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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 July 2009 (02.07.2009)

PCT

(10) International Publication Number
WO 2009/082199 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *G06K 9/00* (2006.01)

(21) International Application Number:
PCT/NL2008/000277

(22) International Filing Date:
17 December 2008 (17.12.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
07123798.6 20 December 2007 (20.12.2007) EP

(71) Applicant *(for all designated States except US)*: **PRIV-ID B.V.** [NL/NL]; High Tech Campus 9, NL-5656 AE Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAN DER VEEN, Minne** [NL/NL]; Pastoor Haseldonklaan 4, NL-5591 BH Heeze (NL). **AKKERMANS, Antonius, Hermanus, Maria** [NL/NL]; Gareel 27, NL-5502 SB Veldhoven (NL). **KEVENAAR, Thomas, Andreas, Maria** [NL/NL]; Steenhoeve 1, NL-6029 SB Sterksel (NL). **VAN LUIJT, Balthasar, Antonius, Gerardus** [NL/NL]; De Sitterlaan 5, NL-5505 AA Veldhoven (NL).

(74) Agent: **VALKONET, Rutger**; Algemeen Octrooi- en Merkenbureau, P.O. Box 645, NL-5600 AP Eindhoven (NL).

(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, 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*

(54) Title: DISTRIBUTED BIOMETRIC DATABASE AND AUTHENTICATION SYSTEM

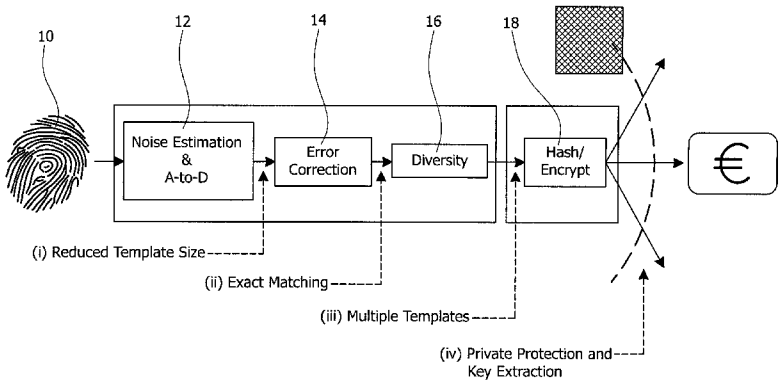

FIG. 1

(57) Abstract: A biometric information system comprising a master database (20), located in a secure, non-networked environment, in which unencrypted biometric data (F1, F2,..., FN) is stored. The system further comprises at least one encrypted operational database (26, 40) in which is stored biometric templates derived from biometric data stored in the master database (20) which has been subjected to biometric encryption such as the application of a one-way transformation of a feature vector representative of the unencrypted biometric data. The master database (20) provides an audit trail should a biometric match be questioned, while the operational database(s) (26, 40) provide the required security for general, day-to-day use.

WO 2009/082199 A1

Distributed biometric database and authentication system.

FIELD OF THE INVENTION

This invention relates generally to a biometric system and, more specifically, to a distributed biometric database and authentication system using biometric encryption.

BACKGROUND OF THE INVENTION

Authentication of physical objects may be used in many applications, such as conditional access to secure buildings or conditional access to digital data (e.g. stored in a computer or removable storage media), or for identification purposes (e.g. for charging an identified individual for a particular activity). Every human being has a unique set of biometric data, such as voice, fingerprints, iris, retina, face, etc. The use of biometrics is, to an ever-increasing extent, considered to be a better alternative to traditional identification means, such as passwords and PIN-codes and, indeed, biometric information is increasingly used to verify and authenticate a person's identity in an ever-growing number of applications and situations.

Typically, the use of biometric information is governed by a trust model, whereby a user receives assurances that the information as provided will only be used for specific purposes and that abuse will be prevented by a security regime for the data. Unfortunately, while in theory this should provide a complete solution that addresses all concerns from citizens and the privacy community, in practice every security regime becomes vulnerable when deployed on a large scale, and widespread use inevitably leads to insider abuse and outside attacks, e.g. by hackers. It will be apparent that biometric applications are a tempting target for identity thieves, so traditional biometric systems have protected biometric templates by storing them in encrypted form. Thus, in order to check the identity of an individual, the template must be decrypted using a key before it can be compared with a live scan. This gives potential identity thieves two opportunities to access the template: intercepting the unencrypted template or stealing the encrypted template and key.

