



(43) International Publication Date
15 April 2010 (15.04.2010)

(10) International Publication Number
WO 2010/040971 A1

PCT

(51) International Patent Classification:
G07D 7/00 (2006.01) **G07F 7/08** (2006.01)
B42D 15/10 (2006.01)

(21) International Application Number:
PCT/GB2009/001122

(22) International Filing Date:
5 May 2009 (05.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0818271.9 6 October 2008 (06.10.2008) GB

(71) Applicant (for all designated States except US): **DE LA RUE INTERNATIONAL LIMITED** [GB/GB]; De La Rue House, Jays Close, Viables, Basingstoke, Hampshire RG22 4BS (GB).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **GREEN, Stephen, Banister** [GB/GB]; 22 Leatherhead Gardens, Hedge End, Southampton, SO30 2TY (GB).

(74) Agent: **GILL JENNINGS & EVERY LLP**; Broadgate House, 7 Eldon Street, London EC2M 7LH (GB).

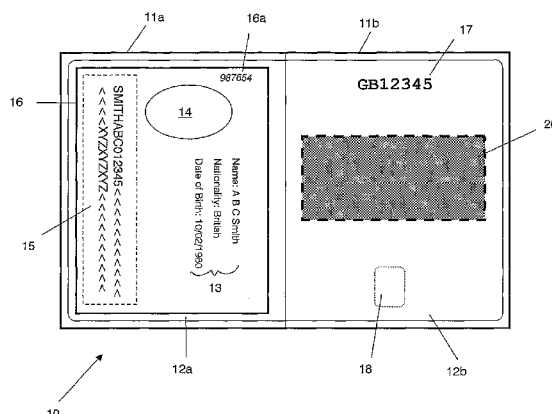
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: DOCUMENT SECURITY FEATURE AND METHOD FOR AUTHENTICATING A DOCUMENT



(57) Abstract: A document is provided comprising a machine readable security feature thereon, the document having two or more security elements, each associated with a corresponding identifier detectable from the respective security element, and the machine readable security feature containing document data representative of at least two of the identifiers corresponding to the security elements, to thereby identify at least two of the security elements of the document. Also provided is a method of determining the authenticity of the document, comprising: reading the machine readable security feature to retrieve at least one identifier contained therein; detecting an identifier associated with at least one of the security elements; and comparing the identifier retrieved from the machine readable security feature with the identifier detected from the at least one security element to determine whether the security element identified by the machine readable security feature is present on the document, to thereby determine whether the document is authentic.

Document Security Feature
and Method for Authenticating a Document

- 5 This invention relates to document security features, in particular machine readable features for use on documents such as passports, and methods of authenticating documents.

Secure documents such as passports, identification documents, certificates and
10 licences are frequently the target of counterfeiters and persons wishing to make fraudulent changes to the data contained therein. Typically such documents are provided with a number of security elements for checking the authenticity of the document. These may include RFID chips, holographic films, optically variable elements (such as colour-changing inks), security inks (such as IR and UV
15 visible inks) and other printed data. Some such security elements may themselves contain personalisation information identifying the owner of the document (e.g. data giving the owner's name, a photograph or biometric data), whereas other security elements may be provided to prevent other data being manipulated (for example a holographic film overlaying printed data).

20

Persons wishing to produce counterfeits of such documents, or to fraudulently alter data in existing documents, typically attempt to do so by substituting security elements with similar ones obtained from other security documents or, depending on the technologies involved, manufactured themselves or obtained
25 illegally. As the sophistication of such techniques improves, it has become more difficult to detect forgeries since in many cases the substituted security element provides the same or similar response to that which an inspector of the document expects.

- 30 The present invention provides a document comprising a machine readable security feature thereon, the document having two or more security elements each associated with a corresponding identifier detectable from the respective security element, and the machine readable security feature containing

document data representative of at least two of the identifiers corresponding to the security elements, to thereby identify at least two of the security elements of the document.

- 5 By associating each security element with a (preferably unique) identifier, such as a number or other code, and recording the identifiers in the machine readable security feature, substitution of any of the security elements can be readily detected, since the identifier (if any) of the substituted security element will no longer match the document data embodied in the machine readable security
10 feature. The identifiers can take any convenient form, such as alphanumeric, symbolic or even binary, provided they serve the purpose of distinguishing one security element from many others of a similar type. For example, a serial number or barcode could be used. The identifiers may or may not be recognisable to an observer, but preferably, at least some of the identifiers are
15 not recognisable, in order to increase the difficulty of producing a copy.

