(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 528 216 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.08.2019 Bulletin 2019/34

(21) Application number: **19157723.8**

(22) Date of filing: **18.02.2019**

(51) Int Cl.:
G07D 7/00 (2016.01)
B42D 25/29 (2014.01)
B42D 25/328 (2014.01)
B42D 25/30 (2014.01)
B42D 25/45 (2014.01)
B42D 25/00 (2014.01)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **19.02.2018 IT 201800002811**

(71) Applicant: **Istituto Poligrafico e Zecca dello Stato S.p.A.**
00138 Roma (RM) (IT)

(72) Inventors:
- **GHISA, Giuseppe**
  00138 Rome (IT)
- **LUCIANI, Laura**
  00138 Rome (IT)
- **INFORTUNA, Francesco Antonio**
  00138 Rome (IT)
- **GUMIERO, Andrea**
  00138 Rome (IT)

(74) Representative: **Papa, Elisabetta et al**
Società Italiana Brevetti S.p.A
Piazza di Pietra, 39
00186 Roma (IT)

(54) DOCUMENT HAVING A SECURITY ELEMENT AND RELATED METHOD

(57) Identification document (1) provided with a security element (101), the latter comprising an authentication data (OK) decomposed into two or more components (O, K) applicated on two or more respective layers (10, 20) superimposed in a position of mutual register. Such layers comprise at least one interfering layer (11, 41, 42) to an electromagnetic wave (R) which incises on the security element (101), said interfering layer being configured in such a way that the authentication data (OK) is detectable as format by all its components exclusively from an only observation direction relating to one of the two opposite faces (A, B) of the security element (101).

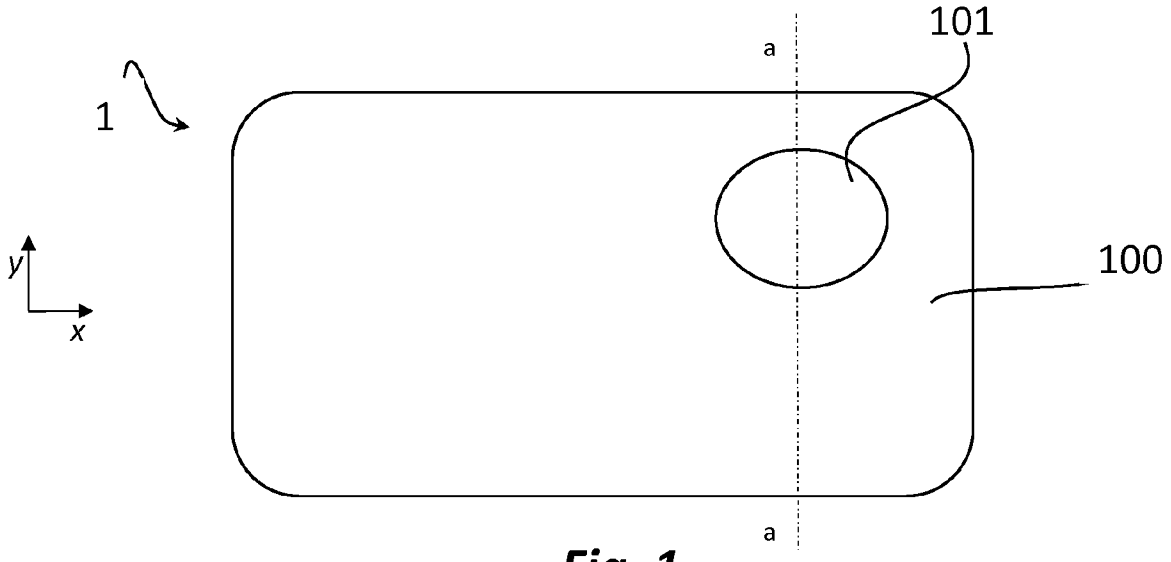

Fig. 1

Printed by Jouve, 75001 PARIS (FR)

Description

Technical field of the invention

[0001] The present invention refers to a document apt to identify with certainty the holder and/or to allow a verification of the authenticity of the document itself. The document may be made, for example, in the form of book, card or banknote.

[0002] In case of identity document, the latter is preferably of the type in accordance with the standard ICAO 9303 (ISO 7810:2003).

[0003] In particular, the document is of the type having a customized security element that bears data selectively detectable by visual observation or by means of measurement or visual instruments.

Background

[0004] On the market, several types of documents are available, such as for example banknotes, recognition documents, passports or the like, that bear one or more portions made in such a way as to be transparent to light (whether widespread or directly incident) and containing security elements capable of confirming or not the authenticity of the document itself.

[0005] For example, US2008/0106091 discloses a security document provided with two optical elements, each of which is placed at a respective transparent window. At the moment of verification, the two transparent windows are superimposed one on the other, folding the document, and the two optical elements so superimposed produce an identification combination.

[0006] WO2017/092865 discloses a security element designed such as to show a first colour visually perceptible if observed in reflected light and a second colour visually perceptible if observed in transmitted light.

[0007] WO2016015130 declares an authentication document provided with a transparent window and of a security element at the latter. The security element comprises an authentication data comprising two components reported respectively on the front and on the rear of the document and a register between them, in such a way that a visual inspection of the document allows to verify the integrity of the information.

[0008] WO 2011/020537 declares an identification document and the corresponding manufacture method, provided with an authentication element comprising two superimposed pictures.

[0009] EP 2 559 563 A1 declares how to realize a security document with a semitransparent intermediate layer bearing portions of an authentication data that is reassembled if observed in transmitted light.

[0010] The documents of prior art above mentioned, even though making use of security elements, represent solutions perfectible regarding aspect such as reliability, ease of implementation and operation, and prevention of counterfeiting attempts.

[0011] In particular, the structure of the security element from the known solutions doesn't achieve a satisfying compromise between an adequate sophistication of security criteria and a simplicity in manufacturing techniques and/or document verification.

[0012] Furthermore, for most of known solutions, the reachable level of security is exclusively limited to protection/verification of the document authenticity, without the possibility to protect/verify even the authenticity of customized sensitive data associated and/or present thereon.

[0013] In addition, the performance of the security element of the known documents can be improved in terms of versatility and durability of materials used both for the element itself and for the whole document, also relating to the mainly portable use of the latter.

Summary of the invention

[0014] The technical problem posed and solved by the present invention is therefore that of providing a document provided with a security element, which allows to overcome one or more drawbacks above mentioned referring to the prior art.

[0015] This problem is solved by a document according to claim 1. The invention also refers to a method of making and verifying the authenticity of above said document according to claim 22 and 27, respectively.

[0016] Preferred features of the present invention represent the subject matter of the dependent claims.

[0017] In this context, the term "document" is to be intended in its broadest sense to include both recognition documents that bear data, for example, to prove the identity of the holder or to allow an authentication of the latter, either banknotes or, more generally, payment devices, without limitation either to the type of material used or to the format of the document itself.

[0018] Similarly, the terms "authentication", "identification", "recognition" or similar words are to be intended to indicate activities associated with proving the origin of the document and/or of identifying the author/holder to which the document is assigned.

[0019] In general terms, the document according to the invention provides a support element, or support, which incorporates a security element. The latter comprises a plurality of superimposed layers that define two opposite faces of the security element. In particular, two or more of such layers bear a corresponding component of an authentication data associated or associable with the support. Such components are arranged according to a position of mutual register between each other.

[0020] Furthermore, the above said plurality of layers comprises at least one layer, which will be recalled as inferring layer, which indeed interfere with an electromagnetic wave that passes therethrough. More in detail, the interfering layer is configured in such a way that the components are all simultaneously detectable to form, or to compose, the authentication data exclusively when observed, or irradiated, from a same observation direction relating to only one of the opposite faces of the security element. In such observation, or irradiation, condition the security element allows to verify the congruity of the authentication data with a reference data. Preferably, the interfering layer is interposed between two of the components of the authentication data and/or between two layers each bearing a respective component of the authentication data.

[0021] Decomposing authentication data in more components to be associated to the different layers of the security element, jointly with the presence of one specific of said layers configured to be transparent selectively to an electromagnetic wave, confers high safety features to the document. In this way, thus, the detection - in its entirely - of the authentication data is exclusively feasible from a single observation direction of the document which - as it will clearly appear from the description below - relates to transmitted radiation. In this condition, the authentication data is reconstructed thanks to the position of mutual register of the above-mentioned components.

[0022] In virtue of such a configuration, the document is therefore hardly adjustable or unduly alterable, for example for the purpose of sabotage or tampering, providing a high level of inviolability of the structural integrity of the security element.

[0023] In a preferred embodiment, the document according to the invention is customizable in such a way that the authentication data contained in the security element coincides with one (or more) reference data, for example arranged on the support element.

[0024] This solution is particularly advantageous as it is possible to associate a reference data uniquely assigned to the document - such as for example a serial number, the reproduction of a face, personal data of the sensitive holder or information of the equivalent type - to the authentication data present in the security element. In this way, it is possible to provide an instrument that certifies both the authenticity of the document itself and the authenticity of sensitive information associated therewith.

[0025] Furthermore, in its embodiments, the document of the invention is easy to be manufactured and easy to be operated during verification.

[0026] Advantageously, the components wherein the authentication data is decomposed are recorded on a corresponding layer of the security element according to a calibration function that allows to observe, or detect, the authentication data formed by two or more components having substantially the same intensity, in this way reducing possible uncertainties associated with the document verification operations.

[0027] Moreover, in virtue of the proposed structure, the security element has high durability.

[0028] Other advantages, characteristics and application methods of the present invention will become apparent from the following detailed description of several embodiments, presented by way of non-limiting examples.

Brief description of the figures

[0029] Reference will be made to the figures of the accompanying drawings, in which:

- Figures 1 and 1A show a front view and an enlargement of a transversal cross-section, respectively, of a security element of a document according to the present invention according to a first embodiment;
- Figure 1B schematically illustrates, in a transversal cross-section view, the behaviour of the security element of the document of the Figures 1 and 1A in an observation or irradiation condition from a selected direction;
- Figure 2 shows a transversal cross-section view of the document of Figure 1;
- Figures 2A and 2B each show, in a schematic prospective view, different observation methods of the document of Figure 1;
- Figures 3 and 3A each show a lateral view of the document according to the present invention according to a second embodiment, respectively in an assembling configuration and in an assembled configuration;
- Figure 4A shows a partial side exploded view of a document according to a third embodiment of the present invention;
- Figure 4B shows a partial side exploded view of a document according to a fourth embodiment of the present invention;
- Figures 5A, 5B, 5C and 5D illustrate a preferred generation method for decomposing into components an authentication data associable with the document according to the invention;
- Figures 6A and 6B each schematically illustrates a corresponding exemplary type of data verifiable by a document according to the present invention;
- Figure 7 schematically illustrates a first elaboration method of a first type of authentication data associable with the document according to the invention;
- Figure 7A and 7B each shows a corresponding flow chart of the operations relating to the elaboration method of Figures 7;
- Figure 7C shows a flow chart of the operations relating to the generation method of Figures 5A, 5B, 5C and 5D;
- Figure 8 schematically illustrates the elaboration method illustrated by figure 7 of a second type of authentication data associable with the document according to the invention;
- Figure 9 schematically illustrates a second elaboration of the first type of authentication data associable with the document according to the invention;
- Figure 9A shows of flow charts of the operations relating to the elaboration method of Figure 9;
- Figures 10 and 11 each schematically illustrates a respective variant of a third elaboration method of a third type of authentication data associable with the

document according to the invention;

- Figure 12 shows a flow chart of a preferred variant of a manufacture method of an embodiment of a document according to the present invention; and
- Figure 13 shows a flow chart of a verification method of the document according to a preferred variant of execution of the the present invention.

Detailed description of preferred embodiments

[0030] With initial reference to Figures 1 and 2, a document according to a preferred embodiment of the invention is overall denoted by the numerical reference 1. Preferably, the document 1 is a document made, for example, in form of book or card, and yet more preferably is of the type pursuant to the standard ICAO 9303 (ISO 7810:2003).

[0031] In the reported examples in the present description, reference will be made to figures that illustrate a document in a format amenable to a card, and preferably with purpose of identification of the holder thereof. However, as already mentioned, the present invention is intended to refer to documents in general, in particular to recognition devices or payment instruments, regardless of the relating format and/or material used to make them.

[0032] It will therefore be understood that the inventive concept of the present invention may be, for example, related to a document provided with pages, suitable for constituting different types of passports with a booklet of existing formats, but at the same time also applicable to a banknote.

[0033] In general terms, the document is structurally defined by, or comprising of, a support 100 and is equipped with a security element 101 integrated in, or jointed to, the support itself. The security element 101 comprises a plurality of layers respectively denoted by the references 10, 11 and 20, and defining a first external layer, an intermediate layer and a second external layer, respectively.

[0034] Preferably, the security element 101 is integrated within the support 100 so that the overall configuration of the document 1 is as such as to define two planar dimensions predominant compared to a third one, with reference to three axes x, y and z mutually orthogonal to each other. In other words, the support 100 and the security element 101 jointed thereto define a document in a card format. The layers 10, 11 and 20 have same form and extension on card plane (x-y plane) and are superimposed along the direction parallel to the axis z which defines the thickness of the card and of the security element 101. The two external layers 10 and 20 define two opposite faces, respectively A and B, of the security element 101 same.

[0035] In the example preferred embodiment hither considered, each of the two opposite faces A and B of the security element 101 corresponds to a respective opposite face of the support 100. In particular, the thickness of the security element 101 defined by the layers 10, 11 and 20 is substantially equal to the overall thickness of the support 100.

[0036] In this case, the opposite faces A and B of the security element 101 and the respective opposite faces of the support 100 jointly determine two opposite sides of the document 1 substantially without discontinuity.

[0037] In the example of Figure 1, the security element 101 is illustrated as having a perimetral profile defined by a closed curve, in particular oval, which borders a region with at least one symmetry axis inside thereof.

[0038] Obviously, different perimetral profiles (and associated dimensions) of the security element 101 - in relation to, for example, the extension of the support 100 - are possible, even depending on the type of document 1 that the person skilled in the art intends to consider.

[0039] It is also possible to provide more than one single security element 101 for a same document 1.

[0040] In general terms, the plurality of layers 10, 11, 20 overall bears an authentication data denoted by the way of example by the abbreviation "OK", which comprises, i.e. is partitioned into, two or more components. In the present example, two components denoted by or and K are provided.

[0041] The OK authentication data is intended to further be associated (or associable) to a reference data, i.e. a variable information, encodable or encoded, as for example a serial number, OCR codes, one-dimensional codes, two-dimensional codes, face reproduction, personal information of the holder of the document 1, or sensitive information of equivalent type.

[0042] Such OK authentication data is encoded within the document 1 by the security element 101.

[0043] In a particularly advantageous embodiment of document 1, the support 100 bears the reference data.

