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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
09 July 2020 (09.07.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/141361 A1

(51) International Patent Classification:
G06K 9/20 (2006.01) *B65D 55/02* (2006.01)

(21) International Application Number:
PCT/IB2019/052080

(22) International Filing Date:
14 March 2019 (14.03.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201941000233 03 January 2019 (03.01.2019) IN

(72) Inventor; and

(71) Applicant: **ANAND, Ashish** [IN/IN]; C-102, Silver Akruthi Appt, 27th Main, Sector-2, Adjacent To Parangipalya Kptcl Power Grid, Hsr Layout, Bangalore 560034 (IN).

(72) Inventors: **BADIGER, Kishor Veerabhadrappa**; 2nd floor residential premises, situated at 10/11, 5th main road, 17th cross, HSR layout sector 6, Bangalore 560102 (IN). **TRIGUNAIT, Aman**; Devarabisnanahhalli, Bengaluru, Karnataka, India, Bangalore 560103 (IN).

(74) Agent: **PUTTAIAH, Kartik**; InvnTree IP Services, 399, 15th Cross, 5th Main, Sector:6, HSR Layout, Bangalore 560102 (IN).

(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,

WO 2020/141361 A1

(54) Title: SYSTEM FOR ENABLING IDENTIFICATION OF TAMPERING

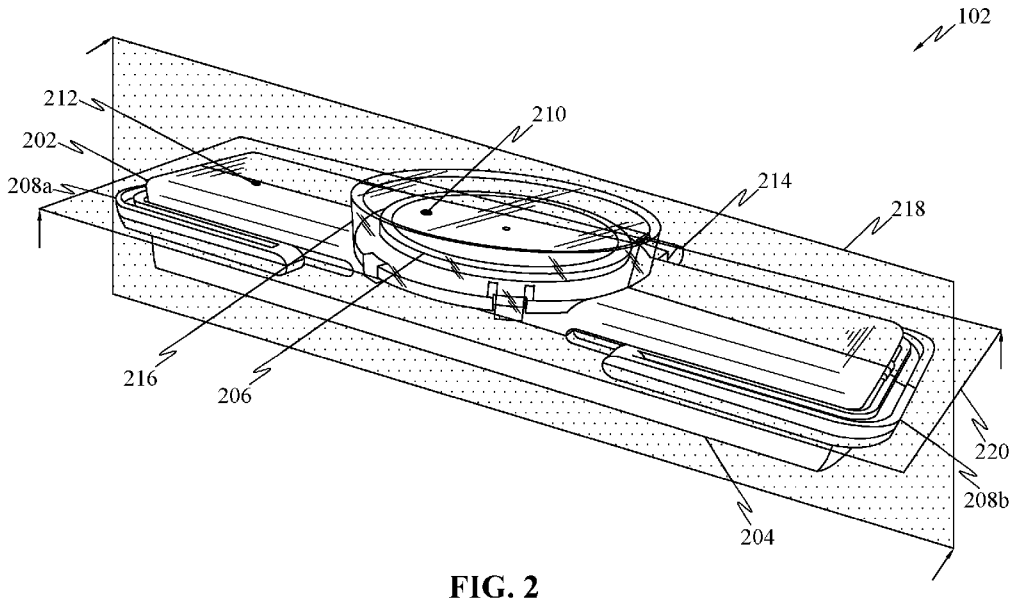

FIG. 2

(57) Abstract: System for enabling identification of tampering. A system (100) for enabling identification of tampering, the system (100) comprises a device (102) engaged to an article (104). The device (100) comprises a movable member (206) and a first reference (210) provided on the movable member (206). The device (102) is operable to assume a first state and a second state. The position of the movable member (206) changes at each instance the device (102) is brought back to the first state. The orientation of the movable member (206) is determined by determining spatial orientation of the first reference (210) with respect to a second reference(212), wherein the second reference (212) is external to the movable member (206).

[Continued on next page]

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).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

SYSTEM FOR ENABLING IDENTIFICATION OF TAMPERING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This patent application claims priority benefit from the Indian provisional application numbered 201941000233, filed on January 03, 2019.

BACKGROUND

[0002] Unless otherwise indicated herein, the materials described in this section are not prior art to the claims in this application and are not admitted to being prior art by inclusion in this section.

Field of Invention

[0003] The disclosed subject matter generally relates to the field of tamper evident technology, and more particularly but not exclusively, to the field of reusable tamper evident devices.

Discussion of Prior Art

[0004] Conventionally, in logistics, the goods to be transported are packed using a protective package. Further, the protective package is sealed using tamper-evident device like a security label. The package and the security label that is used to pack an object are generally meant for a single use. In other words, once the package and the security label are tampered, they become unfit for reuse.

[0005] Generally, the packages are made using materials like paper, cardboard, polyethene bag, and the like and the security label is made using plastic, adhesives, so on and so forth. It can be inferred that, packing an article consumes a significant amount of resources like paper, plastic, and the like. The use of already depleting resources coupled with the inability of the package and the security label to be reused poses a serious threat to the environment.

[0006] In conventional tamper-evident packaging, there are significant disadvantages associated with detecting the tampering of the package. For example, a person with a malicious intent may counterfeit the security label that is used over the package. Further, the person may access the article inside the package and get away from being detected by applying the counterfeit security label over the package.

[0007] US9361532B2 discloses label associated with an external reference, wherein external means reference is not the inherent part of label, it can be outside the label, below a

transparent portion of label or on transparent surface over the label such that label and reference both can be scanned by vision based technologies.

[0008] In light of the foregoing discussion, there is a need for an improved tamper evident device that is reusable and overcomes the aforesaid disadvantages.

SUMMARY

[0009] In an embodiment, a system for enabling identification of tampering is provided. The system comprises a device engaged to an article. The device comprisies a movable member and a first reference provided on the movable member. The device is operable to assume a first state and a second state. The position of the movable member changes at each instance the movable member is brought back to the first state. The orientation of the movable member is determined by determining spatial orientation of the first reference with respect to a second reference, wherein the second reference is external to the movable member.

BRIEF DESCRIPTION OF DRAWINGS

[0010] Embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

[0011] FIG. 1 illustrates a system 100 for enabling identification of tampering, in accordance with an embodiment;

[0012] FIG. 2 illustrates an isometric view of a device 102, in accordance with an embodiment;

[0013] FIG. 3 is a sectional view of the device 102 along a section plane 218, in accordance with an embodiment;

[0014] FIG. 4 is a sectional view of the device 102 in unlock position along a section plane 220, in accordance with an embodiment;

[0015] FIG. 5 is a sectional view of the device 102 in lock position along the section plane 220, in accordance with an embodiment;

[0016] FIGs. 6A-6C illustrate change in position of a movable member 206 during locking and unlocking of the device 102, in accordance with an embodiment;

[0017] FIG. 7 illustrates various modules of a tamper detector 106, in accordance with an embodiment;

[0018] FIG. 8 is a flowchart 800 illustrating a method for identification of tampering of the device 102, in accordance with an embodiment;

[0019] FIG. 9 illustrates a sectional view of an alternate embodiment of the device 102;

[0020] FIG. 10A illustrates a push lock device 1000, in accordance with an embodiment; and

[0021] FIG. 10B illustrates engaging the push lock device 1000 to an article 104, in accordance with an embodiment.

DETAILED DESCRIPTION

[0022] The following detailed description includes references to the accompanying drawings, which form a part of the detailed description. The drawings show illustrations in accordance with example embodiments. These example embodiments, which may be herein also referred to as "examples" are described in enough detail to enable those skilled in the art to practice the present subject matter. However, it may be apparent to one with ordinary skill in the art, that the present invention may be practised without these specific details. In other instances, well-known methods, procedures and components have not been described in detail so as not to unnecessarily obscure aspects of the embodiments. The embodiments can be combined, other embodiments can be utilized, or structural, logical, and design changes can be made without departing from the scope of the claims. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope is defined by the appended claims and their equivalents.

[0023] In this document, the terms "a" or "an" are used, as is common in patent documents, to include one or more than one. In this document, the term "or" is used to refer to a nonexclusive "or," such that "A or B" includes "A but not B," "B but not A," and "A and B," unless otherwise indicated.

