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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 January 2022 (13.01.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/010338 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *G06F 21/60* (2013.01)

(21) International Application Number:
PCT/MY2020/050169

(22) International Filing Date:
25 November 2020 (25.11.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI2020003542 08 July 2020 (08.07.2020) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(72) Inventors: **MAT ISA, Maslan**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **ISMAIL, Ahmad Zuhairi**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **ANBARASAN, Durairaj**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **GOON, Wooi Kin**; Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(74) Agent: **KANDIAH, Geetha**; KASS International Sdn Bhd, Suite 8-13A-2, Menara Mutiara Bangsar, Jalan Liku, off Jalan Riong, Bangsar, Kuala Lumpur, 59100 (MY).

(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, IT, 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,

(54) Title: SYSTEM AND METHOD FOR BIOMETRIC AUTHENTICATION

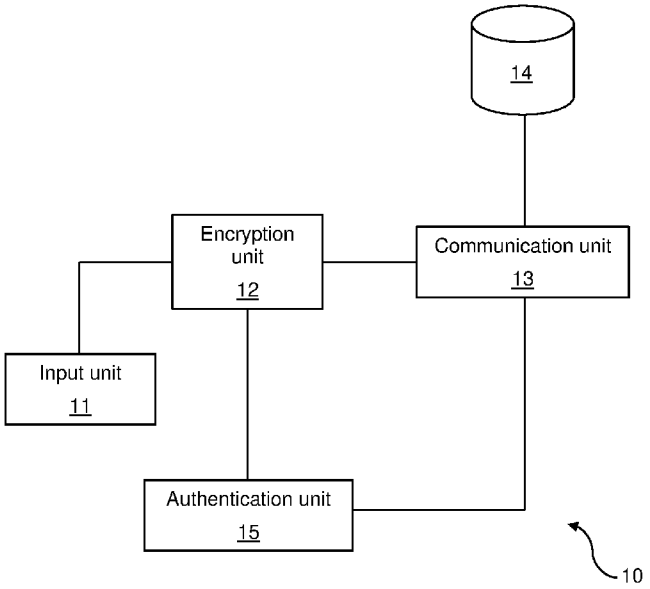

FIGURE 1

(57) Abstract: The present invention relates to a system and method for biometric authentication, wherein the system (10) comprises an input unit (11), an encryption unit (12), a communication unit (13) and a storage unit (14). The input unit (11) inputs a biometric feature of a user as a registration data during user registration and as an authentication data during user authentication. The encryption unit (12) encrypts the registration data during the user registration and encrypts the authentication data during the user authentication. The communication unit (13) forwards the encrypted registration data to the storage unit (14) for storage during the user registration and retrieves the stored registration data from the storage unit (14) during the user authentication. The authentication unit (15) compares the retrieved registration data with the encrypted authentication data during the user authentication and authenticates the user if a comparison score reaches a predefined threshold.

WO 2022/010338 A1

[Continued on next page]

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

SYSTEM AND METHOD FOR BIOMETRIC AUTHENTICATION

FIELD OF THE DISCLOSURE

The present invention relates broadly to the field of biometric authentication. More particularly, the present invention relates to a system and method for biometric authentication by storing a biometric template in a database.

BACKGROUND

Biometric authentication is considered as the strongest form of authentication as a biometric feature for a user is unique and is highly complex to duplicate. In general, a biometric reader device includes an imaging sensor for capturing an image of the biometric feature such as fingerprint, palm print, face print and the like. During registration, the biometric feature is captured and converted into a reference template which is then stored in a local and/or remote storage for verification during authentication process.

Even though biometric features are complicated to duplicate, storage of the template is one of the main problems faced in biometric authentication systems which are vulnerable to external hacker or internal administrator. A simple scenario would be when a hacker gains a digital copy of a biometric template stored in the system of a target person. The hacker can use it to access into systems that require biometric authentication to proceed.

Blockchain was introduced as a network of nodes storing immutable blocks of data time-stamped, secured and bound to each other by cryptographic principles. It is like a distributed ledger or decentralized database storing continuously updated digital records of who owns what. Unlike traditional database such as utilized by banks, governments, accountants, etc., blockchain has a network of replicated databases that are synchronized and visible to public within the network.

