(19) DANMARK

(10) **DK/EP 2499000 T3**

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: *B 42 D 15/00 (2006.01)* *B 42 D 25/00 (2014.01)* *B 42 D 25/23 (2014.01)* *B 42 D 25/309 (2014.01)* *G 06 K 19/08 (2006.01)* *G 06 K 19/10 (2006.01)* *H 04 N 1/32 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2017-10-23**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2017-07-05**

(86) Europæisk ansøgning nr.: **10779525.4**

(86) Europæisk indleveringsdag: **2010-11-09**

(87) Den europæiske ansøgnings publiceringsdag: **2012-09-19**

(86) International ansøgning nr.: **EP2010067122**

(87) Internationalt publikationsnr.: **WO2011058012**

(30) Prioritet: **2009-11-12 EP 09306087**

(84) Designerede stater: **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**

(73) Patenthaver: **Gemalto SA, 6, rue de la Verrerie, 92190 Meudon, Frankrig**

(72) Opfinder: **DIDELOT, Florian, c/o Gemalto SA, Intellectual Property Dpt, 6 rue de la Verrerie, F-92197 Meudon, Frankrig**

(74) Fuldmægtig i Danmark: **Awapatent A/S, Strandgade 56, 1401 København K, Danmark**

(54) Benævnelse: **Identitetsdokumenter omfattende et identitetsfotografi sikret ved hjælp af motiver**

(56) Fremdragne publikationer:
EP-A- 1 318 486
EP-A- 1 684 494
EP-A2- 0 660 260
GB-A- 2 451 482
US-A- 6 095 566
US-A1- 2003 231 785
US-A1- 2005 072 846
US-A1- 2005 109 846

IDENTIFICATION DOCUMENTS COMPRISING AN IDENTIFICATION PHOTOGRAPH SECURED USING A PATTERN

The invention concerns identification documents, in particular the securing of identification documents such as identification cards, driving licences or passports against fraudulent alternation or production.

Identification documents usually include an identification photograph of the holder. In addition, identification documents include a certain number of alphanumeric particulars, such as the name of the holder, their date of birth, their height, their address, the document number, the document issue date or the identity of the authority that issued the document.

Identification photographs often include embossed or superimposed elements. This embossing forms a network of lines superimposed on the photograph, visible to the naked eye. The embossing is intended to ensure any fraudulent modification of the photograph is visible during an identification check. In particular, the embossing is protection against modifications to the colour of the photograph, for example when adding a beard or hair. In this way, the embossing enables level 1 (visual inspection with the naked eye) and level 2 (visual inspection with a simple optical device such as a magnifying glass or an ultraviolet lamp) to be easily implemented.

As the embossing only provides additional security against modifications to the image and does not provide protection against modification of the alphanumeric information, other identification document protection systems are generally implemented.

Watermarking techniques are used to integrate elements visible to the naked eye within an identification photograph, with these elements encoding predefined information. Watermarking provides level 3 security during an inspection. In this way, using a digital analysis and processing device, the identification photograph is analysed in order to extrapolate the data contained within the watermark. The consistency of this data is then verified.

In practice, watermarks have a certain number of disadvantages. On the one hand, watermarks do not enable level 1 or level 2 security checks to be implemented; this limits security checks to personnel equipped with significant resources, which is tricky for mobile checks. In addition, deciphering the watermark requires a significant number of calculations based on the Fourier transform. These calculations prove to be relatively lengthy and complex, which makes the identification check process excessively long. In addition, watermarks may be affected by damage to the identification document, damage which may be caused by a lack of care by the holder during the relatively long period of validity of the document. The analysis of damaged watermarks may therefore lead to incorrect reading of the watermarks, or it may be impossible to read the marks during an inspection. The security check must therefore rely on other authenticity checks, which immediately cancel out the usefulness of the watermark.