[0044] In different embodiments, the reference data may otherwise be contained in remote devices functionally connected to or associable with (for example by wireless connections) the document 1.

[0045] Each of said two or more components indicates instead a respective portion wherein the OK authentication data has been decomposed.

[0046] Therefore, the OK authentication data results to be complete, and thence consistent to the information expressed by the reference data, only when detectable as composed by all components that has been partitioned into.

[0047] Several possible ways, in which this authentication data is decomposed and is physically contained in the plurality of layers of the security element 101, will be illustrated in the following description.

[0048] In any case, the authentication data is overall contained within the plurality of layers of the security element 101, and, as mentioned, each of said layers bears a corresponding component.

[0049] It is possible to provide an authentication data capable of being partitioned into a greater or minor number of components with respect to the number of layers that composes the security element 101 and/or provides more than one component for a same layer.

[0050] With reference to the example illustrated by Figures from 1 to 2B, as previously described, the OK authentication data has been partitioned into two components O, K and the security element 101 comprises the three superimposed layers 10, 11, 20.

[0051] As can be seen from the view along the a-a section of figure 1A, the three layers 10, 11 and 20 are preferably contiguous and bound together.

[0052] Preferably and independently from the type of described embodiment, coupling means (not shown) are provided, configured to stably bind together the several layers that compose the plurality of layers of the security element 101.

[0053] Referring again to the example of the abovementioned figures, and with particular reference to figure 1B, in this configuration the intermediate layer 11 is interposed between the first external layer 10 and the second external layer 20, in particular an interfering layer that acts on the electromagnetic wave R which passes through the security element 101, as illustrated hereinafter.

[0054] The components O, K are respectively contained by the first layer 10 and by the second layer 20 according to one their relating position of mutual register. For simplicity of disclosure, the two layers which bear the components of the authentication data can be later referred as "principal layers" for the sole purpose of identifying them.

[0055] In general, within the context of this description, the relative position of mutual register for the components indicates a relative alignment (as a non-limiting example, of spatial or frequency type) between the components such that a superimposition (again as a non-limiting example, of spatial type) of the latter according to a selective direction, or verse, of observation allows to rebuild correctly and completely the authentication data.

[0056] The coupling means previously mentioned gives the structure of the security element 101 more effectiveness and makes a - rigid - constraint among the layers that allows to keep the components in register, even when the document 1 is subjected to stress that makes it, for example, bend.

[0057] Furthermore, the relative position of the intermediate layer 11 with respect to the first layer 10 and the second layer 20 allows to define which are the layers associated to said "A Side" or "B Side" of the document 1, depending on the direction according to which the electromagnetic wave R incise and crosses the security element 101.

[0058] Each of said "A Side" and "B Side" of the document 1 can be associated, thence, even to observation direction, incidence or irradiation thereof, to which reference will be made by the term "in reflected radiation" or "in transmitted radiation" depending on the interaction between the interfering layer 11 and the electromagnetic wave R.

[0059] In the context of the present invention, it is worth to recall, for better clarity, a few known principles regarding an electromagnetic wave interacting with the surface of a material or with one or more surfaces of a layers' series of material, even if one different from each other.

[0060] In the optical field, layers or surfaces of certain materials - often denoted by thin-film when their thickness is typically comparable to the wavelength of the incident radiation - have the properties of reflecting, transmitting and/or selectively absorbing an electromagnetic radiation that invests it, depending on its frequency and/or of the structural and chemical properties of the material.

[0061] In virtue of such properties, reflected components of the radiation can be, for example, eliminated or totally reflected; it's possible to divide or combine radiations of different wavelengths or with different directions and more.

[0062] The phenomena that form the basis for this reaction to the incident radiation are essentially amenable to diffraction and interference phenomena and to achieve the desired result, at least in general terms, the number of layers (and the involved thicknesses) and the materials which they are made of, must be properly taken into account.

[0063] Without further deepening into the discussion, when an electromagnetic wave crosses one (or more) surface/layer, principally due to multiple reflection phenomena both at the interface with the surface(s) and between the interfaces of different layers whether present, an interference is generally realized either constructive or destructive in function (also) of the optical path travelled by the wave and of the spectral characteristics of the wave itself.

[0064] Therefore, substantially depending on the type of interference obtained, the transmission of specific wavelengths and the reflection of others are selectively determined.

[0065] Exemplary applications of the general principle above illustrated are dichroic filters, prisms, frames and analogous devices based on the same principle, in the knowledge of those skilled in the art and that will be not further depth.

[0066] Referring again to the example of Figures 1 to 2B, for the document 1 is then established an observation direction, or verse, "in transmitted radiation" when the latter is observed from the opposite face towards that whereon the security element 101 is hit by the electromagnetic wave R.

[0067] Such observation direction in transmitted radiation is associated with the radiation coming from the B Side of the document 1, in the current example. In the same way, for the document 1 an observation direction, or verse, "in reflected radiation" is established when the latter is observed from the same face whereon the security element 101 is hit by the electromagnetic wave R. Such observation direction in reflected radiation is then associated with the radiation coming from the A Side of the document 1, still in the current example.

[0068] The interfering layer 11 is therefore configured in such a way that the two components O and K are both detectable to form the OK authentication data exclusively from an observation direction, in particular the observation direction in transmitted radiation, relating to one only - the B Side, in this example - of the two opposite faces of the document 1, and more in general of the security element 101 incorporated therein.

[0069] Specifically, the interfering layer 11 partitions the electromagnetic wave R affecting the security element 101 into at least one transmitted component Rt associated with first wavelengths and into at least one reflected component R_r associated with second wavelengths, as illustrated in Fig. 1B.

[0070] Observing the security element 101 from the A Side of the document 1, it is noted that the reflected component R_r of the wave R conveys the first component O of the OK authentication data contained by the first layer 10.

[0071] Due to the filtering effect realized by interfering layer 11, from the same observation direction (i.e. in reflected radiation), however, it is not possible to detect the transmitted component Rt of the wave which conveys the second component K of the OK authentication data contained by the second layer 20. Otherwise observing the security element 101 from the B Side of the document 1, it is noted that the transmitted component Rt of the wave R, crossing both the first layer 10 and the second layer 20, conveys along both the first component O and the second component K of the OK authentication data, contained by the first layer 10 and by the second layer 20, respectively. Therefore, the solution above described allows to verify congruity of the OK authentication data by a reference data associated therewith.

[0072] Observing in transmitted radiation, it is possible that the reflected component Rr of the wave R involves an attenuated intensity of the signal associated with the first component O, contained by the first layer 10, with respect to the intensity of the signal associated with the second component K, coming from the second layer 20.

[0073] In this case, appropriate configurations of the document 1, in particular of the first 10 and the second layer and 20, of the interfering layer 11 and of the recording modes of the authentication data, allow to balance the intensity of the signals detected from the observation direction in transmitted radiation and associated with the two components O, K of the OK authentication data, in such a way that they have almost identical intensities.

[0074] For this purpose, exemplifying, it is hereinafter described a possible calibration process that uses a greyscale image, as shown in figure 5A, consisting of fields with 100 levels of grey. The flow chart of the operations associated with this preferred example is shown in figure 7C.

[0075] The calibration process of this example provides the image of figure 5A to be decomposed into two components, respectively shown in Figures 5B and 5C. It is to be noted that this example refers to a decomposition into components which makes use of a pattern 72 shown in figure 7, associated with a specific example of one of the preferred decomposition mode of the authentication data, that will be after illustrated more in detail.

[0076] The two components of the greyscale image are thus transferred (o recorded) on a first layer 10 and on a second layer 20 of a security element devoid of the interfering layer 11 (step 740), and that will be used as a reference element for the calibration process. The same components are also transferred (or recorded) on a first layer 10 and on a second layer 20 of a second security element 101 instead provided with an interfering layer 11 (step 750).

[0077] Lightening the two safety elements during transmission, and comparing them with each other, it is possible to measure the variation of the image grey levels - as illustrated in Figure 5D - and to use the data obtained by these measurements in order to determine a "calibration curve" (step 760).

[0078] Said calibration curve is a function that takes into account the properties of the plurality of layers that compose the security element (for example, radiometric - or photometric - properties, such as thickness or material of the involved layers) and the information recording process, which, preferably making advantage of algorithms of the type disclosed by [1], [2], [3] and here incorporated by these references, allows to define the specific transfer modes of each component in the corresponding layers, in order for them to have intensity substantially equal when observed, or detected, from the observation direction in transmitted radiation.

[0079] As previously mentioned, advantageously, in a preferred embodiment of the document 1, the OK authentication data matches one or more reference data prepared on the support 100.

[0080] By the way of example, types of authentication data, used to verify the document 1 authenticity by comparing to a reference data reported on the support 100 of the latter, are provided by the examples of Figures 6A and 6B. It will also be appreciated that, based on the characteristics of the incident electromagnetic wave R, the detection of the authentication data is possible either by visual observation or even by suitable detection means, for example automatic detection means.

[0081] For this reason, the security element 101, although is preferably configured to allow a selective transparency to an electromagnetic wave within the visible spectrum, in alternative embodiments is configured to operate even with electromagnetic waves whose characteristics lay outside said wavelengths (or frequency) range.

[0082] Advantageously, the layers bearing the components wherein the authentication data has been decomposed may be made of materials suitable to be customized (or encoded).

[0083] Furthermore, according to preferred embodiments, the layers opposite to the interfering layer are preferably made of a plastic material transparent to visible radiation.

[0084] Preferably, the phase of the layers bearing the components of the authentication data provides a recording of the latter in a corresponding layer by means of "additive" techniques, such as for example printing techniques, in particular inkjet, laser engraving or the like, and/or "subtractive" techniques, such as for example laser ablation techniques or analogous techniques, even combined together.

[0085] In many embodiments of the present invention, the above-mentioned components of the authentication data are in the form of polarizable coating, in such a way that the authentication data detectable is a variable content data as a function of the polarization type obtained on said polarizable coating.

[0086] In several exemplary embodiments, the components are in the form of photo-activatable pigments and may be contained in a corresponding layer, for example at a their thickness *d* and/or at a their interface surface *S,* as shown in figure 1B.

[0087] In the context of the present description, the expression "interface surface" intends to denote a discontinuity zone, for example between two layers of the security element 101 that are identical but distinguished or between layers contiguous but qualitatively different.

[0088] It is specified that, for embodiments of the security element 101, even the interfering layer itself may bear a component of the authentication data. For this reason, in embodiments is enough for the security element 101 to be provided with at least two layers superimposed, each bearing a respective component of the authentication data.

[0089] Referring again to Figures 1A, 1B and 2, the interfering layer 11 is preferably realized as a coating of the interface surface S of the layer 10 and/or layer 20. Advantageously, such coating is of the thin-film type, preferably comprising metallic elements, metal oxides or other materials having similar properties. The thin-fil type, as previously mentioned, indicates that the coating thickness is substantially comparable to the wavelength of the incident radiation thereon, in particular - in case of document providing a detection within the visible radiation, such thickness may be comprised between 20 and 500 nm. Multiple interfering layers may also be provided in a same security element. Preferably, the interfering layer is obtained by one or more deposition techniques, such as electrodeposition, sputtering, evaporation of metals or of metal oxides.

[0090] With respect to the exemplary embodiment of the document 1 previously disclosed, as stated, different configurations relating to positioning and number of interfering layers 11 of the security element 101 are also feasible. A few examples of such variants are illustrated below.

[0091] In the example of figure 3 and 3A, a preferred configuration of the document 1 is illustrated, in two separate phases of the production process, and provides a security element 101 comprising three superimposed layers, preferably made of plastic transparent material, and denoted by the references 30, 40 and 50.

[0092] In a preliminary phase, as shown in figure 3, the intermediate layer 40 among said three layers is coated on each of its interface surfaces S by a corresponding interfering layer 41, 42, preferably in the form of thin-film. In this example, the optical density of the interfering layers 41 and 42 is comprised in the range 0.1 - 0.5.

[0093] Subsequently, each of said two interfering layers 41, 42 will be provided with a respective component of the two components O, K wherein an OK authentication data has been decomposed.

[0094] The above-mentioned components are thus sent to phase means of the layers which, preferably through one of the previously mentioned techniques and according to the register positioning mode already described, performs the recording of a first component on (or in) the interfering layer 41 and the recording of a second component K on (or in) the interfering layer 42, as indicated in Fig. 3.

[0095] The intermediate layer 40, provided with the interfering layers 41, 42 containing the components O, K, and the remaining two layers 30, 50 are subsequently coupled together, preferably in such a way as to be contiguous and then rigidly bound - as visible in figure 3A - so as to ensure, at least during a verify phase of the document, the detection in perfect register of said two components O, K with each other.

[0096] In figure 4A is illustrated a further embodiment wherein the security element 101 comprises, similarly to the preceding example, three superimposed layers 30, 40 50.

[0097] In this case, the intermediate layer 40 among said three layers is coated on only one of the interface surfaces S by an interfering layer 41, preferably in the form of thin-film.

[0098] An authentication data F is decomposed into three components F1, F2, F3, and two of said three components - F1 and F2 - are respectively recorded on the interface surface Si of the interfering layer 41 and on the interface surface Sm of the intermediate layer 40, preferably though the above-mentioned additive techniques.

[0099] The remaining component F3 is instead recorded on the thickness of the intermediate layer 40, preferably through the laser engraving technique.

[0100] Finally, the embodiment illustrated in figure 4B, provides a security element 101 similar to that illustrated in figure 4A, which differs only due to a different distribution on the three components F1, F2, F3 wherein the authentication data F has been partitioned.

[0101] As visible, in this case the second component F2 is recorded on the interface surface of the interfering layer 41 while the first F1 and the third F3 component are recorded (for example, through laser engraving) in the thickness of a respective 30, 50 external layers of the three layers 30, 40, 50 of the security element 101.

[0102] Preferably, from a standpoint of the realization process, this configuration provides the interfering layer 41 to be provided with the respective component F2 prior to the coupling with the remaining layers 30, 40. Subsequently to said coupling, the remaining layers 30, 40 are provided with the respective components F1, F3.

[0103] As previously mentioned, configurations that provide the decomposition of the authentication data into a greater number of components are also feasible.

[0104] Several types of algorithms are below reported, by the way of non-limiting examples, that are available for decomposing the authentication data into said two or more components, specifically referring to the features of the information that the authentication data contains.

[0105] Preferably, such components are obtained by digitally processing the authentication data and, in this way, each of the algorithms disclosed, due to its specificity, better fit to a certain type of information (for example, alphanumeric characters, photographs, portraits, alphanumeric strings or other).

a) Decomposition of the authentication data by means of regular grids

[0106] Referring to Figures 7, 7A, 7B and 8, the procedure (shown below) of decomposing the authentication data into components is preferably used when the latter relates to images which depict a face 71 or alphanumerical codes 81.