The network is not publicly available but rather only invited organizations can join the network. Each node channel has its own ledger and thus is a totally separated network. Data between channel members are shared through the channel but not between channels. It is possible to communicate between channels but this has to be specifically managed through applications or Digital contract. Otherwise, by design there is a complete data separation between channels.

Blockchain creates blocks in an append-only structure, wherein a block once created cannot be deleted or updated. Any new updates shall be included and added as a new block and each block has its own hash value before adding onto the chain of blocks. While adding a new block, a hash value of the last block is included to the new block, as shown in **FIGURE 4**, which makes it impossible to change or delete data within each block.

United States patent application no.: US 2018/0285879 A1 discloses a system and method for blockchain-based identity and transaction platforms, wherein identity information (e.g., a photo) for a person is encrypted and stored in a blockchain as part of enrolling the person as a user in a blockchain-based identity and transaction platform. During authentication, the stored information is compared with an identity information inputted with an authentication request.

However, there is still a need in the art for a system and method for biometric authentication which improves security of template storage in a database without compromising or complicating the authentication process.

SUMMARY

The present disclosure proposes a system and method for biometric authentication. The system comprises an input unit for inputting a biometric feature of a user as a registration data during user registration and as an authentication data during user authentication. An encryption unit encrypts the registration data during the user registration and encrypts the authentication data during the user authentication. A communication unit forwards the encrypted registration data to a storage unit for storage during the user registration and

retrieves the stored registration data from the storage unit during the user authentication. An authentication unit compares the retrieved registration data with the encrypted authentication data during the user authentication and authenticates the user if a comparison score reaches a predefined threshold.

In one aspect of the present invention, during the user registration, the encryption unit parses the registration data into multiple registration data portions and encrypts each registration data portion using an encryption algorithm. The communication unit forwards each encrypted registration data portion to a different storage location in the storage unit.

During the user authentication, the encryption unit parses the authentication data into the multiple authentication data portions and encrypts each authentication data portion using the encryption algorithm. The communication unit retrieves the encrypted registration data portions corresponding to the user from the storage locations. The authentication unit compares each encrypted authentication data portion with corresponding encrypted registration data portion to generate a comparison score and authenticates the user if the comparison score reaches a threshold.

In another embodiment of the present invention, the encryption unit encrypts each pair of authentication data portion and registration data portion using a different encryption algorithm. Optionally, the encryption unit includes a set of pre-stored encryption algorithms and dynamically chooses one of the encryption algorithms based on type of biometric feature, number of parsed data portions or any other factors related to encryption process.

The present invention parses the registration data, encrypts each parsed data portions and stores each encrypted data portion at a different storage location. By this way, the present invention improves protection of the biometric feature and thus preventing a fraudulent access to confidential data without complicating authentication process.

Various objects, features, aspects and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred

embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

In the figures, similar components and/or features may have the same reference numerals. Further, various components of the same type may be distinguished by following the reference numerals with a second numeral that distinguishes among the similar components. If only the first reference numeral is used in the specification, the description is applicable to any one of the similar components having the same first reference numeral irrespective of the second reference numeral.

FIGURE 1 shows a block diagram of the system for biometric authentication, in accordance with an exemplary embodiment of the present invention.

FIGURE 2 shows a flow diagram of the method for biometric authentication, in accordance with an exemplary embodiment of the present invention.

FIGURE 3 shows a schematic flow diagram of iris based authentication process, in accordance with an exemplary embodiment of the present invention.

FIGURE 4 shows a block representation of blocks within a traditional blockchain.

DETAILED DESCRIPTION

In accordance with the present disclosure, there is provided a system and method for biometric authentication, which will now be described with reference to the embodiments shown in the accompanying drawings. The embodiments do not limit the scope and ambit of the disclosure. The description relates purely to the embodiments and suggested applications thereof.

The embodiments herein and the various features and advantageous details thereof are explained with reference to the non-limiting embodiment in the

following description. Descriptions of well-known components and processes are omitted so as to not unnecessarily obscure the embodiments herein. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein may be practiced and to further enable those of skill in the art to practice the embodiment herein. Accordingly, the description should not be construed as limiting the scope of the embodiment herein.

The description hereinafter, of the specific embodiment will so fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify or adapt or perform both for various applications such specific embodiment without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation.