The invention is aimed at remedying one or more of these drawbacks. The invention relates to a method for securing an identification document comprising an identification photograph and

alphanumeric particulars relating to the holder of the identification document, comprising the following steps:

- collection of alphanumeric information from the alphanumeric particulars intended to feature on the identification document;
- encoding the alphanumeric information collected using properties of patterns intended to feature in predetermined areas of the identification photograph, where the patterns are likely to reveal any alteration of the identification photograph;
- making the identification document so that it comprises said alphanumeric particulars and the identification photograph visibly bearing the patterns with said properties in said predetermined zones.

The invention is characterised in that the patterns are made up of lines superimposed on the identification photograph with line intersections, so that said collected alphanumeric information is coded by the presence and absence of intersections of patterns in said predetermined zones.

In one alternative, the patterns created on the identification photograph are visible to the naked eye.

Another alternative comprises an analysis of the colours or intensity of predetermined zones of the identification photograph and comprises the making of patterns with a colour or intensity contrast in relation to the identification photograph in predetermined zones.

In another alternative, the identification document comprises a microchip, where the method comprises a step for writing the alphanumeric particulars, the alphanumeric information collected, the location of the predetermined zones and/or the identification photograph in the microchip.

In yet another alternative method, the step of encoding with the properties of patterns is preceded by a step where the collected information is encrypted.

In another method, the predetermined zones of the identification photograph have a variable density at different locations of the identification photograph.

In another method, the predetermined zones are not as dense at the eyes of the identification photograph.

With an alternative method, the process composes steps consisting in:

- digitally analysing the identification photograph to extract image statistics;
- encoding the image statistics extracted with pattern properties in some of the predetermined zones.

The invention also relates to a system for testing the authenticity of an identification document, comprising:

- a digital image capturing device;
- a processing module suitable for determining alphanumeric information on a captured image and suitable for identifying pattern properties in predetermined zones of a captured image, where the patterns are likely to reveal any alteration of the identification photograph;
- an authentication module, which indicates to the processing module the predetermined zones to analyse in order to identify the properties of patterns in those zones, which decodes the

information encoded by the properties of those patterns, which compares information from the captured image with the decoded information and generates a signal representative of authenticity depending on the result of the comparison.

In an alternative method, the system also includes a device that reads a microchip of the identification document, where the authentication module compares the decoded information with information saved in the microchip and generates a signal representative of authenticity depending on the result of the comparison.

The invention also relates to an identification document that comprises an identification photograph and alphanumeric particulars relating to the holder; in which:

- the identification photograph bears the patterns, the properties of which encode the alphanumeric particulars collected from this alphanumeric information in predetermined zones of the photograph, where the patterns are likely to reveal any alteration of the identification photograph, and the encoding of the alphanumeric information is defined in a standardised encoding protocol.

In another alternative, the intersection or lack thereof of the patterns in predetermined zones of the photograph encodes the alphanumeric information.

In another alternative, the identification document comprises an electronic microchip capable of communicating with a reader, where the microchip memorises the standardised encoding protocol and/or the location of the predetermined zones and/or the identification photograph.

Other characteristics and benefits of the invention will become clearer in the description below, which is not limitative in any way, by reference to the attached drawings, where:

- figure 1 is a functional schematic representation of an identification document according to the invention;
- figure 2 represents a matrix of the pattern intersection points intended to encode alphanumeric information;
- figure 3 is a schematic representation or an example of the process for printing an identification photograph that encodes numerical information using patterns;
- figures 4 to 6 represent different pattern outline variations;
- figure 7 represents an example of manufacturing process for a card according to the invention;
- figure 8 represents an example of the process of testing the authenticity of the identification document;
- figure 9 represents a system for verifying the authenticity of an identification document.

