



(51) International Patent Classification:

G06K 9/00 (2006.01) G06K 9/22 (2006.01)

(21) International Application Number:

PCT/US2017/056459

(22) International Filing Date:

13 October 2017 (13.10.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16198855.5 15 November 2016 (15.11.2016) EP

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors: **NOWAK, Dawid**; 3 Blackwood Mews, Ongar Chase, Dublin, 15 (IE). **DRUTA, Vladut**; 41 Dorset Square, Upper Gardiner Street, Dublin, 1 (IE).

(74) Agent: **DOBBYN, Colm, J.**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: SYSTEMS AND METHODS FOR SECURE BIOMETRIC SAMPLE RAW DATA STORAGE

(57) Abstract: A method for biometric template extraction and secure biometric sample raw data storage, the method comprising enrolling, at a terminal, at least one biometric sample of a user, storing, in a secure storage on the terminal, the raw data of the biometric sample, extracting, by an extraction application executed on the 5 terminal, a biometric template from the raw data of the sample, fragmenting, by a raw sample splitter executed on the terminal, the raw data of the biometric sample, distributing the fragments of the raw data of the biometric samples from the terminal to independent entities, preferably via a secure communication channel, and deleting the biometric sample raw data from the secure storage of 10 the terminal.



SYSTEMS AND METHODS FOR SECURE BIOMETRIC SAMPLE RAW DATA STORAGE

CROSS-REFERENCE TO RELATED APPLICATION

- 5 This application claims the benefit of, and priority to, European Patent Application No. 16198855.5 filed on November 15, 2016. The entire disclosure of the above application is incorporated herein by reference.

TECHNICAL FIELD

- 10 The present disclosure relates to the field of biometric authentication and biometric sample raw data handling. More particularly, the present disclosure relates to methods and systems for distributed storage of biometric sample raw data. Moreover, the disclosure relates to a computer program product and a computer readable medium. The computer readable medium comprises computer-executable instructions, which, when executed by the respective devices being equipped with
15 processors cause the devices to perform the method steps of the disclosure on the respective device interacting with the respective other device.

BACKGROUND

- 20 Biometric authentication has become a valuable and commonly used tool. This is, on the one hand, because of the comprehensive availability of suitable scanning devices, e.g. in form of smart phones providing scanning functionality on the other hand because of improved network connectivity. According to this, making use of existing hardware, biometric authentication methods can be implemented in many situations, such as authentication, identification and also authorization processes.

- 25 Similar to hand written signatures, which are normally compared by human beings with a provided proof of the signature, e.g. when paying with a credit card, also biometric scans need to be compared to a verified proof. Similar to providing a proof of a hand written signature on the backside of a credit card after receiving the card, when enrolling for biometric authentication, a master of the used
30 biometric sample is taken. Different to the human based comparison of hand written signatures, in biometric authentication the captured biometric is not compared with

the raw data of the biometric sample but with a specific template stored in a bioi database in order to verify the individual is the person it claims to be.

Accordingly, different to the handwritten signature (raw data) on the backside of a credit card, for biometric authentication, certain characterising features
5 are extracted from the raw data sample. In subsequent biometric identification or authentication procedures making use of the biometric authentication, the comparison is based on the extracted features only. By doing this, the authentication process is significantly accelerated, as less data has to be processed, and, in cases of the biometric scanning device and the authentication device being connected over a
10 network (e.g. a biometric authentication application installed on a smartphone communication of an authentication server), less data needs to be transferred.

In case of any doubt with respect to the validity of the biometric verification, the original raw data of the biometric sample might need to be used, such that the original raw data of the biometric sample has to be stored. However, as the
15 original raw data of the biometric sample could also be used for the biometric authentication, as it matches with the template by definition, secure storage of the raw data is fundamental for security of the system. Even though possible, safe storage of the data in physical form, e.g. on a memory stick in a safe deposit box seems unpractical, especially when the original raw data is required for verification
20 purposes. Accordingly, there is a need for secure biometric sample raw data storage.

SUMMARY OF THE INVENTION

The present disclosure provides one or more solutions to the problems and disadvantages of the background art. Other technical advantages of the present disclosure will be readily apparent to one skilled in the art from the following
25 description and claims.

The present disclosure is directed to a computer implemented method for biometric template extraction and secure biometric sample raw data storage, the method comprising:

- enrolling, at a terminal, at least one biometric sample of a user;
- 30 • storing, in a secure storage on the terminal, the raw data of the biometric sample;

- extracting, by an extraction application executed on the terminal, a biom template from the raw data of the sample;
- fragmenting, by a raw sample splitter executed on the terminal, the raw data of the biometric sample;
- 5 • distributing the fragments of the raw data of the biometric samples from the terminal to independent entities, preferably via a secure communication channel; and
- deleting the biometric sample raw data from the secure storage of the terminal.

The present disclosure is further directed to a computer implemented method for biometric template extraction and secure biometric sample raw data storage, the method comprising:

- enrolling, at a terminal, at least one biometric sample of a user;
- transmitting, preferably via a secure communication channel, the raw data of the biometric sample from the terminal to a server;
- extracting, by an extraction application executed on the server, a biometric template from the raw data of the sample;
- 15 • fragmenting, by a raw sample splitter executed on the server, the raw data of the biometric sample;
- distributing the fragments of the raw data of the biometric samples from the server to independent entities, preferably via a secure communication channel; and
- 20 • deleting the biometric sample raw data from the memory of the server.

