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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/006495 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number:
PCT/SE2003/001181

(22) International Filing Date: 8 July 2003 (08.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0202147-5 9 July 2002 (09.07.2002) SE

(71) Applicant *(for all designated States except US)*: **TIBERG TECHNOLOGY** [SE/SE]; Karlsgatan 9 D, S-722 14 Västerås (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **TIBERG, Martin** [SE/SE]; Karlsgatan 9 D, S-722 14 Västerås (SE).

(74) Agents: **REYIER, Ann-Mari** et al.; Bjerkéns Patentbyrå KB, Box 128, S-721 05 Västerås (SE).

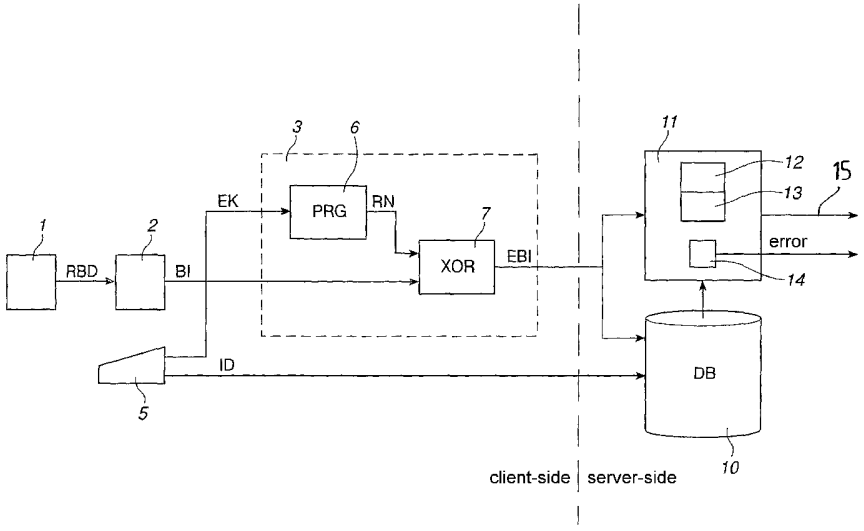
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search 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:** A METHOD AND A SYSTEM FOR BIOMETRIC IDENTIFICATION OR VERIFICATION



(57) **Abstract:** A method and a system for biometric identification or verification of an individual, comprising: a biometric information reader (1), reading reference biometric information, representing a characteristic inherent to the individual, an encrypting unit (3), encrypting the biometric information by means of an encryption key, storing the encrypted reference biometric information as a reference in a database (10), reading current biometric information from an individual, encrypting the current biometric information by means of an encryption key, means for comparing (12) the encrypted current biometric information with the encrypted reference biometric information, and means for deciding (13), based on said comparison, whether the current biometric information originate from the same individual as the reference biometric information (11).

WO 2004/006495 A1

A METHOD AND A SYSTEM FOR BIOMETRIC IDENTIFICATION OR VERIFICATION

FIELD OF THE INVENTION

The present invention relates to a method for biometric identification or verification comprising: reading reference biometric information, representing a characteristic inherent to the individual, encrypting the biometric information by means of an encryption key, storing the encrypted reference biometric information, reading current biometric information from an individual, and encrypting the current biometric information by means of an encryption key.

The present invention also relates to a system for biometric identification or verification of an individual, comprising a biometric information reader for example a scanner, that generates biometric information representing a characteristic inherent to the individual, an encrypting unit, encrypting the biometric information by means of an encryption key, and a memory adapted for storing the encrypted biometric information.

In this application the term biometric information relates to physiological characteristics and behavior such as fingerprints, voiceprints, hand geometry, typing characteristics, facial appearances or signatures representing a characteristic inherent to an individual.

The invention is particularly useful in connection with authorization systems that verify the identity of a known person and authorize the person to perform an action. The action can be for example a financial transaction, such as check cashing, the use

of a credit card or an automatic teller. The invention is also useful for identifying an unknown person by using biometric information. In a biometric identification system, biometric information from an individual is compared with stored information from many individuals in order to identify the individual.