Figure 1 represents an example of identification document 1 according to an embodiment of the invention. Identification document 1 comprises support 7, made of synthetic material, fibrous material or a combination of synthetic and fibrous materials. Identification document 1 comprises an identification photograph 3 of its holder. Identification document 1 also comprises visible,

personalised, alphanumeric particulars 4, such as the full name of the holder, their date of birth or the number of the identification document. Identification document 1 also comprises the signature 5 of its holder. A microchip 2 is also usefully fixed on or in support 7 in a known manner, per se. The microchip typically comprises a microcontroller equipped with a communication interface, a processor, a non-volatile memory and random-access memory. Visible patterns 6 are present on the identification photograph 3. In this scenario, patterns 6 form embossing. The patterns 6 are usefully imprinted on the identification photograph 3, so that any attempt to modify the patterns results in damage to the appearance of this photograph 3. The patterns 6 are therefore likely to reveal a potential alteration of the appearance of the identification photograph.

Figure 2 represents a grid or matrix 61, which defines a set of regular zones or encoding zones 62, in which the properties of the patterns encode information gained from the alphanumeric particulars 4. The zones 62 are located at predefined positions, at the intersections of a rectangular shape in the example illustrated. The properties of the patterns at the regular zones 62 enables the encoding of alphanumeric information collected from the alphanumeric particulars 4. In the example detailed hereafter, the properties of the patterns 6 used to encode the alphanumeric information shall be the presence or absence of an intersection between the lines of patterns at the regular zones 62.

Figure 3 provides a simplified example of a process that leads to the formation of patterns 6 on the identification photo 3 of the identification document 1. In the first stage, the name 41 of the holder is collected from the alphanumerical particulars 4. The name 41 of the holder is encoded to form a binary code 42 over a predetermined number of bits. Each bit of the code 42 corresponds to a regular zone 62 of the grid 61. A matrix of the intersecting points 63 is generated by preserving the regular zones 62 which define the points at which the lines of patterns intersect. A value 1 of the binary code 42 shall be coded by a point of intersection 63 at a connected regular zone 62, while a value 0 of the binary code 42 shall be encoded by the absence of a point of intersection at the connected regular zone 62. Next, the lines of patterns 64 are outlined, so that several lines 64 cross each other at the points of intersection 63, in such a way that a maximum of one line passes through each regular zone 62 without a point of intersection 63. In the example illustrated, the lines 64 are straight. For example, the lines of patterns 6 could be outlined in a known manner, per se, using a Delaunay triangulation method between the points of intersection 63. The patterns 6 generated are then superimposed over the identification photograph 3. The patterns 6 may be superimposed on the identification photograph 3 in digital format, before affixing the identification photograph 3 transformed on support 7. When the patterns 6 are added to the identification photograph 3 prior to its transfer to support 7, the added cost of such additional protection is reduced significantly. Another option could be to add the patterns created by any appropriate method to an identification photograph 3 that has previously been printed on support 7.

The use of patterns 6 to code information gained from the alphanumeric particulars 4 enables an authenticity test to be conducted quickly. For example, the identification of the intersections of the lines 64 in predetermined zones will enable a comparison to be made between

the data encoded in the patterns 6 and the alphanumeric particulars 4, simply based on a numerical entry of the identification photograph 3, followed by image processing, as detailed hereafter. If inconsistencies are noted between the data extracted from the identification photograph 3 and the alphanumeric particulars 4, it may be deduced that the identification document 1 has been fraudulently altered or produced.

To further reinforce the security of such an identification document 1, other information could also be encoded using patterns 6. There is also the option of encoding statistical information regarding the identification photograph 3, in order to be able to identify attempted fraud through the addition or removal of details present between the patterns, for example, a mole, which therefore results in an alteration of the statistics of the photograph. For example, the statistical information could relate to a textural or spectral feature of the identification photograph 3.

Different alphanumeric particulars could be collected in order to encoded on the identification photograph 3 using patterns. The alphanumeric particulars collected for encoding could be fragments of different information fields. For example, a certain number of characters could be collected from the last name, the first name, the identification document number and/or the holder's date or place of birth.

In order to increase the robustness and the speed of processing the alphanumeric information encoded in the patterns 6 during an authenticity test, the matrix 61 may comprise a reduced number of bits, for example 160 bits.

