



- (51) International Patent Classification:
G06F 21/32 (2013.01)
- (21) International Application Number:
PCT/EP2012/067340
- (22) International Filing Date:
5 September 2012 (05.09.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): **NEC EUROPE LTD.** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **KARAME, Ghassan** [LB/DE]; Heinrich-Fuchs-Strasse 59, 69126 Heidelberg (DE).
- (74) Agent: **ULLRICH & NAUMANN**; Schneidmühlstr. 21, 69115 Heidelberg (DE).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR BIOMETRICAL IDENTIFICATION OF A USER

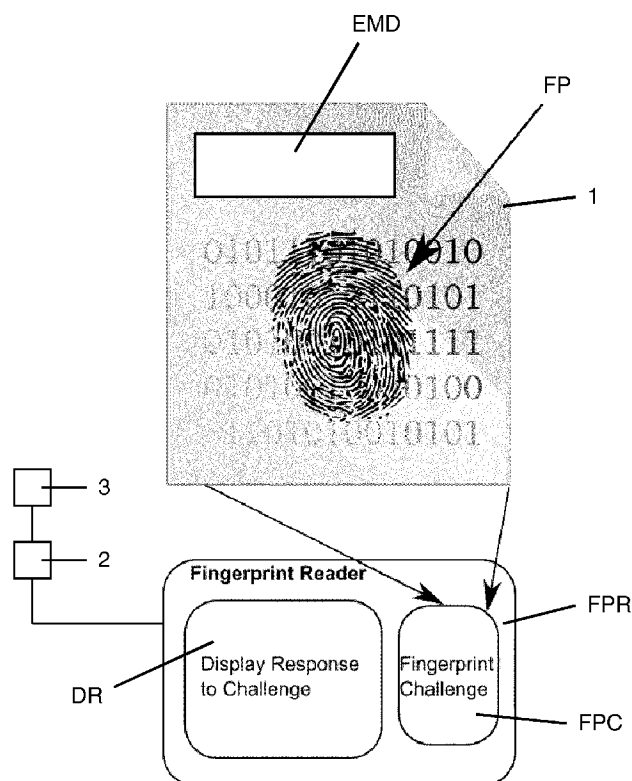


Fig. 2

(57) Abstract: The present invention relates to a method for identification of a user, comprising the steps of a) Inputting biometrical properties of a user, b) Encoding the biometrical properties, c) Checking the encoded biometrical properties with corresponding provided biometrical user information, d) Identifying the user based on a result of step c), and e) Outputting a response of the identification according to step d). wherein f) the inputted biometrical properties of the user are encrypted prior to step b) and wherein g) the encoded biometrical properties are provided as a biometrical challenge, and wherein h) for performing step c) the biometrical challenge is decrypted, and wherein i) the response is verified. The present invention also relates to a system for biometrical identification of a user.



Published:

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

METHOD AND SYSTEM FOR BIOMETRICAL IDENTIFICATION OF A USER

The present invention relates to a method for biometrical identification of a user, comprising the steps of

- a) Inputting biometrical properties of a user,
- b) Encoding the biometrical properties,
- c) Checking the encoded biometrical properties with corresponding provided biometrical user information,
- d) Identifying the user based on a result of step c), and
- e) Outputting a response of the identification according to step d).

The present invention further relates a system for biometrical identification of a user, preferably for performing with a method according the one of the claims 1-10, comprising

a first terminal comprising

- a) an input interface for biometrical properties of a user,
- b) encoding means for encoding the inputted biometrical properties,
- c) a sender for sending the encoded biometrical properties to a checking entity,
- d) a receiver for receiving a response of an identification of the user and
- e) an output interface for outputting the response,

wherein the checking entity is connected to the first terminal, and configured to be operable to check the encoded biometrical information with corresponding provided biometrical user information and

a database, connected to the first terminal and to the checking entity, wherein the database is configured to provide the biometrical user information.

Although applicable to biometrical properties of users in general, the present invention will be described with regard to fingerprints as biometrical property of a user.

Fingerprint-based identification is gaining more and more popularity, e.g. corresponding fingerprint scanners are cheaper available. Fingerprint-based

identification enables users to identify and authenticate themselves to local or remote entities such as login to a local computer or public institutes, electronic portals of governments or the like.