The present invention further provides a method of determining the authenticity of a document, the document comprising a machine readable security feature thereon and having two or more security elements each associated with a
20 corresponding identifier detectable from the respective security element, and the machine readable security feature containing document data representative of at least two of the identifiers corresponding to the security elements, thereby identifying at least two of the security elements of the document, the method comprising:

25 reading the machine readable security feature to retrieve at least one identifier contained therein;

detecting an identifier associated with at least one of the security elements; and

30 comparing the identifier retrieved from the machine readable security feature with the identifier detected from the at least one security element to determine whether the security element identified by the machine readable security feature is present on the document, to thereby determine whether the document is authentic.

In this way, the authenticity of a document can be judged based on the identify of the security elements comprised in the document, which provides a level of security over and above that achieved by simply testing the responses of the security elements. The technique also lends itself particularly well to automation, since at least some of the identifiers as well as the security feature may be machine readable. This reduces the possibility of user error.

The document data representing the identifiers may be embodied in the machine readable security feature in a number of ways. In one embodiment, the document data comprises each of the at least two identifiers. That is, the machine readable security feature could comprise a machine readable list of the identifiers. In other embodiments, the document data comprises a code in which each of the at least two identifiers are incorporated. For example, the various identifiers could be represented by different portions of a barcode or other graphic. These embodiments could also be used in combination, certain of the identifiers being represented individually, and others incorporated into a code.

In certain embodiments, each of the security elements may be independently allocated its own identifier which may or may not match any of the other identifiers. In this case, the document data embodied in the machine readable security feature includes all of the identifiers corresponding to the at least some security elements to be identified. In other preferred embodiments, each of the security elements is associated with the same identifier, common to all of the security elements. That is, each of the security elements is provided with the same detectable serial code or other identifier. In this case, the machine readable security feature need only contain that same identifier, this identifier being compared against the identifiers detected from each of the security elements to be identified.

30

The machine readable security feature may be provided on the document in a number of ways. Preferably, the machine readable security feature is readable by optical recognition (within or outside the visible spectrum). For example, the

machine readable security feature could be printed onto the document, or otherwise applied by means of a label, a transfer or the like. The feature could also comprise perforations or variations in the document thickness such as a watermark, which can be detected in transmitted light.

5

Advantageously, the document data is encrypted such that it is not directly intelligible to an observer. That is, even if the feature itself is visible to a user, it is not understandable without first decoding its meaning. Preferably, the machine readable security feature comprises a 2D barcode, scrambled indicia or
10 a digital watermark. In particularly preferred embodiments, the machine readable security feature is not apparent in the visible spectrum, preferably being formed of a UV, IR or fluorescent ink. As well as hiding the feature from potential counterfeiters, this makes it more difficult to copy since such techniques are not readily available.

15

In other embodiments, the machine readable security feature comprises a RFID chip or a magnetic strip having the document data stored therein. Whilst such features may themselves be visible to an observer, the data therein is not readily accessible without the appropriate reading apparatus. It is also more difficult to
20 manufacture counterfeit features of this sort.

Any number of security elements may be provided on the document, and all or a selection of them may have corresponding identifiers included in the machine readable security feature. The security elements may or may not contain
25 personalisation information. Preferably, at least one of the two or more security elements comprises any of:

- a contactless, readable data store, preferably a RFID chip, containing readable data including a corresponding identifier;

- a printed machine readable code containing a corresponding identifier;

30

- a laser-marked machine readable code containing a corresponding identifier;

- a film applied to the document carrying a machine readable corresponding identifier; and

an optically active element applied to the document carrying data incorporating a machine readable corresponding identifier.

5 The document itself may also form a security element by recording a characteristic of the document and utilising the measurement as an identifier. For example, any dimension, thickness, weight or other measurable characteristic of the document, or a feature thereof, could be used. Preferably, at least one of the two or more security elements comprises at least a portion of the document surface, a surface characteristic of which has been measured and
10 recorded to provide a corresponding identifier. Advantageously, the surface characteristic is obtained by laser surface analysis of the at least a portion of the document surface.

As noted above, it is generally preferable that the identifiers associated with
15 each security element are detectable by machine so that authentication can be carried out automatically. However, such identifiers may still be detectable by a user, e.g. printed data. In some embodiments, it is preferable that the one or more security elements comprises readable indicia incorporating a corresponding identifier which can be compared by an observer against the
20 document data contained in the machine readable security feature. This enables authentication to be carried out with only one machine reading step (or even manually, if the machine-readable security feature is additionally intelligible to an observer).

25 Any number of security elements and corresponding identifiers could be provided. The more security elements for which identifiers are incorporated into the machine readable security feature, the more difficult the document is to forge.

30 The invention can be applied to any document, but preferably, the document is a booklet document comprising more than one page, at least one of the two or more security elements being provided on a first page, and the machine readable security feature being provided on a second page of the booklet

document. In this way, substitution of one or other of the pages will be readily detected.