Therefore, the concept of providing intrinsic security by means of biometric encryption, whereby rather than using the original biometrics, a derived dataset is used that has been created via a one-way transformation. The one-way

properties of the transformation guarantee that the original biometrics can never be reconstructed from the stored data, while the transformations are unambiguous enough to be able to perform matches in the encrypted domain.

Referring to Figure 1 of the drawings, there is provided a schematic diagram illustrative of the basic operation of an exemplary solution in this class of approaches to secure biometrics. As shown, the biometric 10 is first scanned and transformed into a regular biometric feature vector. The signal-to-noise ratio is estimated and used (at 12) to reduce the noise levels and template size without losing useful information. Next, error-correction codes are used (at 14) to eliminate and remaining noise effects and minimize error rates, thereby ensuring, to the greatest extent possible, exact matching between templates and corresponding, subsequently-acquired biometric data. Auxiliary data is then combined (at 16) with the feature vector, thereby enabling different templates to be created from the same biometric. This auxiliary data is essentially a random number but, importantly, that number can be different for each person and application. Finally, the or each biometric template (feature vector and auxiliary data) is hashed (at 18) for secure storage. With auxiliary information, each biometric can give rise to many different templates, so any compromised template can simply be revoked and replaced with a new one using the same biometric 10 but different auxiliary information. Furthermore, as each resultant template is radically different, an identity thief who gains access to one template will not be able to use that template to access other applications.

While the system described above uses biometric encryption to solve many of the intrinsic problems associated with traditional biometric authentication and identification systems, there are still some drawbacks. For example, the matching performance of biometric encryption, while similar to that of traditional biometrics, can differ slightly in error rates. More importantly, biometry is embedded in law and case law where, for example, fingerprint matches are accepted as legal evidence if a certain number of minutiae correspond. Biometric encryption has no direct equivalent supported by years of case law. Furthermore, there are a large number of existing databases filled with biometric data within traditional biometric systems, which need to be dealt with. Finally, biometric encryption is a relatively young discipline, such that improvements in algorithms and ciphers can be expected over coming years, and any systems put in place now

should ideally be modifiable accordingly, in order to maintain a required level of security.

It is therefore an object of the present invention to provide a biometric system, using biometric encryption, in which the above-mentioned issues are addressed so as to provide a biometric system in which the required level of security is attained and can be maintained, whilst ensuring that a legally-acceptable audit trail (back to the original biometric data) can be provided, if a biometric match should be challenged, for example, in a court of law.

SUMMARY OF THE INVENTION

In accordance with the present invention, there is provided a biometric information system comprising a master database in which unencrypted biometric data is stored, and at least one encrypted operational database in which is stored biometric templates derived from biometric data stored in said master database which has been subjected to biometric encryption.

Beneficially, the master database is preferably located in a secure, non-networked environment. In one exemplary embodiment, the system comprises a plurality of operational databases, each containing biometric templates generated from said unencrypted biometric data stored in said master database, preferably by a certified authority.

In an alternative exemplary embodiment, a centralized operational database is provided containing biometric templates generated from said unencrypted data stored in said master database, and a centralized authority is permitted access to the contents of said centralized operational database. Beneficially, said centralized authority is configured to provide an authentication service, preferably on-line, to a plurality of applications in the form of organizations or otherwise.

The biometric data stored in said master database may be single or multi-modal. In one exemplary embodiment, said biometric encryption comprises the application of a one-way transformation, such as a one-way hash function, to a feature vector representative of said unencrypted biometric data.

Also, in accordance with the present invention, there is provided a method of providing a biometric information system, comprising the steps of storing unencrypted biometric data in a master database, placing said master database in a secure, non-networked environment, generating a plurality of encrypted biometric

templates by subjecting a plurality of respective pieces of unencrypted biometric data storing in said master database to biometric encryption, and stating said biometric templates in one or more operational databases.