FIGURE 1 shows a block representation of the system for biometric authentication, in accordance with an exemplary embodiment of the present invention. The system (10) comprises an input unit (11), an encryption unit (12), a communication unit (13), a storage unit (14) and an authentication unit (15). The encryption unit (12) is connected between the input unit (11), communication unit (13) and the authentication unit (15) through a wired and/or wireless connection. Furthermore, the communication unit (13) is connected to the storage unit (14) and the authentication unit (15) through a wired and/or wireless connection. The input unit (11) inputs a biometric feature of a user, wherein the input unit (11) includes a scanning device for scanning the biometric feature. In a preferred embodiment, the biometric feature is fingerprint, palm print, face print, iris, retina and the like. Similarly, the scanning device includes but not limited to optical scanner, capacitive scanner and ultrasound scanner.

The encryption unit (12) receives and encrypts the inputted biometric feature using an encryption algorithm to generate an encryption data. In a preferred embodiment, the encryption unit (12) parses the inputted biometric feature into multiple data portions and encrypts each data portion using the encryption algorithm to generate multiple encryption data. In alternate embodiment, the

encryption unit (12) parses the inputted biometric feature into multiple data portions and encrypts each data portion using a different encryption algorithm to generate multiple encryption data.

In a preferred embodiment, the encryption unit (12) includes an algorithm storage module (not shown) for storing a set of parsing algorithms and encryption algorithms and an algorithm selection module (not shown) for selecting a parsing algorithm and one or more encryption algorithms. Preferably, the encryption algorithm includes a hashing algorithm such as Secure Hashing Algorithm (SHA) 1, Rivest–Shamir–Adleman (RSA) algorithm, SHA3 and Research and Development in Advanced Communications Technologies in Europe (RACE) Integrity Primitives Evaluation (RIPE) Message Digest (RIPEMD)-160 algorithm. Similarly, the biometric feature is parsed into rows, columns, matrix, concentric circles or any other two dimensional geometric shapes.

The selection of the parsing algorithm and the encryption algorithms are based on one or more pre-configured factors such as type of biometric feature, number of parsed data portions and the like, or by a random manner, rotational manner, etc. Additionally, the selection of encryption algorithm may be based on the parsing algorithm.

During a user registration, the encryption unit (12) outputs the encryption data to the communication unit (13) which in turn transmits the encryption data to the storage unit (14) for storage. Preferably, the communication unit (13) transmits each encryption data to a different storage locations in the storage unit (14). Alternatively, the storage unit (14) may include multiple storage databases, and the communication unit (13) includes a selection module (not shown) for selecting a storage location among the databases for storing each encryption data. The selection module may select the storage location in a random manner or based on a preselected factor.

Upon receiving the encryption data, an indexing module (not shown) in the storage unit (14) generates a composite key including a portion of one or more of the encryption data i.e. hash segment, and address of a storage location of each encryption data. Further, the indexing module creates an index table using the

composite key, wherein the index table stores composite keys generated during each user registration process. In a preferred embodiment, the indexing module follows a pre-configured algorithm to obtain a portion of the encryption data for generating the composite key and obtains the addresses from the selection module of the communication unit (13).

On the other hand, during a user authentication, the encryption unit (12) outputs the encryption data to the authentication unit (15). Furthermore, during the user authentication, the communication unit (13) retrieves the stored encryption data corresponding to the user and transfers the retrieved data to the authentication unit (15).

While retrieving the stored encryption data corresponding to the user requesting authentication, the authentication unit (15) transmits a portion of the encryption data generated during the user authentication to the communication unit (13). The communication unit (13) uses the received encryption data portion to obtain the address of each storage location of the corresponding stored encryption data in the storage unit (14). The communication unit (13) compares the received encryption data portion with the composite keys stored in the index table to identify the composite key including the matching encryption data portion and obtains one or more addresses stored in the composite key including the matching encryption data portion.

Based on the obtained addresses, the communication unit (13) retrieves each stored encryption data and transfers the same to the authentication unit (15) which compares each retrieved data with the corresponding encryption data received from the encryption unit (12) to generate a comparison score. The authentication unit (15) includes a calculation module (not shown) for calculating an average of the comparison scores.

If the average of the comparison scores reaches a threshold, the authentication unit (15) authenticates the user by outputting an authentication signal to a security module (not shown) to allow the user to access one or more resources (not shown) secured by the security module. In a preferred embodiment, the security module is a secured storage space e.g. software file, folder, drive and/or server,

for storing one or more confidential data. Alternatively, the security module may also be an electronic lock coupled to a security gate, lift, vehicle, vending machine, point-of-sale (POS) and the like.