The present disclosure includes multiple aspects for secure biometric sample raw data storage. The biometric sample may be based on aspects of human physiology, chemistry or behaviour that show characteristics and as such can be used for biometric authentication. Non-limiting examples for characteristics to be used for biometric authentication may be any one, or combination, of the following:

25 fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent but also behavioural characteristics such as typing rhythm, gait, and voice. Raw data of the biometric data may be any form of unprocessed and/or uncompressed data of the captured information of the respective

30 characteristic(s) to be used for biometric authentication. A terminal may be any

device capable of capturing information related to the characteristic(s) used, such for example, smartphones, personal computers, tablet computers comprising detection means for the respective characteristic(s), such as cameras or scanning devices, microphones, and configured to execute a respective application, but also dedicated
5 biometric scanning devices and combined devices consisting of detection and processing units. The terminal may also comprise communication means and may also be connected to a network, such as the internet.

When the user uses the biometric authentication system for the first time or when the user starts using the biometric authentication system, the enrolment
10 process is initiated. The biometric authentication system may be based on or may be accessible through a dedicated application executed on the terminal or a plugin, an inFrame solution, a SDK or the like implemented on a web site.

During the enrolment, biometric information from the user is captured by the respective detection means and stored. Storage may be on the terminal and/or
15 on a server, however, storage of the captured data (raw data of the biometric sample) is preferably on a secure storage medium. If the raw data of the biometric sample is transmitted from the terminal to a server a secure communication channel may be used.

After the biometric information has been captured, the resulting raw
20 data of the biometric sample is further processed by an extraction application. The extraction application may be executed on the terminal or on the server and may be integrated and as such forming part of other applications of the biometric authentication system. The extraction application extracts characteristic features of the raw data of the biometric sample and thereby creates a biometric template. The
25 features to be extracted depend on the biometric sample used and are known to the person skilled in the art. The biometric template contains at least some characterising features of the biometric sample which will then be used for biometric authentication. The amount of features may depend on the required security level and/or on the available processing capabilities. The template creation may be implemented in the
30 extraction application or may be processed by an additional template creation application.

After feature extraction and template creation the biometric sample raw data is fragmented by a raw data splitter. The raw data splitter may be executed on the terminal or on the server. After fragmentation of the biometric sample raw data

the fragments are distributed to certain, predefined entities for storage and the biometric sample raw data is deleted. The number of fragments depends on the number of target entities, e.g. if fragments of the biometric sample raw data are to be stored on three external entities and on the terminal, the number of fragments has to be 4. In general, the fragmenting process results in at least two fragments. Independent entities used for storage may be physically separated storage entities, electronically separated storage entities and/or distinct and separated legal entities. The physically and/or electronically separated storage entities may be held by the same and/or by different legal entities or combinations thereof. By way of distributing the fragments to different entities, the level of security may be increased.

Fragmenting of the biometric sample raw data may comprise fragmenting the data into equally sized fragments or into fragments of different sizes. If the biometric sample raw data is fragmented into fragments of different sizes, the respective sizes may be based on a predefined sizing pattern or, alternatively, based on a dynamically created random sizing pattern. The fragmenting may be based on the digital data, i.e. separating the file describing the data into portions or on the described data file, e.g. cutting an image of a fingerprint into 4 pieces. In case the recombination of the fragments to regain the initial raw data requires further information, respective reconstruction instructions may be stored as an individual file or may be added to at least one of the fragment files, e.g. as a meta tag. If the reconstruction instructions are stored in an individual file, this file may be stored together with at least one fragment or may be sent for storage to an additional entity. Alternatively, the fragmenting or reconstruction may be defined as preferences and as such may be stored in a configuration file on the server or on the terminal.

In case of verification of a biometric authentication process being required, the fragments of the biometric sample raw data can be consolidated and the biometric sample raw data may be reconstructed. In case of reconstruction instructions being required, the respective instructions may be used.

In another aspect of the present disclosure, at least one of the fragments created from the biometric sample raw data is an essential fragment. Essential fragments are those fragments which contain information of the biometric sample that is un-substitutable or un-rebuildable on the basis of the information of the respective other fragments. According to this, the biometric sample data cannot be reconstructed without the essential data. Fragmentation with creation of at least one

essential fragment may include additional pre-processing, which would further have to be reversed to rebuild the raw data. Non-limiting examples for fragmentations include at least one essential fragment may be for images, e.g. face recognition, the detection of certain elements, e.g. the irises in the face, and to cut out a portion of the image including a essential element, e.g. a circular area such that it covers the whole eye and save this portion as an essential fragment, and divide the remainder in blocks $N \times N$ pixels in size, where N is number of entities storing this image. Another example includes the application of well known algorithms to detect main features of the image, e.g. a face (eyes, nose, lips, etc), randomly select areas of the image and apply effects/filters such as blur, noise to transform the image so the quality of the image is not good enough for biometrics but it might be sufficient to recognize the person by a human, store applied transformations locally in the terminal or in the electronic configuration file and partition the image into N pieces as previously described. Another example, e.g. applicable for voice recognition may be the application of an inverse Fourier transformation to detect key frequencies/cepstral coefficients, taking most impacting coefficient and mark it as the essential fragment, splitting remaining coefficients amongst other entities involved in the process.

In addition or alternatively to this, fragmentation may be done in such a way that reconstruction of the raw data is impossible without the respective reconstruction instructions. For example, in case of erratic fragmentations, the reconstruction instructions may be required for reconstructions of the raw data. In these cases, where the fragments are similar but the reconstruction instructions are essential for reconstructing the data, the reconstruction instruction file may be considered as equivalent to an essential fragment as described above.

In order to revert to the original image the user would have to reveal the applied transformations, the order they were applied and parts of the image that they were applied to.

In yet another aspect of the present disclosure, even though the essential fragment may be stored anywhere, the essential fragment is stored under the responsibility of the user. According to this, the essential fragment may be stored after fragmentation in, preferably, a secure storage on the terminal. If the fragmentation was performed on the server, the essential fragment may be transmitted to the terminal, preferably making use of secure communication channels, for subsequent storage.