[0107] The authentication data is partitioned preferably into two components, following a predetermined pattern 70 using the aid of algorithms, for example filtering algorithms, preferably of the type disclosed in [4], here incorporated by this reference.

[0108] Said pattern is generated as a theme or recurring scheme 72, 82, preferably as a monochromatic bitmap file, in a regular and balanced way, multiplying and adding them to each other, according to a regular and ordered grid, identical basic modules (for example, composed of elementary geometric figures), pursuant to the translational symmetry rules (for example, operating vertical and horizontal translation).

[0109] In the illustrated case, each component (the components illustrated by the references 73, 74 when referring to the portrait 71, the components illustrated by the references 83, 84 when referring to the alpha-numerical code 81) is respectively generated using the portion of the authentication data corresponding to the white and the black ones of the pattern 72, 82.

[0110] Hereinafter it is indicated, as a way of non-limiting example, the flow of operations to be executed.

[0111] *Pattern generation* (Figure 7A):

- choose, during a step or phase 701, the monochromatic recurring theme 70 (in black and white);
- build, during a step or phase 702, the pattern 72, 82 as a monochromatic bitmap file, repeating the recurring scheme, in vertical and horizontal translation, along the entire dimension of the pattern.

[0112] *Generation of the two components* (respectively denoted by the references 73, 74 and 83, 84):

- generate, during a step or phase 710, two selections corresponding with the black and white portions of the pattern by means of selection functions, preferably the selection functions of Adobe Photoshop®;
- superimpose, during a step or phase 720, the selection of the white portion on the authentication data 71, 81 and generate a first component 74, 84 comprising the white portion of the pattern 72, 82 and of the authentication data, at the black portion of the pattern;
- superimpose, during a step or phase 730, the selection of the black portion on the authentication data 71, 81 and generate a second component 73, 83 comprising the black portion of the pattern 72, 82 and of the authentication data, at the white portion of the pattern.

b) Decomposition of the authentication data by means of random grids

[0113] Now referring to Figures 9 and 9A, in the illustrated example the authentication data 91 is decomposed into two components 92, 93 according to a random pattern 90, even in this case making use of algorithms within reach of those skilled in the art, preferably of the type disclosed in [4].

[0114] Similarly to that illustrated in the previous paragraph a), the two components 92, 93 are generated respectively using the portion of the authentication data 91 corresponding to the white and the black of the pattern 90.

[0115] In this case, the pattern 90 is generated as a non-regular theme or scheme, preferably as a monochromatic bitmap file, juxtaposing, according to a disorderly and irregular grid, basic modules different one from each other, preferably following the randomness of a pseudo-random number generator [5], here incorporated by this reference.

[0116] In this case, in other words, it is possible to generate a random grid as a pattern, using for example a reference data associated with, or reported on, the document 1 (for example the card number, personal data or other similar information) as a seed of random generation.

[0117] Such decomposition method is preferably recommended for treatment of photos/images, as illustrated in figure 9.

[0118] Below, and further referring to figure 9A, the flow of operations to be executed to generate the random pattern is indicated, by the way of a non-limiting example.

Generation of the random pattern:

[0119]

- provide, during a phase or step 910, a pseudo-random number generator, for example a generator that uses the Mersenne Twister algorithm [6], here incorporated by this reference;

- select, during a phase or step 920, a generation seed, for example a reference data associated with, or reported on, the document 1;
- provide, during a phase or step 930, one (or more) recurring monochromatic (black or white) theme/scheme to build the pattern 90;
- replicate, during a phase or step 940, the theme/scheme along the entire dimension of the pattern 90 according to the random coordinates given by the pseudo-random number generator.

c) Decomposition of the authentication data when referring to alpha-numerical strings

[0120] In this case, the authentication data 101, 111 is a string, preferably alpha-numerical string, whose elements are sorted following a specific criterion. Referring to Figures 10 and 11, the elements of the string comprise alphabetic characters, and the authentication data is partitioned into two components. In a first case, the components are denoted by the references 102, 103 and in a second case the components are denoted by the references 112, 113.

[0121] In the first case (Figure 10), the elements of the string of each component are regularly distributed among the two components 102, 103, whilst in the second case (Figure 11) said elements are randomly distributed among the two components 112, 113, being compliant with the relative position of said sorting criterion among the elements.

d) Decomposition of the authentication data in three components

[0122] Now referring to the case wherein the authentication data, for example an image, is partitioned into more than two components, preferably in three components, and wherein an interfering layer 11, 41, 42 bears at least one of said components.

[0123] The partition into three components is compliant with, for example, the following criterion:

- a first component contains the close-up of a face illustrated in an image (foreground);
- a second component contains un intermediate level of the image (middleground);
- a third component contains the background of the image (background). Each component can be obtained even by the use of a regular or random pattern, as previously disclosed in paragraph a), preferably with three distinct shades.

[0124] Whether the image was a colour image, the three components can be obtained considering their decomposition in compliance with, for example, models based on principles of additive synthesis (RGB) or subtractive synthesis (YMC).

[0125] It is now described, by way of non-limiting example, a preferred method to manufacture the document 1, in the specific case of the latter being in card ID-1 format and provided with a customized security element 101, i.e. containing an authentication data related to an image depicting the holder (for example, the face) of the card.

[0126] For the sake of simplicity, reference will be made to the structure of the document 1 shown in figures from 1 to 2B, wherein the security element 101 comprises three layers superimposed and the authentication data is partitioned into two components.

[0127] Further referring to the flow chart illustrated by figure 12, is thence described the succession of operations necessary to manufacture said document 1.

[0128] In general terms, the method can be partitioned into two main phases.

[0129] A preliminary phase, overall denoted in the chart by the reference 127, of making the security element 101 and a phase subsequent to the latter with the authentication data.

[0130] To manufacture the security element 101 is firstly necessary to provide a first layer 20 of material, preferably a plastic transparent material and comprising photo-activatable pigments.

[0131] The first layer 20 of the security element 101 is preferably a material having properties such as to be customized through laser engraving techniques.

[0132] On an interface surface S of said first layer 20 is thus laid an interfering layer 11, preferably a thin-film, for example through one of the previously disclosed techniques (electrodeposition, sputtering or evaporation of metals or metal oxides).

[0133] Subsequently, the first layer 20 provided with the interfering layer 11 is coupled to a second layer 10, preferably in plastic transparent material.

[0134] The overall configuration of the three layers 10, 11, 20 is such that the interfering layer 11 is interposed between the first 20 and the second layer 10 and that, preferably, said three layers are contiguous and bound together, by coupling means suitable for the purpose.

[0135] The interfering layer, as above disclosed, has the property to be selectively transparent to an electromagnetic wave R which passes through the security element 101, in the described example preferably a wave within the visible spectrum.

[0136] The security element 101 should be now customized con the authentication data.

[0137] As stated, in the example here considered, the authentication data relates to an image depicting the holder of the document 1. It is, however, clear that is possible to associate other types of information to the authentication data.

[0138] For this purpose, the customization phase provides the step 120 of an initial digitally providing of said image, in such a way that the latter can be processed.

[0139] Preferably, the authentication data is a graphic format image 91, i.e. a digital data in a format that expresses an information intelligible for the human eye. Obviously, such an image may be downloaded from an image database 128, or even be digitally generated according to any modes available for those skilled in art and which, already known, will be no longer discussed.

[0140] Subsequently, in a step 121, a coding algorithm is selected for the authentication data, preferably pursuant to one of the methods (a, b, c, d) above disclosed.

[0141] The algorithm allows to partition the authentication data into more components and, in the current example, the algorithm which predicts the use of random grids will be taken into account.

[0142] Further referring to Figure 9, a random pattern 90 is thus generated, at step 122, and preferably starting from a same theme/scheme for each document, choosing as a random generation seed a characteristic element of the document to be produced, as for example the number of the card itself.

[0143] Once the pattern is obtained, a first component 92 containing the sole portions of the image corresponding to the white of the pattern is generated, referring to step 124a. Similarly, a second component 93 containing the sole portions of the image corresponding to the black of the pattern will be generated (step 124b).

[0144] Preferably, as previously disclosed, a calibration of the intensity of the components is performed (as indicated at step 129), calculating a calibration curve to define the specific transfer modes of each component in the respective layers of the security element, in order for them to have intensity almost equal when detected from the observation direction in transmitted radiation of the security element.

[0145] The two components 92, 93 thus obtained are associated 125 to two separate layers of the security element 101. In particular, the first layer 20 bears the first component 92 and the second layer 10 bears the second component 93, according to a position of mutual register.

[0146] Preferably, the two components 92, 93 are recorded in the thickness of a respective layer 20, 10 through laser engraving techniques.

[0147] Preferably, the document 1, and advantageously the support 100, is further customized by reference data of the card holder, such as, for example, the same image 91 used as authentication data.

[0148] The document 1 is thus ready to be used.

[0149] In the flow chart illustrated in figure 13, the steps of a method to verify the document authenticity 1 are represented according to the present invention, according to a preferred embodiment of the latter.

[0150] Preliminarily, an electromagnetic wave R investing the document 1 is provided. The security element 101 is thence observed 130 in reflected radiation, to detect the authentication data from one or both its opposite faces A, B.

[0151] In this way, it is verified whether only one component of the authentication data contained thereof is detectable.

[0152] The security element 101 is thence observed 131 in transmitted radiation to detect the authentication data in a complete form.

[0153] The completely detected authentication data is then compared 132 to a reference data. Their congruity is therefore verified and, in positive case 133, the document 1 results to be true. On the contrary, the document is counterfeit. Advantageously, the reference data is prepared on the document 1 itself, preferably on the support 100, in such a way that the congruity of the latter to the authentication data allows to verify both the authenticity of document 1 itself and the authenticity of the sensitive information associated therewith. The document 1 may even provide additional security elements that allow (any) congruity verifications 134 in addition to those associated with the authentication data according to the method previously disclosed.

[0154] The present invention has been herein described referring to preferred embodiments. It is to be intended that other embodiments may be implemented which belong to the same inventive core, as defined within the scope of claims set forth below.

[1] Acharya and Ray, Image Processing: Principles and Applications, Wiley-Interscience 2005.

[2] Russ, The Image Processing Handbook: Fourth Edition, CRC 2002.

[3] Specification ICC.1:2010 (Profile version 4.3.0.0).

[4] Functions of filtering and masking Adobe®.

[5] A. Menezes, P, van Oorschot, S. A. Vanstone - Handbook of Applied Cryptography - CRC Press 1996.

[6] Mersenne Twister: A 623 - Dimensionally Equidistributed Uniform Pseudo -Random Number Generator MAKOTO MATSUMOTO Keio University and the Max-Planck-Institut fur Mathematik and TAKUJI NISHIMURA Keio University. ACM Transactions on Modeling and Computer Simulation, Vol. 8, No. 1, January 1998.

Claims

1. A document (1), comprising:

- a support (100); and
- a security element (101) bearing an authentication data (OK; F), which security element (101) comprises a plurality of layers (10, 11, 20; 30, 40, 41, 42, 50) superimposed and fixed one to each other to define two opposite sides (A, B) of the security element (101),

wherein at least two main layers (10, 20; 41, 42) of said plurality each bears a respective component (O, K; F_1, F_2, F_3) of said authentication data (OK; F)

arranged in mutual register,
and wherein said plurality of layers comprises at least one interfering layer (11; 41, 42) interposed among at least two main layers, said interfering layer being configured to selectively transmit first wavelengths and to reflect second wavelengths of an incident electromagnetic radiation (R) thereon, such that said components (O, K; F_1, F_2, F_3) of said authentication data (OK; F) are all observable or detectable to form said authentication data (OK; F) exclusively from one observation direction in transmitted radiation related to only one of said two opposite faces (A, B) of the security element (101),
in such a way that the document (1) allows to verify the congruity of said authentication data (OK; F) with reference data.

2. The document (1) according to claim 1, wherein said two main layers (10, 20) are directly adjacent and in contact with said interfering layer (11).

3. The document (1) according to any one of the preceding claims, wherein an additional layer (40) of said plurality of layers is interposed between said two main layers (30, 50).

4. The document (1) according to any one of the preceding claims, wherein said interfering layer (11; 41, 42) is in the form of a coating of an interface surface (S) of a layer of said plurality of layers.

5. The document (1) according to claim 4, wherein said coating (11; 41, 42) is of the thin-film type, preferably comprising metallic elements or metal oxides.

6. The document (1) according to claim 4 or 5, wherein said interfering layer (11; 41, 42) is obtained by one or more processes comprised in the list comprising electrodeposition, sputtering, evaporation of metals or of metal oxides.

7. The document (1) according to any one of the preceding claims, wherein interfering layer (11; 41, 42) is configured to allow a selective transparency of the security element (101) to an electromagnetic wave within the visible spectrum.

8. The document (1) according to any one of the preceding claims, wherein at least one layer of said plurality of layers is made of plastic and/or transparent material to said incident electromagnetic radiation (R).

9. The document (1) according to any one of the preceding claims, wherein said two main layers (10, 20) each bears the respective component (O, K) of the authentication data at their own thickness and/or at their own interface surface (S).

10. The document (1) according to any of the preceding claims, wherein said components (O, K) of the authentication data are realized by means of photoactivatable pigments.

11. The document (1) according to any one of the preceding claims, wherein said components (O, K) of the authentication data are in the form of polarizable coating and said authentication data (OK) is a variable content data according to the type of polarization obtained on said polarizable coating.

12. The document (1) according to any one of the preceding claims, wherein said two components (O, K) of the authentication data are recorded on the respective layer of said plurality of layers by one or more techniques comprised in the list comprising laser engraving, laser ablation, inkjet.

13. The document (1) according to any one of the preceding claims, wherein the optical density of said interfering layer (11; 41, 42) is comprised between 0.1 and -0.5 approximately.

14. The document (1) according to any one of the preceding claims, wherein said authentication data (OK; F) coincides with one more reference data provided on the support (100).

15. The document (1) according to any one of the preceding claims, wherein said support (100) is in the form of a page, card or banknote.

16. The document (1) according to any one of the preceding claims, wherein said plurality of layers is a laminate.

17. The document (1) according to any one of the preceding claims, wherein the thickness of the security element (101) defined by said plurality of layers is substantially equal to the thickness of the support (100).

18. The document (1) according to any one of the preceding claims, wherein said two or more components (O, K; F_1, F_2, F_3) are transferred on a respective layer of said plurality (10, 11, 20; 30, 40, 41, 42, 50) according to a calibration function obtained from the properties of the latter and in such a way that said two or more components have the same intensity when observed, or detected, to form said authentication data (OK; F).