Advantageously, the document is a document of value, preferably a passport,
5 identification document, banknote, certificate, or licence.

In the method of authenticating, the data contained in the machine readable security feature may be extracted in any manner appropriate for the type of feature in question. Preferably, the machine readable security feature is read by
10 an optical scan of at least a portion of the document.

Likewise, the identifiers may be detected using techniques appropriate to each security element type. Preferably, the identifier associated with at least one of the security elements is detected by at least one of:

15 an optical scan of the security element;
radio frequency interrogation;
magnetic interrogation;
visual observation by a user; and
laser surface analysis.

20

Advantageously, the document data contained in the machine readable security feature is encrypted, and the method further comprises decrypting the document data to retrieve the at least one identifier.

25 Depending on the level of security required, not all of the identifiers stored in the machine readable security feature need be checked against the corresponding security elements. However, preferably, the identifiers associated with each of the security elements for which identifiers are retrieved from the document data are detected and compared with the retrieved identifiers.

30

Examples of documents and methods of authentication in accordance with the present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 schematically illustrates a first embodiment of a document; and

Figure 2 shows a second embodiment of a document viewed in daylight and under UV, with the security elements illustrated at an enlarged scale for clarity.

5

The following description will focus on the example of a passport document. However, as noted above, the invention can be applied to any document type. The invention is most advantageously used in secure documents / documents of value. In the context of a passport, problems that the invention is able to help detect include:-

10

1. Substitution of the MRP (Machine Readable Passport) Data Page
2. Fraudulent Changes to the Data Page (MRZ Zone / Photo)
3. Substitution of the Film (e.g. a holographic overlay film)
4. Chip or Inlay Substitution
- 15 5. Substitution of the page with the passport number on
6. Substitution of a page with a laser perforated number

15

A passport document 10 is shown schematically in Figure 1. The document is of a booklet configuration, having a front cover 11a, a back cover 11b and internal
20 pages including a data page 12a and an adjacent page 12b. On the data page 12a is typically provided personalisation information, such as printed information 13, including the document owner's name, nationality and date of birth, for example, and a photograph 14 of the owner. Commonly, the data page 12a includes a machine readable zone 15 ("MRZ"), in which are printed letters,
25 numbers and other symbols, which can be scanned and processed using optical recognition to retrieve data. The boundary of the MRZ 15 is indicated in Figure 1 using broken lines but in practice this is not typically made visible.

25

30

To protect the personalisation data 13, photograph 14 and MRZ 15, at least a portion of the data page 12a may be covered with a film 16. This typically comprises a polymeric film which is laminated to the page 12a using adhesive and/or heat sealing. The film 16 preferably includes features such as holograms, colour changing inks or other optically variable elements such that

the film cannot easily be reproduced. By covering the data on data page 13 with the film 16, the data cannot be changed without first removing the film 16, which process will typically damage or destroy the film and the security elements contained therein.

5

The document is typically also provided with information on one or more other pages, such as passport number 17 which here is shown on the adjacent page 12b though in practice may be reproduced on every page of the document. The passport number may be printed or could be provided by perforations, for example laser perforations. The passport number 17 may include a check digit symbol such as that disclosed in our International Patent Application Number PCT/GB2007/002551.

The document preferably also includes a data store which can be read without direct contact, such as a RFID chip 18. Figure 1 indicates the RFID chip 18 in the vicinity of internal page 12b, but in practice the RFID chip 18 would typically be provided on the inside face of front cover 11a or back cover 11b, connected to a suitable antenna (not shown). The data contained in RFID chip 18 can be read using a suitable radio frequency reading device as is well known in the art.

20

This embodiment of the invention provides a way of correlating the key security elements found in an MRP (Machine Readable Passport) or ePassport, and to provide a means of detecting whether any of the features have been substituted or changed by using the adjacent page 12b (the one opposite to the MRP data page 12a) of the passport 10 to hold data relevant to at least some of the above-described security elements 15, 16, 17 and 18. This is achieved by providing a machine readable security feature 20 on page 12b containing document data in which is incorporated a number of identifiers associated with at least some of the security elements 15 to 18.

30

In this embodiment, each of the security elements 15 to 18 has been allocated an individual identifier. The manner in which this is done will depend on the type of security element in question. The identifier may be intrinsic to the security

element (e.g. a serial number automatically applied to the element during manufacture), or may be added specially (e.g. printed onto the security element). Generally, the identifier serves to identify the security element itself, rather than the owner of the document: it is preferable that there is no correspondence
5 between the personalisation details and the identifier applied. In this example, MRZ 15 includes an identifier "XYZXYZXYZ" in its machine readable text. This identifier may form part of other information or could be designated as standalone data. The film 16 has marked thereon an identifier 16a formed of the number "987654". The identifier 16a is preferably printed onto the film prior to
10 lamination, on the side of the film 16 which adheres to the data page 12a. Advantageously, the identifier 16a is printed in an ink which responds only outside the visible spectrum (e.g. IR or UV ink), such that it is not visible to an observer.

