

OPTICAL AUTHENTICATION METHOD

Technical field

5 The field of the invention is that of combating infringement and methods of identifying objects by means of identifiers applied to the objects.

Prior art

10 Such an authentication method is known from patent Document W02006/042913.

That authentication method provides a solution for authenticating objects by (1) forming an image of a mark made on each object that is to be identified, specifically a bubble identifier, (2) calculating a digital key for the image, and (3) comparing the digital key of the image with digital keys stored in advance in a remote database and derived from digital images made under predefined conditions in a manufacturing line for producing objects that are to be identified.

20 The characteristics of a digital image of an object depend naturally on the conditions under which the image is taken, such as the type of optical system used for making the image, and also its distance and angular position relative to the object. A digital key derived from the image depends strongly on these parameters, and ends up characterizing as much the conditions under which the image itself was taken as the object shown in the image. Consequently, making use of digital keys for two different images of the same object in order to identify said object remains a major challenge.

30 Ideally, an optical authentication system must make it possible to derive a digital key that is unique and invariant from two different images of the same identifier, and for this to apply in spite of differences and unknowns concerning the conditions under which the two images were taken and also concerning the equipment

used. This applies in particular when an image is formed by an end user, having no special equipment or training.

Patent Documents EP 2 849 118, US 2006/0268259, EP 1 475 242, and EP 1 873 616 disclose methods involving
5 analyzing images of an identifier that comprises elements that form patterns on which the authentication of a product relies, however those methods are complicated and/or based on identifiers that are sophisticated.

10 Summary of the invention

An object of the invention is to remedy those drawbacks.

An optical identification method of the invention relies on using an identifier of structure that is
15 extremely simple to apply on the object that is to be identified, the identifier comprising same-diameter microbeads distributed in a random pattern on a surface of the object that is to be authenticated.

In particular, the authentication method of the
20 invention for authenticating objects uses an identifier that is applied to each object and it comprises the following steps:

- applying the identifier on an object that is to be authenticated;
- 25 · making a first digital image of the identifier applied to the object;
- deriving a first digital key from the first digital image;
- storing the first digital key in a database
30 containing a plurality of first digital keys;
- subsequently, making a second digital image of the identifier applied to the object;
- deriving a second digital key from the second image; and
- 35 · comparing the second digital key with the first digital keys stored in the database in order to detect a

match, and in response to detecting a match, identifying the object as being authentic;

wherein, for the identifier that is applied to an object, use is made of same-diameter microbeads

5 distributed in a random manner on the surface of the object, the microbeads being embedded in a layer of binder sprayed onto the surface of the object; and wherein the derivation of the first digital key from the first image comprises the following steps:

10 · applying an elliptical regression to a distribution of points, each situated at the location of a respective one of the microbeads in the first image, in order to define an ellipse; and

 · applying a change of reference frame consisting in
15 expressing the coordinates of each point of the distribution in a reference frame based on the ellipse.

An advantage of the method of the invention lies in the fact that regardless of the angle and the distance from which the picture is taken, the microbeads are seen
20 as disks or as circles. It is thus easy to identify them in a digital image of the identifier and to determine the pattern that they form. Furthermore, since the microbeads have the same diameter, it is possible, by using their apparent diameters in the image, to perform
25 relatively simple digital processing for the purpose of describing their distribution independently of their coordinates in a reference frame associated with the image by establishing a reference frame that is specific to the pattern formed by the microbeads. In other words,
30 the pattern formed by the microbeads may be characterized independently of the conditions under which the picture was taken.

Such an authentication method of the invention is sufficiently robust to identify reliably the authenticity
35 of an object having an identifier applied thereon, and this can be done by an end user without any special

knowledge and without any equipment dedicated for this purpose.

Unlike other techniques, this identification method does not require association with a predetermined
5 identification code that is associated with an authentication mark. The identifier of the invention can be sufficient in itself, which provides great flexibility in use and simplifies the entire application process, from application the identifier and management of the
10 identification service by a provider to use by an end user.

