



(51) International Patent Classification:
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/US2016/044202

(22) International Filing Date:
27 July 2016 (27.07.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201510447170.9 27 July 2015 (27.07.2015) CN

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED**
[—/US]; Fourth Floor, One Capital Place, P.O. Box 847,
Grand Cayman (KY).

(72) Inventors: **WANG, Xiaofeng**; Alibaba Group Legal Department, 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (CN). **WAN, Weiqin**; Alibaba Group Legal Department, 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (CN). **DONG, Hui**; Alibaba Group Legal Department, 5/F,

Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (CN). **YU, Yang**; Alibaba Group Legal Department, 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (US). **XIE, Daocheng**; Alibaba Group Legal Department, 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (US). **LI, Lizhong**; Alibaba Group Legal Department, 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (US).

(74) Agents: **NELSON, Brett, L.** et al.; Lee & Hayes, PLLC, 601 W. Riverside Ave, Suite 1400, Spokane, WA 99201 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[Continued on next page]

(54) Title: USER IDENTITY VERIFICATION METHOD AND SYSTEM, AND VERIFICATION SERVER

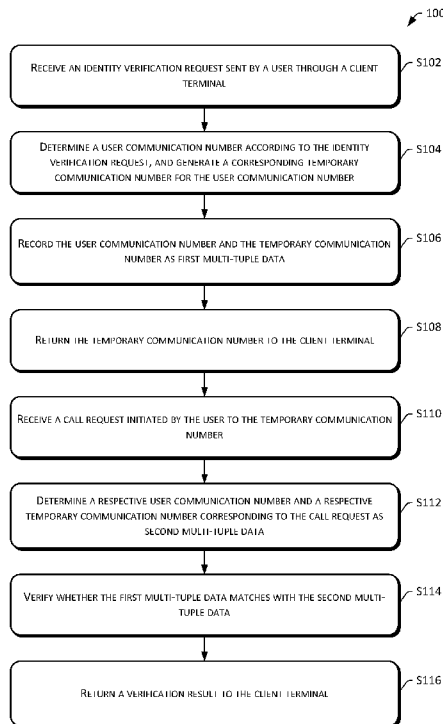


FIG. 1

(57) Abstract: A user identity verification method is disclosed. The method includes receiving an identity verification request sent by a user through a client terminal; determining a user communication number according to the identity verification request and generating a corresponding temporary communication number for the user communication number; recording the user communication number and the temporary communication number as first data; returning the temporary communication number to the client terminal; receiving a call request initiated by the user to the temporary communication number; determining a respective user communication number and a respective temporary communication number corresponding to the call request as second data; verifying whether the first data matches with the second data; and returning a verification result to the client terminal. The method can improve security and reliability of identity verification, reduce a user's waiting time, and enhance user experience.





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))

USER IDENTITY VERIFICATION METHOD AND SYSTEM, AND VERIFICATION SERVER

Cross Reference to Related Patent Application

5 This application claims foreign priority to Chinese Patent Application No. 201510447170.9 filed on July 27, 2015, entitled "User Identity Verification Method and System, and Verification Server", which is hereby incorporated by reference in its entirety.

Technical Field

10 The present disclosure relates to the Internet field, and in particular, to user identity verification methods and systems, and verification servers.

Background

15 With the continuous development of Internet technologies, an increasing number of users can conduct interactive activities or obtain services via the Internet. Under many circumstances, an identity of a user needs to be verified in situations in which the user conducts an Internet or mobile Internet activity, such as in scenarios of registration, login, etc. At present, a verification method primarily includes performing verification using a short message verification code. This method includes sending a short message verification code
20 to a mobile phone number provided by a user who inputs the short message verification code in a corresponding position according to a prompt. A background server may then verify whether the short message verification code entered by the user is consistent with the short message verification code previously sent to the user, and verification is passed if they are consistent. However, short message verification codes are easily intercepted by a third
25 party or Trojan during transmission or after arriving at mobile phones, the security thereof is relatively low. Furthermore, as an arrival rate of short messages cannot be guaranteed, a success rate of identity verification cannot reach an ideal value, thus affecting user experience.

Summary

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify all key features or essential features of the claimed subject matter, nor is it intended to be used alone as an aid in determining the scope of the claimed subject matter. The term “techniques,” for instance, may refer to device(s), system(s), method(s) and/or computer-readable instructions as permitted by the context above and throughout the present disclosure.

The present disclosure aims to resolve technical problems in existing technologies. Accordingly, an objective of the present disclosure is to provide a user identity verification method, which can improve security and reliability of identity verification, reduce waiting times of users, and enhance user experience. A second objective of the present disclosure is to provide a verification server. A third objective of the present disclosure is to provide a user identity verification system.

In order to achieve the above objectives, an example user identity verification method according to a first aspect of the present disclosure may include receiving an identity verification request sent by a user through a client terminal; determining a user communication number according to the identity verification request, and generating a corresponding temporary communication number for the user communication number; recording the user communication number and the temporary communication number as first data; returning the temporary communication number to the client terminal; receiving a call request for the temporary communication number initiated by the user; determining a corresponding user communication number and a corresponding temporary communication number of the call request as second data; verifying whether the first data matches with the second data; and returning an verification result to the client terminal.

According to the example user identity verification method, first data made up of a user communication number and a temporary communication number may be generated according to an identity verification request sent from a client terminal, and the temporary communication number may be returned to the client terminal. In response to a call request for the temporary communication number initiated by a user, verification may be performed

based on whether second data made up of a user communication number and a temporary communication number which correspond to the call request matches with the first data. The method can initiate a call to a temporary communication number allocated by a verification server from a user communication number, so that identity verification can be performed for the user through a voice channel between the user and the verification server. Therefore, security and reliability of the identity verification can be improved, and a waiting time of the user is reduced, thus enhancing user experience.

In order to achieve the above objectives, an example verification server according to a second aspect of the present disclosure may include an verification request receiving module used for receiving an identity verification request sent by a user through a client terminal; a determination module used for determining a user communication number according to the identity verification request; a generation module used for generating a corresponding temporary communication number for the user communication number, and recording the user communication number and the temporary communication number as first data; a first returning module used for returning the temporary communication number to the client terminal; a call request receiving module for receiving a call request initiated by the user to the temporary communication number; a verification module used for determining a respective user communication number and a respective temporary communication number corresponding to the call request as second data, and verifying whether the first data matches with the second data; and a second returning module used for returning a verification result to the client terminal.

According to the example verification server of the present disclosure, first data made up of a user communication number and a temporary communication number may be generated according to an identity verification request sent from a client terminal, and the temporary communication number may be returned to the client terminal. In response to a call request for the temporary communication number initiated by a user, verification may be performed based on whether second data made up of a user communication number and a temporary communication number which correspond to the call request matches with the first data. The method can initiate a call to a temporary communication number allocated by a verification server from a user communication number, so that identity verification can be

performed for the user through a voice channel between the user and the verification server. Therefore, security and reliability of the identity verification can be improved, and a waiting time of the user is reduced, thus enhancing user experience.