PRIOR ART

It is known in the art to use biometric information for identification and verification of an individual. Known methods for biometric identification and verification of an individual comprise reading biometric information from individuals, transferring the biometric information to a database and store the information as references. When a person is to be identified, or the identity of the person is to be verified, biometric information is obtained from the person and compared with the stored reference information. For security reasons the reference biometric information is often encrypted before being transferred to and stored in the database. In some applications, the information is decrypted before being stored in the database and in other applications, the encrypted information is stored and decryption takes place after retrieval from the database. In both cases the comparison is carried out on decrypted biometric information.

An example of such a biometric system is disclosed in the US patent document US 6,317,834 B1. Biometric templates are stored in a biometric database. Before the biometric templates are stored, they are encrypted by means of an encryption algorithm using a cryptographic key derived from a password. When an individual whishes to access a secured resource, he must provide a biometric sample and a correct password to allow the system to decrypt the stored templates before comparing the biometric sample with the biometric templates.

A disadvantage with systems for biometric identification or verification is that once the biometric information has been con-

verted to electronic form it is possible to steal it. Since the biometric information is unique, it is not possible to change it and thus the damage is irreparable. This problem becomes especially severe when you use the same biometric information, for example your fingerprint, in several different security systems. You have only one fingerprint and if it is stolen the security of all biometric system using this fingerprint is compromised. The thief can now and everlastingly penetrate all the security systems, which are based on your fingerprint. It is known to protect the biometric information from being stolen by an outsider by encrypting the information when it is transferred over a network before it is encrypted and compared with the reference information. However, there must always be some trusted insiders to administrate the biometric security system along with the database, where the biometric information is stored, and it is still possible for the trusted insider to get hold of the decrypted information.

SUMMARY OF THE INVENTION

The object of the present invention is to provide a method for biometric identification or verification of an individual, which provides a higher degree of flexibility, integrity and privacy for the individual than existing methods.

This object is achieved by the initially defined method, characterized in that it comprises comparing the encrypted current biometric information with the encrypted reference biometric information, and, based on said comparison, deciding whether the current biometric information originates from the same individual as the reference biometric information. Thanks to the fact that encrypted biometric information is compared, instead of decrypted biometric information, as in the prior art, the decryption step is omitted and no original biometric information will be stored in any database. Thus, the original biometric information is not accessible to any trusted insider. The security and the in-

tegrity and privacy of the individual are improved since only encrypted biometric information is handled. Not even trusted insiders will have the possibility to get hold of the original biometric information.

Since the reference and current encrypted information are compared, a condition for obtaining successful identification/verification of the individual is that the same encryption key is used for encrypting both the current biometric information and the reference biometric information. In an embodiment of the invention that condition has been utilized for further improvement of the security in the biometric system. In this embodiment, the individual biometric information is combined with a secret encryption key chosen by or assigned to the individual. The encryption key may, for example, be derived from a password, from information stored on a smart card, from the biometric information itself, or from a separate computer application. This embodiment comprises receiving a first encryption key, encrypting the reference biometric information by means of the first encryption key, receiving an second encryption key, and encrypting the current biometric information by means of the second received encryption key, and successful verification/identification of the individual is only possible if the first and the second encryption key are equal. If different encryption keys are used the comparison will fail. Accordingly, the security is further enhanced.

This embodiment provides the possibility to feed the encryption key to the system, which allows the encrypted information to easily be changed by simply changing the encryption key. Thus, if the encrypted biometric information is stolen, the user only needs to change to another secret encryption key and store new reference biometric information encrypted by means of the new encryption key in order to render the stolen information useless. It is also possible to use different encryption keys in different identification or authorization systems. This procedure makes it

impossible to discover relationships between the same biometric information stored in different systems and accordingly the privacy of the individual is enhanced. A further advantage with using different encryption keys in different systems is that encrypted biometric information stolen from one system is useless in the other systems.

According to an embodiment of the invention, said comparison is performed by means of a statistical test. Preferably, said comparison comprises calculation of the correlation between the encrypted current biometric information and the encrypted reference biometric information, and the encryption is performed by means of an encryption method that retains the correlation between the encrypted information. Comparing biometric information is not a matter of simply comparing two numbers and determining whether they are equal or not. The exact encoding of each digital copy of the biometric information stemming from the same biometric characteristic of the same individual depends on the outside circumstances and when it is read it may fluctuate between different points of time. For instance, reading of fingerprints may depend on the temperature of the finger, the ambient humidity, and the orientation of the finger. Thus, the result of a reading of a fingerprint is not necessarily the same as the result of an earlier reading of the same finger.