19. A method of making a document (1) according to any one of the preceding claims, comprising the steps of:

- digitally providing an authentication data (OK) to be associated with the document (1);

- providing two or more layers of material configured to bear said authentication data (OK), wherein said two or more layers comprise an interfering layer with an electromagnetic wave passing therethrough;
- coupling at least one layer (20) of said two or more layers with said interfering layer (10);
- decomposing said authentication data (OK) into two or more components;
- transferring, in a position of mutual register, each of said two or more components on a respective of said two or more layers to obtain a security element (101);
- providing a support element (100) of the security element (101) to obtain the document (1),

wherein said two or more layers are coupled in a superimposed manner and wherein said interfering layer is configured in such a way that said two or more components are all detectable to form said authentication data exclusively from an observation direction relating to only one of two opposite sides (A, B) of the security element (101).

20. The method of making a document (1) according to claim 19, comprising the steps of:

- providing three layers of said two or more layers of material, wherein the intermediate layer of said three layers is said interfering layer;
- coupling a first layer of said three layers with the interfering layer and subsequently coupling the latter with the remaining of said three layers;
- transferring a first component of said two or more components on said first layer and a second component of said two or more components on said remaining layer.

21. The method of making a document according to claim 19, comprising the steps of:

- providing four layers of said two or more layers of material wherein one of which is said interfering layer;
- coupling a first layer of said three layers with the interfering layer;
- transferring a first component on said interfering layer and subsequently
- coupling the two remaining layers with said first layer and with said interfering layer, respectively; and subsequently
- transferring on said two remaining layers a second and a third component respectively.

22. The method of making a document according to any one of the claims from 19 to 21, wherein a phase of calibrating the intensity of said two or more components is performed prior to transferring the latter on a respective one of said two or more layers.

23. The method of making a document according to any one of the claims from 19 to 22, comprising the step of preparing one or more reference data on said support element (100), wherein said authentication data (OK) corresponds to said one or more reference data.

24. Method of making a document accord to any one of claims from 19 to 23, wherein said two or more components (O, K; F_1, F_2, F_3) are digitally obtained by processing said authentication data (OK; F) based on regular grid or on patterns obtained by algorithms implemented by random or pseudo-random number generators.

25. A method of verifying the authenticity of a document comprising the steps of:

- providing a document (1) according to any one of the claims from 1 to 18;
- exposing the security element of said document (1) to an electromagnetic wave (R) with a direction of incidence which invests said document (1) from one of two opposite sides (A, B) of a security element (101) of the latter;
- detecting an authentication data (OK) contained by the security element (101) from an observation direction facing the face opposite to the face related to said incidence direction;
- comparing the authentication data (OK) detected with a reference data associated with the document (1) to verify their congruity and therefore the authenticity of the document (1).

