

OFFLINE USER IDENTIFICATION METHODS AND APPARATUSES

TECHNICAL FIELD

[0001] Embodiments of this specification generally relate to the field of user
5 identification, and in particular, to offline user identification methods and apparatuses.

BACKGROUND

[0002] Offline user identification refers to performing identification on a user in an
offline venue by using a biometric feature such as a face. Offline user identification has
been applied to many offline scenarios, such as bank verification, hotel check-in, and
10 offline shopping. In these scenarios, most implementation solutions realize user
identification by using faces and are based primarily on visual features and computer
vision models. However, in the offline scenarios, satisfactory accuracy cannot be
obtained in real-world scenarios only by using computer vision algorithms due to
relatively large changes in postures, illumination, and occlusion. In addition, when a
15 scale of candidate users reaches a billion level, the computer vision algorithms further
need to have very high efficiency and accuracy.

SUMMARY

[0003] In view of the above-mentioned description, embodiments of this specification
provide offline user identification methods and apparatuses. By using the offline user
20 identification methods and apparatuses, modeling is performed on a biometric feature
of a to-be-identified user and graph information in a user behavior relationship
heterogeneous graph to obtain a target user account, a venue, and a biometric feature
embedding representation, and user identification is performed based on the target user
account, the venue, and the biometric feature embedding representation. User offline-
25 habit/behavior information mined from the user behavior relationship heterogeneous
graph can be introduced during user identification, thereby improving accuracy of

offline user identification.

[0004] According to an aspect of the embodiments of this specification, an offline user identification method is provided, including: obtaining biometric feature data of a to-be-identified user at a first venue; retrieving a target user account from a candidate-user-account database based on the obtained biometric feature data; and determining, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user to perform user identification, where the user behavior relationship heterogeneous graph is constructed based on historical venue access data of user accounts.

[0005] Optionally, in an example of the above-mentioned aspect, the determining, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user can include the following: predicting the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account.

[0006] Optionally, in an example of the above-mentioned aspect, the predicting the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account can include the following: performing modeling on the target user account and the first venue by using a first machine learning model based on the user behavior relationship heterogeneous graph to obtain embedding representations of the target user account and the first venue in various heterogeneous relationships; performing modeling on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account by using a second machine learning model to obtain a biometric feature embedding representation used to reflect a similarity between the biometric feature data of the to-be-identified user and the biometric feature data of the target user account; and providing the embedding representations of the target user account and the first venue

in the various heterogeneous relationships and the biometric feature embedding representation for an aggregation layer to predict matchability between the target user account and both of the first venue and the biometric feature data of the to-be-identified user.

5 [0007] Optionally, in an example of the above-mentioned aspect, the first machine learning model includes a graph neural network, and the second machine learning model includes a multilayer perceptron model.

[0008] Optionally, in an example of the above-mentioned aspect, the graph neural network includes an attention mechanism-based graph neural network.

10 [0009] Optionally, in an example of the above-mentioned aspect, the aggregation layer includes an attention mechanism-based aggregation layer.

[0010] Optionally, in an example of the above-mentioned aspect, the first machine learning model, the second machine learning model, and the aggregation layer are trained integrally as one model.

15 [0011] Optionally, in an example of the above-mentioned aspect, a total loss function for training of the model includes a cross-entropy loss function.

[0012] Optionally, in an example of the above-mentioned aspect, a total loss function for training of the model includes a loss function for introducing L2 regularization to a model parameter.

20 [0013] Optionally, in an example of the above-mentioned aspect, the determining, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user can include the following: determining matchability
25 between the target user account and the first venue based on the user behavior relationship heterogeneous graph; determining matchability between the target user account and the biometric feature data of the to-be-identified user based on the biometric feature data of the target user account and the biometric feature data of the to-be-identified user; and determining, in response to that the target user account
30 matches both the first venue and the biometric feature data of the to-be-identified user, that the user identification succeeds.