Furthermore, this method lends itself well to mass production and use of objects. It is easy to adapt the method to a variety of applications, e.g. merely by
15 acting on the size of the identifier itself and/or on the diameter and the number of microbeads.

The authentication method of the invention may also present the following features:

- the derivation of the second digital key from the
20 second image may comprise the steps of:
 - applying an attitude correction step to a distribution of points, each situated at the location of a respective one of the microbeads in the second image, so as to reconstitute an image of the identifier as seen
25 looking along a direction perpendicular to the surface on which the identifier is formed;
 - applying an elliptical regression to the distribution of points, each corresponding to a respective one of the microbeads in the second image that
30 has been subjected to the attitude correction, in order to define an ellipse; and
 - applying a change of reference frame consisting in expressing the coordinates of each point of the distribution in a reference frame based on the
35 ellipse;

- the method may include a step of normalizing the coordinates of the points of the distribution in the reference frame based on the ellipse by multiplying by a scale factor equal to the ratio of the real diameter of the microbeads divided by the mean diameter of the microbeads as seen in the image;
- a circular regression may be applied to the images of the microbeads visible in the first digital image and/or the second digital image;
- use may be made both of microbeads of a first brightness and/or of a first hue and also of microbeads of a second brightness and/or of a second hue that are respectively different from the first brightness and/or the first hue, so that at least some of the microbeads present sufficient visual contrast with the surface of the object for them to be identified automatically from the digital images;
- the binder may be sprayed onto the surface of the object so as to be inscribed in a circle of diameter less than or equal to 15 millimeters (mm);
- the binder may be sprayed onto the surface of the object so as to be inscribed in an ellipse of eccentricity greater than or equal to 1.5 and of major axis less than or equal to 15 mm;
- it is possible to use authentication mark that comprises 10 to 100 microbeads, each having a diameter lying in the range 20 micrometers (μm) to 150 μm ;
- the second image may be made using a smartphone having a camera and a data processor unit, and the second digital key may be derived from the second digital image by means of said data processor unit of the smartphone and/or by means of a remote data processor unit.

Brief summary of the drawings

- The present invention can be better understood and other advantages appear on reading the following detailed

description of an implementation made by way of non-limiting example and illustrated by the accompanying drawings, in which:

- Figures 1A and 1B show respective plan views of an identifier of the invention;
- Figure 1C shows a section view of the Figure 1A identifier;
- Figure 1D shows a line for marking objects that are to be authenticated by using the identifier of Figure 1A or 1B;
- Figure 2A shows an authentication method using the authentication mark of Figure 1A or 1B;
- Figure 2B shows a digital image being made of the identifier of Figure 1A or 1B;
- Figure 3 shows digital processing of an image representing the identifier of Figure 1A or 1B;
- Figures 4A to 4D show steps in the digital processing of Figure 3.

Description of an implementation of the invention

An authentication method of the invention is shown in Figures 2A and 2B.

The first step E10 consists in providing an object that is to be authenticated, e.g. in a stage of producing objects such as wine bottles or identification labels. During the step E20, an identifier 100 is applied to the surface of the object. It should be observed that since the identifier is itself to be used for generating a digital identification key, there is no need to provide an identification code that is associated with the identifier. After the identifier has been applied, a first digital image of the identifier is made during a step E30, and then a first digital key is derived from the first image during a step E35. This key is stored in a database 240 storing a plurality of first digital keys during a step E38.

Subsequently, the object is transferred to a user in a step E40. The user performs a portion of the authentication method by making a second digital image of the identifier during a step E50 by means of a picture-taking device. The picture-taking device may be a smartphone 200 having a camera 210 and a data processor unit 220.

A second digital key is derived from the second image during a step E55. By way of example, the necessary calculation operations may be performed by the data processor unit 220 of the smartphone 200.

During a step E60, the second digital key is compared with one or more first digital keys of the database 240 in order to detect a match.