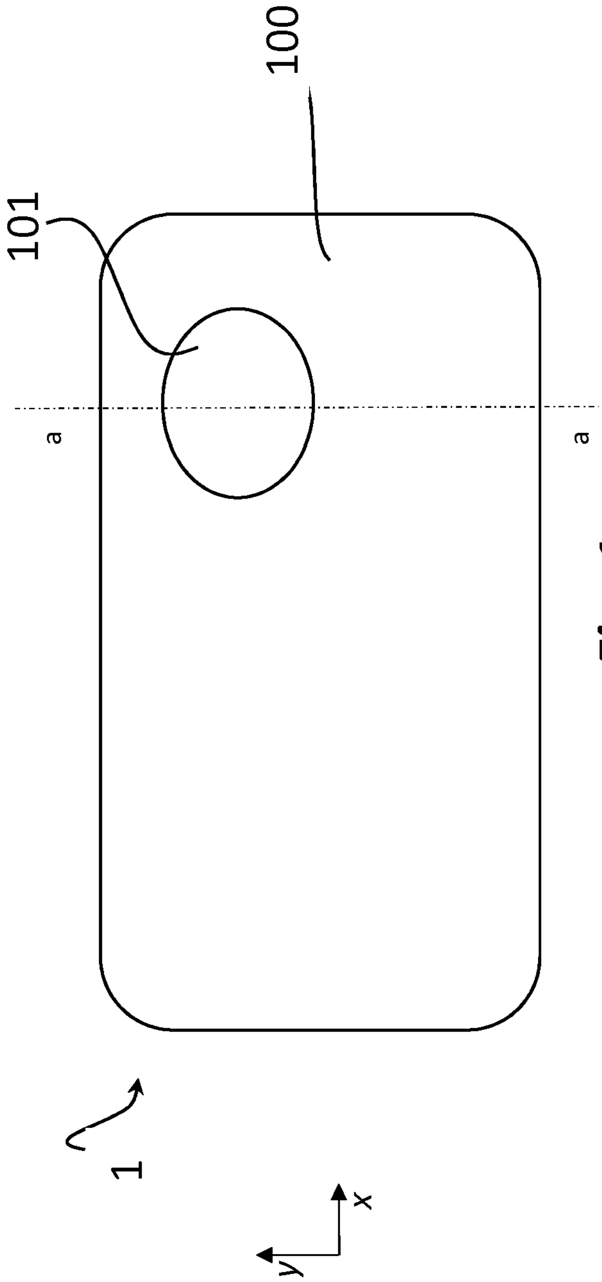

Fig. 1

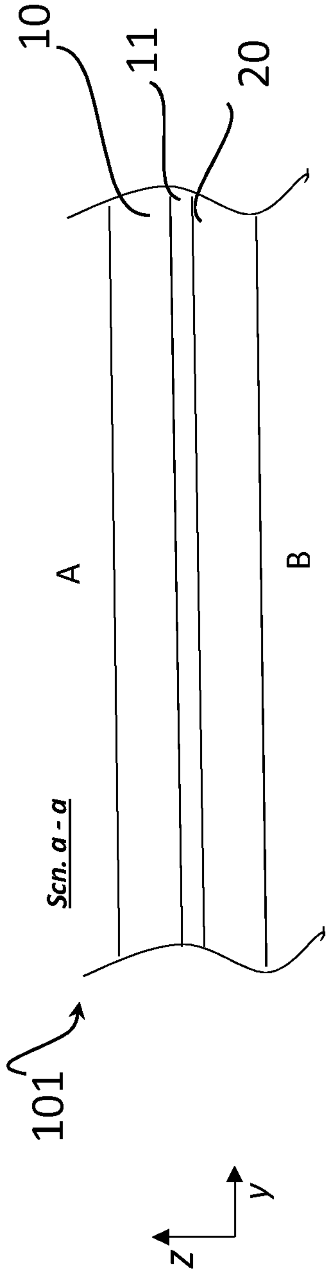

Fig. 1A

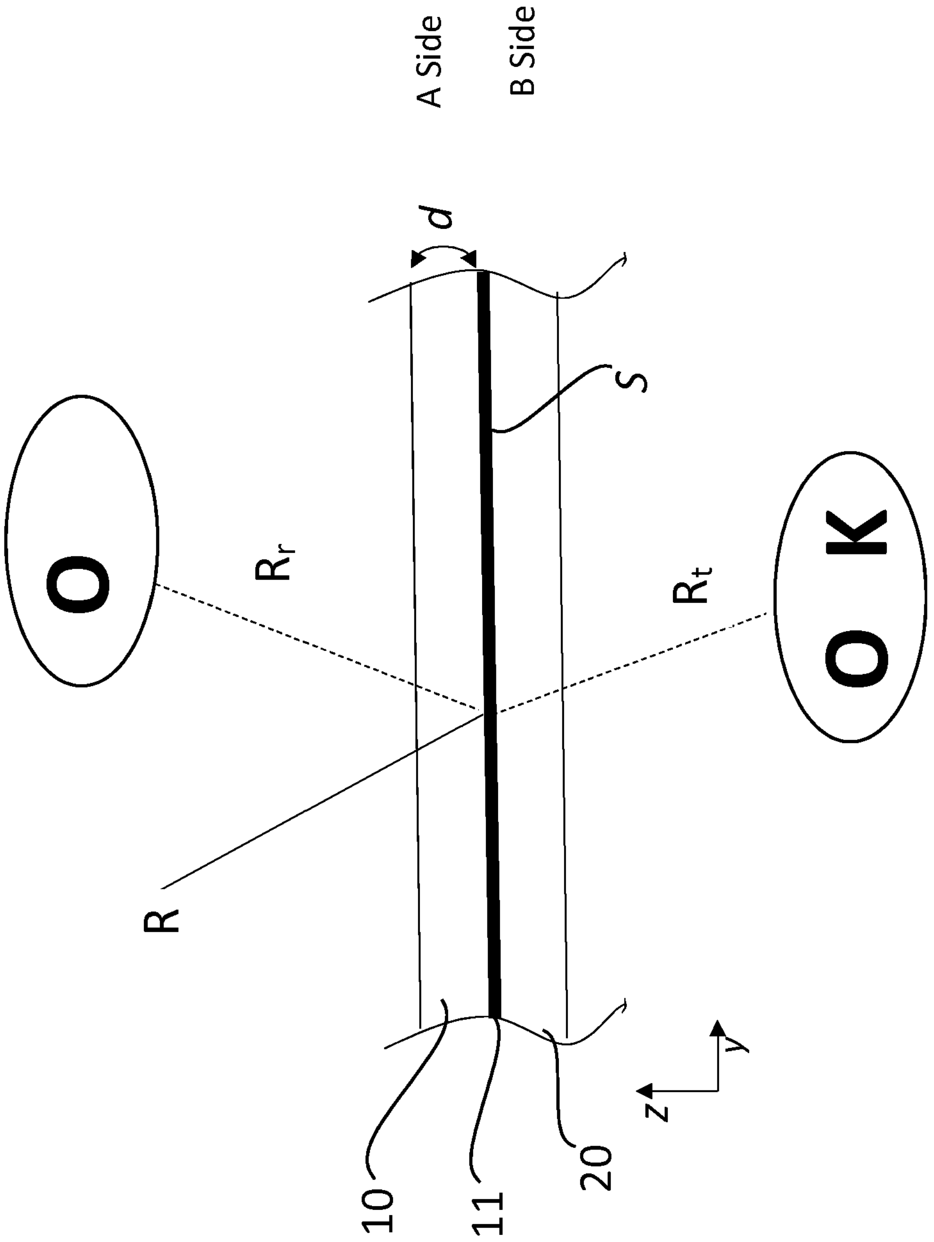

Fig. 1B

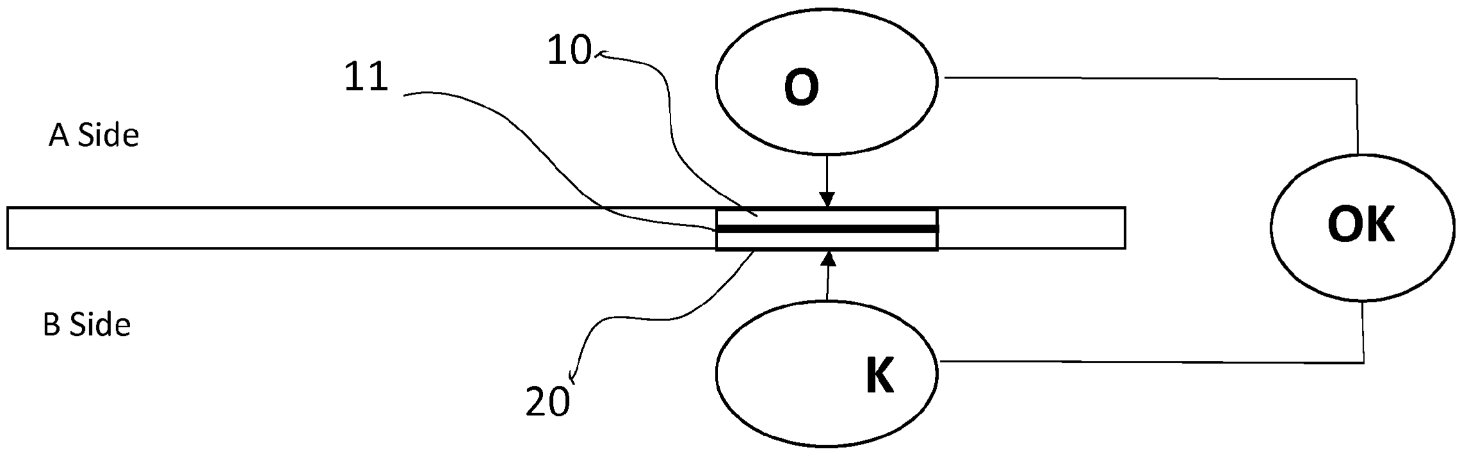

Fig. 2

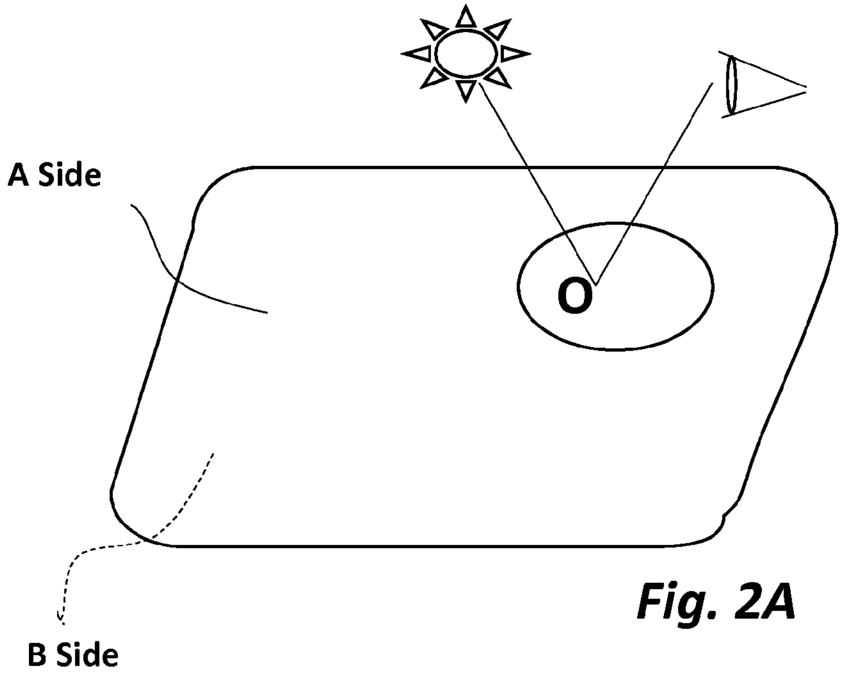

Fig. 2A

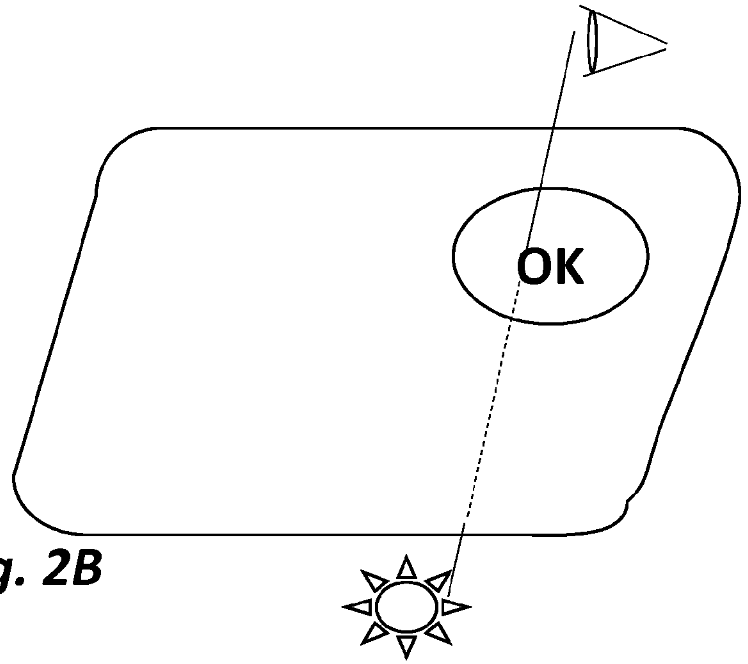

Fig. 2B

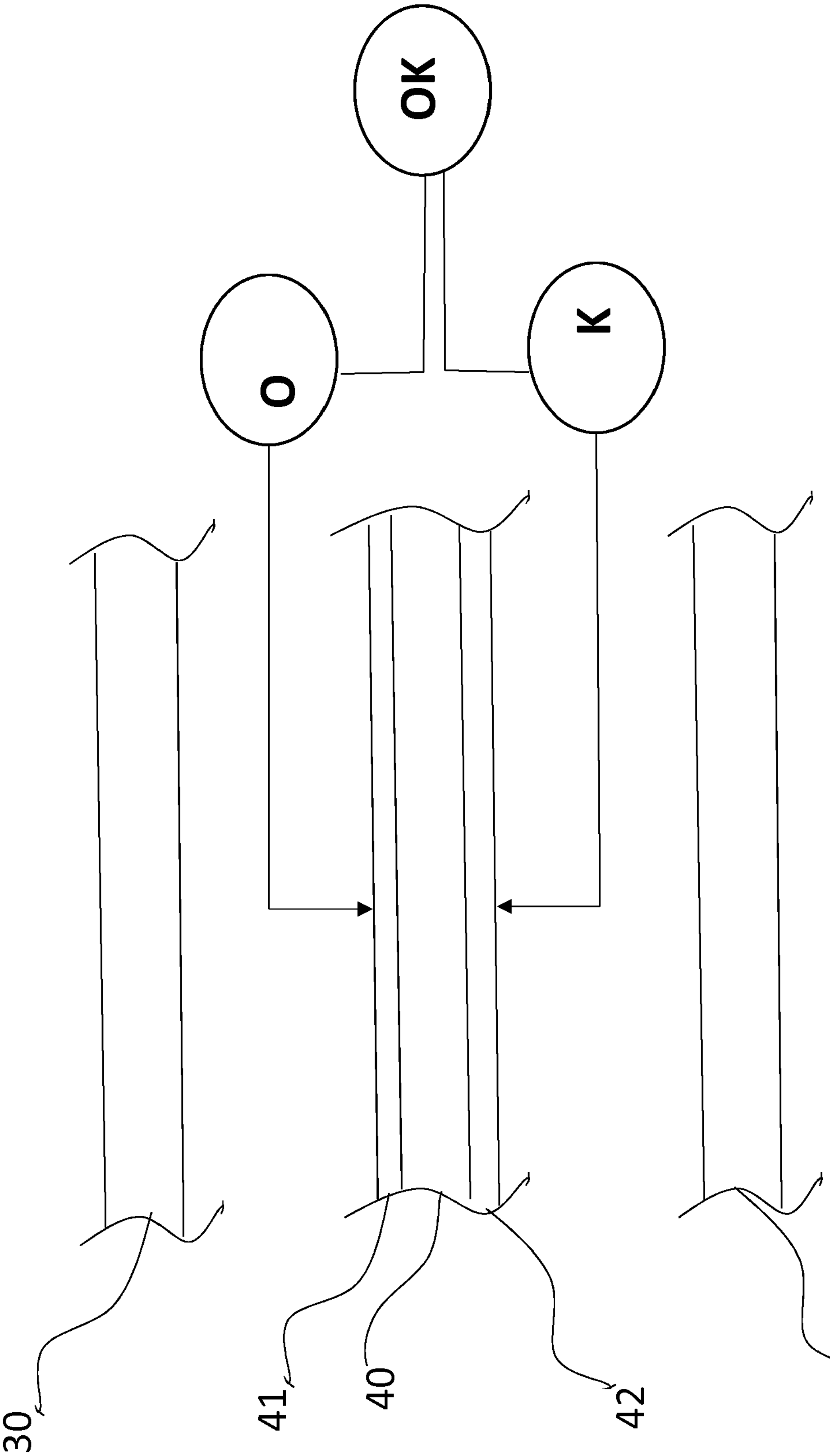

Fig. 3

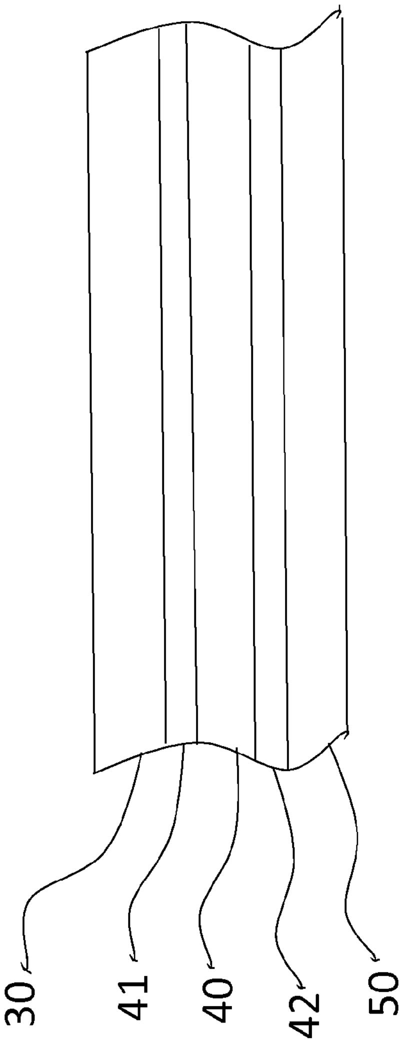

Fig. 3A

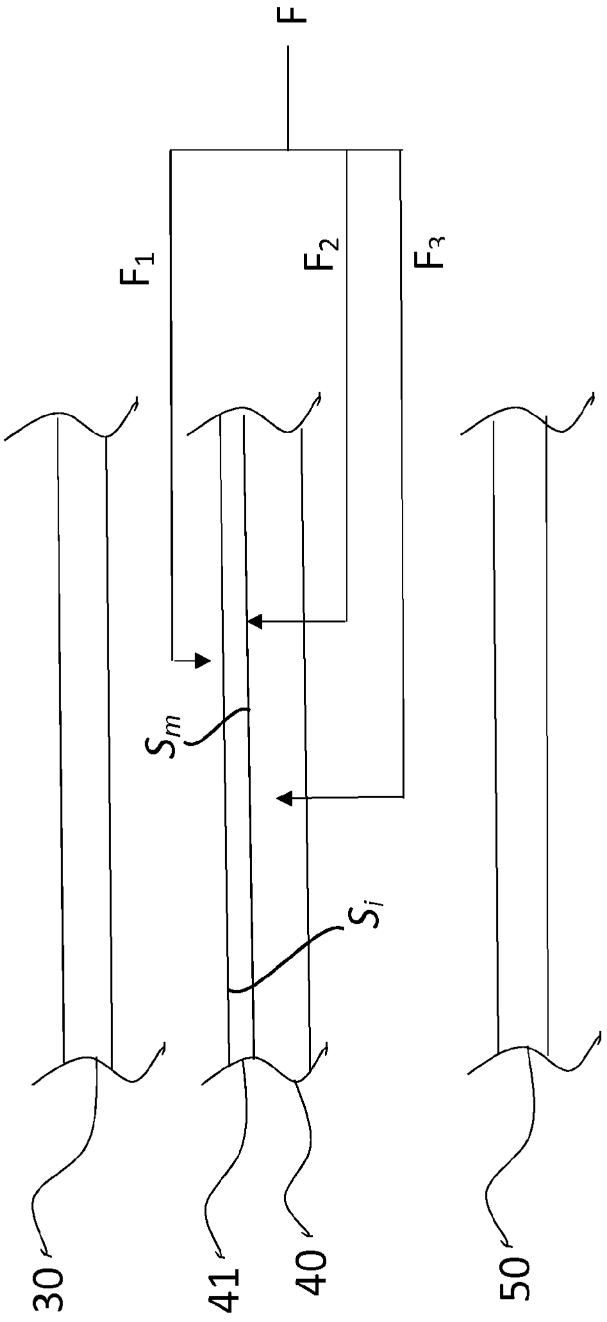

Fig. 4A

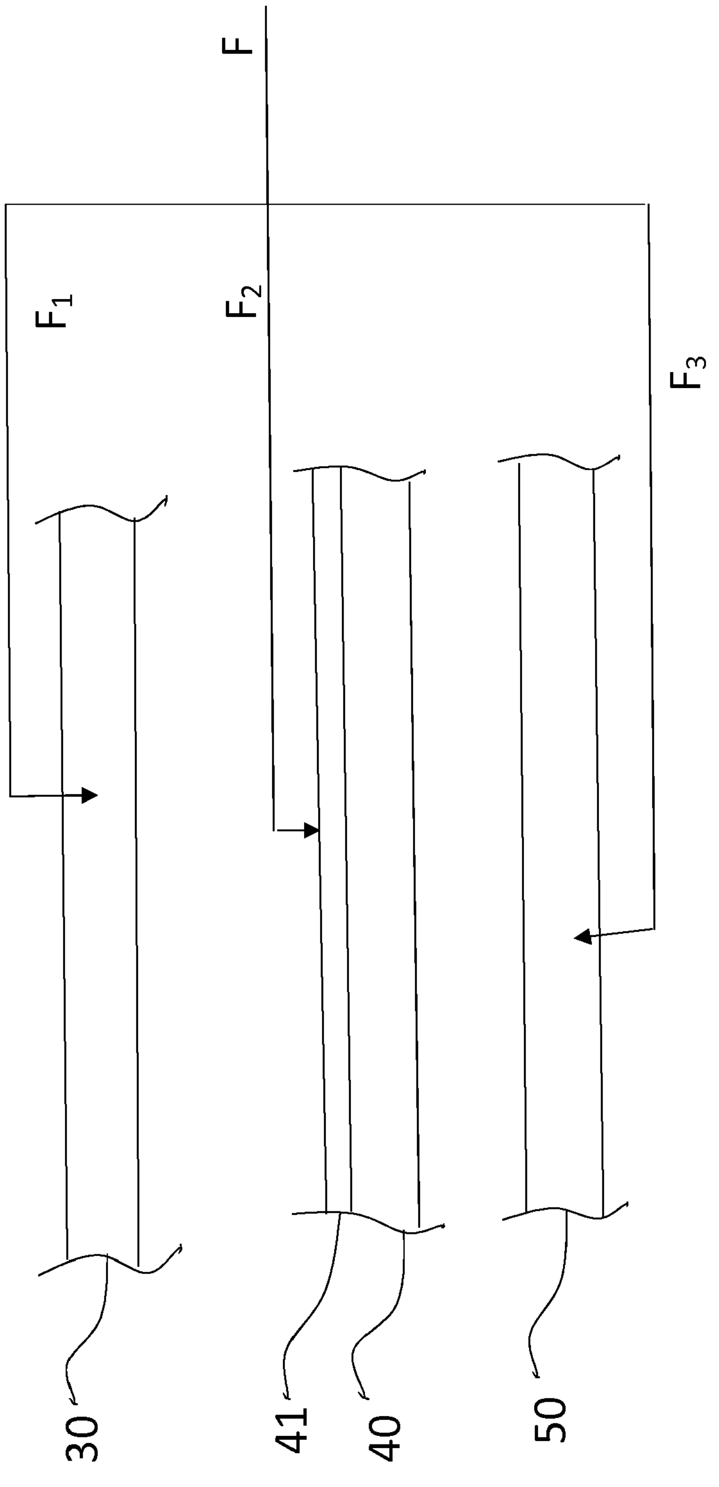

Fig. 4B

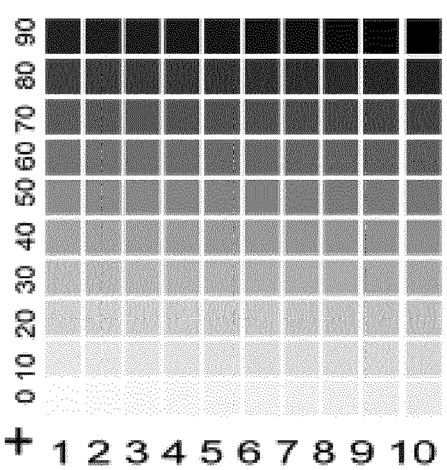

Fig. 5A

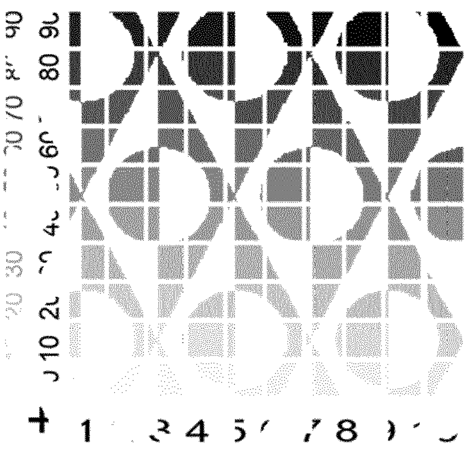

Fig. 5B

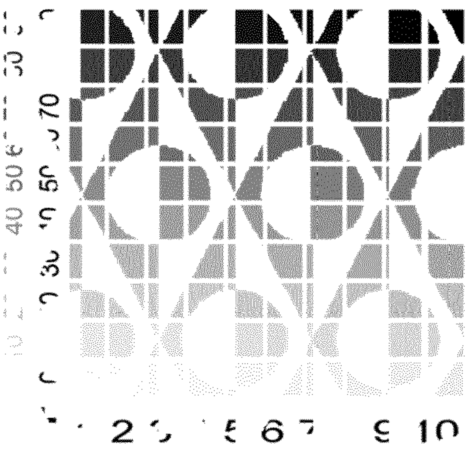

Fig. 5C

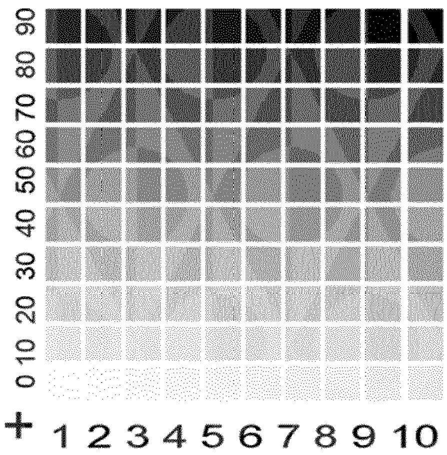

Fig. 5D

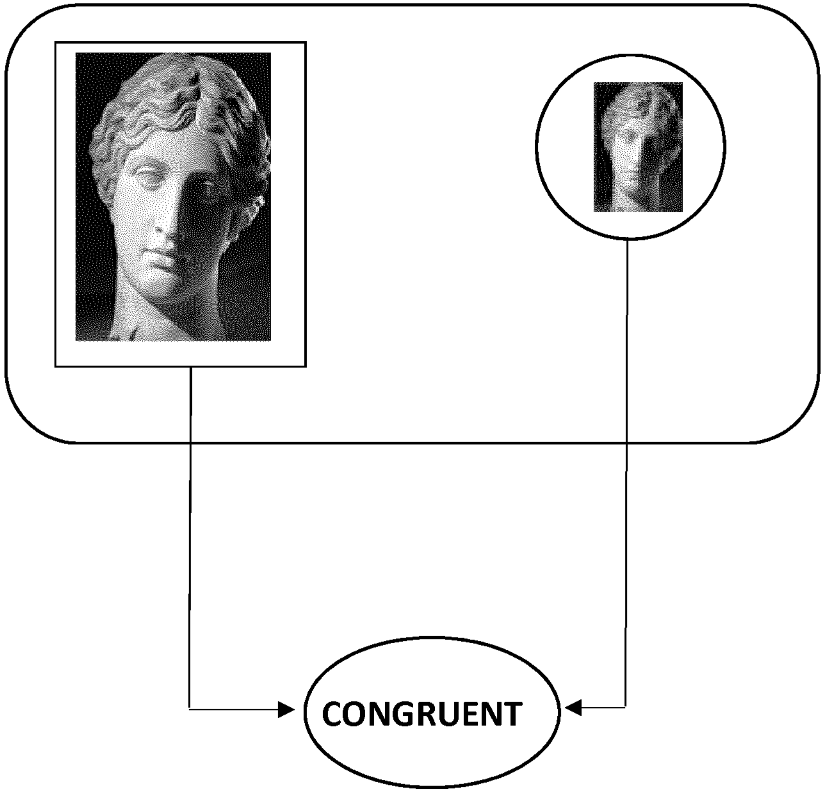

Fig. 6A

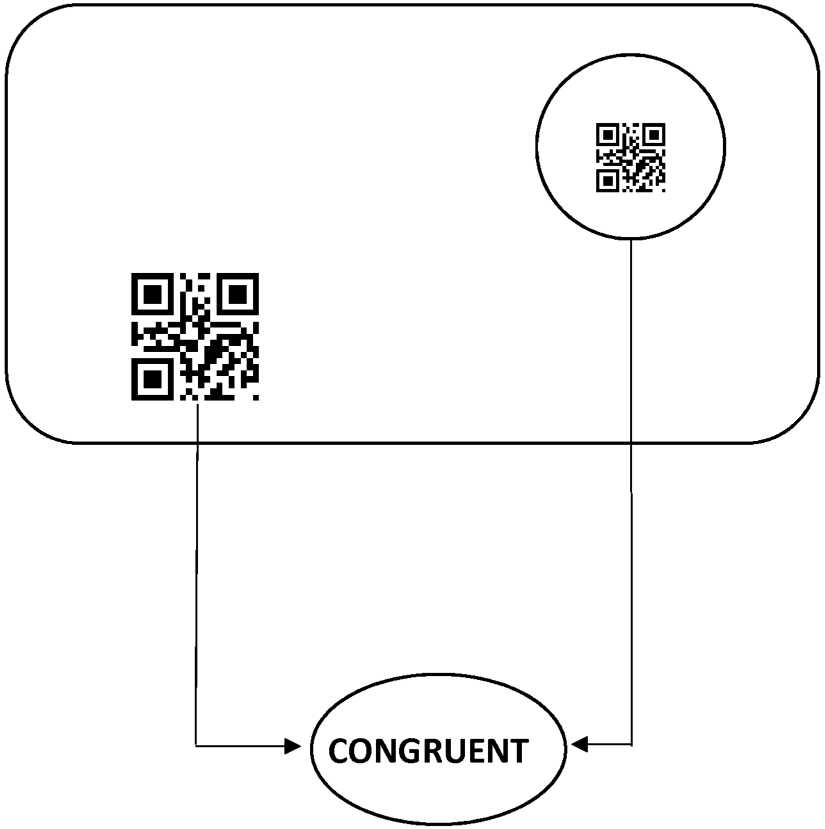

Fig. 6B

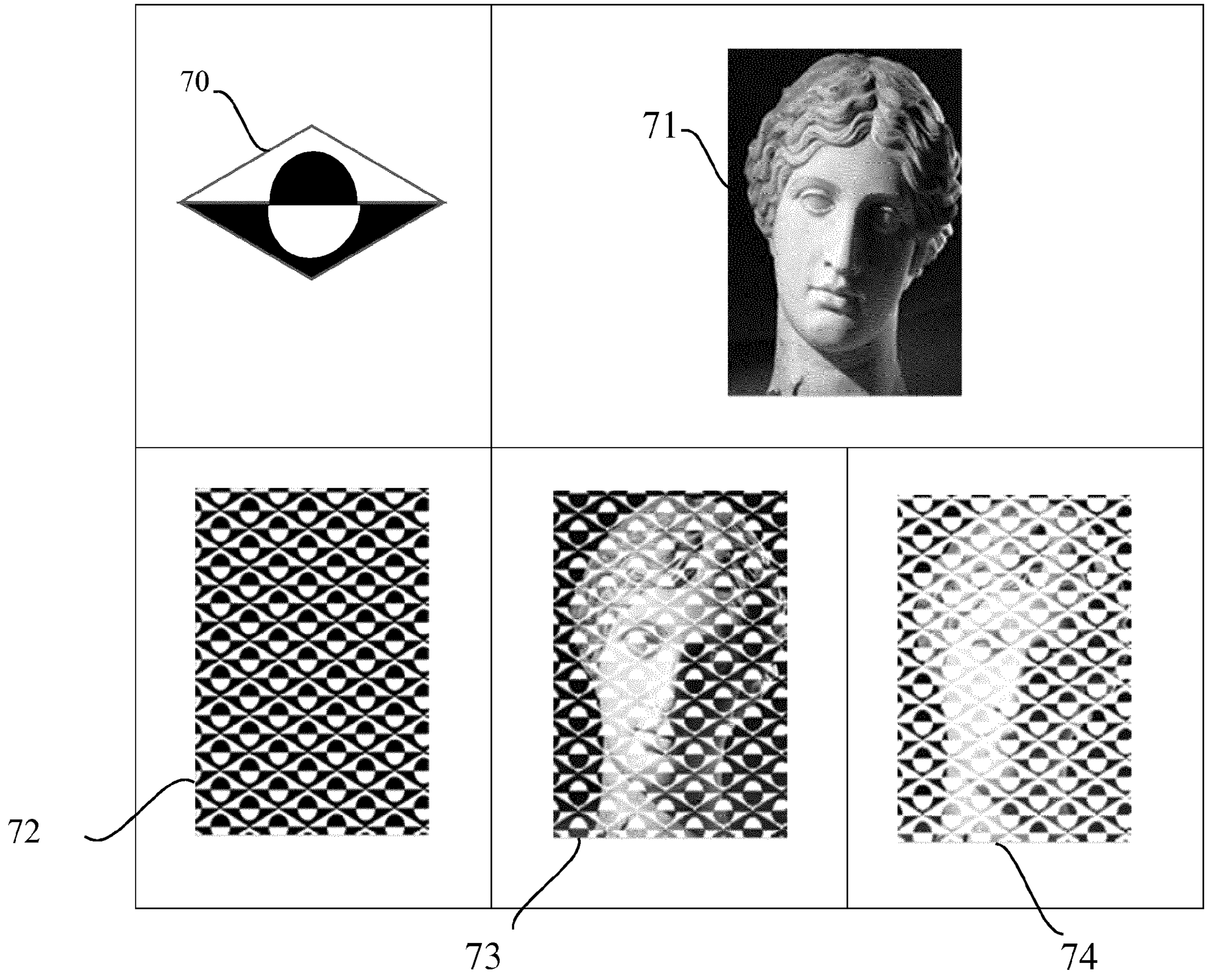

Fig. 7

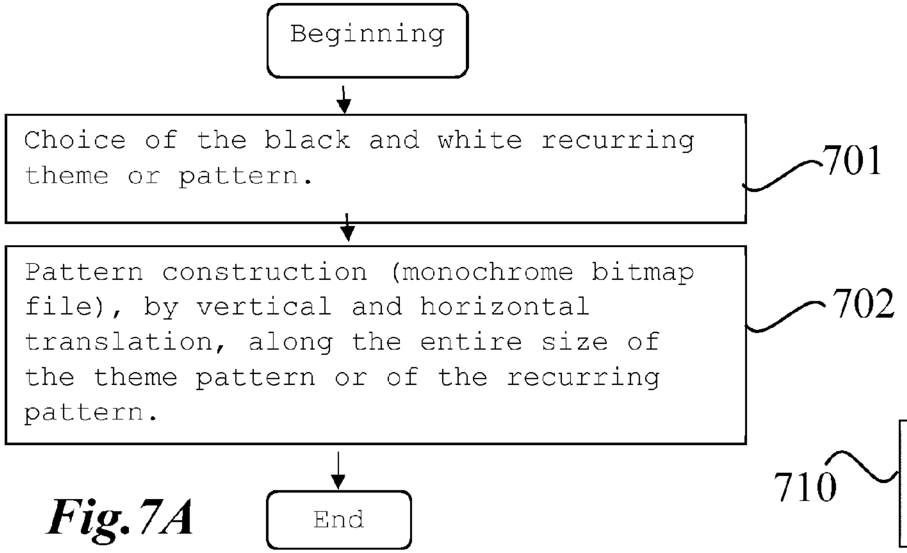
Beginning