FIGURE 2 shows a flow diagram of a method for biometric authentication in accordance with an exemplary embodiment of the present invention. The method (20) comprises the steps of: registering a user using a biometric feature of the user (21) and authenticating the user using the biometric feature (22). While registering the user, the biometric feature is inputted as a registration data at an inputting unit and the registration data is encrypted at an encryption unit and then stored in a storage unit. Furthermore, while authenticating the user, the biometric feature is inputted as an authentication data at the inputting unit and the authentication data is encrypted at an encryption unit and then compared with the encrypted registration data stored in the storage unit.

During user registration, the registration data is parsed into multiple registration data portions and each registration data portion is encrypted using an encryption algorithm. Furthermore, each encrypted registration data portion is stored at a different storage location in a storage unit. During user authentication, the authentication data is parsed into multiple authentication data portions and each authentication data portion is encrypted. Furthermore, the encrypted registration data portions corresponding to the user are retrieved from the corresponding storage locations, and each encrypted registration data portion is compared with the corresponding encrypted authentication data portion to generate a comparison score. If the comparison score reaches a threshold, the user is authenticated.

Entire functionality of the present invention is divided into two sections: 1) User registration, and 2) User authentication. Each section is explained in detail with an example in the forthcoming paragraphs.

In an embodiment, the user is registered by using an iris of the user as the registration data, as shown in **FIGURE 3**. An imaging device captures an image of an eye of the user and extracts the iris from the eye image. The extracted iris is parsed into four equal portions to form a 2X2 matrix and each iris portion is hashed using a hashing algorithm at a digital contract to generate four hashed

templates #I, #II, #III and #IV. Each of the hashed templates #I, #II, #III and #IV is stored at a different block in a blockchain database, wherein no two blocks storing the hashed templates #I, #II, #III and #IV are adjacent to one another.

During the user authentication, the imaging device captures an image of the eye and extracts the iris form the eye image. The extracted iris is parsed into four equal portions to form a 2X2 matrix same as the 2X2 matrix generated during the user registration. Each iris portion is hashed at the digital contract to generate four hashed input data #i, #ii, #iii and #iv using the same hashing algorithm that is used during the user registration to generate the four hashed templates #I, #II, #III and #IV. The hashed templates #I, #II, #III and #IV stored in the blocks are retrieved and compared with the corresponding hashed input data #i, #ii, #iii and #iv to generate a comparison score.

To be precise, the hashed template #I is compared with the hashed input #i to generate a first comparison score and the hashed template #II is compared with the hashed input #ii to generate a second comparison score. Likewise the hashed templates #III and #IV are compared with the corresponding hashed inputs #iii and #iv to generate a third comparison score and a fourth comparison score, respectively. An average of the four comparison scores is computed, and if the average reaches a threshold, an authentication signal is outputted for authenticating the user.

Even though the above embodiment is described using a single encryption algorithm for encrypting the registration data and the authentication data, it is to be understood that each registration -authentication data portion pair may be encrypted using a different encryption algorithm which is selected based on one or more factors. For example, in the above embodiment, the top left portion of the iris image captured for user registration and the top left portion of the iris image captured for user authentication form a top left pair of registration data portion and authentication data portion. Similarly, other three portions of the iris image captured for user registration form three pairs of registration data portion and authentication data portion with the corresponding portions of the iris image captured for user authentication.

Each pair of registration data portion and authentication data portion may be encrypted using a different encryption algorithm. Alternatively, two pairs may be encrypted using one encryption algorithm, while the other two pairs may be encrypted using another encryption algorithm. Furthermore, it is also possible to encrypt three pairs using one encryption algorithm and one pair using another encryption algorithm. Similarly, the iris image may also be parsed, horizontally, vertically, diagonally or radially of equal width.

The biometric feature is split into multiple portions and each portion is separately hashed using a same or different hashing algorithm and is stored in different storage locations. If anyone attempts to wrongfully obtain the biometrics of a user, all template portions corresponding to the user need to be identified in the blockchain. Further, dynamic encryption of each portion of the same templates enhances protection of the template. By this way, the present invention is capable of improving security of template storage in a blockchain database without compromising or complicating the authentication process.

