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

(11) EP 2 559 563 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.03.2014 Bulletin 2014/13

(51) Int Cl.:
B42D 25/351 *(2014.01)* ***B41M 3/14*** *(2006.01)*
G07D 7/20 *(2006.01)*

(21) Application number: **11461534.7**

(22) Date of filing: **18.08.2011**

(54) **A security document with a see-through feature, and methods for manufacturing and authentication thereof**

Sicherheitsdokument mit durchsichtigem Merkmal und Verfahren zu dessen Herstellung und Authentifizierung

Document de sécurité avec fonction de visualisation et procédés de fabrication et d'authentification associés

(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

(43) Date of publication of application:
20.02.2013 Bulletin 2013/08

(73) Proprietor: **Polska Wytwornia Papierow Wartosciowych S.A.**
00-222 Warszawa (PL)

(72) Inventors:
- **Olszynska, Agata**
  00-222 Warszawa (PL)
- **Wojcik, Pawel**
  00-222 Warszawa (PL)
- **Chrzastowski, Szymon**
  00-222 Warszawa (PL)
- **Ziolkowski, Slawomir**
  00-222 Warszawa (PL)
- **Leszczynska-Ambroziewicz, Ewa**
  00-222 Warszawa (PL)

(74) Representative: **Pawlowski, Adam**
Eupatent.PL
ul. Zeligowskiego 3/5
90-752 Lodz (PL)

(56) References cited:
EP-A2- 1 775 932
DE-A1- 19 906 388
US-A- 3 827 726
US-A1- 2010 295 290

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 559 563 B1

Description

[0001] The present invention relates to security documents with a see-through security feature.

[0002] See-through security features, also known as recto-verso or look-through, are one of known counterfeit protection methods. A typical see-through security feature comprises two partial images applied on opposite sides of a semi-transparent substrate, which form a complete image when viewed in transmitted light. See-through security features are commonly applied to documents having a uniform semi-transparent substrate, such as a semi-transparent plastic or paper substrate printed at both sides.

[0003] A European patent EP0388090 "Sheet with security device" describes a sheet comprising a see-through feature, which is provided in a region of the sheet which is more transparent than a majority of the remainder of the sheet. The sheet has a paper substrate.

[0004] The aim of the present invention is to provide an improved security document with a see-through security feature. US 2010/0295290 discloses a security document having corresponding features to those of the preambles of claim 1 and claim 7, respectively.

[0005] The object of the invention is a method for manufacturing a security document by providing transparent external layers, at least one semi-transparent internal layer with a see-through area which is more transparent than the majority of the remainder of the document, laminating the layers to form the security document and applying to the document, before and/or after lamination of layers, personalized data and a see-through security feature in the see-through area, the see-through feature comprising a first partial image applied on one side of the at least one semi-transparent internal layer and a second partial image applied on the other side of the at least one semi-transparent internal layer, wherein the first and second partial images form a complete image when viewed in transmitted light. The method further comprises the steps of: before applying the see-through security feature obtaining the personalized data for the security document, obtaining the complete image for the see-through security feature, and dividing the complete image to the first partial image and to the second partial image using a function having a value dependent on at least part of the personalized data for the security document.

[0006] Preferably, the method further comprises the steps of, when dividing the complete image: generating a mask having a size of the complete image and comprising a plurality of regions using the function having a value dependent on at least part of the personalized data for the security document and assigning the regions of the complete image which coincide with the regions of the mask to the first partial image and the remaining regions to the second partial image.

[0007] Preferably, the function having a value dependent on at least part of the personalized data for the security document is a hash function.

[0008] Preferably, the complete image comprises at least part of the personalized data for the security document.

[0009] Preferably, the see-through security feature is applied by ink jet printing before lamination.

[0010] Preferably, the see-through security feature is applied by laser engraving after lamination.

[0011] The object of the invention is also a security document having a form of a laminate of transparent external layers and at least one semi-transparent internal layer with a see-through area which is more transparent than the majority of the remainder of the document, wherein a see-through security feature is applied in the see-through area, the see-through feature comprising a first partial image applied on one side of the at least one semi-transparent internal layer and a second partial image applied on the other side of the at least one semi-transparent internal layer, wherein the first and second partial images form a complete image when viewed in transmitted light, and wherein the security document comprises personalized data, wherein the fragmentation of the complete image to the first and second partial images is having a value dependent on at least part of the personalized data comprised in the security document.

[0012] Preferably, at least one semi-transparent internal layer comprises a first internal layer of a first transparency with an opening corresponding to the see-through area and a second semi-transparent layer of a second transparency, higher than the first transparency.

[0013] Preferably, the first internal layer of the first transparency is opaque.

[0014] Preferably, the document further comprises an integrated circuit chip with memory in which there is stored a definition of the function on which the fragmentation of the complete image is dependent and/or a mask for verifying the authenticity of the fragmentation of the complete image and/or the first and second partial images and/or the complete image.

[0015] The object of the invention is also a method for authenticating a security document in a form of a laminate of transparent external layers and at least one semi-transparent internal layer with a see-through area which is more transparent than the majority of the remainder of the document, wherein a see-through security feature is applied in the see-through area, the see-through feature comprising a first partial image applied on one side of the at least one semi-transparent internal layer and a second partial image applied on the other side of the at least one semi-transparent internal layer, wherein the first and second partial images form a complete image when viewed in transmitted light, and wherein the security document comprises personalized data. The method comprises the steps of: obtaining at least part of the personalized data of the security document, generating a mask having a size of the complete image and comprising a plurality of regions, using a function having a value dependent on the obtained at least part of the personal-

ized data and verifying whether the first partial image and/or the second partial image are compliant with the generated mask.

[0016] The object of the invention is also a device for authenticating a security document in a form of a laminate of transparent external layers and at least one semi-transparent internal layer with a see-through area which is more transparent than the majority of the remainder of the document, wherein a see-through security feature is applied in the see-through area, the see-through feature comprising a first partial image applied on one side of the at least one semi-transparent internal layer and a second partial image applied on the other side of the at last one semi-transparent internal layer, wherein the first and second partial images form a complete image when viewed in transmitted light, and wherein the security document comprises personalized data. The device comprises a document reader configured to obtain at least part of the personalized data of the security document, as well as the first partial image and/or the second partial image and a verification module configured to generate a mask having a size of the complete image and comprising a plurality of regions, using a function having a value dependent on the obtained at least part of the personalized data and to verify whether the first partial image and/or the second partial image are compliant with the generated mask.

[0017] The object of the invention is shown by way of exemplary embodiments on a drawing, in which:

Fig. 1 shows a top view of the security document,
Fig. 2 shows an assembly view of one exemplary embodiment of the security document,
Fig. 3 shows an assembly view of another exemplary embodiment of the security document,
Fig. 4 shows the steps of a first embodiment of the method according to the invention,
Fig. 5 shows the steps of a second embodiment of the method according to the invention,
Figs. 6-9 show examples of separation of a complete image to a first and to a second partial image using a mask having a value dependent on personalized data,
Fig. 10 shows a structure of a device for authenticating a security document.

[0018] Fig. 1 shows a top view of the security document according to the invention, which may have a form of a plastic card 100 with a dimensions of e.g. approximately 8 cm x 5 cm and with an integrated circuit chip 124 with data 123 stored therein and with a plurality of standard identification elements related to personalized data, such as a photo 121 of a face, embossed, printed and/or engraved name and an ID number 122 of the document holder. As shown in Figs. 2 and 3, the document is a laminate of transparent external layers 101, 102 and at least one semi-transparent internal layer 104 with a see-through area 110 which is more transparent than the majority of the remainder of the document. The see-through area 110 has a see-through security feature comprising a first partial image 111 applied on one side of the at least one semi-transparent internal layer 104 and a second partial image 112 applied on the other side of the at least one semi-transparent internal layer 104, wherein the first partial image 111 and the second partial image 112 form a complete image 113 when viewed in transmitted light.