These and other aspects of the present invention will be apparent from, and elucidated with reference to, the embodiments described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described by way of examples only and with reference to the accompanying drawings, in which:

Fig. 1 is a schematic diagram illustrating the principal steps of a biometric encryption method suitable for use in an exemplary embodiment of the present invention;

Fig. 2 is a schematic diagram illustrating some of the principal components of a biometric system according to a first exemplary embodiment of the present invention;

Fig. 3 is a schematic diagram illustrating a method of biometric encryption suitable for use in the system of Fig. 2;

Fig. 4 is a schematic diagram illustrating some of the principal components of a biometric system according to a second exemplary embodiment of the present invention; and

Fig. 5 is a schematic diagram illustrating a method of authentication of biometric data suitable for use in the system of Fig. 4.

DETAILED DESCRIPTION

Thus, the object of the present invention is met by means of a hybrid solution that is characterized by a "separation of purpose". Referring to Figure 2 of the drawings, in accordance with a first exemplary embodiment of the present invention, a dual system is proposed that is characterized by a master database 20 comprising biometric data in its unencrypted form, and a plurality of operational databases 26a, b, c, protected by biometric encryption, intended for broad and daily use. The biometric data may be single or multi-modal, wherein modes of biometric data may comprise, for example, voice, iris, face, retina, fingerprint, etc. The master database 20 is preferably located in a highly secure, protected and non-networked environment 24 and the encrypted operational databases 26a, b, c are then generated from the unencrypted biometric data in the master database 20 by a certified authority (CA) 22.

There are several types of suitable biometric encryption techniques available for use in generation of the encrypted operational databases 26a, b, c. One exemplary method of biometric encryption will be described in detail. However, it will be appreciated by a person skilled in the art that the present invention is not intended to be limited in relation to the type of biometric encryption employed and, indeed, it is an advantage of the present invention that, as new and improved biometric encryption algorithms are developed, the master database 20 can be used by the certified authority 22 to generate a new set of encrypted operational databases by means of the new algorithm(s).

Referring to Figure 3 of the drawings, a biometric feature vector X is retrieved from the master database, and the signal-to-noise ratio is estimated (at 30) and used to reduce the noise levels and data size without losing useful information, following which error-correction codes are applied to eliminate any remaining noise effects. Auxiliary data W is generated or otherwise retrieved and added to the resultant biometric signal X'. The auxiliary data may be in the form of, for example, a random number and, importantly, can be different for each person or template, thus enabling several different encrypted operational databases to be generated from the same set of biometric data.

A one-way hash function F is finally applied to the biometric template comprised of the feature vector X' and the auxiliary data W to generate F(X', W).

As explained above, this encryption process is performed by the certified authority CA, so if a different algorithm or function is required to be applied to the raw data in order to generate a new set of encrypted operational databases, this too can be performed by the certified authority. Furthermore, the certified authority can thus also provide an audit trail if one of the biometric matches is ever challenged, for example, in a court of law.

Referring to Figure 4 of the drawings, in an alternative exemplary embodiment, the raw biometric data is once again stored in a secure environment within a master database 20. However, in this case, a centralized encrypted operational database 40 is provided which is filled with different protected biometric templates derived from the raw biometric data in the master database using, for example, the encryption technique described above in relation to Figure 3. In this case, several applications 42 (e.g. border control, social services, local authorities,

banks and other private organizations) can be served by a centralized authority 44 having access to the encrypted operational database 40. The centralized authority 44 thus provides an on-line authentication service to the applications 42, whereby a biometric sensor 46 local to the application collects biometric data from an individual and transmits it to the centralized authority 44.

Referring to Figure 5 of the drawings, upon receipt of the collected biometric data Y, the signal-to-noise ratio is estimated (at 50) and used to reduce the noise levels and data size, as in the enrolment phase, following which error-correction codes are applied to eliminate any remaining noise effects. Auxiliary data W associated with the individual to which the biometric data is supposed to belong is retrieved and added to the resultant biometric signal Y'.

The resultant data (Y') is transmitted to the centralized authority 44, auxiliary data W associated with the individual supposed to be represented by the biometric data Y is added, and the one-way hash function F is applied to the combination of the biometric data Y' and the auxiliary data W. If the result of F(Y', W) corresponds to the result of F(X', W), then a signal indicating a match is returned to the requesting application 42. Otherwise, data indicating that there is a mismatch is returned.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the invention as defined by the appended claims. In the claims, any reference signs placed in parentheses shall not be construed as limiting the claims. The word "comprising" and "comprises", and the like, does not exclude the presence of elements or steps other than those listed in any claim or the specification as a whole. The singular reference of an element does not exclude the plural reference of such elements and vice-versa. The invention may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In a device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS

1. A biometric information system comprising a master database (20) in which unencrypted biometric data (F1, F2, ..., FN) is stored, and at least one encrypted operational database (26,40) in which is stored biometric templates derived from biometric data stored in said master database (20) which has been subjected to biometric encryption.

