



(51) International Patent Classification:

G09F 3/00 (2006.01)

G09F 3/03 (2006.01)

(21) International Application Number:

PCT/IB2019/000627

(22) International Filing Date:

31 July 2019 (31.07.2019)

(25) Filing Language:

Italian

(26) Publication Language:

English

(30) Priority Data:

102018000007722 01 August 2018 (01.08.2018) IT

(72) Inventor; and

(71) Applicant: TONELLI, Alfredo [IT/IT]; Contrada Balsamate 25, 66038 San Vito Chietino (IT).

(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: ANTI BREAK-IN SYSTEM AND ANTI-COUNTERFEIT SYSTEM FOR CONTAINERS

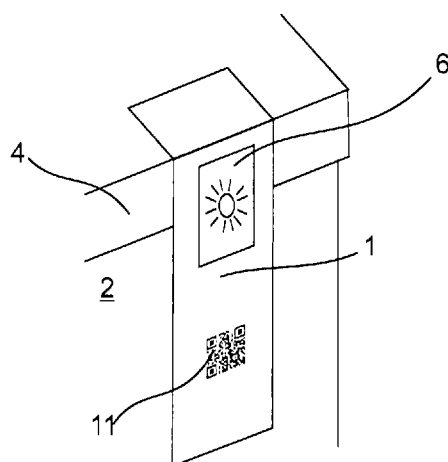


Fig.1C

(57) Abstract: Anti break-in system for a container (2) having an inner compartment (3) and at least one closure element (4) of the compartment (3), comprising: - a label (1) attachable to the container (2) crossing the at least one closure element (4); - a reference image (5); wherein said label (1) comprises a univocal security image (6) equal to said reference image (5) and means configured to change the aspect of said security image (6) with respect to the reference image (5) when the label (1) is at least in part removed from the container (2) and/or from the at least one closure element (4).



TITLE

ANTI BREAK-IN SYSTEM AND ANTI-COUNTERFEIT SYSTEM FOR CONTAINERS

DESCRIPTION**TECHNOLOGICAL FIELD**

The present invention relates to the sector of anti break-in systems, namely to verify the opening, of a container on which the anti break-in system is installed.

In particular, the present invention relates to anti break-in systems for packs, jar, boxes, envelopes, bags, suitcases, doors and any container provided with a compartment and at least one compartment opening element.

The present invention also relates to the field of anti-counterfeiting systems.

STATE OF THE ART

The state of the art includes various known solutions to check if a container has been opened. One of the simplest and most widespread solutions is to affix a fragile security element between an opening element of the container and the body of the container itself, to verify its possible opening. Just think of the lacquer wax that came in antiquity affixed to the letters, or think to the adhesive labels that are normally placed on the food tins, or to the adhesive tapes that are placed on the closing edges of the carton boxes.

All these known systems have the common defect that they are removable and repositionable, without leaving obvious evidence of their corruption. Substantially, these safety elements can be removed at least in part from the container, in order to violate or withdraw the contents of the container, and subsequently reattached to the container without a clear trace of the break-in resulting on the safety element itself.

There are also more advanced security labels, which make it possible to make a writing appear, for example the word "VOID", if the label has been removed from the container on which it was attached.

Adhesive labels with specific carvings are also known, such that, if the label is detached from the container on which it was affixed, the label is irreparably damaged indicating the break-in. However, none of the aforementioned systems makes it possible to be certain that the label has not been tampered with.

Furthermore, it is not known a system which allows to certify the break-in of a container on which a safety label is affixed.

Finally, there is no system available that permits the remote traceability of the violated containers, that is to say opened by removing or corrupting the seal and safety label.

SUMMARY

The aforesaid drawbacks of the known art are now solved by an anti break-in system for containers according to claim 1 and by a method of checking for the break-in of a container according to claim 17. Further drawbacks are solved thanks to the details and to the technical characteristics of the present invention as provided by the dependent claims.

These and other advantages will appear more in detail from the following description of an embodiment given by way of non-limiting example with reference to the accompanying drawings.

DESCRIPTION OF THE DRAWINGS

In drawings:

Fig. 1A-1D show schematic views of the anti break-in system according to the present invention ;

Fig. 2A-2F show schematic views of the anti break-in system applied to various types of containers ;

Fig. 3 show an axonometric schematic view of an anti break-in system label ;

Fig. 4A e 4B show a schematic detail view of the layers that make up the label according to the first embodiment of the present invention ;

Fig. 4C show a label according to the present invention in which half of the label has been altered and the other half is still intact;

Fig. 4D shows a schematic detail view of the alteration suffered by the label when it is removed from the container;

Fig. 5A-5C show a schematic view of a first version of the first embodiment of the anti break-in system label when not violated (Fig. 5A), when the label is violated (Fig. 5B) and when the violated label is repositioned so as to simulate non-break-in (Fig. 5C);

Fig. 6A-6C show a schematic view of a second version of the first embodiment of the anti-break-in system label when not violated (Fig. 6A), when the label is violated (Fig. 6B) and when the violated label is repositioned so as to simulate non-break-in (Fig. 6C);

Fig. 7A-7C show a schematic view of a second embodiment of the anti-break-in system label when not violated (Fig. 7A), when the label is violated (Fig. 7B) and when the violated label is repositioned so as to simulate the non break-in (Fig. 7C);

Fig. 8 illustrates a schematic view of the anti break-in system in which a mobile device, a remote

database and a label according to the present invention is visible;

Fig. 9 illustrates a schematic view of the architecture of the anti break-in system mobile device;

Fig. 10 illustrates a flow chart relating to the method of checking for the break-in of a container according to the present invention.

DETAILED DESCRIPTION

The following description of one or more embodiments of the invention refers to the attached drawings. The same numerical references in the drawings identify identical or similar elements. The object of the invention is defined by the attached claims. The technical details, structures or features of the solutions described below can be combined with each other in any way.

With reference to Fig. 1 there is shown an anti break-in system of a container 2 comprising a label 1 attachable to the container 2.

In particular, Fig. 1A illustrates an adhesive label attached to a container 2 in which there is a security image 6 and a reference image 5. Since the label 1 is integral and completely attached to the container 2, the two images 5, 6 are the same.

In Fig. 1B a second version of the anti break-in system is visible in which the adhesive label, attached to a container 2, comprises a security image 6, while a reference image 5 is represented directly on the container 2. Being the label intact and completely attached to the container 2, the two images 5, 6 coincide.

Fig. 1C illustrates instead a label 1 on which a security image 6 is visible and, at its side, an image pointing to an external database that includes a reference image 5. Specifically, the pointer image is represented from a QR code 11 that points to a specific sector of the database 9 in which the reference image 5 is contained. In this case, the pointer image includes the information relating to the reference image, for this reason, the pointer image can be considered the reference image. This type of label 1 needs a mobile device 7 for using the QR code 11 and retrieving the reference image 5 in order to compare it with the security image 6. The security image 6 can be a code of Data Matrix type.

An optical comparison of the security image 6 with the reference image 5 allows to determine in a certain manner whether the label has been tampered with, for example removed and then reattached, in order to access the inside of the container 2.

Fig. 1D illustrates instead a label 1 on which a security image 6 is visible and, at its side, an image pointer to an external database 9 comprising a reference image 5. Specifically, the pointer image is represented by a QR code 11 that points to a specific sector of the database 9 in which the

reference image 5 is contained. In this particular version of the label 1 depicted in Fig. 1D the safety images are two 6, 24 and can be different from each other. The reference image 11 is of the QR code type as described above for Fig. 1C. In Fig. 1D, the second security image 24 is not visible since arranged on the hidden side of the label 1, in any case its positioning can be understood, since it is arranged on the label 1 in a symmetrical manner with respect to the container 2. In this a particular example of label 1, if the safety images are different from each other, also the reference images are different from each other. In practice, when it is not possible to affix the safety label 6 across the opening area, due to the shape of the container 2 or to particular irregularities of the cap which does not allow accurate adhesion of the safety label 1, it is preferable to use a security image for each contact point of the label 1 with the container 2. In this case, each security image 6, 24 has its corresponding reference image. In the case shown in Fig. 1D, the safety images 5 can be recovered remotely by means of a mobile device 7, by means of the QR code 11. The QR code 11 is preferably one, since it is unique to the label 1. Once the images of reference 5, the mobile device 7 compares the acquired security images 6, also in successive steps, in order to ascertain the possible opening of the container 2.