In order to achieve the above objectives, an example user identity verification system according to a third aspect of the present disclosure may include a client terminal and the verification server according to the second aspect of the present disclosure.

According to the example user identity verification system of the present disclosure, the verification server may generate first data made up of a user communication number and a temporary communication number according to an identity verification request sent by a client terminal, and return the temporary communication number to the client terminal. In response to initiating a call request for the temporary communication number initiated by a user, verification may be performed whether second data made up of a user communication number and a temporary communication number which correspond to the call request matches with the first data. The method can initiate a call to a temporary communication number allocated by the verification server from a user communication number, so that identity verification can be performed for the user through a voice channel between the user and the verification server. Therefore, security and reliability of the identity verification can be improved, and a waiting time of the user is reduced, thus enhancing user experience.

Advantages of additional aspects of the present disclosure will be partially set forth in the following description, which will be made apparent from the following description, or may be understood through implementations of the present disclosure.

Description of the Drawings

FIG. 1 is a flowchart of a user identity verification method according to an embodiment of the present disclosure.

FIG. 2 is a schematic structural diagram of a verification server according to an embodiment of the present disclosure.

FIG. 3 is a sequence diagram of a user identity verification process according to an embodiment of the present disclosure.

FIG. 4 is a schematic structural diagram of a user identity verification system according to an embodiment of the present disclosure.

Detailed Description

5 Exemplary embodiments of the present disclosure are described in detail hereinafter, and examples of the embodiments are illustrated in accompanying drawings, where the same or similar signs represent the same or similar elements or elements having the same or similar functions. The following embodiments described with reference to the accompanying drawings are exemplary, being used only for explaining the present disclosure,
10 and thus should not be construed as limitations to the present disclosure.

A method, a system, a terminal, a verification server and a support server for user identity verification according to the embodiments of the present disclosure are described hereinafter with reference to the accompanying drawings.

FIG. 1 is a flowchart of a user identity verification method 100 according to an
15 embodiment of the present disclosure.

It should be understood that the user identity verification method in the present embodiment may be performed by a verification server.

As shown in FIG. 1, the user identity verification method 100 may include the following operations.

20 S102 receives an identity verification request sent by a user through a client terminal.

When a user registers or logs in through a client terminal, an identity of the user needs to be verified. At this point, the user may send an identity verification request to a verification server through the client terminal. In implementations, the client terminal may provide a registration or login interface, with the interface including a registration or login
25 button. After the user clicks the button, the client terminal sends an identity verification request to the verification server.

In implementations, the client terminal may include a WEB page terminal, an APP terminal, a WAP page terminal or the like.

S104 determines a user communication number according to the identity verification request, and generates a corresponding temporary communication number for the user communication number.

In implementations, if the identity verification request is sent when the user registers a new account, the identity verification request further includes a user communication number. The user communication number is inputted when the user submits the identity verification request. In implementations, when the user registers a new account and identity verification thereof needs to be performed, the client terminal may provide an input box or an input region in a registration interface and instruct the user to input a user communication number. After the user inputs the communication number and clicks a registration button, the client terminal may send the identity verification request including the user communication number to the verification server. Upon receiving the identity verification request, the verification server may obtain the user communication number therein.

In implementations, if the user is a registered user, the identity verification request may include account information of the registered user. Determining the user communication number according to the identity verification request may include determining a corresponding user communication number according to the account information of the registered user. In implementations, since the user may have submitted a user communication number corresponding to registered account information (a username, a user ID and the like) during registration, the verification server may store the user communication number and the registered account information correspondingly in a user information library. Therefore, when the user uses a specific service (for example, login, payment, transfer, etc.) that needs to verify an identity of the user, the verification server may determine corresponding account information of the user according to the identity verification request and search for a corresponding user communication number from the stored user information library.

After the user communication number is determined, the verification server may generate a corresponding temporary communication number for the user communication number. The temporary communication number may include a mobile phone number, a

special service number, a landline telephone number, a network telephone number, etc. The verification server may apply for communication numbers in one or more segments in advance from service providers (mobile communication service providers such as Mobile, Unicom, Telecom, etc.). After the user communication number is determined, a
5 communication number is randomly selected from the applied communication numbers as a corresponding temporary communication number.

In implementations, after a communication number is selected as a temporary communication number, this communication number cannot be used as a temporary communication number corresponding to the user communication number in other
10 verification processes any more. In additional implementations, a temporary communication number may also be allocated according to another allocation rule. For example, a same temporary communication number may be allocated to user communication numbers for identity verification requests initiated from a same client terminal having an identifier according to the identifier of the client terminal. The present disclosure does not impose any
15 limitation on details of a rule of allocating a verification number.

S106 records the user communication number and the temporary communication number as first multi-tuple data.

In implementations, the first multi-tuple data may include two-tuple data including the user communication number and the temporary communication number.

20 In additional implementations, the identity verification request may further include a client terminal identifier, and the first multi-tuple data may be generated based on the user communication number, the client terminal identifier and the temporary communication number.

For example, three-tuple data may be in a form of AX or AXB, where A is a user
25 communication number, X is a temporary communication number, and B is a client terminal identifier.

It should be understood that the temporary communication number is allocated for the user communication number, and thus only the user communication number can initiate a call to the temporary communication number.

30 S108 returns the temporary communication number to the client terminal.

In implementations, the identity verification request may further include a client terminal identifier, and S108 may include returning the temporary communication number to a client terminal corresponding to the client terminal identifier. Thus, the temporary communication number can be accurately returned to the corresponding client terminal, thereby improving the accuracy of the verification.

S110 receives a call request initiated by the user to the temporary communication number.

In implementations, after the client terminal receives the temporary communication number, the temporary communication number may be displayed to the user, and the user may be prompted to initiate a call to the temporary communication number. After receiving the prompt, the user may initiate a call to the temporary communication number via a mobile telephone, a landline telephone or an application program having a voice communication function.

In implementations, the client terminal may display the temporary communication number in a form of a two-dimensional code. The user may use a mobile terminal to initiate a call to the temporary communication number by scanning and parsing the two-dimensional code. Apparently, the client terminal may also display the temporary communication number in another manner, which is not limited in the present disclosure. For example, the temporary communication number may be displayed via a bar code, a pattern, etc.

S112 determines a respective user communication number and a respective temporary communication number corresponding to the call request as second multi-tuple data.

S114 verifies whether the first multi-tuple data matches with the second multi-tuple data.

After receiving the call request initiated by the user, the verification server may determine a user communication number (a communication number of a calling party) and a temporary communication number (a communication number of a called party), and generate second multi-tuple data. Verification may then be performed as to whether the recorded first multi-tuple data matches with the second multi-tuple data.

