

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

(19) World Intellectual Property

Organization

International Bureau

(43) International Publication Date

08 February 2024 (08.02.2024)



(10) International Publication Number

WO 2024/031015 A1

(51) International Patent Classification:

G07D 7/004 (2016.01) G07D 7/206 (2016.01)

B42D 25/00 (2014.01) H04N 1/00 (2006.01)

G07D 7/12 (2016.01)

DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(21) International Application Number:

PCT/US2023/071609

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

(22) International Filing Date:

03 August 2023 (03.08.2023)

Published:

— with international search report (Art. 21(3))  
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/395,483 05 August 2022 (05.08.2022) US

(71) Applicant: **PROOF AUTHENTICATION CORPORATION** [US/US]; 200 Canal View Boulevard, Suite 104, Rochester, New York 14623 (US).

(72) Inventors: **GILBERT, James P.**; 200 Canal View Blvd., Suite 104, Rochester, New York 14623 (US). **MCK-INNON, Daniel J.**; 200 Canal View Blvd., Suite 104, Rochester, New York 14623 (US). **PARRINELLO, Richard**; 200 Canal View Blvd., Suite 104, Rochester, New York 14623 (US). **VALINCOURT, William**; 200 Canal View Blvd., Suite 104, Rochester, New York 14623 (US). **WICKER, David M.**; 200 Canal View Blvd., Suite 104, Rochester, New York 14623 (US).

(74) Agent: **CHERN, Joseph** et al.; ORRICK, HERRINGTON & SUTCLIFFE LLP, 2050 Main Street, Suite 1100, Irvine, California 92614-8255 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ,

(54) Title: SYSTEMS AND METHODS FOR THE GENERATION AND USAGE OF AUTHENTICATION IMAGES IN CONJUNCTION WITH LOW-RESOLUTION PRINT DEVICES

(57) Abstract: Systems and methods applicable, for instance, to the generation and usage of authentication images. In one aspect, unauthorized attempts to duplicate authentication images can be thwarted. In another aspect, there can be provision for authorized authentication image generation using low-resolution print devices.

WO 2024/031015 A1

**SYSTEMS AND METHODS FOR THE GENERATION AND USAGE OF  
AUTHENTICATION IMAGES IN CONJUNCTION WITH LOW-RESOLUTION PRINT  
DEVICES**

**CROSS-REFERENCE TO RELATED APPLICATIONS**

**[0001]** This application claims priority to United States Provisional Application Serial No. 63/395,483, filed August 5, 2022, the contents of which are hereby incorporated by reference in their entirety and for all purposes.

**FIELD OF THE INVENTION**

**[0002]** The present disclosure relates generally to authentication images, and more specifically, but not exclusively, to systems and methods for the generation and usage of authentication images in conjunction with low-resolution print devices (*e.g.*, home/office printers and low-resolution industrial printers).

**BACKGROUND OF THE INVENTION**

**[0003]** Authentication images can serve many useful purposes. For example, an authentication image affixed to an item (and/or to packaging materials thereof) can serve to indicate that the item is genuine. Such authentication image usage can be particularly useful in connection with items that are often the target of counterfeiters. Aircraft parts, pharmaceuticals, sports memorabilia items, luxury watches, and designer handbags are but a few of the items that fall into such a category.

**[0004]** However, where authentication images are used in this way, the authentication images themselves can be the subject of unauthorized duplication. Indeed, a counterfeiter could potentially lend credence to a counterfeit item by affixing to it a counterfeit authentication image. Here, increases in the capabilities of low-resolution print devices (*e.g.*, home/office printers and low-resolution industrial printers) and of home/office capture equipment -- along

with decreases in the prices thereof -- have served to make potential tools for the unauthorized duplication of authentication images readily available.

[0005] From a different vantage point though, allowing for the authorized printing of an authentication image using a low-resolution print device could prove useful under various circumstances. However, conventional approaches do not provide for authentication image generation that can on one hand be successfully performed by a low-resolution print device when authorized. But, on the other, hand that yields an authentication image that cannot be the subject of unauthorized duplication using, say, a home/office scanner in conjunction with a low-resolution print device.

[0006] In view of the foregoing, a need exists for improved systems and methods for implementing authentication images, in an effort to overcome the aforementioned obstacles and deficiencies of conventional approaches.

## SUMMARY

[0007] In accordance with a first aspect disclosed herein, there is set forth an authentication image, comprising:

[0008] one or more latent images, wherein the latent images indicate authenticity; and

[0009] one or more background images, wherein the background images work in conjunction with the latent images to inhibit unauthorized duplication of the authentication image,

[0010] wherein generation of the authentication image utilizes knowledge of idiosyncrasies of one or more of low-resolution print devices or home/office equipment; and

[0011] wherein authorized software uses knowledge regarding the background images and knowledge regarding the latent images to yield one or more of the latent images from the authentication image.

[0012] In some embodiments of the disclosed authentication image, the image further comprises one or more visible targets, wherein the visible targets aid in said yielding of the latent images from the authentication image, wherein the visible targets optionally assist in one or more

of glare detection or automatic zooming or optionally are one or more of in or adjacent to the authentication image.

**[0013]** In some embodiments of the disclosed authentication image, detection of the one or more visible targets utilizes contour extraction.

**[0014]** In some embodiments of the disclosed authentication image, one or more of the latent images or the background images are formulated using image elements, wherein the image elements optionally include one or more of lines, line segments, dots, spots, or non-imaged areas.

**[0015]** In some embodiments of the disclosed authentication image, a first quantity of the image elements are arranged at a first angle and form the one or more background images, and wherein a second quantity of the image elements are arranged at or near a second angle and form the one or more latent images.

**[0016]** In some embodiments of the disclosed authentication image, the authentication image is at least one of printed via a custom font/character set approach, associated with a track and trace element, wherein the authentication image denotes authenticity of the track and trace element, or an onscreen authentication image, and wherein a validity determination can be made by pointing a device at a display showing the onscreen authentication image.

**[0017]** In some embodiments of the disclosed authentication image, the authentication image is an onscreen authentication image, wherein the onscreen authentication image is accompanied by a further authentication image, wherein the further authentication image is formed via one of print, ablation, engraving, or etching, and wherein a validity determination can be made by pointing a device at the further authentication image, and at a display showing the onscreen authentication image.

**[0018]** In accordance with some aspects disclosed herein, there is set forth a system comprising:

**[0019]** at least one processor; and

**[0020]** a memory storing instructions that, when executed by the at least one processor, cause the system to generate the authentication image disclosed herein.

[0021] In accordance with another aspect disclosed herein, there is set forth a computer-implemented method, comprising:

[0022] generating, by a computing system, an uncompensated print file for an authentication image, wherein printing of the uncompensated print file by a low-resolution print device yields a print result not matching the uncompensated print file; and

[0023] generating, by the computing system, from the uncompensated print file, a compensated print file for the authentication image, wherein the generation of the compensated print file utilizes known low-resolution print device idiosyncrasies, and wherein printing of the compensated print file by the low-resolution print device yields an authentication image print result that scans as valid.

[0024] In some embodiments of the disclosed method, the unauthorized duplication of the authentication image print result at least one of incurs image loss or fails to scan as valid.

[0025] In some embodiments of the disclosed method, the authentication image is formulated using at least one of consistent or variable image elements, image elements having a print density that results in one or more of disappearance, distortion, or color hue shift where the authentication image is subjected to unauthorized duplication, or one or more compound image elements, wherein the compound image elements are split into separate color layers.

[0026] In some embodiments of the disclosed method, the generation of the compensated print file utilizes one or more compensatory formulas.

[0027] In some embodiments of the disclosed method, the compensated print file is generated using a custom font/character set approach.

[0028] In some embodiments of the disclosed method, first portions of the authentication image are printed using a colorant invisible under regular light, and second portions of the authentication image are printed using a colorant visible under regular light.

[0029] In accordance with some aspects disclosed herein, there is set forth a system comprising: at least one processor; and

[0030] a memory storing instructions that, when executed by the at least one processor, cause the system to perform the computer-implemented method disclosed herein.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0031] Fig. 1 is an illustration showing an authentication image including a visible target, according to various embodiments.

[0032] Fig. 2 is a representation of a computer having performed a contour extraction, according to various embodiments.

[0033] Fig. 3 is distance-from-center-point plot, according to various embodiments.

[0034] Fig. 4 is an illustration showing a QR code in comparison to an authentication image, according to various embodiments.

[0035] Fig. 5 is an illustration showing an authentication image including a background image and multiple latent images, according to various embodiments.

[0036] Fig. 6 is an illustration showing a thwarted attempt to duplicate an authentication image, according to various embodiments.

[0037] Fig. 7 is an illustration showing depictions of an uncompensated print file and various prints thereof, according to various embodiments.

[0038] Fig. 8 is an illustration showing further authentication images including visible targets, according to various embodiments.

[0039] Fig. 9 is an illustration showing consistent image elements and variable image elements, according to various embodiments.

[0040] Fig. 10 is an illustration showing depictions of authentication images including visible images, according to various embodiments.

[0041] Fig. 11 is an illustration showing depictions of microtext, according to various embodiments.

[0042] Fig. 12 is an illustration showing depictions of supplemental image elements, according to various embodiments.

[0043] Fig. 13 is an illustration depicting compound image elements, according to various embodiments.

[0044] Fig. 14 is an illustration depicting visible targets, according to various embodiments.

[0045] Fig. 15 is an illustration depicting an authentication image printed using a custom font/character set approach, according to various embodiments.

[0046] Fig. 16 is an illustration depicting QR codes along with authentication images, according to various embodiments.

[0047] Fig. 17 is an illustration depicting an authentication image printed using invisible colorant, according to various embodiments.

[0048] Fig. 18 is an illustration depicting usage of a laser ablation approach, according to various embodiments.

[0049] Fig. 19 is an illustration depicting onscreen authentication images, according to various embodiments.

[0050] Fig. 20 is an illustration depicting an onscreen authentication image, and authentication images generated using print and/or laser, according to various embodiments.

[0051] Fig. 21 shows an example computer, according to various embodiments.

## **DETAILED DESCRIPTION**

[0052] According to various embodiments, systems and methods can be employed to generate and utilize authentication images. Such an authentication image can be made up of one or more latent images, and one or more background images. As just some examples, the one or more latent images can serve functions including but not limited to demonstrating an item to which the authentication image is affixed or emblazoned to be an original or authentic item, and/or granting a privilege (e.g., access to a museum, concert, or sporting event). The one or more background images can, as just some examples, serve to camouflage the one or more latent images to the human eye, and/or to thwart attempts to duplicate the authentication image. Such thwarting can arise from the authentication image generation approaches leveraging inadequacies

and/or idiosyncrasies of equipment (e.g., home/office scanners, copiers, smartphone cameras, standalone digital cameras, home/office printers, and/or low-resolution industrial printers) that could be plied by individuals endeavoring to reproduce the authentication image. Where such unauthorized reproduction is attempted, the result can be an image distinguishable from the original authentication image, thus signaling a non-original authentication image. Still, despite the camouflage and duplication-thwarting abilities of the background images, the one or more latent images of the authentication image can nevertheless be extracted using a camera-equipped smartphone (or other device). Further, in various embodiments a visible target (e.g., a plus-shaped visible target) can be located in or adjacent to the authentication image. The visible target can provide benefits including aiding in performing extraction of the latent images from the authentication image.

**[0053]** In various embodiments, the one or more background images and the one or more latent images of an authentication image can be formulated using sets of image elements. The image elements of a given set can share a given angular arrangement, and can formulate either a background image (or a portion thereof) or a latent image (or a portion thereof). As just an illustration, an authentication image can be made up of image elements that are arranged at or near 90 degrees and which form a background image, and image elements that are arranged at or near 45 degrees and which form a latent image. Here, authorized software (e.g., an authorized app running on a smartphone and/or software running on a central computer or website) can utilize knowledge of the 90 degree angular arrangement of the image elements that make up the background image, and of the 45 degree angular arrangement of the image elements that make up the latent image, to subtract the background image from the authentication image, thereby yielding the latent image. As just some examples, the image elements can be lines, line segments, dots, spots, or non-imaged areas (e.g., white spaces). The image elements can be straight, intermittent, modulated (e.g., wavy and/or thickness/thinness modulated), and/or contain noise. The image elements can be of various shapes. As just some examples, the dots can be



circular, the dots can be square, the non-images areas can be circular, and/or the non-imaged areas can be square.

**[0054]** In various embodiments a latent image can consist of image elements that are situated in between (or adjacent to) image elements that are spaced at or about 150 to at or about 300 lines per inch. In other embodiments, other lines per inch spacing ranges than at or about 70 to at or about 300 lines per inch can be used. Also, in various embodiments, background images can be situated around and/or integrated with latent images.

**[0055]** Authentication images and visible targets can be printed, as just some examples, utilizing traditional presses, digital presses, laser printers, using inkjet printers, using split fountain methods, using simulated split fountain methods, and/or via laser etching. Further, authentication images and visible targets can be single or multicolor. The printing can, in various embodiments, be over one or more substrates, such as white and/or toned substrates.

Authentication images and visible targets can be printed via bitmap approaches and/or via custom font/character set approaches. Custom font/character set approaches are discussed in greater detail hereinbelow. Also, printing of authentication images and visible targets can be directed by computers including personal computers, factory computers, and smartphones.

Where, for example, a smartphone is used, an app running on the smartphone can receive data utilizable for printing an authentication image and/or visible target from a central computer or website.

**[0056]** As an example, an authentication image can include image elements that are arranged at or near 90 degrees (or 0 degrees) and which form a background image, and image elements that are arranged at or near 45 degrees and which form a latent image. Here, the at or near 90 degree (or 0 degree) background image can yield benefits including: a) camouflaging the latent image; b) creating distortions that carry over the latent image; c) making the latent image not visible to the human eye, a scanning device, or a camera; and d) causing attempts to capture (e.g., via scanner or smartphone camera) the image elements to fail, resulting in the capture of an image with fewer than the intended image elements (or different than the intended image

elements), thus signaling a non-original authentication image. In this example, image elements for the background image are arranged at or near 90 degrees (or 0 degrees), and image elements for the latent image are arranged at or near 45 degrees. However, in various embodiments other values can be used for the two angles. Also, in this example the authentication image includes a single latent image. However, in various embodiments the authentication image can include several latent images. The several latent images can, as one example, have their image elements arranged at the same degree value (e.g., there can be two latent images, each made up of image elements arranged at or near 45 degrees). As another example, one or more of the several latent images can have their image elements arranged at different degree values (e.g., there can be two latent images, with the first made up of image elements arranged at or near 45 degrees, and the second made up of image elements arranged at a different degree value). In various embodiments, where multiple latent images are employed, one or more of the latent images can be split apart in their color makeup (e.g., such that one or more sections thereof appear in two or more colors).

[0057] As another example, an authentication image can include: a) image elements that are arranged at or near 45 degrees and which form a first background image; b) image elements that are arranged at or near 90 (or 0 degrees) degrees and which form a second background image; and c) image elements that are arranged at or near 135 degrees and which form a latent image. Here, the at or near 45 degree first background image and the at or near 90 degree (or 0 degrees) second background image can yield benefits including those noted above (e.g., making the latent image not visible to the human eye, a scanning device, or a camera). In this example, image elements for the first background image are arranged at or near 45 degrees, image elements for the second background image are arranged at or near 90 degrees (or 0 degrees), and image elements for the latent image are arranged at or near 135 degrees. However, in various embodiments other values can be used for the three angles. Also, in this example the authentication image includes a single latent image. However, in various embodiments the authentication image can, in a manner analogous to that discussed above, include several latent

images. Accordingly, as just one example, there can be two latent images, each made up of image elements arranged at or near 135 degrees. Further accordingly, as just another example, there can be two latent images, with the first made up of image elements arranged at or near 135 degrees, and the second made up of image elements arranged at a different degree value.