While performing the steps E50, E55, and E60, the user may be remote from the database and, for comparison purposes, the smartphone 200 may send the second digital key to the database via a data exchange network ED, such as the Internet, for example. Alternatively, the second digital image may be sent as such to the database 240 and/or may be processed digitally by a remote data processor unit 260 connected to the database 240 in order to derive the second digital key. Another alternative is to perform pre-processing of the image at the user end by means of the data processor unit 220 of the smartphone, e.g. consisting in cleaning the image by eliminating noise, converting it to black and white, adjusting contrast, or indeed compressing it, and then sending the pre-processed image to the remote data processor unit 260 in order to finish off the operation of generating the second digital key and in order to compare it with one or more first digital keys in the database 240.

In response to detecting a match in the database, the object is identified as being an authentic object and an authenticity confirmation message can be sent to the smartphone 200.

The identifier, its application on objects to be authenticated, and the making of the first digital image are shown in Figures 1A to 1D.

5 An identifier 100 has a layer 110 of binder applied to a surface 130 of an object 135 that is to be authenticated. The layer 110 includes same-diameter microbeads 120 distributed in random manner over the surface 130.

10 It should be observed that the term "same-diameter" should be assessed with reference to the intended application and the associated specifications. The important point is that the diameter and the sphericity of the microbeads are sufficiently uniform for it to be possible to perform the method of determining the digital
15 keys. It is possible to use microbeads from the manufacturer Cospheric, e.g. spheres of poly(methyl methacrylate), or "PMMA", guaranteed to have 90% of their diameters in the range 45 μm to 47 μm and sphericity of greater than 99%.

20 A layer 110 of binder, as shown in Figure 1A, may form a disk. Preferably, the layer of binder has a shape that is elongate, such as an ellipse, as illustrated by the layer 110' of the identifier 100' shown in Figure 1B. An elongate shape for the layer 110 greatly enhances the
25 robustness of the identification method by making it easier to determine a reference frame that is specific to the image formed by the microbeads, and thus easier to determine digital keys.

30 As shown in Figure 1D, an object 135 that is to be authenticated by the identifier 100 or the identifier 100' is marked by spraying onto the surface 130 of the object 135 that is to be authenticated one or more drops 140 of a hardenable liquid binder 185, such as a polymerizable liquid that contains microbeads 120.

35 Marking is performed in a marking line 138 in which a plurality of objects 135 that are to be authenticated

travel along the line 138 in the direction D, and are marked in succession.

The hardenable binder 185 is sprayed by a spray system 155 making use of an ejector system 160 having a nozzle 170 and connected to a tank 180 containing the hardenable binder 185 that has the microbeads 126 mixed therein.

The drop(s) 140 spread(s) on the surface 130 of the object 135 that is to be authenticated, and form(s) a liquid thin film 112 in which the microbeads 120 are distributed in a random pattern.

When the hardenable binder is a polymerizable liquid, the marking is finished off by hardening the liquid thin film 112 by means of a polymerizer 180, thereby forming the layer 110 of binder and permanently setting a distribution of microbeads 120 in a distribution that is unique and that cannot be predicted.

By using a nozzle that is asymmetrical or by moving the nozzle relative to the object that is to be authenticated during spraying, it is possible to impart an elongate shape the layer 110.

A particular, but nonlimiting example is that of using a photopolymer as the hardenable binder 185. The polymerizer 180 is then a source of light, preferably of ultraviolet light.

The hardenable binder 185 may also be a paint or a varnish, and the polymerizer 180 may be a source of heat or of infrared radiation. It is preferable for the binder to have a hardening time that is short, so as to avoid slowing down the production line or complicating the method.

As shown in Figure 1D, the marking line 158 includes a picture-taking appliance 190 for making a first image of the physical signature (100) on exiting the line.

Making a layer of binder that is elongate, as shown in Figure 1B (110B), can contribute to facilitating the

creation of a reference frame specific to the identifier, in a manner that is described in detail below.

The microbeads may be microbeads that are transparent or opaque, colored, or colorless, the essential point being to maintain good visual contrast relative to the surface of the object on which the microbeads are deposited. The term "good visual contrast" is used to mean that presently-available automatic digital image processor means are capable of identifying the microbeads as disks or circles in the digital images of the identifier.