Choice of the black and white recurring theme or pattern.
701
Pattern construction (monochrome bitmap file), by vertical and horizontal translation, along the entire size of the theme pattern or of the recurring pattern.
702
End

Fig. 7A

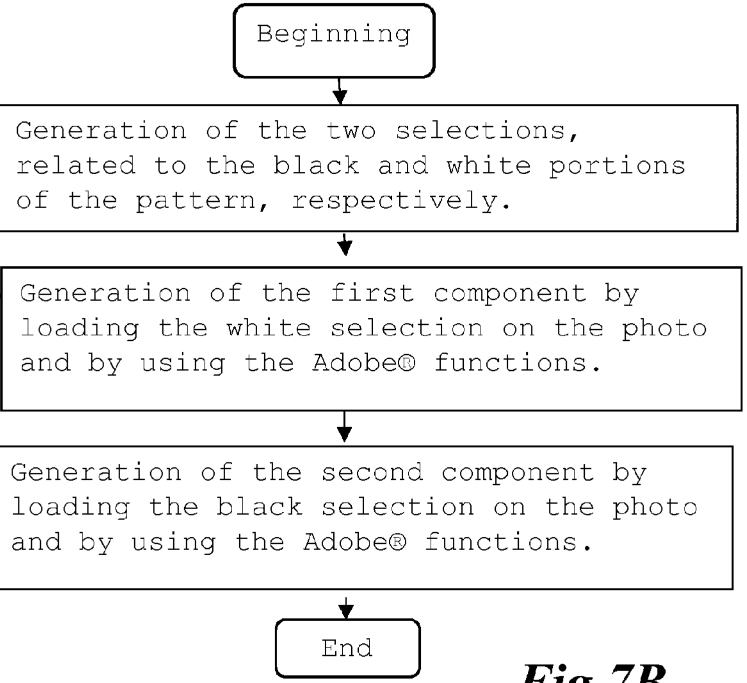
Beginning
710
Generation of the two selections, related to the black and white portions of the pattern, respectively.
720
Generation of the first component by loading the white selection on the photo and by using the Adobe® functions.
730
Generation of the second component by loading the black selection on the photo and by using the Adobe® functions.
End

Fig. 7B

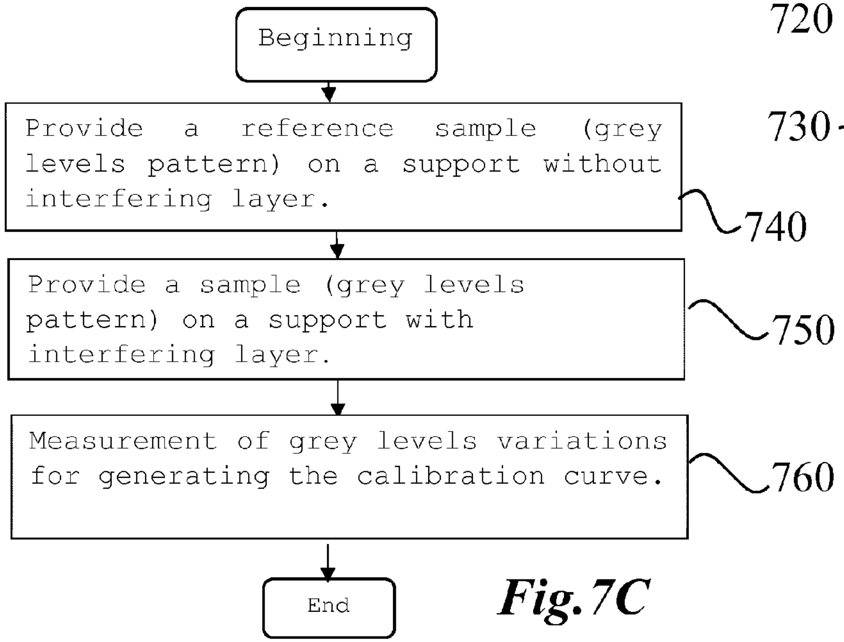
Beginning
Provide a reference sample (grey levels pattern) on a support without interfering layer.
740
Provide a sample (grey levels pattern) on a support with interfering layer.
750
Measurement of grey levels variations for generating the calibration curve.
760
End

