



(51) International Patent Classification:
G07D 7/128 (2016.01)

(21) International Application Number:
PCT/US2019/023895

(22) International Filing Date:
25 March 2019 (25.03.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/648,246 26 March 2018 (26.03.2018) US

(71) Applicant: **VERIFYME, INC.** [US/US]; Clinton Square,
75 S. Clinton Avenue, Suite 510, Rochester, NY 14604
(US).

(72) Inventor: **GOLDSTEIN, Keith**; Clinton Square, 75 S.
Clinton Avenue, Suite 510, Rochester, NY 14604 (US).

(74) Agent: **SLAVIN, Michael A.** et al.; McHale & Slavin,
P.A., 2855 PGA Boulevard, Palm Beach Gardens, FL 33410
(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, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

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))

(54) Title: DEVICE AND METHOD FOR AUTHENTICATION

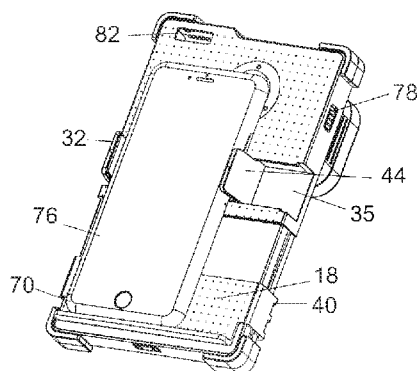


Fig. 5

(57) Abstract: Disclosed is a device and process for marking and detecting labels with spectral band authentication features utilizing a reader that can be affixed to a smart phone and positioned so as to align the lens of the phone's camera with a reader aperture. The reader aperture allows the camera to view an item through a spacer, wherein a UV and IR light source is used to reveal indicia within invisible ink. The light source employs a distinct emission spectrum characterized by narrow peaks and gaps which can illuminate pigment of the invisible ink that is selectively responsive at the wavelengths of specific peaks and/or unresponsive at the gaps in the spectrum. The smart phone captures the indicia revealed and interfaces with a cloud-based database to provide verification of authenticity.

DEVICE AND METHOD FOR AUTHENTICATION

FIELD OF THE INVENTION

The invention relates generally to the field of document authentication and, in particular, to a device for
5 the selective use of light sources having light emission and absorption characteristics in certain corresponding spectral bands that can verify the authenticity of a document.

BACKGROUND OF THE INVENTION

10 Authenticity of documents can be performed by many techniques. For instance, a document may include hidden indicia that can be detected by various means such as optical lenses, light illumination, or coding. The issues of authentication and counterfeit deterrence are
15 critical to the livelihood of manufacturers, and for the protection of consumers. Improved verification and counterfeiting prevention mechanisms are extremely important in labeling, verifying the contents of packaged goods, verifying the source of goods, and so forth.
20 Counterfeit products are, by definition, unauthorized copies of a product, its packaging, labeling, and/or its logo(s). Counterfeiting and product diversion are estimated to have a 1.8 trillion dollar adverse impact on all verticals, as it is difficult to verify originals
25 versus the non-originals.

Attractive targets for counterfeiters are items with significant brand equity. In the commercial manufacturing world, it is not uncommon for counterfeit or otherwise unauthorized goods to be manufactured,
30 distributed, and sold in direct competition with authentic

goods. Counterfeit articles can so closely resemble genuine goods that consumers readily confuse the counterfeit articles with the authentic articles. In other circumstances, the manufacturer segments the world market for different sales and distribution practices, so that the "counterfeit" goods may be essentially identical to authorized goods. Further, in many instances, a manufacturer produces goods under license from an intellectual property owner, and thus sales outside the terms of the license agreement are also "counterfeit".

A wide variety of attempts have been made to limit the likelihood of counterfeiting. For example, some have tried to assure the authenticity of items by putting encoded or unencoded markings thereon (e.g., an artist's signature on his or her painting). Unfortunately, as soon as the code is broken and/or the markings can be replicated, this method becomes worthless for authentication purposes.

U.S. Pat. No. 5,574,790 discloses a multiple-reader system for authentication of articles based on multiple sensed fluorescent discriminating variables, such as wavelengths, amplitudes, and time delays relative to a modulated illuminating light. The fluorescent indicia incorporate spatial distributions, such as bar codes as discriminating features, to define a user-determined and programmable encryption of the articles' authentic identity.

U.S. Pat. No. 5,289,547 discloses a method for authenticating articles including incorporating into a carrier composition a mixture of at least two photochromic compounds that have different absorption maxima in the activated state and other different properties to form the

authenticating display data on the article, subjecting the display data to various steps of the authenticating method, activating all photochromic compounds, preferential bleaching of less than all of the photochromic compounds, and/or bleaching of all the photochromic compounds, and subsequent examination of the display data following the various activation and bleaching steps by verifying means to enable authentication.

U.S. Pat. No. 5,974,150 discloses an anti-counterfeiting system wherein an authentication certificate affixed to a product is impregnated with dichroic fibers containing a fluorescent dye. In order to determine if the imprinted code corresponds to the certificate itself, the fiber pattern, which is completely random, is illuminated by a light and read by a scanner. The resulting pattern is then compared to the encoded pattern to determine authenticity.

U.S. Pat. No. 5,212,558 discloses an encoding system wherein a confidential image is recorded on a substrate using invisible ink. The invisible ink emits visible light having a wavelength of about 360-380 nm when irradiated with light having a wavelength of 250 nm.

U.S. Pat. No. 5,939,468 discloses jet ink compositions suitable for producing marks on objects that are invisible to the unaided eye and are visible only when excited by exciting radiation in the preferred wavelength region of from about 275 nm to about 400 nm.

U.S. Pat. No. 5,093,147 discloses a method for providing intelligible marks that are virtually invisible to the unaided eye on the surface of an article. The invention is based on a jet ink containing an organic laser dye that is poorly absorptive in the visible range of about

400 to 700 nm, is absorptive of radiation in the near infrared range of at least 750 nm, and fluoresces in response to radiation excitation in the infrared range at a wavelength longer than that of the exciting radiation.
5 Thus, the marks remain invisible to the naked eye after excitation.

Prior art patents by the Applicant related to document authentication include U.S. Patents 6,483,576; 6,672,718; 6,813,011; 7,939,239; 8,841,063; 9,183,688 and
10 9,159,016, all of which are incorporated herein by reference.

What is lacking in the art is a simple to use device that can be used to authenticate products by evaluating hidden indicia on product labels using matching
15 and mismatching illumination sources for absorption in certain bands, spectrally matched (or mismatched) pigments to assume a distinctly different appearance based upon the illumination source used, and interfacing with a cloud based server for instant verification of authentication.

20 SUMMARY OF THE INVENTION

Disclosed is a device and method for using a dual verification system to authenticate a document. A visible code can be assigned with an invisible code for use in document or product authenticity. In an exemplary
25 embodiment, a label is printed with a visible and invisible printed image or randomly generated code which can be alpha, numeric, symbol or image that is only visible under a specific wavelength of light. A reader coupled to a smart phone is used to decode the invisible printed code by
30 illuminating the invisible mark with a proper spectrum

light, and the code is then authenticated against a database.