[0014] Optionally, in an example of the above-mentioned aspect, the candidate-user-account database includes a candidate-user-account local database and a candidate-user-account global database. The retrieving a target user account from a candidate-

user-account database based on the obtained biometric feature data can include the following: retrieving the target user account from a corresponding candidate-user-account local database of the first venue based on the obtained biometric feature data; and retrieving the target user account from the candidate-user-account global database
5 based on the obtained biometric feature data in response to a failure in retrieving a matched target user account from the candidate-user-account local database.

[0015] Optionally, in an example of the above-mentioned aspect, each candidate-user-account local database includes a candidate-user-account database constructed based on historical access data at a corresponding venue and historical access data at another
10 venue within a range of a given distance from the corresponding venue.

[0016] Optionally, in an example of the above-mentioned aspect, the biometric feature data includes visual feature data of face information.

[0017] According to some embodiments of this specification, an offline user identification apparatus is provided, including: a biometric feature data acquisition unit,
15 configured to obtain biometric feature data of a to-be-identified user at a first venue; a target user account retrieval unit, configured to retrieve a target user account from a candidate-user-account database based on the obtained biometric feature data; and a user identification unit, configured to determine, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and
20 biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user to perform user identification, where the user behavior relationship heterogeneous graph is constructed based on historical venue access data of user accounts.

[0018] Optionally, in an example of the above-mentioned aspect, the user
25 identification unit predicts the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account.

[0019] Optionally, in an example of the above-mentioned aspect, the user
30 identification unit includes the following: a first embedding representation generation module, configured to perform modeling on the target user account and the first venue by using a first machine learning model based on the user behavior relationship heterogeneous graph to obtain embedding representations of the target user account and

the first venue in various heterogeneous relationships; a second embedding representation generation module, configured to perform modeling on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account by using a second machine learning model to obtain a biometric feature embedding representation used to reflect a similarity between the biometric feature data of the to-be-identified user and the biometric feature data of the target user account; and a prediction module, configured to provide the embedding representations of the target user account and the first venue in the various heterogeneous relationships and the biometric feature embedding representation for an aggregation layer to predict matchability between the target user account and both of the first venue and the biometric feature data of the to-be-identified user.

[0020] Optionally, in an example of the above-mentioned aspect, the user identification unit includes the following: a first matching module, configured to determine matchability between the target user account and the first venue based on the user behavior relationship heterogeneous graph; a second matching module, configured to determine matchability between the target user account and the biometric feature data of the to-be-identified user based on the biometric feature data of the target user account and the biometric feature data of the to-be-identified user; and a user identification module, configured to determine, in response to that the target user account matches both the first venue and the biometric feature data of the to-be-identified user, that the user identification succeeds.

[0021] Optionally, in an example of the above-mentioned aspect, the candidate-user-account database includes a candidate-user-account local database and a candidate-user-account global database. The target user account retrieval unit includes the following: a local retrieval module, configured to retrieve the target user account from a corresponding candidate-user-account local database of the first venue based on the obtained biometric feature data; and a global retrieval module, configured to retrieve the target user account from the candidate-user-account global database based on the obtained biometric feature data in response to a failure in retrieving a matched target user account from the candidate-user-account local database.

[0022] According to another aspect of the embodiments of this specification, an offline user identification apparatus is provided, including at least one processor, a storage coupled to the at least one processor, and a computer program stored in the storage, where the at least one processor executes the computer program to implement

the offline user identification method described above.

[0023] According to another aspect of the embodiments of this specification, a computer-readable storage medium is provided, where the computer-readable storage medium stores executable instructions, and when the instructions are executed, a processor is enabled to perform the offline user identification method described above.

[0024] According to another aspect of the embodiments of this specification, a computer program product is provided, including a computer program, where the computer program is executed by a processor to implement the offline user identification method described above.

10

BRIEF DESCRIPTION OF DRAWINGS

[0025] The essence and advantages of the content of this specification can be further understood by referring to the following accompanying drawings. In the accompanying drawings, similar components or features can have the same reference numerals.