**[0058]** Although authentication images have been discussed herein as being made up of one or more latent images and one or more background images, other possibilities exist for applying the approaches discussed herein. For example, authentication images can, as an alternative to or in addition to including one or more background images, include one or more graphic overlays. Such graphic overlays can be implemented in a manner generally analogous to that discussed herein with respect to background images. However, in various embodiments background images can be situated behind latent images graphic overlays can be situated in front of latent images.

**[0059]** In various embodiments, a visible target can be located in or adjacent to an authentication image. A visible target can, as just some examples, aid in the detection, filtration, and/or decoding of a corresponding authentication image. As just some further examples, a visible target can assist in functions, such as glare detection and automatic zooming, that can make use of the location of the visible target. A visible target can, as just some examples, make use of black and white, colors, and/or pairings of high-contrast colors.

**[0060]** A visible target, which can also be referred to as a proof locator, can, as just an example, be a plus-shaped image. Further, the visible target can have one or more distinct attributes. In various embodiments, these distinct attributes can be known to software running on a camera-equipped smartphone (or other device) that is to perform extraction (or other operations). These extraction operations (or other operations) can include operations performed with respect to an authentication image to which the visible target corresponds. Such knowledge can assist the software in performing the extraction (or other operations). The distinct attributes can, as just some examples, include one or more of: a) size of the visible target relative to the corresponding authentication image; b) position of the visible target in or adjacent to the

corresponding authentication image; c) a distinct and/or specific white space configuration of the visible target; and d) a distinct and/or specific width of an outlined rule of the visible target.

Various colors can be used for the outlined rule. For instance, the outlined rule can be black.

Shown in Fig. 1 is a zoomed-in view of a visible target 103 of an example authentication image 101.

**[0061]** A visible target can take the geometric form of a plus shape. Such plus shape can, for instance be a cross with four arms of equal (or near equal) length. The use of a plus shape for the visible target can yield benefits including balance of simplicity and distinction. For instance, because the plus shape is a simple and distinct shape it can be evaluated mathematically for fast performance when processing large amounts of contours extracted from a high-resolution camera image. Such operations and the capture of such an image can be performed, for instance, by a smartphone.

**[0062]** According to various embodiments, a smartphone (or other computer) can act to detect a visible target from a camera image by first performing a contour extraction operation on the image. Subsequently, the smartphone (or other computer) can, for each of some or all of the extracted contours, measure the distances of the points of that contour from the center of that contour. Where a given contour is a visible target, such distance from center point determination can yield a pattern indicative thereof. In various embodiments, when ascertaining a given contour to be a visible target, the smartphone (or other computer) can ascertain the location of the visible target contour within the image.

**[0063]** For example, shown in Fig. 2 is a representation 201 of a smartphone (or other computer) having performed such a contour extraction operation on an image (e.g., on a smartphone-captured image). As depicted by Fig. 2, the extracted contours include contour 203 corresponding to a visible target, and contours 205 corresponding to other than the visible target (e.g., contours corresponding to noise). Then, shown in Fig. 3 is a distance-from-center-point plot 301 for an extracted contour which corresponds to a visible target. Here, the plot exhibits a pattern indicative of the extracted contour corresponding to a plus-shaped visible target. With

respect to Fig. 3, it is noted that the number of points that correspond to the plus-shaped visible target within the plot can vary. But, the plus-shaped visible target can nevertheless exhibit within the plot a pattern of four evenly distributed peaks and valleys. In various embodiments, evaluation of the peaks and valleys can be made by utilizing the halfway value between the minimum distance from the center to the maximum distance from the center.

**[0064]** As another example advantage of utilizing a plus-shaped visible target, such plus shape can retain detectable form down to a very small scale. As such, benefits such as providing a wider range of proximity in which to detect the visible target can accrue. Additionally, where a plus shape is used for the visible target, the uniformity of the arms of the plus can be used by the smartphone (or other computer) to determine the exterior points of the corresponding authentication image. These exterior points can, as just one example, be used in a reverse-transformation from perspective/3D space to 2D space. Once the smartphone (or other computer) has translated the authentication image in this way, the smartphone (or other computer) can apply filtration to enhance the information for readability. As yet another example advantage of utilizing a plus-shaped visible target, the discrete contrast offered by such a visible target's unprinted area outlined by the visible target's printed area can offer a device camera (e.g., a smartphone's camera) an optimal (or near-optimal) visual component to auto-focus on at a close distance from the visible target.

**[0065]** Once the smartphone (or other computer) has determined a given contour to be a visible target, and/or has determined the location of the visible target within the captured image, various supporting functions (e.g., supporting app functions) can be employed to aid one or more of: a) operations performed by the smartphone (or other computer) with respect to the authentication image (e.g., yielding a latent image from the authentication image); and/or b) user experience. One example supporting function is glare detection. Such glare detection can include identifying an intense (e.g., the most intense) point of brightness on the captured image in relation to the location of the visible target and a surmised area of the authentication image surrounding the visible target (e.g., surmised utilizing one or more of the above-noted distinct

attributes of the visible target). Another example supporting function is an auto-zoom feature. Such auto-zoom feature can include increasing and/or decreasing camera zoom according to an optimal size (or near optimal size) for filtration, extraction, and/or decoding. Such zoom of the camera can be useful, for instance, for capturing small and/or dense information of an authentication image.

**[0066]** The combination of the inner white space of the visible target and the surrounding color of the visible target can, in various embodiments, provide a contrast basis with which the authentication image can be assessed by the smartphone (or other computer). As just an illustration, the center of the visible target being white, and/or the knock-out color of a corresponding print design, can provide a baseline color value with which to perform filtration (e.g., binary thresholding), and/or can be used when calculating various aspects of the authentication image (e.g., printed/unprinted ratio).

**[0067]** With reference to Fig. 4, it is noted that a further advantage of utilizing a plus shape for the visible target can include it having the potential for being visually recognizable and/or iconic, such as when the visible target is deployed in consumer-facing applications. For instance, consider that one of the most familiar consumer-oriented information marks is the QR code 401. The QR code has good recognizability to the public, with its iconic form of four blocky anchor points with one as an anchor. Then, further consider that the authentication image discussed herein (e.g., as depicted in Fig. 4 as authentication image 403): a) has the capability of printing much smaller than a QR code; and b) achieves its own iconic look with, in various embodiments, a plus-shaped visible target at its center. As such, the authentication image discussed herein has the potential for being at least as visually recognizable and/or iconic as the QR code, if not more so.

**[0068]** In some embodiments, an authentication image can be printed using a bitmap approach. In other embodiments, an authentication image can be printed using a custom font/character set approach. Such a custom font/character set approach can include, for example, formulating a custom font and/or character set made up of characters that each provide one or

more image elements of the sort discussed herein, or portions thereof. Such a custom font/character set approach can be used both when printing authentication images that include visible targets of the sort discussed herein, and when printing authentication images that do not include visible targets. When such a custom font/character set approach is used in printing an authentication image that does include a visible target, the custom characters can be used both in printing the visible target component of the authentication image, and when printing other components of the authentication image. In some embodiments, a vector-based approach can be used in the creation of the custom font/character set. In other embodiments, a raster-based approach can be used in the creation of the custom font/character set. However, a vector-based approach can have a potential for yielding more consistent results than a raster-based approach.

**[0069]** Printing an authentication image using a custom font/character set approach can yield various advantages. For example, printing an authentication image in this way (e.g., when using a vector-based approach) does not require knowledge of printer resolution (or other printer specifics) in order to print authentication images across a variety of print devices. Another example advantage of printing an authentication image using a custom font/character set approach is that the number of lines per inch of the authentication image can be changed by changing the size of characters used to compose the authentication image.

**[0070]** Then, yet another example advantage of printing an authentication image using a custom font/character set approach is that of variability when creating the authentication image. In particular, because the authentication image can be composed of custom characters of the sort noted, there is not call that an individual bitmap be generated for each authentication image. Further in particular, because the authentication image can be composed of custom characters of the sort noted, authentication image creation using variable data can be performed (e.g., with the number of characters and/or their positions within the authentication image being variably printed). Additionally in particular, because the authentication image can be composed of custom characters of the sort noted, easier variability when incorporating background image camouflage

features can be achieved (e.g., by variably printing the number of characters and/or positions of characters used to form the background image(s)).

**[0071]** Further, an additional example advantage of printing an authentication image using a custom font/character set approach is that of easier and/or faster authentication image generation (e.g., once the custom character set has been built, generation of an authentication image mainly calls for merely placing appropriate characters of the pre-built set). Yet another example advantage of printing an authentication image using a custom font/character set approach is that of flexibility in terms of authentication image structure. For instance, custom screening patterns can be used in creation of characters, including a variety of angle combinations and line thickness modulations. As such, screening options of characters can advantageously be not dependent on conventional screening. Custom screening patterns can, as just some examples, achieve not only efficient readability (e.g., when utilizing an app running on a smartphone), but also increased distortion when unauthorized duplication attempts are made.

**[0072]** Another example advantage of printing an authentication image using a custom font/character set approach is that the area of the authentication image can be increased. In particular, for instance, the use of a custom font/character set to composite an authentication image allows the location of the latent image portions thereof to be more readily ascertained.

**[0073]** Shown in Fig. 5 is an example authentication image 501 including a background image 503 formed using image elements that are arranged at or near 90 degrees, and further including latent images 505A/505B formed using image elements that are arranged at or near 45 degrees. Then, shown in Fig. 6 is the result of a thwarted attempt to duplicate the authentication image of Fig. 5. Here, because of the authentication image approaches discussed herein, the attempt has failed, resulting in the capture of an image 601 with other than the intended image elements, thus signaling a non-original authentication image.

**[0074]** Also, an authentication image can be authenticated by analyzing the width/spacing (and/or angle) of the image elements that make up the authentication image. The analysis can be performed by authorized software (e.g., an authorized app running on a smartphone). As one



example, the analysis can determine whether the width/spacing (and/or angle) of the image elements is consistent globally (or nearly consistent globally) throughout the authentication image. As another example, the analysis can determine whether the width/spacing (and/or angle) of the image elements exhibits regular variability globally (or near regular variability globally) throughout the authentication image. Here, the analysis can leverage inadequacies and/or idiosyncrasies of low-resolution print devices that would cause an unauthorized printing of a duplicated authentication image to not match an original of that authentication image in terms of image element width/spacing (and/or angle). Still, authorized printing of an authentication image by low-resolution print devices can be provided for by implementing approaches that compensate for the inadequacies and/or idiosyncrasies of these print devices. In this way, such low-resolution print devices can print authentication images exhibiting image element width/spacing (and/or angle) that satisfy the noted authentication analysis. It is noted that low-resolution print devices, as discussed herein throughout, can include home/office printers and low-resolution industrial printers.

**[0075]** Turning to Fig. 7, shown is a depiction of an uncompensated print file 701 for an authentication image. Also shown in Fig. 7 are: a) a depiction 703 of the uncompensated print file 701 as printed by a 2400 dpi flexographic printer; b) a zoom 705 of the uncompensated print file 701 as printed by a 600 dpi inkjet; c) a zoom 707 of the uncompensated print file 701 as printed by a 812 dpi liquid ink printer; and d) a zoom 709 of the uncompensated print file 701 as printed by a 600 dpi toner-based laser printer.

**[0076]** As shown by Fig. 7, when the uncompensated print file 701 is directly printed (i.e., rather than printed using a corresponding compensated print file as discussed herein below) by the 600-dpi inkjet, the print result includes rough line edges 711 and bent lines 713. These rough line edges 711 and bent lines 713 cause the print result to not match the uncompensated print file 701 in terms of image element width/spacing (and/or angle). Likewise, when the uncompensated print file 701 is printed without compensation by the 812-dpi liquid ink printer, the print result includes oversize lines 715 that cause the print result to not match the uncompensated print file

701 in terms of image element width/spacing (and/or angle). Further, when the uncompensated print file 701 is printed without compensation by the 600-dpi toner-based laser printer, the print result includes missing line portions 717 that cause the print result to not match the uncompensated print file 701 in terms of image element width/spacing (and/or angle).

Additionally shown in Fig. 7 are: a) a zoomed-out view 719 corresponding to zoom 705; and b) a depiction 721 of the uncompensated print file 701 as printed by a low-resolution (e.g., home/office) thermal printer. As depicted by the figure, such uncompensated prints deviate from uncompensated print file 701.

**[0077]** As referenced, the authorized printing of an authentication image by low-resolution print devices can be provided for. In particular, such can be achieved by generating a compensated print file from an uncompensated print file. Where, say, a low-resolution (e.g., home/office) 600-dpi inkjet printer prints an authentication image by way of such a compensated print file, the print result can match (or nearly match) a corresponding uncompensated print file, due to the compensated print file compensating for inadequacies and/or idiosyncrasies of the inkjet printer. As such, returning to the example of Fig. 7 the 600-dpi inkjet can generate a print result that matches (or nearly matches) flexographic print result 703, rather than the print result of zoom 705.

**[0078]** The generation of a compensated print file from an uncompensated print file can utilize one or more compensatory formulas and/or rules based on known idiosyncrasies/inadequacies of a given low-resolution print device. For instance, it can be known that the low-resolution print device incorrectly renders an uncompensated print file by weakening instances of a line being situated within a certain known distance range between two other lines. Here, the compensatory formulas and/or rules can thicken these line instances in the compensated print file in such a way that causes those line instances to, when printed, properly match the uncompensated print file.

**[0079]** With further regard to the formulas and/or rules, it is noted that the formulas and/or rules can dictate the thinning or thickening of printed lines, thereby allowing a low-resolution

print device to generate a print result that can satisfy a smartphone app that captures (and determines the validity of) authentication images by considering print consistency of authentication image lines and angles. The formulas and/or rules can utilize various factors to determine how much to thin or thicken lines. As examples, these factors can include: a) print device type; b) print speed; c) print sheet width; d) ink cure and/or air dry time; e) colorant utilized (e.g., inkjet ink, traditional ink, liquid ink, and/or toner); f) substrate utilized (e.g., traditional paper, inkjet receptive paper, metal, and/or plastic); and/or varnish and/or aqueous coatings utilized. As just an illustration, the plastic can be a plastic bag material such as LDPE.

**[0080]** As referenced above, in various embodiments an authentication image can be printed using a custom font/character set approach. Further, such a custom font/character set approach can be used when generating compensated and/or uncompensated print files. For instance, the use of a vector art file based on a custom font/character set can allow a consistent line shape to be retained throughout plating and/or printing processes, via an outlined print file that accomplishes consistent printing without regard to print device dpi.

