2,4,2). The fourth character in the first hash code (L) is located in the next character set S(50) at position k=25. In the reference character set, position 25 is occupied by the character (O). Accordingly, the (L) is encoded as an (O), which can subsequently be encoded as a base-5 RGB color code of (1,0,0). Similarly, the remaining characters {X, g, A} in the first hash code are encoded as (8), (;) and (#) by using character sets S(51), S(52), and S(53), respectively.

[0061] Returning now to FIG. 6, operations 603-608 encompass the processes described above. In operation 603, a first randomly-ordered character set is randomly selected from an ordered plurality of randomly ordered-character sets, wherein each character in the first randomly-ordered character set is assigned a position code. In operation 604, the first character of the first hash code is matched to a corresponding character in the first randomly ordered character set. In operation 605, the first character of the first hash code is replaced with a character from a reference character set at the position code of the corresponding character in the first randomly-ordered character set. Operation 606 begins an iterative process wherein a next character in the first has code is selected for encoding; In operation 607, the next character of the first hash code is matched to a corresponding character in a next randomly ordered character set. In operation 608, the next character of the first hash code is replaced with a character from the reference character set at the position code of the corresponding character in the next randomly

ordered character set. Operations 606-608 are repeated until all of the characters in the first hash code have been encoded, therefore generating the first code.

[0062] It will be appreciated that additional operations may be performed on the first code to provide additional levels of encoding and encryption. For example, the encoded characters in the first code may be translated and/or transposed according to a predetermined algorithm. Such algorithms are known in the art and, accordingly, are not described in detail herein.

[0063] Returning now to FIG. 5, the exemplary method for encoding a digital image continues in one embodiment at operation 504 where a second code is generated from the second plurality of pixel rows. Operation 504 is expanded in FIG. 10, in a flowchart 1000 illustrating an exemplary method for generating the second code. In a preliminary operation 1001, each pixel in the second plurality of pixel rows may be initialized to a predetermined value, such as RGB color code (0,0,0) to render the pixels pure black. Next, in operation 1002, the second plurality of pixel rows is partitioned into a first subset of pixel rows and a second subset of pixel rows. Continuing the example from above, where the second plurality of pixel rows includes 31 pixel rows, the first subset of pixel rows may include a contiguous 27 rows and the second subset may include the remaining four rows, which may be distributed in any convenient manner above, below or both above and below the first subset. Next, in operation 1003, the second plurality of pixel rows is overlaid with an image of the first code. Such an overwrite is illustrated in FIG. 11A for the exemplary case where the first code comprises a 20-character encoded hash code (e.g., CA966180FBB7C0DF5EAF in the example of FIG. 11A) generated using the method illustrated in FIG. 8. Methods for overwriting digital image files with characters are known in the art and are not described in detail herein. Generally understood methods include initializing a field of pixels (e.g., the second plurality of pixels) to an initial color (e.g., RGB (0,0,0) for black) and

then using a character generator to map characters to the initialized field with a contrasting color (e.g., RGB (255,255,255) for white).

[0064] FIG. 11B graphically illustrates the partitioning of the second plurality of pixel rows 1101 into the first subset 1102 and the second subset 1103A and 1103B. Next, in operation 1004, some or all of the metadata 402 may be encoded into the second subset of pixels, as illustrated in FIG.12.

[0065] FIG. 12 is a flowchart 1200 illustrating an exemplary method for encoding the metadata 402 into the second plurality of pixels, which method closely parallels the previously described method for encoding the first hash code. The method begins at operation 1201, where a first character of the metadata is selected for encoding. In operation 1202, a randomly-ordered character set from the ordered plurality of randomly ordered-character sets is selected based on the index r , wherein each character in the randomly ordered character set is assigned a position code.

[0066] In operation 1203, the first character of the metadata is matched to a corresponding character in the next randomly-ordered character set. In operation 1204, the position-based code of the corresponding character in the first randomly-ordered character set is converted into a three-digit base- n number (e.g., a 3-digit base-5 number). In operation 1205, a first pixel in the second subset of pixel rows is encoded with an RGB color code comprising the three-digit base- n number.

[0067] In operation 1206, a next character of the metadata is selected for encoding. In operation 1207, a next randomly-ordered character set is selected from the ordered plurality of randomly ordered-character sets. In operation 1208, the next character of the metadata is matched to a corresponding character in the next randomly-ordered character set. In operation

1209, the position-based code of the corresponding character in the next randomly-ordered character set is converted into a next three-digit base-n number. In operation 1210, a next pixel in the second subset of pixel rows is encoded with an RGB color code comprising the three-digit base-n number. These operations are iterated until the metadata is exhausted (operation 1211), wherein any remaining unencoded pixels in the second subset of pixels are randomized by encoding the pixels with random 3-digit base-n RGB color codes.

[0068] Returning to FIG. 10, the next operation for generating the second code is operation 1005, where any remaining unencoded pixels in the second plurality of pixel rows are randomized by encoding the pixels with random 3-digit base-n RGB color codes. In operation 1006, pixel data (second pixel data) from the second plurality of pixel rows is extracted and, in operation 1007, the second pixel data is hash using a second hashing function to generate the second code. As in the case of the first code, the second code may be further encoded and/or encrypted using predetermined translation and transposition algorithms as are known in the art.

[0069] Returning now to FIG. 5, the next operations in encoding the digital image 401 is operation 505, where a third code is generated based on the first code and the second code, and operation 506, where the first code, the second code and the third code are encoded into the remaining row of pixels. Operations 505 and 506 are expanded in FIG. 13.

[0070] FIG. 13 is a flowchart 1300 illustrating the generation of the third code and the encoding of the remaining row of pixels. In operation 1301, all pixels in the remaining row are encoded with RGB color codes based on random 3-digit base-n numbers (e.g., base-5). In operation 1302, a first subset of pixels is reserved in the remaining row of pixels for the third code, where a hashing function with a known output length is predetermined (e.g., a 20 character output). In operation 1303, the first code, the second code and the R position codes are encoded

as 3-digit base-n RGB color codes into predetermined pixel locations in the remaining row of pixels. The configuration of the remaining row after operation 1303 is illustrated in FIG. 14, where the width of the remaining line is W pixels, the length of the first code is L1, the length of the second code is L2, and the length of the third code will be L3. In an exemplary embodiment, W=600, R=10, and L1=L2=L3=20, such that the first 530 pixels of the remaining row are encoded with random, base-n RGB color codes. It will be appreciated that the codes may be encoded in any locations. All that is required is that the authentication algorithm (described below) is aware of the locations. Returning to FIG. 13, in operation 1304, a concatenated string of pixel data comprising the coded values of the R position codes, the L1 first code characters, the L2 second code characters and the random characters, are hashed using a third hashing function to generate the third code. In operation 1305, the L3 characters of the third code are encoded into the reserved pixels of the remaining row as 3-digit base-n RGB color codes. FIG. 14B illustrates the configuration of the remaining row of pixels after operation 1305 is completed. FIG. 9 illustrates an exemplary digital image that has been encoded according to the methods described above.

[0071] FIGS. 14, 15 and 16 illustrate exemplary methods that may be performed by the authentication apparatus 200 for authenticating digital images that have been encoded using the methods described above. It will be appreciated that the authentication process relies on a priori knowledge of the hashing functions, the reference character set, the ordering of the character sets in the rotating buffer, the number and location of pixel rows in the second plurality of pixel rows and the remaining row of pixels, and the lengths and locations in the remaining row of the R position codes, the L1 characters in the first code, the L2 characters in the second code, and the L3 characters in the third code.

[0072] FIG. 15 is a flowchart 1500 illustrating the use of the third code to authenticate the digital image. In operation 1501, the encoded digital image is received by the image receiving module 201 and delivered to the image authentication module 202. In operation 1502, the authentication module 202 partitions the digital image into the first plurality of pixel rows, the second plurality of pixel rows and the remaining row as illustrated in FIG. 4. In operation 1503, the third code (a first code in the authentication process) is extracted from its location in the remaining row of pixels (a first subset of pixel locations in the authentication process). Next, in operation 1504, the encoded data from all other pixels in the remaining row are extracted as first pixel data. In operation 1505, the first pixel data is hashed using the third hashing function (first hashing function in the authentication process) to generate a first comparison code. In operation 1506, the third code and the first comparison code are compared to determine if the remaining row of pixels has been altered.

[0073] FIG. 16 is a flowchart 1600 illustrating the use of the second code to authenticate the digital image. In operation 1601, the second code is extracted from its location in the remaining row of pixels (a second subset of pixels locations in the authentication process). Next, in operation 1602, the pixel data from the second plurality of pixel rows is extracted as second pixel data. In operation 1603, the second pixel data is hashed using the second hashing function to generate a second comparison code. In operation 1604, the second code is compared with the second comparison code to determine if the second plurality of pixel rows has been altered.

[0074] FIG. 17 is a flowchart 1700 illustrating the use of the first code to authenticate the digital image. In operation 1701 the first code (third code in the authentication process) is extracted from its location in the remaining row of pixels (third subset of pixels in the authentication process). In operation 1702, pixel data from the first plurality of pixel rows is

extracted as third pixel data in the authentication process. In operation 1703, the third pixel data is hashed using the first hashing function (third hashing function in the authentication process) to generate a third comparison code. In operation 1704, the first code is compared to the third comparison code to determine if the first plurality of pixel rows has been altered.

[0075] In one embodiment, if alteration to the first or second plurality of pixel rows is detected, it is possible to determine if the alteration has tampered with the overlaid metadata in the first plurality of pixel rows or with the encoded metadata in the second plurality of pixel rows. FIGS. 18 and 19 illustrate how this process is conducted.

[0076] FIG. 18 is a flowchart 1800 illustrating an exemplary method for extracting metadata from the second plurality of pixel rows. The method begins with operation 1801, where the R position codes are extracted from their location in the remaining row of pixels (fourth subset of pixels in the authentication process). In operation 1802, the position codes are decoded to obtain the R position codes, and the position codes are summed modulo m to obtain the index r to the first randomly-ordered character set used to encode the metadata during the encoding process described above. In operation 1803, the second plurality of pixel rows is partitioned into the first subset of pixel rows in the second plurality of pixel rows, and the second subset of pixel rows in the second subset of pixel rows. In operation 1804, pixel data (containing the encoded metadata) is extracted from the second subset of pixel rows. In operation 1805, the metadata is decoded as detailed in FIG. 19.

[0077] FIG. 19 is a flowchart 1900 illustrating an exemplary method for decoding the metadata. In operation 1901, a first pixel of the metadata is decoded to obtain a first position code. In operation 1902, the first randomly-ordered character set is selected based on the index. In operation 1903, the character in the first randomly-ordered character set at the first position

code is selected. In operation 1904, a next pixel of the second subset of pixels is decoded to obtain a next position code. In operation 1905, a next randomly-ordered character set is selected, and in operation 1906, the character in the next randomly-ordered character set at the next position code is selected. The sequence of operations 1904-1906 is repeated until the metadata is exhausted (operation 1907). The end of the metadata may be detected when an end-of-data character is decoded from the second subset of pixels.

[0078] After the metadata is decoded it may be compared with the printed metadata in the first plurality of pixels to identify any differences in the two data sets.

[0079] It will be appreciated that the methods described herein, and their associated apparatus and computer program products may be modified by those of skill in the art while retaining the inventive features. For example, rather than recruiting rows from the original digital image for the second plurality of pixel rows and the remaining row of pixels by partitioning the original digital image, rows could be added to the original digital image to provide for the second plurality of pixel rows and the remaining row. In one embodiment, the second plurality of rows could be omitted entirely, such that the remaining row is encoded with the first code and the third code, but not the second code.