[0026] FIG. 1 is an example schematic diagram of an offline user identification process;

[0027] FIG. 2 is an example flowchart of an offline user identification method according to some embodiments of this specification;

[0028] FIG. 3 is an example flowchart of a target user account retrieval process according to some embodiments of this specification;

[0029] FIG. 4 is an example schematic diagram of a user behavior relationship heterogeneous graph according to some embodiments of this specification;

[0030] FIG. 5 is an example flowchart of a user verification process according to some embodiments of this specification;

[0031] FIG. 6 is an example schematic diagram of a graph neural network according to some embodiments of this specification;

[0032] FIG. 7 is an example schematic diagram of a user verification process according to some embodiments of this specification;

[0033] FIG. 8 is another example flowchart of a user verification process according to some embodiments of this specification;

[0034] FIG. 9 is an example block diagram of an offline user identification apparatus according to some embodiments of this specification;

[0035] FIG. 10 is an example block diagram of a target user account retrieval unit

according to some embodiments of this specification;

[0036] FIG. 11 is an example block diagram of a user identification unit according to some embodiments of this specification;

[0037] FIG. 12 is another example block diagram of a user identification unit
5 according to some embodiments of this specification; and

[0038] FIG. 13 is an example schematic diagram of an offline user identification apparatus implemented based on a computer system according to some embodiments of this specification.

DESCRIPTION OF EMBODIMENTS

10 [0039] The subject matter described in this specification will now be discussed with reference to example implementations. It should be understood that these implementations are merely discussed to enable a person skilled in the art to better understand and implement the subject matter described in this specification, rather than limiting the protection scope described in the claims, applicability, or examples.

15 Functions and arrangements of elements under discussion can be changed without departing from the protection scope of the content of this specification. In the examples, various processes or components can be omitted, replaced, or added as needed. For example, described methods can be performed in an order different from a described order, and steps can be added, omitted, or combined. In addition, features described
20 relative to some examples can also be combined in other examples.

[0040] As used in this specification, the term "include" and its variant represent open terms, meaning "including but not limited to". The term "based on" means "at least partially based on". The terms "one embodiment" and "an embodiment" represent "at least one embodiment". The term "another embodiment" means "at least one other
25 embodiment". The terms "first", "second", and the like can refer to different objects or the same object. The following can include other definitions, whether explicit or implicit. Unless expressly stated in the context, the definition of one term is consistent throughout this specification.

[0041] User identification performed using biometric features (especially face
30 information) is increasingly applied to fields such as social insurance, finance, and commerce. User identification can be classified into two types: online one-to-one identification and offline one-to-many identification. Online identification usually

occurs on personal mobile devices, for example, during login to applications or online payment on mobile phones. In these scenarios, only one-to-one verification needs to be performed between biometric features and a login account of a user. However, offline identification scenarios are totally different and more complex.

5 **[0042]** FIG. 1 is an example schematic diagram of an offline user identification process 100.

10 **[0043]** As shown in FIG. 1, at 110, an offline identification system performs face scanning. The offline identification system is deployed in offline identification venues, and is provided with a face scanning device including a camera. When a user needs certain specific services at these offline identification venues, for example, when the user enters Universal Studios and purchases products, the face scanning device in the offline identification system scan a face of the user.

15 **[0044]** At 120, the offline identification system retrieves, from all accounts, an account whose face is similar to the scanned face.

20 **[0045]** After an account having a similar face is retrieved, at 130, a computer vision (CV) identification technology is used to perform verification between a user and the retrieved account based on visual features of the scanned face of the user and corresponding visual features of the retrieved account.

25 **[0046]** If a confidence degree of the verification is high, that is, a verification result at 130 is yes, verification processing is completed, and at 150, it is determined that the user identification succeeds, and a corresponding service is obtained. If a confidence degree of the verification is not high, that is, a verification result at 130 is no, further verification needs to be performed at 140, for example, a complete or partial identification card number or other personal information is entered.

30 **[0047]** If a verification result at 140 is yes, at 150, it is determined that the user identification succeeds. If a verification result at 140 is no, at 160, it is determined that the user identification fails.