15 The passport number 17 which is typically printed on or perforated into several internal pages of the document forms its own inherent identifier, in this case consisting of the code "GB12345". The number 17 is typically configured in such a way that the code can be captured using optical recognition techniques. The code may also include a check digit as mentioned above and this can be used
20 on its own or in combination with the rest of the code as an identifier.

The RFID chip 18 is preferably encoded with a serial number during manufacture, as well as personalisation information relating to the passport holder. The serial number can be used as an identifier and can be retrieved by
25 interrogating the RFID chip in the usual way.

Some or all of the above identifiers are incorporated into document data held by the machine readable security feature 20. In this embodiment, this is provided in the form of an optically recognisable printed code applied to page 12b of the
30 document. The code could alternatively be applied in the form of a label, transfer, perforations, etc. Any other page could be used for the feature 20, but the page adjacent the data page 12a is convenient since this is the page the document will be opened to in the usual course of authentication.

The machine readable security feature conveniently embodies the “document data” in a 2D barcode, such as a PDB™ barcode by De La Rue International Limited, or the like. Any type of barcode can be used such as linear barcode, stacked 2D Barcodes (for example Codablock – F and PDF417), and matrix 2D barcodes (for example, Aztec Code, Datamatrix or Semacode). Suitable barcodes and techniques for encoding and decoding the data are disclosed in EP-A-0954801 and EP-A-1471461 to Cobblestone Software, Inc. The barcode may be applied during personalisation of the passport by detecting the identifiers from at least a selection of the security elements provided on the passport, using techniques appropriate to the security elements in question, generating a corresponding barcode by applying predetermined encoding rules, and printing the generated barcode onto the document. Providing the security feature 20 in a format such as a barcode is advantageous because the data contained therein is not directly intelligible to an observer. Further, the potential amount of data which can be stored in the feature 20, and therefore to some degree its security, is significant. Using a barcode allows a greater density of information to be stored per unit area. Also, since the barcode can be unique in its structure, it makes fraudulent alteration of the code extremely difficult. However, in other examples it may be preferred to have at least some of the data in a format which is directly understandable to a user, for example printed in the form of text or numbers.

More than one such barcode or other feature may also be provided, collectively making up the machine readable security feature. In some cases, the various identifiers might be represented individually (i.e. with a code or symbol for each identifier), whereas in other cases the identifiers may be combinedly represented in one code or symbol (such as is the case in the above-mentioned bar code).

For further improved security, the feature 20 may be rendered using security ink, such as an ink which is not perceivable to the human eye under usual lighting conditions, for example a yellow invisible fluorescent ink. The fact the code can

be printed in invisible fluorescent inks adds an additional level of security and complexity to any potential fraudulent alteration or counterfeit attempts.

In this embodiment, the barcode 20 is printed onto page 12b opposite to the MRP page 12a in a resolution that can be detected and read reliably by the optical scanner of an ePassport page reader. Any software that is required for decoding the barcode or other feature can be incorporated into the reader or into a computer system with which the reader communicates. The fact that the decoder software is built into a passport reader makes reverse engineering of the barcode decoder difficult. Since the feature 20 is machine readable, the process of checking and verification can be automatically performed.

The barcode 20 may be read by a dedicated application installed on the passport reader; this would read the barcode, decode the information and then check that all the data matched with that detected elsewhere (from the selected security elements 15 to 18). Although this process could be done on the front desk, at an immigration point, it is more likely to be implemented as a back office check as it may require two separate scans of the passport (e.g. the MRP page 12a and adjacent page 12b in the above embodiment) and/or more sophisticated detection methods for detecting each of the identifiers from the security elements 15 to 18.

It should be noted that whilst the barcode has advantages, as noted above, the use of a barcode is not essential. For example the feature 20 could comprise scrambled indicia (e.g. the document data visually scrambled for reassembly by a suitably programmed reader) or a digital watermark. Alternatively the document data could be printed onto page 12b (or any other page) or stored in some other way in the document 10 (e.g. in the RFID chip 18 or on a magnetic strip). An extension to this would be to hold the document data centrally on a database (as the information would be generated before or during personalisation of the passport) together with the applicant's other biometric and biographic data, with the feature 20 containing a key code for looking-up the relevant identifiers in the database. Information as to which identifier should

correspond to which security element would be pre-programmed. This would enable verification to take place against data held on a central database rather than in the passport itself.