If the first multi-tuple data does not match with the second multi-tuple data, the verification of the user is determined to be failed. Thus, an identity of the user can be verified based on whether the received call request is an identity verification request using a call from the corresponding user communication number to the temporary communication
5 number. Compared with the method of performing verification using a short message verification code, a user communication number is extremely difficult to be counterfeited in this method of initiating a call through a user communication number, and thus the security of verification is higher.

If the first multi-tuple data matches with the second multi-tuple data, a prompt audio
10 message is further played to the user, and information inputted by the user according to the prompt audio message is received. Verification is performed as to whether the inputted information is consistent with the content of the prompt audio message. If the inputted information is consistent with the content of the prompt audio message, the verification succeeds. Otherwise, the verification fails. In implementations, the prompt audio message
15 instructs the user to input a specified key, numerical string or character string.

Furthermore, the verification server may select content of a prompt audio message to be played according to a security level of the verification. For example, if the security level of the verification is a low level, the verification server may play a default prompt audio message, and the verification succeeds after the default prompt audio message is played
20 completely. If the security level of the verification is a middle level, the verification server may instruct the user to press a corresponding key. If the security level of the verification is a high level, the verification server may instruct the user to input a corresponding numerical string or character string. After the user inputs the numerical string or character string, verification is performed to determine whether information inputted by the user is
25 consistent with the content of the prompt audio message. If affirmative, the verification is passed. Otherwise, the verification fails.

A security level may be set by the verification server according to an identity of a user corresponding to an identity verification request. For example, if the user is in a normal state, a low-level verification may be selected. If the user is in an abnormal state (for example, a

remote login, etc.), a mid-level verification may be selected. If the user is flagged, a high-level verification may be selected.

In implementations, the verification server may also carry out verification according to the time at which a user initiates a call request. In implementations, the method may further
5 include verifying whether a time difference between a time of initiating the call request and a time of generating the first multi-tuple data is less than a preset time; and determining that the user verification fails if the time difference is greater than or equal to the preset time; or sending a prompt audio message to perform additional verification otherwise.

S116 returns a verification result to the client terminal.

10 In implementations, a verification result may be returned to a corresponding client terminal according to the client terminal identifier in the identity verification request. Thus, the verification result can be accurately returned to the corresponding client terminal, thereby improving the accuracy of the verification.

In additional implementations, other different verification rules may be set up in
15 advance for different client terminals. Therefore, after receiving a call request, the verification server may select a corresponding verification rule to carry out verification according to a client terminal identifier. Thus, corresponding verification rules may be selected for performing verification according to requirements of different client terminals, thus further enhancing the security and the accuracy of the verification.

20 According to the example user identity verification method, first multi-tuple data made up of a user communication number and a temporary communication number may be generated according to an identity verification request sent from a client terminal, and the temporary communication number may be returned to the client terminal. In response to a call request for the temporary communication number initiated by a user, verification may
25 be performed based on whether second multi-tuple data made up of a user communication number and a temporary communication number which correspond to the call request matches with the first multi-tuple data. The method can initiate a call to a temporary communication number allocated by a verification server from a user communication number, so that identity verification can be performed for the user through a voice channel
30 between the user and the verification server. Therefore, security and reliability of the

identity verification can be improved, and a waiting time of the user is reduced, thus enhancing user experience.

In order to implement the foregoing embodiments, the present disclosure provides a verification server.

5 FIG. 2 is a schematic structural diagram of a verification server 200 according to an embodiment of the present disclosure.

As shown in FIG. 2, the verification server 200 may include one or more processors 202, an input/output (I/O) interface 204, a network interface 206 and memory 208.

10 The memory 208 may include a form of computer-readable media, e.g., a non-permanent storage device, random-access memory (RAM) and/or a nonvolatile internal storage, such as read-only memory (ROM) or flash RAM. The memory 208 is an example of computer-readable media.

15 The computer-readable media may include a permanent or non-permanent type, a removable or non-removable media, which may achieve storage of information using any method or technology. The information may include a computer-readable instruction, a data structure, a program module or other data. Examples of computer storage media include, but not limited to, phase-change memory (PRAM), static random access memory (SRAM), dynamic random access memory (DRAM), other types of random-access memory (RAM), read-only memory (ROM), electronically erasable programmable read-only memory (EEPROM), quick flash memory or other internal storage technology, compact disk read-only memory (CD-ROM), digital versatile disc (DVD) or other optical storage, magnetic cassette tape, magnetic disk storage or other magnetic storage devices, or any other non-transmission media, which may be used to store information that may be accessed by a computing device. As defined herein, the computer-readable media does not include
20 transitory media, such as modulated data signals and carrier waves.
25

30 In implementations, the memory 208 may include program modules 210 and program data 212. The program modules 210 may include a verification request receiving module 214, a determination module 216, a generation module 218, a first returning module 220, a call request receiving module 222, a verification module 224, and a second returning module 226.

In implementations, the verification request receiving module 214 may receive an identity verification request sent by a user through a client terminal.

When a user registers or logs in through a client terminal, an identity of the user needs to be verified. At this point, the user may send an identity verification request to a verification server 200 through the client terminal. In implementations, the client terminal may provide a registration or login interface, with the interface including a registration or login button. After the user clicks the button, the client terminal sends an identity verification request to the verification request receiving module 214.

In implementations, the client terminal may include a WEB page terminal, an APP terminal, a WAP page terminal or the like.

The determination module 216 may determine a user communication number according to the identity verification request.

In implementations, if the identity verification request is sent when the user registers a new account, the identity verification request further includes a user communication number. The user communication number is inputted when the user submits the identity verification request. In implementations, when the user registers a new account and identity verification thereof needs to be performed, the client terminal may provide an input box or an input region in a registration interface and instruct the user to input a user communication number. After the user inputs the communication number and clicks a registration button, the client terminal may send the identity verification request including the user communication number to the verification server 200. After the verification request receiving module 214 receives the identity verification request, the determination module 216 may determine a user communication number from the identity verification request.

In implementations, if the user is a registered user, the identity verification request may include account information of the registered user. Determining the user communication number according to the identity verification request may include determining a corresponding user communication number according to the account information of the registered user. In implementations, since the user may have submitted a user communication number corresponding to registered account information (a username, a

user ID and the like) during registration, the verification server 200 may store the user communication number and the registered account information correspondingly in a user information library. Therefore, when the user uses a specific service (for example, login, payment, transfer, etc.) that needs to verify an identity of the user, the determination
5 module 216 may determine corresponding account information of the user according to the identity verification request and search for a corresponding user communication number from the stored user information library.

The generation module 218 may generate a corresponding temporary communication number for the user communication number, and record the user communication number
10 and the temporary communication number as first multi-tuple data.