In order to counter problems of visual contrast, it is also possible to make use of brightnesses and/or hues that are different from one another. For example, with a surface that presents a black-and-white pattern, using both white microbeads and black microbeads in combination makes it possible to guarantee that at least some of the microbeads remain clearly visible. In other words, at least some of the microbeads present good visual contrast relative to the surface of the object on which they are dispersed.

The microbeads may present a diameter such that presently-available picture-taking appliances are capable of imaging the microbeads with sufficient resolution, in other words of imaging them in the form of disks or circles. In the invention, appropriate microbead diameters may lie in the range of 20 μm to 150 μm .

The layer of binder may be designed to be inscribed in a circle having a diameter of 15 mm, preferably in a disk having a diameter of 10 mm, and more preferably in a disk having a diameter of 7 mm. Alternatively, the layer of binder may be inscribed in an ellipse having eccentricity greater than or equal to 1.5, with a major axis less than or equal to 15 mm, preferably 10 mm, and more preferably 7 mm. The layer of binder may also be transparent. These characteristics, singly or in

combination, have the advantage of leading to marking that is discreet and that does not significantly degrade the external appearance of the object that is to be authenticated.

5 The number and the size of the microbeads 120 may be optimized as a function of the size of the layer 110 in which they are included, for the purposes (1) of enabling the possible number of configurations to be sufficient so that in practice each distribution of microbeads in an
10 identifier is unique, and (2) of keeping the probability of obtaining clusters (bunches of microbeads in contact one another) below a limit that is acceptable given the constraints of the intended application. For binder layers 110 extending over a straight line segment having
15 a length greater than 3 mm and inscribed in a circle having a diameter of 15 mm, it is considered as being acceptable for authentication mark to have a number of microbeads lying in the range 10 to 100, preferably 20 to 100, the microbeads being of diameter lying in the range
20 20 μm to 150 μm , and preferably in the range 30 μm to 70 μm . The probability of finding one or more clusters in the layer 110 is preferably kept below 10%, and more preferably below 5%. The mean number of microbeads in an identifier can be adjusted by acting on the density of
25 microbeads 120 present in the polymerizable liquid 185.

 Digital processing 300 suitable for application to the first image and/or the second image is shown in Figures 3 and 4A to 4D. This digital processing 300, which terminates by generating a digital key, has the
30 purpose of obtaining digital keys that are identical from different images of the same identifier.

 After a digital image of the identifier 100 has been formed in a step E310, circular patterns 410 (circles or disks) are identified in the image during a step E320.
35 These circular patterns correspond to the microbeads 120 of the identifier 100, and they are visible as circular

shapes regardless of the distance or the angle from which the picture is taken, thus making them easily identifiable.

Alternatively, and in preference to detecting
5 circular patterns in the digital image, it is assumed that the contrast spots visible in the image correspond to circles or to disks, thereby considerably simplifying the identification step E328. This assumption is increasingly realistic when the acceptable quantity of
10 microbeads clusters is small. The advantage of this approach is to eliminate any need to search for circular shapes in the image, thereby greatly limiting the burden of calculation. Thus, each visible contrast spot, like each circular pattern, may correspond to one of the
15 microbeads.

In order to be unaffected by pixelization effects, it is possible, during a step E330, to apply a circular regression to each of the circular patterns identified during the step E320. It is then possible to replace the
20 originally-identified circular patterns 210 or contrast spots with calculated circular patterns 420. Applying this circular regression facilitates subsequent calculations and considerably improves their accuracy, in particular during an attitude correction step E350.

25 The diameters and/or the positions of the centers of the circular patterns or of the contrast spots, or of the calculated circular patterns, are determined during a step E340 and they may be expressed in a reference frame specific to the digital image. The positions of the
30 centers correspond to points forming a distribution 430 of points. Generation of the digital key is based on this distribution 430 of points, each of which is situated at the center of the image of one of the microbeads in the digital image of the identifier. It
35 should be observed that methods other than that described above can be applied, so long as a distribution is

determined of points that are distributed in the same manner as the images of the microbeads, and preferably at their centers.