5 In a second embodiment, depicted schematically in Figure 2, the document 10' (shown in daylight at 10'a and as a UV simulation at 10'b) is provided with security elements 15' to 18' which correspond to those described in the first embodiment, the reference numerals having the addition of a prime ('). Here, the passport number 17' is formed by laser perforation and includes a check
10 symbol (circled), and a further security element 19' is provided in the form of a printed number. Optionally, the second embodiment further includes an extra security feature 30 provided by measuring a characteristic of the document 10'. This is described in more detail below.

15 In this example, all of the security elements 15' to 19' are associated with the same identifier, "GB1234996". MRZ 15' includes "GB1234996" on the second line of machine-readable text. The code 16a' provided on the laminate film is also "GB1234996", as is the passport number both laser-perforated 17' and printed 19' onto the document. The RFID chip 18' is programmed with the code
20 "G1234996" in its Datagroup 13 or Datagroup 1 sector, for example. The same code "GB1234996" is stored in the document data embodied by the machine readable security feature 20', which in this case is a 2D barcode but could take any appropriate form as described in the first embodiment. The document data could include the code repeated for each security element. However, since the
25 code is the same for all security elements 15' to 19', the code need only be stored once in the machine readable security feature 20', and can be checked against each of the selected security features.

The first and second embodiments could also be used in combination with each
30 other, for example, a code common to a subset of the security elements (e.g. passport numbers 17' and 19') could be stored alongside individual identifiers for other elements (e.g. the RFID chip 18' and the laminate code 16a').

The second embodiment also makes use of an optional security element 30 in the form of a measured characteristic of the document 10'. In this case, the characteristic is the surface roughness of the document substrate, which can be detected by laser surface analysis. It has been found that many document
5 substrates, such as paper, exhibit surface roughness at a microscopic level which varies from place to place on the substrate, and between substrates (even those of the same type). Hence measuring and recording the surface roughness of a defined area of a substrate is akin to recording a person's fingerprint. Security element 30 therefore consists of a stored surface roughness profile
10 which has been measured for at least a portion of the surface of the document 10', preferably from a page other than that on which the feature 20' is placed. When a document requires authentication, laser surface analysis of the specified area is performed, and the result compared with that retrieved from the document data in the machine readable security feature 20'.

15 Other comparable measurements can also be used as security elements. For example, the measurement could be taken from an element (including a printed element) applied to the document 10' rather than the document itself. For example, the exact dimensions of a line printed in invisible ink could be
20 recorded. Or, if there is a measurable variation in standard page dimensions, weight or thickness, any one or more of these could be measured and recorded.

The scope of the number and/or type of security elements can be a large or small as is required, and could for instance include such features as a laser
25 perforation check digit, laminate film number, taggant information (RFID chip number) etc., as described above. The security elements selected will depend on the application for which the document is intended. Further, it should be noted that not all of the security elements provided on the document need be provided with an identifier and/or recorded in the machine readable security
30 feature. For example, the document may additionally be provided with holograms, embossings, watermarks or any other security elements which may or may not be associated with an identifier recorded in the security feature.

Finally it should be noted that each identifier need not be 'programmed' as such, into the respective security element. A first example is the use of a measured characteristic of the document surface, identified as security element 30 above. In another example, where one of the security elements is an RFID chip, its identifier can be descriptive of its contents, for instance if the chip contains three Datagroup sectors 1, 2 and 7, then this information can be stored in the machine readable security feature as the identifier. If the chip is substituted or the contents of the chip are modified (e.g. a Datagroup is removed), this will be identified by checking the machine readable feature.

Alternatively, the identifier could include a signature of some of the data in the RFID chip. The signature would be generated using the same key as that used to sign the chip data and could be verified using the "Document Signer" key stored in the chip. This is a digital certificate containing a public key which can be used to decrypt a digital signature and verify that it was encrypted with a corresponding private key. The certificate will have been digitally signed by a trusted Certificate Authority and therefore can be validated for authenticity.

Similar 'descriptive' identifiers can be generated for any of the security elements.

CLAIMS

1. A document comprising a machine readable security feature thereon, the document having two or more security elements, each associated with a
5 corresponding identifier detectable from the respective security element, and the machine readable security feature containing document data representative of at least two of the identifiers corresponding to the security elements, to thereby identify at least two of the security elements of the document.
- 10 2. A document according to claim 1, wherein the document data comprises each of the at least two identifiers.
3. A document according to claim 1 or claim 2, wherein the document data comprises a code in which each of the at least two identifiers are incorporated.
15
4. A document according to any of the preceding claims, wherein each of the security elements is associated with the same identifier, common to all of the security elements.
- 20 5. A document according to any of the preceding claims, wherein the machine readable security feature is readable by optical recognition.
6. A document according to any of the preceding claims, wherein the document data is encrypted such that it is not directly intelligible to an observer.
25
7. A document according to any of the preceding claims, wherein the machine readable security feature comprises a 2D barcode, scrambled indicia or a digital watermark.
- 30 8. A document according to any of the preceding claims, wherein the machine readable security feature is not apparent in the visible spectrum, preferably being formed of an ink which luminesces under UV or IR radiation, or an ink which is IR-absorbent.