In another aspect of the present disclosure, the fragments are consolidated upon request from the user and the raw data of the biometric sample ... rebuilt from the fragments. In case reconstruction instructions are required, these may be consolidated together with the fragments. The request from the user may require
5 additional authorisation for processing.

Depending on the type of biometric sample, but also on further requirements, doubtful authentication data may be compared directly with the raw data of the biometric sample. Alternatively or in addition, the raw data of the biometric sample may be processed, e.g. features may be extracted and a new
10 template may be created, and the processed data may be used for comparison and verification.

In yet another aspect of the present disclosure, the consolidated data and the reconstructed data are deleted after re-extraction of the template and/or after finishing the verification process.

15 The present disclosure is also directed to a system for biometric template extraction and secure biometric sample raw data storage, the system comprising a terminal and at least one storage entity, wherein the terminal comprises a scanning device for enrolling at least one biometric sample of a user and is executing an extraction application, a raw sample splitting application,
20 and a fragment distribution application, wherein the terminal is configured to enrol, by the scanning device, at least one biometric sample of the user, to extract, by the extracting application, a biometric template from the enrolled raw biometric data of the sample, to fragment, by the raw sample splitting application, the raw data of the biometric sample and to distribute, by
25 the fragment distribution application, the fragments for storage on the terminal and the at least one storage entity.

The present disclosure is further directed to a terminal for performing the method of biometric template extraction and data fragmentation, the terminal comprising:
30 a scanning unit for capturing raw data of at least one biometric sample of a user;
a processing unit, configured to enrol at least one biometric sample of a user from the captured raw data, to extract a biometric template from the raw data, and to fragment the raw data; and

a communication unit, configured to transmit at least one of the created fragments at least one storage entity.

In yet another aspect of the present disclosure, the terminal further comprises a storage unit for storing raw data of biometric sample and/or a fragment created from the raw data of the biometric sample. The storage unit may be part of a memory unit of the terminal or may be a separate memory unit. In a preferred embodiment, the storage unit is a secure storage unit.

The present disclosure is also directed to a system for biometric template extraction and secure biometric sample raw data storage, the system comprising a terminal, a server and at least one storage entity, wherein a terminal comprising a scanning unit for capturing raw data of at least one biometric sample of a user and communication means for transmitting the captured raw data; a server comprising communication means to receive the raw data from the terminal, the server being configured to execute an extraction application to extract a biometric template from the raw data and a splitter application to fragment the raw data; at least one independent entity comprising communication means to receive at least one fragment of the raw data from the server and storage means to store the received fragment.

Raw data of a biometric sample is captured by the scanning device of the terminal and is transmitted by the communication means of the terminal to the server. The raw data of the biometric sample is associated to user related data used for identifying the biometric raw data and to associate the biometric raw data to a user or a user profile during a subsequent enrolment process on the server. During the enrolment process a biometric template is extracted from the raw data of the biometric sample. The biometric template comprises key features of the biometric sample used in subsequent biometric identification processes. After biometric template extraction, a splitter application is executed on the server for fragmenting the raw data of the biometric sample as described above, which are then distributed to at least one storage entity and to the terminal.

The present disclosure is also directed to a computer program computer program product comprising program instructions for carrying out each of the method steps of the disclosure, when said product is executed on a computer.

Further, the present disclosure is directed to a computer readable medium storing program instructions, which, when executed by a processor of a computer cause the computer to perform each of the method steps of the disclosure.

One advantage that may be realized in the practice of some
5 embodiments of the described methods is that raw data of biometric samples can electronically be stored securely and may be consolidated and rebuilt for verification of an inconclusive biometric authentication process. Other technical advantages of the present disclosure will be readily apparent to one skilled in the art from the following description of preferred embodiments and the claims. Various embodiments of the
10 present application obtain only a subset of the advantages set forth. No single advantage is critical to the embodiments. Any claimed embodiment may be technically combined with any other claimed embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 shows a flowchart biometric template extraction and the secure
15 raw data storage process;

Fig. 2. shows a block diagram showing the entities involved in combination with the steps of the extraction, secure storage and consolidation process;

Fig. 3 shows an example of fragmentation including an essential
fragment; and

20 Fig. 4 shows a block diagram showing fragmentation including an essential fragment.

The accompanying drawings illustrate exemplary embodiments of the disclosure and serve to explain, by way of example, the principles of the disclosure.

DETAILED DESCRIPTION

25 The present disclosure will now be described more fully hereinafter with reference to the accompanying figures, in which preferred embodiments are shown, by way of example only. The method, however, may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. It should be noted that these figures are intended to illustrate the general
30 characteristics of the methods utilized in certain embodiments. However, the figures may not precisely reflect the precise structure or performance characteristic of any

given embodiment. Moreover, in the figures like reference numerals designate corresponding parts throughout the different views or embodiments.

Fig. 1 is a flowchart illustrating exemplary the overall steps for biometric template extraction and secure biometric sample raw data storage. In step 5 101 the user starts the enrolment process for using the biometric authentication system by starting a dedicated application, namely e.g. a biometric authentication application, on his terminal, in this case a smartphone. The smartphone is equipped means for detection of the biometric sample, and detects, at step 102 a biometric sample. In this case a picture of the user's face is captured by the camera of smartphone. First, at step 10 103, the captured image is checked with regard to formal aspects, e.g. face position, exposure, focus, and the like, and, if the image fulfils the requirements for biometrics, it is approved and the enrolment process is continued.