By calculating the correlation between the reference and current biometric information, it is possible to determine whether the two originates from the same individual. Most of the conventional encryption methods change the biometric information such that any correlation between the reference and current information is lost after encryption. Therefore, it is impossible to use the encrypted information to determine whether the information originates from the same individual. According to the invention, an encryption method is chosen that retains the correlation between the encrypted information.

According to an embodiment of the invention, said encryption method comprises generating a random number using said encryption key and then generating encrypted biometric information based on said random number and the biometric information. Methods for encryption and decryption of information using random numbers are well known in the art. If bit-wise XOR-operation is used between the information and the random number it is called stream cipher. Such methods have the property of retaining the correlation between encrypted samples. Although it is known in the art to encrypt and decrypt information based on such methods, it is not known to utilize their property of retaining the correlation between encrypted information, in connection with encryption of biometric information.

The encrypted biometric information may be generated by any kind of transformation method based on the encryption key. It may act on each single bit, on blocks of data or on the whole data set. In an embodiment of the invention the encrypted biometric information is generated by convolving said random number and the biometric information. The convolving includes operations such as XOR, AND, NAND, OR, NOR. Before convolving them, the biometric information and the random number are converted to a binary stream of bits. It is important to have a uniform representation of data during processing. Preferably, the data is represented binary, but other representations are also possible, such as hexadecimal notation.

According to an embodiment of the invention, the method comprises determining whether the encrypted current biometric information and the encrypted reference biometric information are identical and if so generate an error signal. As mentioned before, biometric information from an individual normally fluctuates. It is extremely unlikely that two samples are identical taken at different points in time. If current biometric information is exactly identical to the stored biometric information, it is a potential fraud. Someone may have stolen the encrypted biometric

information and is trying to get access to the system using the stolen information.

A further object of the present invention is to provide a computer program product directly loadable into the internal memory of a computer, comprising software code portions for performing the steps of any of the methods according to the invention, when said product is run on a computer.

A further object of the present invention is to provide a computer readable medium having a program recorded thereon, where the program is to make a computer perform the steps of the method according to the invention when said program is run on the computer.

A further object of the present invention is to provide a system for biometric identification or verification of an individual, which system provides a higher degree of security, privacy and flexibility for the individual than existing systems.

This object is achieved by means of the initially defined system further comprising a comparator, comparing currently generated and encrypted biometric information with previously generated and encrypted biometric information, which is stored as a reference, and means for deciding, based on said comparing, whether the current biometric information originates from the same individual as the reference biometric information

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be explained more closely by the description of different embodiments thereof and with reference to the appended figures.

Fig. 1 shows a block diagram of a verification system for biometric identification or verification of an individual according to an embodiment of the present invention.

Fig. 2 shows flow chart of a method for biometric identification or verification of an individual according to an embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Figure 1 shows a verification system for verifying the identity of a user. The verification system comprises two computationally separated parts: a client side, which acquires the inputs and initiates the verification process, and a server side, which performs matching of current user biometric information and previously stored reference biometric information. The data can be transferred between the client side and the server side in many different ways, for example wirelessly, by means of an optical link, a computer network or the Internet. Data may or may not be secured by encryption during the transfer.

The verification system comprises a biometric reader 1 which is used to read raw biometric data RBD from an individual. The reader is for example a scanner or an ultra sound detector. The present invention is independent of the type of biometrics used. Thus, the biometric reader can be any device that digitalizes any of the user's behavioral or physiological characteristics. The biometric reader is for example an image inputting device and then the raw biometric data is for example image data. The raw biometric data RBD is transferred to a feature extractor 2. The feature extractor 2 extracts from the raw biometric data features that are unique to the user. The output from the feature extractor 2 is biometric information BI comprising said unique features being useful for verification of the identity of the user. For example, if the biometric data represent a fingerprint, the biometric

reader 1 is a fingerprint reader and the feature extractor 2 receives the data read by the fingerprint reader and extracts unique feature of the fingerprint appearing in that image. The biometric information BI generated by the feature extractor 2 is transferred to an encrypting unit 3 for encrypting of the biometric information. The encryption unit 3 comprises a pseudo random number generator 6 and an XOR function 7.