[0080] It is to be understood that the embodiments and features that are described herein may be implemented by hardware, software, firmware or any combination thereof. Various embodiments described herein are described in the general context of methods or processes, which may be implemented in one embodiment by a computer program product, embodied in a computer-readable medium, including computer-executable instructions, such as program code, executed by computers in networked environments. As noted above, a memory and/or a computer-readable medium may include removable and non-removable storage devices

including, but not limited to, Read Only Memory (ROM), Random Access Memory (RAM), compact discs (CDs), digital versatile discs (DVD) and the like. Therefore, the disclosed embodiments can be implemented on non-transitory computer readable media. When implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code means in the form of instructions or data structures and that can be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor.

[0081] Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

[0082] Generally, program modules may include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps or processes.

[0083] The various illustrative logics, logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but, in the alternative, the processor may be any conventional processor, controller, microcontroller or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration. Additionally, at least one processor may comprise one or more modules operable to perform one or more of the steps and/or actions described above.

[0084] For a software implementation, the techniques described herein may be implemented with modules (*e.g.*, procedures, functions and so on) that perform the functions described herein. The software codes may be stored in memory units and executed by processors. The memory unit may be implemented within the processor and/or external to the processor, in which case it can be communicatively coupled to the processor through various means as is known in the art.

Further, at least one processor may include one or more modules operable to perform the functions described herein.

[0085] Moreover, various aspects or features described herein may be implemented as a method, apparatus or article of manufacture using standard programming and/or engineering techniques. The term "article of manufacture" as used herein is intended to encompass a computer program accessible from any computer-readable device, carrier or media. For example, computer-readable media can include but are not limited to magnetic storage devices (*e.g.*, hard disk, floppy disk, magnetic strips, *etc.*), optical disks (*e.g.*, compact disk (CD), digital versatile disk (DVD), *etc.*), smart cards, and flash memory devices (*e.g.*, EPROM, card, stick, key drive, *etc.*). Additionally, various storage media described herein can represent one or more devices and/or other machine-readable media for storing information. The term "machine-readable medium" can include, without being limited to, wireless channels and various other media capable of storing, containing, and/or carrying instruction(s) and/or data. Additionally, a computer program product may include a computer readable medium having one or more instructions or codes operable to cause a computer to perform the functions described herein.

[0086] Further, the steps and/or actions of a method or algorithm described in connection with the aspects disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, a hard disk, a removable disk, a CD-ROM or any other form of storage medium known in the art. An exemplary storage medium may be coupled to the processor, such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. Further, in some embodiments, the processor and the

storage medium may reside in an ASIC. Additionally, in some embodiments, the steps and/or actions of a method or algorithm may reside as one or any combination or set of codes and/or instructions on a machine readable medium and/or computer readable medium, which may be incorporated into a computer program product.

[0087] While the foregoing disclosure discusses illustrative embodiments, it should be noted that various changes and modifications could be made herein without departing from the scope of the described embodiments as defined by the appended claims. Accordingly, the described embodiments are intended to embrace all such alterations, modifications and variations that fall within scope of the appended claims. Furthermore, although elements of the described embodiments may be described or claimed in the singular, the plural is contemplated unless limitation to the singular is explicitly stated. Additionally, all or a portion of any embodiment may be utilized with all or a portion of any other embodiments, unless stated otherwise.

[0088] To the extent that the term “includes” is used in either the detailed description or the claims, such term is intended to be inclusive in a manner similar to the term “comprising” as “comprising” is interpreted when employed as a transitional word in a claim. Furthermore, the term “or” as used in either the detailed description or the claims is intended to mean an inclusive “or” rather than an exclusive “or.” That is, unless specified otherwise, or clear from the context, the phrase “X employs A or B” is intended to mean any of the natural inclusive permutations. That is, the phrase “X employs A or B” is satisfied by any of the following instances: X employs A; X employs B; or X employs both A and B. In addition, the articles “a” and “an” as used in this application and the appended claims should generally be construed to mean “one or more” unless specified otherwise or clear from the context to be directed to a singular form.

We Claim:

1. A method for encoding a digital image, comprising:
 - capturing a digital image comprising a plurality of pixel rows;
 - partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row;
 - generating a first code from the first plurality of pixel rows;
 - overlaying the second plurality of pixel rows with an image representing the first code and embedding the second plurality of pixel rows with metadata;
 - generating a second code from the second plurality of pixel rows;
 - generating a third code based on the first code and the second code; and
 - encoding the first code, the second code and the third code into the remaining row of pixels, wherein encoding the first code, the second code, or the third code into the remaining row of pixels comprises:
 - collecting the metadata in a character string;
 - selecting a first character of the metadata for encoding;
 - selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets based on an index for the first randomly-ordered character set, wherein each character in the first randomly ordered character set is assigned a position code;
 - matching the first character of the metadata to a corresponding character in the first randomly-ordered character set;
 - converting the position code of the corresponding character in the first randomly-ordered character set into a three-digit base-n number; and
 - encoding a first pixel in the remaining row of pixels with an RGB color code comprising the three-digit base-n number.

2. The method of claim 1, wherein generating the first code comprises:
 - extracting first pixel data from the first plurality of pixel rows; and
 - hashing the first pixel data using a first hashing function to generate a first hash code.

3. The method of claim 2, further comprising:

selecting a first character of the first hash code;

randomly selecting the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets, wherein each character in the first randomly-ordered character set is assigned the position code;

matching the first character of the first hash code to a corresponding character in the first randomly ordered character set; and

replacing the first character of the first hash code with a character from a reference character set at the position code of the corresponding character in the first randomly-ordered character set.

4. The method of claim 3, further comprising:

selecting a next character of the first hash code;

matching the next character of the first hash code to a corresponding character in a next randomly ordered character set;

replacing the next character of the first hash code with a character from the reference character set at the position code of the corresponding character in the next randomly ordered character set; and

repeating operations (a) through (c) until the first hash code is exhausted, wherein the first code is generated.

5. The method of claim 3, wherein randomly selecting the first randomly-ordered character set comprises randomly selecting R position codes, wherein a summation of the R position codes modulo m provides an index to the first randomly-ordered character set, wherein m is the number of randomly-ordered character sets.

6. The method of claim 2, wherein the digital image is overlaid with identifying information before extracting the pixel data from the first plurality of pixel rows, wherein the identifying information comprises one or more of a date and time stamp, a user name, GPS coordinates, a street address, a device name, an operating system name and version, and a watermark.

7. The method of claim 4, wherein overlaying the second plurality of pixel rows with an image representing the first code comprises:

initializing each pixel in the second plurality of pixel rows;

partitioning the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows; and

mapping an image of the first code to the first subset of pixels.

8. The method of claim 7,

wherein the metadata comprises one or more of GPS coordinates, a GPS accuracy, a date and time, a date and time source name, a device ID, a device operating system and version, a user ID, an organization ID, an assigned group name, and a reverse geocoded address; the method further comprising:

encoding the metadata into the second subset of pixel rows.

9. The method of claim 8, wherein encoding the metadata into the second subset of pixel rows comprises:

encoding a first pixel in the second subset of pixel rows with the RGB color code comprising the three-digit base-n number.

10. The method of claim 9, further comprising:

(a) selecting a next character of the metadata for encoding;

(b) selecting a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets;

(c) matching the next character of the metadata to a corresponding character in the next randomly-ordered character set;

(d) converting the position code of the corresponding character in the next randomly-ordered character set into a next three-digit base-n number;

(e) encoding a next pixel in the second subset of pixel rows with an RGB color code comprising the next three-digit base-n number;

(f) repeating steps (a) through (e) until the metadata is exhausted; and

(g) encoding an end-of-data character.

11. The method of claim 10, further comprising encoding any remaining pixels in the second subset of pixel rows with random RGB color codes based on random three-digit base-n numbers.

12. The method of claim 11, wherein generating the second code from the second plurality of pixel rows comprises:
extracting second pixel data from the second plurality of pixel rows; and
hashing the second pixel data using a second hashing function to generate the second code.

13. The method of claim 12, further comprising:
encoding each pixel of the remaining row of pixels with RGB color codes based on random 3-digit base-n numbers;
reserving a first subset of pixels of the remaining row of pixels for the third code;
encoding the first code, the second code and the position codes as 3-digit base-n RGB color codes into predetermined pixel locations in the remaining row of pixels;
excluding the first subset of pixels in the remaining row, hashing the pixel data of the remaining line using a third hashing function to generate the third code; and
encoding the third code into the first subset of pixels as 3-digit base-n RGB color codes.

14. The method of claim 2, further comprising salting the first pixel data with a first salt before hashing the first pixel data.

15. The method of claim 2, further comprising translating and transposing characters of the first code after hashing the first pixel data.

16. The method of claim 12, further comprising salting the second pixel data with a second salt before hashing the second pixel data.

17. The method of claim 12, further comprising translating and transposing characters of

the second code after hashing the second pixel data.

18. The method of claim 13, further comprising translating and transposing characters of the third code before encoding the third code into the first subset of pixels.

19. A method for encoding and authenticating digital images,
(1) wherein encoding comprises:

capturing a digital image comprising a plurality of pixel rows;
partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row;

generating a first encoding code from the first plurality of pixel rows;
overlaying the second plurality of pixel rows with an image representing the first encoding code and embedding the second plurality of pixel rows with metadata;

generating a second encoding code from the second plurality of pixel rows;
generating a third encoding code based on the first encoding code and the second encoding code; and

encoding the first encoding code, the second encoding code and the third encoding code into the remaining row of pixels, wherein encoding the first encoding code, the second encoding code, or the third encoding code into the remaining row of pixels comprises:

collecting the metadata in a character string;
selecting a first character of the metadata for encoding;
selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets based on an index for the first randomly-ordered character set, wherein each character in the first randomly ordered character set is assigned a position code;

matching the first character of the metadata to a corresponding character in the first randomly-ordered character set;

converting the position code of the corresponding character in the first randomly-ordered character set into a three-digit base-n number; and

encoding a first pixel in the remaining row of pixels with an RGB color code comprising the three-digit base-n number; and

(2) wherein authenticating comprises:

extracting a first authentication code from a first subset of pixel locations in the remaining row of pixels; excluding the first subset of pixel locations in the remaining row, extracting first pixel data from all other pixels in the remaining row of pixels;
hashing the first pixel data using a first hashing function to generate a first comparison code; and
comparing the first authentication code to the first comparison code to determine if the remaining row of pixels has been altered.

20. The method of claim 19, further comprising:

extracting a second authentication code from a second subset of pixels in the remaining row of pixels; extracting second pixel data from the second plurality of pixel rows;

hashing the second pixel data using a second hashing function to generate a second comparison code; and

comparing the second authentication code to the second comparison code to determine if the second plurality of pixel rows has been altered.

21. The method of claim 19, further comprising:

extracting a third authentication code from a third subset of pixels in the remaining row of pixels; extracting third pixel data from the first plurality of pixel rows;

hashing the third pixel data using a third hashing function to generate a third comparison code; and

comparing the third authentication code to the third comparison code to determine if the first plurality of pixel rows has been altered.

22. The method of claim 20, further comprising:

extracting position codes from a fourth subset of pixels in the remaining row of pixels;

decoding the position codes to obtain the index to the first randomly-ordered character set in the ordered plurality of randomly-ordered character sets, wherein each character in the randomly ordered character sets is assigned a position code;

partitioning the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows;

extracting pixel data from the second subset of pixel rows; and decoding metadata from the second subset of pixel rows.

23. The method of claim 22, wherein decoding the metadata from the second subset of pixel rows comprises:

decoding a first pixel of the second subset of pixel rows to obtain a first position code; selecting the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets based on the index; and

selecting a character in the first randomly-ordered character set at the first position code.