An objective of the invention is to provide a device and method to authenticate a document based on
5 checking an invisible code or mark placed on the document against a database to confirm authenticity.

Another objective of the invention is to disclose a smart phone coupled to a device for use in confirming the authenticity of a document containing an invisible code or
10 mark.

Yet still another objective of the invention is to disclose a reader body having smart phone characteristics for use in confirming the authenticity of a document containing an invisible code or mark.

Still another objective of the invention is to
15 provide a process for confirming the authenticity of an item, wherein a device affixed to a smart phone reveals a hidden code or mark that is read by the camera on the phone and displayed on the phone's screen; wherein a user can
20 visually compare the mark to a database or use a smart phone and take a picture of the mark to upload to a cloud-based system to confirm the authenticity of the mark.

Still another objective of the invention is to provide a device having an emission spectrum light source
25 for illuminating invisible indicia, wherein the spectrum contains concentrated light energy in a narrow band in the visible spectrum. The pigmentation of invisible code is selected such that the material used to implant the code is strongly absorptive at that limited wavelength band. In
30 this way, the code has a distinctly different color appearance under the respective illumination spectra of the two sources.

Another objective of the invention is provide a reader that can be used with multiple sizes of smart phone, or utilized with a designated smart phone. A Bluetooth or any other type of interface recognizes a smart phone
5 previously employed to allow for quick substitution.

Yet still another objective of the invention is to provide two light sources used for comparison, wherein one light source has a broad and continuous spectrum, and the other light source is used to test for the presence of
10 pigment used to write the code, having a strong and exclusive narrow peak emission band, preferably functioning as a primary color component of a summed wavelength set for simulating daylight or human visible light, and which corresponds very closely to the peak in the absorption
15 spectrum of the pigmented code.

Another objective of the invention is to mask a normally visible code in a background of a similar hue, wherein the invention is used to cause the background or foreground to change hue so as to develop a contrast,
20 revealing the particular code. In these and other similar situations, the existence or content of the code is concealed until a particular illumination source is applied.

Still another objective of the invention is to
25 disclose a reading device (light source) that allows a user to check the authentication of a document by reading a hidden number to determine if the hidden number matches a text, email, or phone call information they received from a database.

30 Another objective of the invention is to uniquely identify products and packaging with visible and invisible

indicia providing brand inspectors with a mobile device and process for authenticating products.

Still another objection of the invention is to leverage a single ink for multiple purposes; and leverage
5 the power and capability of digital print technologies to implement the use of invisible ink.

A benefit of the invention is that, if the reading device reveals that the hidden image on a document matches a text, email, or phone call number, then the
10 document is authentic. If the hidden mark is different or hidden, the document is a fake.

Other objectives and further advantages and benefits associated with this invention will be apparent to those skilled in the art from the description, examples and
15 claims which follow.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 is a front perspective view of the reading device of the instant invention;

Figure 2 is a front plane view thereof;

20 Figure 3 is a right side plane view thereof;

Figure 4 is a rear perspective view thereof;

Figure 5 is a rear perspective view of the reading device with a smart phone affixed thereto;

25 Figure 6 is a rear plane view of the reading device with a smart phone affixed thereto;

Figure 7 is a side plane view of the reading device with a smart phone affixed thereto;

Figure 8 is a bottom plane view of the reading device with a smart phone affixed thereto;

Figure 9 is a pictorial view of a bottle label depicting an example of a label with a QR code and invisible indicia;

Figure 10 is a pictorial view depicting the
5 reading device with smart phone positioned to scan a QR code on the bottle label example;

Figure 11 is a pictorial view depicting the reading device with smart phone indicating where hidden indicia is located on the bottle label example;

10 Figure 12 is a pictorial view depicting the reading device with smart phone positioned to scan the area identified as having hidden indicia of the bottle label example; and

Figure 13 is a pictorial view depicting the
15 reading device with smart phone communicating that the bottle label example has been authenticated.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A detailed embodiment of the instant invention is disclosed herein; however, it is to be understood that the
20 disclosed embodiments are merely exemplary of the invention, which may be embodied in various forms. Therefore, specific functional and structural details disclosed herein are not to be interpreted as limiting, but merely as a basis for the claims and as a representation
25 basis for teaching one skilled in the art to variously employ the present invention in virtually any appropriately detailed structure.

Disclosed in Assignee's U.S. Patent 8,551,683, incorporated herein by reference, is a combination light
30 source and subject. The light source has an illumination spectrum characterized by a distinctively stronger narrow

band emission peak that has a predetermined wavelength within a spectrum compared to other wavelengths; and, the document has a pigment applied thereto, wherein the pigment has a reflection spectrum characterized by one of a

5 distinctively stronger reflection peak at the predetermined wavelength compared to said other wavelengths, and a distinctively weaker reflection gap at the predetermined wavelength compared to said other wavelengths. The pigment gives the document or product or the like a distinct

10 appearance when illuminated by the light source due to a color shift from the emission peak matching one of the reflection peak and the reflection gap, as compared to a nominal appearance when illuminated by an alternate light source which does not include the distinctively stronger

15 emission peak at the predetermined wavelength as compared to said other wavelengths. In the preferred embodiment, the ink is marketed under the name RainbowSecure® for use with HP Indigo™ presses. The ink, which operates most covertly at 950nm or 980nm, allows variable printing on HP

20 Indigo™ presses to produce images that cannot be detected by the human eye and, when used in combination with an overt QR and/or 2D barcode, provides a dual layer of protection. The RainbowSecure® ink is placed within an HP Indigo™ cartridge, and other digital printing processes,

25 within one of the seven ink stations within the HP Indigo™ for application of the hidden indicia during the normal printing process. The hidden indicia could be dot patterns, characters, numbers, bar codes, digital water marks, and the like. The hidden indicia may be

30 predetermined or randomly generated.

Applicant has adapted this technology in a device and process for marking and detecting labels with spectral

band authentication features utilizing a smart phone reader 10 for receipt of a smart phone 70. The images cannot be copied or scanned. As illustrated in Figures 1 - 4, the reader 10 has a front surface 12 and a rear surface 14.

5 The front surface 12 having an aperture 16 which is centrally placed to provide a universal alignment to all known commercially available smart phones. A smart phone, used herein, is a mobile telephone capable of performing many microprocessor based computer functions including

10 touch screen interface, and internet access, and includes an operating system capable of running downloaded applications. The smart phone will be equipped with image processing software. The front surface 12 includes an adjustable height bracket 18 having a base 20 for

15 supporting a bottom edge of a smart phone. The adjustable height bracket 18 is slidable along tracks 22, 23 formed on each side edge 24, 26 of the reader 10. The tracks 22, 23 and rear bracket 28 maintain the base 20 in a perpendicular position to each side edge 24, 26 when the adjustable

20 height bracket 18 is slid along the tracks 22, 23. The adjustable height bracket 18 can be moved into a position so that the lens of a smart phone camera is aligned with the aperture 16. A height adjustment screw 30 provides a frictional interface between the screw and the rear surface

25 14 of the reader 10, to maintain the adjustable height bracket 18 in a fixed position.