The client side also comprises an input device 5, for example a keyboard that is used for input of a user's ID and a password. In this case, the password is an encryption key EK, but in another embodiment, an encryption key may be derived from the password. The encryption key EK is transferred to the encrypting unit 3. Thus, input to the encryption unit 3 is the encryption key EK and the biometric information BI from the feature extractor 2. The encryption key and the biometric information must be converted into a stream of binary bits of 0 and 1, in case they are not already in that form. Computers almost exclusively communicate by bit streams; thus, the conversion consists simply of retrieving the input data in their raw forms. However, it is possible to implement a more sophisticated conversion algorithm, which has the biometric information and the encryption key as inputs in non-binary representation and encodes them into binary bit streams using any kind of encoding scheme. Preferably, the encoding scheme makes the bit streams as short as possible.

The encryption key EK is fed as a seed to the pseudo random number generator 6 that outputs a random number RN. The output from the random number generator is terminated when the random number has the same length as the biometric information BI received from the feature extractor 2. The encryption key uniquely determines the output of the pseudo-random number generator and the output cannot be reverse-engineered. A pseudo random number generator has the mathematically proven property: if the encryption key is k bits long and totally

unknown, the random number generated cannot be distinguished from a truly random number of the same length by any statistical test which runs in poly-nominal time in k. Further definitions and properties of pseudo random number generators are disclosed in a book by Goldreich, O., "Foundations of Cryptography: Basic Tools", ch. 3, Cambridge University Press, 2001. A pseudo-random number generator particularly suitable for this application is disclosed in a document written by Gennaro, R., "An Improved Pseudo-Random Generator based on the Discrete Logarithms Problem", Crypto2000, pp. 469-481. For the implementation of the pseudo-random generator assumes knowledge of certain key algorithms, which are found in a book by Schneier, B., "Applied Cryptography", 2nd E d ., John Wiley & Sons, 1996.

The biometric information BI is convolved with to the random number RN by use of an XOR-operation. The output from the encrypting unit 3 is encrypted biometric information EBI. The encrypted biometric information EBI is transferred together with the corresponding user ID to the server side. The server side comprises a database 10 in which encrypted biometric information is stored together with the user ID. Encrypted biometric information samples from all individuals being enrolled in the system are stored as references together with their user ID in the database. The server side also comprises a verifying unit 11, which decides whether or not read biometric information belongs to the eligible person. The verifying unit 11 comprises a comparator 12, comparing current encrypted biometric information with the reference information stored in the data base 10 and means 13 for deciding based on said comparison, whether the current biometric information originates from the same individual as the reference biometric information.

Due to fluctuation in the biometric data received, the comparison has to be based on a statistical test. This statistical test checks whether the encrypted biometric information and the encrypted

reference biometric information match to a satisfactorily high degree. For this purpose, the correlation between the current and the encrypted reference biometric information is calculated. If the correlation is within an allowed range, an approval signal 15 is generated and if the correlation is outside the allowed range, a disapproval signal is generated. The method used for measuring the correlation can be any of the methods known in the art. Which correlation method is used depends on the type of biometric data, how the algorithm inter-operates with the feature extractor and other factors.

The server side may further comprise a second comparator 14, comparing the current and the previously stored encrypted biometric information. This second comparator 14 compares the information and generates an error signal, if the biometric samples are identical. The purpose of this second comparator is to prevent reuse or theft of digital biometric information. The nature of biometrics is such that two samples of the same biometric type from the same individual closely resembles each other. However, it is extremely unlikely that two samples will be identical. If that is the case, it is more likely that someone has duplicated the electronic version of the encrypted biometric information and reuses it. As a protection against such copying, the system comprises a test of whether the encrypted biometric information samples are identical and it generates an error signal if they are identical.

Figure 2 is a flow-chart illustration of the method and the computer program product according to an embodiment of the present invention. It will be understood that each block of the flow-card can be implemented by computer program instructions run on one or several computers. In the present embodiment the program is run on two computers, a client computer and a server computer. In block 20, biometric information BI1 is read from the feature extractor 2, and the password EK and the user ID is read from the keyboard 5. In this embodiment the password is equal

to the encryption key. If the password is not equal to the encryption key, an operation has to be performed to derive the encryption key from the password.