In addition, the microchip 2 is secured and memorises the alphanumeric particulars 4. Therefore, the microchip 2 allows for verification that the alphanumeric particulars 4 or the patterns 6 have not been fraudulently altered, which gives the microchip a double-verification role. In addition, it is not necessary for the microchip 2 to memorise the identification photograph with no patterns 6 in order to decode the alphanumeric information encoded in the photograph 3.

The use of visible patterns enables a authenticity test to be carried out even when it is impossible to read the microchip 2. For example, in the event of deactivation or involuntary damage to the microchip 2 of the identification document 1, the authorities may agree to settle for the decoding of the patterns 6 present on the identification photograph 3. As another benefit, the use of patterns visible to the naked eye dissuades crude attempts at fraud and allows for visual authenticity checks, even in the absence of equipment to analyse the identification photograph. In addition, patterns 6 visible to the naked eye are particularly robust and can withstand wear to the identification document 1 when this document is not always stored in optimal conditions, and it is often possible to decode these patterns for a very long period of validity.

The intersections of the patterns 6 are usefully contrasted in comparison with the identification photograph 3, so that they remain analysable following numerical entry and processing. The colour or brightness or the patterns 6 are therefore in contrast in relation to the identification photograph at the intersections in the predetermined encoding zones. Such contrast also makes the authenticity checks more robust when faced with potential alterations to the identification document 1.

In the examples illustrated in figures 4 to 6, the predetermined zones that encode a first binary value are identified with black circles; a second binary value is identified with unfilled circles. These circles are not indicated on the patterns present in identification photograph 3. The circles are only indicated to facilitate understanding of the figures, and to highlight the encoding carried out using lines 64.

In the example of figure 4, the lines 64 that form the patterns 6 are not straight. Such lines 64 make it more difficult for a potential fraudster to identify the intersections considered for the encoding. Lines 64 may also have characteristic curves, such as sinusoidal curves, which enable false patterns to be identified during a level 1 or level 2 check.

In the example of figure 5, the matrix that defines the intersection zones considered for the encoding has been deformed into a more spherical shape in comparison with the matrix of figure 2. Such deformation is useful for reducing the density of the lines in certain zones of the photograph, which must not be subject to significant alteration to ensure the holder of document 1 remains recognisable. In this way, the density of the lines of patterns 6 around the nose or eyes of the user may be reduced. In the example of figure 6, the matrix that defines the intersection zones considered for the encoding has been deformed into a more spiral shape in comparison with the matrix of figure 2.

Figure 7 represents an example of manufacturing process according to the invention, implemented at the identification document 1 personalisation stage. During stage 101, alphanumeric information is collected from the alphanumeric particulars 4 intended to feature on the identification document 1. The alphanumeric information collected is chosen from the alphanumeric particulars 4 according to reproducible rules, so that authenticity checks may be implemented subsequently. The information collected is then entered in numerical form in stage 102, so that it can be subject to numerical processing.

During stage 103, the information collected is subject to a hash function to generate a binary sequence. The hash function enables a binary sequence of a predefined size to be generated. Therefore, even if the information collected is relatively long, the binary sequence generated shall be of the appropriate size for encoding through matrix 61. In addition, a hash function enables the information collected to be encoded.

During stage 104, the binary sequence is subject to an encoding process, in a manner known per se. The encoding generates an encoded binary sequence. The ability of a fraudster to determine how to encode the alphanumeric particulars onto the photograph they wish to print on the card is therefore reduced. During stage 105, the encoded binary sequence is transformed into the points of intersection 63 matrix, as illustrated in figure 3. During stage 106, the lines of the patterns are outlined so that they form intersections at the points 63. This outlining is carried out so that the other regular zones 62 of the matrix do not feature intersection of the lines of the patterns.