5 The process of the fingerprint scanning and matching involves a fingerprint scanner, i.e. a device that copies an image of fingerprints. The fingerprint scanner is connected via a network, for example the internet, to a remote database server, for example hosted by a governmental agency. When a user puts one of his fingers on the fingerprint scanner, the fingerprint scanner receives a fingerprint
10 candidate and transmits it via the network to the database server. The database server then uses a fingerprint matching algorithm in order to match the candidate fingerprint to a fingerprint target stored in the database. If a correct target is found, then the database server transmits a response to the fingerprint scanner including the corresponding access policy associated with the correct fingerprint.

15 Fingerprint scanners are usually installed in trusted environments such as airports, embassies, governmental agencies or the like. The reason is that users are generally reluctant to trust in fingerprint scanners if these scanners are deployed in uncontrolled environments like local shops, supermarkets, etc.. Users cannot
20 check if the fingerprint scanners have been tampered with or not. Since those fingerprint scanners temporarily store and transmit personal sensitive material, i.e. fingerprints, there are considerable incentives for attackers to compromise such scanners.

25 In the non-patent literature of Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, Dario Fiore, Riccardo Lazzeretti, Vincenzo Piuri, Fabio Scotti, Alessandro Piva, Privacy-preserving fingercode authentication, Proceedings of the 12th ACM workshop on Multimedia and security, September 09-10, 2010, Roma, Italy and in the non-patent literature
30 of Yan Huang, Lior Malka, David Evans, Jonathan Katz: Efficient Privay-Presering Biometric Identification, Proceedings of NDSS 2011 a prevention of database servers from learning any information about fingerprints is described while executing a fingerprint matching algorithm. Assuming that the fingerprint scanner

is honest or trusted privacy preserving fingerprint matching algorithms are proposed.

5 However, the methods described therein rely on trusted fingerprint scanners. It is therefore a disadvantage, that such fingerprint scanners can only be used in a controlled, i.e. secure environment. A further disadvantage is that rogue fingerprint scanners may try to impersonate users therefore provide an increased risk for stealing personal data.

10 It is therefore an objective of the present invention to provide a method and a system for biometrical identification of a user which enable obtaining biometrical data in untrusted environments which are more secure.

15 It is a further objective of the present invention to provide a method and a system for biometrical identification of a user which are easy to implement and cost effective.

20 It is an even further objective of the present invention to provide a method and a system for biometrical identification of a user which do not penalize non-privacy aware users.

According to the invention the aforementioned objectives are accomplished by a method of claim 1 and a system of claim 11.

25 According to claim 1 the method for biometrical identification of a user, comprising the steps of

- a) Inputting biometrical properties of a user,
- b) Encoding the biometrical properties,
- c) Checking the encoded biometrical properties with corresponding
30 provided biometrical user information,
- d) Identifying the user based on a result of step c), and
- e) Outputting a response of the identification according to step d).

According to claim 1 the method is characterized in that

- f) the inputted biometrical properties of the user are encrypted prior to step b) and that
- g) the encoded biometrical properties are provided as a biometrical challenge, and that
- h) for performing step c) the biometrical challenge is decrypted, and that
- i) the response is verified.

According to claim 11 the system for biometrical identification of a user, preferably for performing with a method according to one of the claims 1-10, comprising a first terminal comprising

- a) an input interface for biometrical properties of a user,
- b) encoding means for encoding the inputted biometrical properties,
- c) a sender for sending the encoded biometrical properties to a checking entity,
- d) a receiver for receiving a response of an identification of the user and
- e) an output interface for outputting the response,

wherein the checking entity is connected to the first terminal, and configured to be operable to check the encoded biometrical information with corresponding provided biometrical user information and a database, connected to the first terminal and to the checking entity, wherein the database is configured to provide the biometrical user information.

According to claim 11 the system is characterized by

a protecting terminal, connected to the first terminal, comprising

- a2) a second input interface for input biometrical properties of a user, and
- b2) a second output interface wherein an output interface of the second terminal is connected to the input interface of the first terminal, and

being configured to be operable to encrypt the biometrical information and to output the encrypted biometrical information via the second output interface and to provide the encrypted biometrical properties in form of a biometrical challenge and wherein

the checking entity is configured to be operable to decrypt the biometrical challenge
and by
a verifying entity, preferably the user, is configured to be operable to verify the response.