24. The method of claim 23, further comprising:

(a) decoding a next pixel of the second subset of pixel rows to obtain a next position code;

(b) selecting a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets;

(c) selecting a character in the next randomly-ordered character set at the next position code; and

(d) repeating operations (a) through (c) until an end-of-data character is decoded.

25. An apparatus for encoding a digital image, comprising:
a processor; and

a memory comprising processor executable code that, when executed by the processor, configures the apparatus to:

capture a digital image comprising a plurality of pixel rows;

partition the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row;

generate a first code from the first plurality of pixel rows;

overlay the second plurality of pixel rows with an image representing the first code and embed the second plurality of pixel rows with metadata;

generate a second code from the second plurality of pixel rows; generate a third code based on the first code and the second code; and

encode the first code, the second code and the third code into the remaining row of pixels, wherein encoding the first code, the second code, or the third code into the remaining row of pixels comprises:

collecting the metadata in a character string;

selecting a first character of the metadata for encoding;

selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets based on an index for the first randomly-ordered character set, wherein each character in the first randomly ordered character set is assigned a position code;

matching the first character of the metadata to a corresponding character in the first randomly-ordered character set;

converting the position code of the corresponding character in the first randomly-ordered character set into a three-digit base-n number; and

encoding a first pixel in the remaining row of pixels with an RGB color code comprising the three-digit base-n number.

26. The apparatus of claim 25, wherein to generate the first code, the apparatus is further configured to:

extract first pixel data from the first plurality of pixel rows; and

hash the first pixel data using a first hashing function to generate a first hash code.

27. The apparatus of claim 26, further configured to: select a first character of the first hash code;

randomly select the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets, wherein each character in the first randomly-ordered character set is assigned the position code;

match the first character of the first hash code to a corresponding character in a next randomly ordered character set; and

replace the first character of the first hash code with a character from a reference character set at the position code of the corresponding character in the first randomly-ordered character set.

28. The apparatus of claim 27, further configured to:

(a) select a next character of the first hash code;

(b) match the next character of the first hash code to a corresponding character in a next randomly ordered character set;

(c) replace the next character of the first hash code with a character from the reference character set at the position code of the corresponding character in the next randomly ordered character set; and

(d) repeat operations (a) through (c) until the first hash code is exhausted, wherein the first code is generated.

29. The apparatus of claim 27, wherein to randomly select the first randomly-ordered character set, the apparatus is further configured to randomly select R position codes, wherein a summation of the R position codes modulo m provides an index to the first randomly-ordered character set, wherein m is the number of randomly-ordered character sets.

30. The apparatus of claim 26, further configured to overlay the digital image with identifying information before extracting the pixel data from the first plurality of pixel rows, wherein the identifying information comprises one or more of a date and time stamp, a user name, GPS coordinates, a street address, a device name, an operating system name and version, and a watermark.

31. The apparatus of claim 28, wherein to overlay the second plurality of pixel rows with an image representing the first code, the apparatus is further configured to:

initialize each pixel in the second plurality of pixel rows;

partition the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows; and

map an image of the first code to the first subset of pixels.

32. The apparatus of claim 28,

wherein the metadata comprises one or more of GPS coordinates, a GPS accuracy, a date and time, a date and time source name, a device ID, a device operating system and version, a user ID, an organization ID, an assigned group name, and a reverse geocoded address; the apparatus further configured to:

encode the metadata into the second subset of pixel rows.

33. The apparatus of claim 32, wherein to encode the metadata into the second subset of pixel rows, the apparatus is further configured to:

encode a first pixel in the second subset of pixel rows with the RGB color code comprising the three-digit base-n number.

34. The apparatus of claim 33, further configured to:

(a) select a next character of the metadata for encoding;

(b) select a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets;

(c) match the next character of the metadata to a corresponding character in the next randomly-ordered character set;

(d) convert the position code of the corresponding character in the next randomly-ordered character set into a next three-digit base-n number;

(e) encode a next pixel in the second subset of pixel rows with an RGB color code comprising the three-digit base-n number;

(f) repeat steps (a) through (e) until the metadata is exhausted; and

(g) encode an end-of-data character.

35. The apparatus of claim 34, further configured to encode any remaining pixels in the second subset of pixel rows with random RGB color codes based on random three-digit base-n numbers.

36. The apparatus of claim 35, wherein to generate the second code from the second

plurality of pixel rows the apparatus is further configured to:

extract second pixel data from the second plurality of pixel rows; and

hash the second pixel data using a second hashing function to generate the second code.

37. The apparatus of claim 36, further configured to:

encode each pixel of the remaining row of pixels with RGB color codes based on random 3-digit base-n numbers;

reserve a first subset of pixels of the remaining row of pixels for the third code;

encode the first code, the second code and the position codes as 3-digit base-n RGB color codes into predetermined pixel locations in the remaining row of pixels;

exclude the first subset of pixels, and hash the pixel data of the remaining line using a third hashing function to generate the third code; and

encode the third code into the first subset of pixels as 3-digit base-n RGB color codes.

38. The apparatus of claim 26, further configured to salt the first pixel data with a first salt before hashing the first pixel data.

39. The apparatus of claim 26, further configured to translate and transpose characters of the first code after hashing the first pixel data.

40. The apparatus of claim 36 further configured to salt the second pixel data with a second salt before hashing the second pixel data.

41. The apparatus of claim 36, further configured to translate and transpose characters of the second code after hashing the second pixel data.

42. The apparatus of claim 37, further configured to translate and transpose characters of the third code before encoding the third code into the first subset of pixels.

43. An apparatus for encoding and authenticating digital images, comprising: a processor;
and

a memory comprising processor executable code that, when executed by the processor, configures the apparatus to:

(1) encode a digital image by:

capturing the digital image, the digital image comprising a plurality of pixel rows;

partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row;

generating a first encoding code from the first plurality of pixel rows;

overlaying the second plurality of pixel rows with an image representing the first encoding code and embedding the second plurality of pixel rows with metadata;

generating a second encoding code from the second plurality of pixel rows;

generating a third encoding code based on the first encoding code and the second encoding code; and

encoding the first encoding code, the second encoding code and the third encoding code into the remaining row of pixels, wherein encoding the first encoding code, the second encoding code, or the third encoding code into the remaining row of pixels comprises:

collecting the metadata in a character string;

selecting a first character of the metadata for encoding;

selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets based on an index for the first randomly-ordered character set, wherein each character in the first randomly ordered character set is assigned a position code;

matching the first character of the metadata to a corresponding character in the first randomly-ordered character set;

converting the position code of the corresponding character in the first randomly-ordered character set into a three-digit base-n number; and

encoding a first pixel in the remaining row of pixels with an RGB color code comprising the three-digit base-n number;

and (2) authenticate the digital image by:

extracting a first authentication code from a first subset of pixel locations in the remaining row of pixels;

excluding the first subset of pixel locations and extract first pixel data from all other pixels in the remaining row of pixels;

hashing the first pixel data using a first hashing function to generate a first comparison code; and

compare the first authentication code to the first comparison code to determine if the remaining row of pixels has been altered.

44. The apparatus of claim 43, further configured to:

extract a second authentication code from a second subset of pixels in the remaining row of pixels; extract second pixel data from the second plurality of pixel rows;

hash the second pixel data using a second hashing function to generate a second comparison code; and

compare the second authentication code to the second comparison code to determine if the second plurality of pixel rows has been altered.

45. The apparatus of claim 43, further configured to:

extract a third authentication code from a third subset of pixels in the remaining row of pixels; extract third pixel data from the first plurality of pixel rows;

hash the third pixel data using a third hashing function to generate a third comparison code; and

compare the third authentication code to the third comparison code to determine if the first plurality of pixel rows has been altered.

46. The apparatus of claim 44, further configured to:

extract position codes from a fourth subset of pixels in the remaining row of pixels; decode the position codes to obtain the index to the first randomly-ordered character set in the ordered plurality of randomly-ordered character sets, wherein each character in the randomly ordered character sets is assigned a position code;

partition the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows;

extract pixel data from the second subset of pixel rows; and decode metadata from the second subset of pixel rows.

47. The apparatus of claim 46, wherein to decode the metadata from the second subset of pixel rows, the apparatus is further configured to:

decode a first pixel of the second subset of pixel rows to obtain a first position code;
select the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets based on the index; and
select a character in the first randomly-ordered character set at the first position code.

48. The apparatus of claim 47, further configured to:

(a) decode a next pixel of the second subset of pixel rows to obtain a next position code;
(b) select a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets;
(c) select a character in the next randomly-ordered character set at the next position code;
and
(d) repeat operations (a) through (c) until an end-of-data character is decoded.

49. An article of manufacture, comprising a non-transitory machine-readable storage medium containing instructions that, when executed by a machine configures the machine to perform operations, comprising:

capturing a digital image comprising a plurality of pixel rows;
partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row;
generating a first code from the first plurality of pixel rows;
overlaying the second plurality of pixel rows with an image representing the first code;
generating a second code from the second plurality of pixel rows;
generating a third code based on the first code and the second code; and
encoding the first code, the second code and the third code into the remaining row of pixels, wherein encoding the first code, the second code, or the third code into the remaining row of pixels comprises:
collecting the metadata in a character string;
selecting a first character of the metadata for encoding;

selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets based on an index for the first randomly-ordered character set, wherein each character in the first randomly ordered character set is assigned a position code;

matching the first character of the metadata to a corresponding character in the first randomly-ordered character set;

converting the position code of the corresponding character in the first randomly-ordered character set into a three-digit base-n number; and

encoding a first pixel in the remaining row of pixels with an RGB color code comprising the three-digit base-n number.

50. The article of manufacture of claim 49, wherein generating the first code comprises: extracting first pixel data from the first plurality of pixel rows; and

hashing the first pixel data using a first hashing function to generate a first hash code.

51. The article of manufacture of claim 50, wherein the machine is further configured to perform operations comprising:

selecting a first character of the first hash code;

randomly selecting the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets, wherein each character in the first randomly-ordered character set is assigned the position code;

matching the first character of the first hash code to a corresponding character in the first randomly ordered character set; and

replacing the first character of the first hash code with a character from a reference character set at the position code of the corresponding character in the first randomly-ordered character set.

52. The article of manufacture of claim 51, wherein the machine is further configured to perform operations comprising:

(a) selecting a next character of the first hash code;

(b) matching the next character of the first hash code to a corresponding character in a next randomly ordered character set;

(c) replacing the next character of the first hash code with a character from the reference character set at the position code of the corresponding character in the next randomly ordered character set; and

(d) repeating operations (a) through (c) until the first hash code is exhausted, wherein the first code is generated.

53. The article of manufacture of claim 51, wherein randomly selecting the first randomly- ordered character set comprises randomly selecting R position codes, wherein a summation of the R position codes modulo m provides an index to the first randomly- ordered character set, wherein m is the number of randomly-ordered character sets.

54. The article of manufacture of claim 50, wherein the digital image is overlaid with identifying information before extracting the pixel data from the first plurality of pixel rows, wherein the identifying information comprises one or more of a date and time stamp, a user name, GPS coordinates, a street address, a device name, an operating system name and version, and a watermark.

55. The article of manufacture of claim 52, wherein overlaying the second plurality of pixel rows with an image representing the first code comprises:

initializing each pixel in the second plurality of pixel rows;

partitioning the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows; and

mapping an image of the first code to the first subset of pixels.

56. The article of manufacture of claim 55,

wherein the metadata comprises one or more of GPS coordinates, a GPS accuracy, a date and time, a date and time source name, a device ID, a device operating system and version, a user ID, an organization ID, an assigned group name, and a reverse geocoded address; wherein the machine is further configured to perform operations comprising:

encoding the metadata into the second subset of pixel rows.

57. The article of manufacture of claim 56, wherein encoding the metadata into the second subset of pixel rows comprises:

encoding a first pixel in the second subset of pixel rows with the RGB color code comprising the three-digit base-n number.