At step 104, captured and approved image is stored in a secure portion of the memory of the smart phone. At step 105, an extraction application integrated 15 into the biometric authentication application extracts the adequate features for the face recognition method at the required security level and extracts a template for use in biometric authentication. The template is stored (step 106) for future use, preferably in a secure portion of the memory.

At step 107 a raw sample splitter integrated in the biometric 20 authentication application fragments the stored raw data of the biometric sample based security requirements. If fragments of the data are to be sent to three entities, e.g. third party trustees, four fragments are created, three for the entities, one to be kept on the user terminal. If a higher security level is selected, an essential fragment is created, in certain embodiments this essential fragment may be subject to stronger 25 encryption than the remaining fragments. In the present example, the eye portion of the captured image of the face is cut out and stored, as the essential fragment on the user terminal. The remainder of the image is divided into three fragments. At the same time the biometric authentication application created an electronic configuration file for storing information regarding the fragmentation as well as the destinations of the 30 fragments.

At step 108 the created fragments are sent to destination entities for storage. The destination entities, responsive to receiving the fragment, are sending a confirmation receipt to the terminal. The confirmation receipt is added to the

electronic configuration file. Subsequently, at step 109, the raw data of the biom sample is deleted from the memory of the smartphone.

Fig. 2. shows a block diagram showing the entities involved in combination with the steps of the extraction, secure storage and consolidation process.

5 A user 1 of a mobile device 2 makes use of biometric authentication. A biometric authentication application 3, interacting with the hardware of the mobile device and providing a user interface 4 is installed and executed on the mobile device. The biometric authentication application 3 includes an extraction application 5, a secure memory 6 and a raw sample splitter 7. When an image to be used for the biometric authentication system is captured, either for enrolment or for subsequent use for authentication purposes, the image is transferred 201 to the extraction application 5 for extraction of characteristic features and the creation of a biometric template. The picture used for enrolment is stored in the secure memory 6. Subsequently, the raw data of the biometric template is further processed by the raw sample splitter, wherein an essential fragment Part 1 and further fragments Part N, Part M are created. The essential fragment Part 1 is stored 202 in the secure memory 6 and the other parts Part N, Part M are distributed 203 to third party trustees 8, 8' and the storage system 13 service provider 9 for the biometric authentication services. When using the biometric authentication system, the biometric authentication application 3 on the mobile device 2, interacts and communicates 204, 205 with an enrolment portal 10 and a verification portal 11 in the responsibility of the service provider 9. In case of a complaint regarding a doubtful authentication, the user initiates a complaint request, which is submitted to the complaints portal 12 of the service provider. In order to deal with the complaint, the fragments are consolidated 207, 209, 209 and the raw data is rebuilt.

25 Fig. 3 shows an example of fragmentation including an essential fragment based on an image used for face recognition. In a face the irises are detected and circular areas covering the eyes and a surrounding portion of the eyes are marked. The necessary size of the marked area can be determined based on calculating the scale between the size of the iris and the size of an image pixel. Subsequently, the two marked areas are connected, resulting in an ellipsoidal shaped area. The ellipsoidal shaped area is then cut out and saved as an essential fragment. The remainder of the image is then divided into four fragments for subsequent distribution.

Fig. 4 shows a block diagram of the fragmentation process including the generation of an essential fragment based in the context of voice recognition. At a

first step (step 401), the user starts the enrolment process based on voice recognition as biometric characteristic to be used. The user is prompted by the biometric authentication application on his terminal, in this case a smartphone, to speak into the detection means, i.e. the microphone of the smartphone in order to record at step 402 a voice sample. Subsequently, at step 403, the quality of the recorded voice sample is checked. If the quality of the recorded voice sample does not allow further processing, the step is repeated until a sample with sufficient quality has been recorded. If the voice sample fulfils the quality requirements, the sample is stored at step 404 in a secure portion of the memory of the smart phone.

At step 405 the recorded voice sample undergoes mathematical transformations in order to identify the voice characteristics to be used for biometric authentication. For this purpose the excitation signal produced by the glottis of the user is separated from the filter caused by the physical characteristics of the user. Known techniques are linear prediction and Fourier transformation based cepstral analysis, which allow detection of key frequencies and/or cepstral coefficients which are used for voice based biometric authentication. According to this, the filter data revealed by the mathematical transformation is used as the basis for the biometric authentication and the template used for biometric authentication is based on said filter data.

At step 406, a template for use in biometric authentication is extracted from the transformed data and, at step 407, stored in a secure portion of the memory of the smart phone.

At step 408, the most impacting characteristics of the filter revealed by the mathematical transformation is identified as an essential portion of the transformed data. At step 409, the essential portion of the data is separated and is stored (step 410) as essential data in a secure portion of the memory. In some embodiments the essential portion of the data has a stronger level of encryption than the remaining portions of the data.

At step 410 the remainder of the filter data is fragmented and, at step 412 distributed to the respective entities for storage. Subsequently, the raw data of the biometric sample, i.e. the voice recording, and the results of the mathematical transformation, i.e. the excitation signal and the filter data are deleted from the memory.

This description uses examples to disclose the invention, including best mode, and also to enable any person skilled in the art to practice the invention including making and using any devices or systems and performing any incorporated methods. The patentable scope of the invention is defined by the claims, and may

5 include other examples that occur to those skilled in the art.