**[0081]** Where an uncompensated print file is printed by a low-resolution print device, the ensuing print result can exhibit various flaws (e.g., large amounts of spatter and/or unevenness on line edges). Due to these flaws, the ensuing print result can be expected to not scan (or not consistently scan) as valid with a phone app. In various embodiments, the establishment of compensatory formulas and/or rules can involve utilizing an automated process that works backwards. In these embodiments, image element width/spacing (and/or angle) can initially be created in an original, uncompensated print file. Subsequently, operations can be performed to establish compensatory formulas and/or rules applicable to generate a final, compensated print file. Working backwards can include using an automated process that measures, in a print result arising from a low-resolution print device directly printing an uncompensated print file, aspects such as intensity of the colorant splatter. As examples, such colorant splatter can occur from colorant overspray, substrate absorption, wicking, and/or incomplete ink adherence.

**[0082]** Specifically, the establishment of the compensatory formulas and/or rules can seek to yield a compensated print file that, when printed by a low-resolution print device under consideration, satisfies two criteria. Firstly, that printing of the compensated print file by the low-resolution print device yields an authentication image that stays clean enough (e.g., in terms of white space percentage to black image percentage ratio) to scan (and/or consistently scan) as valid with a smartphone app. And, secondly, that if an unauthorized attempt is made to duplicate (e.g., using a home/office copier or desktop scanner) the print result arising from the printing of the compensated print file, that such duplication will fail, with interference and/or image loss ensuing. In particular, the failure can be such that the authentication image will not scan (and/or will not consistently scan) as valid with the phone app. In this way, presentation of a non-genuine authentication image can be signaled.

**[0083]** Returning to Fig. 7, also depicted is a zoom 723 of a compensated print file as printed by the 600-dpi toner-based laser printer. Here, the compensated print file corresponds to the uncompensated print file 701. It is observed that, due to the use of the compensated print file, the zoom 723 does not exhibit the missing line portions 717 of the zoom 709.

**[0084]** The discussed use of compensated print files can yield various benefits. For example, according to conventional approaches low-resolution print devices have not been considered to be capable of being used for security printing due to failings including their low dpis and their print processes. In particular, according to conventional approaches on order of 2400 dpi has been considered to be the minimum dpi necessary to perform security printing. For perspective, it is noted that digital/thermal ink presses exhibit dpi capabilities ranging from on order of 203 dpi to on order of 812 dpi. However, via the discussed use of compensated print files, low-resolution print devices (e.g., low-resolution industrial printers, desktop printers, toner-based printers, digital inkjet presses, and pad printing presses) can be used for security printing (e.g., allowing for home printing of a theater ticket that includes an authentication image). Beyond allowing security printing to be performed using low-resolution print devices conventionality considered incapable of that task, as another example benefit via the discussed use of

compensated print files various colorants (e.g., home/office colorants and colorants used in conjunction with low-resolution industrial printers) conventionality considered incapable of being used for security printing (e.g., due to the splatter that they exhibit) can be used. In this way the use of such colorants (e.g., inkjet fluids, toner, and liquid inks) can be enabled, where intaglio, flexographic, and/or offset inks were traditionally thought required. As a further example benefit, via the discussed use of compensated print files various substrates (e.g., home/office substrates and substrates used in conjunction with low-resolution industrial printers) conventionality considered incapable of being used for security printing (e.g., due to their absorption characteristics) can be used for this purpose. As just some examples, such substrates can include thermal print papers, fabrics, polyesters, rough/ coarse surfaced substrates, and/or porous surfaced substrates. Traditionally, low resolution printers (especially desktop units) have been excluded from printing security features because of their inability to accurately produce a consistent, effective, smartphone authenticatable image. However, via the discussed use of compensated print files this limitation can be overcome. More generally, the functionality discussed herein can yield an authentication image that contains image elements that affect the consistency of print colorant applied to and/or absorbed by a substrate such that: a) unauthorized copying of the authentication image is impeded; and b) analysis software (e.g., running on a smartphone) can determine that the authentication image is not genuine, and can signal such to a user. The configuration of such image elements can be termed intentional spacing.

**[0085]** As discussed above, in various embodiments a visible target can be located in or adjacent to the authentication image. Shown in Fig. 8 is a visible target 801 that is situated adjacent to (and in particular adjacent and at a corner of) an authentication image 803. According to the example of Fig. 8, the visible target 801 takes the form of a character, in particular the letter "M." Additionally shown in Fig. 8 is a visible target 805 that is situated in an authentication image 807. According to the example of Fig. 8, the visible target 805 takes the form of a plus shape. The use of a visible target can yield benefits including aiding the ability of a smartphone (or other capture device) to locate, orient, focus, detect glare and/or adjust captured

image contrast levels. Still further shown in Fig. 8 is a visible target 804 that is situated in the authentication image 803.

**[0086]** As discussed, authentication of an authentication image can include determining whether image element width/spacing (and/or angle) is consistent globally throughout an authentication image. As also discussed, such authentication can include determining whether image element width/spacing (and/or angle) exhibits regular variability globally throughout an authentication image. Shown in Fig. 9 is an example authentication image 901 in which the width and spacing of both print and white space is consistent globally throughout authentication image 901. In this way, the consistency of the width and spacing of the image elements of authentication image 901 lends itself to on one hand authenticity determination, and on the other hand to destruction of a duplicated authentication image. Then, also shown in Fig. 9 is an example authentication image 903 in which the width, spacing, and angle of image elements varies globally throughout authentication image 903. Here, the variability of the width, spacing, and angle of the image elements of authentication image 903 lends itself to on one hand authenticity determination and on the other hand to destruction of a duplicated authentication image. Additionally shown in Fig. 9 is a zoom 905 of authentication image 903.

**[0087]** With further regard to the discussed variability, it is noted that the relation of any image element to any other image element can be variable within an authentication image. In this regard, shown in Fig. 9 is an example of image elements 907 being variable within an authentication image to image elements 909. Also in this regard, shown in Fig. 9 is a further example of image elements 911 being variable within an authentication image to image elements 913.

**[0088]** An authentication image can include a visible graphic (e.g., visible to the naked eye). In particular, various properties of image elements of the authentication image can be variable and integrated throughout the authentication image so as to create the visible graphic. The visible graphic can, for instance, be a logo, an emblem, a design, or a trademark. Shown in Fig. 10 is an example authentication image that includes a soccer ball visible image 1001. The soccer ball

visible image 1001 arises from the noted application of image elements. Also shown in Fig. 10 is an example authentication image that includes a lock visible image 1003 that arises from the noted application of image elements.

**[0089]** An authentication image can include non-segmented and/or segmented image elements that are placed at or near a given print density (e.g., at or near a print density under 30%). In this way, the image elements can, when subjected to unauthorized duplication, disappear, distort, and/or exhibit a shift in color hue. In some embodiments the image elements can form one or more microimage, microdot, and/or microtext instances that are viewable under magnification in an authorized print (e.g., printed using a compensated print file).

**[0090]** As an example, using this approach placed rows of dot image elements can form microtext (e.g., the letters “AUT” signifying an authenticated image). This microtext can change hue, distort, and/or disappear upon unauthorized copy or scanning. Turning Fig. 11, shown is a cropped view 1101 of an authorized print of microtext. Then, view 1103 shows a zoom of the authorized microtext print. Where an unauthorized copy is made, the microtext can disappear.

**[0091]** Also, an authentication image can include supplemental image elements. These supplemental image elements can be placed out of sync with the angulation of other image elements of the authentication image. Because unauthorized copying distorts image elements of an authentication image, such supplemental image elements can be distorted in an unauthorized copy. As just some examples, supplemental image elements can be situated with: a) latent images; b) background images; and/or c) characters. The noted out of sync placement of supplemental image elements can include turning, tipping, and/or twisting of image elements that exist elsewhere in an authentication image. As an example, there can be only a single supplemental image element (e.g., within a latent images). As another example, there can be multiple supplemental image elements.

**[0092]** The use of supplemental image elements in an authentication image can provide for a covert means of authentication (e.g., by a user or by software analysis). In particular, information regarding a supplemental image element (e.g., the angle and/or location thereof) can be made

available (e.g., stored on a server and/or otherwise available to a smartphone app). Using this information, the supplemental image element can be found in an authorized print. But, due to distortion the supplemental image element will not be locatable in an unauthorized print. In this way, search (e.g., by a smartphone app) for a supplemental image element can provide a covert means of authentication.

**[0093]** Turning to Fig. 12, shown is an authentication image 1201 including a supplemental image element 1203. The supplemental image element 1203 is placed out of sync with the angulation of other image elements of authentication image 1201. Also shown in Fig. 12 is a corresponding zoom 1205. Turning further to Fig. 12, shown is a background image 1207 that includes supplemental image elements 1209. As depicted by the figure, supplemental image elements 1209 are placed out of sync with the angulation of other image elements of background image 1207. Also shown in Fig. 12 is a character 1211 that includes supplemental image element 1213. Supplemental image element 1213 is placed out of sync with the angulation of other image elements of character 1211.

**[0094]** A set of multiple image elements can be used to form a compound image element. An authentication image can include multiple compound image elements. Furthermore, those image elements that form a compound image element can be split into separate color layers for purposes of printing.

**[0095]** The use of compound image elements in an authentication image can serve to inhibit unauthorized copying of that authentication image. In particular, home/office capture devices (e.g., scanners and smartphone cameras) typically capture colors individually, and partial loss of a compound image element occurs when capturing in a particular color. Also, home/office capture devices typically utilize a CMY-based approach. CMY-based approaches typically do not capture non-CMY images in their entirety. As such, where a compound image element is formed in a non-CMY fashion, such can serve to further inhibit unauthorized authentication image copying. Shown in Fig. 13 is an example compound image element 1301. The compound image element 1301 is made up of red color layer image elements 1303 and green color layer



image elements 1305. For purposes of illustration, the red of Fig. 13 is shown using dark gray, and the green of Fig. 13 is shown using light gray. Also shown in Fig. 16 is a zoom 1307 of an authentication image that incorporates instances of compound image element 1301.

**[0096]** Turning to Fig. 14, it is noted that a visible target can exhibit discrete contrast, such as discrete contrast arising from the unprinted area of the visible target as outlined by the printed area of the visible target. Such discrete contrast can offer a smartphone (or other camera device) running authorized software a visual component to assist with auto-focus, such as when the capture device is in close proximity to an authentication image that includes the visible target. Shown in Fig. 14 is an authentication image 1401 including such visible targets in the form of: a) a visible target 1403 that is located in authentication image 1401 and centered therewith; and b) a visible target 1405 that is located in authentication image 1401 and at the upper left corner thereof. Then, zoom 1407 shows detail of visible target 1405, and zoom 1409 shows detail of visible target 1403.

**[0097]** As discussed, printing an authentication image via a custom font/character set approach can allow for variability when creating the authentication image. Using such an approach (e.g., where a vector-based technique is used in creation of a custom font/character set) enables variable authentication images to be generated: a) using an existing data file; b) across a variety of low-resolution print devices; and c) across a variety of home/office imaging devices. Such an existing data file can include: a) a library of font characters; and/or b) a library of visible targets that are prerendered in place (pre-RIPed). Shown in Fig. 15 is a zoom 1501 of an example authentication image printed using the noted custom font/character set approach. In particular, within the authentication image compound image elements 1505 of a single color (depicted as cyan here) are placed over a colorized toned area 1503 of a different color (depicted as light magenta here). For purposes of illustration, the cyan of Fig. 15 is shown using dark gray, and the light magenta of Fig. 15 is shown using light gray.

**[0098]** An authentication image can be placed within or in the vicinity of (e.g., adjacent to) a track and trace element (e.g., a bar code, a QR code, a 2D code, or track and trace text).

Alternatively or additionally, a track and trace element can be placed within an authentication image. The authentication image can be used in determining the authenticity of the track and trace element. The authentication image, after being validated, can allow access to the track and trace system via the track and trace element (e.g., barcode). Thus, if the authentication image is not valid, access is not allowed. In particular, where, for instance, the authentication image scans as valid with a phone app, the track and trace element can be considered proper. In some embodiments, further placed in the vicinity of the track and trace element can be a secondary track and trace numerical code.

**[0099]** As an example, image element width/spacing (and/or angle) can be consistent throughout the authentication image. As another example, image element width/spacing (and/or angle) can exhibit regular variability throughout the authentication image. In some embodiments, a smartphone app can decode such regular variability to one or more values (e.g., one or more spacing values). The smartphone app can use these one or more values to consult a server (or other source) that maps such values to secondary track and trace numerical codes. The smartphone app can then compare a determined secondary track and trace numerical code with a secondary track and trace numerical code placed in the vicinity of a track and trace element under consideration (e.g., a QR code under consideration). Where the comparison yields a match, the smartphone app (or other software) can consider the track and trace element under consideration to be proper. As an alternative, the smartphone app can present the determined secondary track and trace numerical code to a user.

**[00100]** Turning to Fig. 16, shown is a QR code 1601, along with an adjacent authentication image 1603, and a secondary track and trace numerical code 1605. Also shown in Fig. 16 is a QR code 1607, along with situated-therein authentication image 1609, and a secondary track and trace numerical code 1611.

**[00101]** Additionally, an authentication image can be formulated such that certain portions thereof are printed using a colorant invisible under regular light, while other portions thereof are printed using a colorant that is visible under regular light. Portions can be latent images and/or

compound image elements. Such colorant invisible under regular light can be ultraviolet or infrared colorant. As an illustration, with reference to Fig. 17 an authentication image 1701 can include one latent image 1703 printed using invisible colorant, and three latent images printed using visible colorant (not shown). Continuing with the illustration, an authentication image of this sort can provide for both consumer user and investigator user functionality within a single authentication image. In particular, the consumer user can present (e.g., for validity determination using smartphone app) the authentication image under regular light. Under such regular light, the three latent images printed using visible colorant can be exposed. Further, the investigator user can present the authentication image under, say, a blacklight. In this way, the investigator user can have access to all four latent images.

**[00102]** Through the use of such approaches, various benefits can accrue. Continuing with the illustration, the regular light invisibility of the fourth latent image can lead to it remaining undetected by a consumer user, thereby impeding attempts by the consumer user to make an unauthorized copy of the authentication image. As another example, the inclusion of a latent image typically only accessible to investigator users can help assure investigator users of authentication image validity.

**[00103]** Further to printing an authentication image using a low-resolution print device, an authentication image can be created using laser ablation, and/or laser engraving/etching approaches. Such laser ablation approaches can include firstly printing a solid area with black colorant. Subsequently the solid area can be ablated by a laser so as to yield an authentication image. Such laser engraving/etching approaches can include firstly printing a solid area with white or clear colorant. Subsequently the solid area can be engraved/etched by a laser so as to yield an authentication image. Further, these ablation and/or engraving/etching approaches can include generating one or more uncompensated and/or compensated print files in agreement with that which is discussed above (e.g., taking into account ablation and/or engraving/etching device inadequacies and/or idiosyncrasies). In this way a laser ablation and/or engraving/etching can provide an authentication image that on one hand stays clean enough to scan (and/or consistently

scan) as valid, but on the other hand if subjected to unauthorized duplication attempts yields an authentication image that fails to scan (and/or consistently scan) as valid.