After the determination module 216 determines the user communication number, the generation module 218 may generate a corresponding temporary communication number for the user communication number. The temporary communication number may include a mobile phone number, a special service number, a landline telephone number, a network
15 telephone number, etc. The verification server 200 may apply for communication numbers in one or more segments from service providers (for example, mobile communication service providers such as Mobile, Unicom, Telecom, etc.) in advance. After the user communication number is determined, the generation module 218 may randomly select a communication number from the applied communication numbers as a corresponding temporary
20 communication number.

In implementations, after a communication number is selected as a temporary communication number, this communication number cannot be used as a temporary communication number corresponding to the user communication number in other verification processes any more. In additional implementations, a temporary communication
25 number may also be allocated according to another allocation rule. For example, a same temporary communication number may be allocated to user communication numbers for identity verification requests initiated from a same client terminal having an identifier according to the identifier of the client terminal. The present disclosure does not impose any limitation on details of a rule of allocating a verification number.

In implementations, the first multi-tuple data may include two-tuple data including the user communication number and the temporary communication number.

In implementations, the identity verification request may further include a client terminal identifier. The generation module 218 may generate the first multi-tuple data based on the user communication number, the client terminal identifier and the temporary communication number.

For example, three-tuple data may be in a form of AX or AXB, where A is a user communication number, X is a temporary communication number, and B is a client terminal identifier.

It should be understood that the temporary communication number is allocated for the user communication number, and thus only the user communication number can initiate a call to the temporary communication number.

The first returning module 220 may return the temporary communication number to the client terminal.

In implementations of the present disclosure, the identity verification request may further include a client terminal identifier. The first returning module 220 may return the temporary communication number to a client terminal corresponding to the client terminal identifier. Thus, the temporary communication number can be accurately returned to the corresponding client terminal, thereby improving the accuracy of the verification.

The call request receiving module 222 may receive a call request to the temporary communication number initiated by the user.

In implementations, after the client terminal receives the temporary communication number, the temporary communication number may be displayed to the user, and the user may prompted to initiate a call to the temporary communication number. After receiving the prompt, the user may initiate a call to the temporary communication number via a mobile telephone, a landline telephone or an application program having a voice communication function. At this point, the call request receiving module 222 may receive the call request.

In implementations, the client terminal may display the temporary communication number in a form of a two-dimensional code. The user may use a mobile terminal to initiate a call to the temporary communication number by scanning and parsing the

two-dimensional code. Apparently, the client terminal may also display the temporary communication number in another manner, which is not limited in the present disclosure. For example, the temporary communication number may be displayed via a bar code, a pattern, etc.

5 The verification module 224 may determine a respective user communication number and a respective temporary communication number corresponding to the call request as second multi-tuple data, and verify whether the first multi-tuple data matches with the second multi-tuple data.

10 After the call request receiving module 222 receives the call request initiated by the user, the verification module 224 may determine a respective user communication number (a communication number of a calling party) and a respective temporary communication number (a communication number of a called party), and generate second multi-tuple data. Verification may then be performed as to whether the recorded first multi-tuple data matches with the second multi-tuple data.

15 If the first multi-tuple data does not match with the second multi-tuple data, the verification module 224 determines that the verification of the user fails. Thus, an identity of the user can be verified based on whether the received call request is an identity verification request using a call from the corresponding user communication number to the temporary communication number. Compared with the method of performing verification using a short
20 message verification code, a user communication number is extremely difficult to be counterfeited in this method of initiating a call through a user communication number, and thus the security of verification is higher.

25 If the first multi-tuple data matches with the second multi-tuple data, the verification module 224 may further play a prompt audio message to the user, receive information inputted by the user according to the prompt audio message, and verify whether the inputted information is consistent with content of the prompt audio message. If the inputted information is consistent with the content of the prompt audio message, the verification succeeds. Otherwise, the verification fails. In implementations, the prompt audio message instructs the user to input a specified key, numerical string or character string.

Furthermore, the verification module 224 may select content of a prompt audio message to be played according to a security level of the verification. For example, if the security level of the verification is a low level, the verification module 224 may play a default prompt audio message, and the verification succeeds after the default prompt audio message is played completely. If the security level of the verification is a middle level, the verification module 224 may instruct the user to press a corresponding key. If the security level of the verification is a high level, the verification module 224 may instruct the user to input a corresponding numerical string or character string. After the user inputs the numerical string or character string, verification is performed to determine whether information inputted by the user is consistent with the content of the prompt audio message. If affirmative, the verification is passed. Otherwise, the verification fails.

A security level may be set by the verification server according to an identity of a user corresponding to an identity verification request. For example, if a state associated with the user is normal, a low-level verification may be selected. If the state associated with the user is abnormal (e.g., a remote login, etc.), a mid-level verification may be selected. If the user is flagged, a high-level verification may be selected.

In implementations, the verification module 224 may also carry out verification according to the time at which a user initiates a call request. In implementations, the verification module 224 may further verify whether a time difference between a time of initiating the call request and a time of generating the first multi-tuple data is less than a preset time, and determine that the user verification fails if the time difference is greater than or equal to the preset time, or send a prompt audio message to perform additional verification otherwise.

The second returning module 226 may return a verification result to the client terminal.

In implementations, the second returning module 226 may return a verification result to a corresponding client terminal according to the client terminal identifier in the identity verification request. Thus, the verification result can be accurately returned to the corresponding client terminal, thereby improving the accuracy of the verification.

The example verification server 200 may generate first multi-tuple data that is made up of a user communication number and a temporary communication number according to an

identity verification request sent from a client terminal, and return the temporary communication number to the client terminal. In response to a call request for the temporary communication number initiated by a user, verification may be performed based on whether second multi-tuple data made up of a user communication number and a temporary communication number which correspond to the call request matches with the first multi-tuple data. The method can initiate a call to a temporary communication number allocated by a verification server from a user communication number, so that identity verification can be performed for the user through a voice channel between the user and the verification server 200. Therefore, security and reliability of the identity verification can be improved, and a waiting time of the user is reduced, thus enhancing user experience.

It should be understood that, in implementations, the verification server 200 may be an integral entity, or may be divided into a client terminal server part corresponding to the client terminal and a support verification part for allocating a temporary user number. In implementations, using the embodiment shown in FIG. 2 as an example, the verification request receiving module 214, the determination module 216 and the first returning module 220 may belong to the client terminal server part, whereas the generation module 218, the call request receiving module 222, the verification module 224 and the second returning module 226 may belong to the support verification part.

In implementations, an example process of user identity verification according to an embodiment of the present disclosure is described below with reference to FIG. 3. FIG. 3 is a sequence diagram of a process 300 of user identity verification according to an embodiment of the present disclosure. In implementations, the verification server 200 may be divided into a client terminal server part corresponding to a client terminal and a support verification part (i.e., a support server) for allocating a temporary user number.