58. The article of manufacture of claim 57, wherein the machine is further configured to perform operations comprising:

- (a) selecting a next character of the metadata for encoding;
- (b) selecting a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets;
- (c) matching the next character of the metadata to a corresponding character in the next randomly-ordered character set;
- (d) converting the position-based code of the corresponding character in the next randomly-ordered character set into a next three-digit base-n number;
- (e) encoding a next pixel in the second subset of pixel rows with an RGB color code comprising the three-digit base-n number; and
- (f) repeating steps (a) through (e) until the metadata is exhausted; and
- (g) encoding an end-of-data character.

59. The article of manufacture of claim 58, wherein the machine is further configured to perform operations comprising encoding any remaining pixels in the second subset of pixel rows with random RGB color codes based on random three-digit base-n numbers.

60. The article of manufacture of claim 57, wherein generating the second code from the second plurality of pixel rows comprises:

extracting second pixel data from the second plurality of pixel rows; and
hashing the second pixel data using a second hashing function to generate the second code.

61. The article of manufacture of claim 60, wherein the machine is further configured to perform operations comprising:

encoding each pixel of the remaining row of pixels with RGB color codes based on random 3-digit base-n numbers;
reserving a first subset of pixels of the remaining row of pixels for the third code;
encoding the first code, the second code and the position codes as 3-digit base-n RGB color codes into predetermined pixel locations in the remaining row of pixels;
excluding the first subset of pixels, hashing the pixel data of the remaining line using a third hashing function to generate the third code; and
encode the third code into the first subset of pixels as 3-digit base-n RGB color codes.

62. The article of manufacture of claim 50, wherein the machine is further configured to perform operations comprising salting the first pixel data with a first salt before hashing the first pixel data.

63. The article of manufacture of claim 50, wherein the machine is further configured to perform operations comprising translating and transposing characters of the first code after hashing the first pixel data.

64. The article of manufacture of claim 60, wherein the machine is further configured to perform operations comprising salting the second pixel data with a second salt before hashing the second pixel data.

65. The article of manufacture of claim 60, wherein the machine is further configured to perform operations comprising translating and transposing characters of the second code after hashing the second pixel data.

66. The article of manufacture of claim 61, wherein the machine is further configured to perform operations comprising translating and transposing characters of the third code before encoding the third code into the first subset of pixels.

67. An article of manufacture, comprising a non-transitory machine-readable storage medium containing instructions that, when executed by a machine configures the machine to

perform operations, comprising:

(1) encoding a digital image by:

capturing the digital image, the digital image comprising a plurality of pixel rows;

partitioning the digital image into a first plurality of pixel rows, a second plurality of pixel rows, and a remaining pixel row;

generating a first encoding code from the first plurality of pixel rows;

overlaying the second plurality of pixel rows with an image representing the first encoding code and embedding the second plurality of pixel rows with metadata;

generating a second encoding code from the second plurality of pixel rows;

generating a third encoding code based on the first encoding code and the second encoding code; and

encoding the first encoding code, the second encoding code and the third encoding code into the remaining row of pixels, wherein encoding the first encoding code, the second encoding code, or the third encoding code into the remaining row of pixels comprises:

collecting the metadata in a character string;

selecting a first character of the metadata for encoding;

selecting a first randomly-ordered character set from an ordered plurality of randomly ordered-character sets based on an index for the first randomly-ordered character set, wherein each character in the first randomly ordered character set is assigned a position code;

matching the first character of the metadata to a corresponding character in the first randomly-ordered character set;

converting the position code of the corresponding character in the first randomly-ordered character set into a three-digit base-n number; and

encoding a first pixel in the remaining row of pixels with an RGB color code comprising the three-digit base-n number; and

(2) authenticating the digital image by:

extracting a first authentication code from a first subset of pixel locations in the remaining row of pixels; excluding the first subset of pixel locations in the remaining row, extracting first pixel data from all other pixels in the remaining row of pixels;

hashing the first pixel data using a first hashing function to generate a first comparison code; and

comparing the first authentication code to the first comparison code to determine if the remaining row of pixels has been altered.

68. The article of manufacture of claim 67, further comprising:

extracting a second authentication code from a second subset of pixels in the remaining row of pixels;

extracting second pixel data from the second plurality of pixel rows;

hashing the second pixel data using a second hashing function to generate a second comparison code; and

comparing the second authentication code to the second comparison code to determine if the second plurality of pixel rows has been altered.

69. The article of manufacture of claim 67, wherein the machine is further configured to perform operations comprising:

extracting a third authentication code from a third subset of pixels in the remaining row of pixels; extracting third pixel data from the first plurality of pixel rows;

hashing the third pixel data using a third hashing function to generate a third comparison code; and

comparing the third authentication code to the third comparison code to determine if the first plurality of pixel rows has been altered.

70. The article of manufacture of claim 68, wherein the machine is further configured to perform operations comprising:

extracting position codes from a fourth subset of pixels in the remaining row of pixels; decoding the position codes to obtain the index to the first randomly-ordered character set in the ordered plurality of randomly-ordered character sets, wherein each character in the randomly ordered character sets is assigned a position code;

partitioning the second plurality of pixel rows into a first subset of pixel rows and a second subset of pixel rows;

extracting pixel data from the second subset of pixel rows; and decoding metadata from the second subset of pixel rows.

71. The article of manufacture of claim 70, wherein decoding the metadata from the second subset of pixel rows comprises:

decoding a first pixel of the second subset of pixel rows to obtain a first position code;
selecting the first randomly-ordered character set from the ordered plurality of randomly ordered-character sets based on the index; and
selecting a character in the first randomly-ordered character set at the first position code.

72. The article of manufacture of claim 71, wherein pixels in the second subset of pixel rows are encoded with 3-digit base-n RGB color codes.

73. The article of manufacture of claim 71, wherein the machine is further configured to perform operations comprising:

(a) decoding a next pixel of the second subset of pixel rows to obtain a next position code;

(b) selecting a next randomly-ordered character set from the ordered plurality of randomly ordered-character sets;

(c) selecting a character in the next randomly-ordered character set at the next position code; and

(d) repeating operations (a) through (c) until an end-of-data character is decoded.