**[00104]** Also, an authentication image can be generated using both colorant (e.g., as printed by a low-resolution print device) and laser ablation and/or engraving/etching. Here, certain image elements of the authentication image can be formed using colorant, and other image elements of the authentication image can be formed via laser. Where both colorant and laser approaches are used, a certain portion (e.g., 50%) of image elements can be generated using the colorant approach, and a certain portion (e.g., 50%) of image elements can be generated using the laser approach. Further the colorant-generated image elements can be consistent and/or variable. Likewise, the laser-generated image elements can be consistent and/or variable. As such, as just an illustration, an authentication image can be generated wherein  $m\%$  (e.g.,  $m = 50\%$ ) of the image elements thereof are colorant-generated and consistent, and  $n\%$  (e.g.,  $n = 50\%$ ) of the image elements thereof are laser-generated and variable. As just another illustration, an authentication image can be generated wherein  $m\%$  (e.g.,  $m = 50\%$ ) of the image elements thereof are colorant-generated and variable, and  $n\%$  (e.g.,  $n = 50\%$ ) of the image elements thereof are laser-generated and consistent. In various embodiments where both colorant and laser approaches are used in authentication image generation, a Datalase/SUNlase process can be employed. Turning to Fig. 18, depicted is an example of the discussed laser ablation approach. Firstly, a solid area 1801 can be printed using a black colorant. Afterwards the solid area 1801 can be laser engraved/etched so as to yield an authentication image 1803.

**[00105]** Further to generating an authentication image using a printer, or using or laser ablation or engraving/etching, an onscreen authentication image can be created. A smartphone (or other capture device) can be pointed at a display showing such an onscreen authentication image, and a validity determination can be made for the onscreen authentication image. Devices on which onscreen authentication images can be displayed for validity determination purposes include laptop/desktop screens, television screens, smartphone (or other mobile/smart device) screens, and barcode scanner screens. As just an illustration, an onscreen authentication image

can be displayed on a first smartphone, and a second smartphone can be pointed at the display of the first smartphone.

**[00106]** Generation of an onscreen authentication image can, in a manner analogous to that which is discussed above, include generating one or more uncompensated and/or compensated virtual (e.g., pdf) print files. The generation of these virtual files can take into account display device inadequacies and/or idiosyncrasies. As such, there can be generation of an onscreen authentication image that on one hand stays clean enough to scan (and/or consistently scan) as valid, but on the other hand if subjected to unauthorized duplication attempts yields an authentication image that fails to scan (and/or consistently scan) as valid. As just some examples, like an authentication image generated using print and/or ablation and/or engraving/etching approaches, an onscreen authentication image can be used as a printing plate quality control (QC) image, for printed image on-press, and/or for products undergoing a customs, distribution, brand check, and/or retail environment inspection.

**[00107]** Turning to Fig. 19, shown are a depiction 1901 of a first example onscreen authentication image being displayed on a smartphone screen, and a depiction 1903 of the first example onscreen authentication image being displayed on a laptop/desktop screen. Also shown in Fig. 19 is a depiction 1905 of a second example onscreen authentication image.

**[00108]** Moreover, authentication images generated using print and/or ablation and/or engraving/etching approaches can be used in conjunction with onscreen authentication images. As just an illustration, there can be call that a user use a smartphone to scan as valid both: a) an authentication image generated using print, and/or ablation and/or engraving/etching approaches; and b) an onscreen authentication image. Further according to this illustration, the user can proceed in this way in order to make an authenticity determination of a sports memorabilia item. Here, for instance, the authentication image generated using print and/or ablation and/or engraving/etching approaches can be attached to the memorabilia item, and the onscreen authentication image can be provided to the user via a text message (or via a website to which the user is directed).

[00109] Turning to Fig. 20, shown are: a) a depiction 2001 of an example onscreen authentication image; b) a first example authentication image generated using print and/or ablation and/or engraving/etching approaches 2003; and c) a second example authentication image generated using print and/or ablation and/or engraving/etching approaches 2005.

### **Hardware and Software**

[00110] According to various embodiments, various functionality discussed herein can be performed by and/or with the help of one or more computers. Such a computer can be and/or incorporate, as just some examples, a personal computer, a server, a smartphone, a system-on-a-chip, and/or a microcontroller. Such a computer can, in various embodiments, run Linux, MacOS, Windows, or another operating system.

[00111] Such a computer can also be and/or incorporate one or more processors operatively connected to one or more memory or storage units, wherein the memory or storage may contain data, algorithms, and/or program code, and the processor or processors may execute the program code and/or manipulate the program code, data, and/or algorithms. Shown in Fig. 21 is an example computer employable in various embodiments of the present invention. Example computer 2101 includes system bus 2103 which operatively connects two processors 2105 and 2107, random access memory (RAM) 2109, read-only memory (ROM) 2111, input output (I/O) interfaces 2113 and 2115, storage interface 2117, and display interface 2119. Storage interface 2117 in turn connects to mass storage 2121. Each of I/O interfaces 2113 and 2115 can, as just some examples, be a Universal Serial Bus (USB), a Thunderbolt, an Ethernet, a Bluetooth, a Long Term Evolution (LTE), a 5G, an IEEE 488, and/or other interface. Mass storage 2121 can be a flash drive, a hard drive, an optical drive, or a memory chip, as just some possibilities. Processors 2105 and 2107 can each be, as just some examples, a commonly known processor such as an ARM-based or x86-based processor. Computer 2101 can, in various embodiments, include or be connected to a touch screen, a mouse, and/or a keyboard. Computer 2101 can additionally include or be attached to card readers, DVD drives, floppy disk drives, hard drives,

memory cards, ROM, and/or the like whereby media containing program code (e.g., for performing various operations and/or the like described herein) may be inserted for the purpose of loading the code onto the computer.

**[00112]** In accordance with various embodiments of the present invention, a computer may run one or more software modules designed to perform one or more of the above-described operations. Such modules can, for example, be programmed using Python, Java, JavaScript, Swift, C, C++, C#, and/or another language. Corresponding program code can be placed on media such as, for example, DVD, CD-ROM, memory card, and/or floppy disk. It is noted that any indicated division of operations among particular software modules is for purposes of illustration, and that alternate divisions of operation may be employed. Accordingly, any operations indicated as being performed by one software module can instead be performed by a plurality of software modules. Similarly, any operations indicated as being performed by a plurality of modules can instead be performed by a single module. It is noted that operations indicated as being performed by a particular computer can instead be performed by a plurality of computers. It is further noted that, in various embodiments, peer-to-peer and/or grid computing techniques may be employed. It is additionally noted that, in various embodiments, remote communication among software modules may occur. Such remote communication can, for example, involve JavaScript Object Notation-Remote Procedure Call (JSON-RPC), Simple Object Access Protocol (SOAP), Java Messaging Service (JMS), Remote Method Invocation (RMI), Remote Procedure Call (RPC), sockets, and/or pipes.

**[00113]** Moreover, in various embodiments the functionality discussed herein can be implemented using special-purpose circuitry, such as via one or more integrated circuits, Application Specific Integrated Circuits (ASICs), or Field Programmable Gate Arrays (FPGAs). A Hardware Description Language (HDL) can, in various embodiments, be employed in instantiating the functionality discussed herein. Such an HDL can, as just some examples, be Verilog or Very High Speed Integrated Circuit Hardware Description Language (VHDL). More generally, various embodiments can be implemented using hardwired circuitry without or

without software instructions. As such, the functionality discussed herein is limited neither to any specific combination of hardware circuitry and software, nor to any particular source for the instructions executed by the data processing system.



## CLAIMS

1. An authentication image, comprising:
  - one or more latent images, wherein the latent images indicate authenticity; and
  - one or more background images, wherein the background images work in conjunction with the latent images to inhibit unauthorized duplication of the authentication image, wherein generation of the authentication image utilizes knowledge of idiosyncrasies of one or more of low-resolution print devices or home/office equipment; and
  - wherein authorized software uses knowledge regarding the background images and knowledge regarding the latent images to yield one or more of the latent images from the authentication image.
  
2. The authentication image of claim 1, further comprising one or more visible targets, wherein the visible targets aid in said yielding of the latent images from the authentication image, wherein the visible targets optionally assist in one or more of glare detection or automatic zooming or optionally are one or more of in or adjacent to the authentication image.
  
3. The authentication image of claim 1 or claim 2, wherein detection of the one or more visible targets utilizes contour extraction.
  
4. The authentication image of any one of claims 1-3, wherein one or more of the latent images or the background images are formulated using image elements, wherein the image elements optionally include one or more of lines, line segments, dots, spots, or non-imaged areas.

5. The authentication image of any one of claims 1-4, wherein a first quantity of the image elements are arranged at a first angle and form the one or more background images, and wherein a second quantity of the image elements are arranged at or near a second angle and form the one or more latent images.

6. The authentication image of any one of claims 1-5, wherein the authentication image is at least one of printed via a custom font/character set approach, associated with a track and trace element, wherein the authentication image denotes authenticity of the track and trace element, or an onscreen authentication image, and wherein a validity determination can be made by pointing a device at a display showing the onscreen authentication image.

7. The authentication image of any one of claims 1-6, wherein the authentication image is an onscreen authentication image, wherein the onscreen authentication image is accompanied by a further authentication image, wherein the further authentication image is formed via one of print, ablation, engraving, or etching, and wherein a validity determination can be made by pointing a device at the further authentication image, and at a display showing the onscreen authentication image.

8. A system comprising:

at least one processor; and

a memory storing instructions that, when executed by the at least one processor, cause the system to generate the authentication image of claim 1.

9. A computer-implemented method, comprising:

generating, by a computing system, an uncompensated print file for an authentication image, wherein printing of the uncompensated print file by a low-resolution print device yields a print result not matching the uncompensated print file; and

generating, by the computing system, from the uncompensated print file, a compensated print file for the authentication image, wherein the generation of the compensated print file utilizes known low-resolution print device idiosyncrasies, and wherein printing of the compensated print file by the low-resolution print device yields an authentication image print result that scans as valid.

10. The computer-implemented method of claim 9, wherein unauthorized duplication of the authentication image print result at least one of incurs image loss or fails to scan as valid.

11. The computer-implemented method of claim 9 or claim 10, wherein the authentication image is formulated using at least one of consistent or variable image elements, image elements having a print density that results in one or more of disappearance, distortion, or color hue shift where the authentication image is subjected to unauthorized duplication, or one or more compound image elements, wherein the compound image elements are split into separate color layers.

12. The computer-implemented method of any one of claims 9-11, wherein the generation of the compensated print file utilizes one or more compensatory formulas.

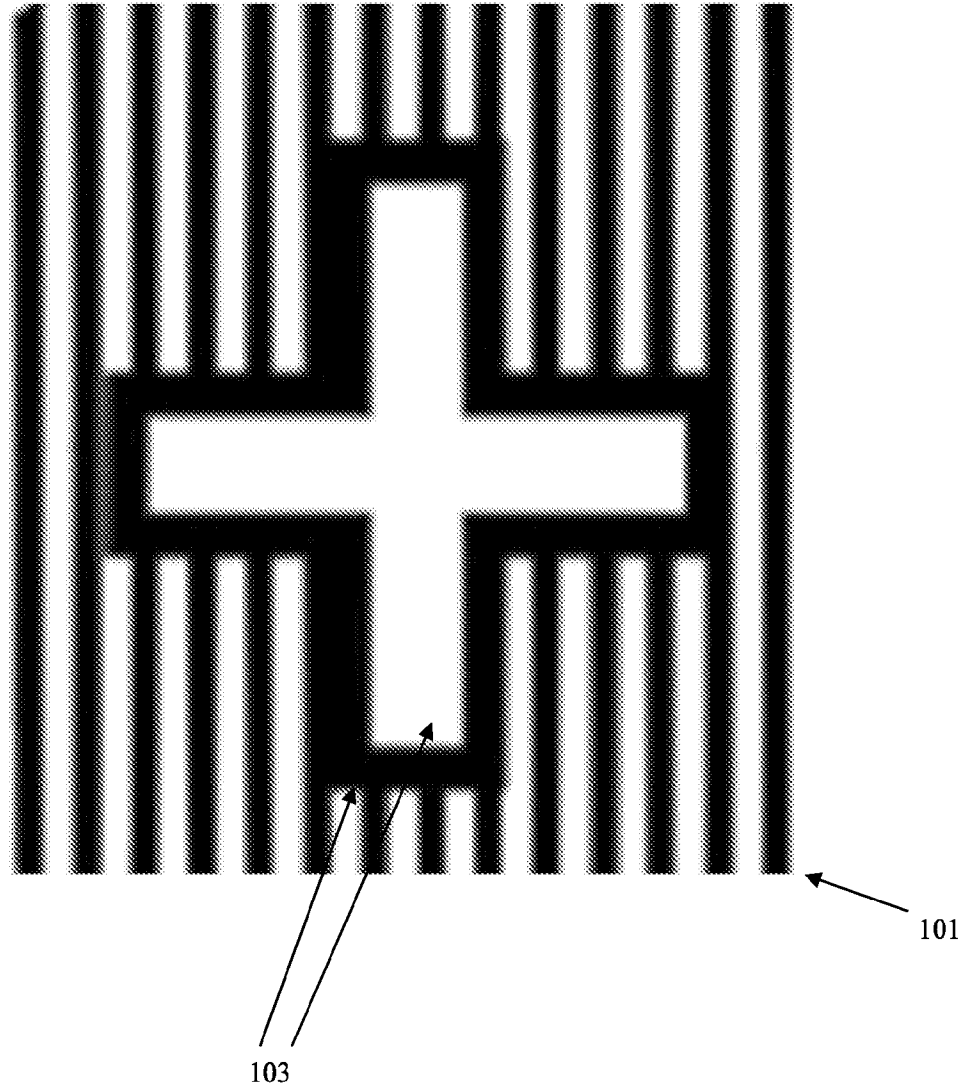
13. The computer-implemented method of any one of claims 9-12, wherein the compensated print file is generated using a custom font/character set approach.

14. The computer-implemented method of any one of claims 9-13, wherein first portions of the authentication image are printed using a colorant invisible under regular light, and second portions of the authentication image are printed using a colorant visible under regular light.

15. A system comprising:

at least one processor; and

a memory storing instructions that, when executed by the at least one processor, cause the system to perform the computer-implemented method of claim 9.