During stage 107, the patterns and the predetermined encoding zones are distorted, as detailed in the example of figures 5 and 6. The density of the encoding zones may therefore be reduced in zones of the identification photograph that feature details that must not be altered. During stage 108, the intensity or the colour of the patterns is adapted based on the identification photograph on which they are to be superimposed. Sufficient visual contrast between the photograph and the patterns is therefore generated. For example, a pattern line will be light in a dark zone of the photograph.

During stage 109, an image is generated by superimposing patterns on the identification photograph. During stage 110, information is stored in the microchip 2 of the identification document. This information may contain the digitised identification photograph, with and/or without superimposed patterns, and/or image analysis statistics concerning the identification photograph, and/or the alphanumeric particulars 4. During stage 111, the identification document 1 is formed by affixing the identification photograph 3, with the patterns 6, onto the support 7, through printing or any other appropriate method.

Figure 9 represents a system for verifying the authenticity 8 of an identification document 1. The authenticity check system 8 comprises a terminal 81. A scanner 82 is connected to the terminal 81. A chip card reader 83 is also connected to the terminal 81. This may be a contactless chip card reader, in particular to read the chip if it is hidden in the cover of the identification document 1. The terminal 81 is configured to execute one or more authenticity check management applications.

An example of the authenticity testing process is detailed in figure 8. During stage 201, the identification document is scanned using the scanner 82. In particular, the identification photograph 3 and the alphanumeric particulars 4 are digitised. A decoding application executed on the terminal 81 orders a certain number of image-processing operations. During stage 202, an image processing application identifies the alphanumeric particulars 4. During stage 203, an image processing application determines the presence or absence of intersections of the lines of the patterns 6 in the predetermined locations provided by the decoding application. During stage 204, a binary code is extrapolated based on the locations for which pattern 6 intersections were identified. During stage 205, the decoding application collects alphanumeric information from the alphanumeric particulars identified, in accordance with a standardised coding protocol. During stage 206, the decoding application generates a binary code from the alphanumeric information by applying this standardised coding protocol. During stage 207, the binary code created from the alphanumeric information and the binary code extrapolated from the patterns are compared. During stage 208, the alphanumeric particulars memorised in the microchip 2 are also read by the reader 83. During stage 209, a binary code is generated from the alphanumeric information read in the microchip 2. During stage 210, the binary codes created from the microchip 2 are compared with the binary code extrapolated from the patterns 6. During stage 211, the result of the authenticity test is displayed on the screen 84.

Therefore, from an identification document 1 in which patterns encode alphanumeric information concerning the holder, an additional authenticity test can be carried out using the standardised encoding protocol provided to the authorities. It is also possible for the type of encoding and the locations of the encoding zones of the identification photograph to be identified in the microchip 2.

In the completion methods described in figures 1 to 6, the properties of the patterns in the encoding zones are limited to the presence or absence of an intersection of the patterns. However, other properties may also be used independently or in combination with the pattern intersections. In particular, encoding could be carried out based on the position of the intersection in the aforementioned zones, based on the colour of the pattern intersection, based on the angles between the patterns at the intersection or based on the shapes of the patterns at the intersection. Independent encoding of pattern intersections could also be carried out, based on the colour or contrast of the patterns in relation to the identification photograph in the background, or encoding based on the thickness of the lines of the patterns in the encoding zones.

The colour or brightness of the patterns is advantageously adapted to the background on which they are superimposed. One option would therefore be to have the patterns in contrast in relation to the identification photograph. In this way, the patterns are easily visible to the naked eye when observing the identification photograph. The colour or brightness of a pattern could also vary based on the background on which it is superimposed.

The use of patterns with the invention does not exclude the use of other, supplementary security patterns, such as watermarks.

In this case, the identification document 1 illustrated is a secure-access chip card. The invention, of course, applies to any other type of identification document, such as a driving licence, a passport or a national identification card.