5

According to the invention it has first been recognized, that a privacy-preserving biometric extraction in spite of untrusted biometric readers or scanners is enabled.

10

According to the invention it has further been first recognized, that a mutual authentication between users and a database without the need to agree on secrets using an untrusted biometric reader is enabled.

15

According to the invention it has further been first recognized, that existing biometric readers and operation of databases require only few modifications.

According to the invention it has further been first recognized, that an impersonation of biometrical data by means of replay attacks is prevented.

20

Further features, advantages and preferred embodiments are described in the following subclaims.

25

According to a preferred embodiment the second terminal adds metadata-information, preferably encrypted. One of the advantages is, that the second terminal may add information, for example information about the second terminal itself, to the biometrical information of the user. For example properties of the second terminal could be implemented in the metadata information so that the database respectively the checking entity could use this information when checking the biometrical information with corresponding stored information. Alternatively or additionally a key for encryption may be included in the metadata-information.

30

According to a further preferred embodiment lifetime-information of the second terminal are included in the metadata-information. Lifetime-information reflect a

“freshness” of the second terminal enabling for example to reflect one-time second terminals for encryption which further enhances the security.

5 According to a further preferred embodiment different biometrical property data and data identifiers are included in the biometrical raw data, wherein the data identifiers are well-defined and assigned to the different biometrical property data. In case of fingerprints as biometrical property of the user and assumed that the database has stored fingerprints of fingers with corresponding indices a scanned fingerprint pertaining one of these fingers, has a reduced that an adversary not
10 knowing a priori the fingerprints of these indices guessing the correct association fingerprint index. Therefore security is further enhanced.

According to a further preferred embodiment the result of step e) includes, preferably is provided in form of, the identifier corresponding to the checked
15 biometrical information of the biometrical raw data. By providing the result including the identifier a fingerprint scanner may be used to output this result to the user enabling the user to decide if the fingerprint scanner is to be trusted or if the user has used a rogue scanner.

20 According to a further preferred embodiment the result is provided unencrypted. One of the advantages is, that resources like computational resources for encryption are saved, since the result is provided unencrypted, i.e. in plaintext form. A further advantage is, that this does not reduce the security of the method since for example an untrusted fingerprint scanner is not able to require any
25 meaningful information about the inputted fingerprint of the user.

According to a further preferred embodiment the lifetime-information is provided in form of a nonce. A unique nonce, for example an incremental counter provides a very simple and easy-to-implement way to reflect the “freshness” respectively
30 lifetime of the second terminal.

According to a further preferred embodiment the result of step e) includes a result of a performed function on the lifetime-information. This enables to further increase the resilience of the method to possible guessing attacks.

According to a further preferred embodiment the result of the performed function on the lifetime-information is provided to be human-readable. This enables for example users to an easy and quick recognition, if the first terminal is to be trusted e.g. for example a QR-codes/barcodes may be provided.

5

According to a preferred embodiment of the system according to claim 10 the protecting terminal is a pad, preferably a one-time pad. One of the advantages is, that the pad is lightweight and easy to transport even in high numbers. A further advantage of a pad is that it is very cost-effective.

10

According to a further preferred embodiment the second input interface comprises optical means, preferably a camera. With a camera for example a pad encryption can be emulated. Since current mobile phone cameras are of very high precision a corresponding software on the mobile phone can take a photo of a fingerprint or other biometrical properties of a user, encrypt the image suing pad-cryptography. The user may place the mobile phone for example on a fingerprint reader in order to transmit the encrypted fingerprint to the checking entity respectively the database. One of the further advantages of a camera is, that users nowadays have in general mobile phones equipped with a camera with sufficient resolution. Therefore users do not have to carry further hardware.

15

20

According to a further preferred embodiment the pad, preferably the one-time pad, comprises a transparency layer. Each transparency layer present a one-time pad token used for encryption. For example the user can easily acquire a set of transparencies from the government when registering its fingerprints and can use them one at the time subsequently.