The terminology used herein is for the purpose of describing particular example embodiments only and is not intended to be limiting. As used herein, the singular forms "a", "an" and "the" may be intended to include the plural forms as well, unless the context clearly indicates otherwise.

The terms "comprises," "comprising," “including,” and “having,” are inclusive and therefore specify the presence of stated features, integers, steps, operations, elements, or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, or groups thereof.

The use of the expression “at least” or “at least one” suggests the use of one or more elements, as the use may be in one of the embodiments to achieve one or more of the desired objects or results.

While the foregoing describes various embodiments of the invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof. The scope of the invention is determined by the claims that follow. The invention is not limited to the described embodiments, versions or

examples, which are included to enable a person having ordinary skill in the art to make and use the invention when combined with information and knowledge available to the person having ordinary skill in the art.

CLAIMS:

1. A system (10) for biometric authentication, comprising:
   i. at least one input unit (11) for inputting a biometric feature of a user as a registration data during user registration and as an authentication data during user authentication;
   ii. at least one encryption unit (12) for encrypting said registration data during said user registration and for encrypting said authentication data during said user authentication;
   iii. at least one storage unit (14) for storage during said user registration;
   iv. at least one communication unit (13) for forwarding said encrypted registration data to said storage unit (14) for storage during said user registration and for retrieving said stored registration data from said storage unit (14) during said user authentication;
   v. at least one authentication unit (15) for comparing said retrieved registration data with said encrypted authentication data during said user authentication and authenticating said user if a comparison score reaches a predefined threshold, characterized in that,

   during said user registration,
   - said encryption unit (12) parses said registration data into multiple registration data portions and encrypts each registration data portion; and
   - said communication unit (13) forwards each encrypted registration data portion to a different storage location in said storage unit (14) for storage, and

   during said user authentication,
   - said encryption unit (12) parses said authentication data into multiple authentication data portions and encrypts each authentication data portion;
   - said communication unit (13) retrieves said encrypted registration data portions corresponding to said user from said storage locations; and
   - said authentication unit (15) compares each encrypted registration data portion with corresponding encrypted

authentication data portion to generate at least one comparison score and authenticates said user if said comparison score reaches a threshold.

2. The system of claim 1, wherein said encryption unit (12) includes:
   - an algorithm storage module for storing one or more encryption algorithms and parsing algorithms; and
   - an algorithm selection module for selecting a parsing algorithm for parsing said registration data and said authentication data, and for selecting an encryption algorithm for encrypting each registration data portion and each authentication data portion.
3. The system (10) of claim 2, wherein said encryption unit (12) encrypts said registration data portions and said authentication data portions using an encryption algorithm.
4. The system (10) of claim 2, wherein said encryption unit (12) encrypts each registration-authentication data portion pair using a different encryption algorithm.
5. The system (10) of claim 2, wherein said encryption algorithms include a hashing algorithm.
6. The system (10) of claim 2, wherein said encryption unit (12) parses said registration data and said authentication data based on a parsing algorithm.
7. The system (10) of claim 1, wherein said storage unit (14) includes at least one blockchain database.
8. A method (20) for biometric authentication, comprising the steps of:
   i. registering a user using at least one biometric feature of said user (21), wherein said biometric feature is inputted as a registration data at an input unit and said registration data is encrypted at an encryption unit and then stored in at least one storage unit; and
   ii. authenticating said user using said biometric feature (22), wherein said biometric feature is inputted as an authentication data at said input unit

and said authentication data is encrypted at an encryption unit and then compared with said encrypted registration data stored in said storage unit, characterized in that,

said step of registering said user includes:

- parsing said registration data into multiple registration data portions;
- encrypting each registration data portion; and
- storing each encrypted registration data portion at a different storage location in said storage unit, and

said step of authenticating said user includes:

- parsing said authentication data into multiple authentication data portions;
- encrypting each authentication data portion;
- retrieving said encrypted registration data portions corresponding to said user from said storage locations;
- comparing each encrypted registration data portion with corresponding encrypted authentication data portion to generate at least one comparison score; and
- authenticating said user if said comparison score reaches a threshold.