OVERVIEW

[0024] In an embodiment, a system for enabling identification of tampering is provided. The system comprises a device that is configured to be engaged to an article. The device comprises a movable member that changes its position when the device is being locked or unlocked. The movable member comprises a first reference which is spatially associated with a second reference that is external to the movable member. When the device is locked to the article, the spatial orientation between the first reference and the second reference is registered in a server. If the device is tampered, due to the change in position of the movable member, the spatial orientation between the first reference and the second reference changes. At the time of verification, the instant spatial orientation between the first reference and the second reference of the device is compared with the registered spatial orientation. If the instant spatial orientation and the registered spatial orientation are the same, then it is determined that the device is not

tampered. On the other hand, if the instant spatial orientation and the registered spatial orientation are not same, then it is determined that the device is tampered.

SYSTEM FOR ENABLING IDENTIFICATION OF TAMPERING

[0025] Referring to FIG. 1, a system 100 for enabling identification of tampering is provided, in accordance with an embodiment. The system 100 comprises a device 102, an article 104, a tamper detector 106, a communication network 108 and a server 110. The device 102 may be a tamper evident device comprising a first reference 210 (shown in FIG. 2) and a second reference 212 (shown in FIG. 2), that is operable to assume a first state and a second state.

[0026] The article 104 may be a package containing a product that may be configured to be engaged to the device 102. The tamper detector 106 may be configured to identify the tampering of the device 102. For instance, the tamper detector 106 may be a scanning device that may scan the device 102 to detect tampering.

[0027] In an embodiment, the server 110 may be configured to store information corresponding to the device 102. The information may correspond to spatial orientation of the first reference 210 with respect to the second reference 212. As an example, the device 102 may be scanned at a registration phase to determine the spatial orientation between the first reference 210 and the second reference 212. The determined spatial orientation may be stored against the device 102 in the server 110.

[0028] The tamper detector 106 may be configured to communicate with the server 110 using the communication network 108 to determine the tampering of the device 102.

[0029] In an embodiment, the first state of the device 102 is a lock position when the device 102 is engaged to the article 104, thereby restricting access to the product that may be placed inside the article 104. The second state of the device 102 is an unlock position to allow access to the product that may be placed inside the article 104.

[0030] FIG. 2 illustrates an isometric view of the device 102 along with section planes 218, 220, in accordance with an embodiment. The device 102 comprises a first part 202 and a second part 204 hinged to each other using a hinge 214. The first part 202 comprises a movable member 206 and levers 208a, 208b. The levers 208a, 208b may be configured to lock and unlock the device 102 to the article 104.

[0031] The movable member 206 may comprise the first reference 210 that may be associated with the second reference 212. The second reference 212 may be located on the first part 202 but external to the movable member 206. The second reference 212 may be disposed

at a location wherein the second reference 212 is stationary irrespective of the state (lock or unlock) of the device 102.

[0032] The change in position of the movable member 206 causes a change in spatial orientation of the first reference 210 with respect to the second reference 212 (will be referred to as orientation of the movable member 206 hereafter).

[0033] In an embodiment, the movable member 206 may be configured to change its position whenever the device 102 is locked to assume the first state. The movable member 206 may be circular or in any other similar configuration, wherein location of the first reference 210 with respect to the periphery of the movable member 206 is indistinguishable to the human eye.

[0034] In an embodiment, the movable member 206 may comprise a pattern that defines the first reference 210. Further, the first reference 210 may be configured to be recognised by a machine (for example, a scanner). For example, the first reference 210 may be a barcode, a QR code or the like.

[0035] In another embodiment, a label, generally a security label, comprising the first reference 210 may be affixed to the movable member 206.

[0036] In an embodiment, the first part 202 may comprise an outer cover 216, covering the movable member 206, to prevent manual change of the position of the movable member 206.

[0037] In an embodiment, the outer cover 216 may be a transparent cap that allows the scanning of the first reference 210.

[0038] Referring to FIGs. 3, 4 and 5, the second part 204 may comprise projections 312a, 312b that may be configured to pass through eyelets 314a, 314b defined by the article 104. The projections 312a, 312b may be configured to be engaged with the first part 202, thereby locking the device 102 with the article 104. The projections 312a, 312b may define holes 308a, 308b such that longitudinal axis 320 of the projections 312a, 312b are perpendicular to longitudinal axis 322 of the holes 308a, 308b.

[0039] In an embodiment, each lever 208a, 208b may be attached to a lever shaft 302a, 302b. Side face 326 of the first part 202 may define a slot 328. The lever shaft 302a, 302b moves laterally along length of the slot 328, when the levers 208a, 208b are pulled away from each other or pulled close to each other.

[0040] In an embodiment, a pair of rods 306a, 306b may be connected to the lever shafts 302a, 302b, wherein free end of the rods 306a, 306b may be configured to be received by the holes 308a, 308b. Inward and outward motion of the rods 306a, 306b into the holes 308a, 308b may couple and decouple the first part 202 with the second part 204 respectively.

[0041] In an embodiment, a stem 316 of the movable member 206 may be rigidly attached to a ratchet 304 such that the rotation of the ratchet 304 results in the rotation of the movable member 206. A pair of racks 310a, 310b may be in contact with the ratchet 304 such that racks 310a, 310b are diametrically opposite to each other. Inside of the racks 310a, 310b that is in contact with the ratchet 304, may comprise teeth like projections 324. One end of the rack 310a may be in contact with the lever shaft 302a and one end of the rack 310b may be in contact with the lever shaft 302b. The linear movement of the racks 310a, 310b causes the ratchet 304 to rotate about its axis.

[0042] In an embodiment, the device 102 may comprise a pawl 318. The pawl 318 may be engaged to the ratchet 304 such that the pawl 318 arrests the rotation of the ratchet 304 in one direction (as an example, counter clockwise) and allows the rotation of the ratchet 304 in the opposite direction (clockwise).

[0043] Referring specifically to FIG. 4, the levers 208a, 208b may be pulled close to each other to unlock the device 102. When the levers 208a, 208b are pulled close to each other, the lever shafts 302a, 302b move close to each other laterally along the length of the slot 328. The racks 310a, 310b attached to the lever shafts 302a, 302b move linearly to rotate the ratchet 304 in an anti-clockwise direction 330. The pawl 318 that is in contact with the ratchet 304, restricts the rotation of the ratchet 304, thereby restricting the rotation of the movable member 206. This results in the racks 310a, 310b sliding over the ratchet 304. As the racks 310a, 310b move linearly, the rods 306a, 306b move out of the holes 308a, 308b, thus unlocking the first part 202 from the second part 204. At this point, the device 102 is in the unlocked position (second state). The movable member 206, which is in contact with the ratchet 304, will have the same position as it had when the device 102 was in the locked position, prior to the unlocked position.

[0044] Now, referring specifically to FIG. 5, the levers 208a, 208b may be pulled away from each other to lock the device 102. When the levers 208a, 208b are pulled away from each other, the lever shafts 302a, 302b move away from each other laterally along the length of the slot 328. The racks 310a, 310b attached to the lever shafts 302a, 302b move linearly to rotate the ratchet 304 in a clockwise direction 332. The pawl 318 slides over the ratchet 304, thereby allowing the rotation of the ratchet 304. The rotation of the ratchet 304 results in the rotation of the movable member 206. As the racks 310a, 310b move linearly, the rods 306a, 306b move into the holes 308a, 308b, thus locking the first part 202 and the second part 204. At this point, the device 102 is in the locked position (first state). The movable member 206, which is in contact with the ratchet 304, will rotate to assume a position that may be different from the immediately preceding position of the movable member 206 when the device 102 was in a

locked position.

[0045] FIGs. 6A-6C illustrate the change in the position of the movable member 206 during the locking and unlocking of the device 102, in accordance with an embodiment. Referring specifically to FIG. 6A, the device 102 is in locked position and may be registered. The registration may be done by scanning the first reference 210 and the second reference 212 to determine spatial orientation. At the time of registering, it may be determined that the first reference 210 is at a position wherein angle between the line joining the second reference 212 and the geometric centre 602 of the movable member 206 and the line joining the first reference 210 and the second reference 212 is 20 degrees. This data may be stored in the server 110 at the time of registration.

[0046] Now referring specifically to FIG. 6B, the levers 208a, 208b are pulled close to each other to unlock the device 102. As the levers 208a, 208b are pulled close, the racks 310a, 310b move linearly to rotate the ratchet 304. But the pawl 318 restricts the rotation of the ratchet 304. The non-rotation of the ratchet 304 results in the movable member 206 retaining the position it had when the device 102 was in the locked position. That is, the orientation of the movable member 206 remains 20 degrees.