P A T E N T K R A V

1. Fremgangsmåde til sikring af et identitetsdokument (1), som omfatter et identitetsfotografi (3) og alfanumeriske påtegninger (4) vedrørende indehaveren af identitetsdokumentet, hvilken fremgangsmåde omfatter trinene at:

- indsamle alfanumeriske informationer blandt de alfanumeriske påtegninger (4) bestemt til at figurere på identitetsdokumentet;
- kode de indsamlede alfanumeriske informationer med egenskaber af motiver bestemt til at figurere i forud bestemte zoner af identitetsfotografiet (3), hvor motiverne er egnede til at afsløre en eventuel ændring af identitetsfotografiet;
- realisere identitetsdokumentet på en sådan måde, at det bærer de alfanumeriske påtegninger (4), og på en sådan måde at det bærer identitetsfotografiet (3), på hvilket motiverne (6) med de nævnte egenskaber figurerer på synlig måde i de forud bestemte zoner,

k e n d e t e g n e t ved, at motiverne udgøres af linjer overlejrede med identitetsfotografiet og omfatter skæringer af linjer, og ved at de indsamlede alfanumeriske informationer kodes ved tilstedeværelsen og ikke-tilstedeværelsen af skæringer af motiver i de forud bestemte zoner (62).

2. Fremgangsmåde til sikring af et identitetsdokument ifølge krav 1, ved hvilken farven eller klarheden af motiverne med fordel er tilpasset til baggrunden, på hvilken de er overlejrede.

3. Fremgangsmåde til sikring af et identitetsdokument ifølge krav 1, ved hvilken motiverne (6) omfatter en farve- eller klarhedskontrast i forhold til identitetsfotografiet (3) for at være let synlige for det blotte øje.

4. Fremgangsmåde til sikring af et identitetsdokument ifølge et hvilket som helst af de foregående krav, som omfatter analyse af farvesammensætningen eller intensiteten af forud bestemte zoner af identitetsfotografiet (3), og som omfatter realisering af motiver (6) med en farvesammensætnings- eller intensitetskontrast i forhold til identitetsfotografiet i de forud bestemte zoner.

5. Fremgangsmåde til sikring af et identitetsdokument ifølge et hvilket som helst af de foregående krav, ved hvilken identitetsdokumentet (1) omfatter en chip (2), og hvor fremgangsmåden omfatter et trin til at skrive alfanumeriske påtegninger, indsamlede alfanumeriske informationer, placeringen af de forud bestemte zoner og/eller identitetsfotografiet på chippen.

6. Fremgangsmåde til sikring af et identitetsdokument ifølge et hvilket som helst af de foregående krav, ved hvilken der forud for trinet at kode med egenskaber af motiver går et trin til chifrering af de indsamlede informationer.

7. Fremgangsmåde til sikring af et identitetsdokument ifølge et hvilket som helst af de foregående krav, ved hvilken de forud bestemte zoner af identitetsfotografiet (3) omfat-

ter en densitet, der varierer med forskellige placeringer på identitetsfotografiet.

8. Fremgangsmåde til sikring af et identitetsdokument ifølge krav 7, ved hvilken de forud bestemte zoner omfatter en mindre intensitet på niveau med øjnene i identitetsfotografiet.

9. Fremgangsmåde til sikring af et identitetsdokument ifølge et hvilket som helst af de foregående krav, og omfattende trinene at:

- numerisk analysere identitetsfotografiet for derfra at ekstrahere billedstatistikker;
- i visse forud bestemte zoner at kode de ekstraherede billedstatistikker med egenskaber af motiver.

10. System (8) til autenticitetstest af et identitetsdokument (1), k e n d e t e g n e t ved, at det omfatter:

- en indretning (82) til numerisk billedoptagelse;
- et behandlingsmodul, som er egnet til at bestemme alfanumeriske informationer i et optaget billede, og som er egnet til at identificere egenskaber af motiver i forud bestemte zoner af et optaget billede, hvor motiverne er egnede til at afsløre en eventuel ændring af identitetsfotografiet;
- et autentificeringsmodul (81), som over for behandlingsmodulet indikerer forud bestemte zoner, som skal analyseres til identifikation af egenskaber af motiver i disse zoner, afkoder kodede informationer med egenskaberne af disse motiver, sammenligner informationerne fra det optagede billede med de afkodede informationer, og genererer et signal, der er repræsentativt for autenticiteten som funktion af resultatet af sammenligningen, og ved hvilken motiverne udgøres af linjer overlejrede med identitetsfotografiet og omfatter skæringer af linjer, hvilke informationer er kodet ved tilstedeværelsen og ikke-tilstedeværelsen af skæringer af linjer i de forud bestemte zoner (62).