The label 1 comprises means configured to alter the security image 6 when the label is removed, at least in part, from the container 2, as better explained in the following. Each security image 6 is unique for each label 1, thus different for each label 1. This fact reduces the possibility to counterfeit the label 1 itself.

If the security image 6 does not coincide with the reference image 5 it is possible to establish with certainty that the label has been violated and therefore the container 2 opened.

The optical comparison of the safety image 6 with the reference image 5 can be made by a user which examines the two images by comparing them or, to obtain a more objective comparison, it can be performed by an electronic device appropriately configured as illustrated in Fig. 7. In particular, it is possible to use a mobile device 7 such as a smartphone or a tablet equipped with a camera 8, to acquire the security image 6. The same mobile device 7, which is part of the anti-break-in system, comprises a unit processing 12 configured to execute a program installed in a memory 13 of the mobile device 7. The program is configured so as to compare the security image 6 acquired by means of the camera 8 with the reference image 5, also acquired with the camera 8. If the reference image 5 is arranged on the label 1 as in the case 1A or on the container as in the case 1B, the comparison is carried out by acquiring both the images 5,6, simultaneously or in successive moments, and verifying the correspondence of the two images 5,6 acquired. The camera 8 of a mobile device 7 allows a more objective image to be acquired, and the program

allows a comparison, by overlapping, that the human eye cannot perform. This type of comparison is therefore more reliable. If the safety image 6 and the reference image 5 coincide, the label is attested by the program of the device 7 as integral. Otherwise, the program will certify the violation of label 1. The certificate can then be shown on the display 10. The mobile device 7 can also notify the label supplier or the company that affixed the labels, as a security system, that a violation has been detected. This allows you to create an archive of the violations occurred. Since the labels are different from each other, the label provider can keep track of which labels, and therefore which products or customers, have suffered a violation and also in which geographical location the violation took place. The labels are different from each other in the sense that they have security images 6, and therefore reference images 5, always different from each other, so that it is impossible for the counterfeiter to know which image will be reproduced on a specific label 1. Said security image 6 is therefore unique, i.e. the security image of a label is different from the security image of another label.

As shown in Fig. 9, the mobile device 7 comprises known means and available to the person skilled in the field of smartphones or tablets, able to acquire images 5,6 by means of the camera 8 of the mobile device 7. The mobile device 7 further comprises a display 10 connected to a processing unit 12, as well as a memory 13, a camera 8 and a possible local database 9'. In practice, the user, through the mobile device 7, frames the images 5,6 by the camera 8 and using the display 10, and acquires them. This acquisition occurs when the distance and the framing of the image 5,6 is appropriate for the acquisition.

As described more clearly below and illustrated in Fig. 8, the reference image 5 can also be contained in an archive. Said archive or database can be local 9', that is installed directly in the mobile device 7, or remote 9, so to remotely interrogated by means of the mobile device 7 through a communication network. In the latter case, the label 1 comprises an image pointing to the position in which the reference image 5 relating to the specific label 1 can be recovered.

Said image pointer can contain an internet address to be typed on a browser pre-installed in the mobile device 7, or a QR code 11 containing the information to recover said reference image 5 from the remote database 9. In the latter case, the program installed in the memory 13 of the mobile device 7 comprises a reading function of the QR code 11 configured for acquiring, by means of the camera 8, the QR code 11 and decoding it, i.e. extrapolating the address from which the reference image 5 is stored.

The reference image 5 thus recovered from the database 9 can be displayed on the display 10 and/or compared with the security image 6 acquired previously or simultaneously. In fact, the QR

code 11 can be arranged beside the security image 6 on the label 1 so as to allow the acquisition of both information simultaneously, i.e. by means of a single shot of the camera 8. The program in this case is configured to distinguish the acquired information, and in particular to temporarily store the security image 6 acquired in the memory 13 of the device 7 and to recover the reference image 5 from the database 9 and temporarily store it also in the memory 13. The images of safety 6 and reference 5 can therefore be compared by the program installed in the memory 13 of the device 7 to check whether the images 5,6 coincide or not coincide.

As previously mentioned, the program includes functions that, if from the graphic comparison of said images 5,6 results that they are different, the label 1 is declared violated. Otherwise, label 1 is recognized as intact and therefore not violated.

The program installed in the memory 13 can compare the security image 6 with the reference image 5 by superimposing or comparing the images 5, 6 pixel by pixel. Specifically, said program is configured to perform a colorimetric analysis of the pixels of the pictures 5,6. The colors of the images 5,6 are compared and, if they do not coincide, the label is considered violated.

Said program makes it possible to automate the comparison and make it more reliable than the version in which the comparison between the reference images 5 and the safety images 6 is carried out by graphic comparison by the user inspecting the label 1.

Advantageously, however, the graphic comparison carried out by the user makes it possible to disregard the mobile device 7 and therefore makes the anti-break-in system usable anywhere and by anyone, even in the absence of an internet network.

The use of a QR code 11 permits to not supply a reference image directly on the label 1, thus making the counterfeiting of the label itself even more complex.

The safety image 6 is such as to coincide with the reference image 5 when the label 1 is correctly attached to the container 2.

In practice, when a customer buys labels, he receives a series of labels 1, for example a roll of labels, and places them on a plurality of containers 2 of his products. Optionally, each of these labels 1 needs activation. The mobile device 7 or a similar device, read the identification code of the label 1, for example the QR code 11, and communicate it to a remote server. In this way, the system is able to keep track that the label 1 has been affixed to a container 2. The label 1 is preferably positioned in correspondence with the opening of the container 2 so that, in the case of opening of the container 2, the label is damaged or broken.

If the label 1 is damaged or broken, attesting the opening of the container 2 is very simple, as already happens in many anti-break-in systems.

If, on the other hand, you try to remove the label 1 to open the container 2 illegally, the label 1 is configured so that the security image 6 become altered and, comparing it with the reference image 5, it is possible to notice that they are no longer equal. This comparison makes it possible to detect the alteration of the label and therefore suspect the opening of the container 2. In this case, the security image 6 and the reference image 5 will no longer coincide, since a colorimetric alteration will have been generated on the label security image 6.

Labels 1 can be customized for a specific type of container or for a specific product or for a specific customer. Basically, the reference image 5, being univocal, also acts as an identifier of the label itself and therefore of the product on which it is used.

In this way, the same reference images 5 refers to a specific container, product or customer, and when an infringement occurs, in addition to discover the violation itself, it is possible to identify which product or container, and which customer, has been infringed.

When the comparison between the security image 6 and the reference image 5 is performed by the program installed in the mobile device 7, the program itself is configured to send a break-in report to a remote server. The break-in report, besides indicating the successful violation of the label 1, indicates the reference image 5 shown on the label 1. This report information permits to the server to associate the label 1 with the container, product or customer for which label 1 is intended.

Furthermore, the break-in report may contain information relating to the position of the mobile device 7 and therefore to the position in which the violation of the label was recorded 1. This also allows to create statistics of violation of product families or types of products or products of certain customers. For example, imagining that a label is appropriately shaped to be attached to a leather bag of a popular brand of women's bags, by analyzing the break-in reports received from the server, it will be possible to detect the break-in rate of bags and accessories of a certain popular brand and the places where they occurred.

As shown in Fig. 2, in the anti-break-in system the label 1 can be attached to the container 2. Preferably the label is attached straddling the opening of the container 2. More specifically, it is attached between the closure element 4 and the container 2 itself. The closing elements 4 can be more than one. For example, when the container 2 is an envelope, the label 1 can be attached to the body of the envelope and to the closing flap, once it is glued to the body. Alternatively, when the container is a carton box, the label 1 can be attached to the two closing edges of the box, where normally the packing tape is placed. This positioning prevents the container 2 from being opened without violating the label 1. In this way, any violation of the label 1 attests to a potential

opening of the container 2.

Positioning the label 1 on the container 2, the security image 6 is preferably positioned astride the container and its closure element 4. In practice, the security image 6 falls at the portion of the container 2 which normally it must be open to access compartment 3. In this way, the compartment 3 of the container 2 cannot be inspected without violating the label 1 and in particular altering the security image 6. In this case, as will be seen better later on, if the label 1 comprises one or more notches 19, the security image 6 will break at least in part, altering itself, in the case of opening of the container 2.