35 **[0048]** If the above-mentioned user identification solution based on visual features is applied to industrial scenarios with offline user identification, because environments of the offline user identification scenarios are very complex, some similar users can be found for almost every user due to impact of a surrounding environment such as a posture, a makeup, dim light, or backlight, making it very difficult to perform face recognition based only on visual features. In addition, billions of candidate users exist in the offline user identification scenarios. The user identification solution needs to have

high efficiency for such a large data scale.

[0049] In view of the descriptions above, some embodiments of this specification provide an offline user identification solution. In an offline user identification scenario, users, venues, and different types of interaction thereof can form a heterogeneous graph.

5 A large amount of information about user offline habits and behaviors can be obtained by mining the heterogeneous graph. In the provided offline user identification solution, historical venue access information of users is mined to construct a heterogeneous relationship graph between the users and venues. During offline user identification, in addition to performing comparative verification based on biometric features, supplementary verification is further performed to determine, based on the constructed
10 heterogeneous relationship graph, whether a retrieved user account accesses a current venue. As such, user identification can be assisted based on offline behaviors and habits of the users, thereby improving accuracy of offline user identification.

[0050] The following describes offline user identification methods and offline user
15 identification apparatuses according to embodiments of this specification with reference to the accompanying drawings.

[0051] FIG. 2 is an example flowchart of an offline user identification method 200 according to some embodiments of this specification.

[0052] As shown in FIG. 2, at 210, biometric feature data of a to-be-identified user is
20 obtained at a first venue. For example, the obtained biometric feature can include but is not limited to a face feature, a voiceprint feature, a gesture feature, and a posture feature. For example, a corresponding biometric feature can be obtained by using a data collection device corresponding to the biometric feature. For example, a face scanning device, a sound capture device, a camera device, and the like can be used to collect a
25 face feature, a voiceprint feature, a gesture feature, a posture feature, and the like. The collected data can include image data and audio data. For the collected data, data preprocessing can be further performed to obtain expected biometric feature data.

[0053] For example, when the collected data is a face image, preprocessing such as an image quality check, face and key point detection, alignment, and clipping can be
30 performed. Then, the preprocessed image is input into a ResNet-based model to extract a visual feature of the face image. The extracted visual feature is represented as a 256-dimensional floating point vector. This vector can describe, for example, a 2D feature and a 3D feature of the face. All face images experience the data preprocessing to extract corresponding visual features, and the extracted visual features are used as the

biometric feature data of the user.

[0054] At 220, a target user account is retrieved from a candidate-user-account database based on the obtained biometric feature data.

[0055] The candidate-user-account database can be created based on historical venue
5 access data of users. A candidate-user-account global database can be created and maintained based on historical venue access data of all users. In some embodiments, the target user account can be retrieved from the candidate-user-account global database based on the obtained biometric feature data.

[0056] In some embodiments, in addition to creating and maintaining the candidate-
10 user-account global database, a candidate-user-account local database can be further created and maintained. The candidate-user-account local database is a venue-based database. In other words, a candidate-user-account local database is created and maintained for each venue. In the candidate-user-account local database for each venue, biometric feature data of users accessing the venue is recorded. Optionally, in an
15 example, the candidate-user-account local database for each venue can record only biometric feature data of users accessing the venue within a specified time period, for example, biometric feature data of users accessing the venue within one recent year. In addition, optionally, in another example, the candidate-user-account local database for each venue can include a candidate-user-account database constructed based on
20 historical access data at the venue and historical access data at another venue within a range of a given distance from the venue. In other words, the candidate-user-account local database for each venue can record biometric feature data of users accessing the venue and biometric feature data of users accessing the another venue within the range of the given distance from the venue.

[0057] FIG. 3 is an example flowchart of a target user account retrieval process 300
25 according to some embodiments of this specification. In the example of FIG. 3, a created and maintained candidate-user-account database includes a candidate-user-account local database and a candidate-user-account global database.

[0058] As shown in FIG. 3, at 310, a corresponding candidate-user-account local
30 database of a first venue is determined. Then, at 320, the target user account is retrieved from the corresponding candidate-user-account local database of the first venue based on the obtained biometric feature data, and at 330, it is determined whether a matched target user account is retrieved.