As shown in FIG. 3, the client terminal sends 302 an identity verification request to the client terminal server for a user. In response to receiving the identity verification request, the client terminal server sends 304 a support request to the support server to request three-tuple data (i.e., first multi-tuple data). In response to receiving the support request, the support server allocates 306 a temporary communication number for a user communication number corresponding to the support request, and records 308 three-tuple

data which is made up of the user communication number, the temporary communication number and a client terminal identifier. The three-tuple data may have a particular period of validity (i.e., the aforementioned preset time), and the three-tuple data is invalid after the period of validity expires. The support server returns 310 the three-tuple data to the client terminal server, and the client terminal server sends 312 the temporary communication number in the three-tuple data to the client terminal. The client terminal displays 314 the temporary communication number, and prompts 316 the user to initiate a call request to the temporary communication number within the period of validity. The user may use his/her own user communication number to initiate 318 a call request to the displayed temporary communication number, with the call request reaching the support server to establish a connection with the support server through voice. The support server interacts 320 with the user differently according to a security level selected by the client terminal server (e.g., plays a default prompt audio message, instructs the user to press a designated key, and/or instructs the user to input a specific sequence of numbers and/or characters, etc.), and returns 322 data to the client terminal server during the verification process. The client terminal server determines 324 a verification result according to the returned data and returns 326 the verification result to the client terminal. In the foregoing process, the process 300 proceeds to an identity verification process if dialing to the temporary communication number is performed via the user communication number in the three-tuple data within the preset time, i.e., a corresponding identity verification process is performed according to the security level selected by the client terminal server. Otherwise, the verification fails. The support server may return data of interaction between the support server and the user (for example, a prompt audio message played by the support server, an operation fed back by the user, etc.) in the identity verification process 300 to the client terminal server. The client terminal server may determine whether the verification is passed according to whether the operation fed back by the user is consistent with the content of the prompt audio message, and send a verification result to the client terminal to notify the user.

In implementations, since the user actively dials the temporary communication number of this identity verification, a success rate of verification is greatly enhanced as compared to

the existing method of performing verification using a short message verification code. The time period during which the user is waiting anxiously is reduced, thus improving user experience. In addition, as the degree of difficulty of counterfeiting a user communication number to make a call is very high, the security of the verification process in the present disclosure is greatly enhanced as compared to the existing verification method.

In order to achieve the foregoing embodiments, the present disclosure further provides a user identity verification system.

FIG. 4 is a schematic structural diagram of a user identity verification system 400 according to an embodiment of the present disclosure.

As shown in FIG. 4, the user identity verification system 400 may include a client terminal 402 and a verification server 404.

The client terminal 402 may include a WEB page terminal, an APP terminal or a WAP page terminal.

The verification server 404 may include the verification server of any embodiment in the present disclosure.

According to the example user identity verification system of the present disclosure, the verification server may generate first multi-tuple data made up of a user communication number and a temporary communication number according to an identity verification request sent by a client terminal, and return the temporary communication number to the client terminal. In response to initiating a call request for the temporary communication number initiated by a user, verification may be performed whether second multi-tuple data made up of a user communication number and a temporary communication number which correspond to the call request matches with the first multi-tuple data. The method can initiate a call to a temporary communication number allocated by the verification server from a user communication number, so that identity verification can be performed for the user through a voice channel between the user and the verification server. Therefore, security and reliability of the identity verification can be improved, and a waiting time of the user is reduced, thus enhancing user experience.

In the description of the present disclosure, it should be understood that directional or positional relationships indicated by terms such as "center", "longitudinal", "transversal",

"length", "width", "thickness", "upper", "lower", "front", "back", "left", "right", "vertical", "horizontal", "top", "bottom", "inner", "outer", "clockwise", "counterclockwise", "axial", "radial", "circumferential", etc., are directional or positional relationships as shown according to the accompanying drawings. These terms are merely intended to facilitate
5 describing the present disclosure and simplify the description, rather than indicating or implying that an apparatus or element indicated thereby needs to have a particular direction, and to be constructed and operated in a particular direction. Thus, they cannot be construed as limitations to the present disclosure.

In addition, terms such as "first" and "second" are merely used for the purpose of
10 description, but should not be understood as indicating or implying a relative importance or implicitly indicating a number of technical features indicated thereby. Thus, features defined with "first" and "second" may explicitly or implicitly include at least one of these features. In the description of the present disclosure, "multiple" means at least two, for example, two, three, etc., unless specifically defined otherwise.

In the present disclosure, unless specifically defined otherwise, terms such as
15 "installed", "connected", "linked", "fixed", etc., should be understood in a broad sense. These terms may be a fixed connection, a removable connection or an integral entity, for example. Additionally or alternatively, these terms may be a mechanical connection or an electrical connection; a direct connection or a connection through an intermediate medium;
20 an internal communication of two elements or an interactive relationship between two elements, unless specifically defined otherwise. One of ordinary skill in the art can understand the specific meaning of the above terms in the present disclosure according to specific situations.

In the present disclosure, unless specifically defined otherwise, a first feature being at
25 an "upper" or "lower" position of a second feature may indicate that the first feature and the second feature are in direct contact, or the first feature and the second feature are in indirect contact through an intermediate medium. Moreover, a first feature being "above", "over" and "on" a second feature may indicate that the first feature is directly over or obliquely over the second feature, or may merely indicate that a horizontal height of the first
30 feature is higher than that of the second feature. A first feature being "below", "beneath"

and "under" a second feature may indicate that the first feature is directly beneath or obliquely beneath the second feature, or may merely indicate that a horizontal height of the first feature is less than that of the second feature.

5 In the description of the disclosure, descriptions of reference terms such as "one embodiment", "some embodiments", "an example", "a specific example" or "some examples", etc., mean that specific features, structures, materials or characteristics described in combination with the embodiment/embodiments or example/examples are included in at least one embodiment or example of the present disclosure. In the disclosure, schematic expressions of the terms are not necessarily directed to the same embodiment or
10 example. Moreover, the described features, structures, materials or characteristics can be combined in a suitable manner in any one or more embodiments or examples. In addition, in a situation in which no mutual conflict exists, one skilled in the art can unite and combine different embodiments or examples and features of different embodiments or examples described in the specification.

15 Although the embodiments of the present disclosure have been shown and described above, it should be understood that the above embodiments are exemplary and cannot be construed as limitation to the present disclosure. One of ordinary skill in the art can make changes, modifications, replacements and alternations to the above embodiments within the scope of the present disclosure.

Claims

1. A method implemented by one or more computing devices, the method comprising:
receiving an identity verification request sent from a first client terminal of a user;
determining a first communication number according to the identity verification

5 request;

generating a temporary communication number for the first communication number;

recording the first communication number and the temporary communication number
as first data; and

10 returning the temporary communication number to the first client terminal, a call to
the temporary communication number initiating an identity verification of the user
associated with the temporary communication number.

2. The method of claim 1, further comprising:

15 receiving a call request to the temporary communication number from a second client
terminal;

determining a second communication number corresponding to the call request and
the temporary communication number as second data;

verifying whether the first data matches with the second data; and

returning a verification result.