Fig. 7C

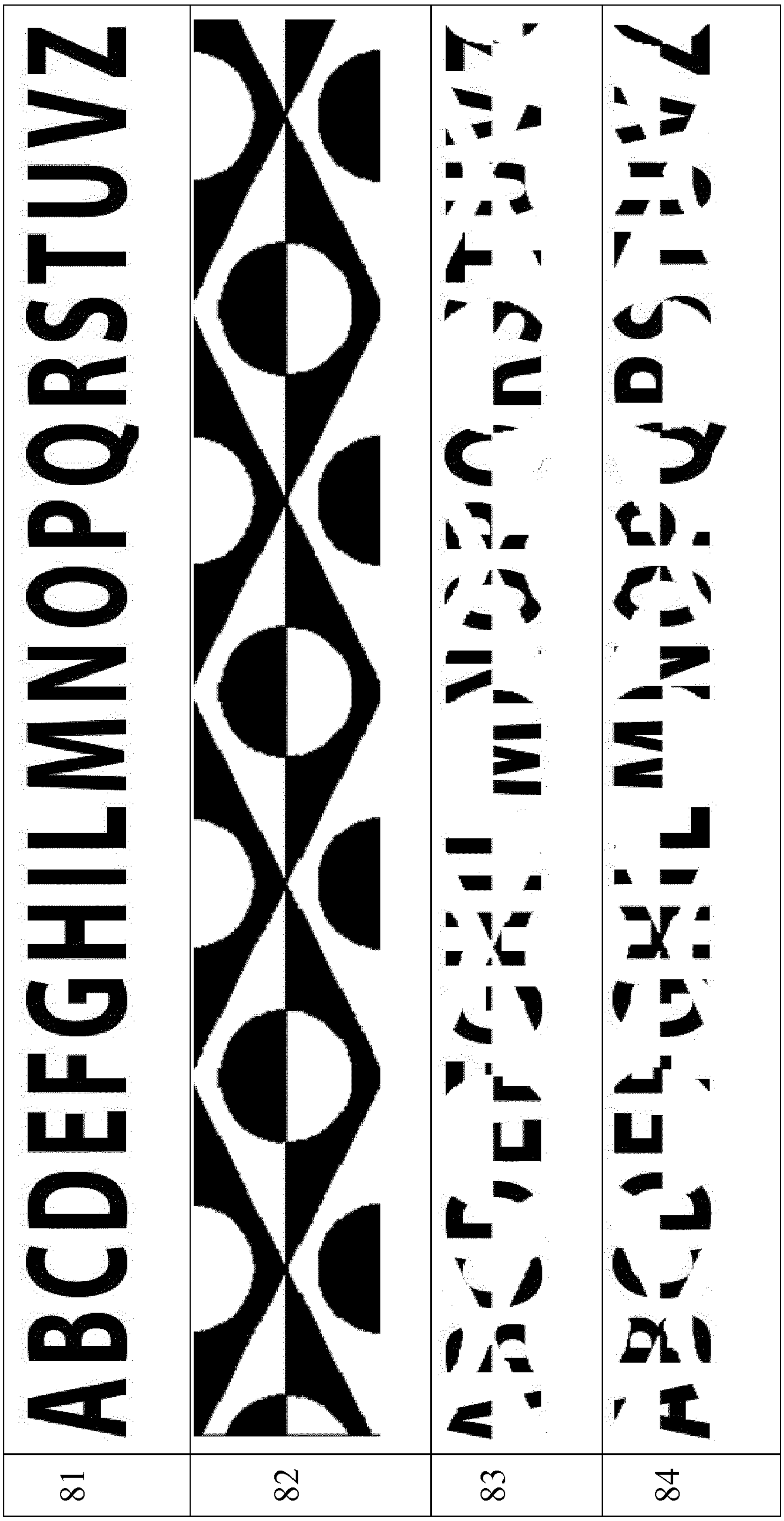

Fig.8

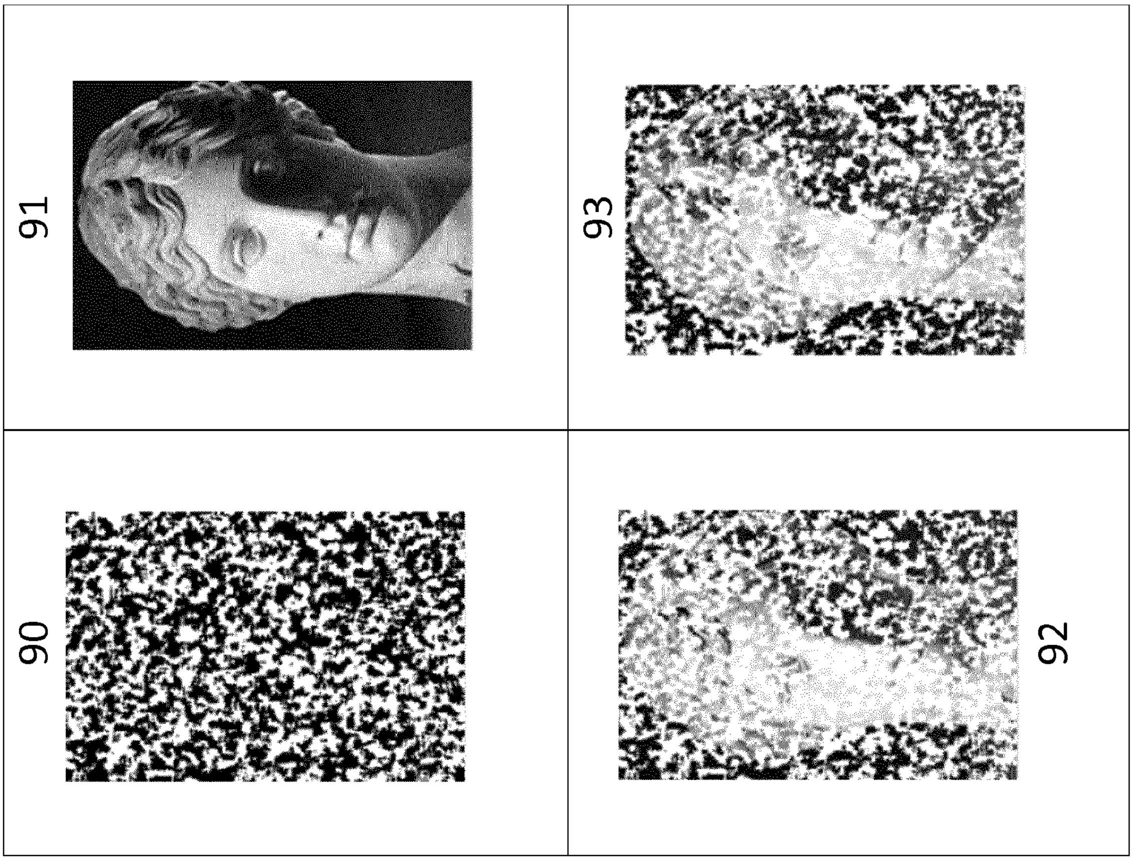

Fig.9

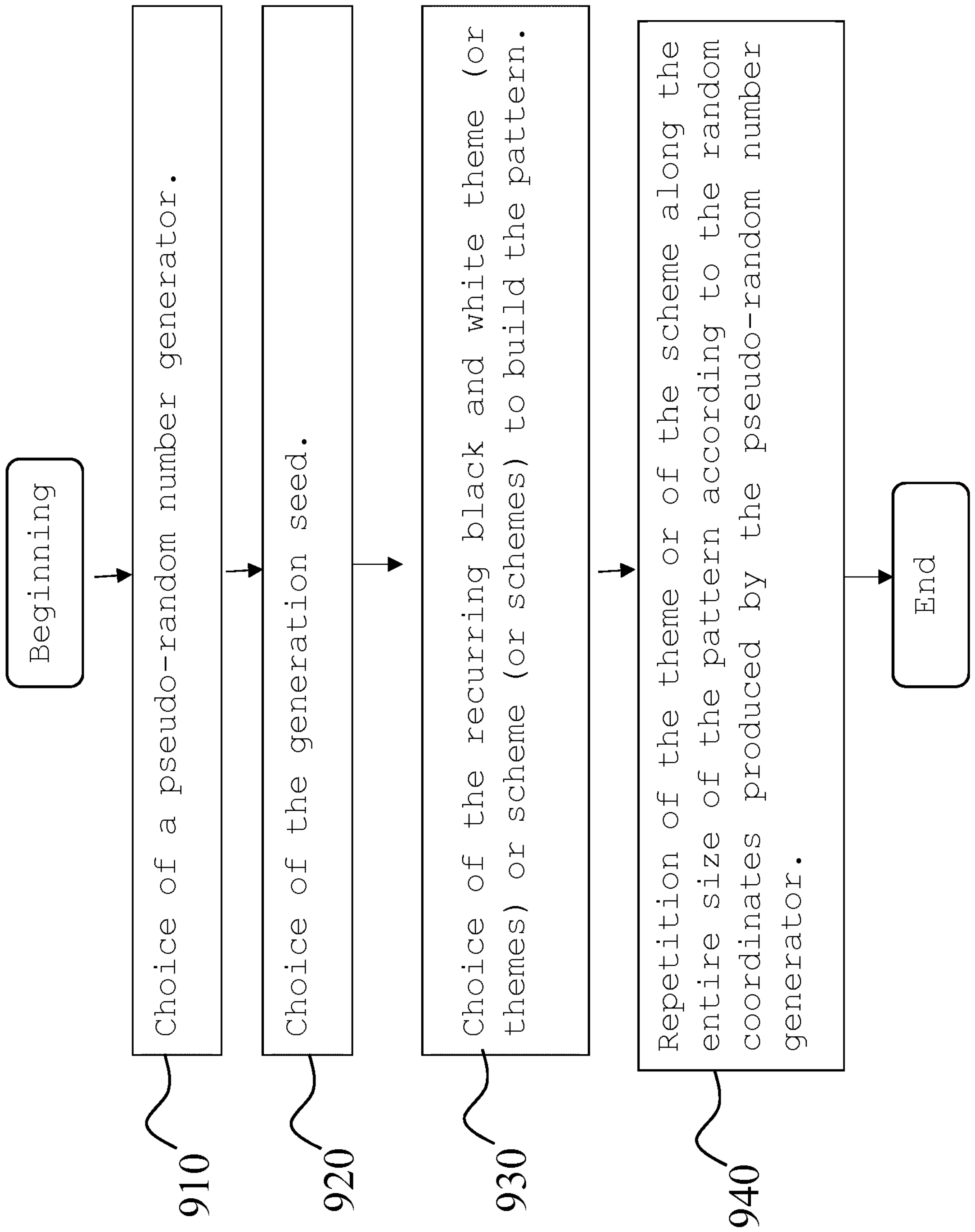
Beginning
Choice of a pseudo-random number generator.
910
Choice of the generation seed.
920
Choice of the recurring black and white theme (or themes) or scheme (or schemes) to build the pattern.
930
Repetition of the theme or of the scheme along the entire size of the pattern according to the random coordinates produced by the pseudo-random number generator.
940
End