The digital processing may include an attitude
 5 correction step E350 for correcting the effects that the orientation of the picture-taking appliance can have on the digital image. This correction, which serves to reconstitute an image of the identifier as seen looking
 10 along a direction perpendicular to the surface on which it is formed, is made possible by knowing the real diameter of the microbeads. This step can be useful for correcting a digital image of the identifier that has been acquired while looking along a direction that
 15 departs from the perpendicular to the surface on which the identifier is formed by an amount that is too great for it to be possible to form a digital key that is invariant.

The correction may comprise determining two angles, θ and φ , that correspond respectively to first and second
 20 attitude differences of a photographic sensor of the picture-taking appliance used for making the digital image relative to first and second axes of that appliance, the second axis being perpendicular to the first axis. The first angle, written θ , may be
 25 determined as follows. The first axis and the second axis of the sensor may correspond to two perpendicular edges of the digital image acquired by the picture-taking appliance.

The distance between the photographic sensor and the
 30 authentication mark is written D , and the focal length of the picture-taking appliance is written f . The diameter $\varnothing_{b \text{ image}}$ of a microbead in the image is the product of multiplying the magnification by the real microbead diameter $\varnothing_b$, i.e.:

$$35 \quad \varnothing_{b \text{ image}} = \varnothing_b \frac{f}{D}$$

In the image plane of the picture-taking device, the diameter of a microbead k may be written as follows:

$$\emptyset_{b\ image}^k = \emptyset_b \frac{f}{D - l_k \tan \theta} = \emptyset_{b\ image} \frac{1}{1 - \frac{l_k}{D} \tan \theta}$$

Where l_k is the distance from the microbead k to the
5 first axis.

For a small angle θ , this relationship can be simplified as follows:

$$\emptyset_{b\ image}^k = \emptyset_{b\ image} (1 + \frac{l_k}{D} \theta)$$

This relationship enables θ to be determined by a
10 linear regression applied to a cloud of points having pairs of coordinates $(l_k; \emptyset_{b\ image}^k)$. Thereafter, the points of the distribution are rotated through an angle θ about the corresponding axis using well-known methods. On the same principle, φ is determined and rotation
15 through the angle φ is applied to the points of the distribution. After these two rotations, all of the microbeads should have the same apparent diameter in the image.

The purpose of steps E360, E370, and E380 is to
20 generate a reference frame specific to the distribution 430. To do this, an elliptical regression is applied in the step E360 to the points of the distribution, whether or not they have been subjected to the attitude correction, thereby defining the ellipse 440 that is the
25 best fit for the set of points of the distribution.

It should be observed that although a distribution of points set in a generally elongate layer 110' of binder, as shown in Figure 4A, is favorable for generating the reference frame, it remains possible to
30 use a generally circular layer 110, as shown in Figure 1A.

The step E370 consists in determining the center of the ellipse, its major axis, its minor axis, and the

angle of the major axis in the reference frame of the initial digital image. The center of the ellipse, its major axis, and its minor axis may serve respectively to define the center, the abscissa axis, and the ordinate axis of a new reference frame, specific to the distribution of points.

The coordinates of each point of the distribution are expressed in the reference frame based on the ellipse during the step E380 for changing reference frame. After this change of reference frame, the points of the distribution have coordinates that are expressed in a reference frame that is linked purely to the distribution itself, and that is not linked to the digital image, as applies prior to this step.

A step E390 consists in normalizing the contents of the points of the distribution by multiplying by a scale factor equal to the ratio of the real diameter of the microbeads divided by a mean diameter for the circular shapes calculated in the image, i.e. divided by the mean diameter of the microbeads as seen in the image.

This step makes generating the digital key independent of the angle of field of the optical device used for making the image and/or independent of the distance between the center of the optical device and the authentication mark while acquiring the image, and thus facilitates generating a digital key that is invariant.

Using an image of the authentication mark as described above and after the digital processing of steps E322 to E390, a digital key that is independent of picture-taking conditions can be generated during a step E395 for generating a digital key.