[0019] Fig. 2 shows an assembly view of one exemplary embodiment of the security document. The document is a laminate of plastic layers. The embodiment shown in Fig. 2 comprises transparent layers 101, 102, between which there is an internal layer 103 of a first transparency with an opening 110 corresponding to the see-through area and a second semi-transparent layer 104 of a second transparency, higher than the first transparency. Preferably, the internal layer 103 of a first transparency is opaque. The first and second partial images 111, 112 can be applied by laser engraving the opposite sides of the semi-transparent layer 104 after lamination of the layers.

[0020] Fig. 3 shows an assembly view of another exemplary embodiment of the security document. The document is a laminate of plastic layers. The embodiment shown in Fig. 3 is similar to that shown in Fig. 2, but it comprises two additional transparent or semi-transparent layers 105, 106 located at opposite sides of the semi-transparent layer 104. The total transparency of the layers 104, 105, 106 should be higher than the total transparency of layers 103, 104, 105, 106, such that the transparency of the area 110 is higher than the transparency of the remaining portion of the document. The see-through security feature can be is applied by ink jet printing the first image and the second image on layers 105, 106 before lamination of the layers. It can be also applied by laser engraving of a laminated document, or by any other method applicable for applying see-through security features. The first partial image 111 (e.g. the recto image) can be applied by using different print or engraving parameters than the second partial image 112 (e.g. the verso image) in order to achieve similar shades of the complete image 113 when viewed in transmitted light.

[0021] The total transparency of all layers in the see-through area 110 should be such as to allow the see-through feature to be seen in certain light conditions.

[0022] The layers 101-106 can be made of materials typical to plastic card laminates, such as polycarbonate, polyvinyl chloride and/or polyester.

[0023] The definition of the function, the mask image 114, the partial images 111, 112 and/or the complete image 113 can be stored in the integrated circuit chip 124, which facilitates verification of the security document.

[0024] Fig. 4 shows the steps of a first embodiment of the method according to the invention. First, in step 201 at least part of personalized data for applying to the document 100 is obtained, such as a name of the document holder, a personal ID number, a date of issuance of the

document, a photo etc. Next, in step 202 a complete see-through image is obtained. The complete see-through image can be common for a group of documents, for example it can be a country code, a document type, a common symbol, year of issuance etc. Alternatively, the complete see-through image can be personalized and include a personal ID number, a name, a surname, a photo etc. Exemplary complete see-through images 113 are shown in Figs. 6-9. Next, a mask image 114 is generated in step 203 as a function of the at least part of personalized data. The mask image 114 has the size of the complete see-through image 113 and comprises a plurality of regions 115 generated as a function having a value dependent on the at least part of the personalized data 121-123 for the security document.

[0025] For example, the function can be a hash function for the card holder's name. The hash function should generate substantially unique outputs for unique personalized data. For example, an MD5 hash function can generate a 128-bit hash value, which guarantees with a very high probability that all card holder names will be assigned different hash values.

[0026] The hash value can be used to generate a mask. As a simple example, shown with reference to Fig. 6, the MD5 hash value for personalized data = "JOHN SMITH" is (in a hexadecimal form) "f3c686cf530baf2269e7442163cb602e". The individual bits of the hash value can be used to define the regions of the mask image. For example, the mask image 114 can be divided into 4x4 squares and the consecutive squares can be defined as active/inactive depending on the value (1/0) of the first 16 bits of the hash value (which in this example is "F3C6" = "1111001111000110"), as shown in the example of Fig. 6. In practice, more bits of the 128-bit MD5 hash value should be used, or even longer hash value should be used, in order to guarantee uniqueness of the mask.

[0027] In step 204, the first partial image 111 and the second partial image 112 are generated, by overlaying the mask 114 on the complete image 113. The regions of the complete image 113 which coincide with the regions of the mask can be assigned to the first partial image 111 and the remaining regions can be assigned to the second partial image 112.

[0028] Next, blank layers 101-106 are provided in step 205. The personalized data 121-123 and the partial see-through images 111, 112 are applied in step 206, for example by Ink-jet method. Then, the layers are laminated in step 207.

[0029] Fig. 5 shows the steps of a second embodiment of the method according to the invention. Steps 211-214 are equivalent to steps 201-204 of the method shown in Fig. 4. In step 215, a blank or partially personalized laminate is provided. In step 216, the see-through images and optionally the rest of the personalized data are applied to the laminate, for example by laser engraving.

[0030] Figs. 7-9 show further exemplary embodiments of masks 114 applied to exemplary complete images 113 and resulting partial images 111, 112.

[0031] Fig. 7 shows an example, wherein the mask 114 comprises a plurality of rectangles, wherein the top-left corner point and the bottom-right corner points are defined by the function having a value dependent on at least part of the personalized data. In order to avoid a situation where a large rectangle would cover most of the mask region, the maximum size of the rectangle is limited.

[0032] Fig. 8 shows an example, wherein the mask 114 comprises a plurality of regions obtained by drawing lines having coordinates defined by the function having a value dependent on at least part of the personalized data and active regions selected in areas between the lines.

[0033] Fig. 9 shows an example, wherein the mask 114 comprises a plurality of regions obtained by drawing ellipses having center points and radii defined by the function having a value dependent on at least part of the personalized data.

[0034] Fig. 10 shows a structure of a device for authenticating the security document according to the invention. The device comprises a document reader 301 configured to obtain at least part of the personalized data 121-123 of the security document (for example by an optical reader or an IC chip interface), as well as the first partial image 111 and/or the second partial image 112 (for example by an optical reader). A verification module 302 is configured to generate a mask 114 having a size of the complete image 113 and comprising a plurality of regions 115, as a function having a value dependent on the obtained at least part of the personalized data 121-123 and to verify whether the first partial image 111 and/or the second partial image 112 are compliant with the generated mask 114. The mask 114 can be generated by a mask generator 304 on the basis of the value of the hash function 303, wherein the mask generator 304 receives the personalized data 121-123 from the document reader 301. The hash function 303 and the mask generator 304 operate in the same manner as corresponding units in the system for manufacturing the card. The verification can be performed by an image comparator 305 receiving as input the mask 114 from the mask generator 304 and the partial images 111, 112 from the document reader 301 and providing an output determining whether the images overlap or not.

[0035] The security document with a see-through security feature is improved in that the see-through security feature is personalized not only by applying personalized data in the see-through area, but also by personalized method of generating the regions which belong to the first and second partial images. In order to falsify the security document according to the invention by changing the personalized data, the see-through security feature should be changed as well. This not only requires additional manipulation within the see-through area, but knowledge of the function having a value dependent on the personalized data as well, in case when the hash function is not stored on the card chip. Therefore, the see-through security feature according to the invention

can be used for authenticating the document and for verifying the data contained therein.

Claims

1. A method for manufacturing a security document by providing transparent external layers (101, 102), at least one semi-transparent internal layer (103-106) with a see-through area (110) which is more transparent than the majority of the remainder of the document, laminating the layers (101-106) to form the security document and applying to the document, before and/or after lamination of layers (101-106), personalized data (121-123) and a see-through security feature in the see through area (110), the see-through feature comprising a first partial image (111) applied on one side of the at least one semi-transparent internal layer (104) and a second partial image (112) applied on the other side of the at least one semi-transparent internal layer (104), wherein the first and second partial images (111, 112) form a complete image (113) when viewed in transmitted light, the method **characterized by** further comprising the steps of: before applying the see-through security feature: obtaining the personalized data (121-123) for the security document, obtaining the complete image (113) for the see-through security feature, and dividing the complete image (113) to the first partial image (111) and to the second partial image (112) using a function having a value dependent on at least part of the personalized data (121-123) for the security document.