20

3. The method of claim 2, further comprising:

determining whether a time difference between a time at which the call request is
received and a time at which the first data is generated is less than a preset time; and

25 determining that the identity verification of the user fails in response to determining
that the time difference is greater than or equal to the preset time.

4. The method of claim 2, further comprising determining that the identity verification
of the user fails in response to determining that the first data does not match with the
second data.

30

5. The method of claim 2, wherein in response to determining that the first data matches with the second data, the method further comprises:

providing a prompt audio message to the second client terminal for playing to the user;

receiving information inputted by the user according to the prompt audio message; and

5 verifying whether the inputted information is consistent with content of the prompt audio message.

6. The method of claim 5, wherein the prompt audio message instructs the user to input a particular key, a particular numerical string or a particular character string.

10

7. The method of claim 1, wherein the identity verification request is received in response to an event of a registration of a new account by the user, and wherein the identity verification request includes the first communication number that is inputted by the user.

15 8. The method of claim 1, wherein the identity verification request comprises account information of the user, and determining the first communication number comprises determining a corresponding communication number according to the account information of the user.

20 9. The method of claim 1, further comprising causing the client terminal to display the temporary communication number via a two-dimensional code, the two-dimensional code enabling the call request to the temporary communication number upon being scanned.

10. A server comprising:

25 one or more processors;

memory;

a verification request receiving module stored in the memory and executable by the one or more processors to receive an identity verification request from a first client terminal of a user;

a determination module in the memory and executable by the one or more processors to determine a first communication number according to the identity verification request;

a generation module in the memory and executable by the one or more processors to generate a temporary communication number for the first communication number, and
5 record the first communication number and the temporary communication number as first data;

a first returning module in the memory and executable by the one or more processors to return the temporary communication number to the first client terminal;

a call request receiving module in the memory and executable by the one or more
10 processors to receive a call request to the temporary communication number from a second client terminal;

a verification module in the memory and executable by the one or more processors to determine a second communication number corresponding to the call request and the temporary communication number as second data, and verify whether the first data
15 matches with the second data; and

a second returning module in the memory and executable by the one or more processors to return a verification result to the client terminal, the verification result depending at least in part on whether the first data matches with the second data.

20 11. The server of claim 10, wherein the verification request receiving module receives the identity verification request in response to an event of a registration of a new account by the user, and wherein the identity verification request includes the first communication number that is inputted by the user during the registration.

25 12. The server of claim 10, wherein the identity verification request comprises account information of the user, and the determination module determines the first communication number based at least in part on the account information of the user.

30 13. The server of claim 10, wherein the verification module further determines whether a time difference between a time at which the call request is received and a time at which

the first data is generated is less than a preset time, and determines that an identity verification of the user fails in response to determining that the time difference is greater than or equal to the preset time.

5 14. The server of claim 10, wherein the verification module determines that an identity verification of the user fails in response to determining that the first data does not match with the second data.

10 15. The server of claim 10, wherein in response to determining that the first data matches with the second data, the verification module further causes the second client terminal to play a prompt audio message to the user, receives information inputted by the user according to the prompt audio message from the second client terminal, and determines whether the inputted information is consistent with content of the prompt audio message.

15 16. The server of claim 15, wherein the prompt audio message instructs the user to input a specified key, a specified numerical string or a specified character string.

20 17. The server of claim 10, wherein the first returning module returns the temporary communication number in a form of a two-dimensional code, the two-dimensional code initiating the call request to the temporary communication number upon being scanned.

25 18. One or more computer-readable media storing executable instructions that, when executed by one or more processors, cause the one or more processors to perform acts comprising:

receiving an identity verification request sent from a first client terminal of a user;

determining a first communication number according to the identity verification request;

generating a temporary communication number for the first communication number;

recording the first communication number and the temporary communication number as first data; and

returning the temporary communication number to the first client terminal, a call to the temporary communication number initiating an identity verification of the user
5 associated with the temporary communication number.

19. The one or more computer-readable media of claim 18, the acts further comprising:
receiving a call request to the temporary communication number from a second client terminal;

10 determining a second communication number corresponding to the call request and the temporary communication number as second data;
verifying whether the first data matches with the second data; and
returning a verification result to the second client terminal.

15 20. The one or more computer-readable media of claim 19, the acts further comprising:
determining whether a time difference between a time at which the call request is received and a time at which the first data is generated is less than a preset time; and
determining that the identity verification of the user fails in response to determining that the time difference is greater than or equal to the preset time.