In block 21, the biometric information BI1 is encrypted. The encryption key EK is used as a seed to the pseudo-random generator 6 that generates a random number RN. The random number RN and the biometric information BI1 are convolved by an XOR operation. As a result, encrypted biometric information EBI1 is obtained. The encrypted biometric information EBI1 and the ID are transferred from the client side to the server side. The encrypted biometric information EBI1 and the ID are stored in the database 10 as a reference for future verification of that person, block 22. The database comprises encrypted reference biometric information from all persons being authorized in the system.

When a person is to be authorized by the system, his biometric data are read and he enters the password and the user ID. If necessary, the encryption key is derived from the password. For the authorization to be successful, the encryption key must be the same as the encryption key used for encryption of the reference biometric information. If the encryption key is not the same, the verification process will fail. The biometric information BI2, the encryption key EK, and the user ID are read by the system, block 23, and encrypted in the same way as the reference biometric information BI1, block 24. The encrypted biometric information EBI2 is transferred to the server side together with the user ID. The encrypted reference biometric information EBI1 corresponding to the ID is retrieved from the database 25.

In block 26, the received encrypted biometric information EBI2 is compared, bit-by-bit, with the stored encrypted reference biometric information EBI1. If they are identical, an error signal is generated. The encrypted biometric information EBI2 is also

compared with the reference encrypted biometric information EBI1 by calculation of the correlation between them, block 27. Based on the degree of correlation between EBI1 and EBI2, it is decided whether the current biometric information EBI2 originates from the same individual as the reference biometric information EBI1, block 28. If the correlation is high, the system generates an approval signal, block 29, and if the correlation is low, a disapproval signal is generated, block 30.

The present invention is not limited to the embodiments disclosed but may be varied and modified within the scope of the following claims. For example the method is described in connection with verifying the identity of a user, but it could just as well be used for identifying a user. If a user is to be identified, no user ID is provided to the system. The encrypted biometric information is compared with stored encrypted reference biometric information originating from many individuals, and if any of the database records with reference information is found having a high correlation with the current biometric information the person is identified.

The step of determining whether the current encrypted biometric information and the previously stored encrypted biometric information match to a satisfactorily high degree for approval, comprises the use of a criterion, for example a range for the correlation. This matching criterion could either be fixed or adjustable, such that a third-party application or some other component connected to the system can specify the required criterion and range. The adjustable range or criterion may be specified for each user or application. In an embodiment of the invention, the encrypted reference biometric information in the database may be automatically adjusted in connection with approval. By blending the current and the reference encrypted biometric information using some blending criterion, new encrypted biometric information may be created, which can replace the encrypted reference biometric information. This new encrypted

biometric information is likely to better corresponding to the real biometric of the person, since it is created using an additional biometric sample, which is acquired more recently than the old reference sample.

In another embodiment, it is possible to use several types of biometrics. A third-party application or some other component of or connected to, the system can specify the required criterion for approval. That criterion may be based on any one of the biometrics used in the system or a combination of several biometrics.

In the embodiment disclosed, the system comprises two separate parts each including at least one computer. However, those separate parts do not necessary need to be separated. Those parts may be put together and be integrated in a stand-alone application, which needs a biometric security mechanism.

The invention is not limited to identification/verification of human beings but could also be applicable on animals. The biometric characteristics may also comprise a physical object belonging to an individual, such as a watch or piece of jewellery.

CLAIMS

1. A method for biometric identification or verification of an individual, comprising:
- reading reference biometric information, representing a characteristic inherent to the individual,
- encrypting the biometric information by means of an encryption key,
- storing the encrypted reference biometric information as a reference,
- reading current biometric information from an individual,
- encrypting the current biometric information by means of an encryption key, characterized in that the method further comprises:
- comparing the encrypted current biometric information with the encrypted reference biometric information, and
- deciding, based on said comparison, whether the current biometric information originate from the same individual as the reference biometric information.

2. A method according to claim 1, characterized in that the same encryption key is used for encrypting the reference biometric information and the current biometric information.

3. A method according to claim 1, characterized in that it further comprises: receiving a first encryption key, encrypting the reference biometric information by means of the first encryption key, receiving an second encryption key, and encrypting the current biometric information by means of the second received encryption key, and a condition for successful verification/identification of the individual is that the first and the second encryption key are equal.