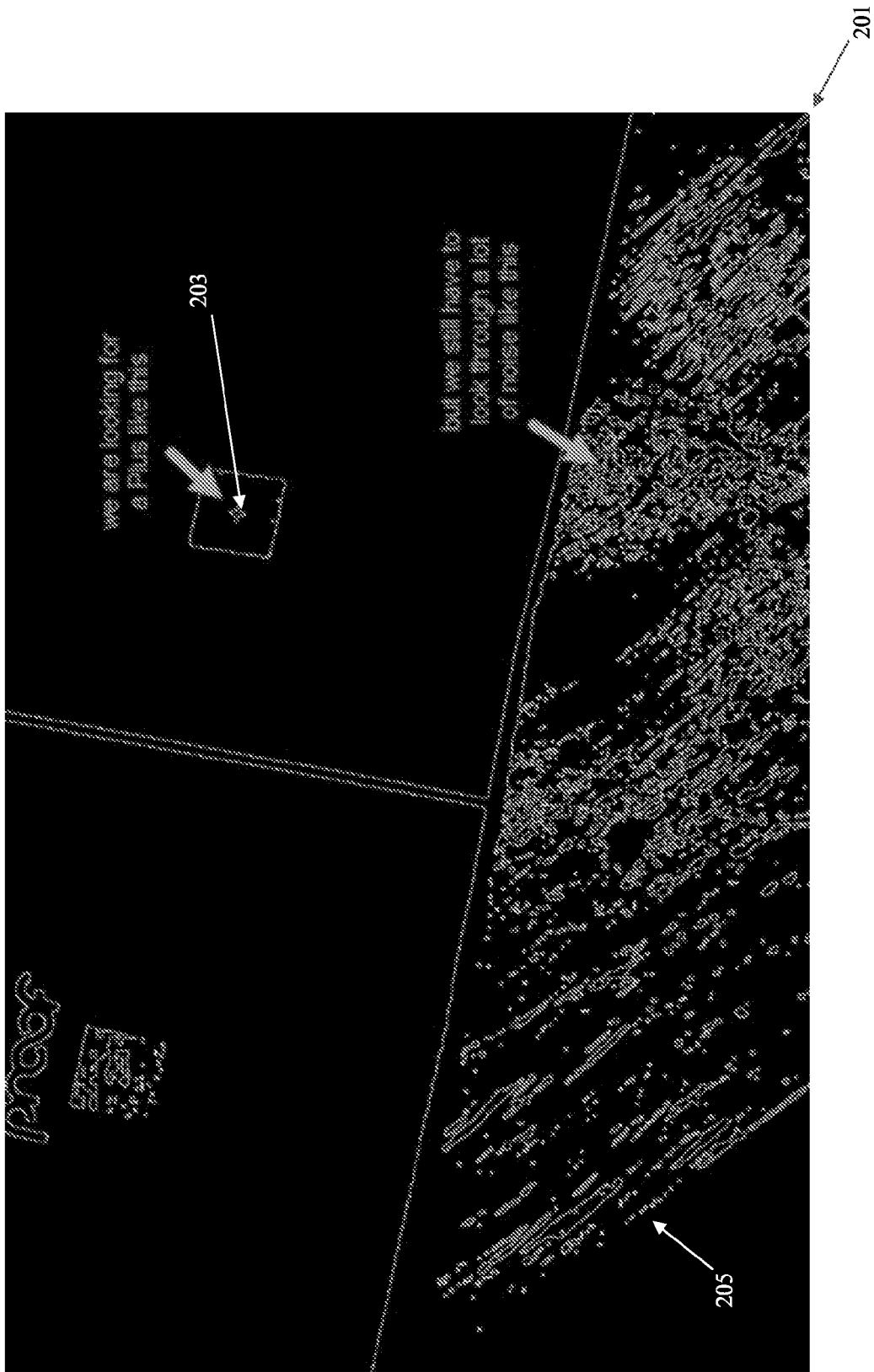


Fig. 2

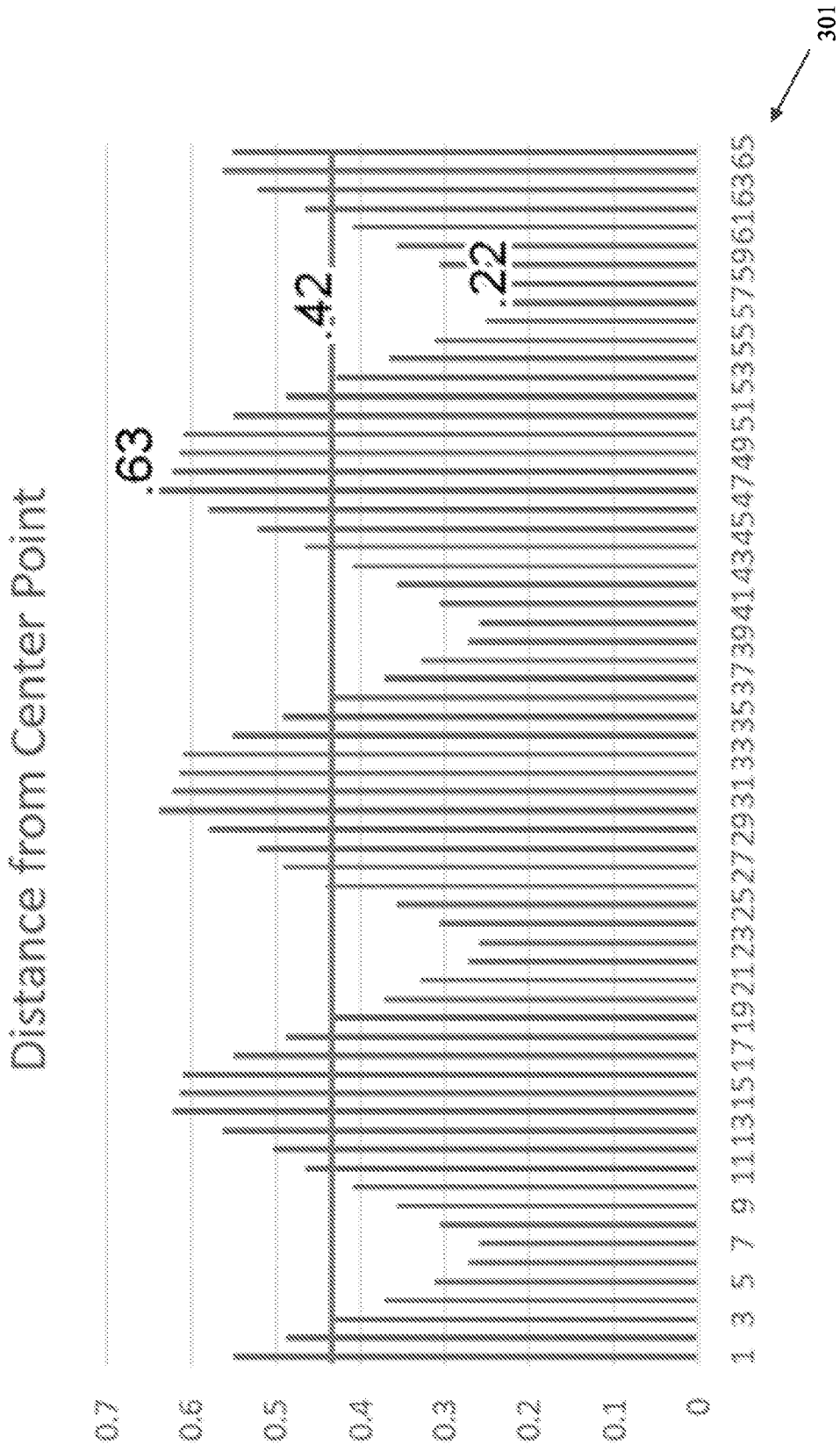


Fig. 3

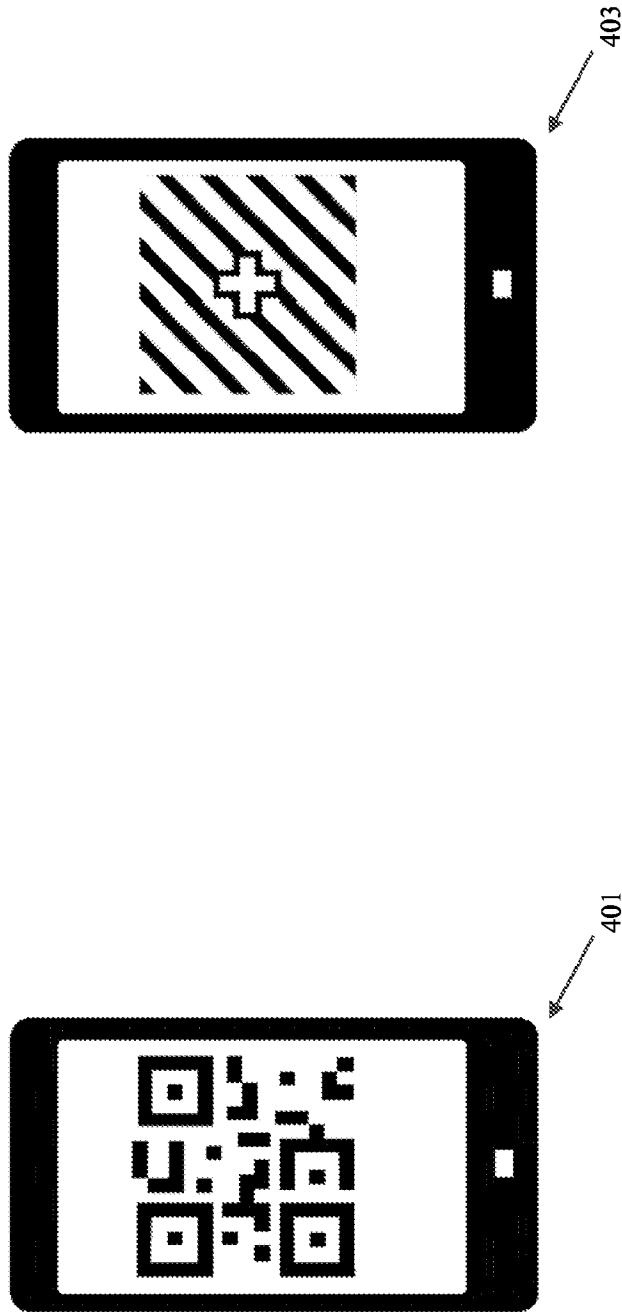


Fig. 4



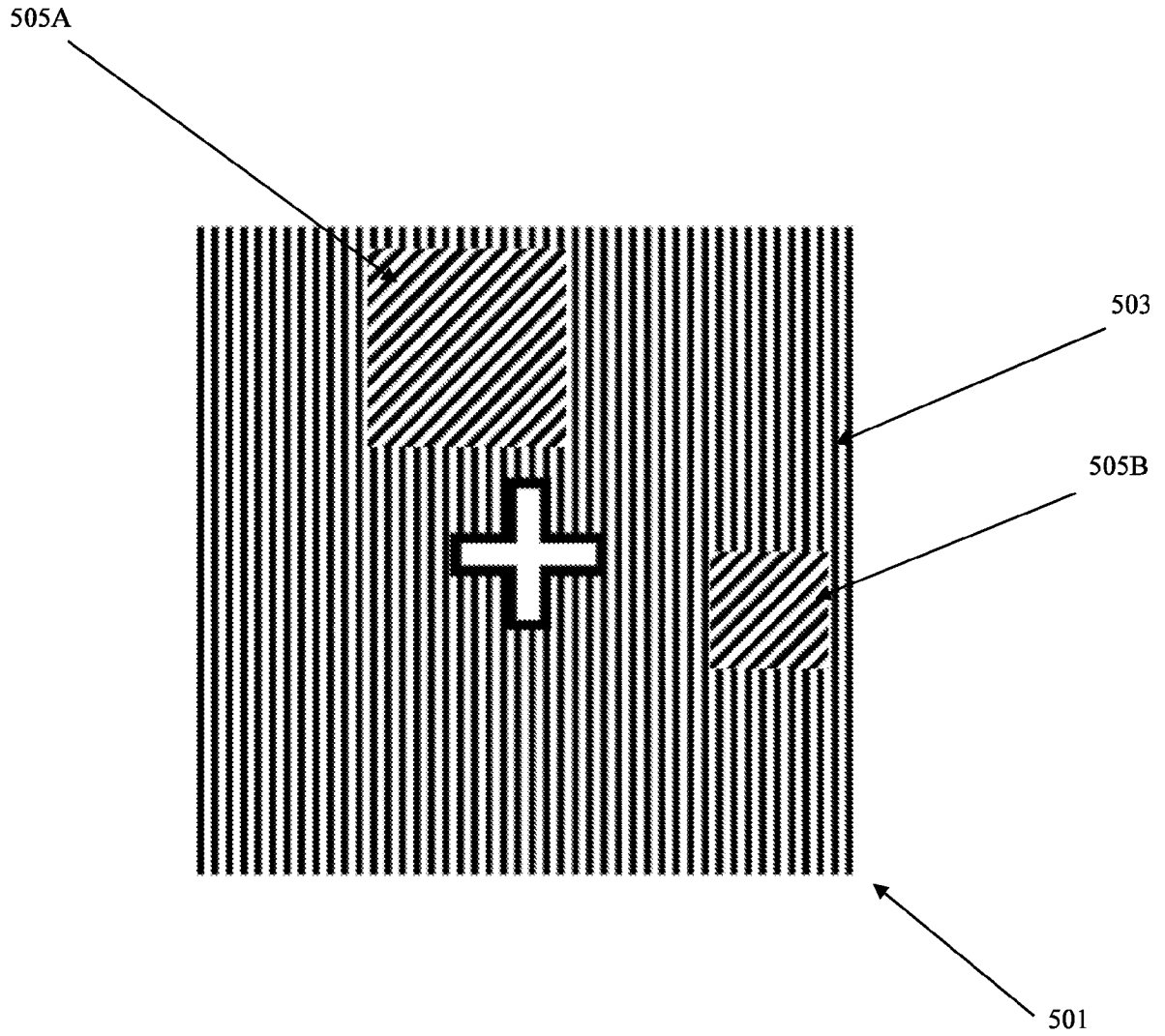


Fig. 5

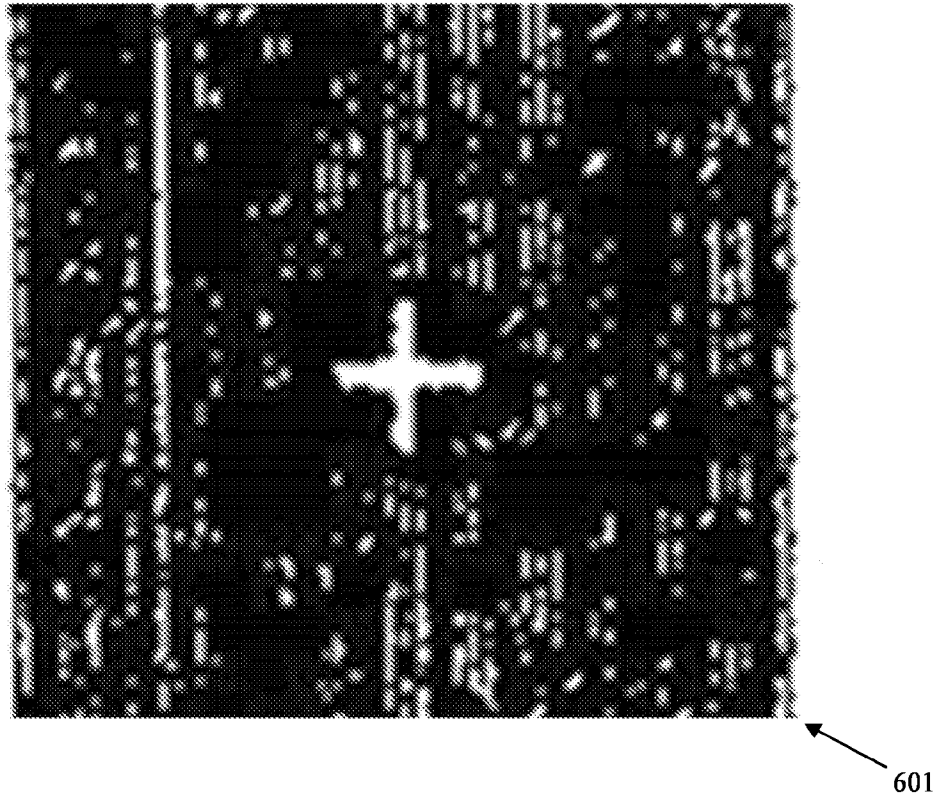


Fig. 6