[0059] If a matched target user account is retrieved, the target user account is

determined at 360. If no matched target user account is retrieved, at 340, the target user account is retrieved from the candidate-user-account global database based on the obtained biometric feature data, and at 350, it is determined whether a matched target user account is retrieved.

5 **[0060]** If a matched target user account is retrieved, the target user account is determined at 360. If no matched target user account is retrieved, at 370, it is determined that the target user account is not retrieved. Therefore, it is determined that the user identification fails, and the user identification process ends.

10 **[0061]** Behavior tracks of users are usually local and stable. For example, the users usually go to venues near their houses or offices. In view of this, the candidate-user-account local database and the candidate-user-account global database are maintained, and the target user account is first retrieved from the candidate-user-account local database. Retrieval is performed from the candidate-user-account global database only when the target user account is not retrieved from the candidate-user-account local database. In other words, the target user account can be more quickly retrieved by using
15 a local-global retrieval mechanism, thereby improving retrieval efficiency of the target user account. In addition, the candidate-user-account local database is limited to a database created based on biometric feature data of users accessing the venue within a specified time period, so that the created candidate-user-account local database is time-
20 limited, and a size of the candidate-user-account local database can be reduced, thereby further improving the retrieval efficiency of the target user account. In addition, the candidate-user-account local database for each venue is limited to a database constructed based on historical access data at the venue and historical access data at another venue within a range of a given distance from the corresponding venue, so that
25 the created candidate-user-account local database has increasing spatial locality, thereby increasing a retrieval hit rate of the target user account. In addition, if the candidate-user-account local database for each venue is limited to based on a database constructed based on historical access data at the venue within a specified time period and historical access data at another venue within a range of a given distance from the
30 corresponding venue, the created candidate-user-account local database for each venue has increasing spatiotemporal locality, thereby increasing retrieval efficiency while ensuring a retrieval hit rate of the target user account.

[0062] Referring back to FIG. 2, after the target user account is retrieved as described above, matchability between the target user account, the first venue, and the biometric

feature data of the to-be-identified user is determined based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account to perform user identification.

[0063] Specifically, at 230, the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user is determined based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account. Then, at 240, it is determined whether the target user account, the first venue, and the biometric feature data of the to-be-identified user match. If they match, at 250, it is determined that the user identification succeeds. If they do not match, at 260, it is determined that the user identification fails.

[0064] The user behavior relationship heterogeneous graph can be constructed in advance based on historical venue access data of user accounts. For example, heterogeneous relationships between user accounts and accessed venues can be extracted from the historical venue access data of user accounts, and the user behavior relationship heterogeneous graph is created based on the user accounts, the venues, and the heterogeneous relationships. In this specification, a heterogeneous relationship is used to reflect a user behavior relationship of a user account in a venue, for example, a user performs code-scanning payment in a venue or a user performs face-scanning payment in a venue.

[0065] In this specification, the user behavior relationship heterogeneous graph can be represented as $G = \{V, E, X^{nd}, X^{eg}\}$, where V represents a node set, E represents an edge set, $X^{nd} \in R^{|V| \times d^{nd}}$ represents a node attribute matrix, and $X^{eg} \in R^{|E| \times d^{eg}}$ represents an edge attribute matrix. The user behavior relationship heterogeneous graph G can also be associated with a node type mapping function $\Phi: V \rightarrow A$ and an edge type mapping function $\Psi: E \rightarrow R$, where A represents a node type set and R represents an edge type set (a heterogeneous relationship type set). In this specification, A can be formed by, for example, users and venues, and R can include, for example, code-scanning payment and face-scanning payment.

[0066] FIG. 4 is an example schematic diagram of a user behavior relationship heterogeneous graph according to this specification. In the example of FIG. 4, an edge feature represents strength of a relationship between a user and a venue, and may be, for example, a payment frequency and a payment amount, which are key indicators for

representing the relationship between a user and a venue.

[0067] In an example, matchability between the target user account, the first venue, and a biometric feature data of the to-be-identified user can be predicted by using a machine learning model based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and a biometric feature data of the target user account.