4. A method according to any of the previous claims, characterized in that said comparing is performed by means of a statistical test.

5. A method according to any of the previous claims, characterized in that said comparing step comprises calculation of the correlation between the encrypted current biometric information and the encrypted reference biometric information, and that the encryption is performed by means of an encryption method that retains the correlation between the encrypted information.

6. A method according to claim 5, characterized in that said encryption method comprises generating a random number using said encryption key and then generating encrypted biometric information based on said random number and the biometric information.

7. A method according to claim 6, characterized in that the encrypted biometric information is generated by convolving said random number and the biometric information.

8. A method according to claim 7, characterized in that the biometric information and said random number are converted into a binary stream of bits before convolving them.

9. A method according to any of the previous claims, characterized in that the method comprises determining whether the encrypted current biometric information and the encrypted reference biometric information are identical and generate an error signal if they are identical.

10. A computer program product directly loadable into the internal memory of a computer, comprising software code portions for performing the steps of any of the claims 1–9, when said product is run on a computer.

11. A computer readable medium having a program recorded thereon, where the program is to make a computer perform the

steps of any of the claims 1–9, when said program is run on the computer.

12. A system for biometric identification or verification of an individual, comprising
- a biometric information reader (1), reading biometric information representing a characteristic inherent to the individual,
- an encrypting unit (3), encrypting the read biometric information by means of an encryption key (EK),
- a memory (10), adapted for storing the encrypted biometric information, characterized in that the system further comprises
- a comparator (12), comparing currently read and encrypted biometric information with previously read and encrypted reference biometric information, and
- means for deciding (13), based on said comparison, whether the current biometric information originates from the same individual as the reference biometric information.

13. A system according to claim 12, characterized in that said comparator (12) comprises means for calculation of the correlation between the encrypted current biometric information and the encrypted reference biometric information, and that said encryption unit (3) is using an encryption method that retains the correlation between the encrypted information.

14. A system according to claim 13, characterized in that said encryption unit (3) comprises a pseudo-random number generator (6) using the encryption key (EK) for generation of a random number and the encryption means is adapted to generate encrypted biometric information based on said random number and the biometric information.

15. A system according to claim 14, characterized in that the encrypting unit (3) is adapted to generate encrypted biometric information by convolving said random number and the biometric information.

16. A system according to any of the claims 12-15, characterized in that it comprises a second comparator (14), comparing said currently read and encrypted biometric information with said previously read and encrypted reference biometric information, and an error signal generator, generating an error signal if the encrypted current biometric information and the encrypted reference biometric information are identical.

17. A system according to any of the claims 12-16, characterized in that is comprises an input means (5), for feeding said encryption key (EK) to the system.