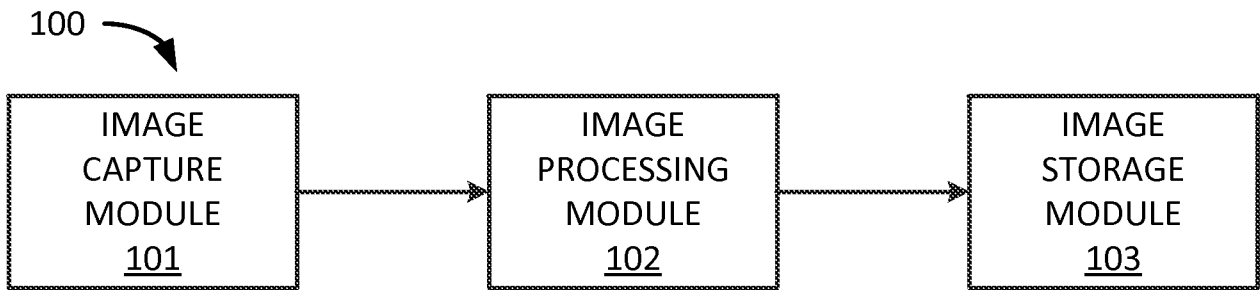


FIG. 1

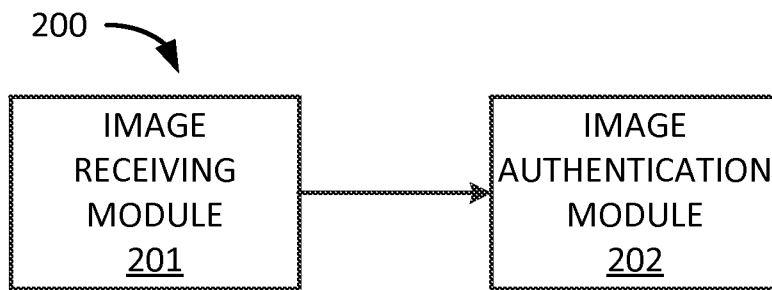


FIG. 2

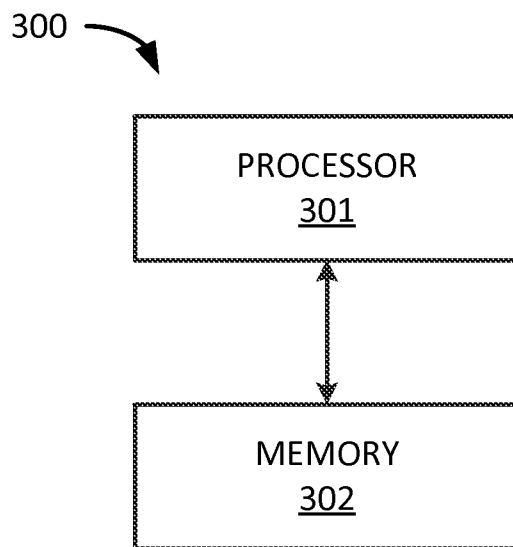


FIG. 3

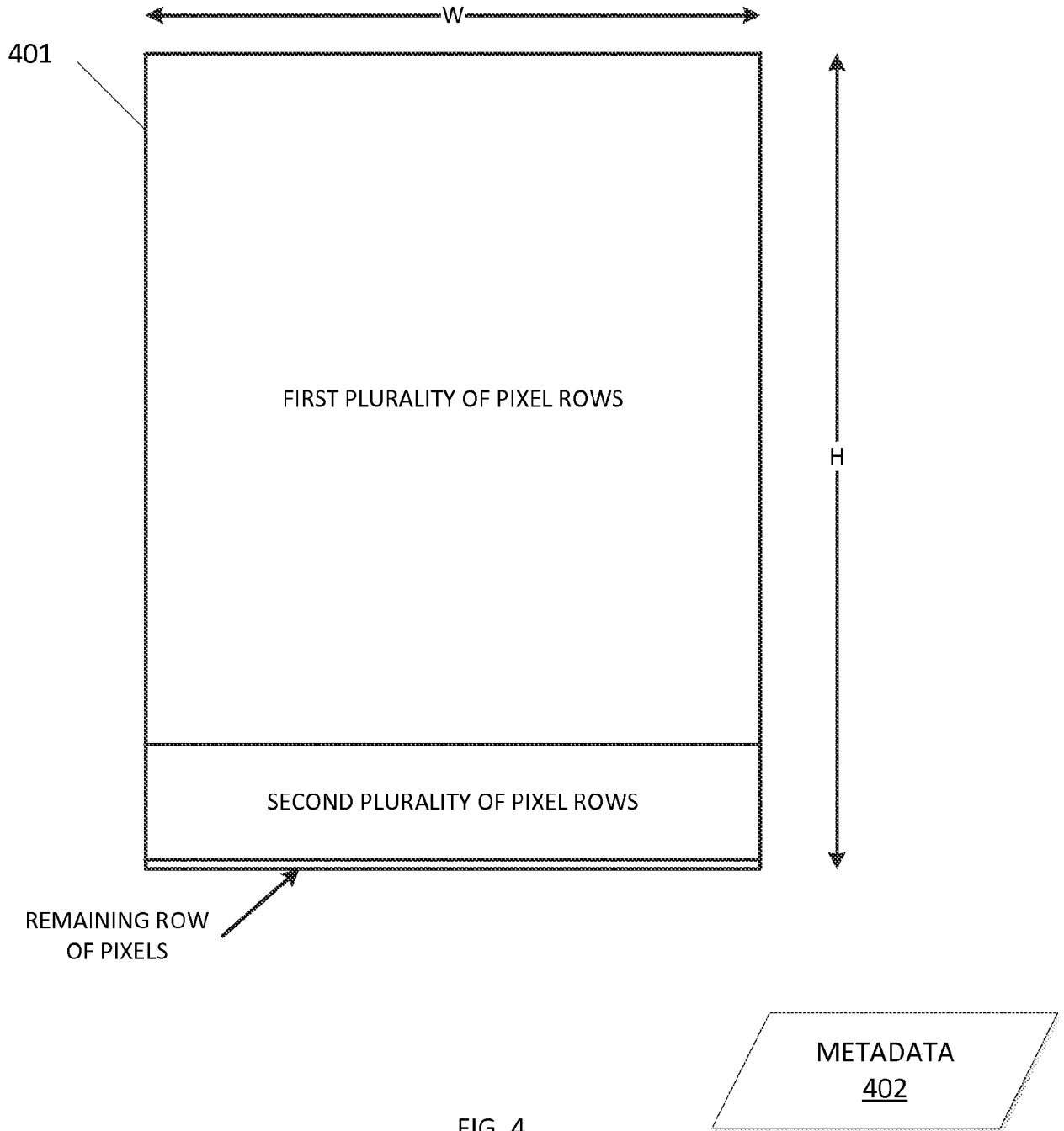


FIG. 4

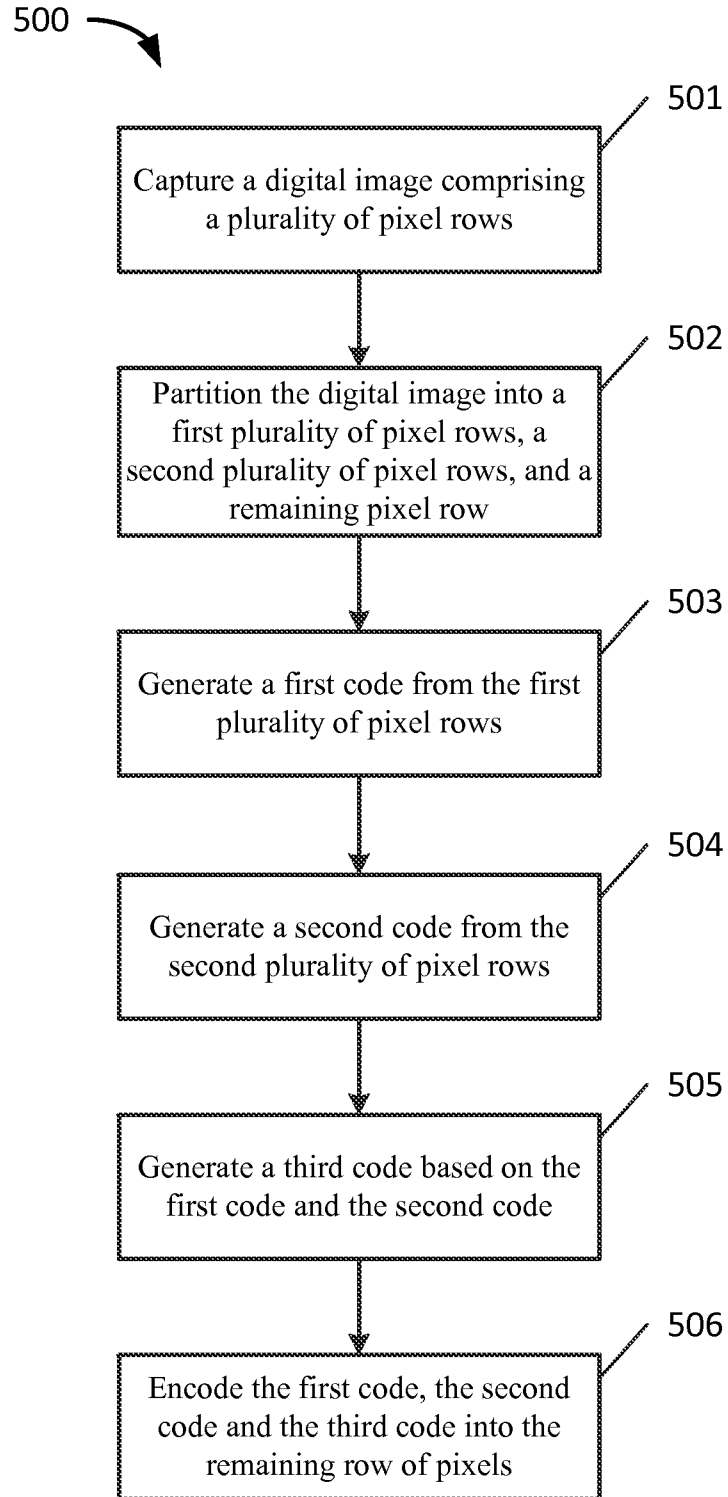


FIG. 5

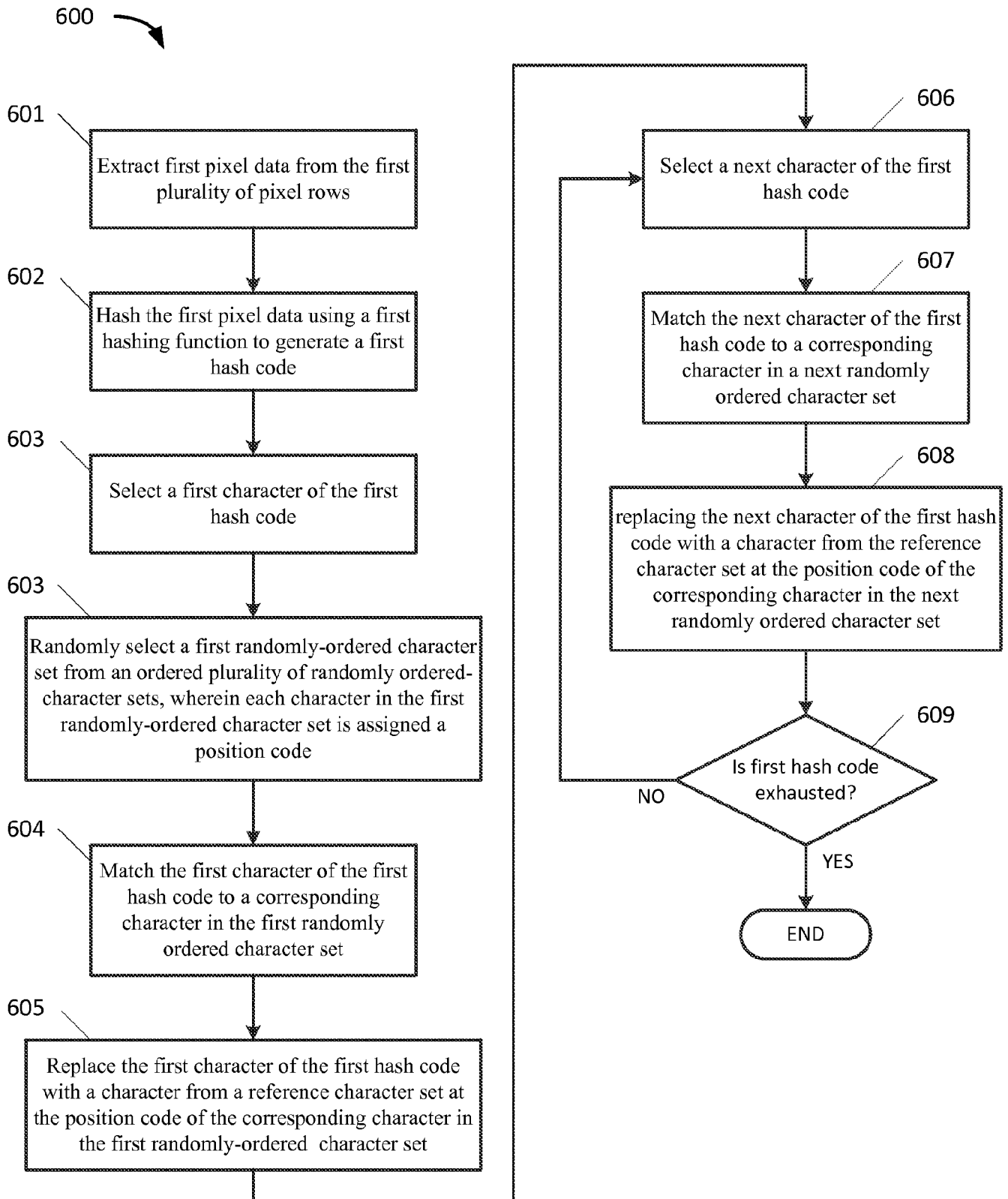


FIG. 6

702

REFERENCE CHARACTER SET:

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ~:;<=>?@^_!#\$%&'()*+,-./

703

RANDOM POSITION CODES: 32, 50, 59, 22, 42, 80, 71, 67, 48, 88

704

STARTING INDEX: $r = (32+50+59+22+42+80+71+67+48+88)\text{mod}(256) = (559)\text{mod}(256) = 47$

701

STARTING INDEX (r=47)