The label 1, according to a first embodiment shown in Fig. 4A, comprises various layers of material as described below. Some of said layers represent the means suitable to alter the appearance of the safety image 6, in particular the transparent layers 30, anti-adhesive 31 and the intermediate layer 32, as better explained in the following. The label 1 comprises a security image 6 which preferably is reproduced on one of the outermost layers of the label 1. For example, the security image 6 can be a painted external layer 36 placed on a layer of transparent material 30. Said transparent material 30 can preferably be a transparent polypropylene layer. The painted external layer 36, preferably with black paint, is arranged on the transparent layer 30 so as to assume a predetermined shape corresponding to the safety image 6. In the example illustrated in Fig. 4A, the painted external layer reproduces a bar code, therefore rows of black paint deposited on the transparent layer 30. In this example, the bar code is therefore the security image 6. Preferably, labels 1 relating to different containers or products differentiate between them. Even more preferably, the security image 6 is different for each label 1, so two labels 1 never reproduce the same security image.

An intermediate layer of colored paint 32 is placed under the transparent layer 30 and a layer of anti-adhesive material, preferably wax, is interposed between these two layers. The anti-adhesive layer does not completely cover the neighboring layers 30 and 32, but is arranged on the layer 30 so as to reproduce a predetermined image or shape. In the illustrated example, the anti-adhesive layer 31 is made up of a few rows of waxy material arranged perpendicular to the lines of the painted outer layer 36.

The intermediate layer of colored paint 32 comprises a uniform and homogeneous layer of paint. Preferably said first layer of colored paint comprises a clear varnish.

The intermediate layer of colored paint 32 is connected to a layer of deforming glue 33 arranged uniformly on the intermediate layer side of colored paint 32 which does not face the anti-adhesive layer 31 and therefore towards the transparent layer 30.

The painted external layer 36 reproducing the safety image 6, the transparent layer 30, the anti-adhesive layer 31, the intermediate layer of colored paint 32 and the deforming glue layer 33, represent the most important layers of the label 1 according to the first embodiment, also illustrated in Figs. 5 and 6.

In the version illustrated in Fig. 4A, to eliminate the chromatic differences which the intermediate layer of colored paint 32 could take, seen through the transparent layer 30, the label comprises an additional layer of colored paint 34 deposited on the deforming glue layer 33 which does not faces towards the middle layer of colored paint 32. The further layer of colored paint 34 can comprise a dark paint, so as to increase the chromatic contrast with the intermediate layer of colored paint 32. Alternatively, the middle layer of colored paint 32 can be dark and the further layer of colored paint 34 may be clear.

On the side of the additional layer of colored paint 34 opposite to that connected to the deforming glue layer 33 is also arranged, in a uniform and homogeneous manner, a layer of non-deforming glue 35.

The deforming glue layer 33 is finally glued on the container 2 from the side opposite to that of the further layer of colored paint 34.

The non-deforming glue of the layer 35 is more tenacious than the deforming glue of the layer 33. The deforming glue 33 has a degree of toughness such as to remove the parts of paint of the intermediate layer of colored paint 32 from the transparent layer 30 of polypropylene in the areas where the anti-adhesive material (usually wax) of the layer 31 has been placed. In practice, by pulling the transparent layer 30 on which the security image 6 is reproduced (painted outer layer 36), the portions of intermediate layer of colored paint 32 which lie at the anti-adhesive material of the layer 31, remain glued to the deforming glue layer 33, while the other portions remain attached to the transparent layer 30. In this condition, the paint of the intermediate layer of colored paint 32 which remains attached to the deforming glue 33 and is detached from the transparent layer 30, clotting, as shown in Fig. 4D. In this way, even if the transparent layer 30 is perfectly repositioned on the deforming glue layer 30, for example because the label 1 has not been completely removed, the spaces in which the anti-adhesive layer 31 was deposited become like windows transparent through which the additional layer of colored paint is seen 34.

In the case shown in Figure 4C, the security image 6 of the label 1 viewed from the front takes on different appearance following the partial violation of the label 1. Fig. 4C represents a label 1 in which only the left side has been partially removed from the container 2. The left side of the label

1 in Fig. 4C reproduces the lines of the bar code of the security image 6 (external painted layer 36) and allows to see the background, i.e. the further layer of colored paint 34 through the torn portions of the middle layer of colored paint 32. The effect generated is the alteration of the security image 6, i.e. that the bar code is transformed into a grid of lines, no longer readable by a reader bar code. This solution therefore makes it possible to avoid the sale of forced goods. The right side of the label 1 of Fig. 4C is still not violated and perfectly glued to the container 2. In this case, the further layer of colored paint 34 cannot be visible because it is perfectly concealed by the intermediate layer of colored paint 32 still intact.

Alternatively, the first embodiment of the label 1 can assume a different arrangement of layers, as illustrated in Fig. 4B. The label 1 in addition to comprising the painted outer layer 36, reproducing the safety image 6, the transparent layer 30, the anti-adhesive layer 31 and the deforming glue layer 33, comprises an intermediate layer of double-colored paint 32, that is composed of a first intermediate layer of colored paint 32' and a second intermediate layer of colored paint 32''.

The first intermediate layer of colored paint 32' comprises a colored paint, preferably dark or red, uniformly and homogeneously arranged on the transparent layer 30 with the anti-adhesive layer sandwiched between the two. The second intermediate layer of 32'' colored paint instead includes a white paint arranged uniformly and homogeneously under the first intermediate layer of colored paint 32'. The second intermediate layer of colored paint 32'', white in color, makes it possible to uniform the color of the first intermediate layer of colored paint 32', making the chromatic differences of the container 2 irrelevant, which for example could have a colored pattern on the outer surface which would alter the security image 6 by itself. The container 2 may in fact have color differences or patterns which in itself could alter the perception of the security image 6 by the user or by the mobile device 7.

The second intermediate layer of colored paint 32'', used to uniform the background can be replaced by an intermediate layer of colored paint 32 of greater thickness or more opaque, that is not transparent, so as to eliminate the chromatic alterations created by the container 2. In the version of Fig. 4B, the label 1 comprises fewer layers, in particular of glue, with respect to the version of Fig. 4A, therefore it is more economical to produce.

In the version of Fig. 4B, the label 1 also comprises a white uniforming layer 39 between the painted outer layer 36 and the transparent layer 30. In this way, the safety image 6 is sharper and more visible when viewed from the front. This uniforming white layer 39 can also be introduced into the label of the version of Fig. 4A.

Both versions of the first embodiment of the label 1 of Fig. 4A and 4B can comprise an

identification element 22, for example a unique biometric trace. This additional guarantee label 1 allows you to univocally associate one or more labels 1 to a specific origin, for example to a specific product or merchant. This biometric material can be associated with a specific code that can be displayed using a special pen soaked in alcohol solvent and a reagent map including an alphanumeric scale, according to the known technique. For example, the biometric trace can be of the type called "ink crypt" of the company of the same name.

Fig. 4D shows the label 1 of Fig. 4C viewed from the side, during the partial removal of the label 1 from the container 2. In Fig. 4C it can be seen how a part of the intermediate layer of colored paint 32 remains glued to the deforming glue 33 and how it clumps together. The remaining part of an intermediate layer of colored paint 32 remains adherent to the transparent layer 30 which reproduces on its outer surface the safety image 6 (external painted layer 36). Thus openings are created within the intermediate layer of colored paint 32 joined to the transparent layer 30 through which the container 2 is seen, or any layers interposed between the deforming glue 32 and the container 2.

With reference to both versions of the first embodiment of Figs. 4A and 4B, through the openings that are created in the middle layer of colored paint 32 if the label 1 is violated, a background with a different color from that of the security image 6. The resulting effect is an alteration or a staining of the security image 6, which no longer appears to have the original appearance, ie the one equal to the reference image 5.