2. A system according to claim 1, wherein said master database (20) is located in a secure, non-networked environment.

3. A system according to claim 1, comprising a plurality of operational databases (26), each containing biometric templates generated from said unencrypted biometric data stored in said master database (20).

4. A system according to claim 3, wherein said biometric templates are generated by a certified authority.

5. A system according to claim 1, comprising a centralized operational database (40) containing biometric templates generated from said unencrypted data stored in said master database (20), and a centralized authority (44) is permitted access to the contents of said centralized operational database (40).

6. A system according to claim 5, wherein said centralized authority is configured to provide an authentication service to a plurality of applications (42).

7. A system according to claim 6, wherein said authentication service is made available to said applications on-line.

8. A system according to claim 1, wherein said biometric encryption comprises the application of a one-way transformation, to a feature vector representative of said unencrypted biometric data.

9. A method of providing a biometric information system, comprising the steps of storing unencrypted biometric data (F1, F2, ..., FN) in a master database (20), placing said master database (20) in a secure, non-networked environment, generating a plurality of encrypted biometric templates by subjecting a plurality of respective pieces of unencrypted biometric data storing in said master database (20) to biometric encryption, and storing said biometric templates in one or more operational databases (26,40).

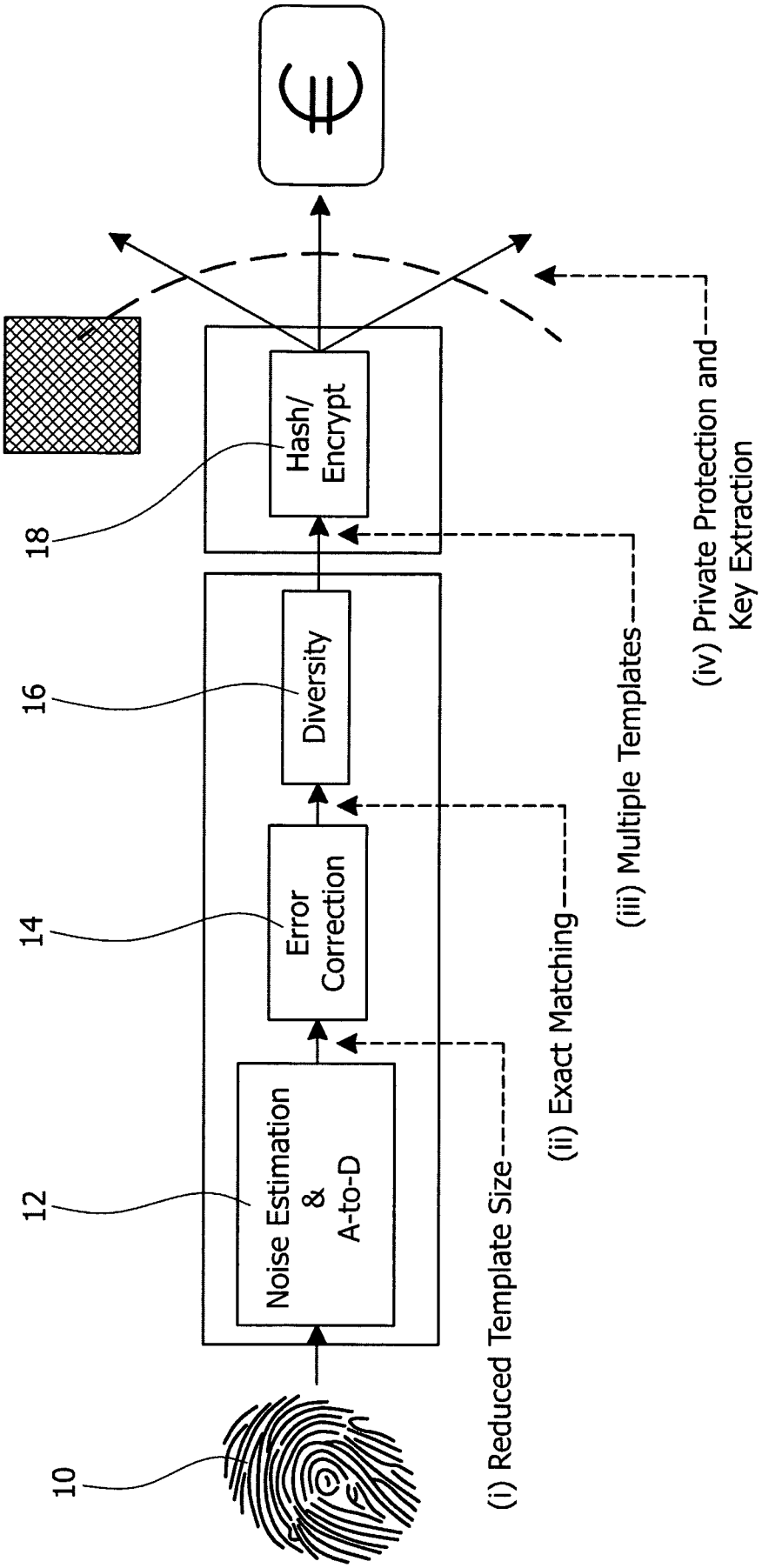
10
12
Noise Estimation & A-to-D
14
Error Correction
16
Diversity
18
Hash/ Encrypt
(i) Reduced Template Size
(ii) Exact Matching
(iii) Multiple Templates
(iv) Private Protection and Key Extraction