The front surface 12 further includes an adjustable width bracket 32 having a side wall 34 for supporting a first side edge of a smart phone. The

30 adjustable width bracket 32 is slidable along a guideway 35 having side surfaces 36 and 38. The adjustable width bracket 32 is movable by use of width adjustment screw 40

that can move along slot 42 formed on the rear surface 14. Additionally, a base bracket 44 frictionally engages the guideway 35, providing a moveable bracket to capture a second side edge of a smart phone.

5 A lens spacer 50 extends from the rear surface 14 a distance "d". The lens spacer 50 is preferably constructed of aluminum, having a series of slits 52 formed thereon to operate as a passive heat sink to regulate temperatures of the lens spacer 50 during prolonged LED
10 light operation. A shroud 54, preferably constructed of flexible rubber, is attached to a distal end 56 of the lens spacer 50. The shroud 54 provides a shield to reduce ambient light from affecting light produced by the lights located within the lens spacer 50. In the preferred
15 embodiment, the shroud 54 provides sufficient flexibility to conform to the curvature of a bottle. The lens spacer 50 houses a light source 51 comprising a plurality of infrared (IR) lights, ultraviolet (UV) lights and visible lights use LED's. When the reader is affixed to a smart
20 phone, the brackets 18, 32 are moved so as to position the camera lens of the smart phone over the aperture 16. The lens spacer 50 provides a predetermined distance "d", taking the thickness "t" of the reader 10 into consideration, where the smart phone camera will be
25 properly positioned to view an image through the lens spacer. The lens spacer 50 can include either an aperture or a secondary lens to allow the smart phone camera to view an image. With proper spacing, the lens spacer 50 may only need a cover lens to protect the internal light source. In
30 operation, the smart phone screen will display an image covered by the lens spacer on the smart phone display screen. The spacer is not needed for UV or visible light.

Referring to Figures 5-8, illustrated is the reader 10 having a front surface 12 with a smart phone 70 secured thereto. In this example, the smart phone 70 has a camera positioned along a corner edge 72 which is positioned over the aperture 16. The smart phone has a touch screen display 76 that is uninhibited by adjustable height bracket 18 or the adjustable width bracket 32. In this example, the base bracket 44 is moved along the guideway 35 so as to position the smart phone and adjustable width bracket 34 used to capture the smart phone 70 therebetween. The light source is powered by a rechargeable battery enclosed within said reader 10, replaceable batteries, or direct power. An on-off power switch 78 couples the light source 51 to the internal battery. A selector switch 80 can override the app and be used to toggle between the various LED's that provide the light source and operational aspects of the LED selected; battery condition and blue tooth interface can be viewed on display screen 82.

The light source 51 has narrow spectral band peaks, exemplified by certain types of IR 60 or UV 62 lighting. In such a light source, a combination of narrow wavelength bands (typically three primary color wavelengths) when added normally simulate illumination from a broadband source such as sunlight, having a given color temperature. The light source 51 is applied to a wavelength absorptive pigment that is matched to at least one narrow band in the light source, by virtue of a band, at which the pigment is strongly absorptive. The preferably narrow absorptive band of the pigment is at least partly complementary to one of the color peaks emitted from the light source.

An exemplary narrow band light source for use in accordance with the invention may have discrete spectral peaks at particular wavelengths at visible blue, green and red wavelength bands. When these spectral peaks are added at appropriate relative amplitudes, the illumination is perceived by the eye as substantially white broadband light. A blue peak at 440nm $\pm$.15 nm, a green peak at 544nm $\pm$.15 nm, and a red peak at 611nm $\pm$.15 nm are provided. Preferably, the bands are added at energy levels that cause the sum of the three sources to appear as a nominal color, for example the white of sunlight.

A particular pigment having a nominal color when illuminated with a true broadband source is specifically matched to the narrow band illumination source as described. Preferably, the pigment has an absorptive peak (i.e., a reflective spectral gap) that is sufficiently strong and sufficiently matched to the wavelength band of one of the illumination source peaks that the overall color or hue, from the summed proportions of reflected colors from the pigment, shifts substantially and noticeably based on whether the particular narrow band keying peak wavelength is present in the illumination source.

In the preferred embodiment, there are four IR lights generating a wavelength between 700nm to 1100nm, and four UV lights generating a wavelength between 200nm to 400nm. With the light source shining, the pigment allows the reader to view the hidden mark, and can display the mark on the screen of the smart phone. The IR and UV light can be used independently, or combined. For instance, data may be encoded on a document or label which can be read only by IR or UV. Data may also be encoded on a document or label which can be read only by IR and UV. Further,

pigments can be overlapped or juxtapositioned wherein the IR and UV light deciphers both hidden images simultaneously. In one embodiment, the user can then take a picture of the hidden mark, which could be a bar code or serial number, or any other distinguishing mark, which can also be called data. The picture can then be uploaded to an online or cloud-based system to confirm the authenticity of the item.

Because the pigment can be obscured when ambient light is present, the lens spacer 50 can include the shroud 54 to cover over the area of the item containing the mark. The shroud can also prevent others from seeing the hidden mark, so that the only display is on the screen of the phone, viewed through the reader. The lens spacer has a transparent cover 57 over the distal end 56. In a preferred embodiment, the transparent cover 57 may be adjoined by a filter lens such as an anti-reflective coating, or the transparent cover and filter characteristics combined, allowing the smart phone camera to receive a brighter and crisper image.

In one embodiment of the invention, an app is installed on the phone to aid in security. With the app installed, the smart phone can electronically connect to the reader through a wired connection or a wireless connection, such as Near Field Communication (NFC), Bluetooth, or other standard wireless connection. A NFC/RFID reader can be included, wherein a visible barcode could be replaced with an NFC (RFID) tag commonly used as part of a serialization / track and trace solution. In this regard, the reader may obtain an embedded serial number and forward the data string to the cloud based authentication database. The authentication step may again

indicate the location of hidden indicia, and the light source would be used for revealing the pigment for capture by the smart phone.