[0047] Referring specifically to FIG. 6C, the levers 208a, 208b are pulled away from each other to re-lock the device 102. As the levers 208a, 208b are pulled away, the racks 310a, 310b move linearly to rotate the ratchet 304. Rotation of the ratchet 304 results in the rotation of the movable member 206. This results in change in the spatial orientation between the first reference 210 and the second reference 212, which is 45 degrees. The first reference 210 and the second reference 212 may be scanned to determine the spatial orientation. Change in orientation of the movable member 206 may indicate tampering.

[0048] It is clearly understood that the tampering of the device 102 is detected by detecting the change in the orientation of the movable member 206. In theory, if the angle of rotation of the movable member 206 is known (every time the device 102 is locked), the first reference 210 can be brought back to initial position (position of the movable member 206 at the time of registration) by locking and unlocking the device 102 for a particular number of times.

[0049] However, practically speaking, even if the first reference 210 is brought back to the initial position, the system 100 may still detect tampering of the device 102. This is because, the first reference 210 may not be brought to the exact position due to discrepancies caused by friction, backlash, wear or the like.

[0050] In an embodiment, the device 102 may be reused once the article 104 is delivered at the point of delivery, thereby avoiding the use of a new device 102 every time a new article

104 has to be shipped.

[0051] Referring to FIG. 7, various modules of the tamper detector 106 are disclosed, in accordance with an embodiment. The tamper detector 106 comprises an image capturing module 702, a processor 704, a memory module 706, input modules 708, output modules 710 and a communication module 712.

[0052] The image capturing module 702 may be a camera that captures one or more images of the first reference 210 along with the second reference 212.

[0053] The processor 704 may be implemented in the form of one or more processors and may be implemented as appropriate in hardware, computer-executable instructions, firmware, or combinations thereof. Computer-executable instruction or firmware implementations of the processor 704 may include computer-executable or machine-executable instructions written in any suitable programming language to perform the various functions described.

[0054] The processor 704 may be configured to receive information corresponding to the orientation of the movable member 206 from the image capturing module 702. Further, the processor 704 may be configured to compare the instant orientation of the movable member 206 and the orientation registered against the device 102 in the server 110 at the time of registration. The processor 704 may determine tampering of the device 102 based on the difference in the orientation of the movable member 206.

[0055] The memory module 706 may include a permanent memory such as hard disk drive, may be configured to store data, and executable program instructions that are implemented by the processor 704. The memory module 706 may be implemented in the form of a primary and a secondary memory. The memory module 706 may store additional data and program instructions that are loadable and executable on the processor 704, as well as data generated during the execution of these programs. Further, the memory module 706 may be volatile memory, such as random-access memory and/or a disk drive, or non-volatile memory. The memory module 706 may comprise of removable memory such as a Compact Flash card, Memory Stick, Smart Media, Multimedia Card, Secure Digital memory, or any other memory storage that exists currently or may exist in the future.

[0056] The input modules 708 may provide an interface for input devices such as keypad, touch screen, mouse, microphone and stylus among other input devices.

[0057] The output modules 710 may provide an interface for output devices such as display screen, speakers, printer and haptic feedback devices, among other output devices.

[0058] Alternatively, or in addition, the communication module 712 may be used by the tamper detector 106 to communicate with the server 110 via the communication network 108.

The communication module 712, as an example, may be a GPRS module, or other modules that enable communication. The communication module 712 may include a modem, a network interface card (such as Ethernet card), a communication port, or a Personal Computer Memory Card International Association (PCMCIA) slot, among others. The communication module 712 may include devices supporting both wired and wireless protocols. Data in the form of electronic, electromagnetic, optical, among other signals may be transferred via the communication module 712.

[0059] In an embodiment, the tamper detector 106 may include a scanning module that may scan the device 102 and communicate the same to the server 110. The server 110 may use the scanned information to compare the orientation of the movable member 206 at the time of registration and verification.

[0060] FIG. 8 is a flowchart 800 illustrating a method for identification of tampering of the device 102, in accordance with an embodiment. Referring to step 802, the device 102 is engaged to the article 104 in the locked position. The device 102 may be engaged automatically to the article 104 by a machine that is configured to engage the device 102 to the articles 104 in a packaging line.

[0061] At step 804, the orientation of the movable member 206 is determined at a point of registration. The scanning module of the tamper detector 106 may be used to scan the orientation of the movable member 206.

[0062] At step 806, the determined orientation of the movable member 206 is associated to an ID of the device 102 (or the article 104) and is registered in the server 110. The ID of the device 102 may be a unique identifier such as barcode, QR code or the like, that uniquely identifies the device 102. The ID of the device 102 may be scanned by a scanning device (may be similar to the scanning module of the tamper detector 106) that may be configured to associate the orientation of the movable member 206 with the ID of the device 102.

[0063] At step 808, the device 102 is verified for tampering at a point of verification. The orientation of the movable member 206 is determined. The tamper detector 106 may be configured to scan the orientation of the movable member 206. The tamper detector 106 may be configured to communicate with the server 110 to obtain the information pertaining to the orientation of the movable member 206 to the corresponding ID of the device 102.

[0064] At step 810, the orientation of the movable member 206 pertaining to ID of the device 102 that is recognized by the tamper detector 106 is compared with the orientation information available in the server 110. If the orientation of the movable member 206 matches with the orientation associated to the ID of the device 102, the tamper detector 106 indicates

no tampering (step 812). If the orientation of the movable member 206 does not match with the orientation associated to the ID of the device 102, the tamper detector 106 indicates tampering of the device 102 (step 814).

[0065] FIG. 9 is a section view of the device 102 in the unlocked position along the section plane 220 (shown in FIG. 2), without the pawl 318, in accordance with an embodiment. The device 102 comprises a set of racks 902a, 902b that are in contact with the ratchet 304. The racks 902a, 902b have a plurality of set of teeth 904 placed at a preconfigured distance. This configuration of the teeth 904 causes a difference in the angle of rotation of the ratchet 304 every time the device 102 is locked and unlocked. For example, the ratchet 304 may rotate for 60 degrees clockwise when the device 102 assumes the locked position and the ratchet 304 may rotate for 30 degrees counter clockwise when the device 102 assumes the unlocked position. This results in change in orientation of the movable member.

[0066] FIG. 10A illustrates a push lock device 1000, in accordance with an embodiment. The device 1000 comprises the movable member 206, the outer cover 216 and a retractable member 1004. The outer cover 216, as described earlier, may be a transparent cover that covers the movable member 206.

[0067] In an embodiment, the movable member 206 may comprise the first reference 210 and the outer cover 216 may comprise the second reference 212.

[0068] In an embodiment, the movable member 206 may be rotatably in contact with the outer cover 216. That is, the movable member 206 is configured to rotate about its axis, independent of the rotation of the outer cover 216. One end of the outer cover 216 may define a plurality of teeth like projections 1002.

[0069] In an embodiment, the retractable member 1004 may be connected to the movable member 206 such that the linear motion of the retractable member 1004 translates into a rotational motion of the movable member 206.

[0070] Referring to FIG. 10B, the projections 1002 may be configured to be engaged to a surface 1006 of the article 104 when the push lock device 1000 is pushed against the surface 1006. The projections 1002 arrest the rotational motion of the outer cover 216. However, the retractable member 1004 does not penetrate the surface 1006, instead retracts, causing the movable member 206 to rotate. The orientation of the movable member 206 may be registered and stored in the server 110.

[0071] When the push lock device 1000 is disengaged from the surface 1006, the retractable member 1004 extends, but the rotation of the movable member 206 is restricted. Thus, when the push lock device 1000 is re-engaged to the surface 1006, the movable member

206 rotates causing a change in the orientation. The instant orientation may be cross checked against the orientation that was stored in the server 110 at the time of registration to determine tampering.

[0072] In another embodiment, the device 102 may comprise an intelligent tag such as an NFC tag. The smart tag may be configured to log data such as time, temperature, shock or the similar intelligent tracking data at each instance the device 102 is scanned. Optionally, the intelligent-tag can be mechanically linked with opening and closing of the reusable device 102 such as to record the time of opening and closing. Further, the data may be stored at the server 110. Whenever the device 102 is scanned, the smart tag may be scanned parallelly with the scanning of the spatial orientation of the first reference 210 with respect to the second reference 212. Further, the data stored at the server 110 may be validated only upon the validation of the spatial orientation of the first reference 210 with respect to the second reference 212. This configuration aids in detecting mishandling or tampering of the device 102.