Figures 5 illustrates the first embodiment of the label 1 and in particular how the security image 6 alters if the label 1 is partially removed from the container 2. As illustrated in Figures 5A-5C or 6A-6C, if the label 1 is detached from the container 2, the upper part of the label 1 (identified by the reference 14), which we can identify with the painted outer layer 36, reproducing the security image 6, the transparent layer 30, the anti-adhesive layer 31, and part of the intermediate layer of colored paint 32, is detached from the lower part of the label 1 (identified by reference 15), which we can identify with the remaining part of the intermediate layer of colored paint 32 and with the layer of glue deforming. In Fig. 5A and 6A, the label 1 is not broken in and the security image 6 and the reference image 5 are the same. In these images, the reference image 5 is represented directly on the label 1 to facilitate understanding of the effect generated by the present invention, but nothing prevents the reference image from being represented on the container 2 or is it a pointer image, QR code type, which enables the reference image 5 to be retrieved remotely using appropriately structured electronic devices.

In Fig. 5B and 6B, the label 1 has been at least partially removed from the container 2 and the

lower part 15 of the label 1 remains glued to the container 2. In removing the label 1 from the container 2, the security image appearance 6' changes, since part of the paint of the intermediate layer of colored paint 32 remains glued to the lower part 15 of the label 1. Even by repositioning the upper part 14 of the label 1 perfectly in its original position, the security image 6 does not it will be more equal to the reference image and anyone can declare that the label 1 has been broken.

The portion of intermediate layer of colored paint 32 remaining on the lower part 15 of the label 1 detaching itself from the upper part 14 of the label itself is a function of the amount of anti-adhesive material 31 placed on the transparent layer 30. In Fig. 5B the layer anti-adhesive is disposed rather randomly, whereas in Fig. 6B, the anti-adhesive material 31 is arranged to represent a moon 18' inside a sun 18. The moon-shaped portion of an intermediate layer of colored paint 32 removed by the deforming glue 33 is now clotted 19 on the container 2. Alternatively, the intermediate layer of colored paint 32 detached from the deforming glue 32 can remain attached, in shreds, to the intermediate layer of colored paint 32 itself (non illustrated). It is also possible that the lower part 15 of the label 1 does not remain attached to the container 2, but that it also comes off the container 2 itself. In this case, the tenacity of the deforming glue 33 is such as to remove the portion of intermediate layer of colored paint 32 covered with an anti-adhesive material 31, but not able to remain perpetually attached to the container 2.

In Fig. 5C and 6C it is perceptible even to the naked eye as the security image 6 differs from the reference image 5, although the upper part 14 has been perfectly superimposed again on the lower part 15 of the label 1 itself.

In a second embodiment, shown in Fig. 7A-7C, the label 1 comprises one or more notches 20 preferably arranged on the periphery of the label 1. Said notches 20 cross at least in part the security image 6 so as to trigger break lines 20' of the label 1 at the security image 6, if the label 1 is removed at least in part from the container 2. The security image 6 is equal to the reference image 5 when the label 1 is attached entirely to the container 2, as shown in Fig. 7A. In this way, by trying to remove the label 1 from the container 2, the label 1 and the security image 6 tear or break along said notches 20, and even beyond, leaving a part of the safety image 6, as shown in Fig. 7B. The security image 6'', present at this point on the label 1, is carved or broken and therefore different from the reference image 5 and can be seen, both with the naked eye and through said mobile device 7 (in case of even minimal tears), the violation of the label 1. In particular, the notches 20 can be oriented radially with respect to the center of the security image 6. Even repositioning the label 1 in its original configuration, the security image 6 will no longer be

the same as the reference image 5.

Since the adhesives and adhesive layers generally lose their adhesiveness as the temperature increases, the label 1 in its various embodiments may comprise a portion of thermosensitive material 21 capable of modifying its appearance or color when the temperature exceeds one predetermined threshold, for example 60° C, as illustrated in Fig. 3. In this way, it is possible to ascertain whether someone has tried to remove the label 1 by dissolving the adhesive layer or the adhesive which held it together with the container 2.

Furthermore, the label 1 can include a unique identification system to certify in a certain and irrefutable way that the label is original and not counterfeit.

As shown in Fig. 3, said identification system can comprise at least one of the following identification elements 22:

- a nano ink sensitive to the detection of UV light with a unique colorimetric trace ;
- an ink comprising a unique biological trace ; or
- a magnetic ink with a unique magnetic trace.

The above inks or paints all include a unique element, that is unique compared to the other inks available. This means that, by applying a drop of said ink on the label, this is uniquely attributable to a single origin or to a single subject. For example, if company X corresponds to the univocal trace Y, all the labels 1 of company X will include a quantity of trace Y so that it is impossible to forge the label for the one who does not have the trace Y. Such trace Y can be of the colorimetric, biological or magnetic type and is dispersed in an ink or a paint to facilitate its application on the label 1. Said ink with a unique trace can be applied in any element of the label 1, preferably to the element attached to the container 2.

Optionally, as shown in Fig. 3, the label 1 can furthermore comprise an RFID system 23 to facilitate the electronic tracking of the label 1 itself.

A second object of the present invention is a method for verifying whether a container has been opened by violating the label which keeps it closed. In particular, said method is suitable for verifying the break-in of a container 2 which comprises an internal space 3 and at least one closing element 4 of the space 3.

As shown in Fig. 10, said method comprises the step of attaching (step A) a label 1 to the container 2 and to the at least one closure element 4. Said label 1 comprising a security image 6 configured to change appearance with respect to a reference image 5 if the label 1 is removed at least in part from the container 2 and / or from the at least one closing element 4. The label has the technical characteristics described previously suitable for varying the appearance of the image. safety device

6 with respect to the reference image 5 if the label 1 is also only partially detached from the container 2.

Said method further comprises a second and following phase B which provides for comparing the safety image 6 of the label 1 with the reference image 5, which can be affixed to the label 1 itself or to the container 2.

Said method also comprises a third and following phase C which provides for attesting the violation of the label 1 and therefore the potential opening of the container 2 if as a result of said comparison B, the security image 6 is different from the reference image 5 .

The method may further comprise the optional step of recovering the reference image 5 remotely. In this case, the reference image affixed to the label 1, or to the container 2, is an image pointing to a remote database where the reference image 5 is contained. The said intermediate phase comprises the steps of acquisition (phase D), by means of the camera 8 of a mobile device 7, a portion of the label 1 comprising said pointer, which may preferably be a QR code 11. Said image pointer, or QR code 11, is configured so as to address the mobile device 7 to a position within the database 9 in which the reference image 5 is located.

Once the mobile device 7 finds the reference image 5 in the database 9, the image is retrieved (step E) from the database 9 by means of the mobile device 7 for the subsequent comparison step B.

Said comparison step B can comprise two sub-phases. The first sub-phase F envisages acquiring by a camera 8 of the mobile device 7 the security image 6. The second sub-phase G provides to execute a program installed in a memory 13 of the mobile device 7 to compare the security image 6 acquired at phase F, with the reference image 5 recovered at stage G.

Finally, this label is suitable for a combined use with a blockchain digital register. As is known, the blockchain is a shared and immutable data structure, designed to manage the transfer of values and assets. A blockchain is in practice a digital archive of all transactions or passages suffered by a specific physical asset, such as a house, a medical record, a paper document, or a digital asset, such as a cryptocurrency.

In this digital archive all the steps of the asset are recorded and these cannot be changed, avoiding the possibility of fraudulent actions. In other words, it is a data structure that can be defined as a digital register divided into blocks concatenated in chronological order and regulated by a shared protocol. Once entered in the blockchain, the records are permanent, unalterable and transparent for anyone who accesses them. As already described, the label according to the present invention allows to guarantee the demonstrability of its removal from a physical object, therefore a given

label can be associated with certainty with certainty to a specific physical object, for example a product, a contract, a paper document , a medical record, etc. If a specific label is therefore associated with a specific blockchain register, said label becomes a physical correspondent that guarantees the digital transaction recorded via blockchain.

To the specific digital transaction registered via blockchain it is sufficient to indicate a unique identification code associated with the label. Each label can therefore include a progressive and unique identification code that can be indicated in the transaction recorded in blockchain. For clarity, for example, if a purchase transaction of a very rare and very expensive bottle of wine is concluded on the web and this transaction is recorded through a blockchain register, associating the identification code of the label applied to the said bottle with the aforementioned digital purchase contract in blockchain, the buyer will be certain that the bottle that will be delivered corresponds exactly to the one purchased. The purchaser of the bottle is therefore certain, before concluding the purchase contract, and paying the good, that this good will really be what will be delivered to him.