Claims:

1. A method for biometric template extraction and secure biometric sample data storage, the method comprising:
 - a) enrolling, at a terminal, at least one biometric sample of a user;
 - 5 b) storing, in a secure storage on the terminal, the raw data of the biometric sample;
 - c) extracting, by an extraction application executed on the terminal, a biometric template from the raw data of the sample;
 - d) fragmenting, by a raw sample splitter executed on the terminal, the raw data of the biometric sample;
 - 10 e) distributing the fragments of the raw data of the biometric samples from the terminal to independent entities, preferably via a secure communication channel; and
 - f) deleting the biometric sample raw data from the secure storage of the terminal.
- 15 2. A method for biometric template extraction and secure biometric sample raw data storage, the method comprising:
 - a) enrolling, at a terminal, at least one biometric sample of a user;
 - 20 b) transmitting, preferably via a secure communication channel, the raw data of the biometric sample from the terminal to a server;
 - c) extracting, by an extraction application executed on the server, a biometric template from the raw data of the sample;
 - d) fragmenting, by a raw sample splitter executed on the server, the raw data of the biometric sample;
 - 25 e) distributing the fragments of the raw data of the biometric samples from the server to independent entities, preferably via a secure communication channel; and
 - f) deleting the biometric sample raw data from the memory of the server.
- 30 3. The method according to claim 1 or 2, wherein independent entity is selected from the group consisting of physically separated entities, electronically separated entities and/or distinct and separate legal entities and/or combinations thereof.

4. The method according to any of the preceding claims, wherein the fragmenting process produces at least two fragments.
5. The method according to claim 4, wherein the number of fragments corresponds to the number of entities used for storing the fragments.
6. The method according to claims 4 or 5, wherein at least one of the at least two fragments is an essential fragment which contains information of the biometric sample that is un-substitutable or un-rebuildable on the basis of the information of the respective other fragments, and, optionally, wherein the essential fragment is stored in a secure storage on the terminal.
7. The method according to any of the preceding claims, wherein the fragments consolidated upon a request from the user and the raw data of the biometric sample is rebuild from the fragments.
8. The method according to claim 7, wherein the biometric template is extracted from the rebuilt biometric sample.
9. The method according to claim 8, wherein the data used for biometric authentication or identification is compared with the extracted biometric template.
10. The method according to claim 7, wherein the consolidated fragments and the rebuilt biometric template are deleted after extraction of the biometric template.
11. A system for biometric template extraction and secure biometric sample raw data storage, the system comprising a terminal and at least one storage entity, wherein the terminal comprises a scanning device for enrolling at least one biometric sample of a user and is executing an extraction application, a raw sample splitting application, and a fragment distribution application,

wherein the terminal is configured to enrol, by the scanning device, at least one biometric sample of the user, to extract, by the extracting application, a biometric template from the enrolled raw biometric data of the sample, to fragment, by the raw sample splitting application, the raw data of the biometric sample and to distribute, by the fragment distribution application, the fragments for storage on the terminal and the at least one storage entity.

12. A terminal for performing the method according to claim 1, the terminal comprising:
 - 10 a capturing unit for capturing information related to a biometric sample of a user;
 - a processing unit, configured to enrol at least one biometric sample of a user from the captured information, to extract a biometric template from the biometric sample, and to fragment the biometric template; and
 - 15 a communication unit, configured to transmit at least part of the created fragments of the biometric template to independent entities.
13. A system for biometric template extraction and secure biometric sample raw data storage, the system comprising
 - 20 a terminal comprising capturing means for capturing information related to a biometric sample of a user and communication means for transmitting the captured raw data of the biometric sample;
 - a server comprising communication means to receive the raw data from the terminal, the server being configured to execute an extraction application to
 - 25 extract a biometric template from the raw data and a splitter application to fragment the raw data;
 - at least one independent entity comprising communication means to receive at least one fragment of the raw data from the server and storage means to store the received fragment.
- 30 14. A computer program product comprising computer executable instructions embodied in a computer readable medium for performing steps any of the method claims 1 to 10.

15. A computer readable medium storing program instructions, which, when executed by a processor of a computer cause the computer to perform each of the method steps of claims 1 to 10.