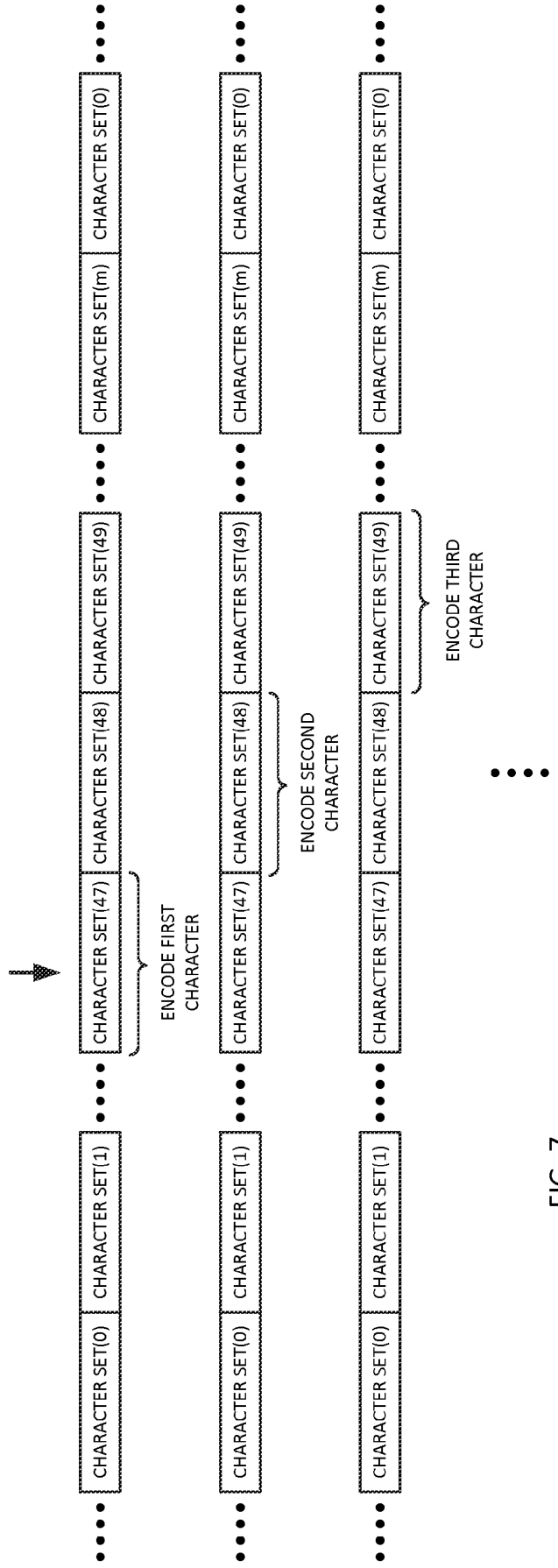


FIG. 7

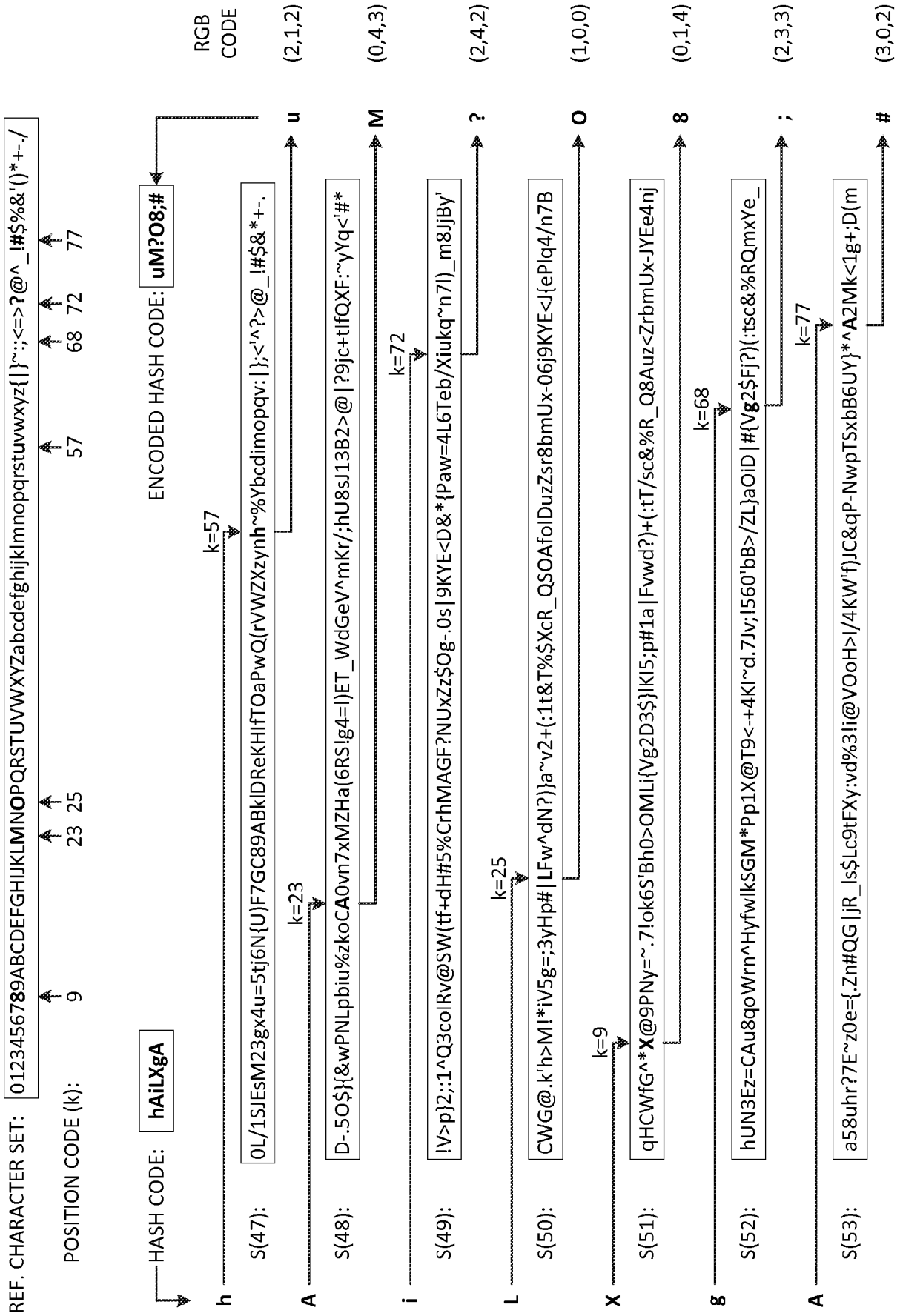


FIG. 8



FIG. 9

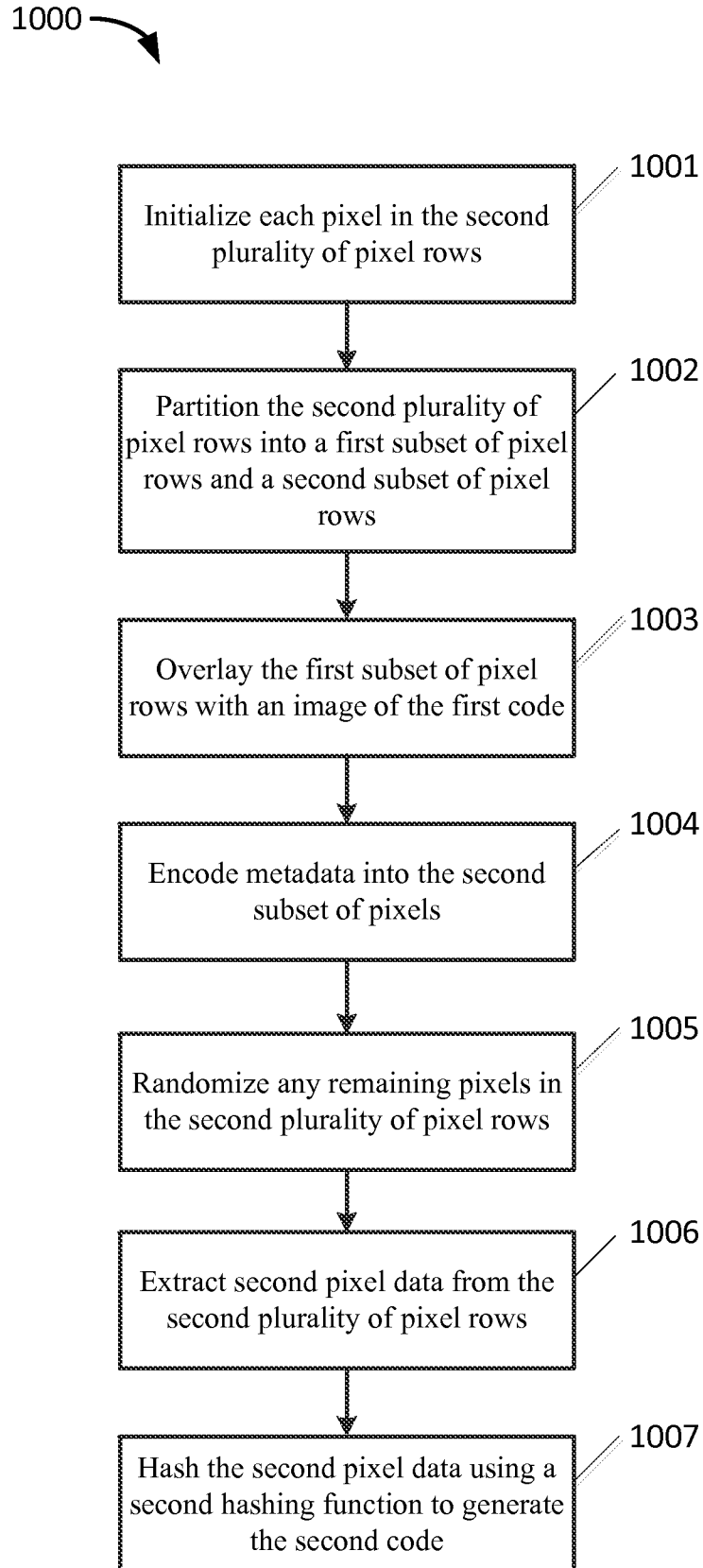
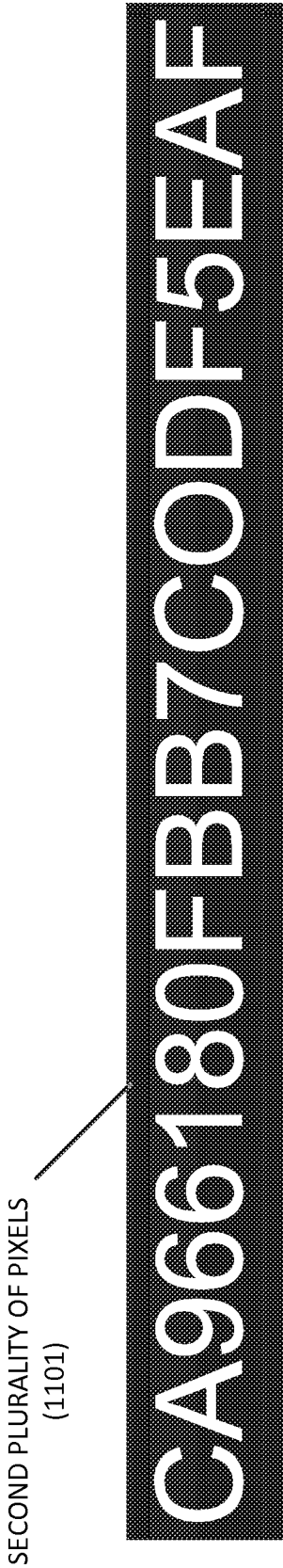
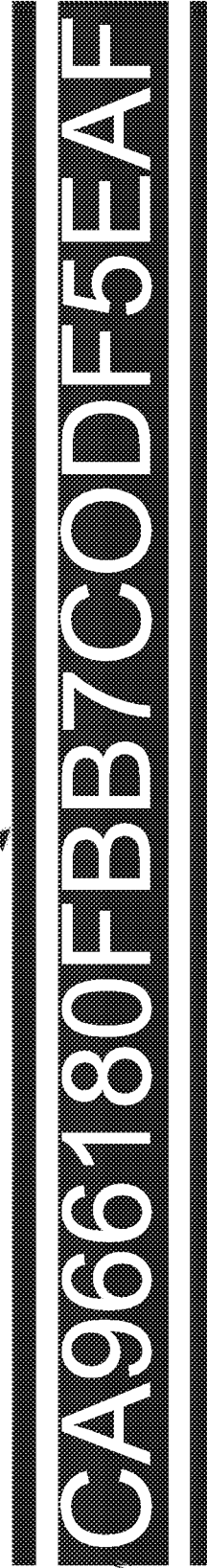


FIG. 10



SECOND SUBSET OF PIXEL ROWS
(1103A)