2. The method according to claim 1, further comprising the steps of: when dividing the complete image: generating a mask (114) having a size of the complete image and comprising a plurality of regions (115) using the function having a value dependent on at least part of the personalized data (121-123) for the security document and assigning the regions (115) of the complete image (113) which coincide with the regions of the mask to the first partial image (111) and the remaining regions to the second partial image (112).

3. The method according to any of previous claims, wherein the function having a value dependent on at least part of the personalized data (121-123) for the security document is a hash function.

4. The method according to any of previous claims, wherein the complete image (113) comprises at least part of the personalized data (121-123) for the security document.

5. The method according to any of previous claims, wherein the see-through security feature is applied by ink jet printing before lamination.

6. The method according to any of previous claims, wherein the see-through security feature is applied by laser engraving after lamination.

7. A security document having a form of a laminate of transparent external layers (101, 102) and at least one semi-transparent internal layer (103-106) with a see-through area (110) which is more transparent than the majority of the remainder of the document, wherein a see-through security feature is applied in the see-through area (110), the see-through feature comprising a first partial image (111) applied on one side of the at least one semi-transparent internal layer (104) and a second partial image (112) applied on the other side of the at least one semi-transparent internal layer (104), wherein the first and second partial images (111, 112) form a complete image (113) when viewed in transmitted light, and wherein the security document comprises personalized data (121-123) **characterized in that** the division of the complete image (113) into the first and second partial images (111, 112) is dependent on at least part of the personalized data (121-123) comprised in the security document.

8. The security document according to claim 7, wherein the at least one semi-transparent internal layer comprises a first internal layer (103) of a first transparency with an opening corresponding to the see-through area (110) and a second semi-transparent layer (104) of a second transparency, higher than the first transparency.

9. The security document according to claim 8, wherein the first internal layer (103) of the first transparency is opaque.

10. The security document according to any of claims 7-9, further comprising an integrated circuit chip (124) with memory in which there is stored a definition of the function on which the fragmentation of the complete image (113) is dependent and/or a mask (114) for verifying the authenticity of the fragmentation of the complete image (113) and/or the first and second partial images (111, 112) and/or the complete image (113).

11. A method for authenticating the security document of any one of claims 7-10 : the method **characterized by** comprising the steps of:

    - obtaining at least part of the personalized data (121-123) of the security document,
    - generating a mask (114) having a size of the complete image (113) and comprising a plurality of regions (115), using a function having a value

dependent on the obtained at least part of the personalized data (121-123),
- verifying whether the first partial image (111) and/or the second partial image (112) are compliant with the generated mask (114).

12. A device for authenticating the security document of any one of claims 7-10 the device **characterized by** comprising:

- a document reader (301) configured to obtain at least part of the personalized data (121-123) of the security document, as well as the first partial image (111) and/or the second partial image (112),
- a verification module (302) configured to generate a mask (114) having a size of the complete image (113) and comprising a plurality of regions (115), using a function having a value dependent on the obtained at least part of the personalized data (121-123) and to verify whether the first partial image (111) and/or the second partial image (112) are compliant with the generated mask (114).

Patentansprüche

1. Verfahren zum Herstellen eines Sicherheitsdokumentes durch Bereitstellen von transparenten externen Schichten (101, 102), mindestens einer halbtransparenten internen Schicht (103-106) mit einer Durchsichtsfläche (110), die transparenter als der größte Rest des Dokumentes, Laminieren der Schichten (101-106), um das Sicherheitsdokument zu bilden, und, vor und/oder nach dem Laminieren der Schichten (101-106), Aufbringen von personalisierten Daten (121-123) und eines Durchsichtssicherheitsmerkmals in der Durchsichtsfläche (110) auf das Dokument, wobei das Durchsichtsmerkmal ein erstes Teilbild (111) umfasst, das auf eine Seite der mindestens einen halbtransparenten internen Schicht (104) aufgebracht ist, und ein zweites Teilbild (112), das auf die andere Seite der mindestens einen halbtransparenten internen Schicht (104) aufgebracht ist, wobei das erste und zweite Teilbild (111, 112) ein vollständiges Bild (113) bilden, wenn es im Durchlicht betrachtet wird, wobei das Verfahren **dadurch gekennzeichnet ist, dass** es die folgenden Schritte umfasst: Vor dem Aufbringen des Durchsichtssicherheitsmerkmals: Erhalten der personalisierten Daten (121-123) für das Sicherheitsdokument, Erhalten des vollständigen Bildes (113) für das Durchsichtssicherheitsmerkmals und Teilen des vollständigen Bildes (113) in das erste Teilbild (111) und in das zweite Teilbild (112) unter Verwendung einer Funktion, die einen Wert hat, welcher von mindestens einem Teil der personalisierten Daten (121-123) für das Sicherheitsdokument abhängt.

2. Verfahren nach Anspruch 1, das ferner die folgenden Schritte umfasst: Beim Teilen des vollständigen Bildes: Erzeugen einer Maske (114), die eine Größe des vollständigen Bildes hat und mehrere Bereiche (115) umfasst, unter Verwendung der Funktion, die einen Wert hat, welcher zumindest von einem Teil der personalisierten Daten (121-123) für das Sicherheitsdokument abhängt, und Zuweisen der Bereiche (115) des vollständigen Bildes (113), die mit den Bereichen der Maske übereinstimmen, zum ersten Teilbild (111) und der restlichen Bereiche zum zweiten Teilbild (112).

3. Verfahren nach einem der vorherigen Ansprüche, wobei die Funktion, die einen Wert hat, welcher zumindest von einem Teil der personalisierten Daten (121-123) für das Sicherheitsdokument abhängt, eine Hash-Funktion ist.

4. Verfahren nach einem der vorherigen Ansprüche, wobei das vollständige Bild (113) mindestens einen Teil der personalisierten Daten (121-123) für das Sicherheitsdokument umfasst.

5. Verfahren nach einem der vorherigen Ansprüche, wobei das Durchsichtssicherheitsmerkmal durch Tintenstrahldruck vor dem Laminieren aufgebracht wird.

6. Verfahren nach einem der vorherigen Ansprüche, wobei das Durchsichtssicherheitsmerkmal durch Lasergravur nach dem Laminieren aufgebracht wird.

7. Sicherheitsdokument, das eine Form eines Laminats von transparenten externen Schichten (101, 102) und mindestens eine halbtransparente interne Schicht (103-106) mit einer Durchsichtsfläche (110) hat, welche transparenter als größte Teil des Restes des Dokumentes ist, wobei ein Durchsichtssicherheitsmerkmal auf die Durchsichtsfläche (110) aufgebracht wird, wobei das Durchsichtsmerkmal ein erstes Teilbild (111) umfasst, welches auf eine Seite der mindestens einen halbtransparenten internen Schicht (104) aufgebracht ist, und ein zweites Teilbild (112) umfasst, das auf die andere Seite der mindestens einen halbtransparenten internen Schicht (104) aufgebracht ist, wobei das erste und zweite Teilbild (111, 112) ein vollständiges Bild (113) bilden, wenn es im Durchlicht betrachtet wird, und wobei das Sicherheitsdokument personalisierte Daten (121-123) umfasst, **dadurch gekennzeichnet, dass** das Aufteilen des vollständigen Bildes (113) in das erste und zweite Teilbild (111, 112) zumindest teilweise von den personalisierten Daten (121-124) abhängt, die im Sicherheitsdokument enthalten sind.