1/4

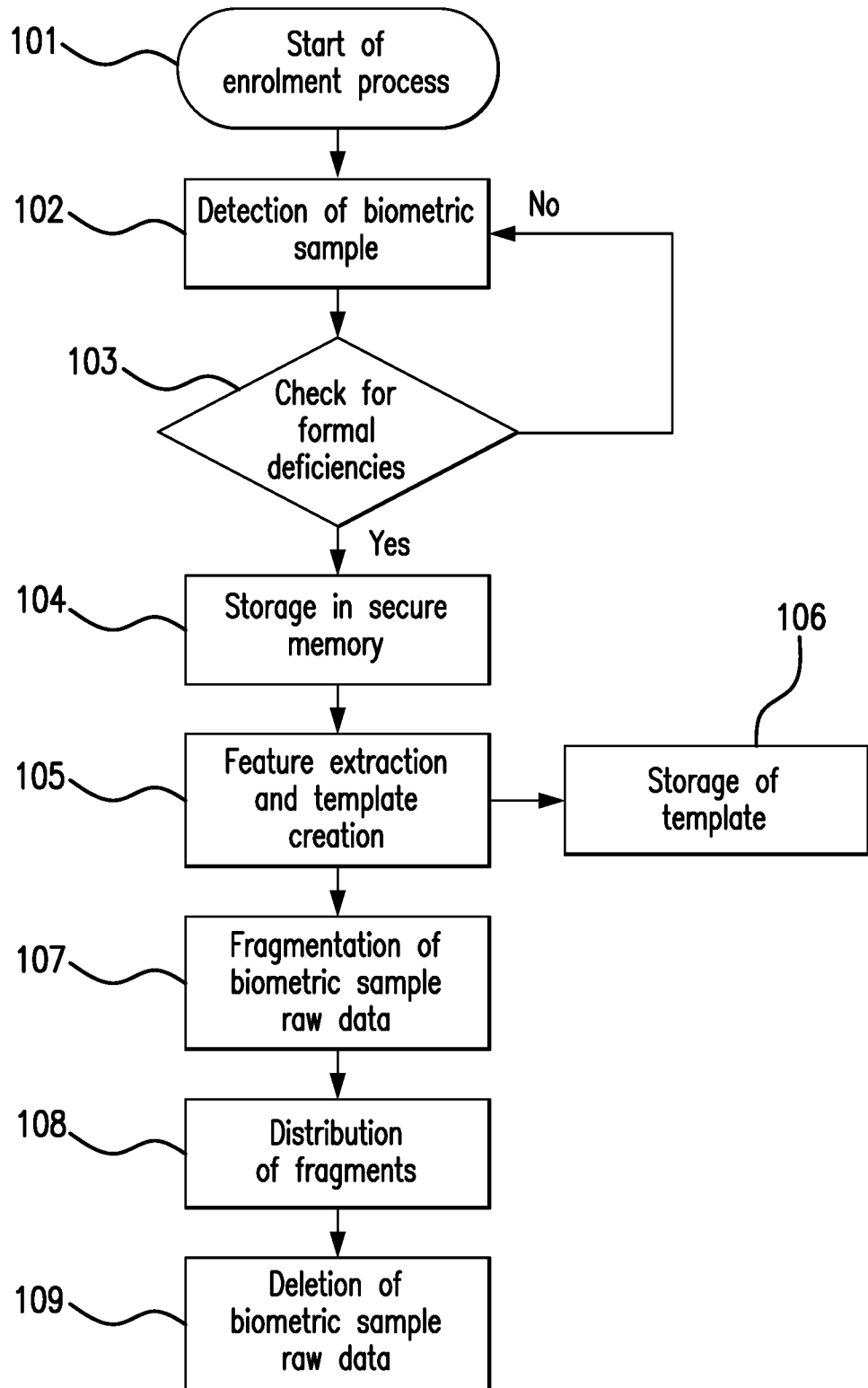
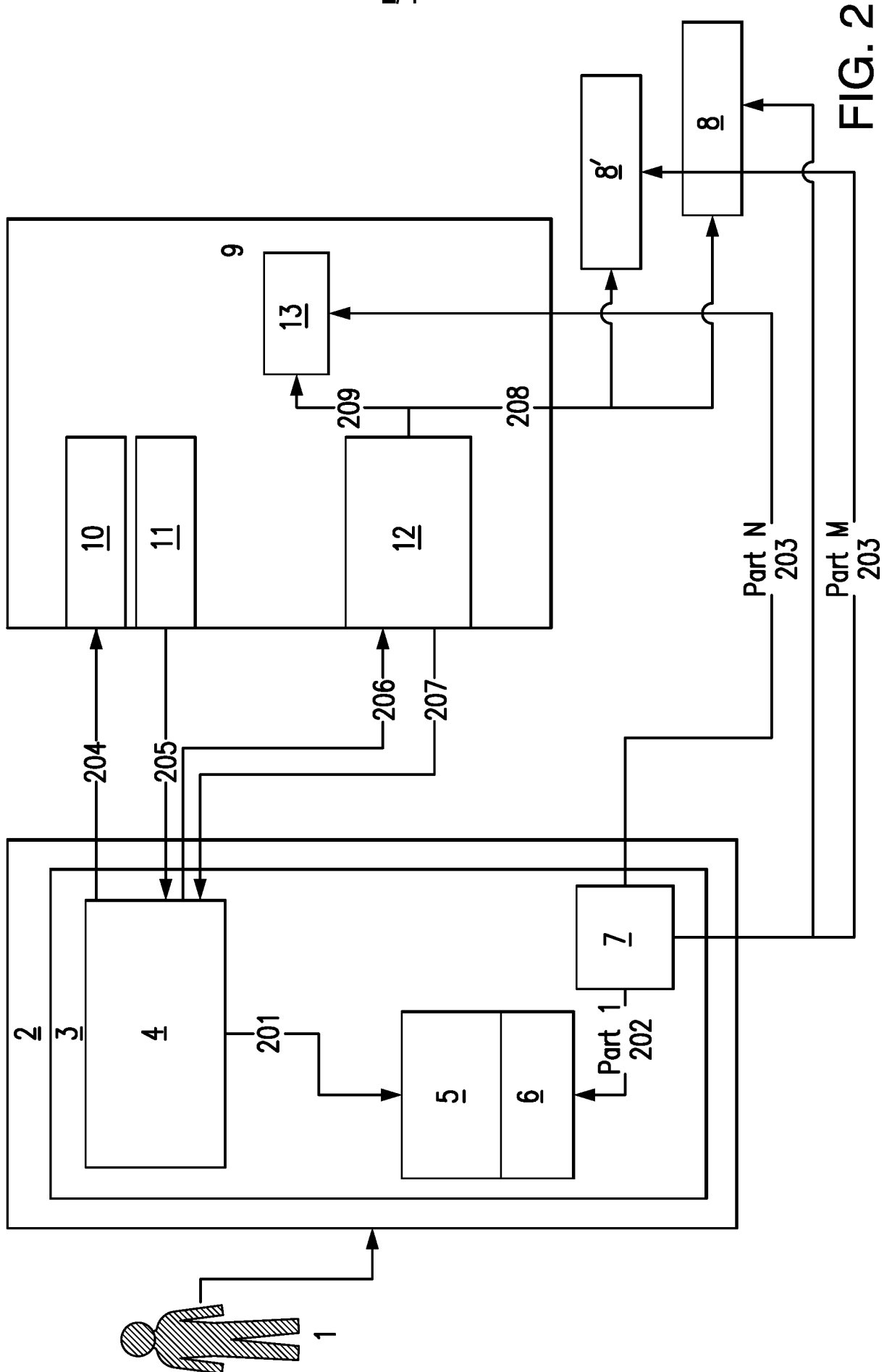


