(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2007 (28.06.2007)

PCT

(10) International Publication Number
WO 2007/072031 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/GB2006/004876

(22) International Filing Date:
21 December 2006 (21.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0526012.0 22 December 2005 (22.12.2005) GB

(71) Applicant *(for all designated States except US)*: **ADVANCED ANALYSIS AND INTEGRATION LIMITED** [GB/GB]; 120 Riverpark Business Centre, Riverpark Road, Manchester, M40 2XP (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CORRY, John** [GB/GB]; Advanced Analysis and Integration Limited, 120 Riverpark Business Centre, Riverpark Road, Manchester, M40 2XP (GB).

(74) Agent: **McNEIGHT, David, Leslie**; Hill Dickinson LLP, 50 Fountain Street, Manchester, M2 2AS (GB).

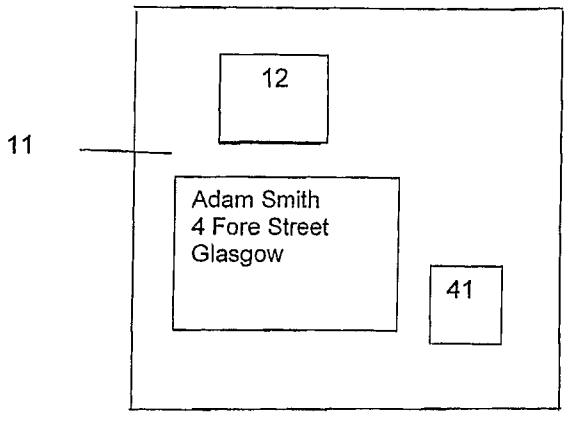
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, 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, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** DOCUMENT VERIFICATION



(57) **Abstract:** A method for personal document verification to confirm whether a document is genuine and/or the holder is the person to whom the document was issued, comprising: • applying to the document a representation of the holder; • sampling the representation at a set of locations thereon and assigning values to the sampled set; • making a record of the assigned values; • checking the document by sampling the representation or a fresh representation made when the document is checked at said set of locations and assigning new values to the sampled set; • correlating the assigned new values with the assigned values in the record; and • indicating a pass or a fail depending on the correlation.

WO 2007/072031 A2

Document Verification

This invention relates to document verification.

Documents can be, and frequently are, forged. There is a need to produce passports, visas and ID cards, for example, that cannot be forged, and one measure that has long been adopted is to include on the document a photograph of the holder, or some other representation that is unique to the holder, such as an iris scan or a fingerprint, or a signature. This representation can then be compared with the appearance of the presenter, or with his signature (widely done with credit cards, for example). A digitised iris scan can be compared against an image made by a camera at the point of examination.

A problem with that is, of course, that a document can be created that is exactly like a passport, say, and a photograph or other representation of the (illegal) holder used, so that the test is passed. However, such a document, while appearing on the face of it to be a genuine document bearing a representation of the holder, would never have been issued, and so a simple check against the database of all such documents issued and not withdrawn would show that the document was a fake.

However, again, a genuine document can be procured, as by theft, and a representation of the new holder substituted for the true holder's representation. While tampering with a genuine document might be detected, the creation of a new document using a true holder's details and a substitute holder's representation, would pass the test and would not have been tampered with, while a database check to see if the document had been issued would show that it had been.

The database might, however, hold the original representation, against which the representation on the document as presented for inspection, or the aspect of the holder freshly imaged at the point of inspection, or both, might be compared. Whilst this might appear to be a huge logistical problem, in the case of credit cards, ID cards, passports and visas, in the context of modern IT, it is well within the competence of systems engineers.

Unfortunately, photographs can fade over time, certainly within the lifespan of a passport, and might not match up with a database record, and fresh images might show substantial differences with an image taken some years ago, as the subject might have aged, or grown or shaved a beard, or undergone plastic surgery, or simply appear under different lighting conditions. So, if an unacceptable level of false negative matches is to be avoided, considerable latitude must be allowed in any comparison, and this gives rise to a risk that forged documents would pass the tests.

The present invention provides improved means for document authentication that overcome these problems.

The invention comprises a method for personal document verification to confirm whether a document is genuine and/or the holder is the person to whom the document was issued, comprising:

- applying to the document a representation of the holder;
- sampling the representation at a set of locations thereon and assigning values to the sampled set;
- making a record of the assigned values;
- checking the document by sampling the representation, at said set of locations. or a fresh representation made when the document is checked and assigning new values to the sampled set;
- correlating the assigned new values with the assigned values in the record; and
- indicating a pass or a fail depending on the correlation.

It has been found that, with photographs, for example, a small number, say ten, of locations, which can be randomly chosen, gives a strong correlation as between faded and fresh data, and between two photographs of the same face, but a low correlation as between photographs of different faces. The locations need not correspond to the usual 'salients', namely, point of chin, tip of nose, centre of pupil and so forth, but of course must correspond as between the two representations. A set of locations might, for example, be chosen as points on a straight line drawn between the centre of the pupil of the left eye and the point of the chin.