It should be observed that there is no need to apply all of the above-described digital processing steps on each occasion. For example, the attitude correcting step E350 applies particularly to the situation of a user making a handheld image of the authentication mark under

conditions that are poorly controlled, in particular concerning the picture-taking angle. Under such circumstances, it is likely that attitude correction is necessary. In contrast, under factory conditions, the
5 orientation of the picture-taking device can be controlled so as to make the attitude correction step superfluous.

CLAIMS

1. An authentication method for authenticating objects by using an identifier (100, 100') that is applied to each object (135), the method comprising the following steps:
 - 5 · applying (E20) the identifier on an object that is to be authenticated;
 - making (E30) a first digital image of the identifier (100, 100') applied to the object;
 - deriving (E35) a first digital key from the first
 - 10 digital image;
 - storing (E38) the first digital key in a database (240) containing a plurality of first digital keys;
 - subsequently, making (E50) a second digital image of the identifier (100, 100') applied to the object;
 - 15 · deriving (E55) a second digital key from the second image; and
 - comparing the second digital key with the first digital keys stored in the database (E60) in order to detect a match, and in response to detecting a match,
 - 20 identifying the object as being authentic;
 - wherein, for the identifier (100, 100') that is applied to an object (135), use is made of same-diameter microbeads (120) distributed in a random manner on the surface of the object (135), the microbeads (120) being
 - 25 embedded in a layer (110, 110') of binder sprayed onto the surface of the object (135); and
 - characterized in that the derivation of the first digital key from the first image comprises the following steps:
 - 30 · applying (E360) an elliptical regression to a distribution (430) of points, each situated at the location of a respective one of the microbeads in the first image, in order to define an ellipse (440); and
 - applying (E380) a change of reference frame
 - 35 consisting in expressing the coordinates of each point of

the distribution in a reference frame based on the ellipse (440).

2. An authentication method according to claim 1,
5 characterized in that the derivation of the second digital key from the second image comprises the steps of:
 - applying an attitude correction step (E350) to a distribution (430) of points, each situated at the location of a respective one of the microbeads in the
10 second image, so as to reconstitute an image of the identifier as seen looking along a direction perpendicular to the surface on which the identifier is formed;
 - applying (E360) an elliptical regression to the
15 distribution (430) of points, each corresponding to a respective one of the microbeads in the second image that has been subjected to the attitude correction, in order to define an ellipse (440); and
 - applying (E380) a change of reference frame
20 consisting in expressing the coordinates of each point of the distribution in a reference frame based on the ellipse (440).
3. An authentication method according to claim 1 or claim
25 2, characterized in that it includes a step of normalizing the coordinates of the points of the distribution in the reference frame based on the ellipse by multiplying by a scale factor equal to the ratio of the real diameter of the microbeads divided by the mean
30 diameter of the microbeads as seen in the image.
4. An authentication method according to any one of claims 1 to 3, characterized in that a circular regression is applied to the images of the microbeads
35 (120) visible in the first digital image and/or the second digital image.

5. An authentication method according to any one of claims 1 to 4, characterized in that use is made both of microbeads (120) of a first brightness and/or of a first hue and also of microbeads of a second brightness and/or of a second hue that are respectively different from the first brightness and/or the first hue, so that at least some of the microbeads (120) present sufficient visual contrast with the surface of the object (135) for them to be identified automatically from the digital images.

6. An authentication method according to any one of claims 1 to 5, characterized in that the binder (185) is sprayed onto the surface of the object (135) so as to be inscribed in a circle of diameter less than or equal to 15 mm.

7. An authentication method according to any one of claims 1 to 5, characterized in that the binder (185) is sprayed onto the surface of the object (135) so as to be inscribed in an ellipse of eccentricity greater than or equal to 1.5 and of major axis less than or equal to 15 mm.

8. An authentication method according to any one of claims 1 to 5, characterized in that an identifier (100, 100') is used that comprises a number of microbeads (120) lying in the range 10 to 100, each having a diameter lying in the range 20 μm to 150 μm .

9. An authentication method according to any one of claims 1 to 8, characterized in that the second image is made using a smartphone (200) having a camera (210) and a data processor unit (220), and in that the second digital key is derived from the second digital image by means of

said data processor unit (220) of the smartphone (200)
and/or by means of a remote data processor unit (260).