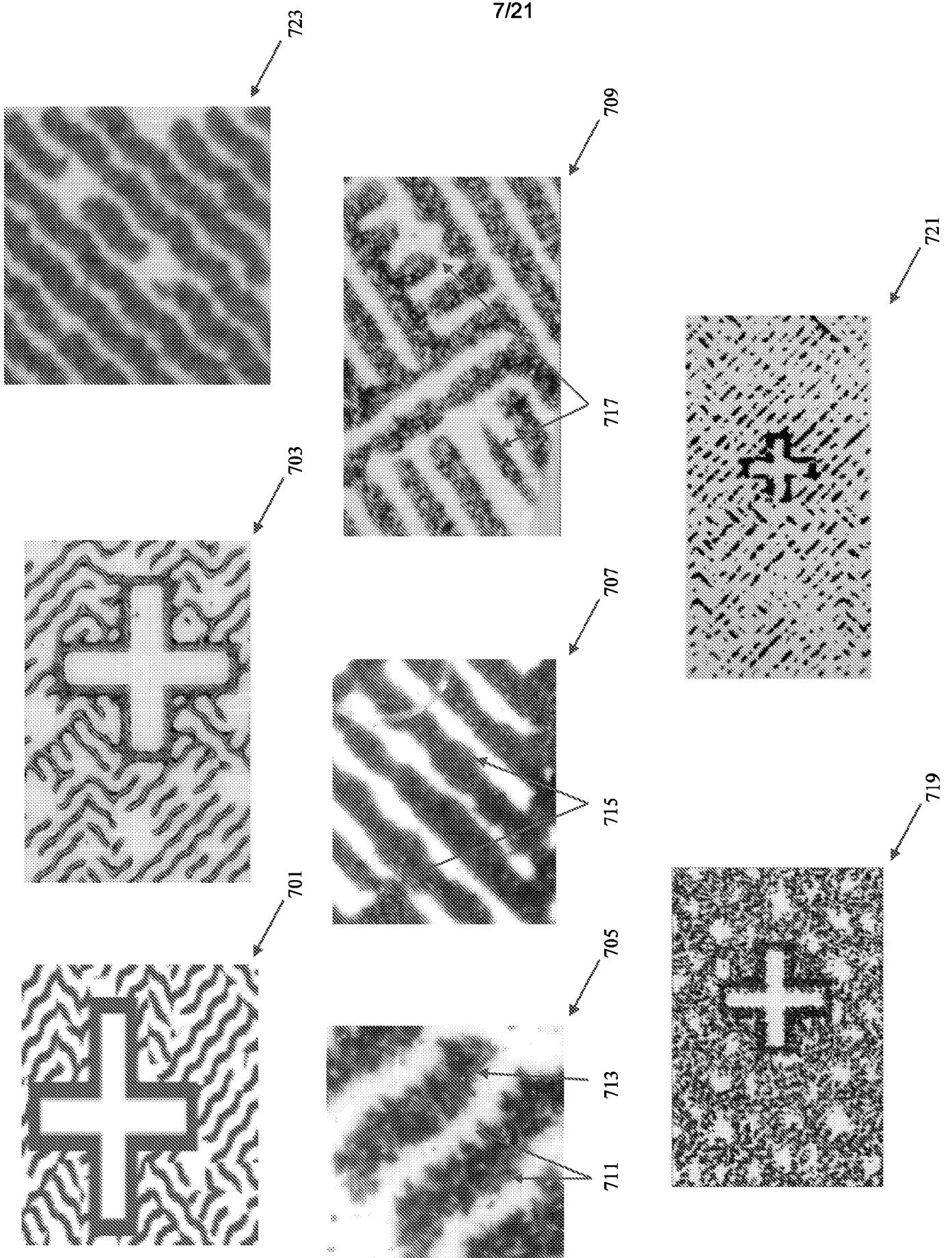


Fig. 7

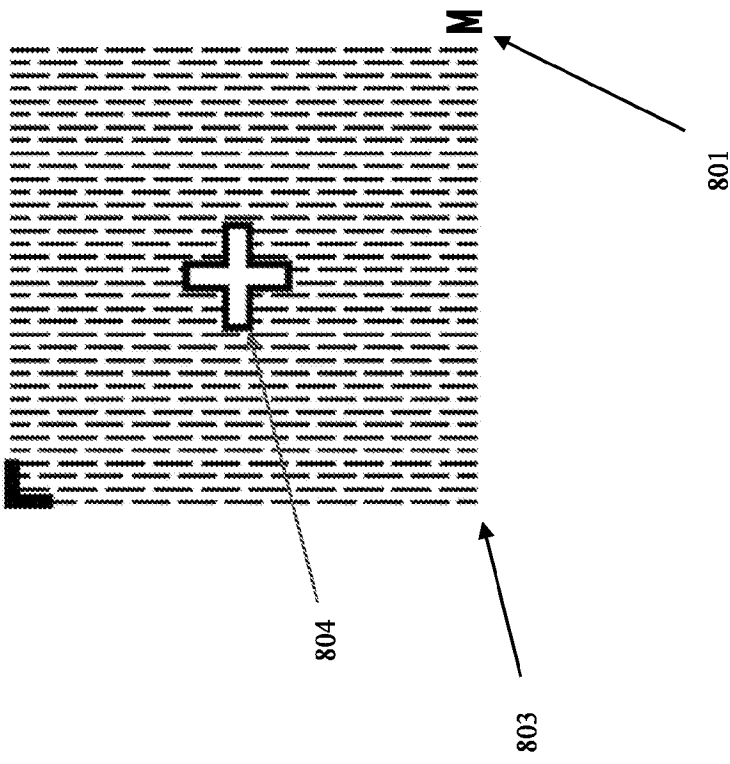
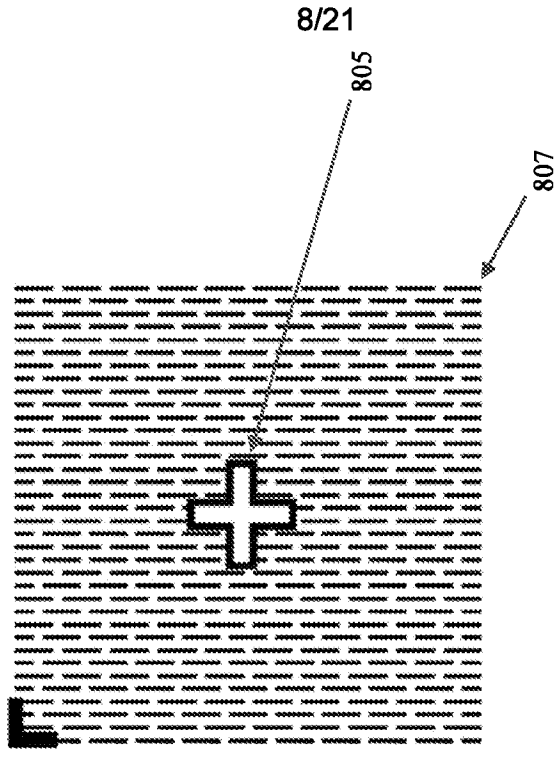


Fig. 8

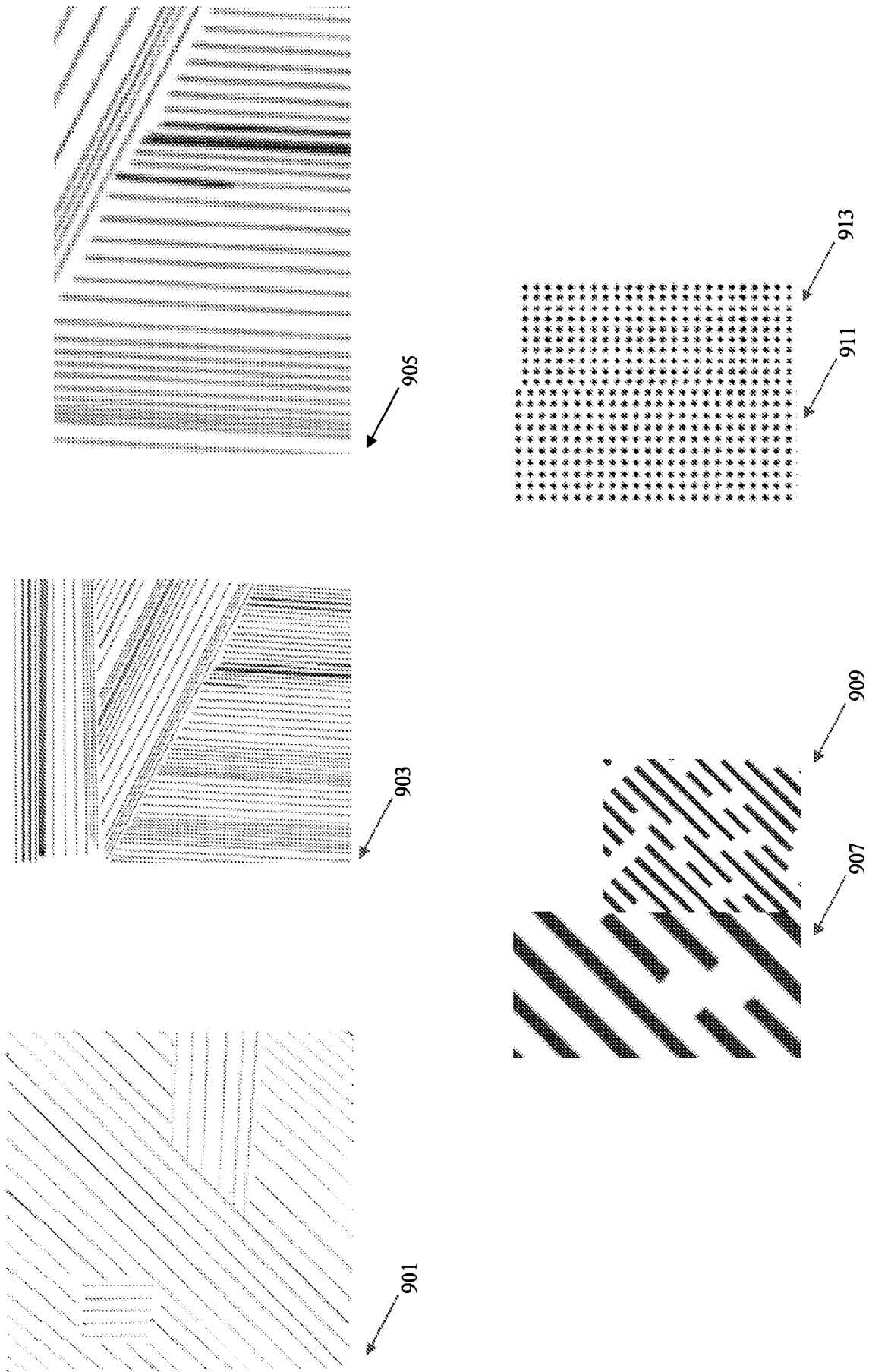


Fig. 9

10/21

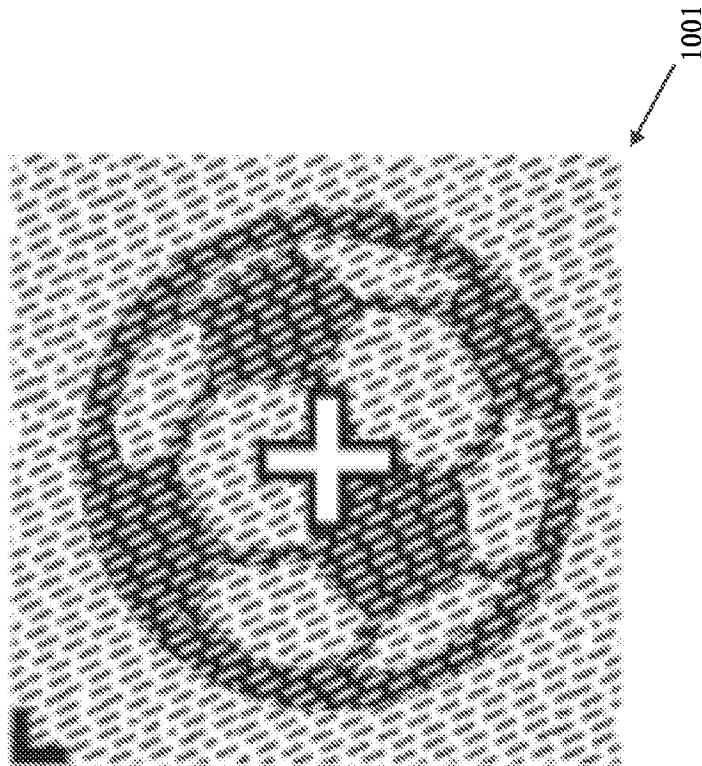
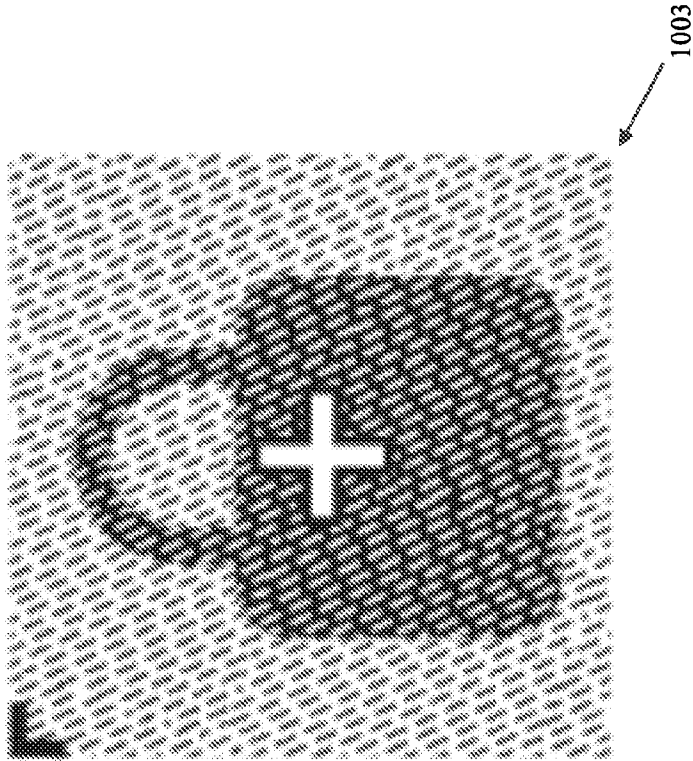