25

According to a further preferred embodiment steps a)-i) are performed at least twice. This further reduces the impersonation probability of the method.

30

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end it is to be referred to the patent claims subordinate to patent claims 1 and 10 on the one hand and to the following explanation of preferred embodiments of the invention by way of

example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained. In the drawing the only

5

Fig. 1 shows different biometrical property data with corresponding data identifiers according to a first embodiment of the present invention;

10

Fig. 2 shows a system according to a second embodiment of the present invention.

Fig. 1 shows different biometrical property data with corresponding data identifiers according to a first embodiment of the present invention.

15

In Fig. 1 indices of fingers denoted with "1", "2", ... of the left and right hand corresponding to the fingerprints of the respective fingers of a human user are shown.

20

Fig. 2 shows a system according to a second embodiment of the present invention.

25

In Fig. 2 a fingerprint reader FPR is shown. The fingerprint reader is connected to a checking entity 2 and the checking entity 2 is further connected to a database 3. In the database 3 fingerprints of the fingers of the left and right hand according to figure 1 as well as the corresponding indices are stored. Further the fingerprint reader FPR comprises a display response region DR for displaying a response corresponding to a challenge and a second region FPC for fingerprint challenge.

30

When the user would like to use the fingerprint reader FPR the user first takes his one-time pad 1 together with encrypted metadata EMD stored on it and puts on the one-time pad 1 its fingerprint FP. The one-time pad 1 encodes and encrypts the fingerprint data. When the user then submits its encrypted fingerprint and the metadata EMD via the one-time pad 1 i.e. puts the one-time pad 1 on the fingerprint challenge region FPC of the fingerprint reader FPR, the fingerprint

reader FPR encodes a corresponding challenge to the database 3. This challenge provides an encrypted fingerprint of any of the finger indices or any combination of pairs of these indices, for example chosen at random.

5 Upon receiving the fingerprint challenge FPC the database 3 performs a fingerprint matching algorithm after it has decrypted the encrypted metadata and the encrypted fingerprint data. A result of the fingerprint matching algorithm is used for response including the number of the finger indices that the user has used. This response maybe sent in plaintext form and displayed to the user using a display of
10 the fingerprint reader FPR. If the user sees in the display of the fingerprint reader FPR a response that matches the fingerprint challenge FPC the user may assume that the fingerprint reader communicates with a correct checking entity 2 and database 3.

15 In this way an untrusted fingerprint reader cannot trick with overwhelming probability any user to submit its fingerprint without communicating the fingerprint immediately to the database 3. Although the response of the database 3 or the checking entity 2 may be sent in plaintext form an untrusted fingerprint reader is not able to extract any meaningful information about the fingerprint inputted by the
20 user. Even if the checking entity 2 does not find a match in the database 3 for the fingerprint FP, the checking entity 2 outputs a plaintext answer to the randomly from a set of possible answers.

To provide encryption the checking entity 2 respectively the database 3 and the
25 one-time pad 1 maybe provided with corresponding public/private keys, for example for each one-time pad 1 a seed s is chosen uniformly at random. The one-time pad encryption maybe then $G(s)$. The "encrypted metadata" of the one-time pad is then $C = F_{\text{encrypted, PK}}(s, N, \text{server})$, where N denotes a unique nonce, for example an incremental counter to reflect the freshness of the one-time pad 1,
30 "server" is an ID of the checking entity 2 and F is the function to perform the encryption. After receiving the encrypted metadata C the checking entity 2 may then easily recover the encrypted fingerprint using its private key and the "encrypted metadata" field in the transmitted biometrical information. The checking entity 2 may then check the database 3 for matching fingerprints. The checking

entity 2 outputs then a response to the user challenge FPC. For example a probability that an adversary that does not know a priori the fingerprints of fingers with corresponding indexes for example 2, 3, 4, 7, 8, 9 in guessing the response is bounded by $1/42=2,4\%$. This computation is specific to the case where users rely on a camera snapshot; since fingerprints of each finger index are stored in the database 3 the user may decode the same fingerprint twice within one fingerprint challenge FPC, hence a total of 42 possibilities. The user can repeat the protocol many times to reduce the probability of guessing. Further for example more than 2 fingers may be inputted and then checked by the checking entity 2 which also then reduces the probability of guessing.