With a prepared app installed, the smart phone
5 can take a picture of the hidden mark without displaying the image on the phone, or by displaying it in a way to help obscure the image from anyone else nearby. The picture of the mark can then be uploaded through the app to a cloud-based database to confirm the authenticity of the
10 item. The app accesses the smart phone image processing software which can allow for image enhancement and convert serial numbers to alpha numerics. The app first provides a list of products to scan a visible or invisible QR code (bar code), serial number, or any type of code. In one
15 embodiment, a smart phone is coupled to a reader 10; the reader 10 having IR lights, UV lights, and visible lighting. A shroud around the filter lens provides a predetermined distance between the smart phone and the image to be scanned. The shroud is preferably constructed
20 of aluminum with heat dissipating surface cuts. An end of the shield includes a flexible edge covering that ideally conforms to the surface of the label to be scanned. For instance, the flexible edge covering might be used to conform to the curvature of a bottle, blocking the ambient
25 light from reaching the label area to be scanned. The lighting from the reader 10 is enhanced when the ambient light is reduced or eliminated. In addition, the lens, formed convex to enlarge the image without refocusing the smart phone, includes a reflective coating, allowing more
30 controlled light to reach the camera lens. The reader 10 has an integrated battery with a switching mechanism to energize the appropriate light. Upon scanning of the QR

code (or any code), the app interfaces with a cloud-based server which verifies the serial number of the QR code to authenticate the product. The smart phone, in combination with the reader 10 and cloud-based database, illuminates
5 invisible barcodes and serial numbers, and displays them on the phone, returning an image of the label being scanned to display the location of an invisible serial number or other indicia. The smart phone with the reader 10 is then positioned over the location of the invisible indicia to
10 decode and verify the serial number with the matching serial number in the database. Upon verification that the serial number on the label matches the serial number in the database, the smart phone will indicate that the product is genuine by stating "Product Authenticated" or the like.
15 The cloud-based database will record granular data such as the product scanned, date, time and location recorded. Global tracking is provided by the scan, wherein both an inspector scan can be tracked, as well as a consumer scan. The result is a global view of the supply chain, providing
20 a complete picture of inspector and consumer activity, wherein authentic, bogus, and duplicate scans are tracked.

The reader 10 is bluetooth equipped, or any wireless protocol, and will match a smart phone, allowing ease of coupling. The reader 10 can be used with most any
25 type of smart phone, wherein movable brackets can be adjusted to accommodate a particular style of phone. It should be noted that a smart phone can be permanently assigned to the reader 10, or essential formed integral thereto in instances where the reader 10 is used
30 commercially, such as in a port entry or customs office. Having a smart phone permanently assigned to the reader 10, or formed integral thereto, eliminates the need to address

software changes that frequent conventional smart phones. Alternatively, the use of conventional smart phones allows the reader 10 to be used on a temporary basis, leaving the smart phone to be used in its conventional manner when not
5 coupled to the reader 10. When a smart phone is formed integral to the reader, the reader essentially has the same functions of a smart phone. Namely, the reader would having microprocessor based computer functions including touch screen interface, and internet access, and include an
10 operating system capable of running downloaded applications.

Figure 9 is a pictorial view of a bottle 100 having a label 102 depicting an application example of the invention. The label 102 in this example is equipped with
15 a QR code 104 and hidden/invisible indicia which, in this example, is embedded in a green leaf, the pigment matching the background. Figure 10 depicts the reader 10 with the smart phone 70 aligned so that the lens spacer 50 is placed over the QR code as illustrated on the display screen 76.
20 The app placed on the smart phone 70 automatically interfaces with a cloud-based database to determine if the scan label is authentic 106. The operator can then request a scan 108 of the invisible indicia which, in this example, is a serial number. As shown in Figure 11, a reproduction
25 112 of the label 102 is pictured on the display screen, indicating the location of the hidden indicia 110 using a text message 114. Figure 12 depicts the reader 10 with the smart phone 70 aligned so that the lens spacer 50 is placed over the location described by the text message 114. The
30 display screen 76 reveals the hidden indicia serial number 116. The app placed on the smart phone 70 again automatically interfaces with the cloud-based database.

Figure 13 is a pictorial depicting the reader 10 with the smart phone 70 displaying that the bottle label hidden indicia has been authenticated 118. The hidden indicia can be dot patterns, character, numbers, bar codes, digital
5 water marks and so forth.

The invention provides a process for authenticating a document comprising the steps of printing hidden indicia on a document with a RainbowSecure® invisible ink; affixing a reader device to a smart phone,
10 said reader having a power supply and a selectable IR or UV light source producing a predetermined wavelength; placing said reader device and said smart phone over a document containing said invisible ink; decoding said invisible ink with said light source to reveal a first image; capturing
15 said first image with said smart phone; communicating said first image to a cloud based database containing authentic images; comparing said first image with said authentic images; and displaying confirmation of the authenticity of said first image on said smart phone. The process further
20 includes the steps of forwarding an photo or text message describing a location of a second image; placing said reader device over said location of said second image; decoding invisible ink over said location with said light source to reveal said second image; capturing said second
25 image with said smart phone; communicating said second image to said cloud based database containing authenticating codes; comparing said second image with said authenticating codes; and receiving confirmation of the authenticity the second image. The process can be used to
30 record when and an image was scanned, as well as where the image was scanned by use of the smart phone gps connection.

The use of the word "a" or "an" when used in conjunction with the term "comprising" in the claims and/or the specification may mean "one," but it is also consistent with the meaning of "one or more" or "at least one." The use of the term "or" in the claims is used to mean "and/or" unless explicitly indicated to refer to alternatives only or the alternative are mutually exclusive, although the disclosure supports a definition that refers to only alternatives and "and/or." The terms "comprise" (and any form of comprise, such as "comprises" and "comprising"), "have" (and any form of have, such as "has" and "having"), "include" (and any form of include, such as "includes" and "including") and "contain" (and any form of contain, such as "contains" and "containing") are open-ended linking verbs. As a result, a method or device that "comprises," "has," "includes" or "contains" one or more steps or elements, possesses those one or more steps or elements, but is not limited to possessing only those one or more elements. Likewise, a step of a method or an element of a device that "comprises," "has," "includes" or "contains" one or more features, possesses those one or more features, but is not limited to possessing only those one or more features. Furthermore, a device or structure that is configured in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

All patents mentioned in this specification are indicative of the levels of those skilled in the art to which the invention pertains. One skilled in the art will readily appreciate that the present invention is well adapted to carry out the objectives and obtain the ends and advantages mentioned, as well as those inherent therein.

The embodiments, methods, procedures and techniques described herein are presently representative of the preferred embodiments, are intended to be exemplary, and are not intended as limitations on the scope. Changes
5 therein and other uses will occur to those skilled in the art which are encompassed within the spirit of the invention and are defined by the scope of the appended claims. Although the invention has been described in connection with specific preferred embodiments, it should
10 be understood that the invention as claimed should not be unduly limited to such specific embodiments. Indeed, various modifications of the described modes for carrying out the invention which are obvious to those skilled in the art are intended to be within the scope of the following
15 claims.

CLAIMS

What is claimed is:

Claim 1. An authentication device comprising:

a reader body having a microprocessor based computer function including a touch screen interface, a camera, memory, internet access, an operating system and a power source;

a lens attached to said reader body, said lens housing a light source coupled to said power source for producing light of a predetermined wavelength capable of reacting with an invisible ink to reveal a hidden image, said lens communicating with said camera to capture said hidden image;

wherein said light source illuminates an invisible ink to reveal said hidden image, said hidden image captured by said smart phone and compared with an authentic image stored on a cloud based database to determine authentication.