In this way, the security of a smart contract in blockchain can be paralleled, with maximum security, to a label in accordance with the present invention, so as to associate a physical asset with a digital transaction.

In conclusion, it is clear that the invention thus conceived is susceptible of numerous modifications or variations, all of which are included in the invention; furthermore all the details may be replaced by technically equivalent elements. In practice, the quantities can be varied according to technical requirements.

CLAIMS

1. Anti break-in system for a container (2) having an inner compartment (3) and at least one closure element (4) of the compartment (3), comprising:

- a label (1) attachable to the container (2) crossing the at least one closure element (4);
- a reference image (5);

wherein said label (1) comprises a univocal security image (6) equal to said reference image (5) and means configured to change the aspect of said security image (6) with respect to the reference image (5) when the label (1) is at least in part removed from the container (2) and/or from the at least one closure element (4).

2. Anti break-in system according to claim 1, wherein said reference image (5) is reproduced on a portion of the label (1), preferably beside the security image (6).

3. Anti break-in system according to claim 1, wherein said reference image (5) is reproduced on the container (2).

4. Anti break-in system according to any of the preceding claims, wherein said label (1) comprises a pointer image to a database (9) wherein the reference image (5) is contained, preferably said pointer image is a QR code (11).

5. Anti break-in system according to claim 4, wherein said system comprises said database (9) and a mobile device (7), said mobile device (7) being configured to download from a database (9) the reference image (5) via the pointer image, preferably said pointer image is read through a camera (8) of the mobile device (7).

6. Anti break-in system according to claim 5, wherein said mobile device (7) is configured to also acquire through the said camera (8) said security image (6), said mobile device (7) also comprises a processing unit (12) adapted to execute a program installed in a memory (13) of the mobile device (7), when said program is executed it is configured to verify the matching of said security image (6) with said reference image (5) downloaded from the database (9) and to generate a signal characteristic of the label status.

7. Anti break-in system according to claim 6, wherein said mobile device (7) comprises a display (10) adapted to display said signal related to the status of the label (1) for informing a user of the eventual violation of the label (1).

8. Anti break-in system according to claim 7, wherein said pointer image is a QR code (11) and said program comprises a function for reading the QR code (11) through the camera (8) and decoding the QR code for obtaining the position of reference image (5) in the database (9).

9. Anti break-in system according any of preceding claims, wherein the label (1) comprises:

- a layer of transparent material (30);
- a painted external layer (36) reproducing the security image (6) and laid directly or indirectly on the transparent layer (30);
- an intermediate layer of colored paint (32);
- an anti-adhesive material (31) interposed between the transparent layer (30) and the intermediate layer of colored paint (32);
- a layer of deforming glue (33) joined to the side of the intermediate layer of colored paint (32) opposed to its side facing the transparent layer (30).

10. Anti break-in system according to previous claim, wherein the label (1) also comprises:

- a further layer of colored paint (34) arranged under the layer of deforming glue (33), preferably having a shade of color contrasted, from the point of view of color, to the shade of color of the intermediate layer of colored paint (32);
- a layer of not-deforming glue (35).

11. Anti break-in system according to any of claims 1 to 9, wherein intermediate layer of colored paint (32) comprises:

- a first intermediate layer of colored paint (32');
 - a second intermediate layer of colored paint (32'') arranged on the side of the first intermediate layer of colored paint (32') opposed to the side facing the transparent layer (30);
- wherein said second intermediate layer of colored paint (32'') consisting of a uniform and homogeneous layer of white paint.

12. Anti break-in system according to any of the preceding claims, wherein the label (1) also

comprises a levelling white layer (39) arranged between the painted external layer (36) and the transparent layer (30).

13. Anti break-in system according to any of claims 1 to 8, wherein the label (1) comprises one or more incisions (20) configured to at least partially break the portion of label (1) on which is reproduced the security image (6), modifying the security image (6) with respect to the reference image (5), when the label (1) is removed at least partially from the container (2).

14. Anti break-in system according to any of the preceding claims, wherein said label (1) comprises a thermosensitive material (21) configured to modify its aspect or color if the temperature exceeds 60°C.

15. Anti break-in system according to any of the preceding claims, wherein said label (1) comprises at least one of the following identification elements (22):

- a nanoink sensible to the UV light with a unique colorimetric trace;
- an ink comprising a unique biologic trace; or
- a magnetic ink having a unique magnetic trace.

16. Anti break-in system according to any of the preceding claims, wherein said label (1) comprises a RFID system (23) for electronically tracking the label (1).

17. Method for verifying the violation of a container (2) comprising a compartment (3) and at least one closure element (4) of the compartment (3), comprising the steps of:

A- attaching the label (1) to the container (2) crossing said at least one closure element (4), said label (1) comprising a univocal security image (6) equal to said reference image (5) and means configured to change the aspect of said security image (6) with respect to the reference image (5) when the label (1) is at least in part removed from the container (2) and/or from the at least one closure element (4).

B- comparing said security image (6) of the label (1) with the reference image (5) placed on the label (1) or on the container (2);

C- assessing the opening of the container (2) if said security image (6) is different from said reference image (5) following the comparison step.

18. Method for verifying the violation of a container (2) according to claim 17, wherein said reference image (5) is a pointer image to a database (9), preferably a QR code (11), and wherein said method comprises, between the step A and the step B, the further steps of:

D- acquiring through the camera (8) of the mobile device (7) a portion of the label (1) comprising said pointer image configured to direct the mobile device (7) toward a position on the database (9) wherein the reference image (5) is stored;

E- downloading from the database (9) the reference image (5) through said mobile device (7).

19. Method for verifying the violation of a container (2) according to claim 18, wherein said comparison step comprises the sub-steps of:

F- acquiring through the camera (8) of the mobile device (7) said security image (6);

G- executing a program installed on a memory (13) of the mobile device (7) for comparing the acquired security image (6) with the downloaded reference image (5).