Fig.9A

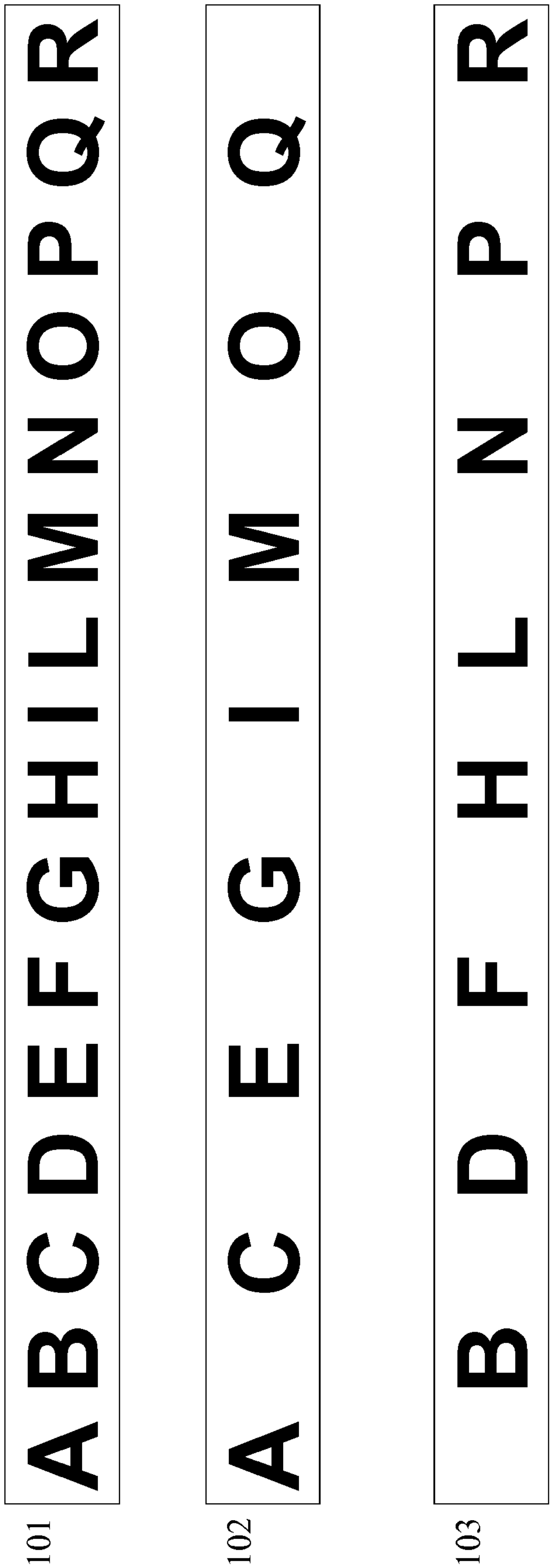

Fig.10

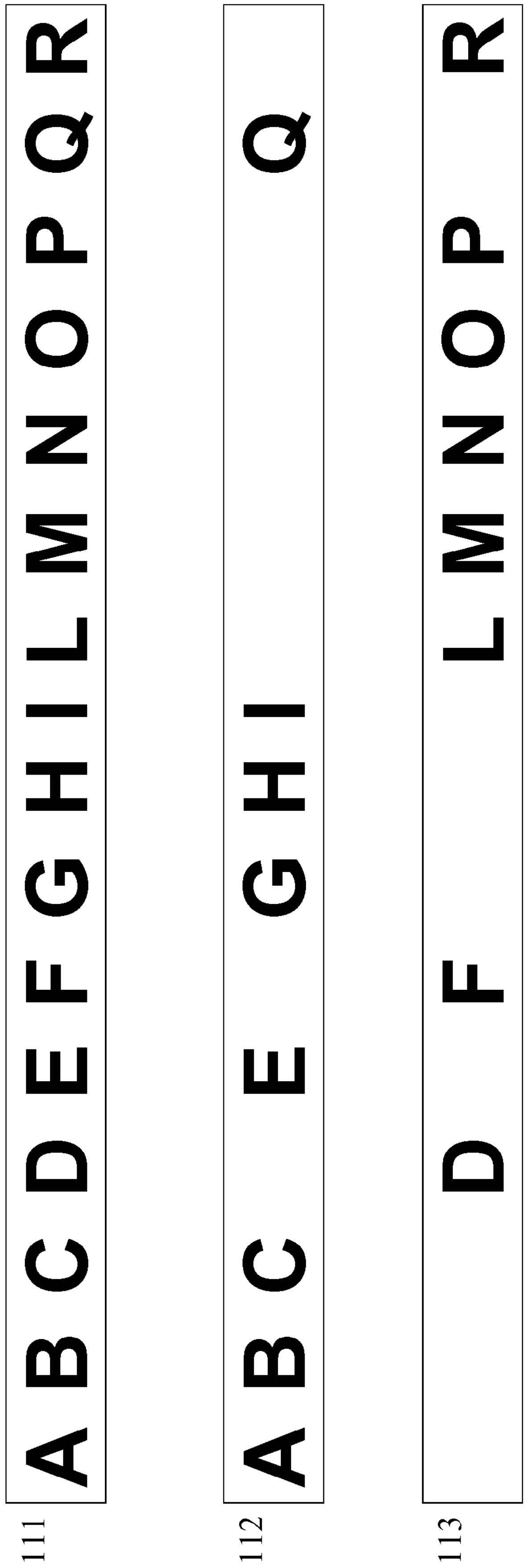

Fig.11

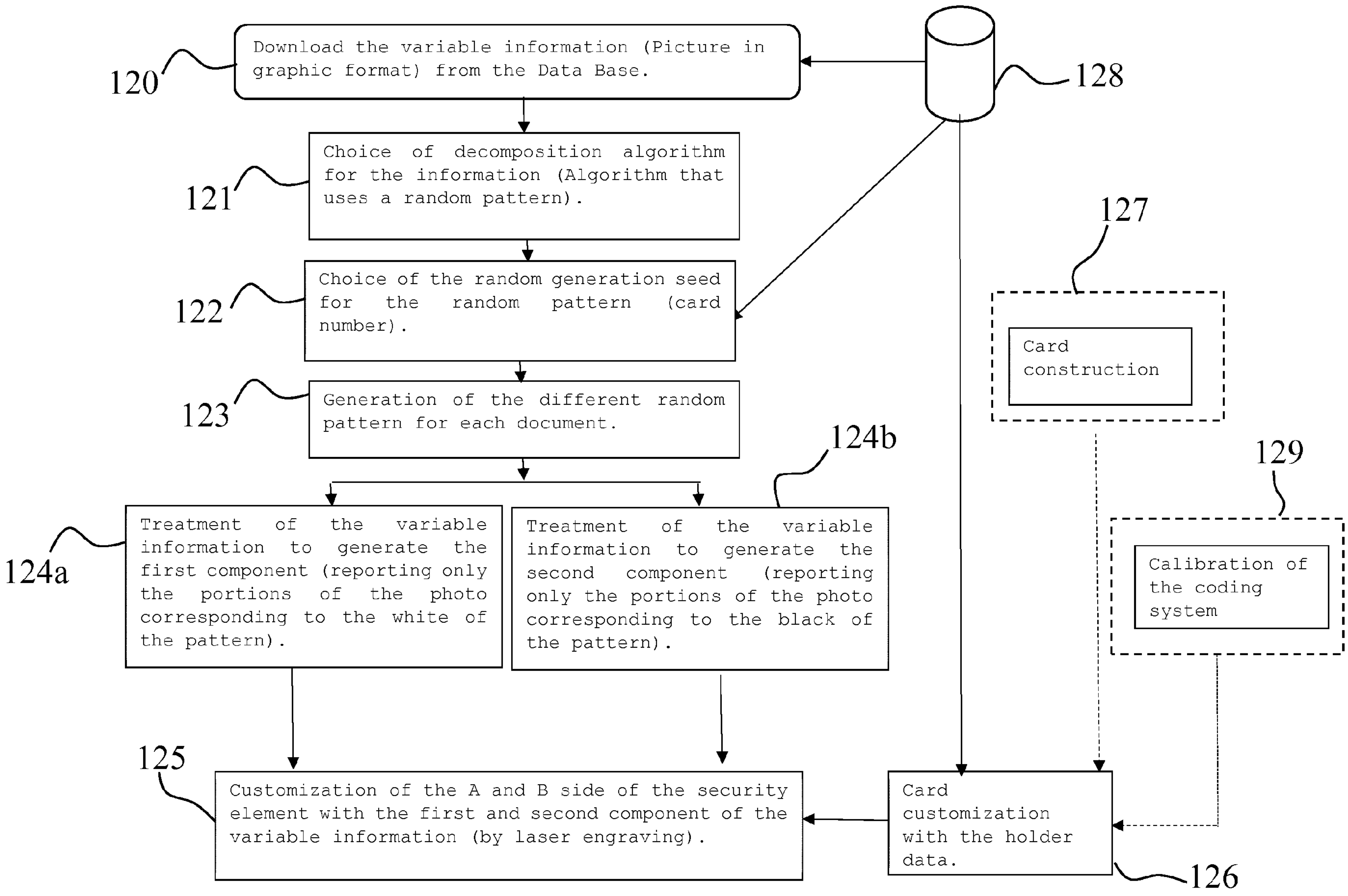
120
Download the variable information (Picture in graphic format) from the Data Base.
128
121
Choice of decomposition algorithm for the information (Algorithm that uses a random pattern).
127
122
Choice of the random generation seed for the random pattern (card number).
Card construction
123
Generation of the different random pattern for each document.
124b
129
124a
Treatment of the variable information to generate the first component (reporting only the portions of the photo corresponding to the white of the pattern).
Treatment of the variable information to generate the second component (reporting only the portions of the photo corresponding to the black of the pattern).
Calibration of the coding system
125
Customization of the A and B side of the security element with the first and second component of the variable information (by laser engraving).
Card customization with the holder data.
126

Fig. 12

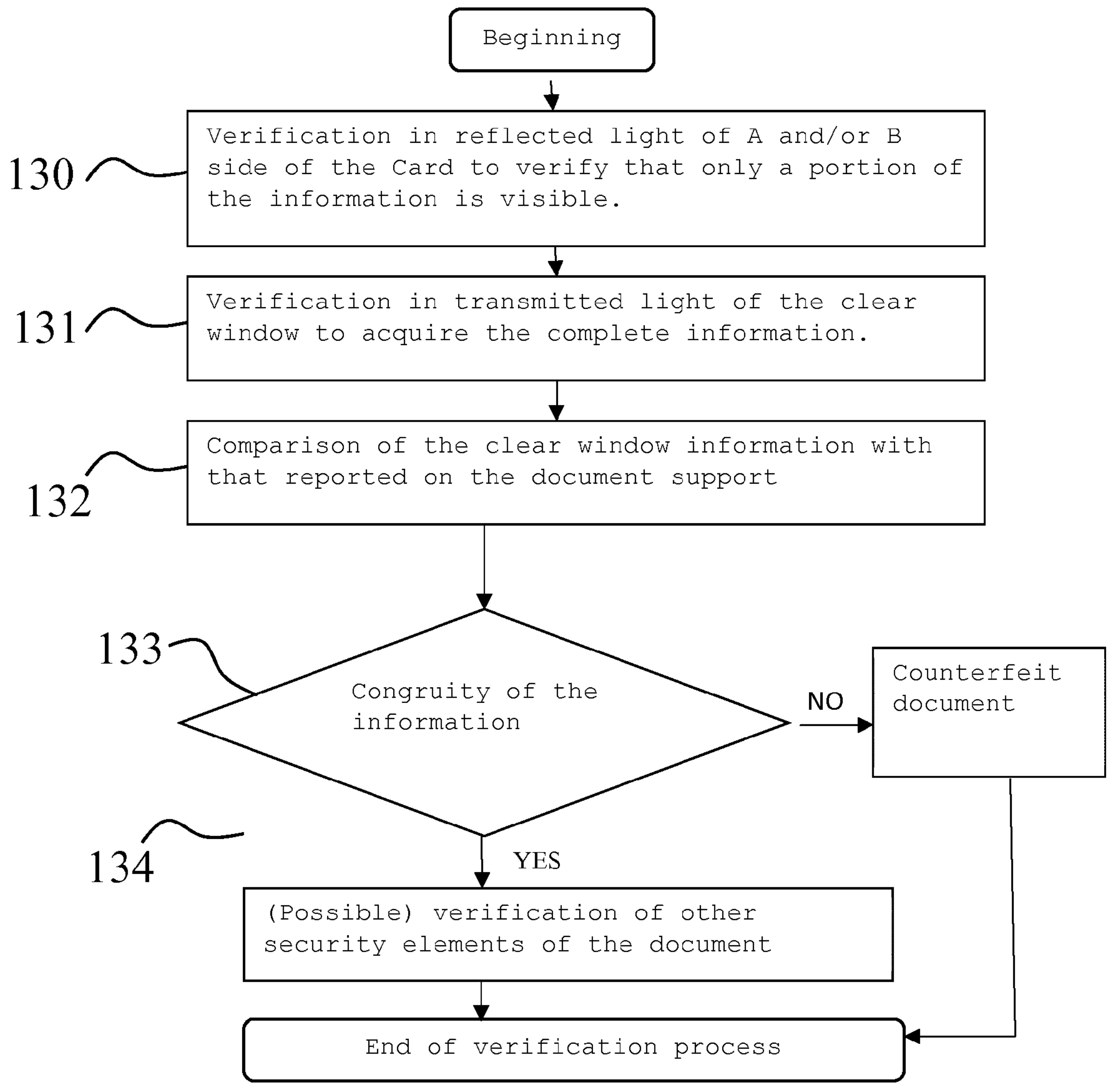
Beginning
130
Verification in reflected light of A and/or B side of the Card to verify that only a portion of the information is visible.
131
Verification in transmitted light of the clear window to acquire the complete information.
132
Comparison of the clear window information with that reported on the document support
133
Congruity of the information
NO
Counterfeit document
134
YES
(Possible) verification of other security elements of the document
End of verification process

Fig. 13

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 19 15 7723

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 2011/020537 A1 (MUEHLBAUER AG [DE]; WANJEK MICHAEL [DE]; BRUNNER ANTON [DE]) 24 February 2011 (2011-02-24) * page 12, line 24 - page 14, line 20; figures 1,2 * * page 15, line 27 - page 16, line 28; figure 6 * -----	1-25	INV. G07D7/00 B42D25/30 B42D25/29 B42D25/45 B42D25/328 B42D25/00
A	EP 2 559 563 A1 (POLSKA WYTWORNIA PAPIEROW WARTOSCIOWYCH S A [PL]) 20 February 2013 (2013-02-20) * paragraphs [0018] - [0029], [0034]; figures 1-5,10 * -----	1-25	
A	WO 97/47478 A1 (THOMAS DE LA RUE INTERNATIONAL [GB]; HOWLAND PAUL [GB]; DRINKWATER KEN) 18 December 1997 (1997-12-18) * page 5, lines 10-29 * * page 11, line 34 - page 16, line 10; figures 1-6 * -----	1-25	TECHNICAL FIELDS SEARCHED (IPC)
A	EP 1 415 828 A1 (XEROX CORP [US]) 6 May 2004 (2004-05-06) * paragraphs [0028] - [0038]; figures 1-8 * -----	1-25	G07D B42D G09F B41M
A	EP 0 628 408 A1 (ANDRIC DRAGISA [YU]; STOJANOVIC BORISLAV [YU]) 14 December 1994 (1994-12-14) * page 7, line 42 - page 9, line 15; figures 1,2 * -----	1-25	

The present search report has been drawn up for all claims

1

Place of search	Date of completion of the search	Examiner
Munich	11 April 2019	D'Incecco, Raimondo

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 19 15 7723

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-04-2019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011020537 A1	24-02-2011	DE 102009037832 A1	03-03-2011
		EP 2467266 A1	27-06-2012
		SG 178511 A1	27-04-2012
		WO 2011020537 A1	24-02-2011
EP 2559563 A1	20-02-2013	NONE	
WO 9747478 A1	18-12-1997	AU 723787 B2	07-09-2000
		AU 734937 B2	28-06-2001
		CA 2258251 A1	18-12-1997
		DE 19781815 B3	27-12-2012
		DE 19781815 T1	17-06-1999
		GB 2330111 A	14-04-1999
		GB 2350319 A	29-11-2000
		US 6089614 A	18-07-2000
		WO 9747478 A1	18-12-1997
EP 1415828 A1	06-05-2004	BR 0304759 A	31-08-2004
		CA 2447016 A1	30-04-2004
		EP 1415828 A1	06-05-2004
		MX PA03009920 A	19-04-2005
		US 2004084894 A1	06-05-2004
EP 0628408 A1	14-12-1994	AT 190554 T	15-04-2000
		AU 680882 B2	14-08-1997
		BG 62390 B1	29-10-1999
		BR 9405422 A	08-09-1999
		CA 2102271 A1	09-12-1994
		CN 1112359 A	22-11-1995
		CN 1254777 A	31-05-2000
		CN 1257787 A	28-06-2000
		CZ 289588 B6	13-02-2002
		CZ 289651 B6	13-03-2002
		CZ 289712 B6	13-03-2002
		DE 69328085 D1	20-04-2000
		DE 69328085 T2	16-11-2000
		DK 0628408 T3	14-08-2000
		EG 20711 A	29-12-1999
		EP 0628408 A1	14-12-1994
		ES 2145022 T3	01-07-2000
		FI 950529 A	05-04-1995
		HU 219008 B	29-01-2001
		JP 3164823 B2	14-05-2001
		JP H08501838 A	27-02-1996
		KR 100255715 B1	01-05-2000
		MY 131650 A	30-08-2007

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 19 15 7723

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-04-2019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		NO 301530 B1	10-11-1997
		NZ 262767 A	26-03-1996
		PL 180127 B1	29-12-2000
		PL 180252 B1	31-01-2001
		PL 307349 A1	15-05-1995
		PT 628408 E	29-09-2000
		RO 111921 B1	31-03-1997
		RU 2110408 C1	10-05-1998
		SG 52378 A1	28-09-1998
		SK 28995 A3	10-01-1996
		US 5449200 A	12-09-1995
		WO 9429105 A1	22-12-1994

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20080106091 A **[0005]**
- WO 2017092865 A **[0006]**
- WO 2016015130 A **[0007]**
- WO 2011020537 A **[0008]**
- EP 2559563 A1 **[0009]**

Non-patent literature cited in the description

- **ACHARYA ; RAY.** Image Processing: Principles and Applications. Wiley-Interscience, 2005 **[0154]**
- **RUSS.** The Image Processing Handbook. CRC, 2002 **[0154]**
- **A. MENEZES ; P, VAN OORSCHOT ; S. A. VANSTONE.** Handbook of Applied Cryptography. CRC Press, 1996 **[0154]**
- Mersenne Twister: A 623 - Dimensionally Equidistributed Uniform Pseudo -Random Number Generator MAKOTO MATSUMOTO Keio University and the Max-Planck-Institut fur Mathematik and TAKUJI NISHIMURA Keio University. *ACM Transactions on Modeling and Computer Simulation,* January 1998, vol. 8 (1 **[0154]**