Claim 2. The authentication device according to claim 1 wherein said invisible ink is a wavelength absorptive pigment that is matched to at least one band of light.

Claim 3. The authentication device according to claim 2 wherein said invisible ink is RainbowSecure®.

Claim 4. The authentication device according to claim 2 wherein said band of light is either an infra-red (IR) light having a wavelength between 700nm to 1100nm, an ultra-violet (UV) light having a wavelength between 200nm to 400nm, or both lights combined.

Claim 5. The authentication device according to claim 1 wherein said lens includes an anti-reflective coating.

Claim 6. The authentication device according to claim 1 wherein said microprocessor based computer function is a smart phone.

Claim 7. The authentication device according to claim 1 wherein said reader body is defined by a front surface and a rear surface spaced apart by a continuous sidewall forming a cavity therebetween, said reader body having a power supply formed within said cavity, said front surface having a connector constructed and arranged to physically secure a smart phone to said reader body.

Claim 8. The authentication device according to claim 7 wherein said connector is an adjustable height bracket and an adjustable width bracket, said height and width bracket are adjustable to maintain said smart phone camera in a position relative to said lens spacer.

Claim 9. The authentication device according to claim 7 including an IR lens spacer formed on said rear surface having a reader body, and a flexible shroud coupled to a distal end of said lens spacer to reduce ambient light.

Claim 10. The authentication device according to claim 8 wherein said lens spacer is constructed of aluminum with a plurality of slits providing a passive heat sink.

Claim 11. The authentication device according to claim 1 wherein said reader includes an NFC/RFID reader.

Claim 12. An authentication device comprising:

a reader having a front surface and a rear surface spaced apart a continuous sidewall forming a cavity with a power supply, said front surface having a connector mechanism constructed and arranged to physically couple a smart phone to said reader;

a light source attached to said reader, said light source having a light of a predetermined IR or UV wavelength to which an invisible ink having a wavelength absorptive pigment matched to at least one narrow band of said light source and is reactive to reveal a hidden image;

a lens spacer attached to said support body, said lens spacer housing said light source and communicating with a smart phone camera to capture said hidden image;

a shroud coupled to a distal end of said lens spacer constructed and arranged to reduce or eliminate ambient light;

wherein said light source illuminates an invisible ink to reveal a hidden image, said hidden image captured by said smart phone and compared with an authentic image stored on a cloud based database to determine authentication.

Claim 13. The authentication device according to claim 12 wherein said invisible ink is RainbowSecure®.

Claim 14. The authentication device according to claim 12 wherein said shroud is flexible to conform to the curvature of a bottle.

Claim 15. The authentication device according to claim 12 wherein said lens spacer includes a filter lens having an anti-reflective coating.

Claim 16. The authentication device according to claim 12 wherein said reader includes an NFC/RFID reader.

Claim 17. The authentication device according to claim 12 wherein said lens spacer is constructed and arranged to operated as a passive heat sink.

Claim 18. A process for authenticating an image on a product or document comprising the steps of:

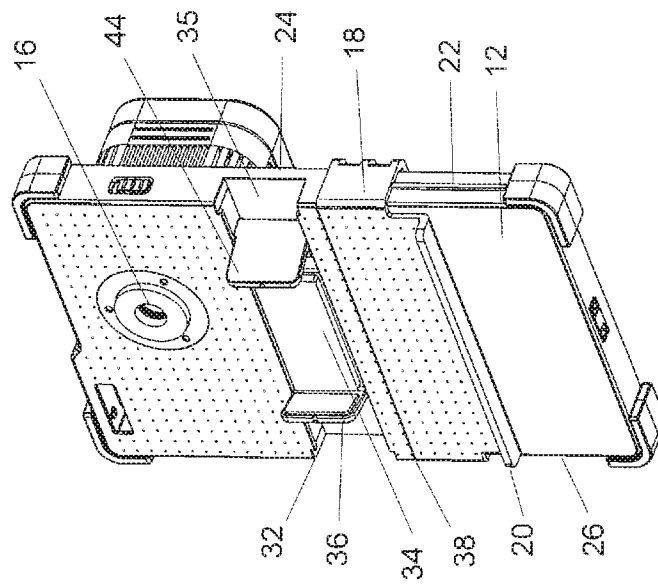
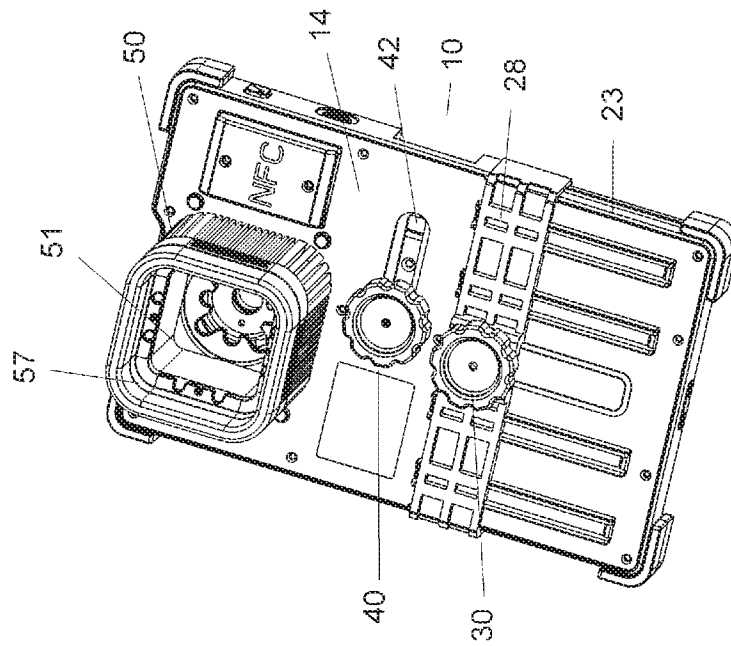
- printing hidden indicia with an invisible ink;
- affixing a reader device to a smart phone, said reader having a power supply and a selectable IR or UV light source producing a predetermined wavelength;
- placing said reader device and said smart phone over a document containing said invisible ink;
- decoding said invisible ink with said light source to reveal a first image;
- capturing said first image with said smart phone;
- communicating said first image to a cloud based database containing authentic images;
- comparing said first image with said authentic images;
- and
- displaying confirmation of the authenticity of said first image on said smart phone.

Claim 19. The process for authenticating an image according to Claim 18 including the steps of:

- forwarding an photo or text message describing a location of a second image;
- placing said reader device over said location of said second image;
- decoding invisible ink over said location with said light source to reveal said second image;

capturing said second image with said smart phone;
communicating said second image to said cloud based
database containing authenticating codes;
comparing said second image with said authenticating
codes; and
receiving confirmation of the authenticity the second
image.

Claim 20. The process for authenticating an image
comprising according to claim 18 wherein said invisible ink
is RainbowSecure® ink.