In summary the present invention provides a biometrical protector to achieve full privacy/secretcy in biometrical extraction, in particular of fingerprints. The present invention further enables constructing a stateless one-time pad protector wherein a key to decrypt the biometrical protector is encoded within the biometrical protector itself in the EMD field. The present invention further provides encrypting the biometrical input by users as a challenge/response mechanism to enable mutual authentication between end parties, i.e. the checking entity and the one-time pad.

The present invention enables privacy-preserving biometric extraction in spite of untrusted biometric readers as well as a mutual authentication between users and checking entities, for example database servers without the need to agree on secrets using and untrusted biometric reader. The present invention does not require considerable modification to existing biometrical readers and to the operation of databases. The present invention does not penalize non-privacy aware users. Users that do not wish to follow the method according to the present invention may simply use conventional insecure biometrical identification.

The present invention increases the trust of users in biometrical readers as means to support their large scale deployment. The present invention prevents impersonation of biometrical information by means of replay attacks. The present invention ensures full secrecy of the biometrical properties to any external party, i.e. that is neither the user nor the checking entity and/or database. The present

invention ensures mutual authentication between end parties without requiring modifications/changes to the current operation of biometrical readers, in particular fingerprint readers. The present invention can be easily implemented with conventional methods and systems installed on the database or checking entity side to ensure privacy-preserving biometrical property matching.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

The present invention is not solely specific to fingerprints, but can although be used to enable the secure and privacy-preserving retinal scan/extraction. Other biometrics such as voice recognition, etc. may also be used.

Claims

1. Method for biometrical identification of a user,
comprising the steps of
 - a) Inputting biometrical properties of a user,
 - b) Encoding the biometrical properties,
 - c) Checking the encoded biometrical properties with corresponding
provided biometrical user information,
 - d) Identifying the user based on a result of step c), and
 - e) Outputting a response of the identification according to step d).
- characterized in that
 - f) the inputted biometrical properties of the user are encrypted prior to
step b) and that
 - g) the encoded biometrical properties are provided as a biometrical
challenge, and that
 - h) for performing step c) the biometrical challenge is decrypted, and that
 - i) the response is verified.
2. Method according to claim 1, characterized in that metadata-information,
preferably encrypted, is added.
3. Method according to one of the claims 1-2, characterized in that lifetime-
information are included in the metadata-information.
4. Method according to one of the claims 1-3, characterized in that different
biometrical properties are inputted and data identifiers are included, wherein the
data identifiers are well-defined and assigned to the different biometrical
properties.
5. Method according to claim 4, characterized in that a result of step d)
includes, preferably is provided in form of, the data identifier corresponding to the
checked biometrical challenge.

6. Method according to one of the claims 1-5, characterized in that the result is provided unencrypted.

5 7. Method according to one of the claims 1-6, characterized in that the lifetime-information is provided in form of a nonce.

8. Method according to one of the claims 3-6, characterized in that the result of step d) includes a result of a performed function on the lifetime-information.

10 9. Method according to one of the claims 7-8, characterized in that the result of the performed function on the lifetime-information is provided to be human-readable.

15 10. Method according to one of the claims 1-9, characterized in that steps a)-i) are performed at least twice.

11. System for biometrical identification of a user, preferably for performing with a method according the one of the claims 1-10, comprising a first terminal (FPR) comprising

- 20 a) an input interface for biometrical properties of a user,
b) encoding means for encoding the inputted biometrical properties,
c) a sender for sending the encoded biometrical properties to a checking entity (2),
d) a receiver for receiving a response of an identification of the user and
25 e) an output interface for outputting the response,

wherein the checking entity (2) is connected to the first terminal (FPR), and configured to be operable to check the encoded biometrical information with corresponding provided biometrical user information and

a database (3), connected to the first terminal (FPR) and to the checking entity (2),
30 wherein the database (3) is configured to provide the biometrical user information, characterized by

a protecting terminal (1), connected to the first terminal (FPR), comprising

- a2) a second input interface for input biometrical properties of a user,
and

b2) a second output interface wherein an output interface of the second terminal is connected to the input interface of the first terminal, and being configured to be operable to encrypt the biometrical information and to output the encrypted biometrical information via the second output interface and to provide the encrypted biometrical properties in form of a biometrical challenge and wherein the checking entity is configured to be operable to decrypt the biometrical challenge and by a verifying entity, preferably the user, is configured to be operable to verify the response.