FIG. 1

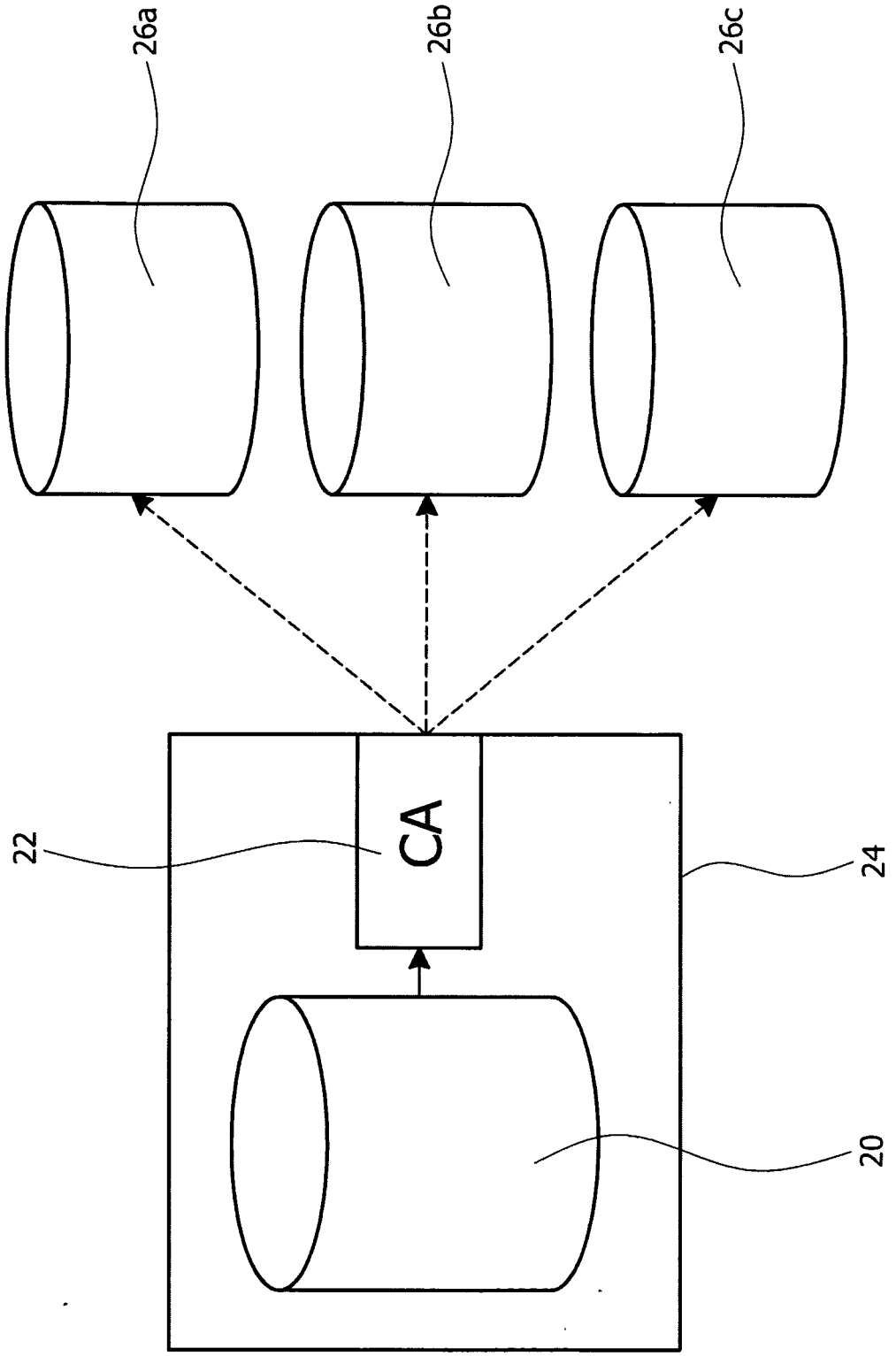

FIG.2

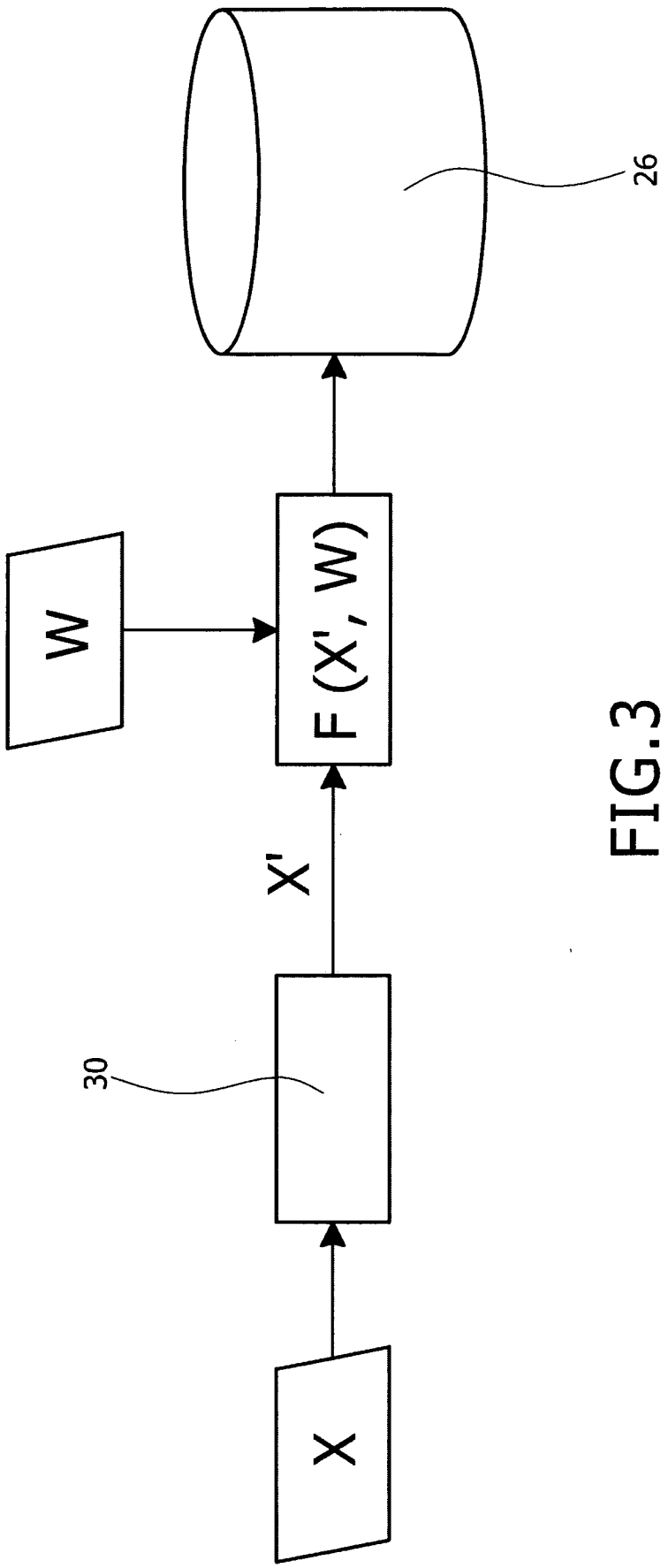

FIG.3

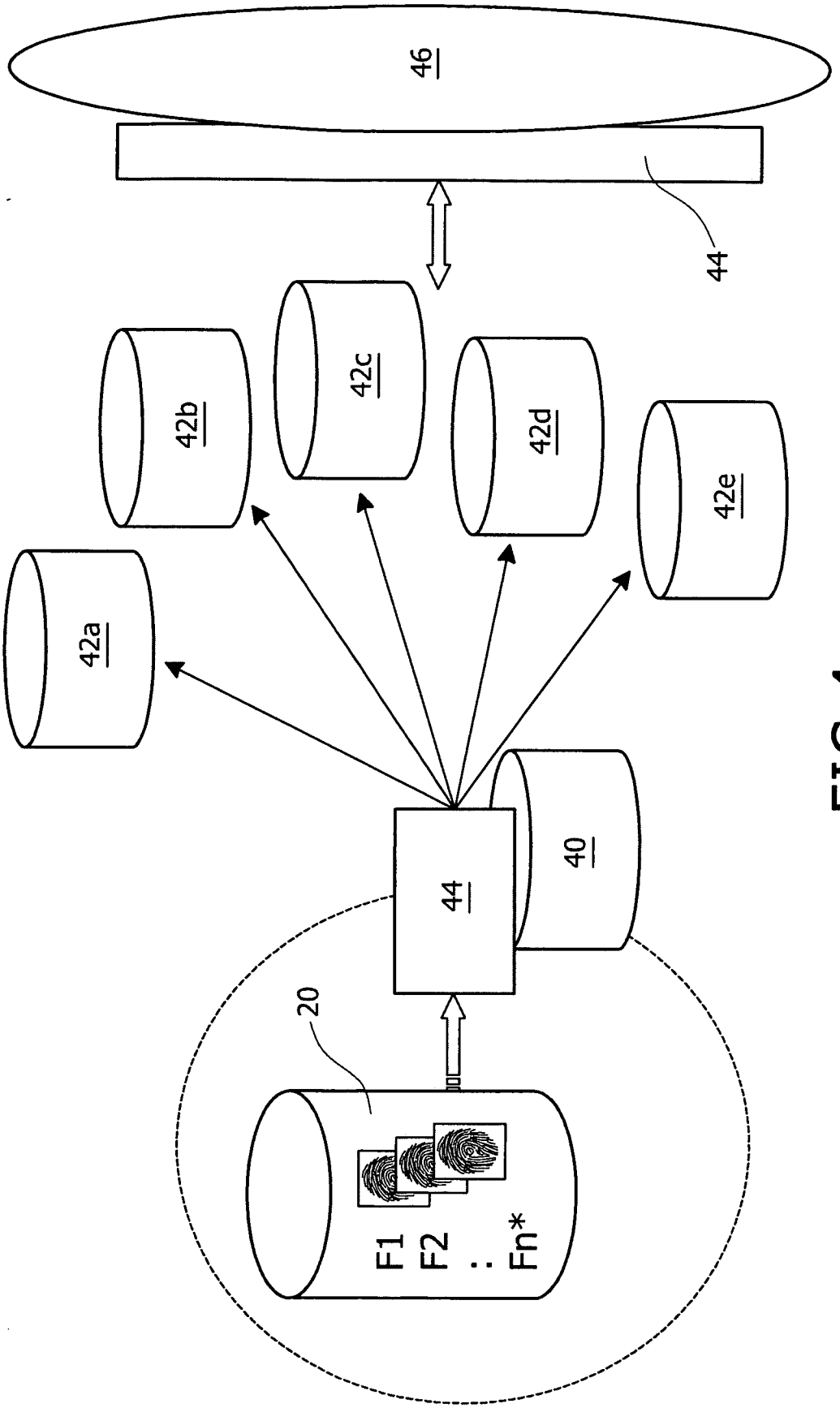

FIG.4

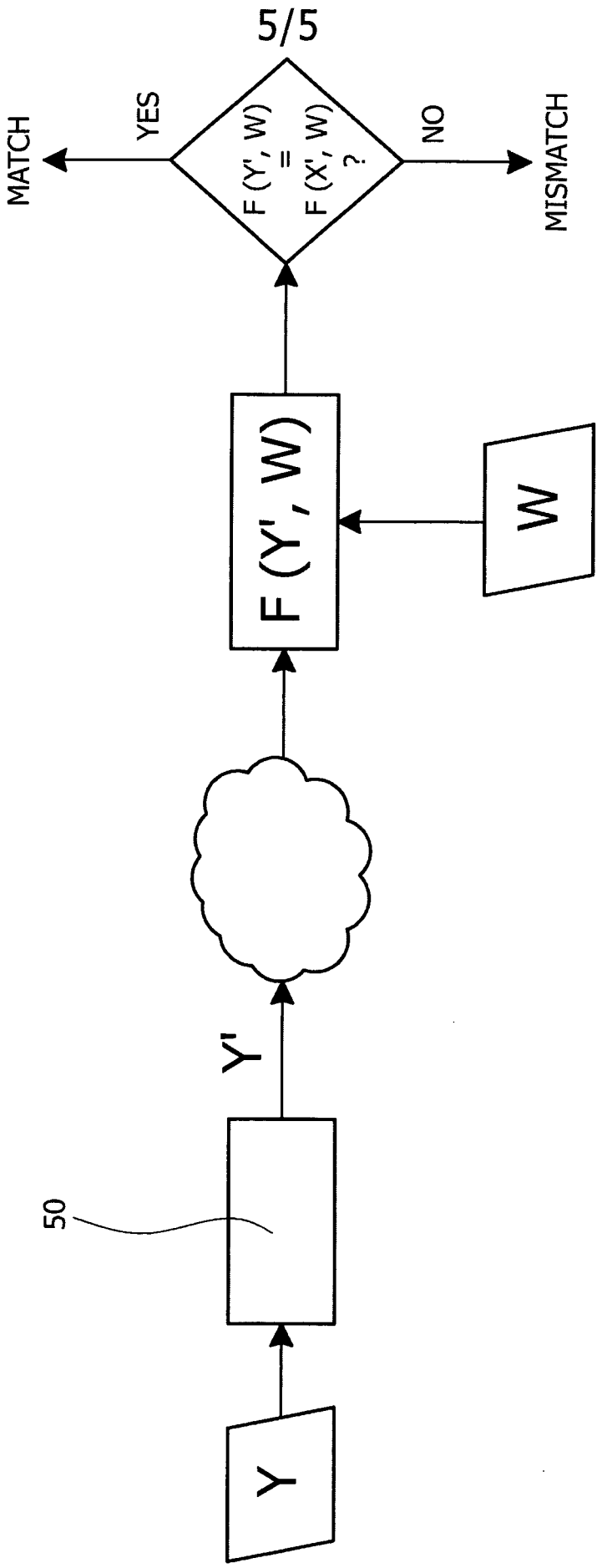

FIG.5

INTERNATIONAL SEARCH REPORT

International application No
PCT/NL2008/000277

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 G06K9/00

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)
G07C G06K

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	US 2007/253608 A1 (TULYAKOV SERGEY [US] ET AL) 1 November 2007 (2007-11-01)	1,2,9
Y	abstract paragraph [0006] - paragraph [0010] paragraph [0027] - paragraph [0029] paragraph [0087]	3-8
Y	WO 02/095657 A (IRIDIAN TECHNOLOGIES INC [US]; BRAITHWAITE MICHAEL [US]; VON SEELEN UL) 28 November 2002 (2002-11-28) abstract page 3, line 1 - line 11 page 10, line 31 - page 13, line 10	3-8
A	US 2004/019570 A1 (BOLLE RUDOLF MAARTEN [US] ET AL) 29 January 2004 (2004-01-29)	1-9

☐ 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	Date of mailing of the international search report
9 March 2009	25/03/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Teutloff, Ivo

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/NL2008/000277

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007253608 A1	01-11-2007	NONE	
WO 02095657 A	28-11-2002	CA 2447578 A1	28-11-2002
		EP 1402681 A2	31-03-2004
		JP 2004537103 T	09-12-2004
		US 2006235729 A1	19-10-2006
		US 2004193893 A1	30-09-2004
US 2004019570 A1	29-01-2004	NONE	