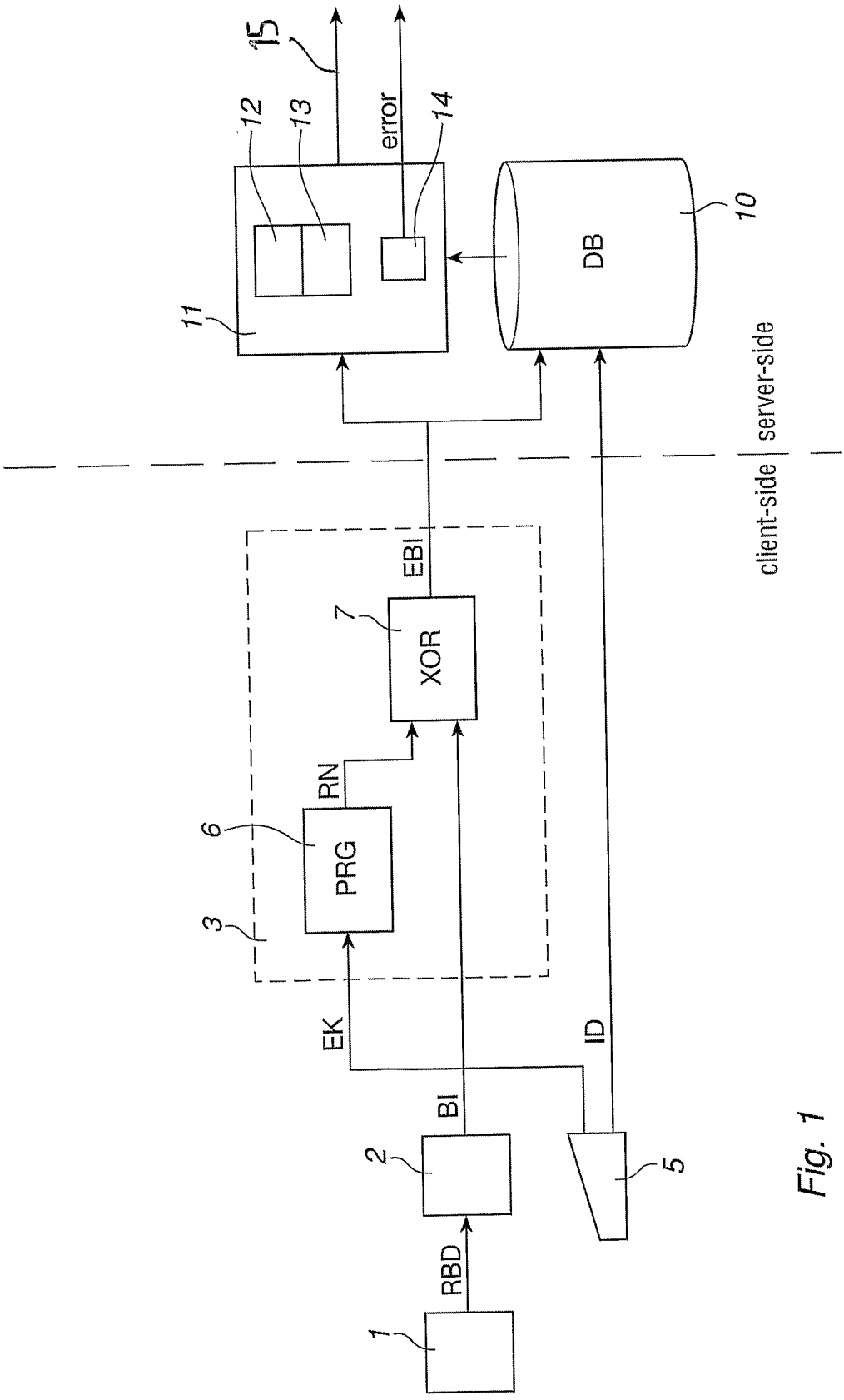

15
12
13
error
14
11
DB
10
client-side
server-side
EBI
7
XOR
RN
6
PRG
3
EK
ID
BI
2
5
RBD
1