The same applies also to iris scans, fingerprints, signatures and indeed any biometric image that may be used.

This, then, deals with the problem of degradation of images, reducing the incidence of false negative comparisons so that the matching criteria can be made quite strict.

The set of assigned values, which might be termed the 'profile', can be recorded in different ways.

The profile might be stored, for example, as digital data in or on the document itself. This would militate against substitution of a representation, e.g. a photograph, for an original on the document. In order to substitute a profile that would match the new representation, it would be necessary to know which set of locations had been used to generate the original profile in order to create a new profile, and substitute the new profile. If the selected location set is not published, this would be impossible.

More than one set of locations might be used across a 'universe' of documents, the set used being noted in or on the document itself in encrypted form. A document reader would extract the appropriate location set from the encrypted information and apply it to generate the new set of values to be correlated against the original profile. This militates against a forger accidentally discovering a selected location set, or figuring out the selected location set by generating all possible location sets and choosing the set which gave the profile recorded on the document from which he was working. This would be a large problem, but not an impossible one for a supercomputer. Multiple location sets, however, would mean that the solution to the problem for one document could not be used in respect of other documents, and would make large scale forgery a very expensive business.

A further measure is to maintain a database holding all, or at least part, of the information on the document, including the assigned values record. In fact, this might be an alternative to holding that record on the document itself, especially where access to the database is readily available, as could be arranged at passport control posts, for example. Moreover, whenever a check is made, the database could write a changed location set to the document so that the next check would involve the changed set.

Writing to a document may be effected using an RFID tag as a component of the document. The tag may itself have a unique identification number, which may be generated from a serial number or from a tag manufacturer's assigned number using a secret algorithm - this militates against the creation of a new tag except by copying from an existing tag, as the number is easily checked for compliance with the algorithm, and in addition, a change can be made to the information carried on the tag each time it is checked, the change being copied to the database. The change can be a simple as incrementing a counter, but may also include detail about thee location of the checkpoint and the date of the check. In the - by now - extremely unlikely event of a document being successfully forged by copying an existing document, with the forger overcoming the problems posed by the biometric measures, it would readily be apparent to the database that more than one document was in circulation, as the counters and the check detail would get out of synchronisation as the two documents circulated.

Whilst these latter measures, used on their own, however, are perfectly satisfactory for frequently-presented items, such as currency notes and credit cards, where it will rapidly become apparent that there are two or more identical cards circulating, passports and visas are not normally presented sufficiently frequently for this to be a full solution to the problem of forgery. And, if a forged or stolen passport is used to enter a country for terrorist purposes, a single presentation is all that may be required of it. In such cases, the biometric measures will be the primary line of defence, but, since with available RFID tags, there is ample space for information and, having set up a database system covering the biometric measures, there is no substantial oncost in attaching the other detail, the comprehensive system would appear to have much to commend it.

Methods for personal document authentication according to the invention, and systems for implementing the same will now be described with reference to the accompanying drawings, in which:

Figure 1 shows a typical personal document such as a passport or ID card;

Figure 2 is a schematic of the registers of an RFID tag;

Figure 3 shows a photograph as might appear on a personal document, marked up with sets of locations for sampling;

Figure 4 is a graph generated from values measured at the locations of one of the sets; and

Figure 5 is a diagrammatic illustration of a checkpoint and a central data processing arrangement including a database containing records including profiles as shown in Figure 4.

The drawings illustrate methods for personal document verification to confirm whether a document is genuine and/or the holder is the person to whom the document was issued, comprising:

- applying to the document - the passport or ID card 11 - a representation, in this case a photograph 12, of the holder;
- sampling the representation 12 at a set of locations - marked on Figure 3 with crosses on line 13 drawn on the representation - and assigning values to the sampled set, such values being, for example grey scale levels of pixels making up a digital image;
- making a record of the assigned values - e.g. digitised co-ordinates of the sample points on the graph of Figure 4 - the record being kept on a RFID tag 41 on the document 11 or in a remote database 55 in a central data processing unit 54, Figure 5;
- checking the document 11 by sampling the representation - as by a linescan or area scan camera 51, Figure 5 - at said set of locations, or a fresh representation, made, for example, by a camera 52, when the document is checked, and reading the profile record by a tag reader 56
- assigning new values to the sampled set;
- correlating, in a data processing arrangement 53, Figure 5, at the checkpoint, or at the central data processing unit 54, the assigned new values with the assigned values in the record; and

- indicating, as on a VDU 55, a pass or a fail depending on the correlation.

The RFID tag 41 can have multiple registers, shown as #1 to #7. Register #1 usually holds a tag manufacturer-assigned number, which, or another user-assigned number, kept, for instance, in register #2, can be used to calculate another number using a secret algorithm. This gives a ready check on authenticity, inasmuch as the only way to produce a number conforming to the algorithm would be to copy an existing number. In documents which are frequently checked and reported back to the central data processing unit, the fact that there were two identical documents would be rapidly noticed, and other measures, such as incrementing a counter in another of the registers, together, perhaps, with entering data concerning the date and place of checks, would rapidly point a trail to discovery of the forged document.