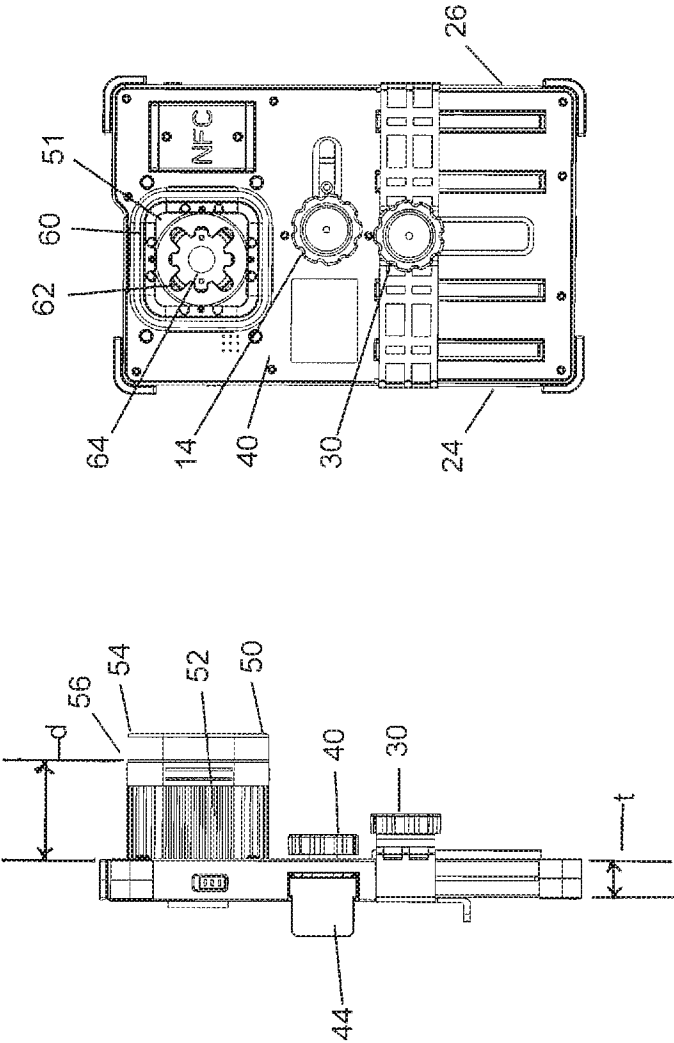


Fig. 2

Fig. 3

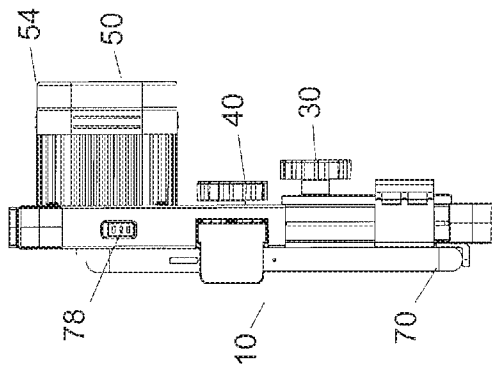


Fig. 7

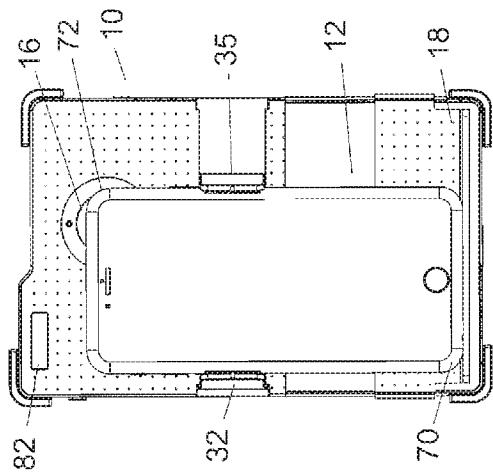


Fig. 6

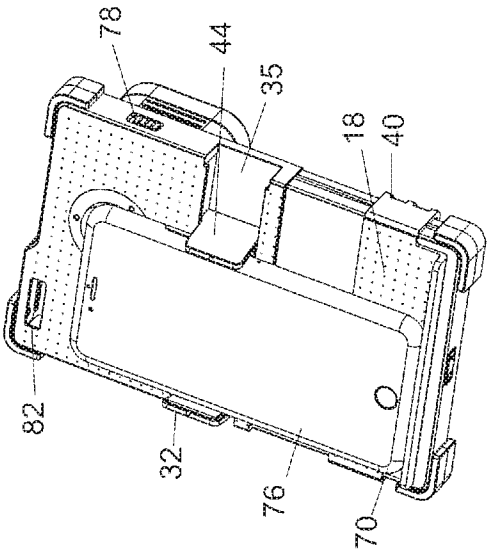


Fig. 5