11. System (8) til autenticitetstest af et identitetsdokument (1), som desuden omfatter en indretning (83) til at læse en chip (2) af identitetsdokumentet (1), hvor autentificeringsmodulet (81) sammenligner de afkodede informationer med informationer lagret i chippen og genererer et signal, der er repræsentativt for autenticiteten som funktion af resultatet af denne sammenligning.

Fig. 1

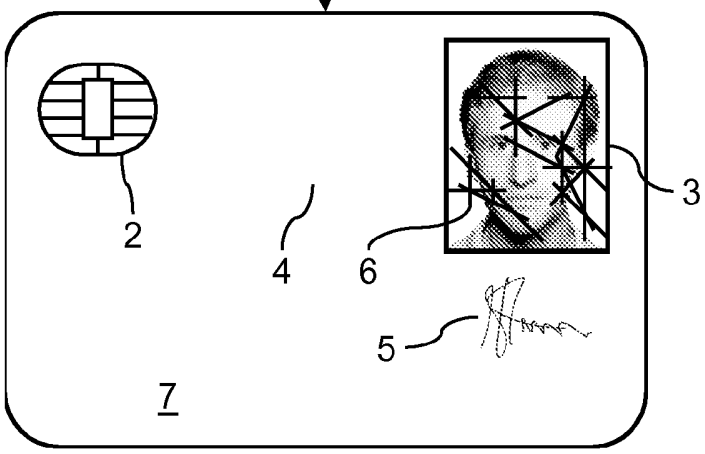


Fig. 2

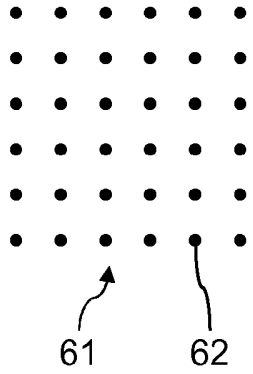


Fig. 3

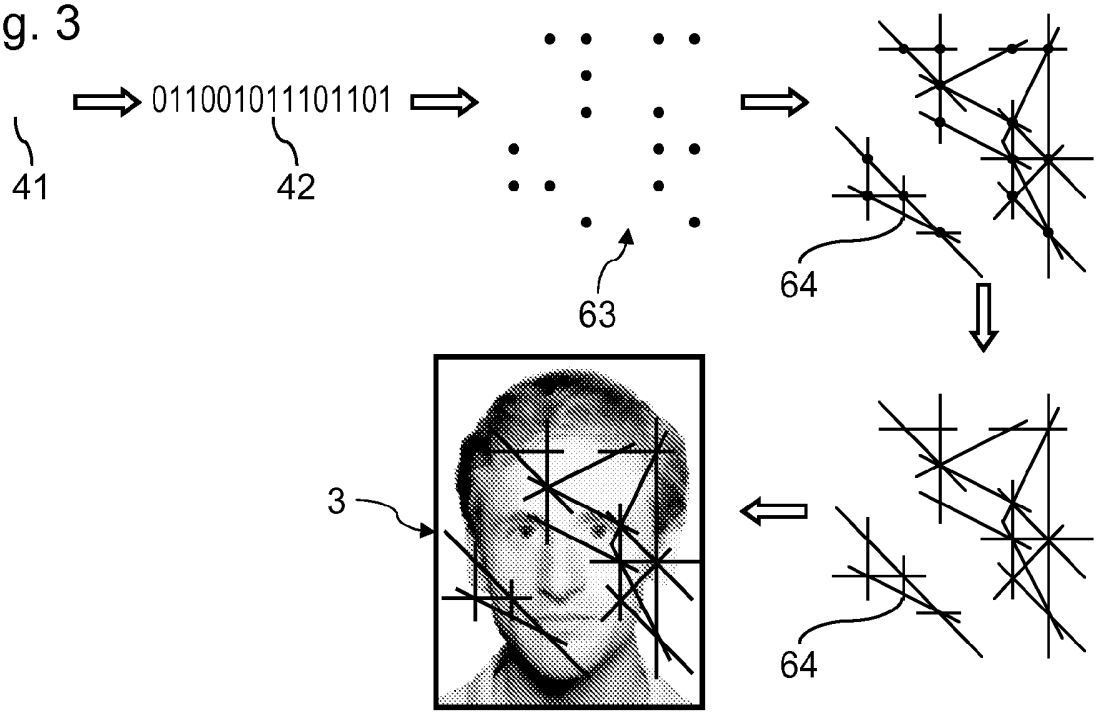


Fig. 4

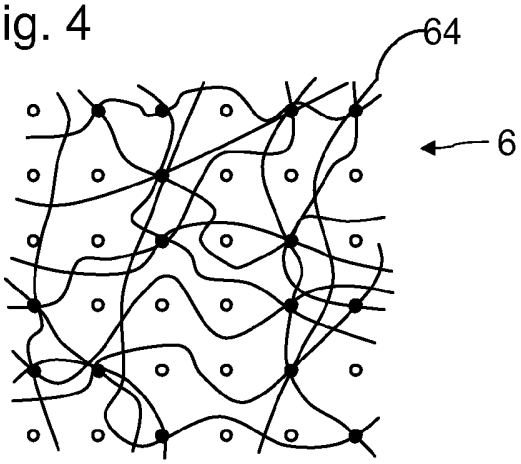


Fig. 5

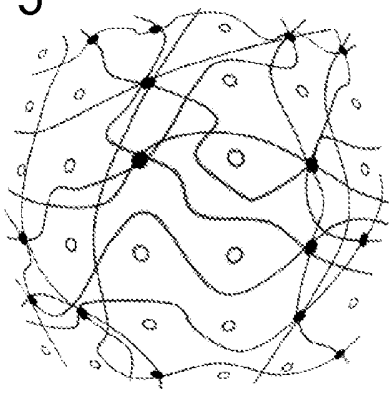


Fig. 6

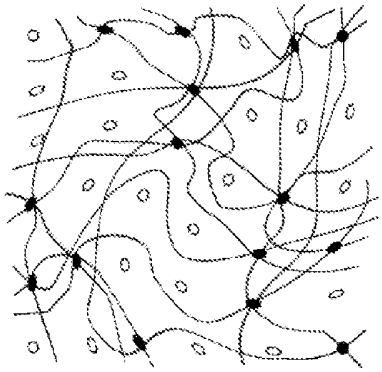


Fig. 7

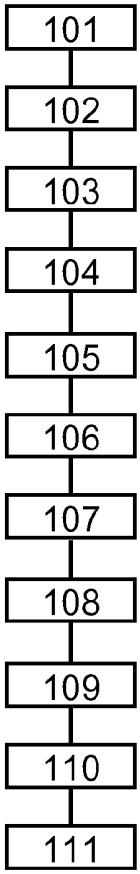


Fig. 8

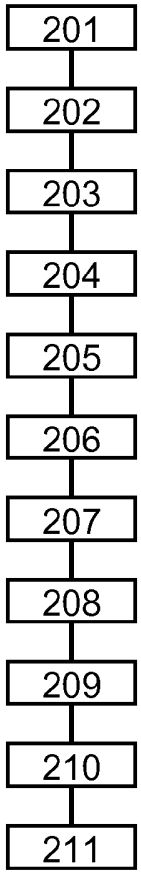


Fig. 9