9. A document according to any of the preceding claims, wherein the machine readable security feature comprises a RFID chip or a magnetic strip having the document data stored therein.

5

10. A document according to any of the preceding claims, wherein at least one of the two or more security elements comprises any of:

a contactless, readable data store, preferably a RFID chip, containing readable data including a corresponding identifier;

10

a printed machine readable code containing a corresponding identifier;

a laser-marked machine readable code containing a corresponding identifier;

a film applied to the document carrying a machine readable corresponding identifier; and

15

an optically active element applied to the document carrying data incorporating a machine readable corresponding identifier.

11. A document according to any of the preceding claims, wherein at least one of the two or more security elements comprises at least a portion of the document surface, a surface characteristic of which has been measured and recorded to provide a corresponding identifier.

20

12. A document according to claim 11, wherein the surface characteristic is obtained by laser surface analysis of the at least a portion of the document surface.

25

13. A document according to any of the preceding claims, wherein at least one of the two or more security elements comprises readable indicia incorporating a corresponding identifier which can be compared by an observer against the document data contained in the machine readable security feature.

30

14. A document according to any of the preceding claims, wherein the or each corresponding identifier is a unique identifier.

15. A document according to any of the preceding claims, wherein the document is a booklet document comprising more than one page, at least one of the two or more security elements being provided on a first page, and the
5 machine readable security feature being provided on a second page of the booklet document.

16. A document according to any of the preceding claims, wherein the document is a document of value, preferably a passport, identification document,
10 certificate, or licence.

17. A method of determining the authenticity of a document, the document comprising a machine readable security feature thereon and having two or more security elements each associated with a corresponding identifier detectable
15 from the respective security element, and the machine readable security feature containing document data representative of at least two of the identifiers corresponding to the security elements, thereby identifying at least two of the security elements of the document, the method comprising:

reading the machine readable security feature to retrieve at least one
20 identifier contained therein;

detecting an identifier associated with at least one of the security elements; and

comparing the identifier retrieved from the machine readable security feature with the identifier detected from the at least one security element to
25 determine whether the security element identified by the machine readable security feature is present on the document, to thereby determine whether the document is authentic.

18. A method according to claim 17, wherein at least two identifiers are
30 retrieved from the machine readable security feature; identifiers associated with at least two of the security elements are detected and the two retrieved identifiers are compared with the two detected identifiers to determine whether the document is authentic.

19. A method according to claim 17 or 18, wherein the machine readable security feature is read by an optical scan of at least a portion of the document.

5 20. A method according to any of claims 17 to 19, wherein the identifier associated with at least one of the security elements is detected by at least one of:

an optical scan of the security element;

radio frequency interrogation;

10 magnetic interrogation;