[0073] In another embodiment, the smart tag may be placed below a label, affixed to the movable member 206, comprising the first reference 210. The tampering of the smart tag results in tampering of the label thereby causing a change in the spatial orientation of the first reference 210 with respect to the second reference.

[0074] The processes described above is described as a sequence of steps, this was done solely for the sake of illustration. Accordingly, it is contemplated that some steps may be added, some steps may be omitted, the order of the steps may be re-arranged, or some steps may be performed simultaneously.

[0075] The example embodiments described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware.

[0076] Although embodiments have been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the system and method described herein. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

[0077] Many alterations and modifications of the present invention will no doubt become apparent to a person of ordinary skill in the art after having read the foregoing description. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. It is to be understood that the description above contains many specifications, these should not be construed as limiting the scope of the invention but as

merely providing illustrations of some of the personally preferred embodiments of this invention.

CLAIMS

I claim,

1. A system for enabling identification of tampering, the system comprising a device engaged to an article the device comprising:
   a movable member; and
   a first reference provided on the movable member, wherein,
      the device is operable to assume a first state and a second state;
      position of the movable member changes at each instance the device is brought back to the first state; and
      orientation of the movable member is determined by determining spatial orientation of the first reference with respect to a second reference, wherein the second reference is external to the movable member.
2. The system as claimed in claim 1, wherein the second reference is stationary when the device assumes the first state and the second state.
3. The system as claimed in claim 1, wherein the first reference and the second reference are machine readable.
4. The system as claimed in claim 1, comprising a label, wherein:
   the label is affixed to the movable member; and
   the first reference is present in the label.
5. The system as claimed in claim 1, the first state is a lock position and the second state is an unlock position, wherein,
   the device, in the lock position, restricts access into an article which is locked by the device; and
   the device, in the unlock position, allows access into an article which is locked by the device.
6. The system as claimed in claim 1, comprising at least one processor configured to:
   receive orientation of the movable member in the first state at a registration phase;
   receive orientation of the movable member in the first state at a verification phase;
   compare whether the orientation of the movable member in the first state received at the verification phase is same as the orientation of the movable member in the first state received at the registration phase; and
   indicate tampering of the device if the orientation of the movable member in the first state received at the verification phase is not same as the orientation of the movable member in the first state received at the registration phase.

7. The system as claimed in claim 1, wherein the device is dis-engageable from the article by operating the device to assume the second state, and reusable to engage the device to another article.
8. The system as claimed in claim 1, wherein at least a position, which is visible to human eye, of the movable member, has a generally circular configuration.
9. The system as claimed in claim 8, wherein the movable member comprises a peripheral configuration, which limits human ability to compare between positions assumed by the movable member.
10. The system as claimed in claim 1, wherein the movable member comprises a pattern that limits human ability to distinguish the first reference in the pattern.
11. The system as claimed in claim 1, wherein the device comprises a smart tag configured to:

    report previously logged data at each instance of scanning of the device; and

    validate the reported data upon validation of the spatial orientation of the first reference with respect to the second reference.
12. The system as claimed in claim 1, wherein the device comprises a smart tag that is placed below a label, affixed to the movable member, comprising the first reference in a manner that any tampering of the smart tag results in tampering of the spatial orientation of the first reference with respect to the second reference.

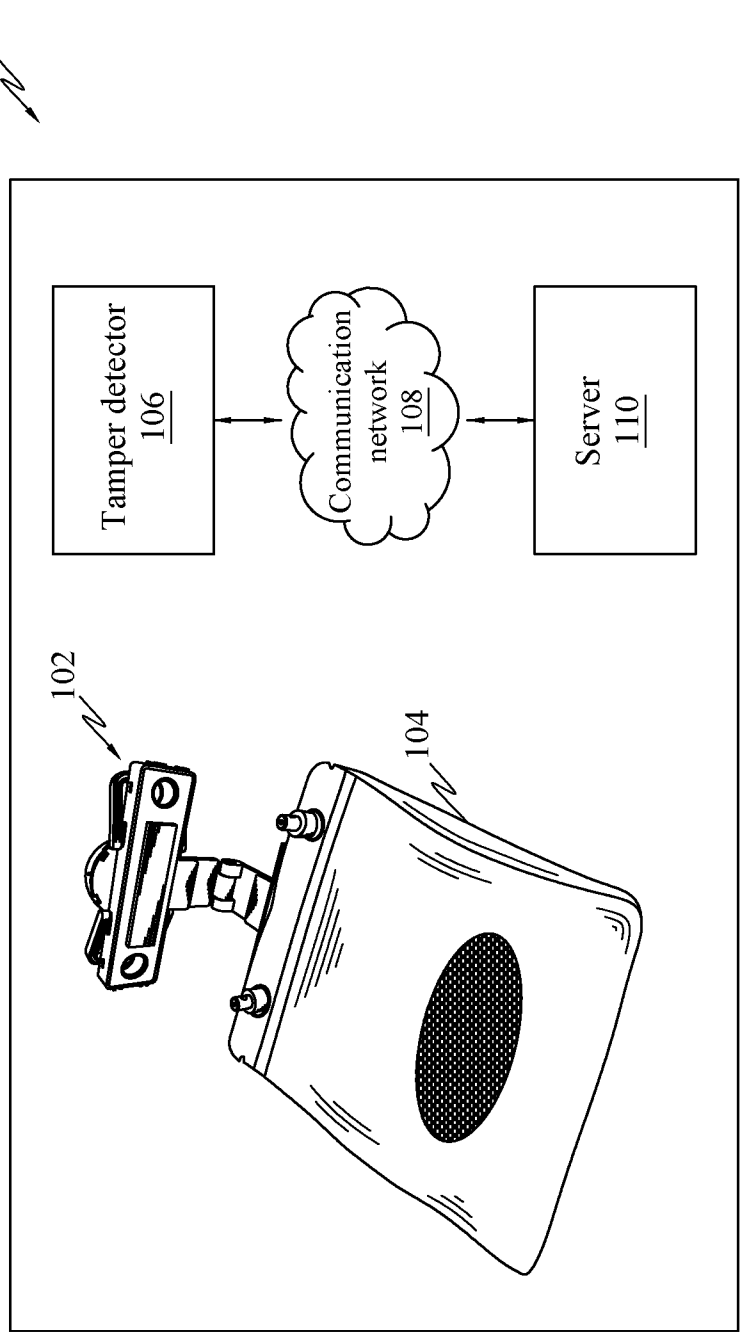
100
Tamper detector
106
Communication
network
108
Server
110
102
104