Fig. 1

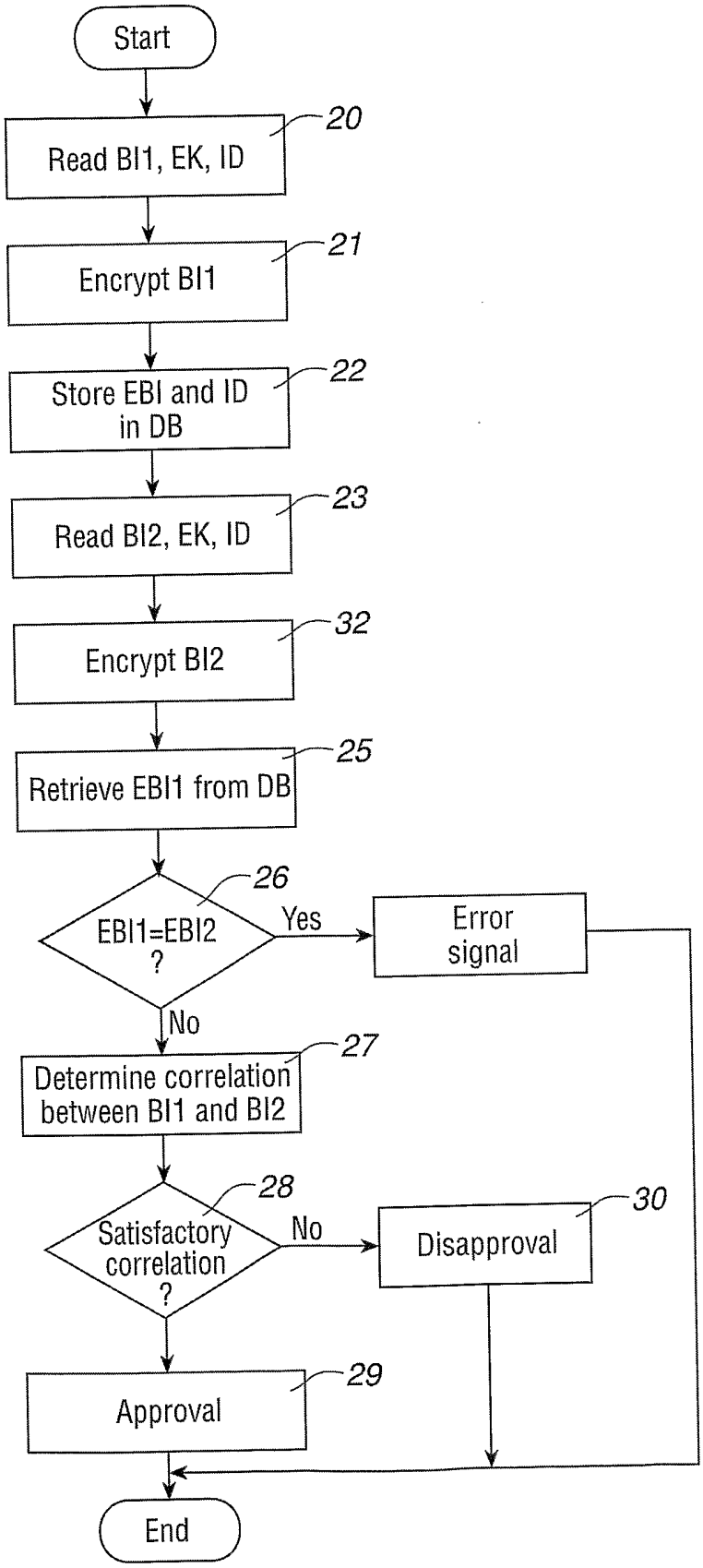

Start
Read BI1, EK, ID
20
Encrypt BI1
21
Store EBI and ID in DB
22
Read BI2, EK, ID
23
Encrypt BI2
32
Retrieve EBI1 from DB
25
EBI1=EBI2 ?
26
Yes
Error signal
No
Determine correlation between BI1 and BI2
27
Satisfactory correlation ?
28
No
Disapproval
30
Approval
29
End

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 03/01181

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/08
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)

IPC7: H04L

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, 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 0201314 A2 (MULTIMEDIA GLORY SDN BHD), 3 January 2002 (03.01.02), figure 4, claim 1	1,10-12
A		2-9,13-17
	--	
A	EP 0973123 A1 (LUCENT TECHNOLOGIES INC.), 19 January 2000 (19.01.00), see the whole document	1-17
	--	
A	EP 0918300 A2 (TRW INC.), 26 May 1999 (26.05.99), see the whole document	1-17
	--	
A	US 5280527 A (LAWRENCE S. GULLMAN ET AL), 18 January 1994 (18.01.94), see the whole document	1-17
	--	

[X] Further documents are listed in the continuation of Box C. [X] 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 application or patent 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
18 Sept 2003	23 -09- 2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/mj Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 03/01181

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5930804 A (YUAN-PIN YU ET AL), 27 July 1999 (27.07.99), see the whole document --	1-17
A	US 6317834 B1 (ROSARIO GENNARO ET AL), 13 November 2001 (13.11.01), cited in the application -- --------	1-17

INTERNATIONAL SEARCH REPORT

Information on patent family members

26/07/03

International application No.
PCT/SE 03/01181

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0201314 A2	03/01/02	AU 7122901 A	08/01/02
		US 2002010857 A	24/01/02
EP 0973123 A1	19/01/00	JP 2000048208 A	18/02/00
EP 0918300 A2	26/05/99	DE 69810581 D	00/00/00
		JP 3053388 B	19/06/00
		JP 11250261 A	07/09/99
		US 6134340 A	17/10/00
US 5280527 A	18/01/94	CA 2105404 A	03/03/95
US 5930804 A	27/07/99	EP 0923756 A	23/06/99
		JP 2000516746 T	12/12/00
		US 6182076 B	30/01/01
		WO 9857247 A	17/12/98
US 6317834 B1	13/11/01	NONE	