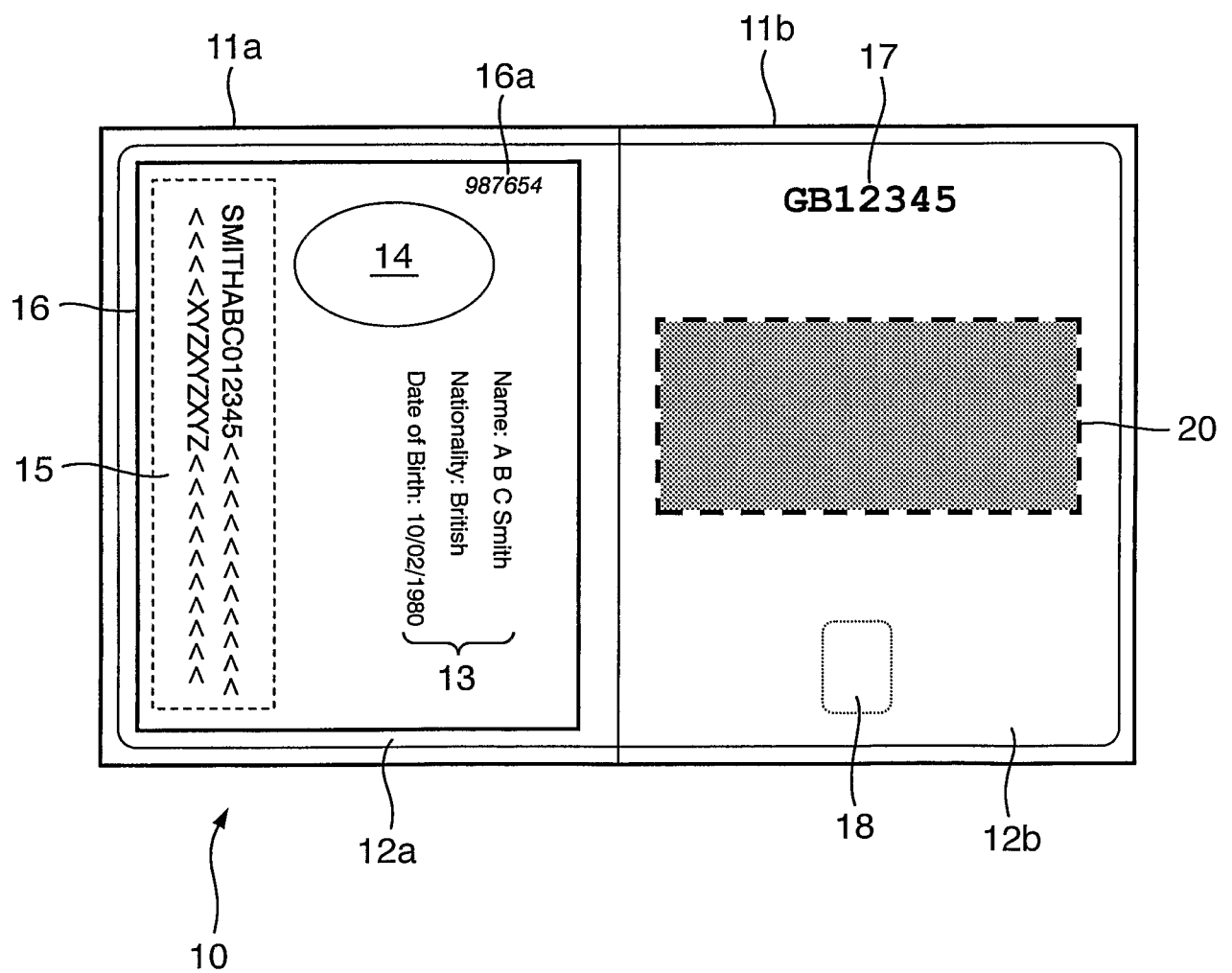
visual observation by a user; and

laser surface analysis.

21. A method according to any of claims 17 to 20, wherein the document data
15 contained in the machine readable security feature is encrypted, and the method further comprises decrypting the document data to retrieve the at least one identifier.

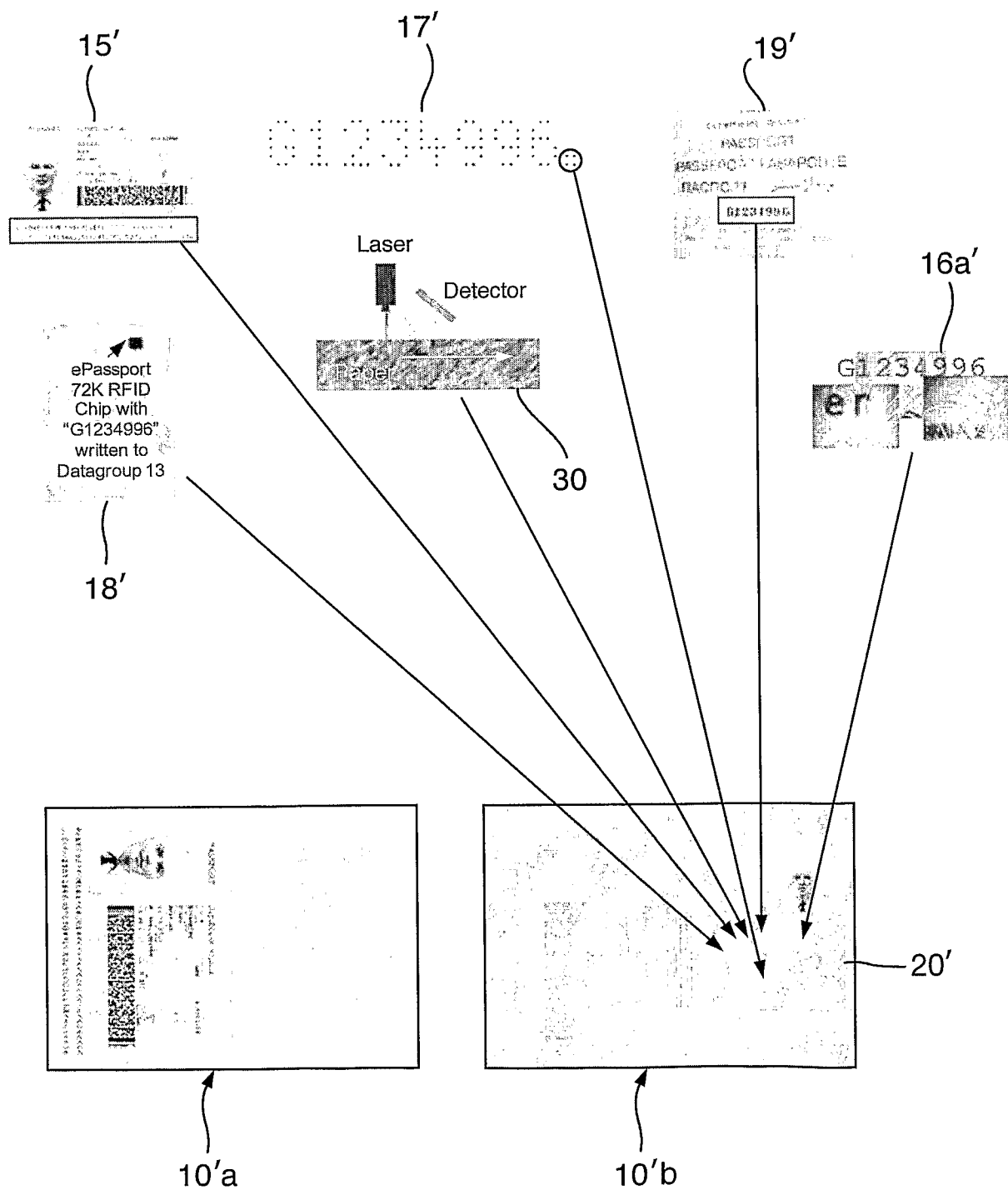
22. A method according to any of claims 17 to 21, wherein the identifiers
20 associated with each of the security elements for which identifiers are retrieved from the document data are detected and compared with the retrieved identifiers.