FIG. 1

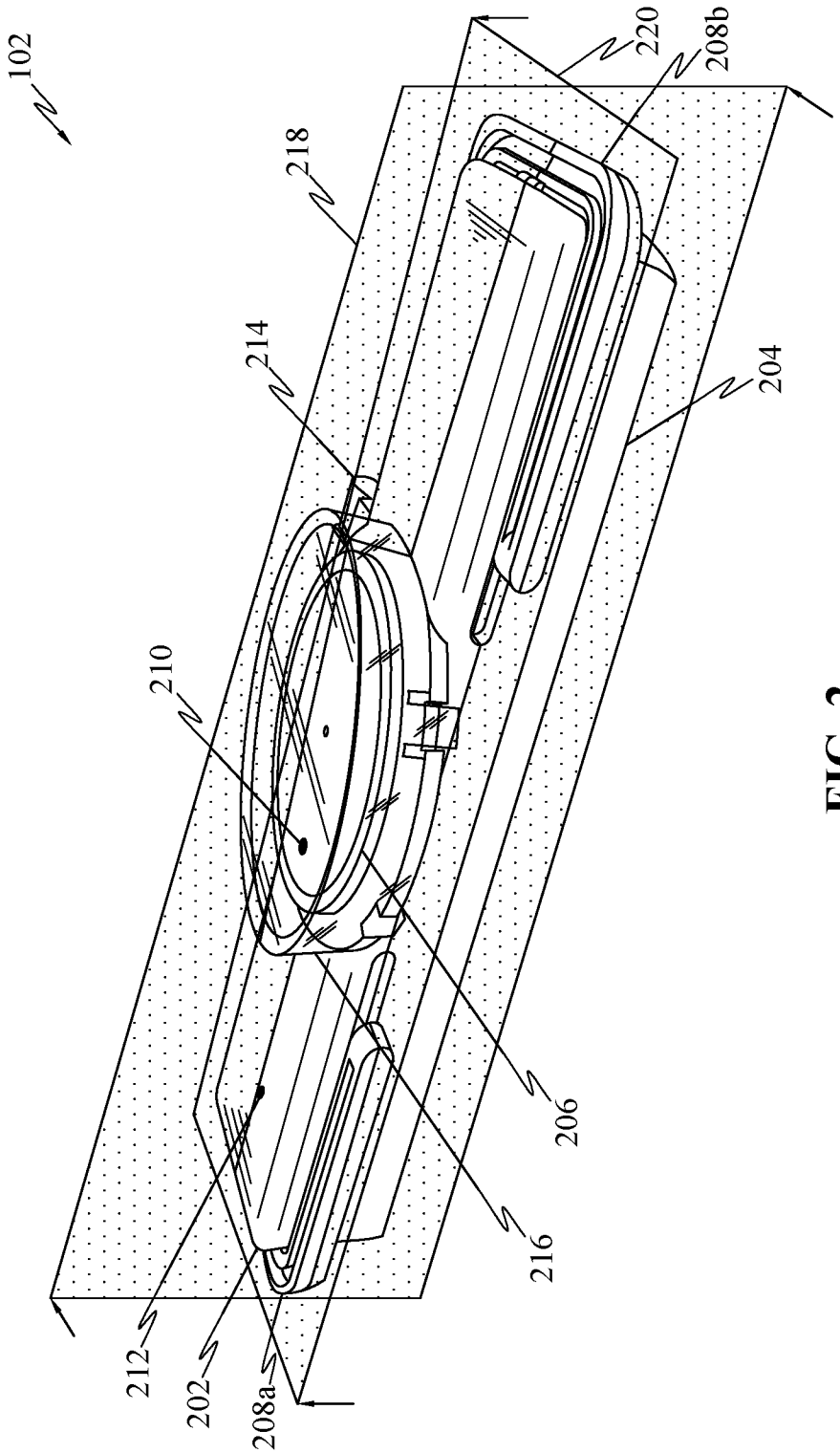

FIG. 2

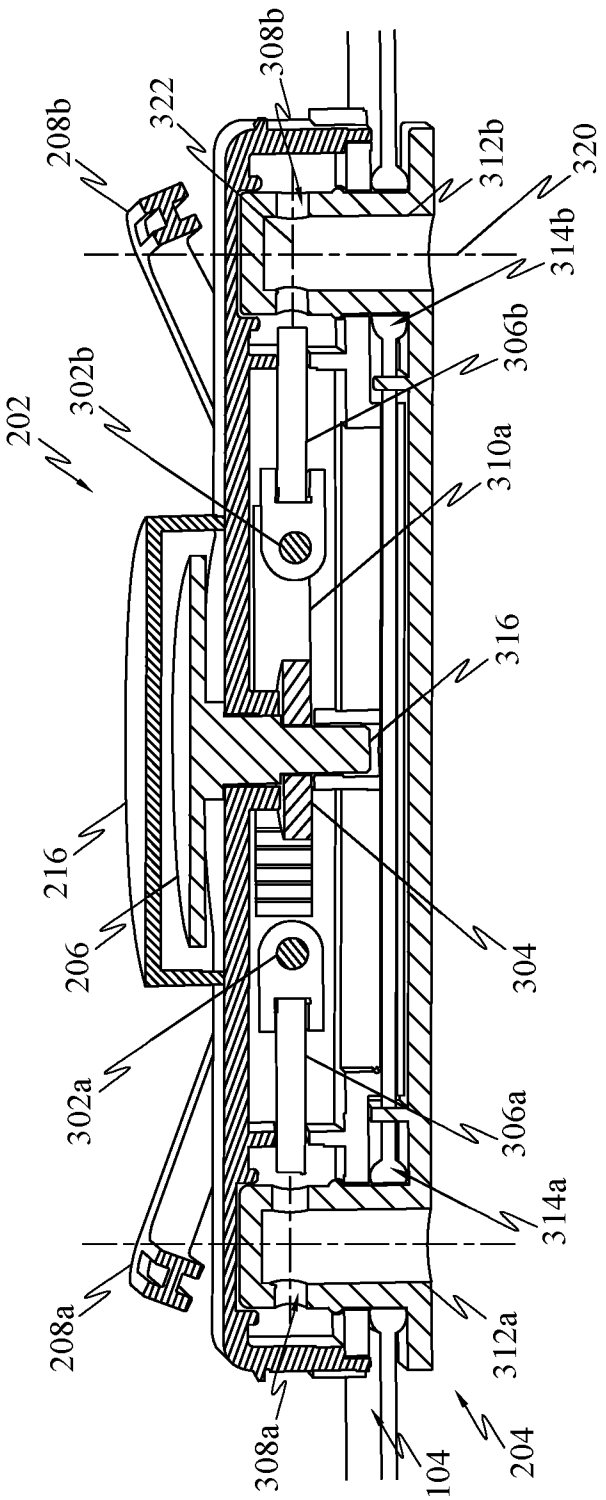
308b
322
208b
312b
320
314b
306b
302b
202
310a
316
216
206
304
302a
306a
314a
208a
312a
308a
104
204

FIG. 3

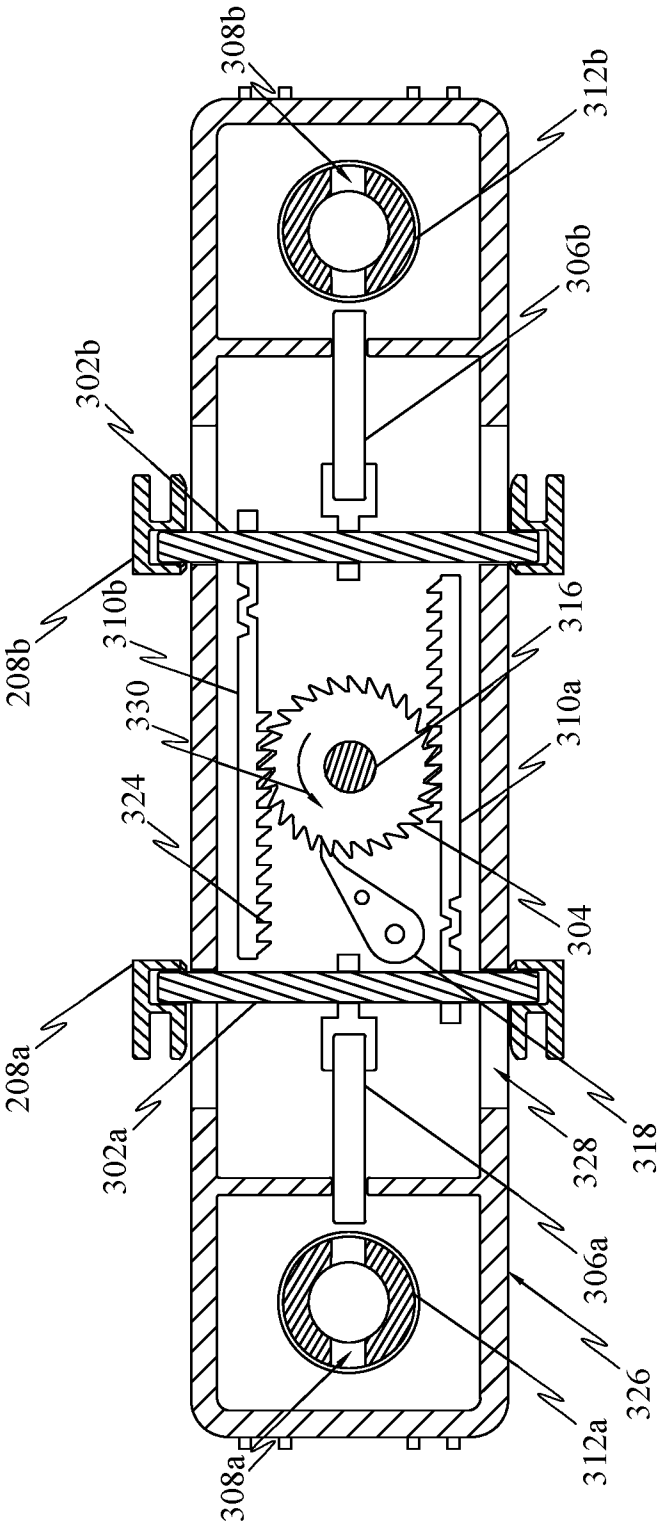
308b
312b
306b
302b
208b
310b
316
330
310a
324
304
208a
302a
328
318
306a
326
312a
308a