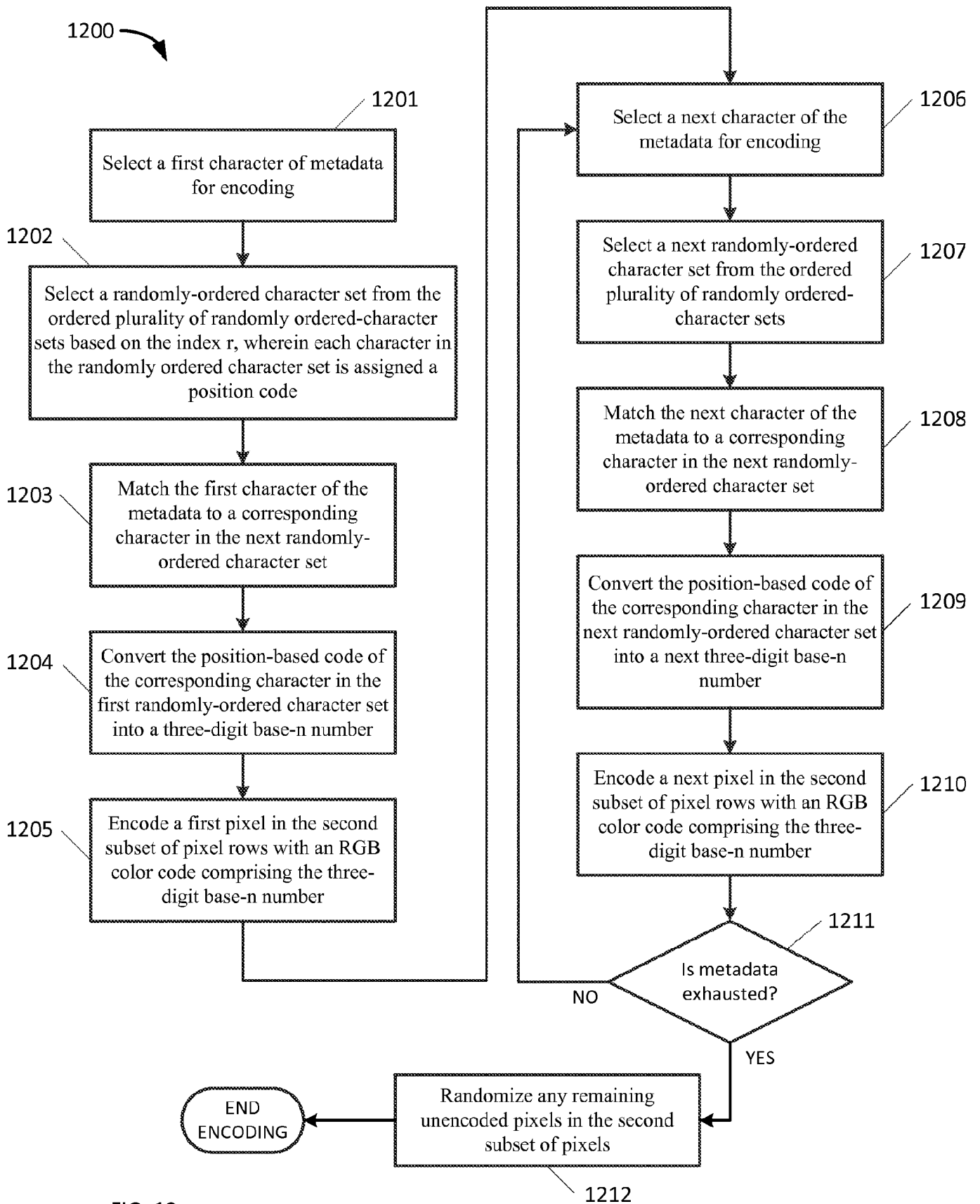


FIG. 12

1300

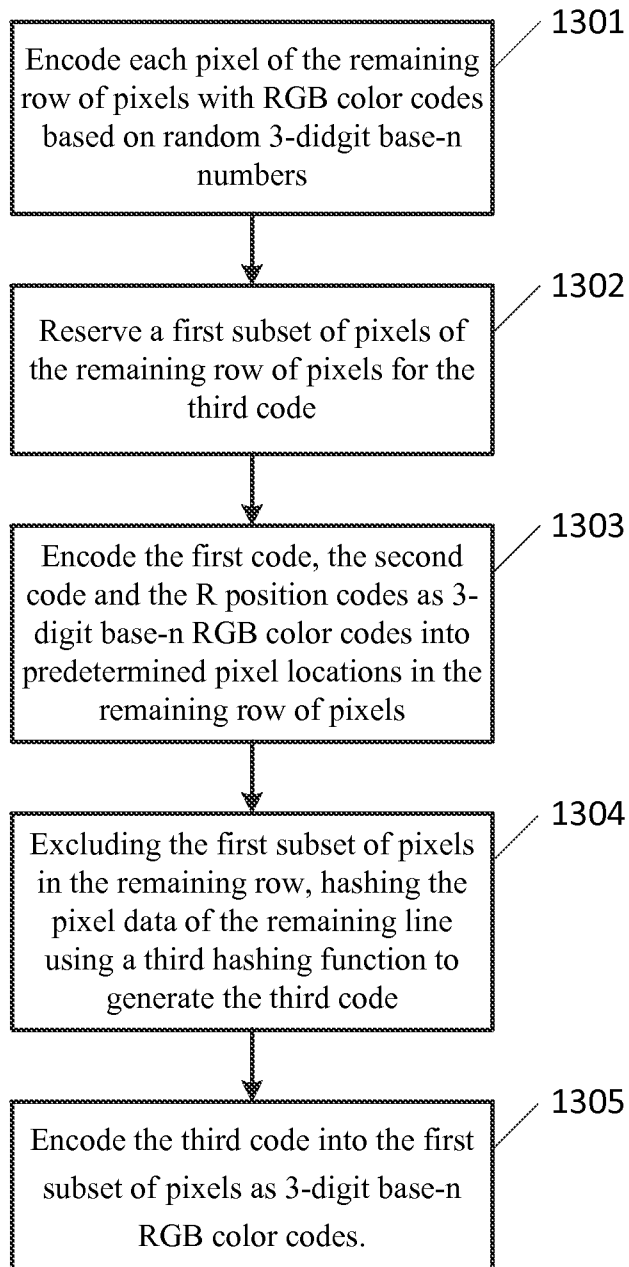
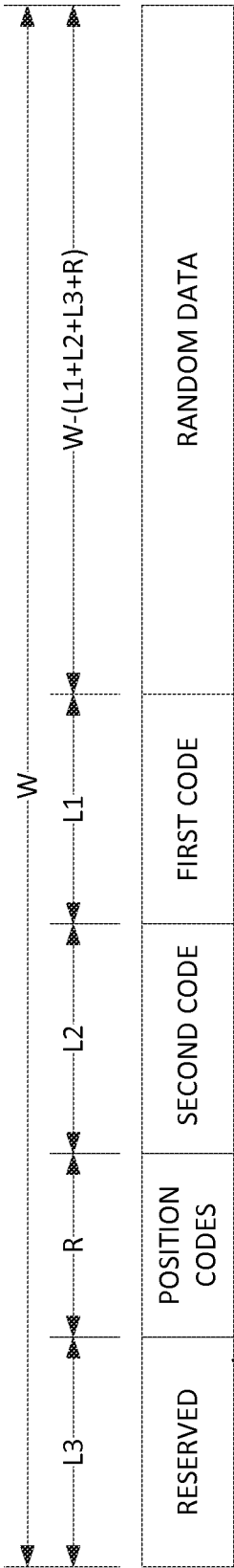
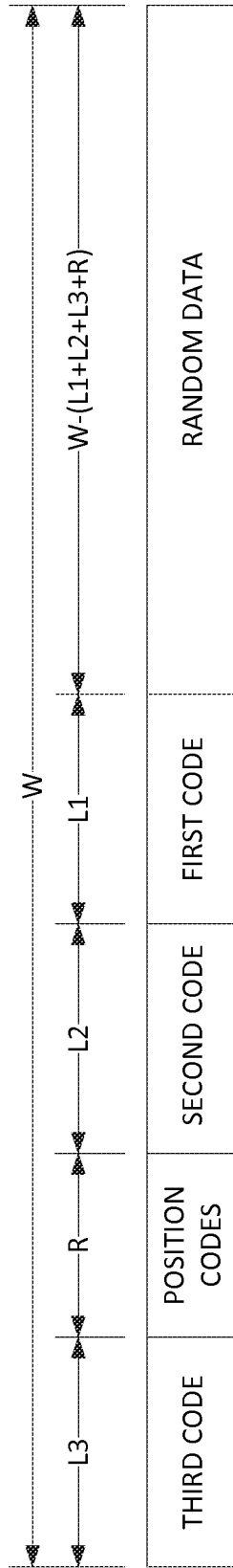