8. Sicherheitsdokument nach Anspruch 7, wobei die mindestens eine halbtransparente interne Schicht eine erste interne Schicht (103) einer ersten Transparenz mit einer Öffnung umfasst, die der Durchsichtsfläche (110) entspricht, und die eine zweite halbtransparente Schicht (104) einer zweiten Transparenz umfasst, die größer als die erste Transparenz ist.

9. Sicherheitsdokument nach Anspruch 8, wobei die erste interne Schicht (103) der ersten Transparenz lichtundurchlässig ist.

10. Sicherheitsdokument nach einem der Ansprüche 7-9, das ferner eine integrierte Schaltung (124) mit Speicher umfasst, in dem eine Definition der Funktion gespeichert ist, von der die Fragmentierung des vollständigen Bildes (113) abhängig ist, und/oder eine Maske (114) zum Überprüfen der Echtheit der Fragmentierung des vollständigen Bildes (113) und/oder das erste und zweite Teilbild (111, 112) und/oder das vollständige Bild (113).

11. Verfahren für die Authentifizierung des Sicherheitsdokumentes nach einem der Ansprüche 7-10, wobei das Verfahren **dadurch gekennzeichnet ist, dass** es folgende Schritte umfasst:

    - Erhalten von mindestens einem Teil der personalisierten Daten (121-123) des Sicherheitsdokumentes,
    - Erzeugen einer Maske (114), die eine Größe des vollständigen Bildes (113) hat und mehrere Bereiche (115) umfasst, unter Verwendung einer Funktion, die einen Wert hat, welcher zumindest von einem Teil der erhaltenen personalisierten Daten (121-123) abhängt,
    - Überprüfen, ob das erste Teilbild (111) und/oder das zweite Teilbild (112) mit der erzeugten Maske (114) konform sind.

12. Vorrichtung zum Authentifizieren des Sicherheitsdokumentes nach einem der Ansprüche 7-10, wobei die Vorrichtung **dadurch gekennzeichnet ist, dass** sie Folgendes umfasst:

    - ein Dokumentenlesegerät (301), das zum Gewinnen zumindest eines Teils der personalisierten Daten (121-123) des Sicherheitsdokumentes ausgelegt ist, sowie des ersten Teilbildes (111) und/oder des zweiten Teilbildes (112),
    - ein Überprüfungsmodul (302), das zum Erzeugen einer Maske (114), welche eine Größe des vollständigen Bildes (113) hat und mehrere Bereiche (115) umfasst, unter Verwendung einer Funktion ausgelegt ist, die einen Wert hat, welcher zumindest von dem gewonnenen Teil der personalisierten Daten (121-123) abhängig ist, und zum Überprüfen, ob das erste Teilbild (111) und/oder das zweite Teilbild (112) mit der erzeugten Maske (114) konform sind.

Revendications

1. Procédé de fabrication d'un document de sécurité par la fourniture de couches externes transparentes (101, 102), d'au moins une couche interne semi-transparente (103-106) avec une zone translucide (110) qui est plus transparente que la majorité du reste du document, la stratification des couches (101-106) pour former le document de sécurité et l'application au document, avant et/ou après la stratification de couches (101-106), de données personnalisées (121-123) et d'une caractéristique de sécurité translucide dans la zone translucide (110), la caractéristique translucide comprenant une première image partielle (111) appliquée sur un côté de l'au moins une couche interne semi-transparente (104) et une deuxième image partielle (112) appliquée sur l'autre côté de l'au moins une couche interne semi-transparente (104), dans lequel les première et deuxième images partielles (111, 112) forment une image complète (113) lorsqu'elles sont visualisées à une lumière transmise, le procédé étant **caractérisé en ce qu'**il comprend en outre les étapes de : avant l'application de la caractéristique de sécurité translucide, l'obtention des données personnalisées (121-123) pour le document de sécurité, l'obtention de l'image complète (113) pour la caractéristique de sécurité translucide, et la division de l'image complète (113) en la première image partielle (111) et la deuxième image partielle (112) en utilisant une fonction ayant une valeur dépendant d'au moins une partie des données personnalisées (121-123) pour le document de sécurité.

2. Procédé selon la revendication 1, comprenant en outre les étapes de : lors de la division de l'image complète, la génération d'un masque (114) ayant une taille de l'image complète et comprenant une pluralité de régions (115) utilisant la fonction ayant une valeur dépendant d'au moins une partie des données personnalisées (121-123) pour le document de sécurité et l'affectation des régions (115) de l'image complète (113) qui coïncident avec les régions du masque à la première image partielle (111) et des régions restantes à la deuxième image partielle (112).

3. Procédé selon l'une quelconque des revendications précédentes, dans lequel la fonction ayant une valeur dépendant d'au moins une partie des données personnalisées (121-123) pour le document de sécurité est une fonction de la hachage.

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'image complète (113) comprend au moins une partie des données personnalisées (121-123) pour le document de sécurité.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel la caractéristique de sécurité translucide est appliquée par impression à jet d'encre avant la stratification.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel la caractéristique de sécurité translucide est appliquée par gravage laser après la stratification.

7. Document de sécurité ayant une forme d'une stratification de couches externes transparentes (101, 102) et d'au moins une couche interne semi-transparente (103-106) avec une zone translucide (110) qui est plus transparente que la majorité du reste du document, dans lequel une caractéristique de sécurité translucide est appliquée dans la zone translucide (110), la caractéristique translucide comprenant une première image partielle (111) appliquée sur un côté de l'au moins une couche interne semi-transparente (104) et une deuxième image partielle (112) appliquée sur l'autre côté de l'au moins une couche interne semi-transparente (104), dans lequel les première et deuxième images partielles (111, 112) forment une image complète (113) lorsqu'elles sont visualisées à une lumière transmise, et dans lequel le document de sécurité comprend des données personnalisées (121-123), **caractérisé en ce que** la division de l'image complète (113) en la première image partielle (111) et la deuxième image partielle (112) dépend d'au moins une partie des données personnalisées (121-123) comprises dans le document de sécurité.

8. Document de sécurité selon la revendication 7, dans lequel l'au moins une couche interne semi-transparente comprend une première couche interne (103) d'une première transparence avec une ouverture correspondant à la zone translucide (110) et une deuxième couche semi-transparente (104) d'une deuxième transparence supérieure à la première transparence.

9. Document de sécurité selon la revendication 8, dans lequel la première couche interne (103) de la première transparence est opaque.

10. Document de sécurité selon l'une quelconque des revendications 7 à 9, comprenant en outre une puce de circuits intégrés (124) avec une mémoire dans laquelle est mémorisée une définition de la fonction de laquelle dépend la fragmentation de l'image complète (113) et/ou un masque (114) pour vérifier l'authenticité de la fragmentation de l'image complète (113) et/ou des première et deuxième images partielles (111, 112) et/ou de l'image complète (113).

11. Procédé d'authentification du document de sécurité selon l'une quelconque des revendications 7 à 10, le procédé étant **caractérisé en ce qu'**il comprend les étapes de :

- l'obtention d'au moins une partie des données personnalisées (121-123) du document de sécurité,
- la génération d'un masque (114) ayant une taille de l'image complète (113) et comprenant une pluralité de région (115), en utilisant une fonction ayant une valeur dépendant de l'au moins une partie obtenue des données personnalisées (121-123),
- la vérification si la première image partielle (111) et/ou la deuxième image partielle (112) sont conformes au masque généré (114).

12. Dispositif d'authentification du document de sécurité selon l'une quelconque des revendications 7 à 10, le dispositif étant **caractérisé en ce qu'**il comprend :

- un lecteur de document (301) configuré pour effectuer l'obtention d'au moins une partie des données personnalisées (121-123) du document de sécurité, ainsi que de la première image partielle (111) et/ou la deuxième image partielle (112),
- un module de vérification (302) configuré pour effectuer la génération d'un masque (114) ayant une taille de l'image complète (113) et comprenant une pluralité de région (115), en utilisant une fonction ayant une valeur dépendant de l'au moins une partie obtenue des données personnalisées (121-123) et la vérification si la première image partielle (111) et/ou la deuxième image partielle (112) sont conformes au masque généré (114).