Fig.1.



2/2

Fig.2.



INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2009/001122

A. CLASSIFICATION OF SUBJECT MATTER

INV. G07D7/00 B42D15/10 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07D B42D G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/38932 A1 (OVD KINEGRAM AG [CH]; TOMPKIN WAYNE ROBERT [CH]; STAUB RENE [CH]) 6 July 2000 (2000-07-06)	1-10, 13-22
A	page 2, line 17 - page 8, line 12 claims 1,9; figures	11-12
X	WO 00/39953 A1 (KENT RIDGE DIGITAL LABS [SG]; WU JIANKANG [SG]; SUN QIBIN [SG]; DENG H) 6 July 2000 (2000-07-06)	1-7, 11-12, 14-17, 19-22
	page 9, line 2 - page 14, line 19 figures 1-7	
	----- -/--	

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

21 July 2009

Date of mailing of the international search report

28/07/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bocage, Stéphane

INTERNATIONAL SEARCH REPORT

International application No

PCT/GB2009/001122

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 991 028 A2 (PANDA ENG INC [US]) 5 April 2000 (2000-04-05) paragraph [0023] - paragraph [0027] paragraph [0057] - paragraph [0073] paragraph [0101] - paragraph [0102] paragraph [0117] - paragraph [0127] figures 1,2,7-18 -----	1-22
A	US 5 913 542 A (BELUCCI BARRY [US] ET AL) 22 June 1999 (1999-06-22) column 3, line 3 - column 6, line 29 figures -----	1,17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2009/001122

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0038932	A1	06-07-2000	AT 224307 T 15-10-2002
		AU 2099500 A 31-07-2000	
		CA 2356314 A1 06-07-2000	
		CH 693986 A5 28-05-2004	
		DE 59902802 D1 24-10-2002	
		EP 1140521 A1 10-10-2001	
		ES 2184519 T3 01-04-2003	
		HK 1038538 A1 28-02-2003	
		PT 1140521 E 28-02-2003	
WO 0039953	A1	06-07-2000	GB 2364513 A 30-01-2002
		US 6748533 B1 08-06-2004	
EP 0991028	A2	05-04-2000	AU 755678 B2 19-12-2002
		AU 5257799 A 06-04-2000	
		CA 2284358 A1 03-04-2000	
US 5913542	A	22-06-1999	AT 193490 T 15-06-2000
		CA 2171450 A1 23-03-1995	
		DE 69424792 D1 06-07-2000	
		DK 719220 T3 16-10-2000	
		EP 0719220 A1 03-07-1996	
		ES 2149283 T3 01-11-2000	
		GR 3034318 T3 29-12-2000	
		PT 719220 E 30-11-2000	
		WO 9507824 A1 23-03-1995	
		US 5505494 A 09-04-1996	
		US 5635012 A 03-06-1997	