FIG. 13



REMAINING LINE
FIG. 14A



REMAINING LINE
FIG. 14B

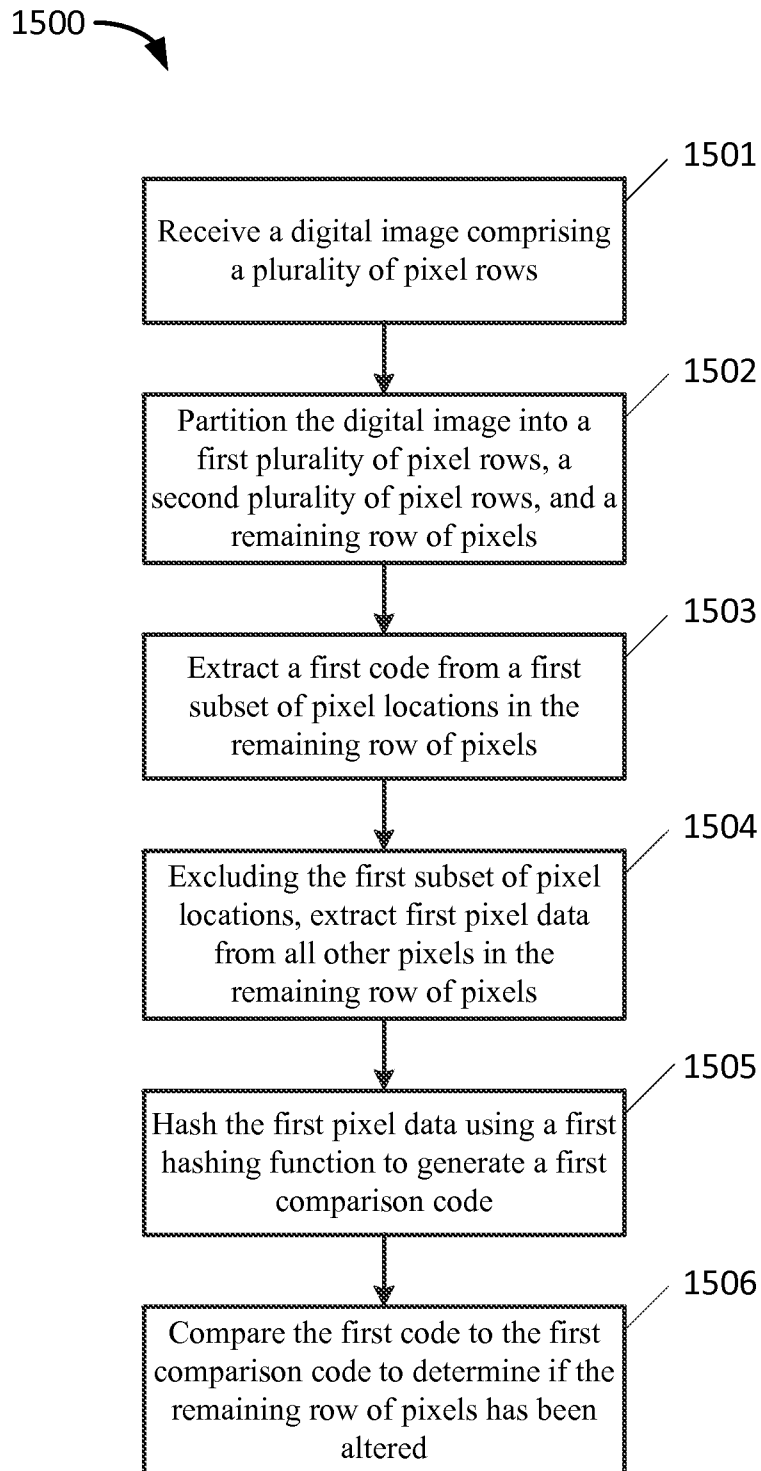


FIG. 15

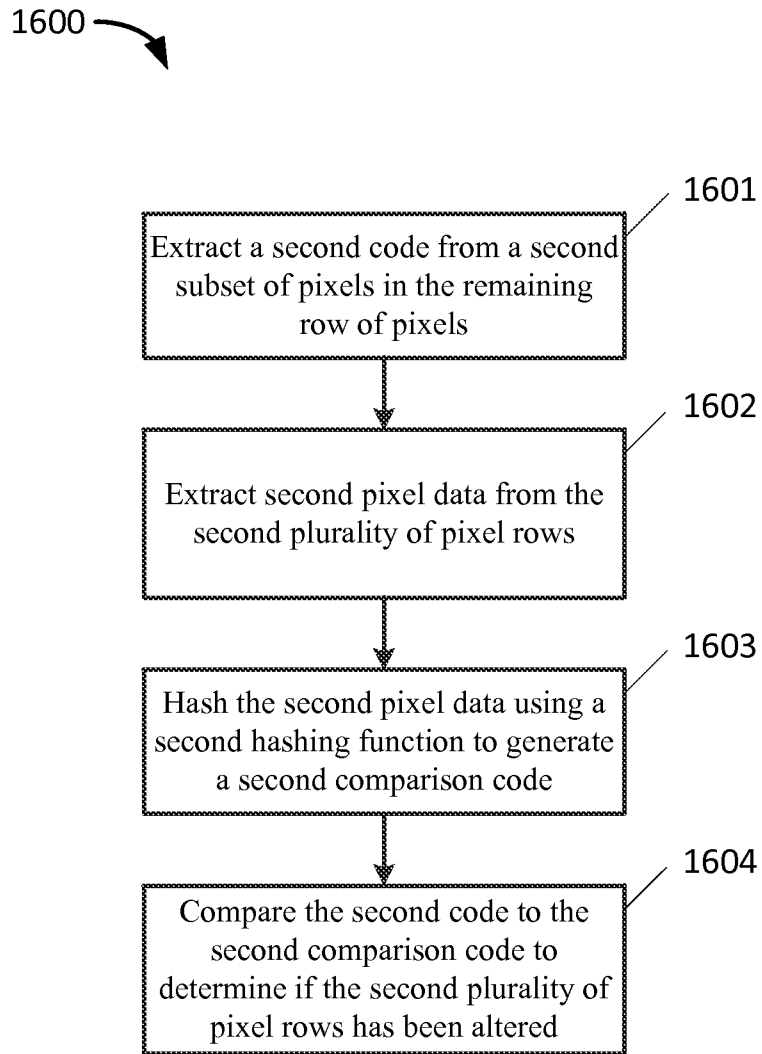


FIG. 16

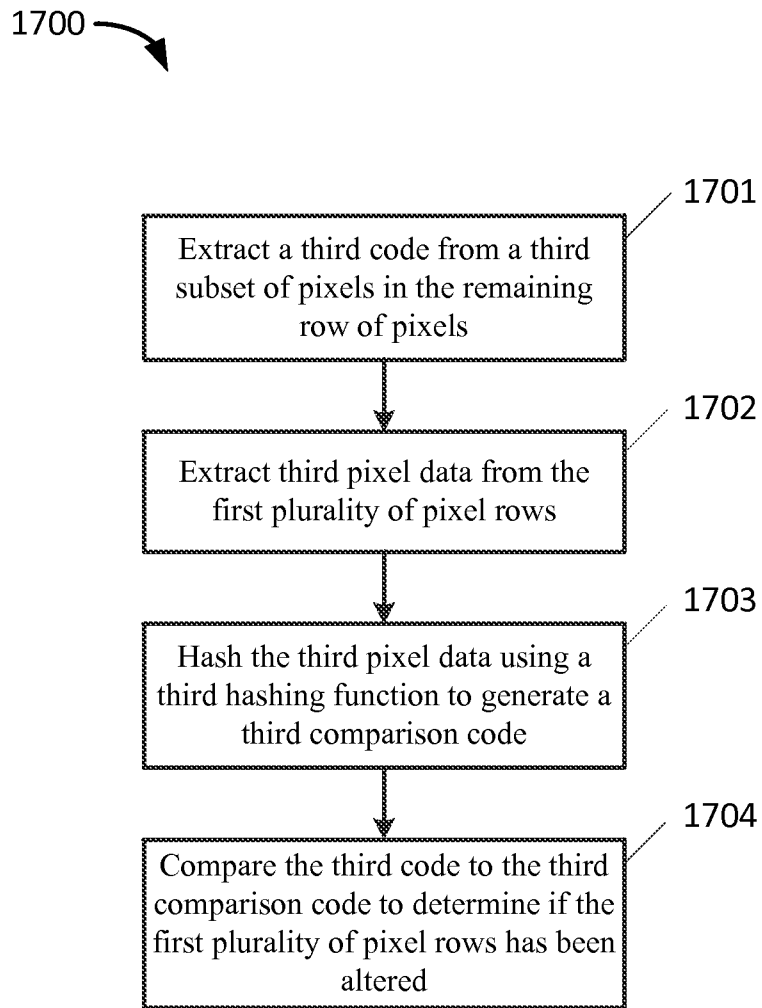


FIG. 17

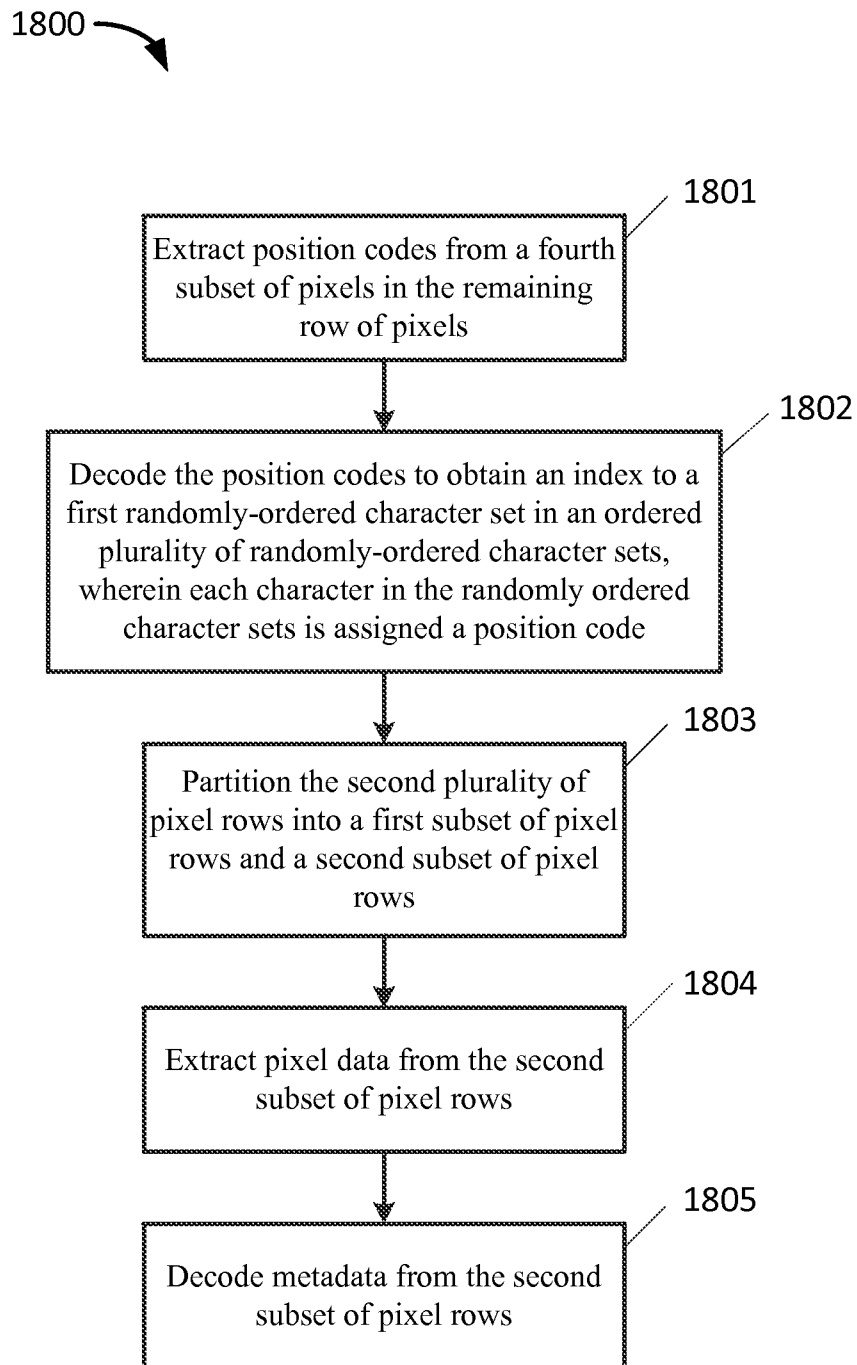


FIG. 18

1900

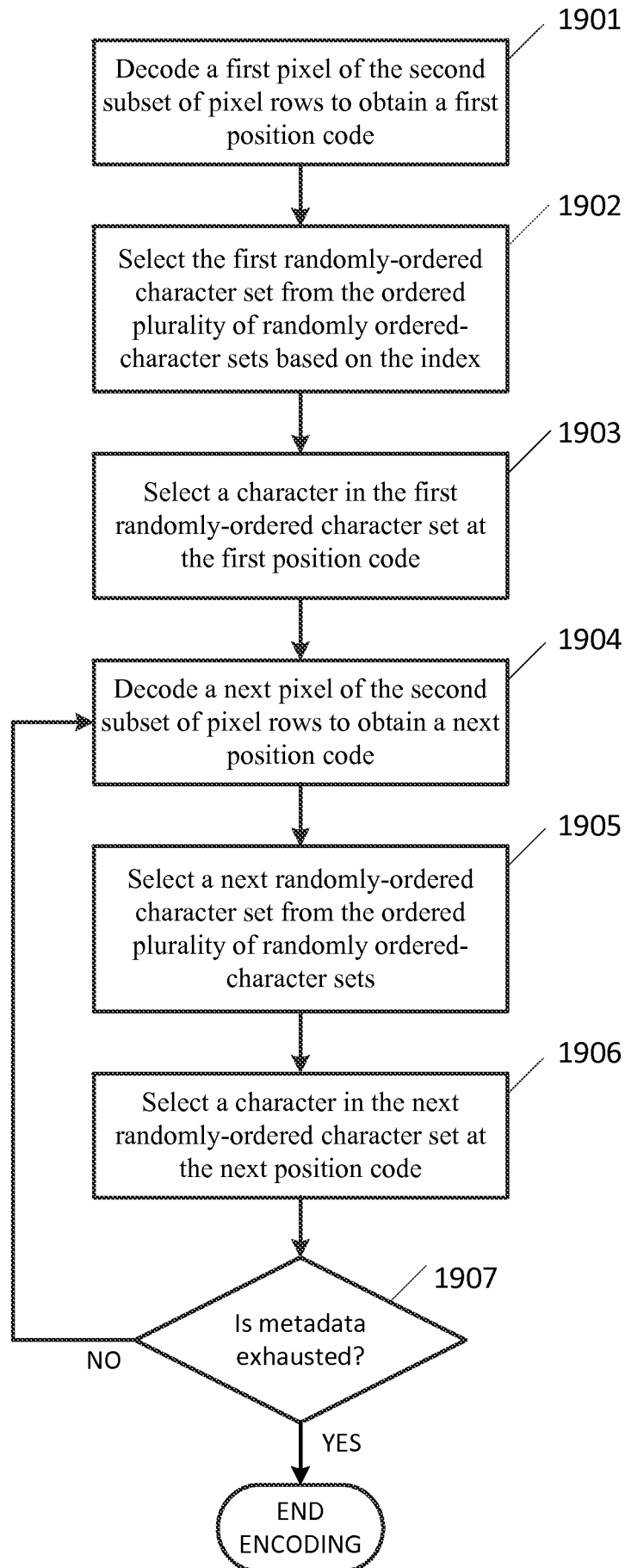


FIG. 19

702 ↘

REFERENCE CHARACTER SET:

0123456789ABCDEFGHIJKLMNPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz{|}~:;<=>?@^_!#\$%&'()*+,-./

703 ↘

RANDOM POSITION CODES: 32, 50, 59, 22, 42, 80, 71, 67, 48, 88

704 ↘

STARTING INDEX: $r = (32+50+59+22+42+80+71+557+48+88)\text{mod}(256) = (559)\text{mod}(256) = 47$

701 ↘