12. System according to claim 11, characterized in that the protecting terminal (1) is a pad, preferably a one-time pad.

13. System according to one of the claims 11-12, characterized in that the second input interface comprises optical means, preferably a camera.

14. System according to claim 12, characterized in that the pad, preferably the one-time pad, comprises a transparency layer.

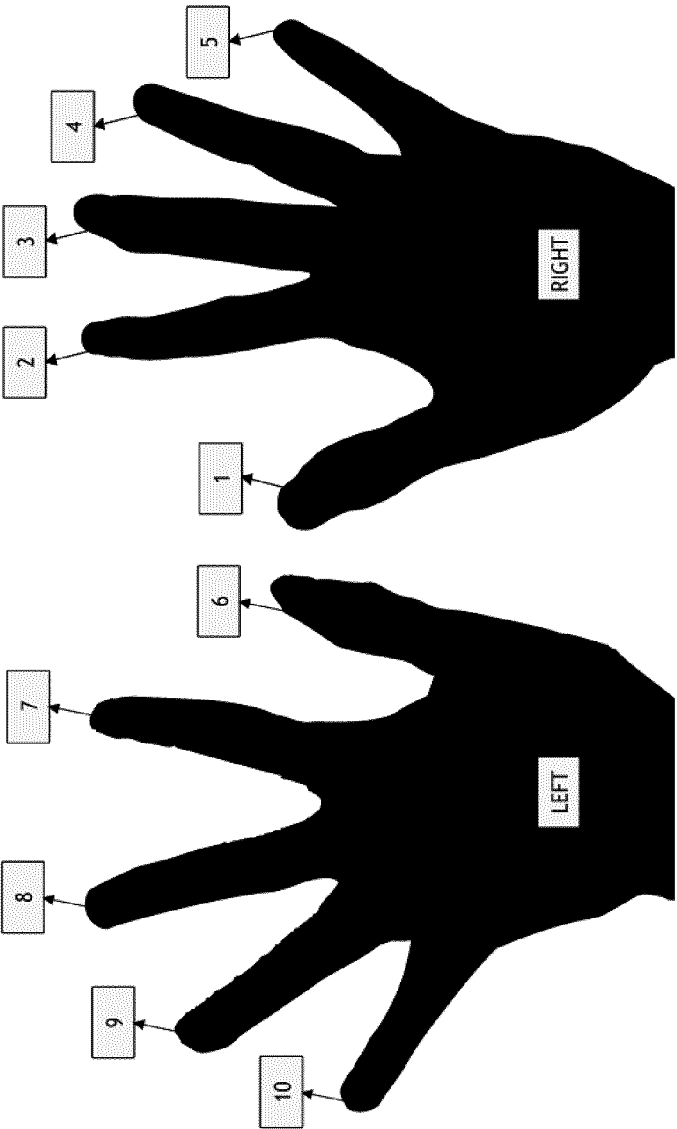


Fig. 1

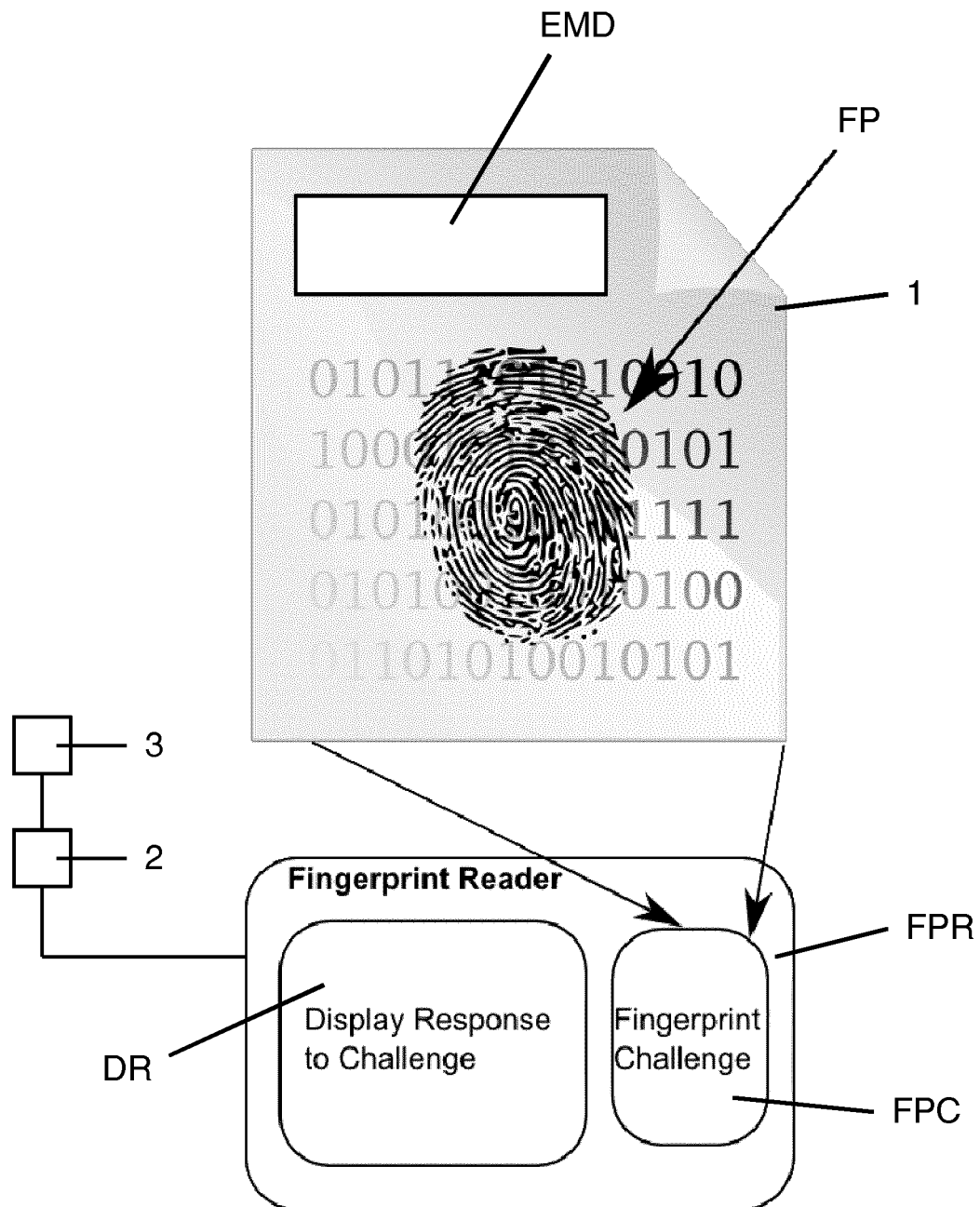


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/067340

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32
ADD.

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)
G06F G07C

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 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	US 2011/302420 A1 (DAVIDA GEORGE I [US]) 8 December 2011 (2011-12-08) abstract; figures 1-7 paragraph [0008] paragraph [0125] - paragraph [0152] paragraph [0157] - paragraph [0169] paragraph [0174] - paragraph [0211] paragraph [0229] - paragraph [0246] claims 1-17	1-14
A	----- US 2005/055557 A1 (YAMADA MIKI [JP] ET AL) 10 March 2005 (2005-03-10) the whole document	1-14
A	----- US 2005/204149 A1 (WATANABE KEISUKE [JP]) 15 September 2005 (2005-09-15) the whole document -----	1-14



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 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

10 December 2012

Date of mailing of the international search report

18/12/2012

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

Powell, David

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2012/067340

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011302420	A1	08-12-2011	NONE

US 2005055557	A1	10-03-2005	JP 4176898 B2 05-11-2008
		JP 2000242750 A	08-09-2000
		US 6910131 B1	21-06-2005
		US 2005055557 A1	10-03-2005

US 2005204149	A1	15-09-2005	JP 2005301988 A 27-10-2005
		US 2005204149 A1	15-09-2005