9. The method (20) of claim 8, wherein said step of encrypting includes:

- selecting a parsing algorithm from one or more parsing algorithms pre-stored in a storage module;
- parsing said biometric feature using said selected parsing algorithm;
- selecting at least one encryption algorithm from one or more encryption algorithms pre-stored in said storage module; and
- encrypting each data portion using said selected encryption algorithm.

10. The method (20) of claim 8, wherein said step of comparing each encrypted registration data portion with corresponding encrypted authentication data portion includes:

- comparing said encrypted registration data portions with corresponding encrypted authentication data portions to generate respective comparison scores;
- calculating an average score of said comparison scores; and
- outputting said average scare as a final comparison score.

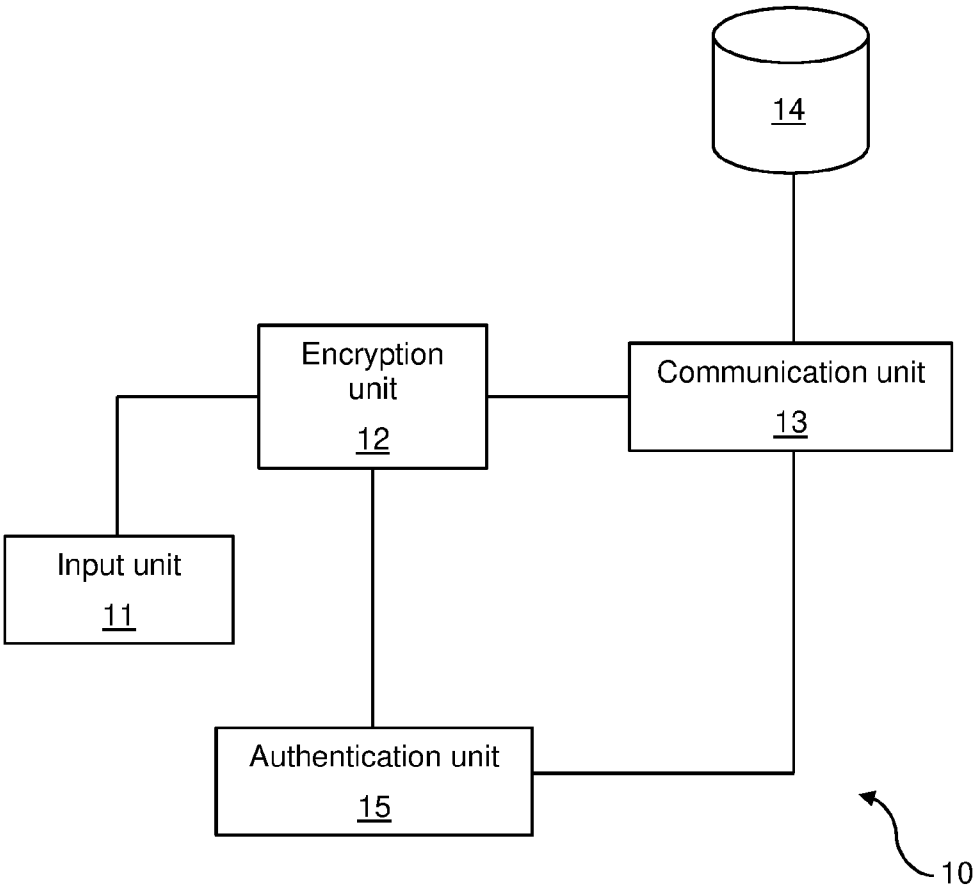

FIGURE 1

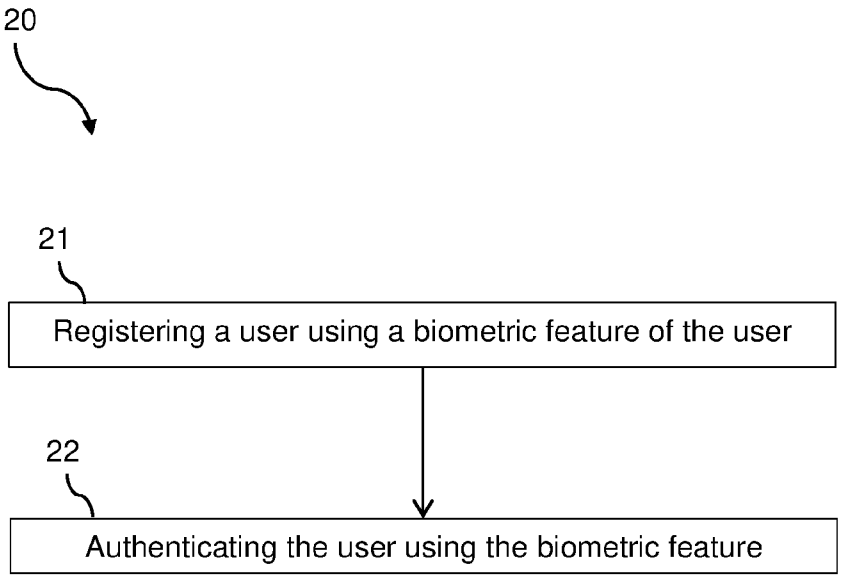

FIGURE 2

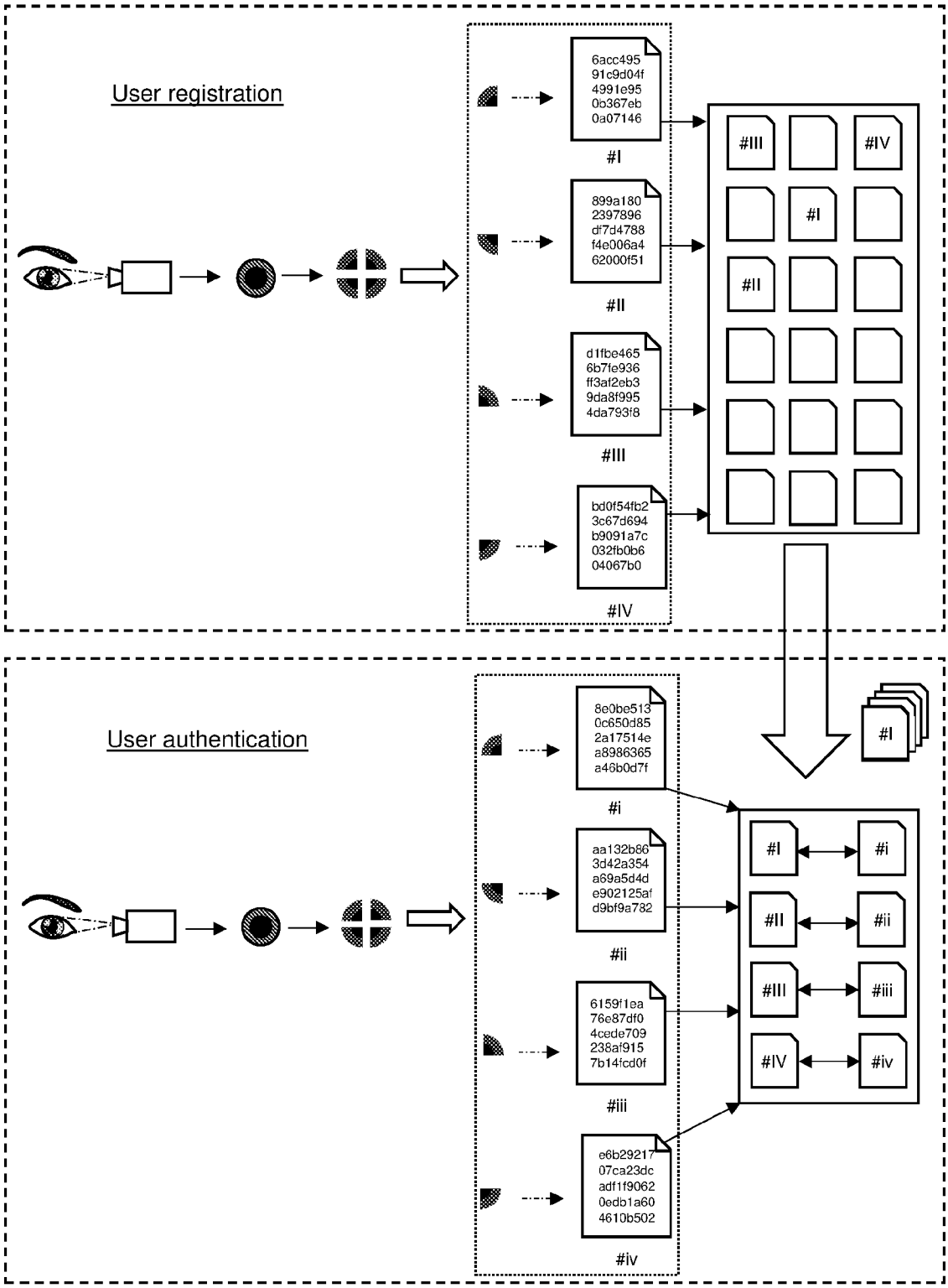
User registration
6acc495
91c9d04f
4991e95
0b367eb
0a07146
#I
899a180
2397896
df7d4788
f4e006a4
62000f51
#II
d1fbe465
6b7fe936
ff3af2eb3
9da8f995
4da793f8
#III
bd0f54fb2
3c67d694
b9091a7c
032fb0b6
04067b0
#IV
#III
#IV
#I
#II
User authentication
8e0be513
0c650d85
2a17514e
a8986365
a46b0d7f
#i
aa132b86
3d42a354
a69a5d4d
e902125af
d9bf9a782
#ii
6159f1ea
76e87df0
4cede709
238af915
7b14fcd0f
#iii
e6b29217
07ca23dc
adf1f9062
0edb1a60
4610b502
#iv
#I
#I
#i
#II
#ii
#III
#iii
#IV
#iv