FIG. 1



3/4

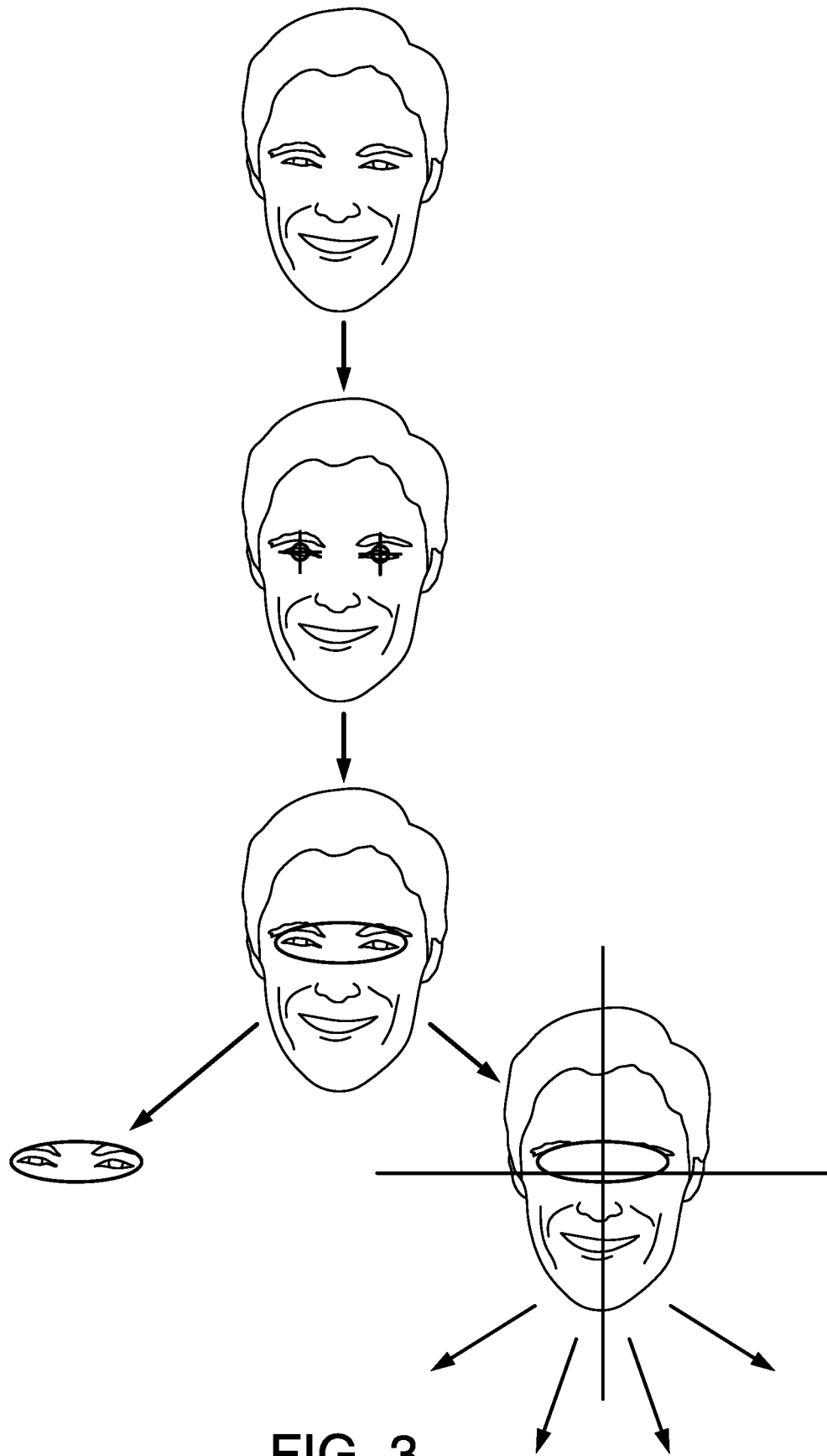


FIG. 3

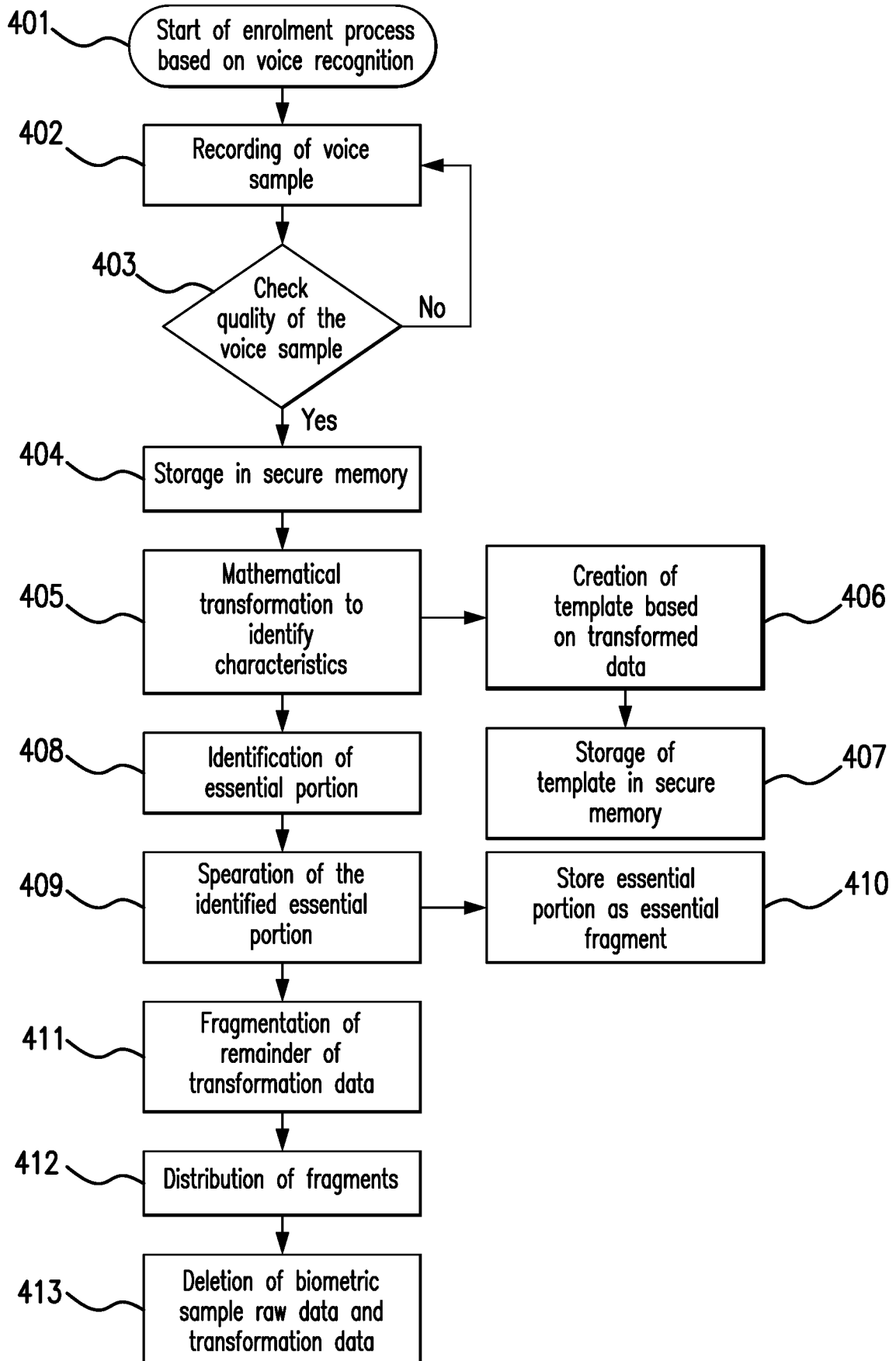


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2017/056459

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06K9/00 G06K9/22
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)

G06K G06F H04L

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, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/058639 A1 (EXOUDUS PAYMENT SYSTEMS LLC [US]; MCNEAL JOAN TIBOR [US]) 3 May 2012 (2012-05-03) paragraphs [0002], [0005], [0006], [0008] - [0018], [0035], [0050], [0051], [0055] - [0059], [0087] - [0091] -----	1-15
X	WO 2005/064547 A1 (TELECOM ITALIA SPA [IT]; BALTATU MADALINA [IT]; D ALESSANDRO ROSALIA []) 14 July 2005 (2005-07-14) page 4, lines 1-10 page 5, line 10 - page 6, line 26 page 8, line 5 - page 9, line 5 ----- -/-	1-15



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

8 January 2018

Date of mailing of the international search report

16/01/2018

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

Miclea, Sorin

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/056459

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/339749 A1 (SPUEHIER PHILIPPE [CH] ET AL) 19 December 2013 (2013-12-19) paragraphs [0003], [0008], [0010], [0019], [0021], [0024], [0027], [0030], [0035] - [0039] -----	1-15
A	WO 2015/175411 A1 (CLOUD CROWDING CORP [US]) 19 November 2015 (2015-11-19) paragraphs [0005], [0014] - [0016], [0040], [0045], [0046], [0051], [0075], [0076], [0105], [0106], [0120], [0129] -----	1-15