FIG. 4

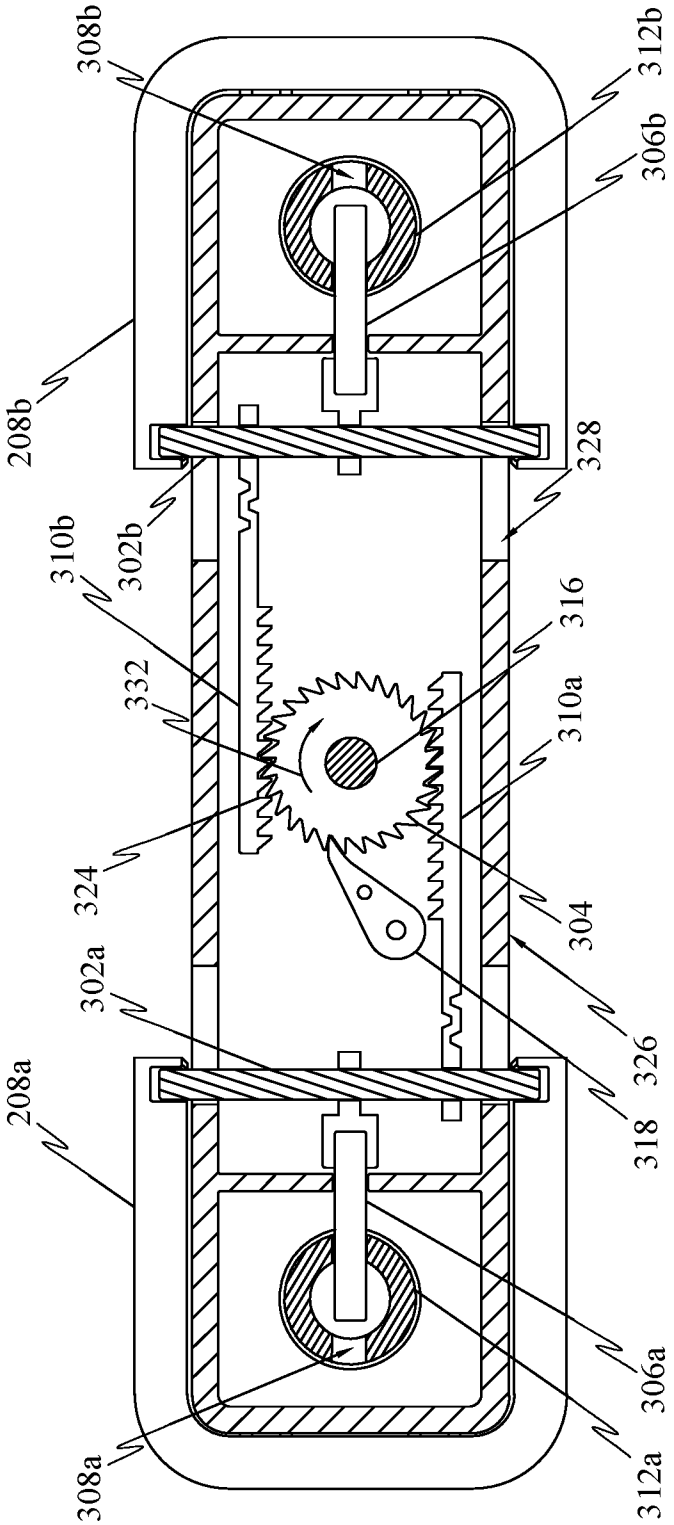
308b
312b
306b
208b
328
310b
302b
316
332
310a
324
304
302a
326
208a
318
306a
308a
312a