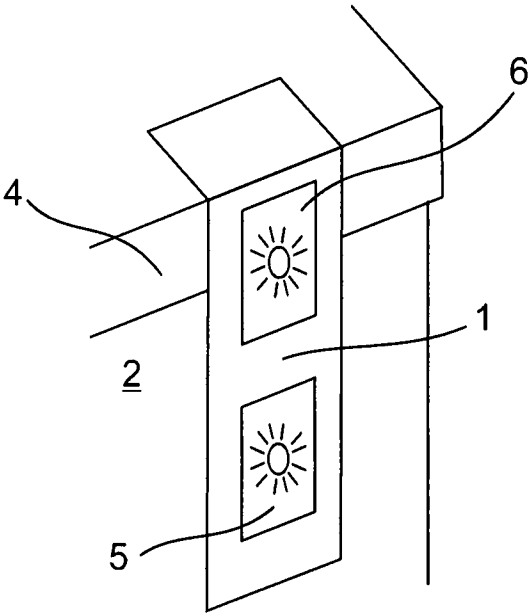


Fig.1A

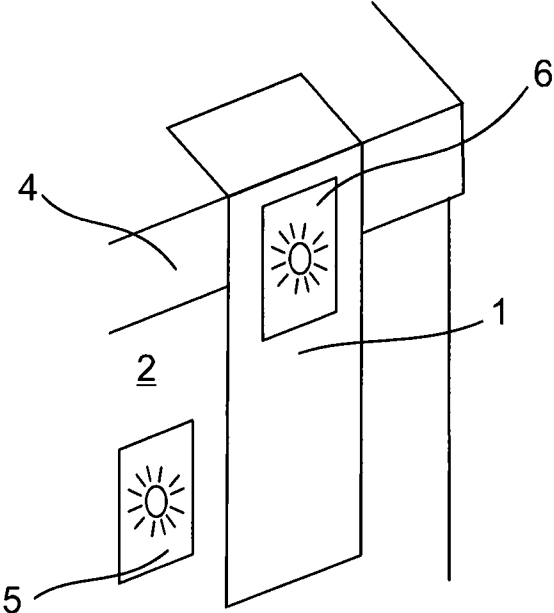


Fig.1B

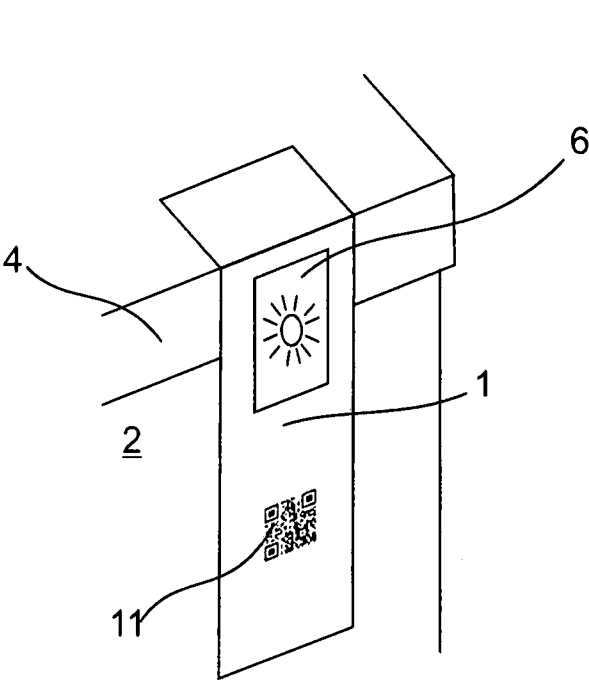


Fig.1C

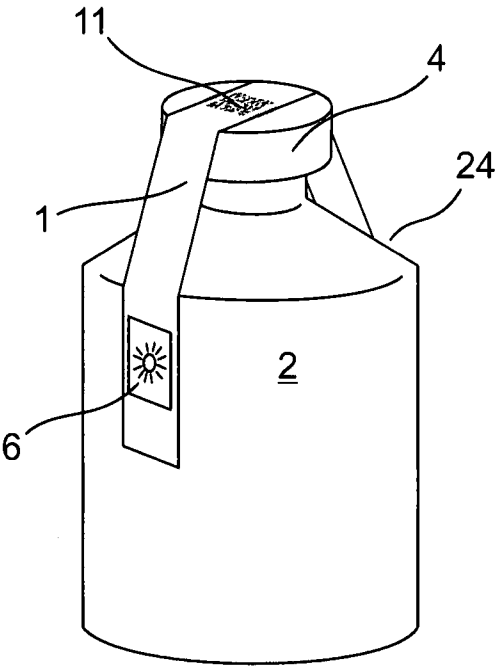


Fig.1D

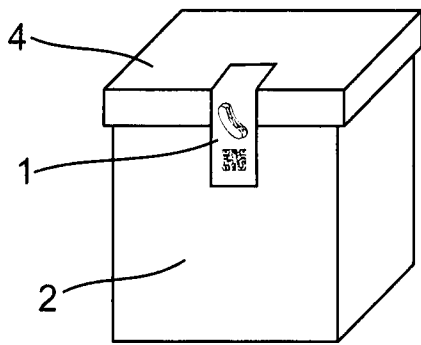


Fig.2A

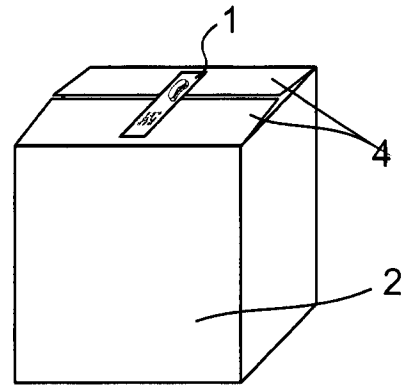


Fig.2B

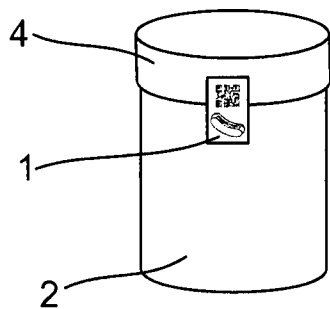


Fig.2C