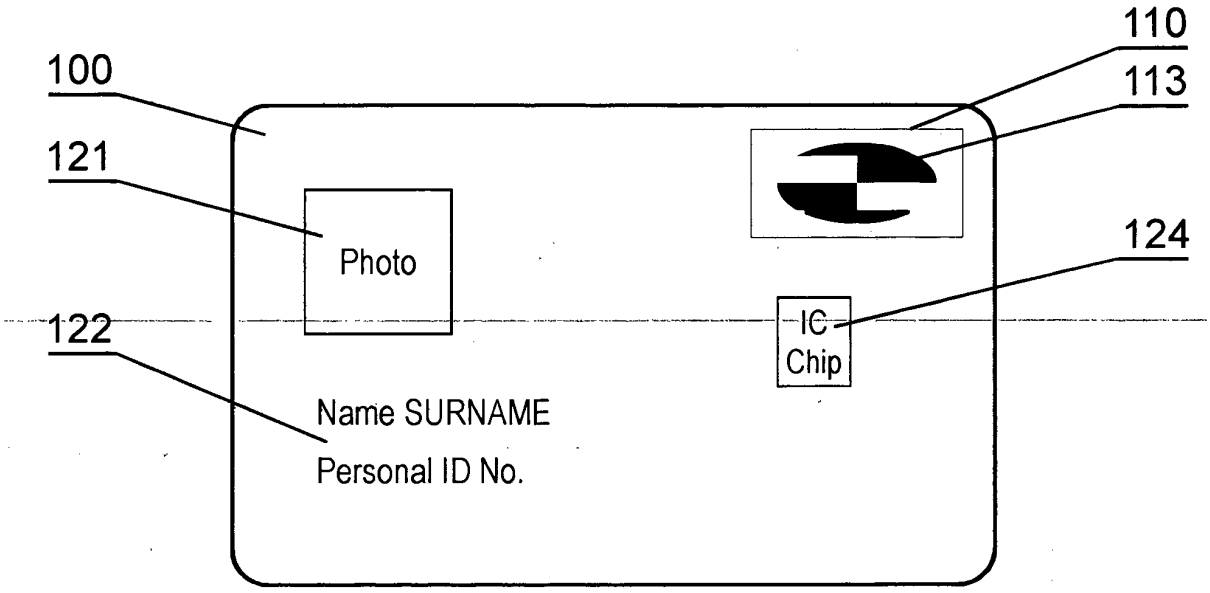


Fig. 1

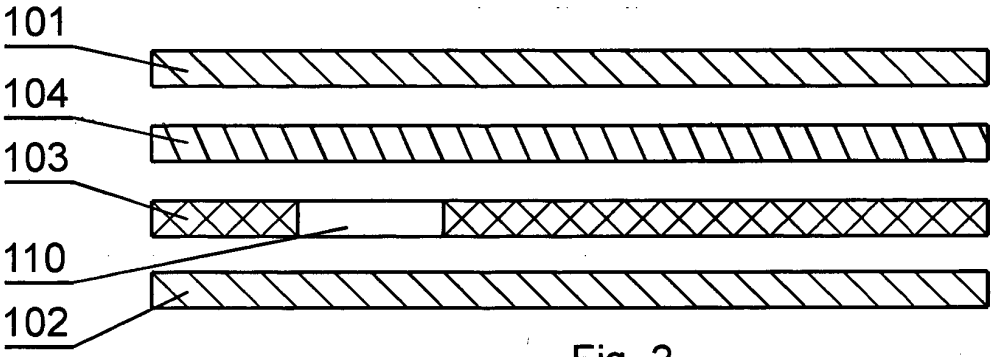


Fig. 2

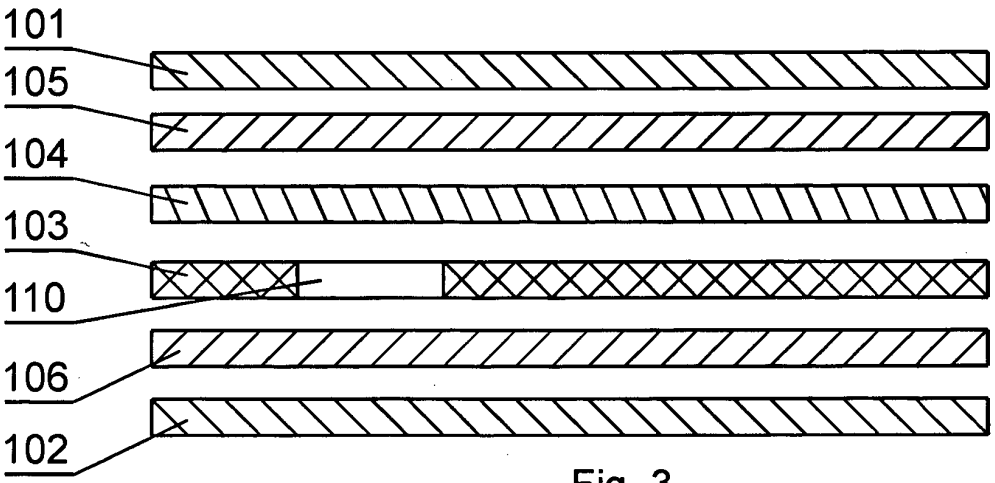


Fig. 3

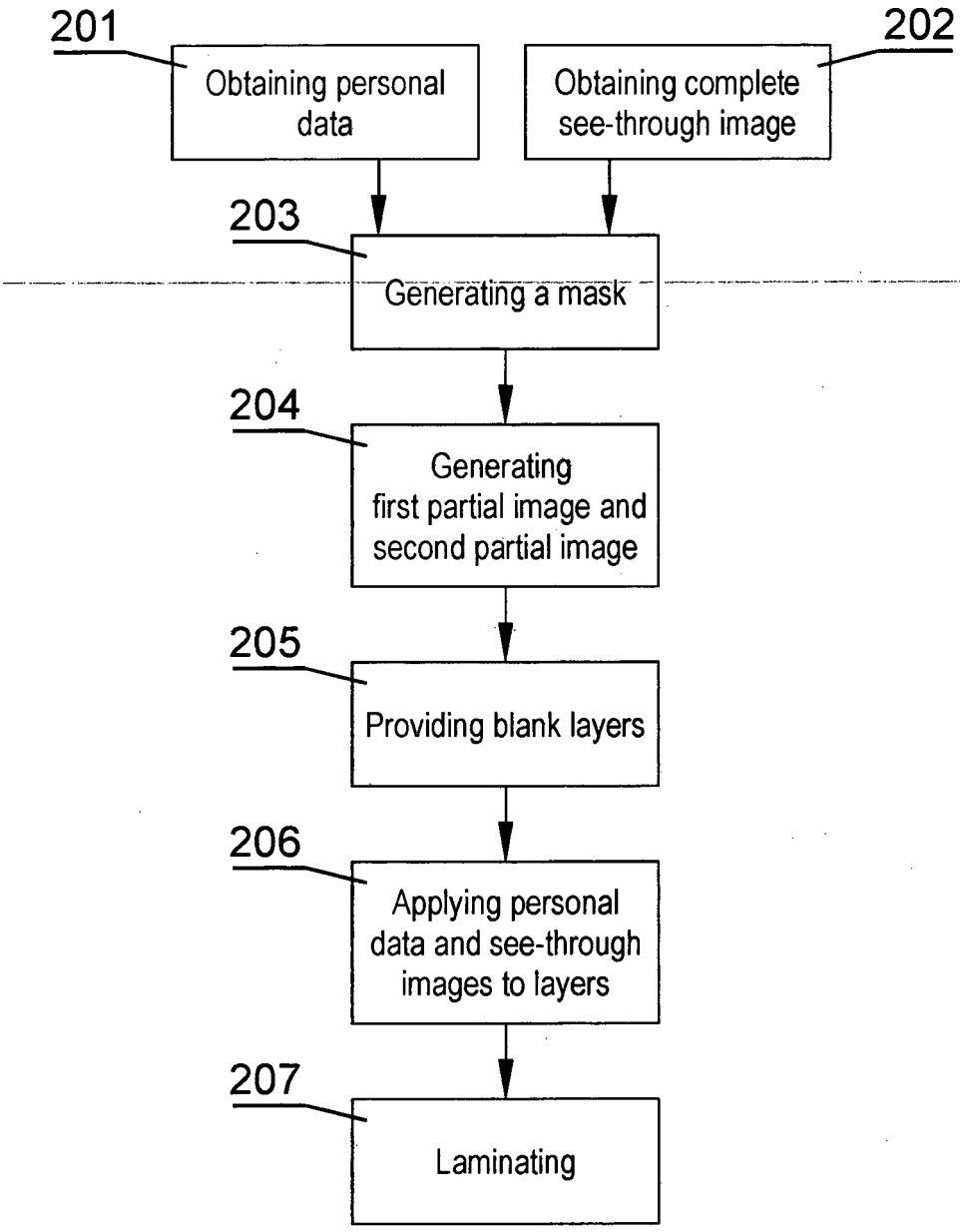

201
Obtaining personal data
202
Obtaining complete see-through image
203
Generating a mask
204
Generating first partial image and second partial image
205
Providing blank layers
206