Where documents are not frequently checked, as will be the case with passports and ID cards, the biometric measures will make it extremely difficult to forge a document that will pass the correlation test.

It will be difficult to substitute a photograph, because the set of locations at which the photograph must be sampled is not known. It could theoretically be deduced by systematically selecting sets of sample points and matching the measurements to data on the RFID tag on the document (if there, indeed, is one - even this would be defeated if the only record were kept in the remote database), but this would be a very large problem requiring a long time on a supercomputer.

Figure 3 shows several sets of sample locations - using data from two or more sets for the correlation would make the forgery much more difficult, probably to the point where it would not even be attempted, but switching the data set used for the correlation between available data sets would be daunting in the extreme, especially if it could not be predicted which data set would be used at the next checkpoint.

The representation, as has been suggested above, could be of anything personal to the true holder, a photograph, a fingerprint, an iris scan, a signature, even a voiceprint, all of which can be sampled, sampled values digitised, and correlated.

Where a fresh representation is made at a checkpoint, the image taken, e.g. by a video camera, can be processed by conventional image processing techniques to be scaled and oriented to correspond to the image or other representation on the document.

Claims:

1 A method for personal document verification to confirm whether a document is genuine and/or the holder is the person to whom the document was issued, comprising:

- applying to the document a representation of the holder;
- sampling the representation at a set of locations thereon and assigning values to the sampled set;
- making a record of the assigned values;
- checking the document by sampling the representation or a fresh representation made when the document is checked at said set of locations and assigning new values to the sampled set;
- correlating the assigned new values with the assigned values in the record; and
- indicating a pass or a fail depending on the correlation.

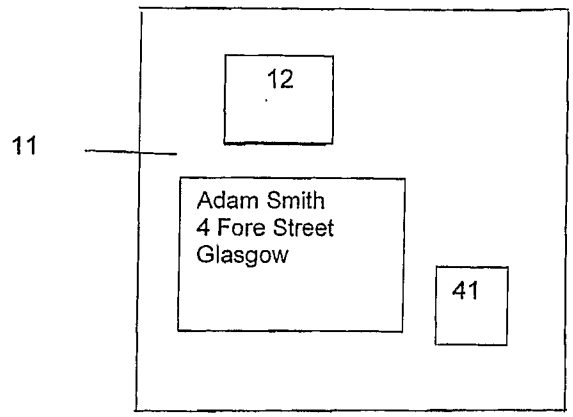


Fig 1

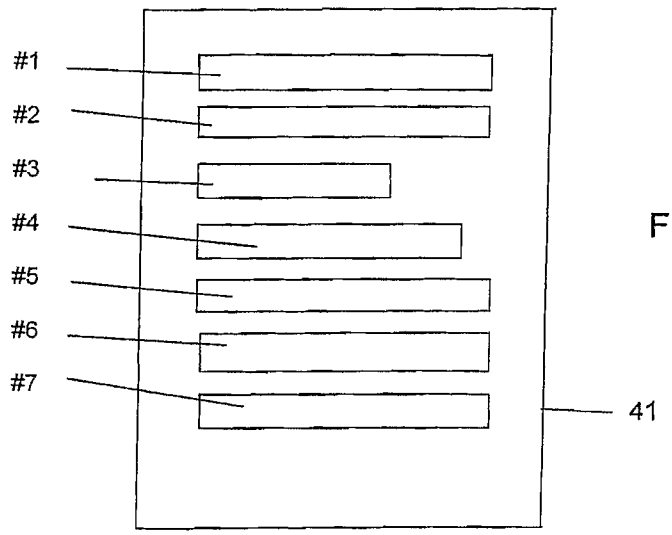


Fig 2

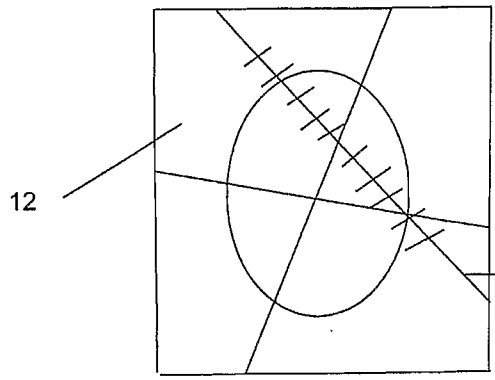


Fig 3

Fig 4

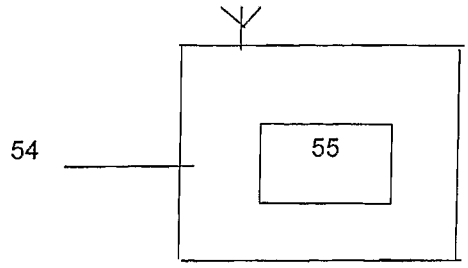


Fig 5