FIGURE 3

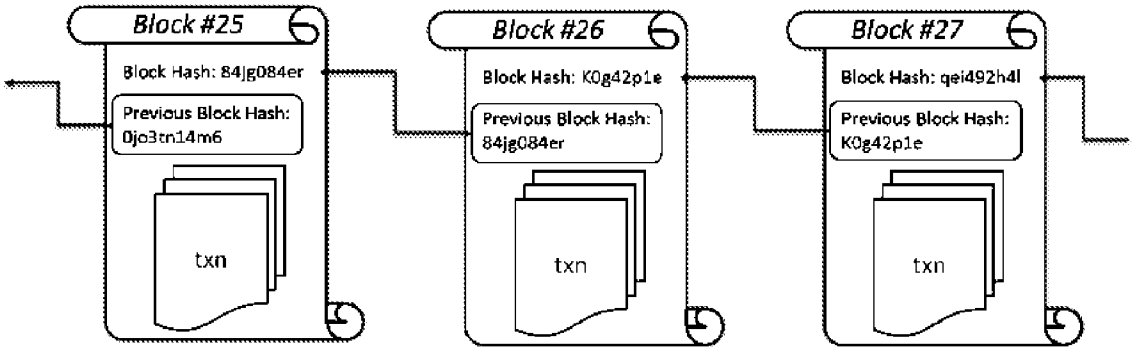
Block #25
Block Hash: 84jg084er
Previous Block Hash:
0jo3tn14m6
txn
Block #26
Block Hash: K0g42p1e
Previous Block Hash:
84jg084er
txn
Block #27
Block Hash: qei492h4l
Previous Block Hash:
K0g42p1e
txn

FIGURE 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2020/050169

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i; ***G06F 21/60***(2013.01)i
FI: G06F21/32; G06F21/60 320

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)

G06F21/32; G06F21/60

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2021
Registered utility model specifications of Japan 1996-2021
Published registered utility model applications of Japan 1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1564686 A1 (FUJITSU LIMITED) 17 August 2005 (2005-08-17) claims 1,4,8, pars. [0087]-[0098], figs. 11-14	1-10
A	JP 2006-293712 A (GLORY LTD.) 26 October 2006 (2006-10-26) claim 9, pars. [0133]-[0150], figs. 15-17	1-10
A	WO 2009/146315 A1 (NEWPORT SCIENTIFIC RESEARCH, LLC) 03 December 2009 (2009-12-03) claim 1	1-10

☐ 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	Date of mailing of the international search report
06 January 2021	**19 January 2021**
Name and mailing address of the ISA/JP **Japan Patent Office** **3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo** **100-8915, Japan**	Authorized officer **HIRAI, Makoto 5S 9071** Telephone No. **+81-3-3581-1101 Ext. 3546**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/MY2020/050169

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
EP 1564686 A1	17 August 2005	WO 2004/088591 A1 claims 1,4,8, p.18, line 25-p.21, line 21, figs. 11-14 US 2005/0223003 A1 CN 1689040 A	
JP 2006-293712 A	26 October 2006	(Family: none)	
WO 2009/146315 A1	03 December 2009	US 2009/0300737 A1	