Fig. 10

11/21

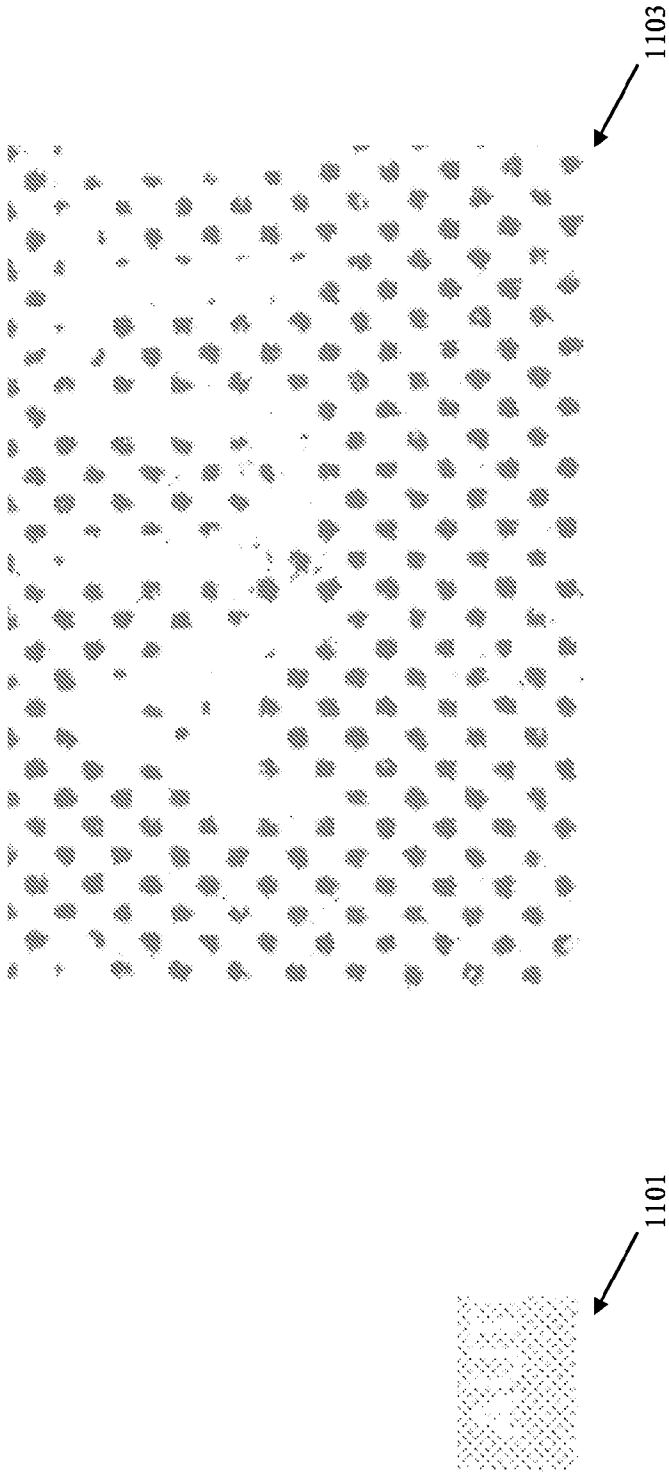


Fig. 11

12/21

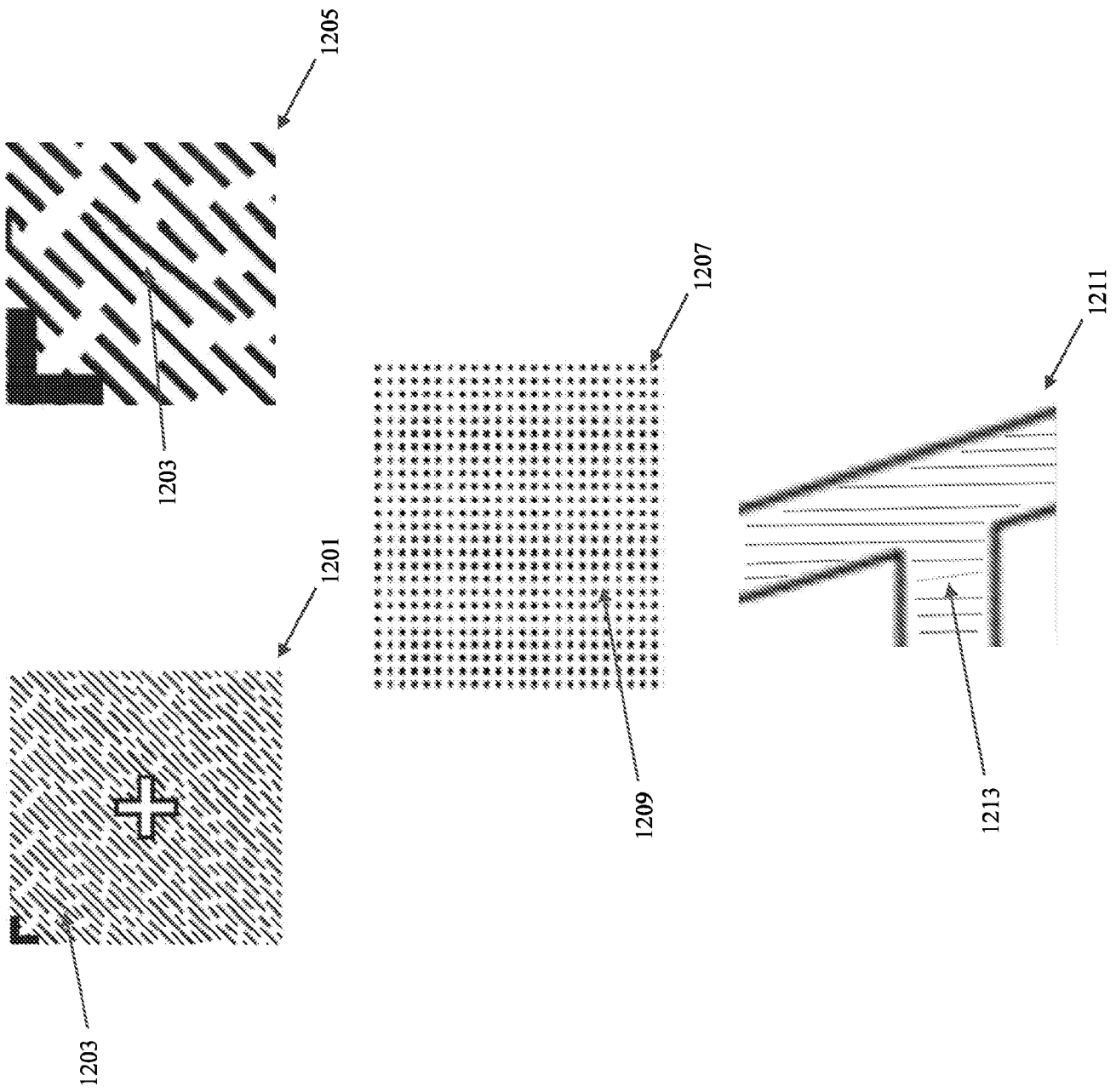


Fig. 12



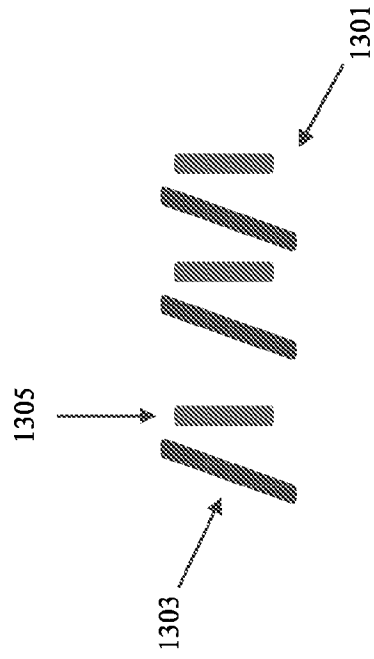
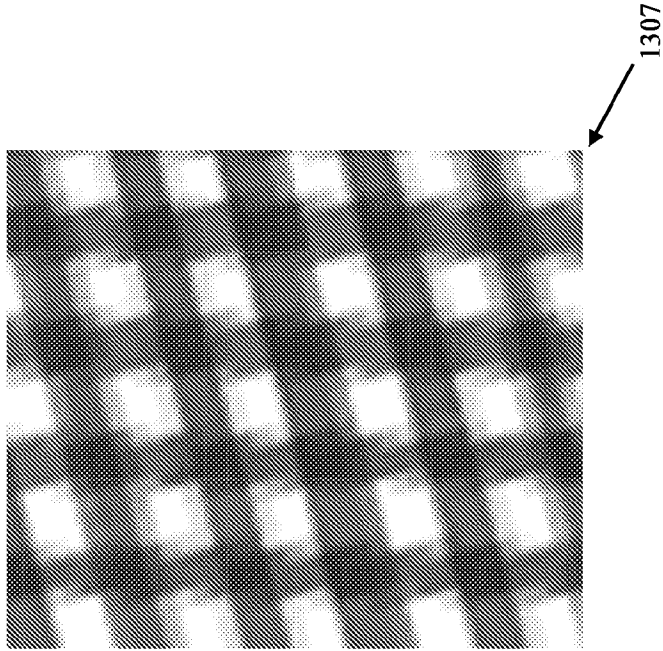