20

1/4

100

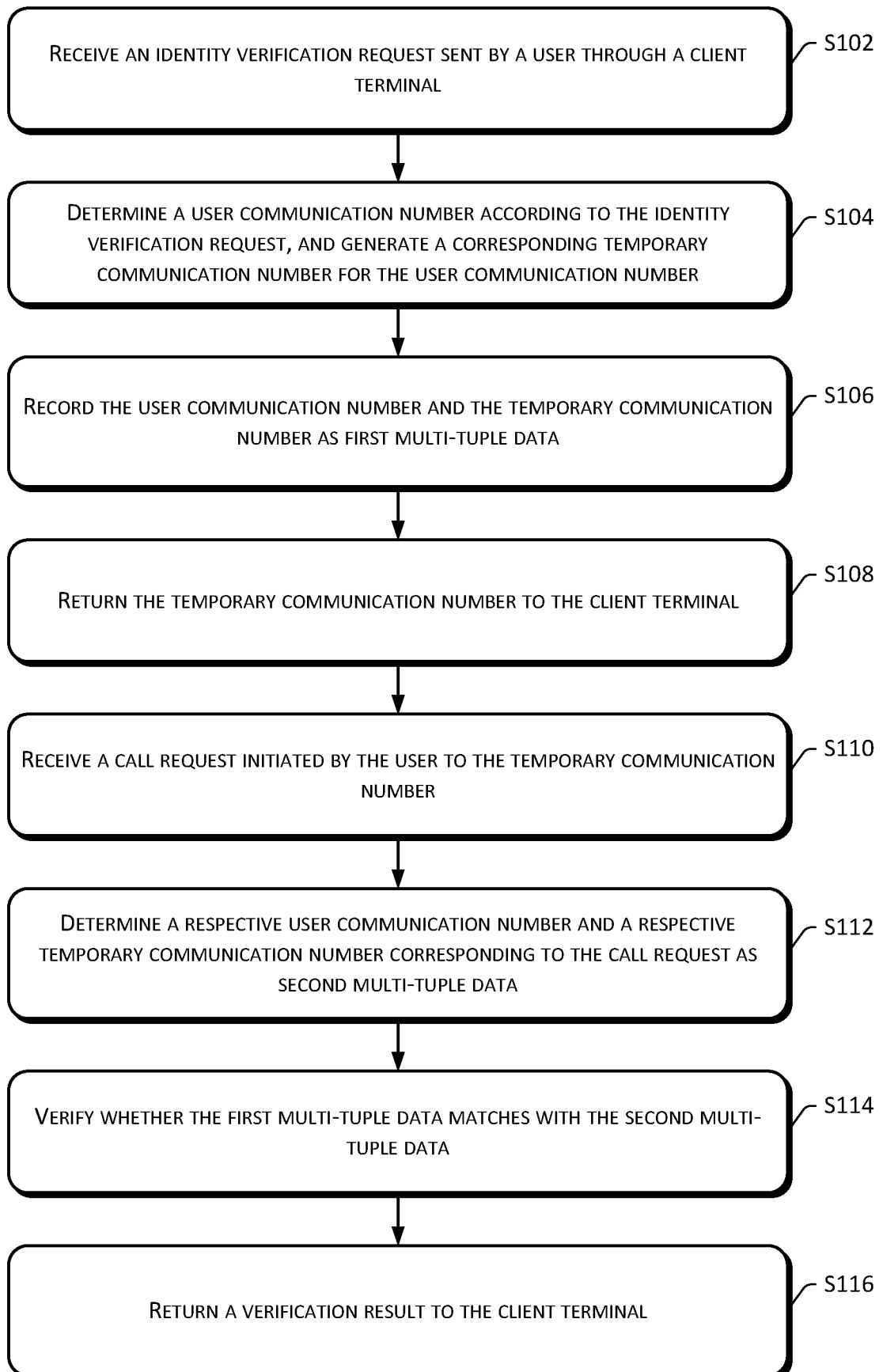


FIG. 1

2/4

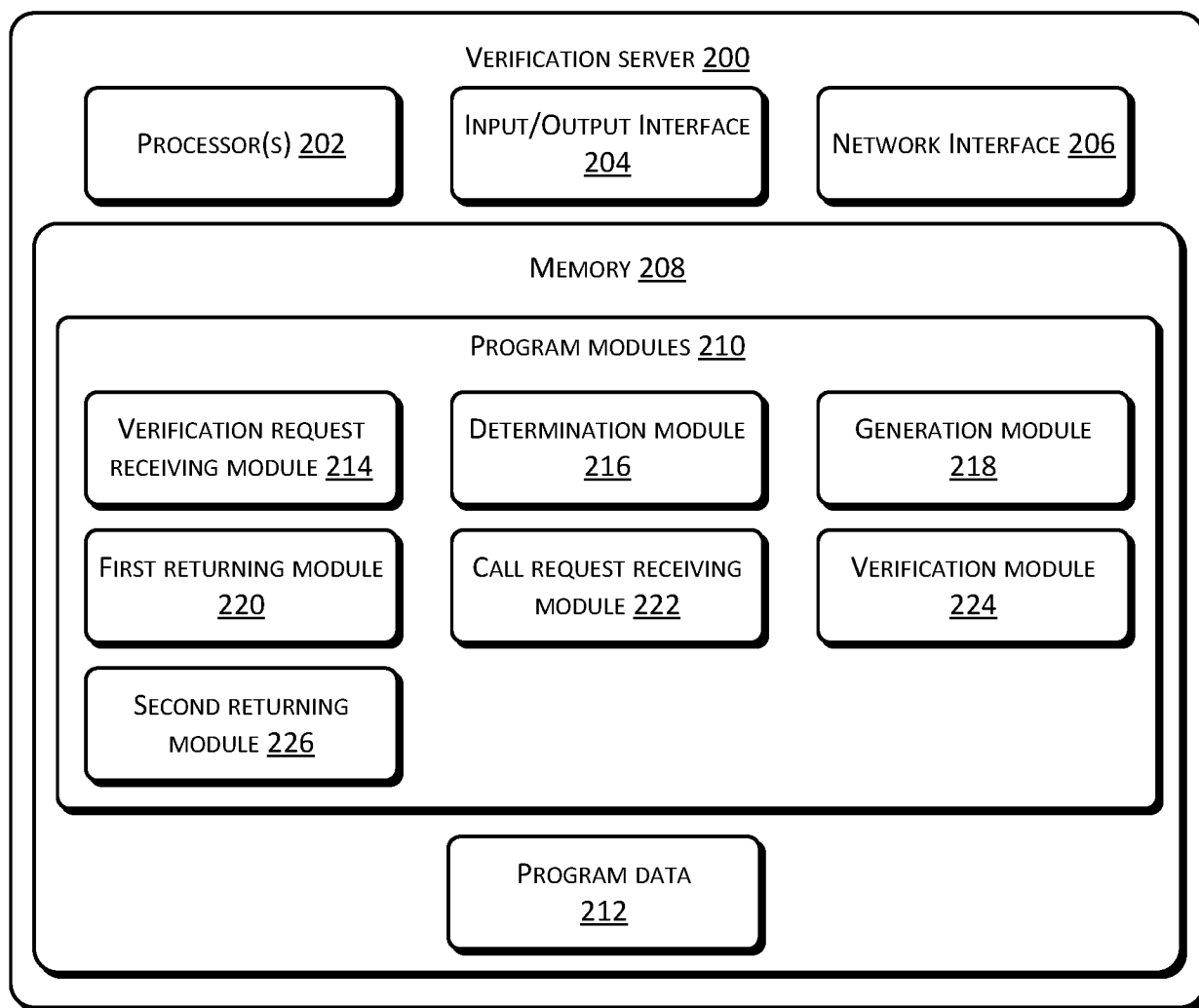


FIG. 2

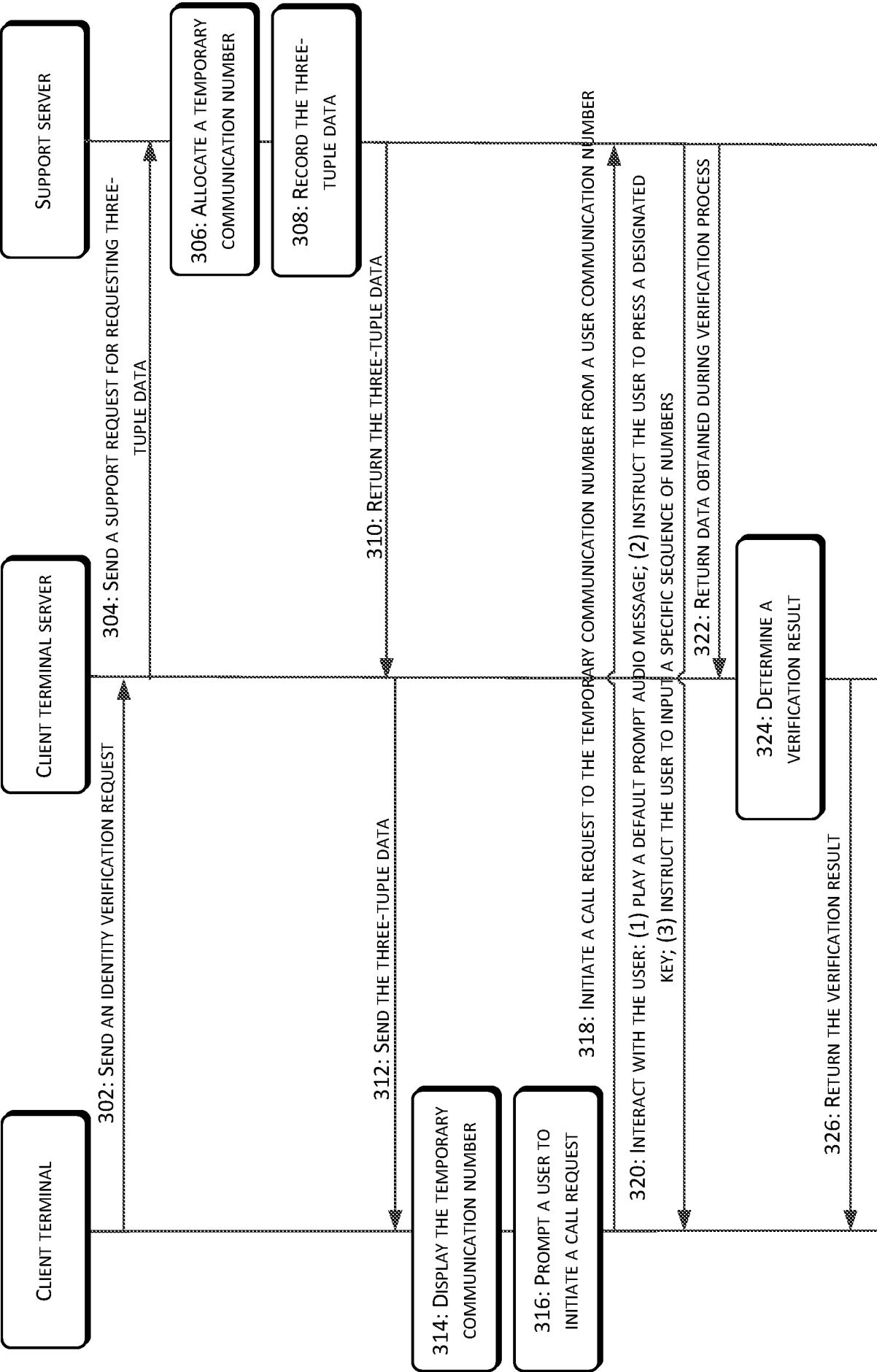


FIG. 3

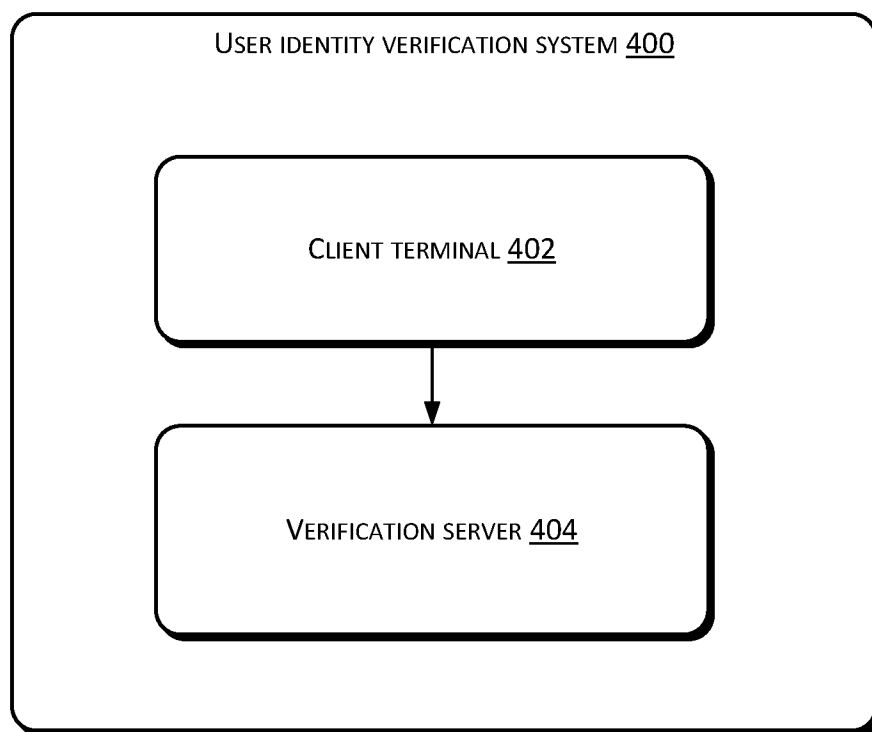


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2016/044202

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 20/40 (2016.01)

CPC - G06Q 20/40, G06Q 20/4014 (2016.08)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC - G06F 7/04; G06F 21/60; G06K 9/00; G06K 9/62; G06Q 20/10; G06Q 20/20; G06Q 20/32; G06Q 20/38; G06Q 20/40

CPC - ; G06Q 20/3255; G06Q 20/382; G06Q 20/385; G06Q 20/40; G06Q 20/401; G06Q 20/4014; G06Q 20/40145; G06Q 20/425

G06K 9/00892; G06K 9/6211; G06K 9/6293; G06K 9/685; G06Q 20/10; G06Q 20/1085; G06Q 20/202; G06Q 20/206

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

USPC: 379/142.170; 380/270; 455/410; 705/44; 726/7; 726/14 (keyword delimited)

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

Orbit, Google Patents, Google Scholar, Google

Search terms used: user, identity, verification, system, server, computer, challenge, response, phone, telephone, number, communication, temporary, audio, message, barcode, QR code

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/0322612 A1 (PETRACK et al) 05 December 2013 (05.12.2013) entire document	1-4, 8, 10, 12-14, 18-20
---		---
Y		5-7, 9, 11, 15-17
Y	US 2014/0010357 A1 (AVAYA INC.) 09 January 2014 (09.01.2014) entire document	5, 6, 15, 16
Y	US 2015/0206126 A1 (ROCKHARD) 23 July 2015 (23.07.2015) entire document	7, 9, 11, 17
P,A	US 2015/0350224 A1 (ALIBABA GROUP HOLDING LIMITED) 03 December 2015 (03.12.2015) entire document	1-20
P,A	US 2015/0347857 A1 (ALIBABA GROUP HOLDING LIMITED) 03 December 2015 (03.12.2015) entire document	1-20
A	US 2011/0016050 A1 (EVANS) 20 January 2011 (20.01.2011) entire document	1-20
A	US 2009/0305667 A1 (SCHULTZ) 10 December 2009 (10.12.2009) entire document	1-20
A	US 2013/0291089 A1 (WANG et al) 31 October 2013 (31.10.2013) entire document	1-20



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

26 September 2016

Date of mailing of the international search report

07 OCT 2016

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774