FIG. 5

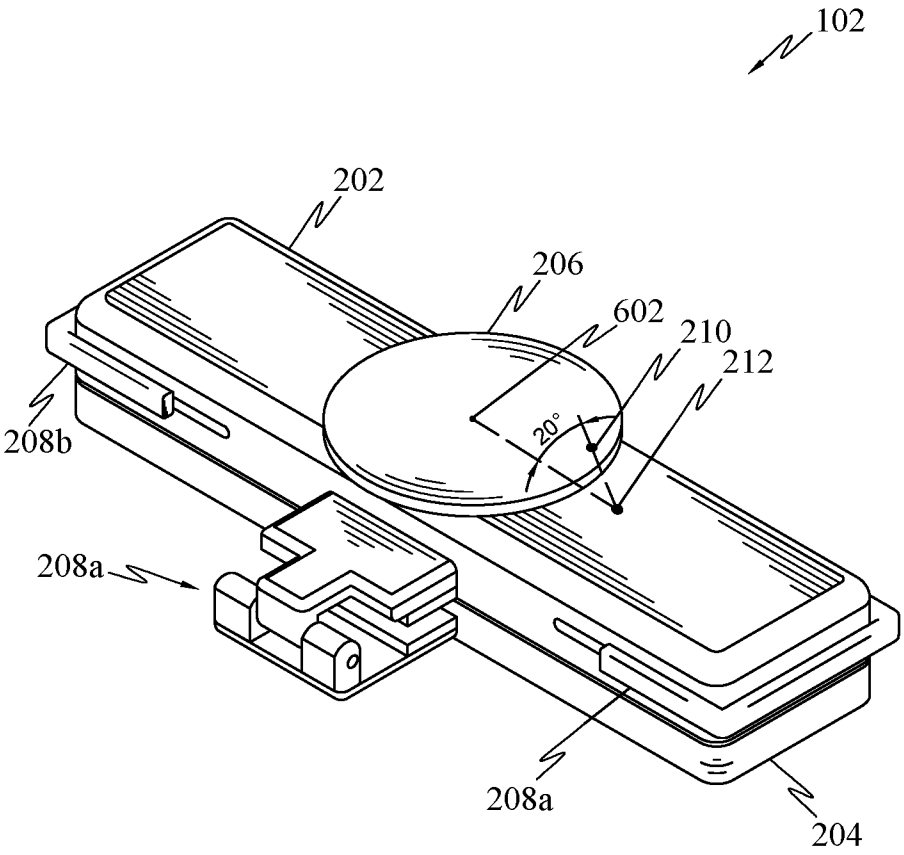

FIG. 6A

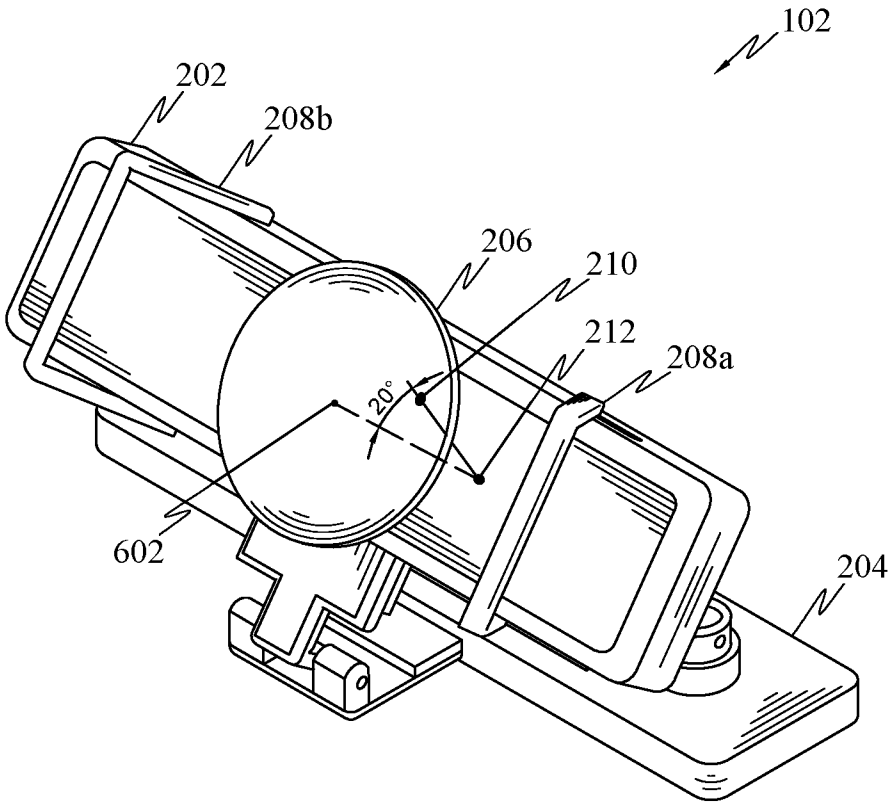

FIG. 6B

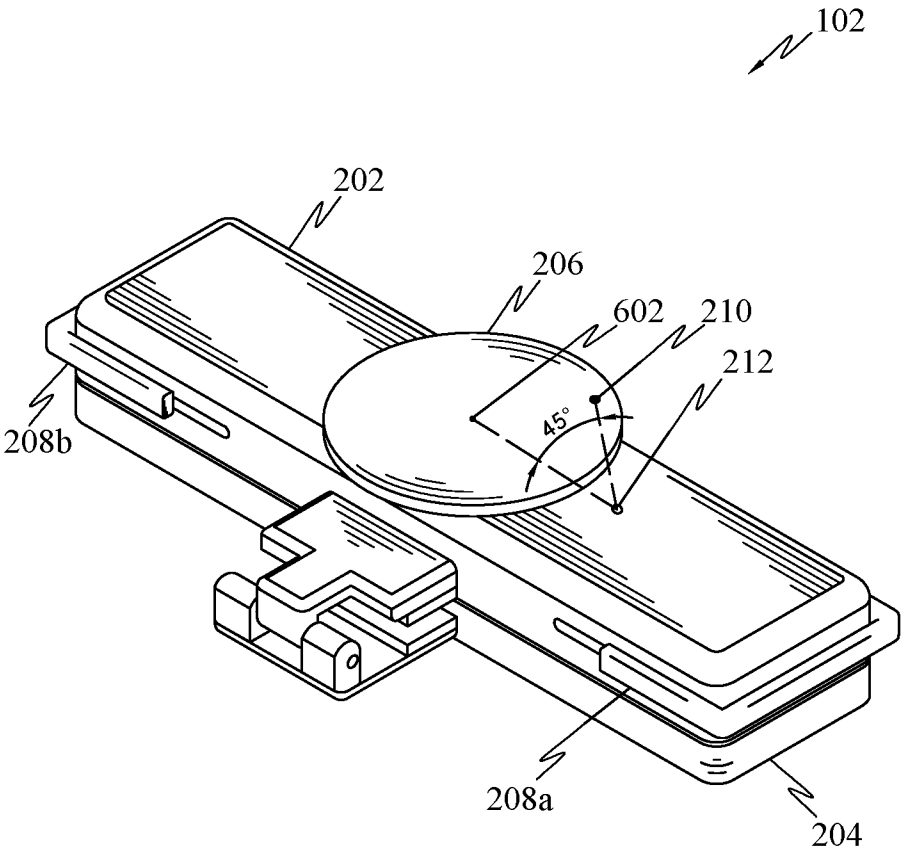

FIG. 6C

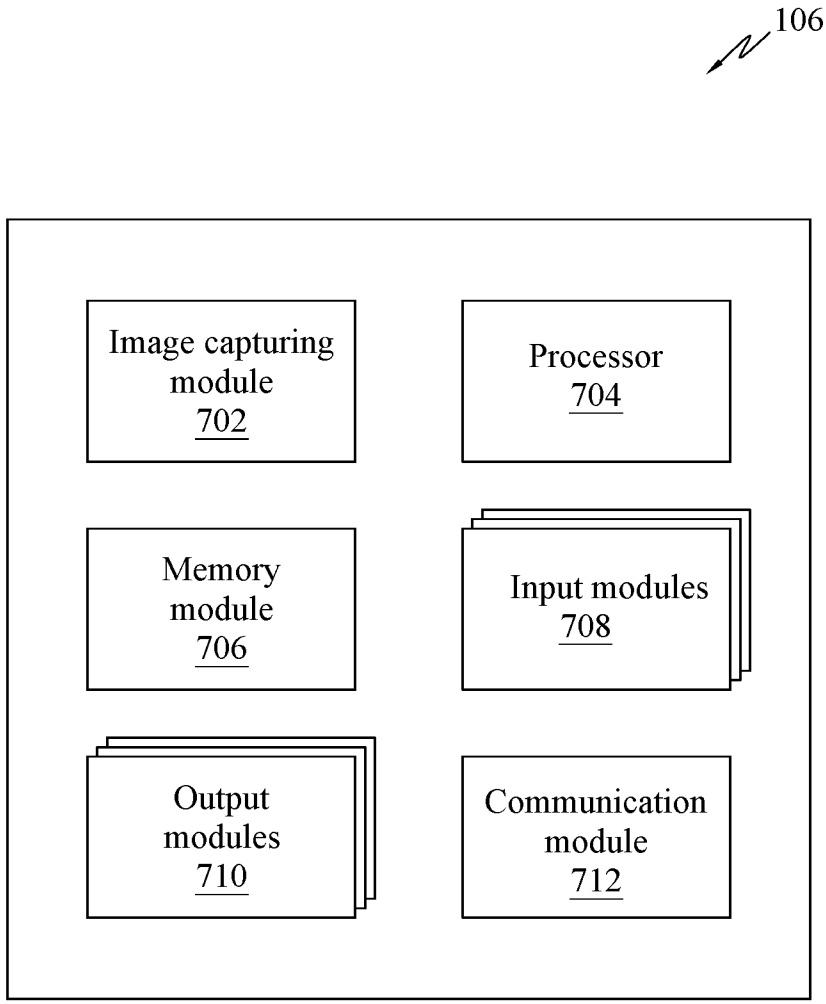
106
Image capturing module 702
Processor 704
Memory module 706
Input modules 708
Output modules 710
Communication module 712

FIG. 7

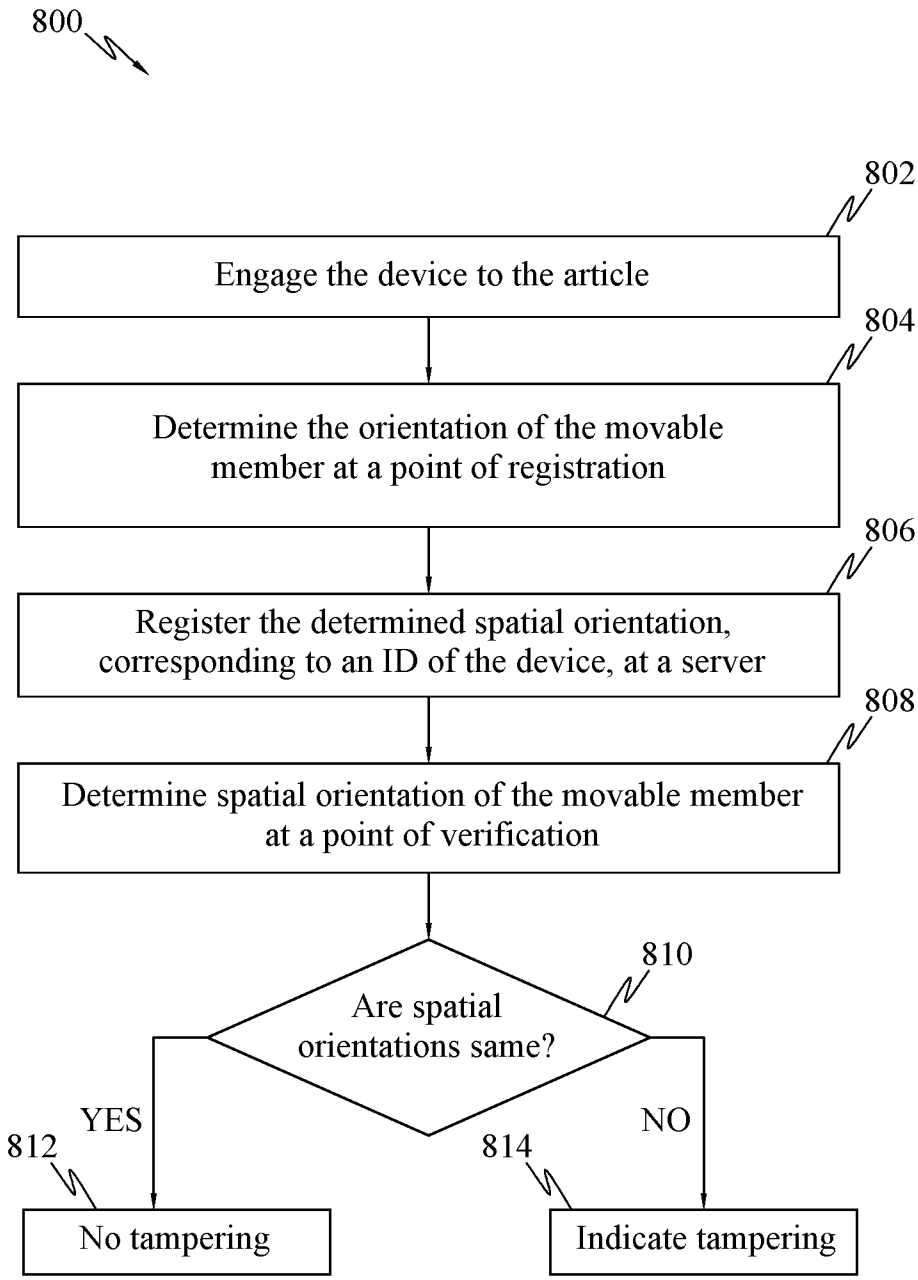
800
802
Engage the device to the article
804
Determine the orientation of the movable member at a point of registration
806
Register the determined spatial orientation, corresponding to an ID of the device, at a server
808
Determine spatial orientation of the movable member at a point of verification
810
Are spatial orientations same?
YES
NO
812
814
No tampering
Indicate tampering