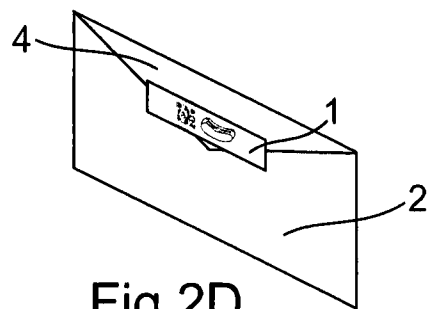


Fig.2D

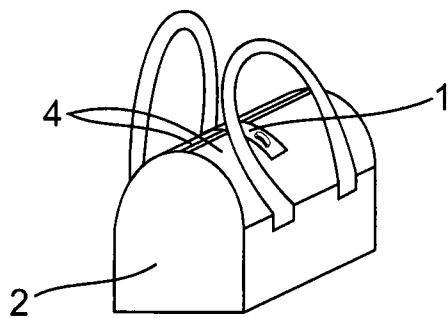


Fig.2E

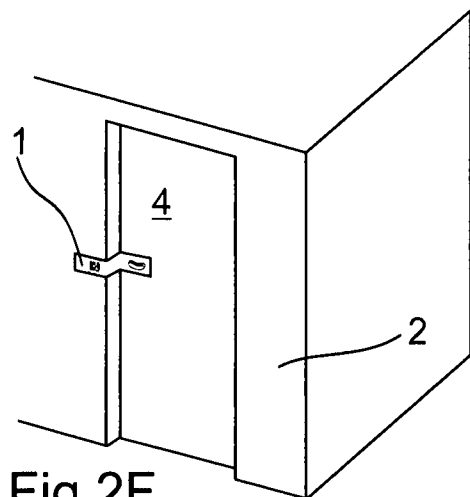
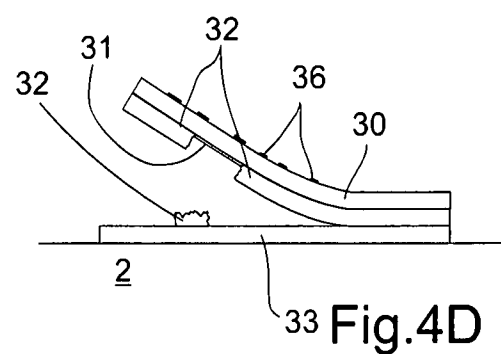
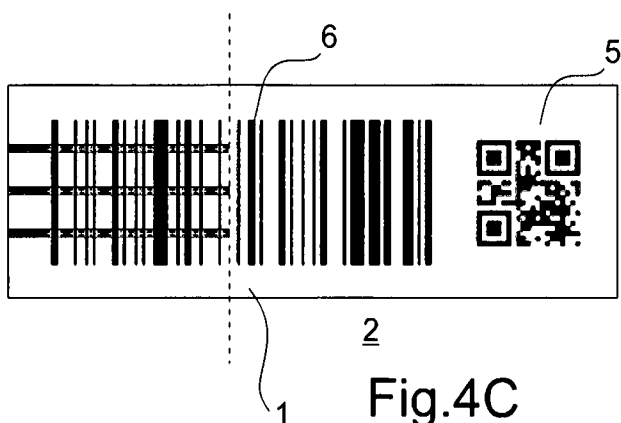
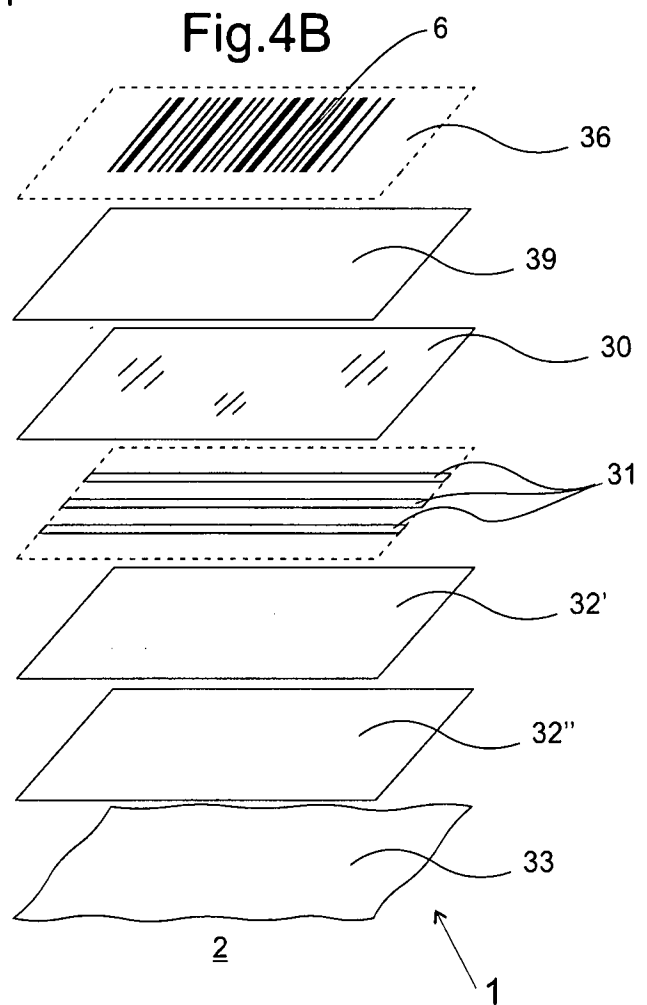
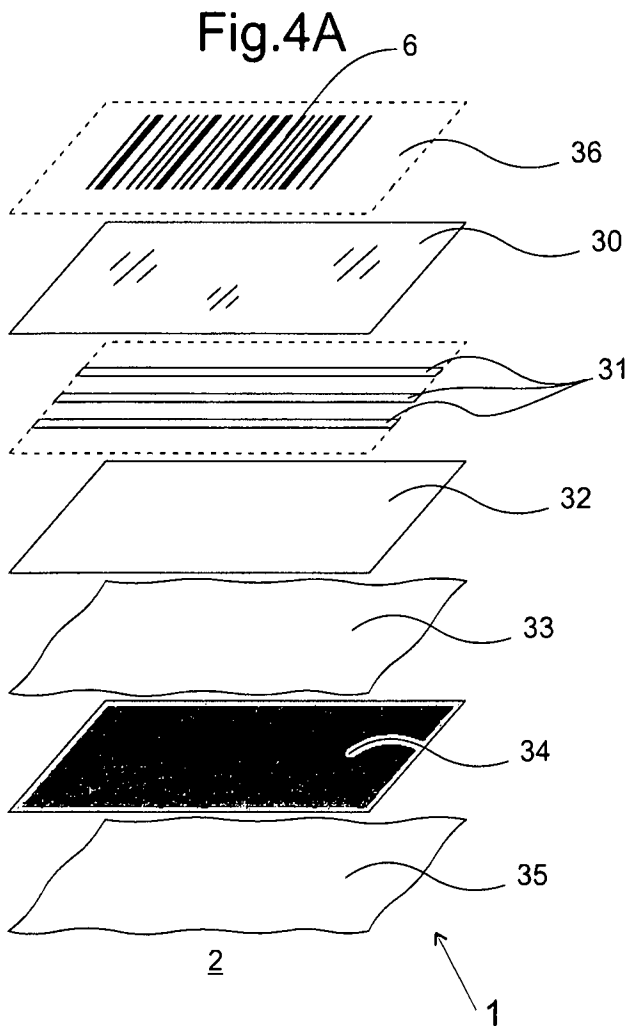
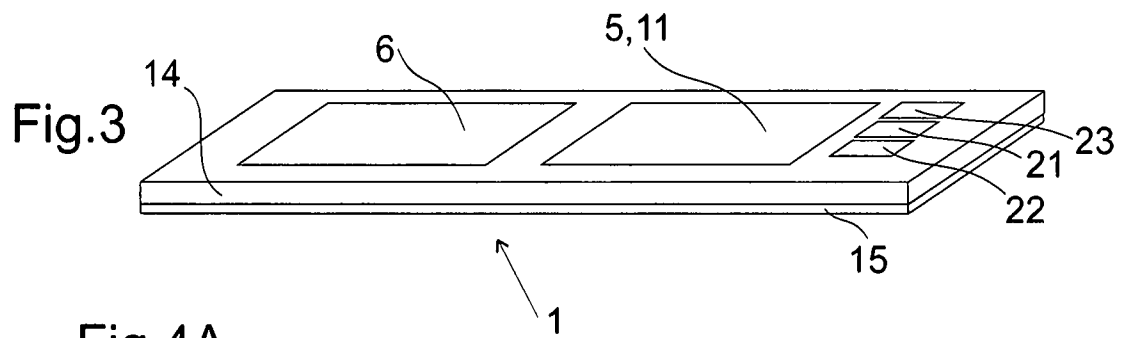