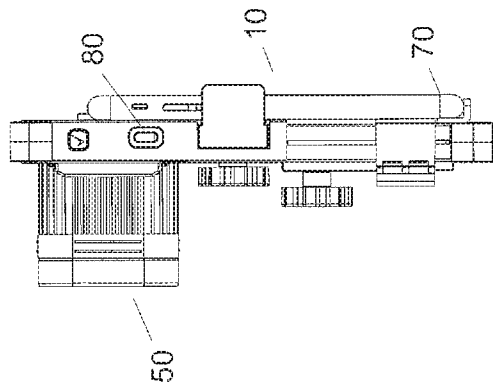


Fig. 8

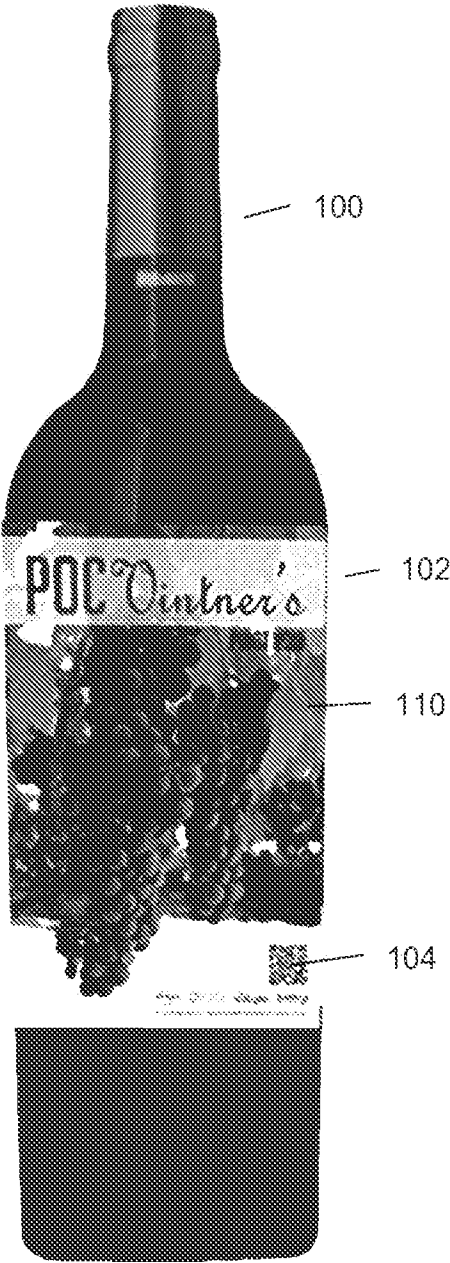


Fig. 9

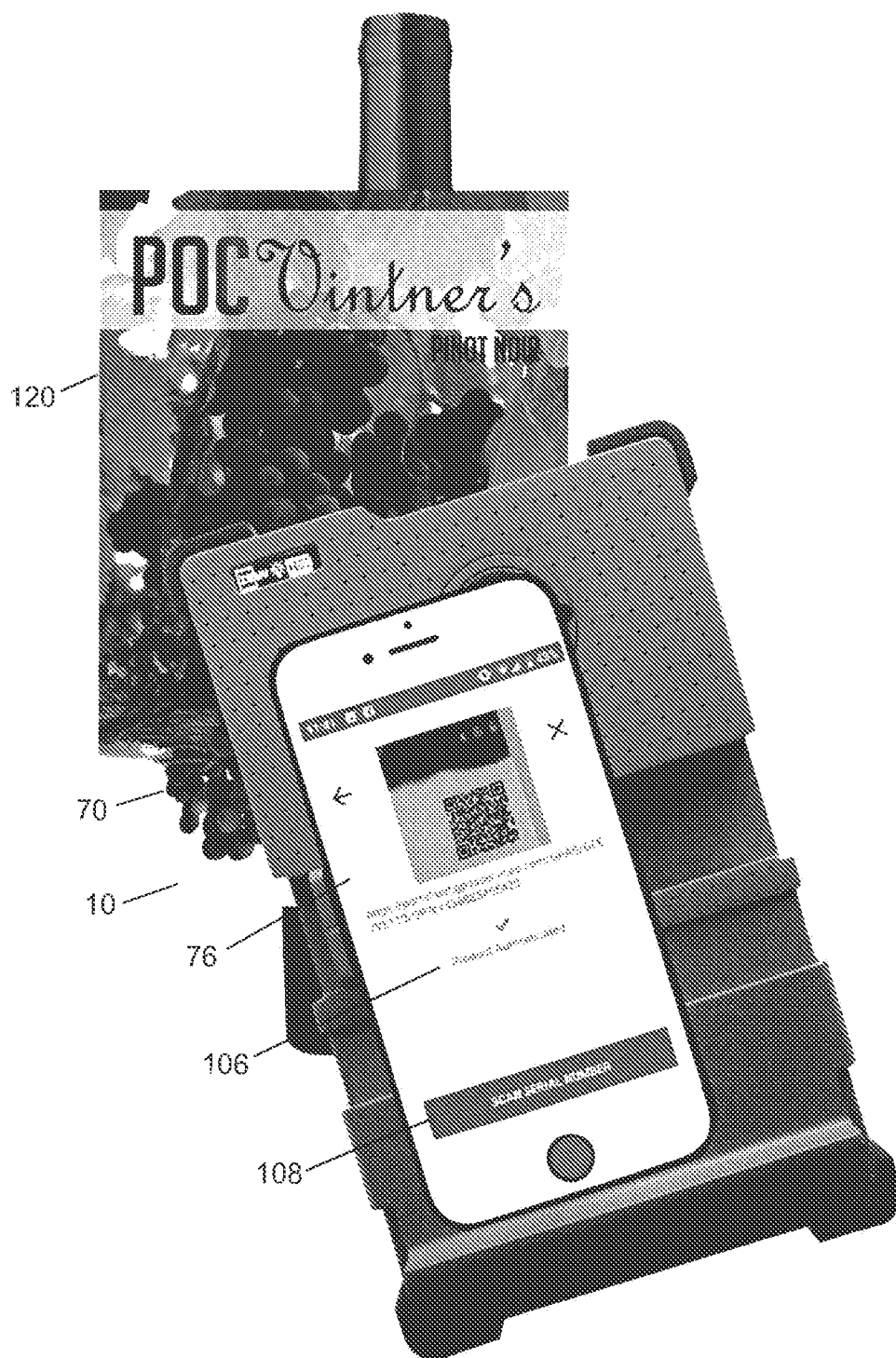
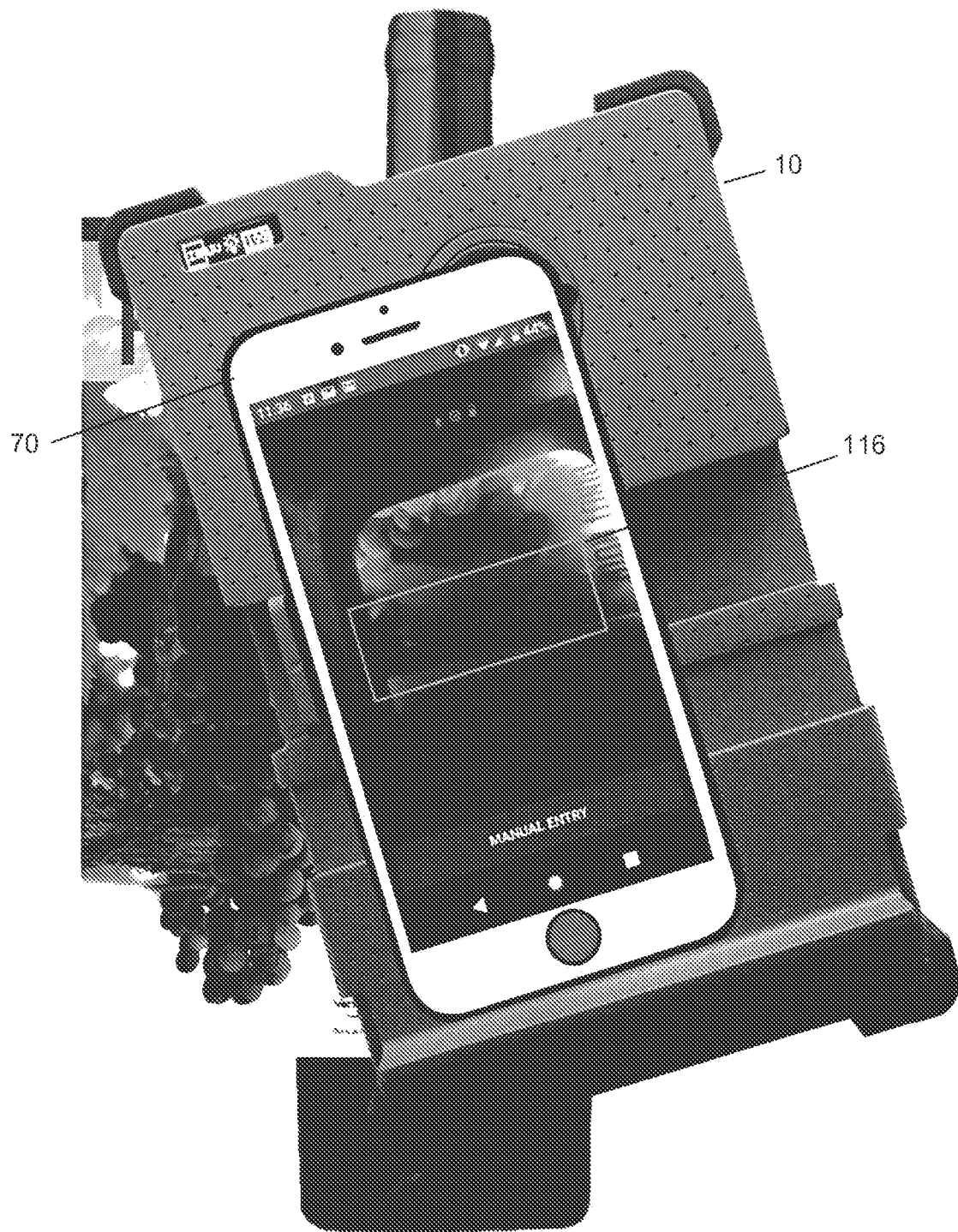
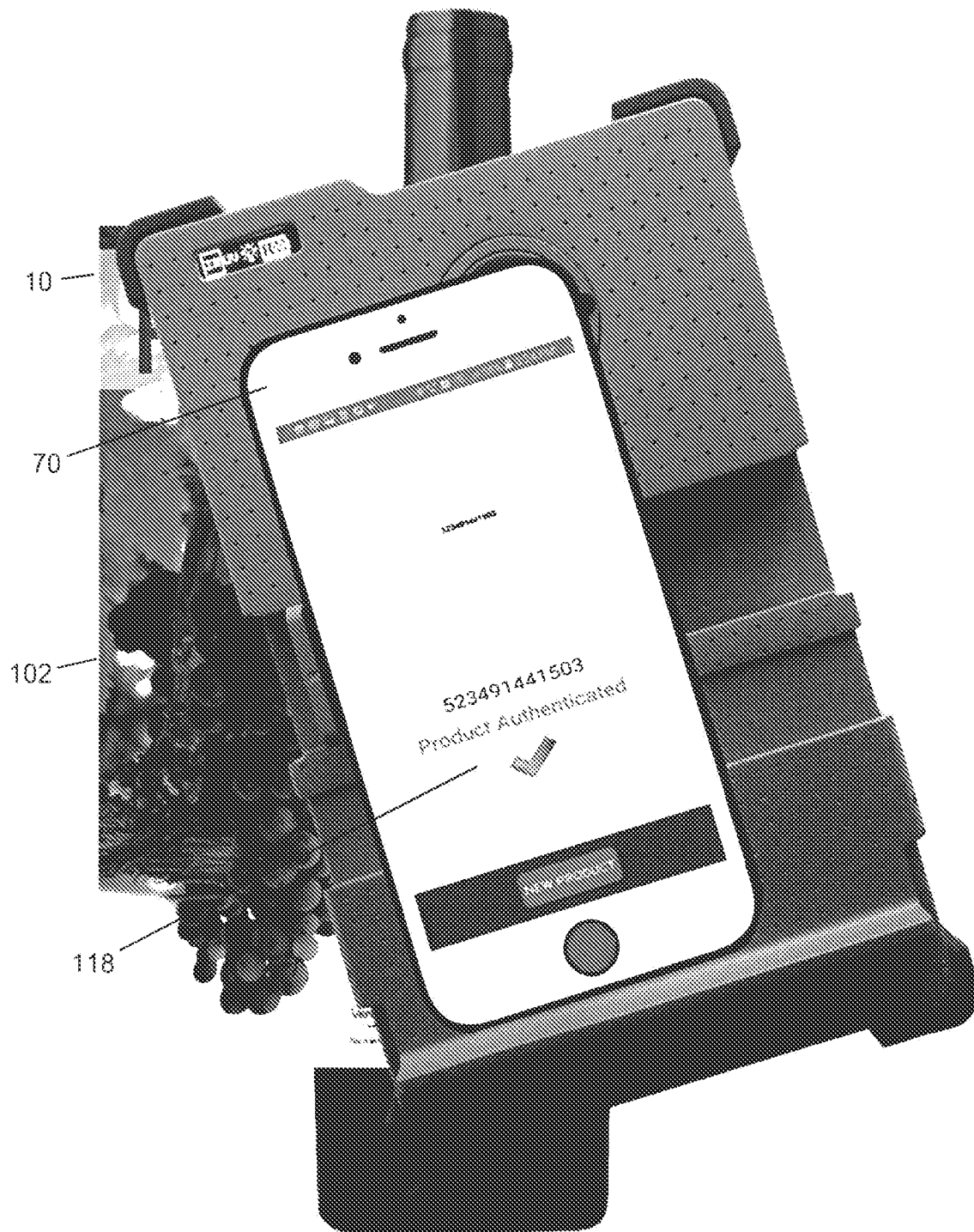