FIG. 8

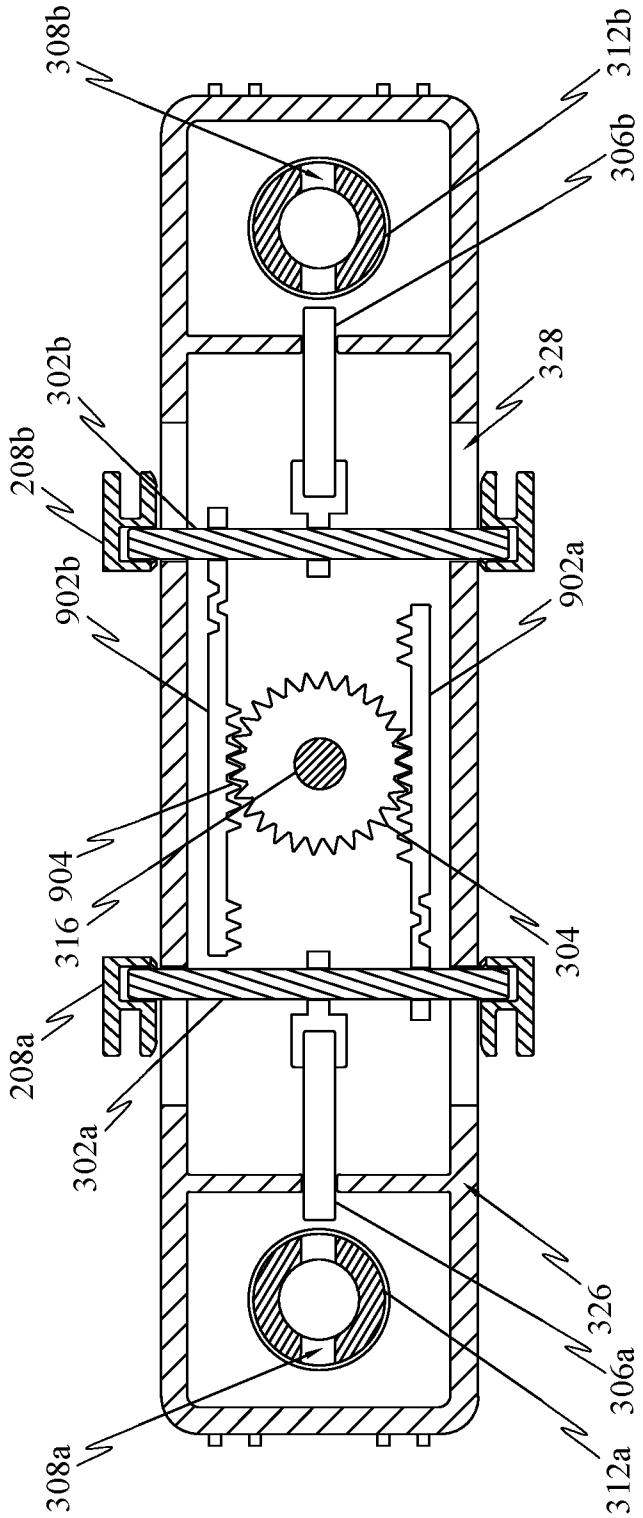
308b
312b
306b
328
302b
208b
902b
902a
904
316
304
208a
302a
326
306a
308a
312a

FIG. 9

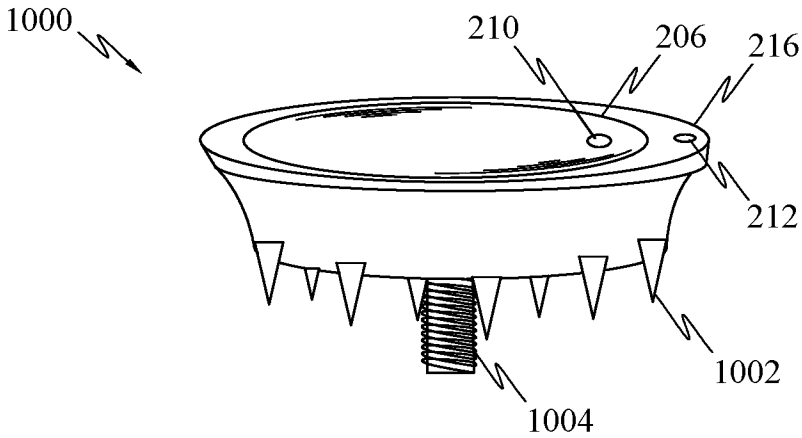

FIG. 10A

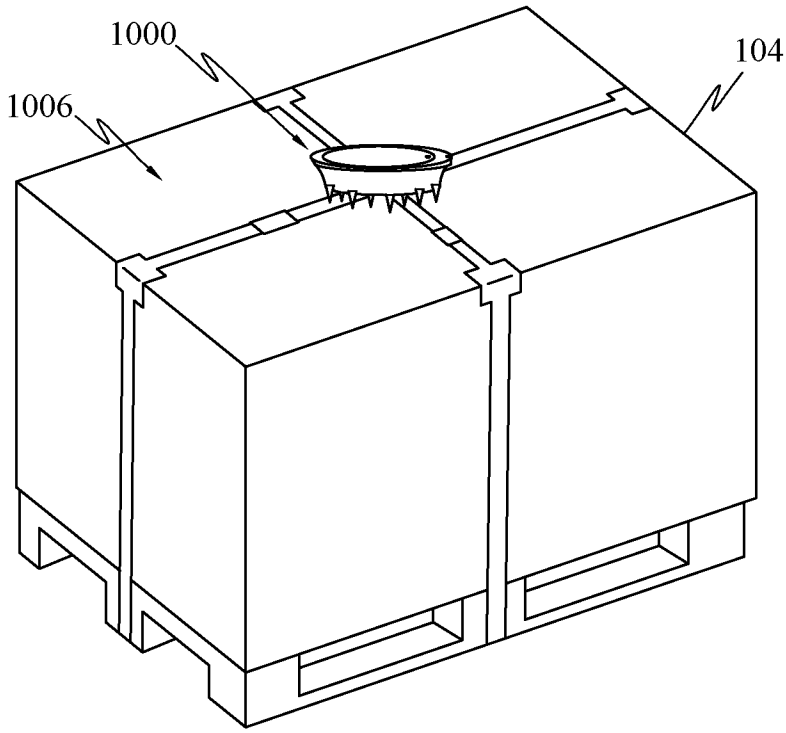

FIG. 10B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2019/052080

A. CLASSIFICATION OF SUBJECT MATTER
G06K9/20,B65D55/02 Version=2019.01

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)

G06K, B65D

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)

Databases:- TotalPatent One, IPO Internal Database
Keywords:- spatial orientation, security label, external reference, scan

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO2018/073699A1 (ASHISH ANAND) 26 April 2018 (26-04-2018) Abstract; Paragraphs [0001]-[0002], [0007]-[0012], [0018], [0027], [0056]-[0059]	1-12

☐ 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
"D" document cited by the applicant in the international application
"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	Date of mailing of the international search report
26-09-2019	26-09-2019
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Anil Tagale Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2019/052080

Citation	Pub.Date	Family	Pub.Date
WO 2018/073699 A1	26-04-2018	US 20190225395 A1	25-07-2019