Applying personal data and see-through images to layers
207
Laminating

Fig. 4

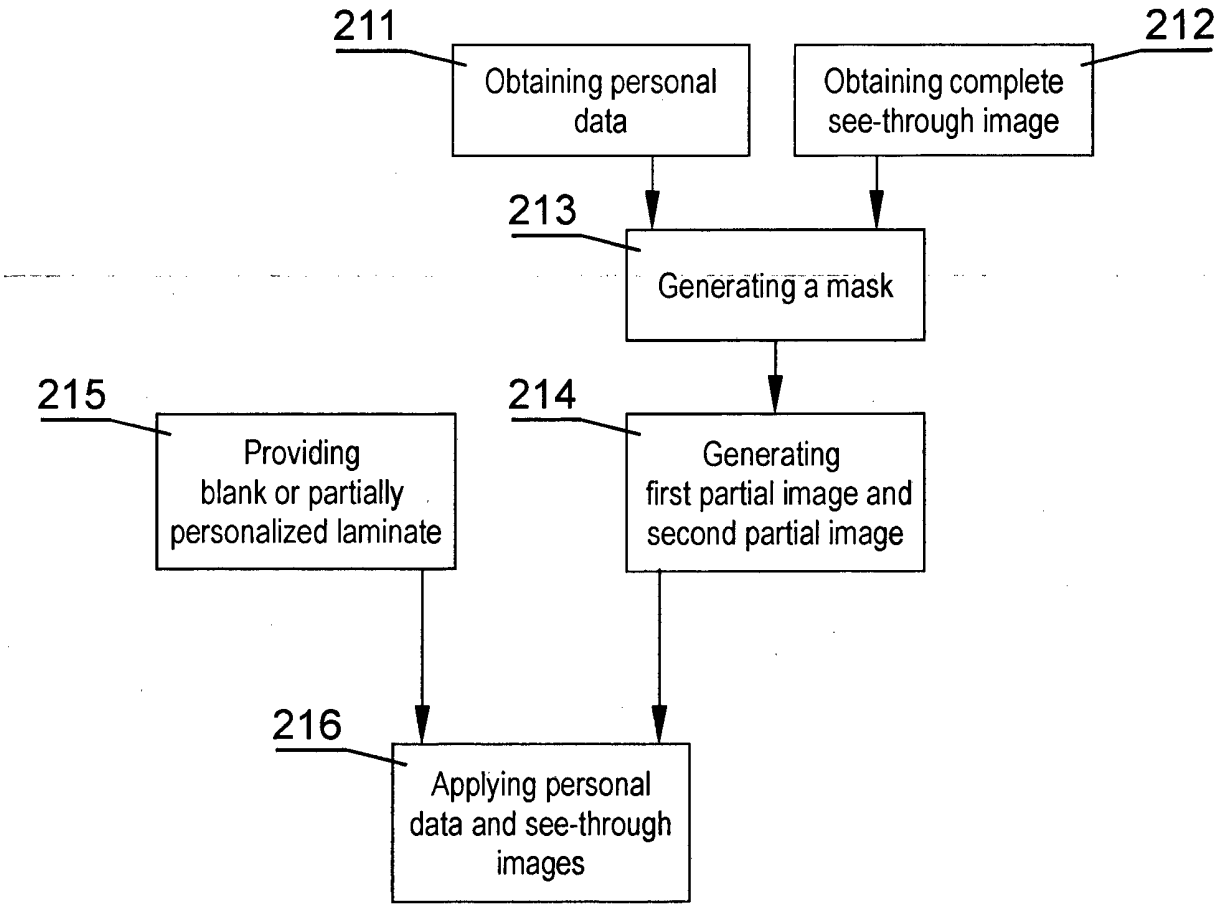

211
Obtaining personal data
212
Obtaining complete see-through image
213
Generating a mask
215
Providing blank or partially personalized laminate
214
Generating first partial image and second partial image
216
Applying personal data and see-through images