Fig.2F



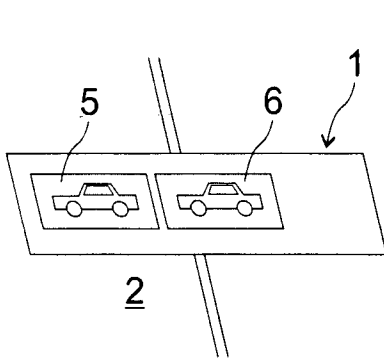


Fig. 5A

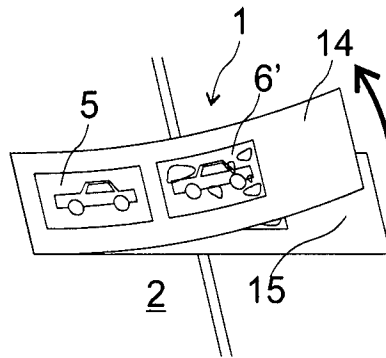


Fig. 5B

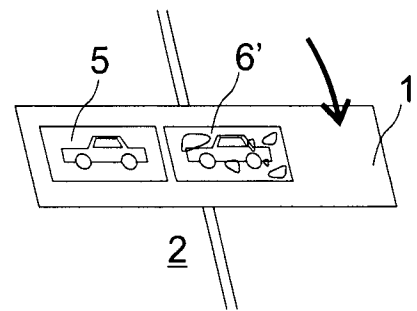


Fig. 5C

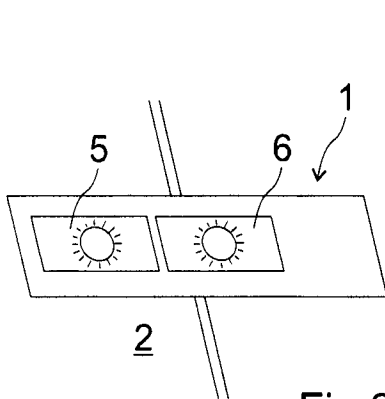


Fig. 6A

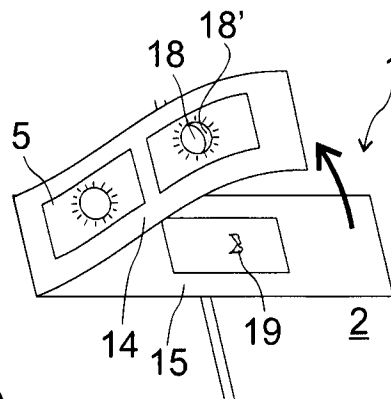


Fig. 6B

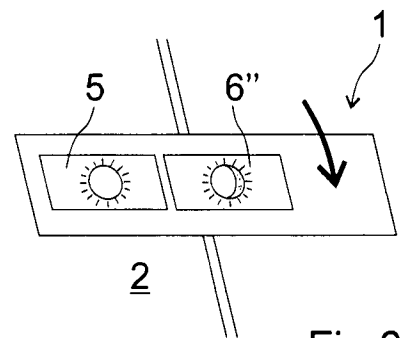


Fig. 6C

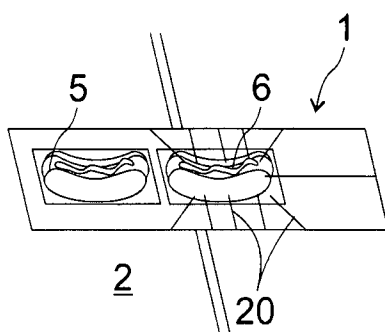


Fig. 7A

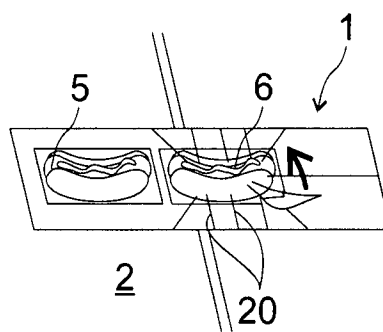


Fig. 7B

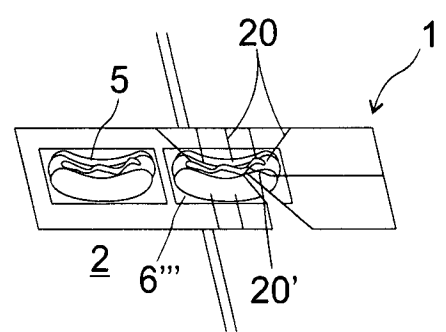


Fig. 7C

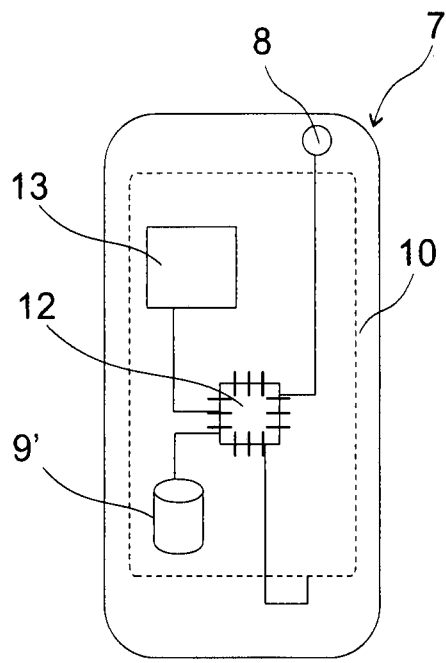
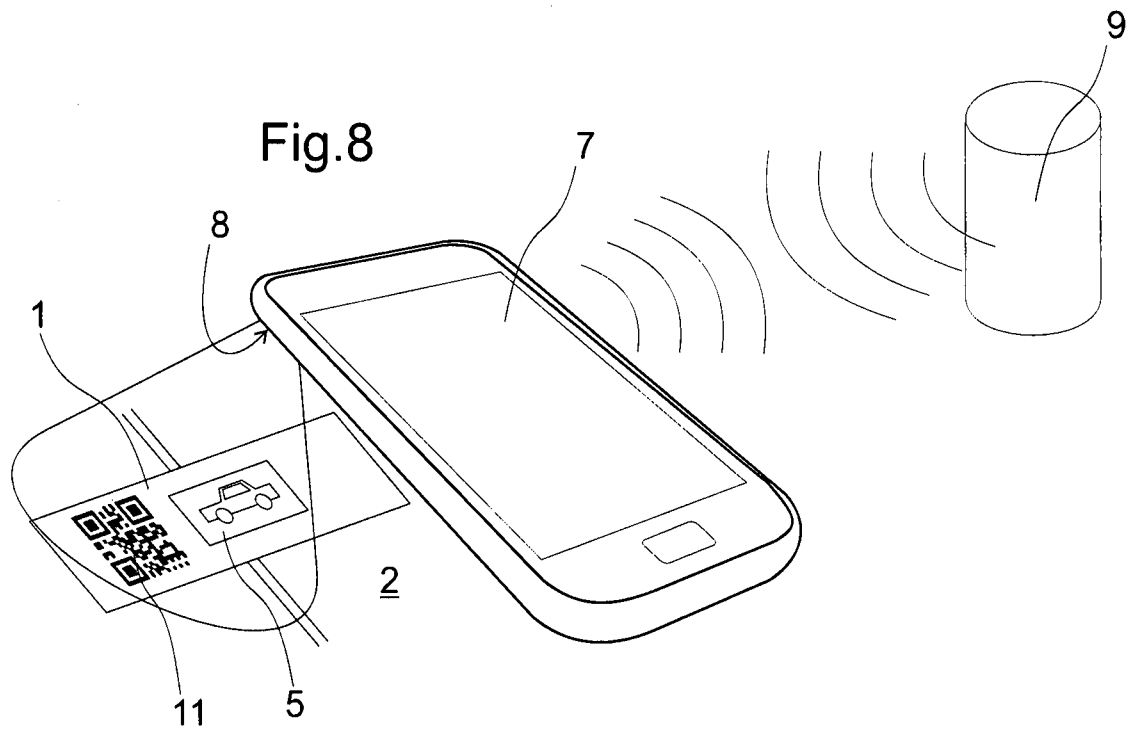


Fig.9

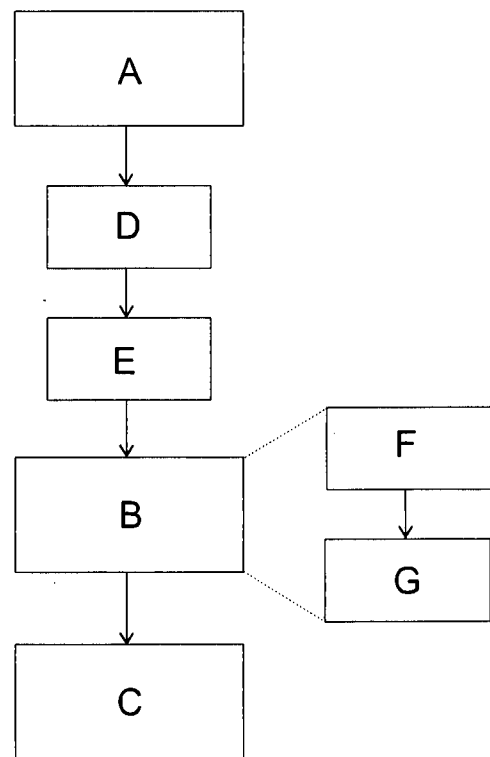


Fig.10

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2019/000627

A. CLASSIFICATION OF SUBJECT MATTER
INV. G09F3/00 G09F3/03
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)
G09F 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)

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	WO 2010/050928 A1 (LO ALLEN K [CN]) 6 May 2010 (2010-05-06)	1-8, 17-19
Y	paragraph [0001] paragraph [0020] - paragraph [0023] figures 1-10	13, 16
X	EP 2 717 243 A2 (TESA SE [DE]) 9 April 2014 (2014-04-09)	1-3, 9-12, 14, 15
	paragraph [0032] - paragraph [0035] paragraph [0042] - paragraph [0054] figures 1-3d paragraph [0001]	
	----- -/--	



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

7 November 2019

Date of mailing of the international search report

27/11/2019

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

Pantoja Conde, Ana

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2019/000627

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 2016/103129 A1 (PALLADIO ZANNINI IND GRAFICHE CARTOTECNICHE S P A [IT]; ITALNASTRI S P) 30 June 2016 (2016-06-30) page 1, line 1 - line 7 page 9, line 15 - page 11, line 21 page 12, line 15 - page 14, line 16 figures 1-6 -----	1-3
X	EP 3 038 075 A2 (UPM RAFLATAC OY [FI]) 29 June 2016 (2016-06-29) paragraph [0041] - paragraph [0056] figures 1-7b -----	1-3
Y	WO 2016/071172 A1 (TESA SCRIBOS GMBH [DE]) 12 May 2016 (2016-05-12) page 8, line 1 - page 10, line 12 figures 1-12 -----	13
Y	US 2016/027021 A1 (KERDEMELEIDIS ANDREW [GB]) 28 January 2016 (2016-01-28) paragraph [0089] - paragraph [0090] figure 4 -----	16
A	FR 2 976 845 A1 (ADVANCED TRACK & TRACE [FR]) 28 December 2012 (2012-12-28) the whole document -----	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2019/000627

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010050928 A1	06-05-2010	CN 102265658 A WO 2010050928 A1	30-11-2011 06-05-2010
EP 2717243 A2	09-04-2014	DE 102012218033 A1 EP 2717243 A2	03-04-2014 09-04-2014
WO 2016103129 A1	30-06-2016	EP 3238202 A1 WO 2016103129 A1	01-11-2017 30-06-2016
EP 3038075 A2	29-06-2016	EP 3038075 A2 US 2016180747 A1	29-06-2016 23-06-2016
WO 2016071172 A1	12-05-2016	DE 102014222807 A1 WO 2016071172 A1	12-05-2016 12-05-2016
US 2016027021 A1	28-01-2016	NONE	
FR 2976845 A1	28-12-2012	NONE	