Fig. 10

**Fig. 11**

**Fig. 12**

**Fig. 13**

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/023895

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07D7/128
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

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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2011 077904 A1 (BUNDESDRUCKEREI GMBH [DE]) 27 December 2012 (2012-12-27) paragraphs [0005], [0007], [0008], [0019], [0030], [0057], [0058], [0059], [0063] - [0066], [0067], [0070]; figure 2 abstract	1,7,8, 11,12, 16,18
A	WO 2013/034603 A1 (BUNDESDRUCKEREI GMBH [DE]; PAESCHKE MANFRED [DE] ET AL.) 14 March 2013 (2013-03-14) the whole document ----- -/--	1-8,11, 12,15,16

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search

3 September 2019

Date of mailing of the international search report

23/09/2019

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

Lindholm, Anna-Maria

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/023895

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2014/130573 A1 (LASERLOCK TECHNOLOGIES INC [US]) 28 August 2014 (2014-08-28) abstract paragraphs [0027], [0036] - [0037] paragraph [0044] -----	1-6, 13, 20
A	WO 2009/158324 A1 (GRAPHIC SECURITY SYSTEMS CORP [US]; ALASIA ALFRED VICTOR [US] ET AL.) 30 December 2009 (2009-12-30) paragraphs [0010], [0012], [0025], [0094], [0101], [0102] -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2019/023895

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102011077904 A1	27-12-2012	NONE	

WO 2013034603 A1	14-03-2013	CN 103875026 A	18-06-2014
		EP 2718911 A1	16-04-2014
		PL 2718911 T3	31-07-2017
		WO 2013034603 A1	14-03-2013

WO 2014130573 A1	28-08-2014	US 2014233842 A1	21-08-2014
		WO 2014130573 A1	28-08-2014

WO 2009158324 A1	30-12-2009	CA 2728338 A1	30-12-2009
		EP 2304646 A1	06-04-2011
		WO 2009158324 A1	30-12-2009