Fig. 5

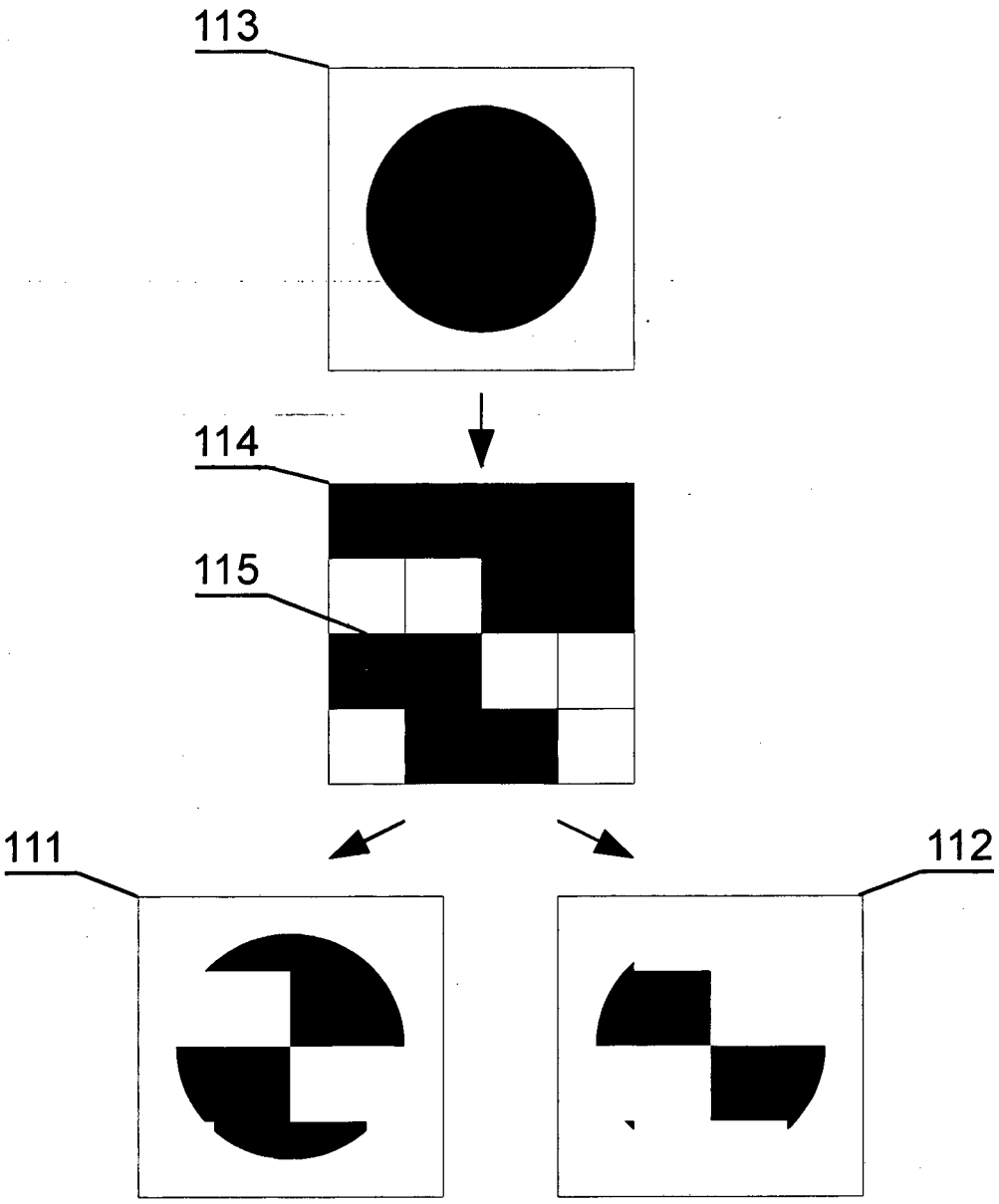


Fig. 6

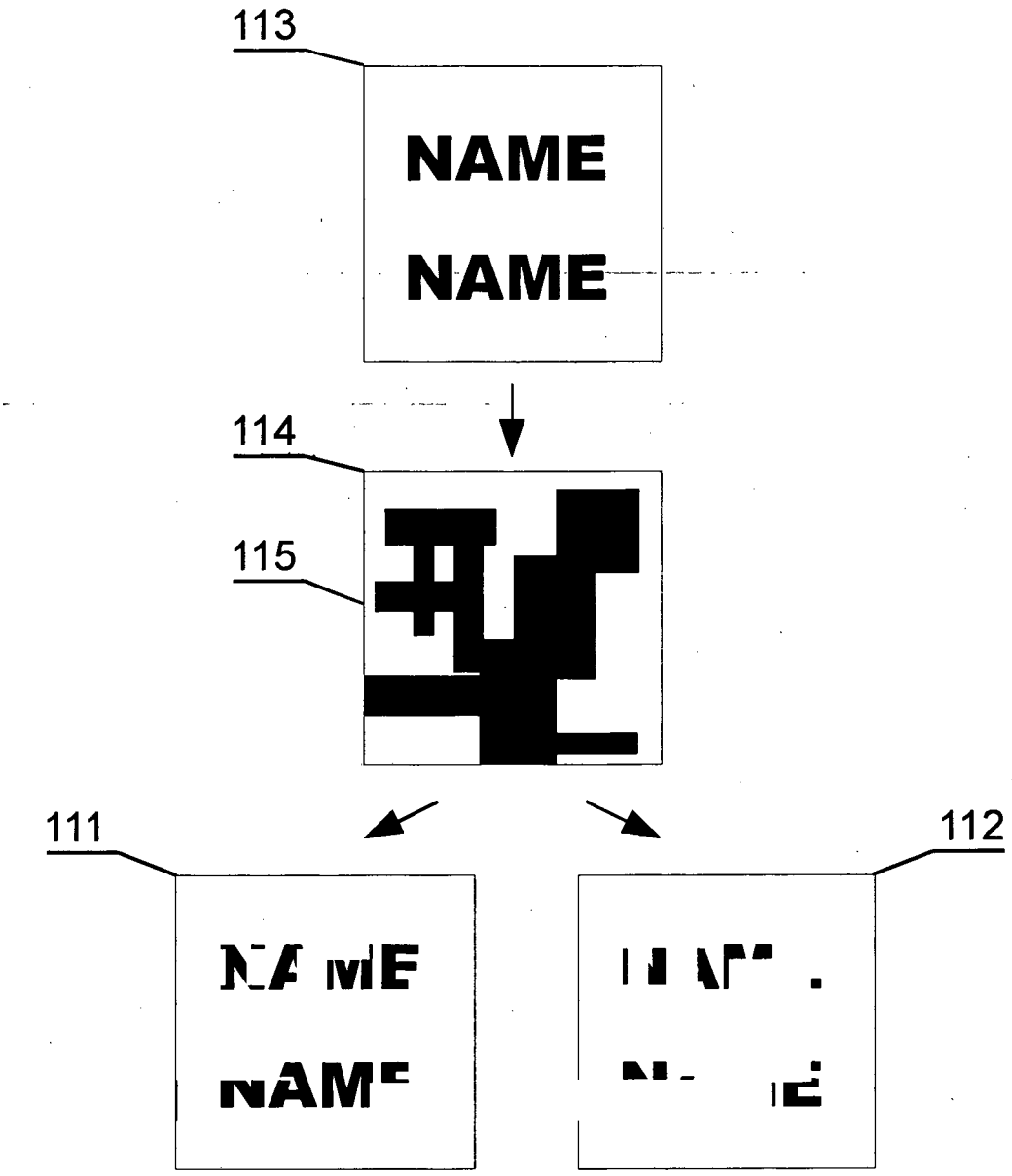


Fig. 7

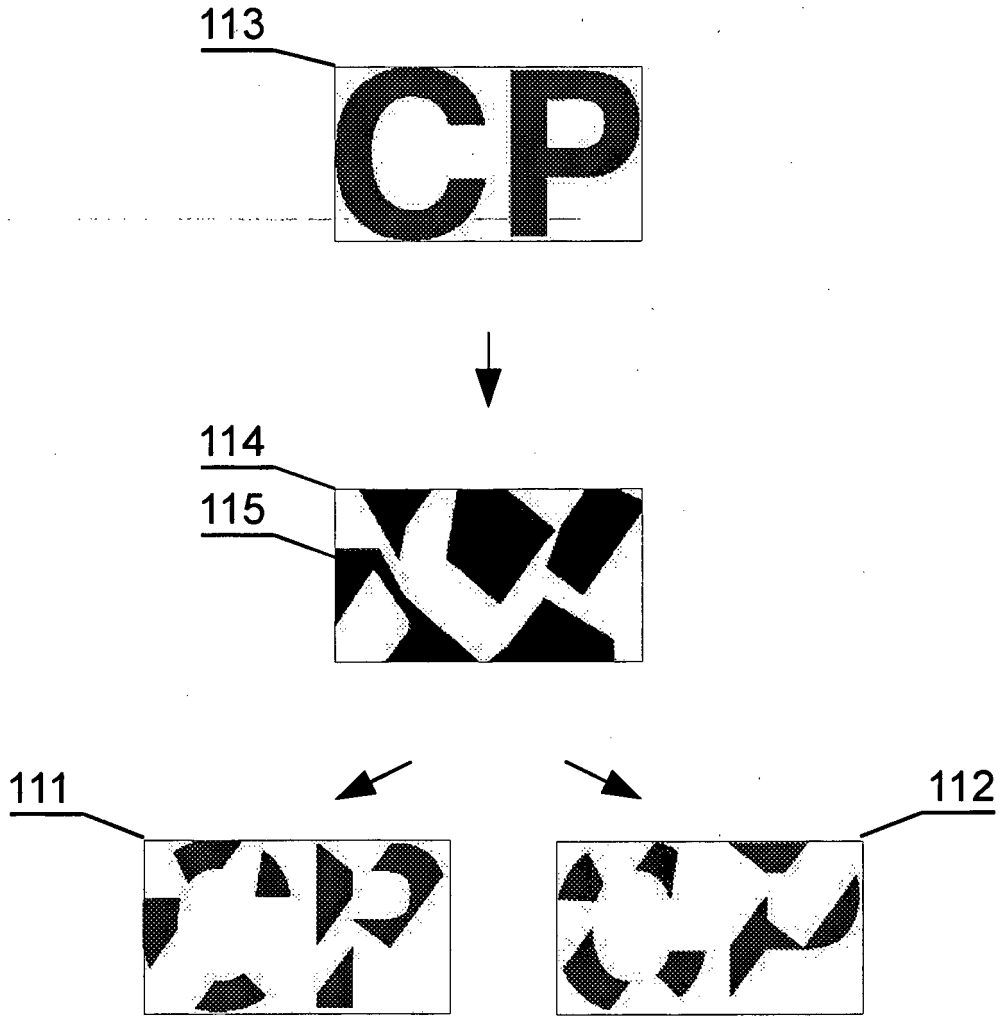


Fig. 8

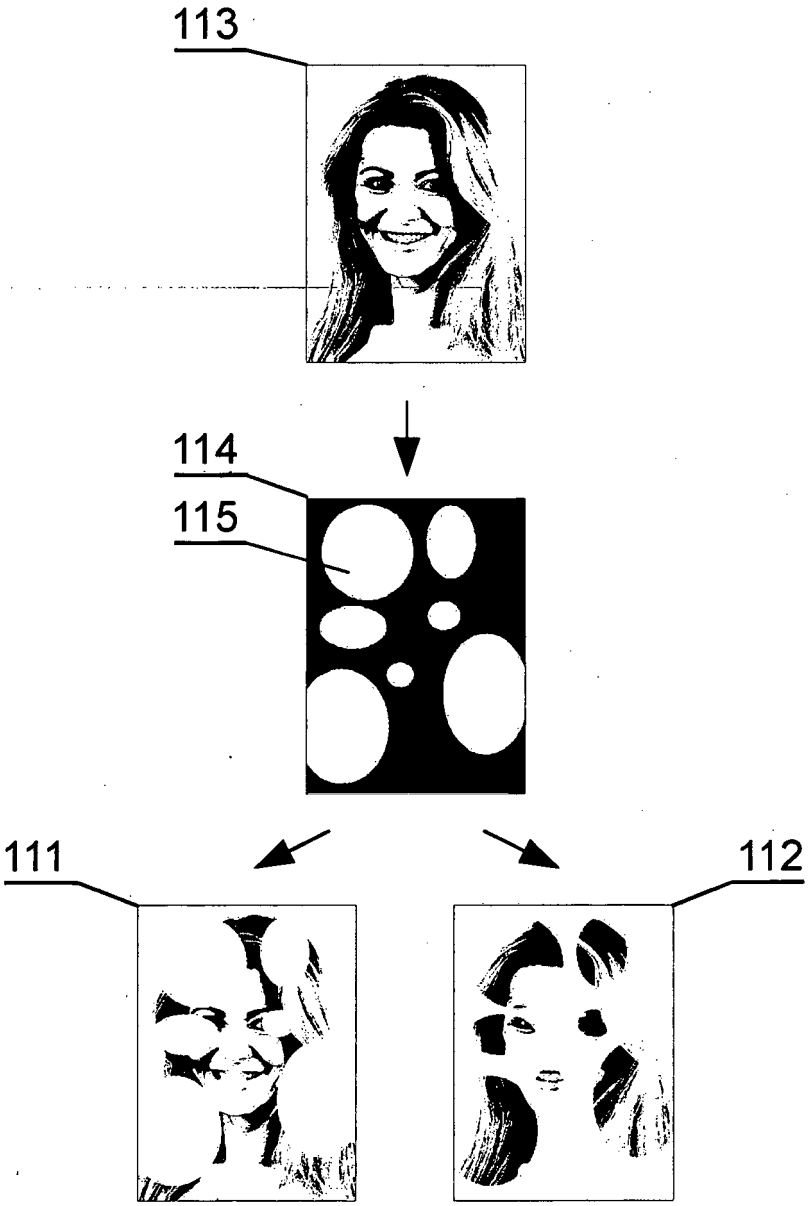


Fig. 9

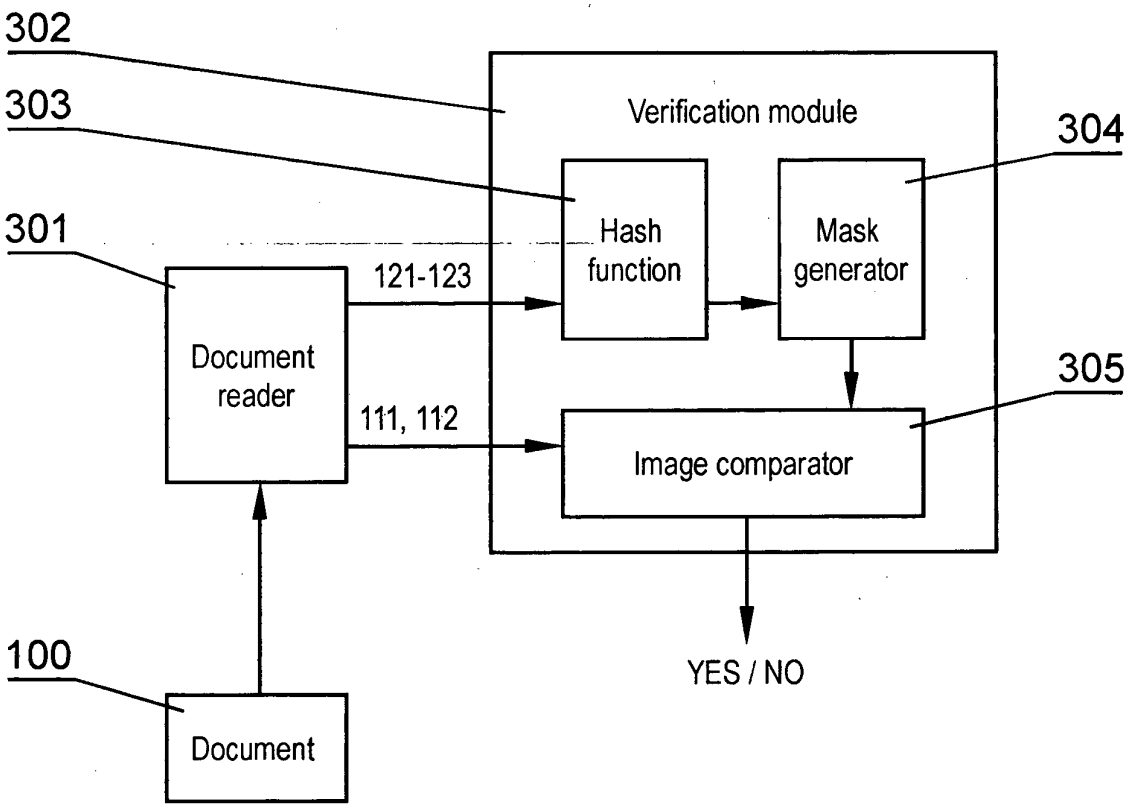

302
303
301
304
305
100
Verification module
Hash function
Mask generator
Image comparator
Document reader
Document
121-123
111, 112
YES / NO

Fig. 10

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

- EP 0388090 A **[0003]**
- US 20100295290 A **[0004]**