Fig. 13

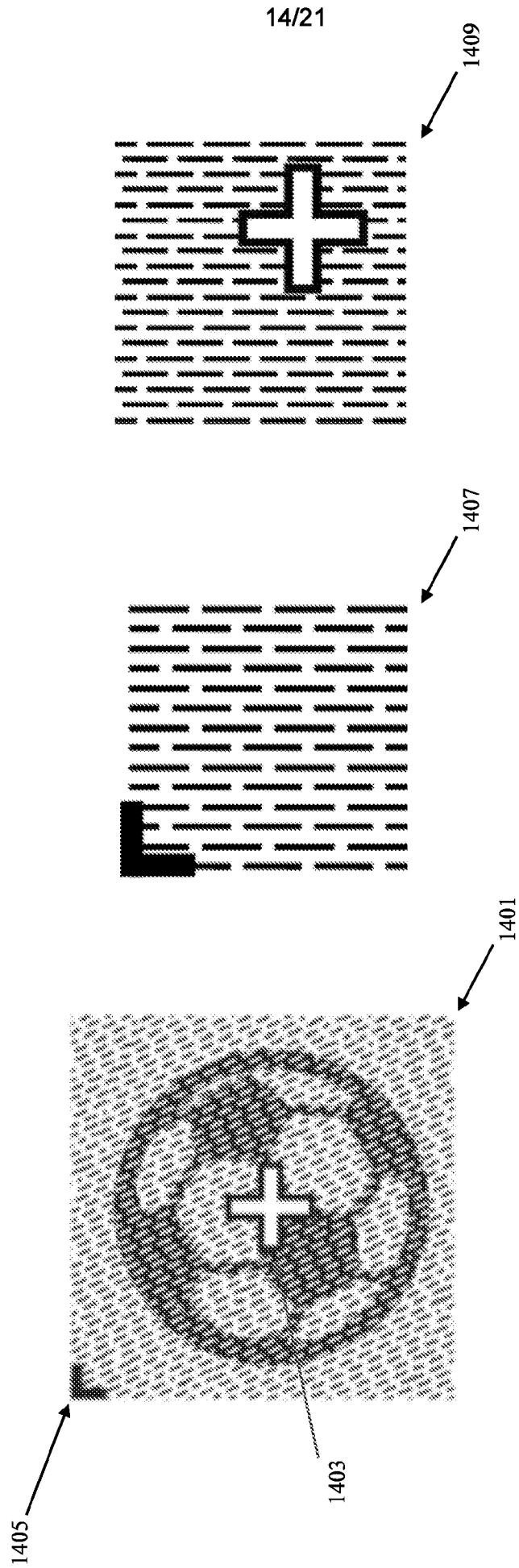


Fig. 14

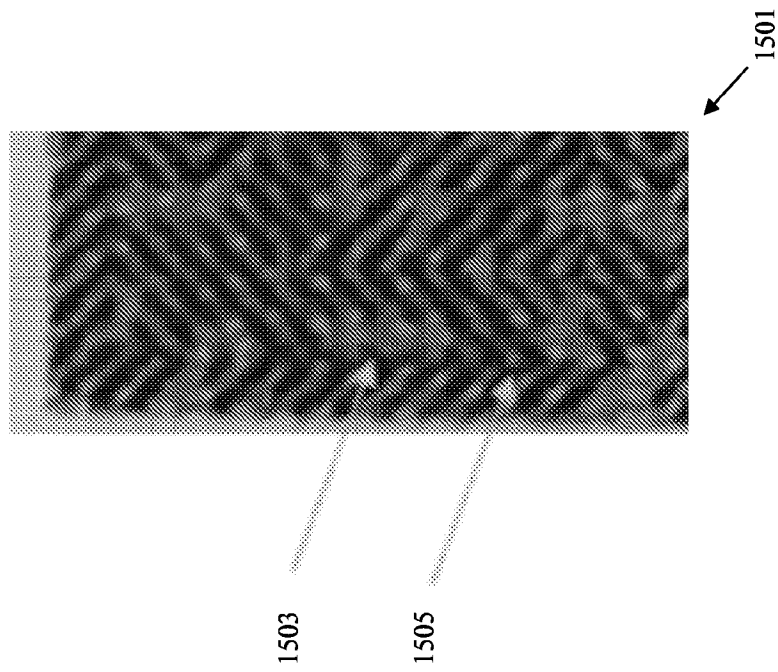


Fig. 15

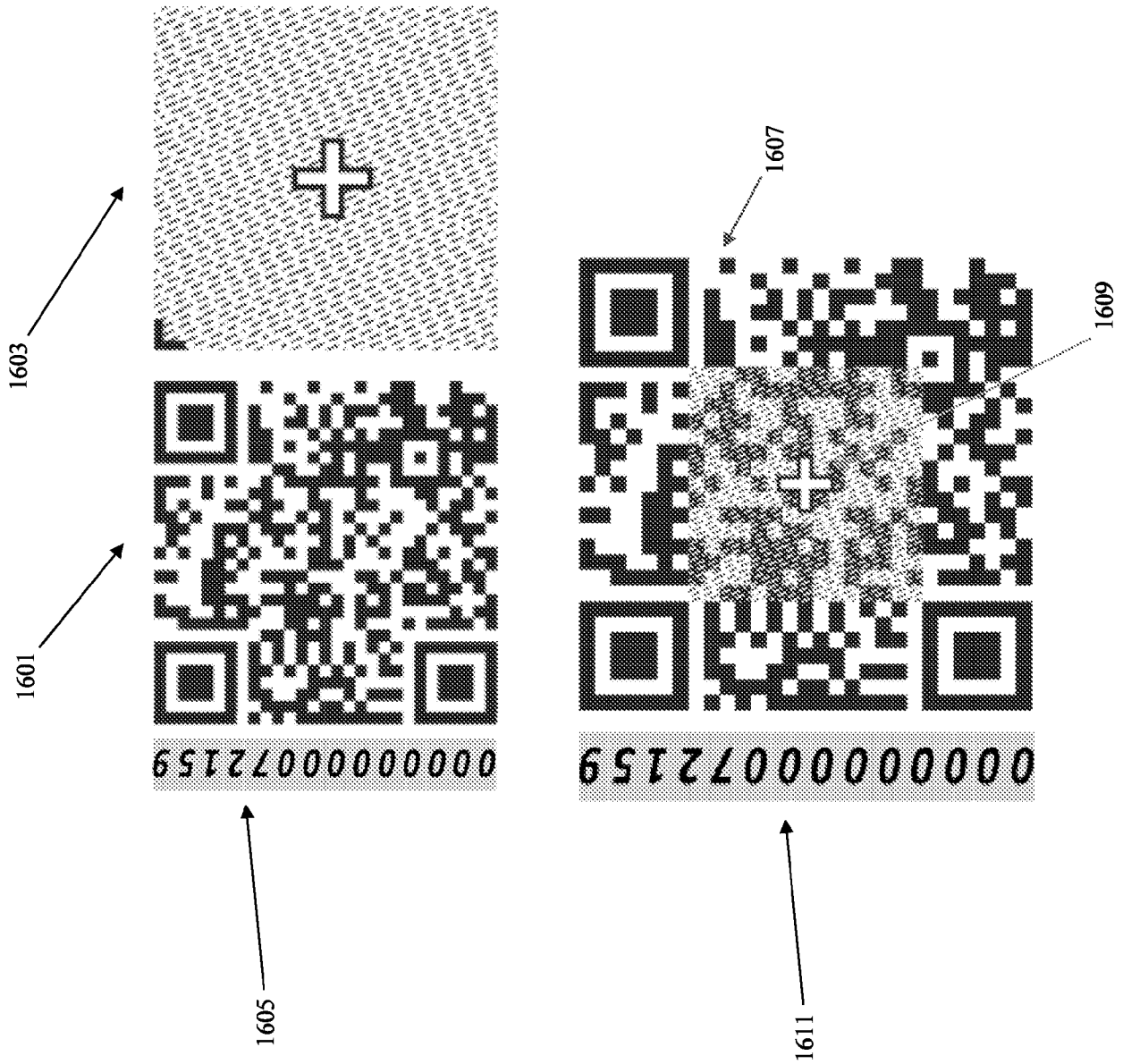


Fig. 16

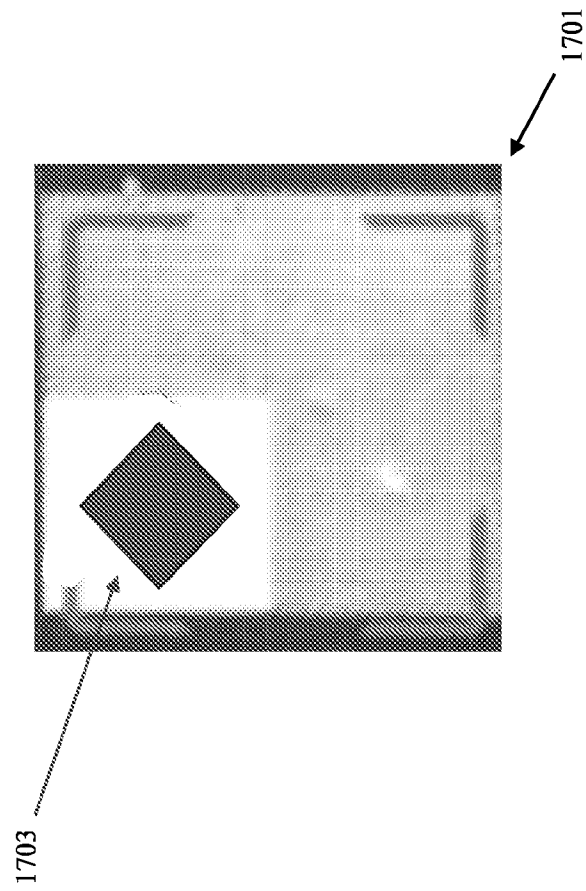


Fig. 17

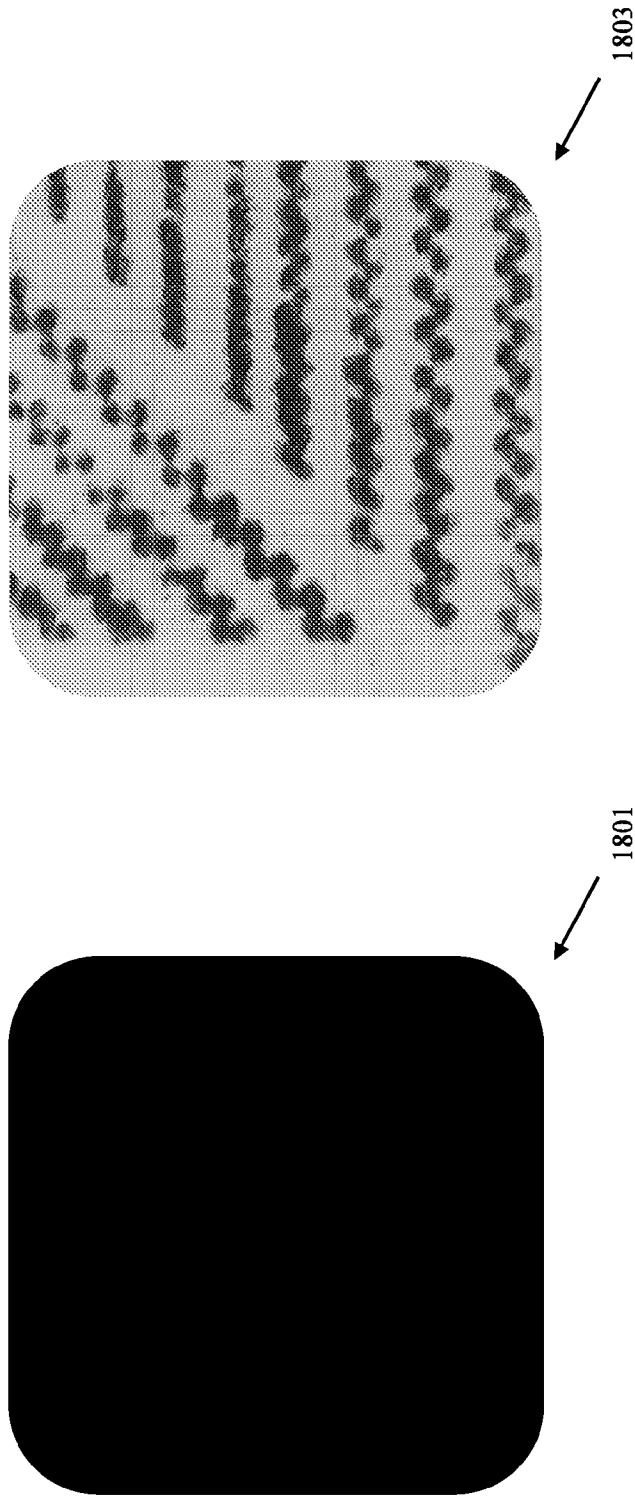


Fig. 18

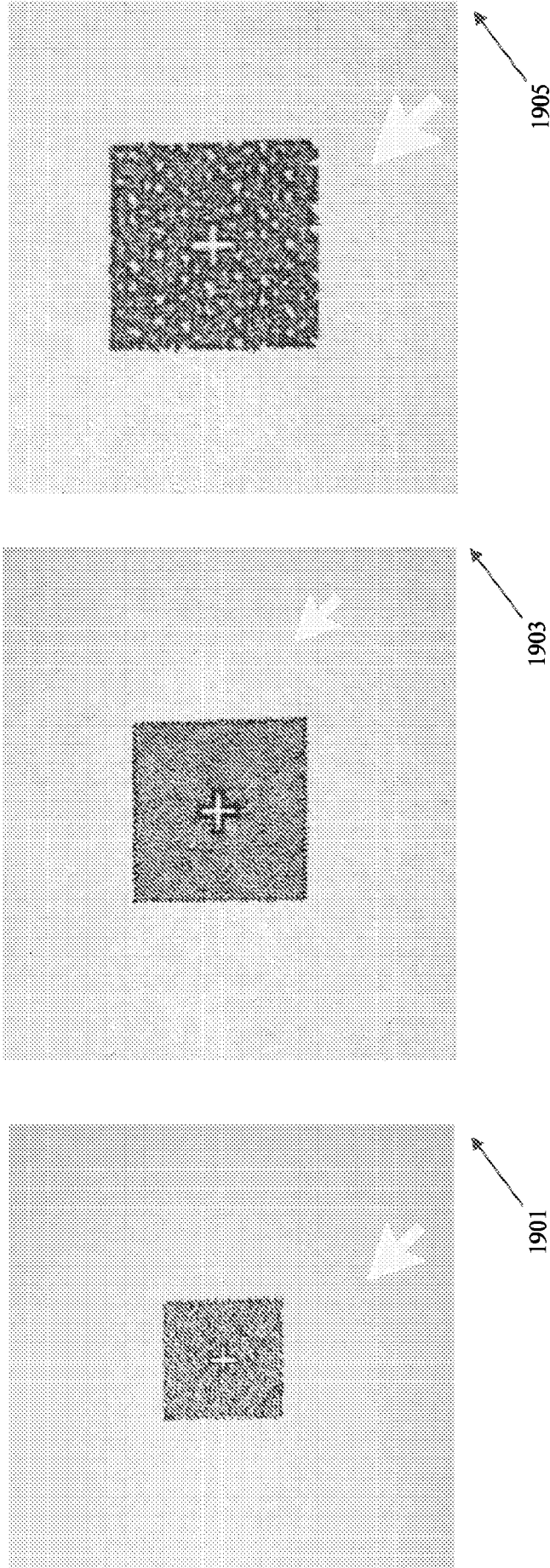


Fig. 19

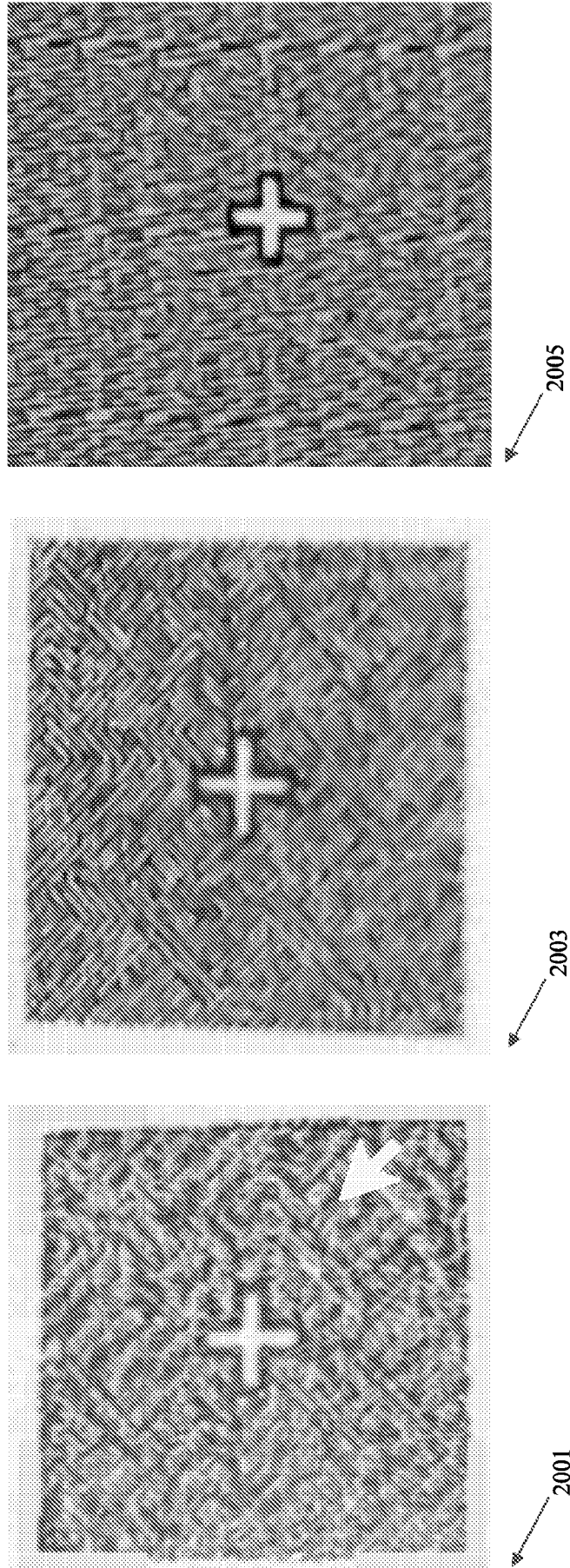
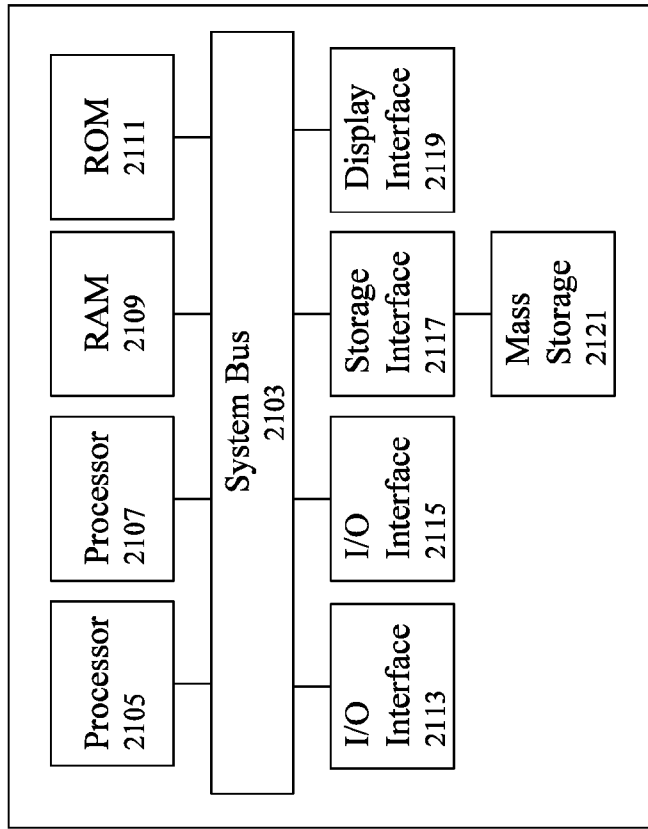


Fig. 20





2101

Fig. 21

# INTERNATIONAL SEARCH REPORT

International application No <b>PCT/US2023/071609</b>
--

**A. CLASSIFICATION OF SUBJECT MATTER**  
**INV. G07D7/004 B42D25/00 G07D7/12 G07D7/206 H04N1/00**  
**ADD.**

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**  
 Minimum documentation searched (classification system followed by classification symbols)  
**G07D H04N B42F B42D G03G**

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
**EPO-Internal**

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
<b>X</b>	<b>US 2009/244641 A1 (WU JUDY WAILING [CA])</b> <b>1 October 2009 (2009-10-01)</b> <b>paragraphs [0008], [0027]</b> <b>figures 11, 13, 14, 15, 16</b> -----	<b>1-6</b>
<b>X</b>	<b>US 2014/334665 A1 (QUINN CARY M [US] ET AL)</b> <b>13 November 2014 (2014-11-13)</b> <b>paragraphs [0006], [0037], [0054], [0116], [0147]</b> <b>figure 15</b> -----	<b>1-3, 6-15</b>
<b>X</b>	<b>US 2006/284411 A1 (WU JUDY W [CA])</b> <b>21 December 2006 (2006-12-21)</b>	<b>1</b>
<b>A</b>	<b>paragraph [0004]</b> <b>figures 2a, 2b, 4</b> -----	<b>10</b>
	----- -/--	

Further documents are listed in the continuation of Box C.       See patent family annex.

\* Special categories of cited documents :

<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>
---	---

Date of the actual completion of the international search  <b>18 November 2023</b>	Date of mailing of the international search report  <b>01/12/2023</b>
--	---

Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer  <b>Schikhof, Arnout</b>
--	---

## INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2023/071609

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2021 030730 A (XEROX CORP) 1 March 2021 (2021-03-01)	1-4, 6
A	paragraphs [0017], [0018] figure 2B -----	14
A	US 2013/335784 A1 (KURTZ ANDREW F [US] ET AL) 19 December 2013 (2013-12-19) paragraphs [0100], [0102], [0103] figure 2a -----	2, 3, 6

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2023/071609

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009244641 A1	01-10-2009	NONE	
US 2014334665 A1	13-11-2014	NONE	
US 2006284411 A1	21-12-2006	US 2006284411 A1 US 2014327237 A1	21-12-2006 06-11-2014
JP 2021030730 A	01-03-2021	JP 2021030730 A US 10812675 B1	01-03-2021 20-10-2020
US 2013335784 A1	19-12-2013	NONE	