A	HASAN HAZILA ET AL: "Secured data partitioning in multi cloud environment", 2014 4TH WORLD CONGRESS ON INFORMATION AND COMMUNICATION TECHNOLOGIES (WICT 2014), IEEE, 8 December 2014 (2014-12-08), pages 146-151, XP032755421, DOI: 10.1109/WICT.2014.7077319 Sections II, III, IV.A, IV.D -----	1-15
A	US 2016/188974 A1 (MULLIN SEAN [US]) 30 June 2016 (2016-06-30) paragraphs [0042] - [0052] -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/056459

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012058639	A1	03-05-2012	CN 103314386 A 18-09-2013
		EP 2633484 A1 04-09-2013	
		RU 2013118922 A 10-12-2014	
		US 2012109829 A1 03-05-2012	
		WO 2012058639 A1 03-05-2012	

WO 2005064547	A1	14-07-2005	EP 1697907 A1 06-09-2006
		JP 4869944 B2 08-02-2012	
		JP 5470344 B2 16-04-2014	
		JP 2007522540 A 09-08-2007	
		JP 2012044670 A 01-03-2012	
		KR 20060127080 A 11-12-2006	
		US 2008019573 A1 24-01-2008	
		WO 2005064547 A1 14-07-2005	

US 2013339749	A1	19-12-2013	NONE

WO 2015175411	A1	19-11-2015	AU 2015259417 A1 01-09-2016
		CA 2948815 A1 19-11-2015	
		CN 106462605 A 22-02-2017	
		EA 201650049 A1 28-04-2017	
		EP 3143525 A1 22-03-2017	
		JP 2017523493 A 17-08-2017	
		KR 20170010787 A 01-02-2017	
		PH 12016502261 A1 06-02-2017	
		SG 11201609471T A 29-12-2016	
		US 2017048021 A1 16-02-2017	
		WO 2015175411 A1 19-11-2015	

US 2016188974	A1	30-06-2016	NONE