[0068] FIG. 5 is an example flowchart of a user verification process 500 according to some embodiments of this specification. In the example of FIG. 5, the machine learning model can include a first machine learning model, a second machine learning model, and an aggregation layer.

[0069] At 510, modeling is performed on the target user account and the first venue by using the first machine learning model based on the user behavior relationship heterogeneous graph to obtain embedding representations of the target user account and the first venue in various heterogeneous relationships.

[0070] In an example, the first machine learning model can include a graph neural network. The graph neural network is a network used to extract node feature representations (embedding representations, embedding) from graph structured data. FIG. 6 is an example schematic diagram of a graph neural network according to some embodiments of this specification.

[0071] As shown in FIG. 6, the graph neural network can include multiple hidden layers, for example, a hidden layer 1 to a hidden layer N in FIG. 6. At each hidden layer, each graph node can receive and aggregate node embedding representations output by a previous hidden layer of neighbor nodes of the graph node. As such, a node embedding representation of the graph node at the hidden layer is generated, and the generated node embedding representation of the graph node is subsequently propagated to neighboring nodes at a next hidden layer. With such layer-by-layer propagation, node embedding representations obtained at the last layer are output as node embedding representations processed by the graph neural network. Here, the term "hidden layer" can also be referred to as a "message transfer layer".

[0072] When modeling is performed on the target user account and the first venue by using the first machine learning model based on the user behavior relationship heterogeneous graph, information from first-order venues and higher-order neighbors of user accounts can be propagated by using heterogeneous relationships so as to capture behavior preferences of the user accounts in offline scenarios. However, the

heterogeneous relationships have different characteristics. For example, face-scanning payment relationships are relatively scarce, but more directly indicate a face-scanning payment trend of a user. On the contrary, code-scanning payment relationships are relatively rich, and can provide more information about user expense habits. In consideration of different statistical attributes of the two types of relationships, modeling can be performed on information propagation in each type of heterogeneous relationship, and then embedding representations learned from different heterogeneous relationships can be aggregated.

[0073] For user embedding representations and venue embedding representations in each type of heterogeneous relationship, a sub-graph of a user or a venue can be constructed based on the heterogeneous relationship, and then information of neighbors is aggregated layer by layer by using an information propagation idea of the graph neural network so as to obtain an embedding representation of the user or the venue. The following provides descriptions by using an example in which a user embedding representation e_u^s in a code-scanning payment relationship is learned.

[0074] In an example, the graph neural network can be an attention mechanism-based graph neural network. In this case, modeling can be performed on the target user account and the first venue according to the following equation (1):

$$\begin{aligned}
 \mathbf{h}_u^{(l+1)} &= \text{ReLU} \left(\sum_{v \in N_u^s} (\alpha_{uv}^{(l)} \mathbf{h}_v^{(l)} \mathbf{W}_{nd}^{(l)} + \beta_{uv}^{(l)} g(\mathbf{x}_{uv}^s) \mathbf{W}_{eg}^{(l)}) \right) \\
 \mathbf{h}_v^{(l)} &= \text{ReLU} \left(\sum_{u \in N_v^s} (\alpha_{uv}^{(l-1)} \mathbf{h}_u^{(l-1)} \mathbf{W}_{nd}^{(l-1)} + \beta_{uv}^{(l-1)} g(\mathbf{x}_{uv}^s) \mathbf{W}_{eg}^{(l-1)}) \right) \\
 \mathbf{h}_n^0 &= \mathbf{x}_n, n \in \{u, v\},
 \end{aligned} \tag{1}$$

where $\mathbf{h}_u^1$ and $\mathbf{h}_v^1$ respectively represent node embeddings of the target user account u and the first venue v at the 1st hidden layer; N_u^s and N_v^s respectively define neighboring nodes of the target user account u and the first venue v in the code-scanning payment relationship; $\mathbf{x}_n$ represents an input feature of a node n ; $\mathbf{x}_{u,v}^s$ represents an edge feature of an edge $e_{u,v}$ in the code-scanning payment relationship; $g(\cdot)$ represents a layer of perceptual projection function that uses ReLU as an activation function; $\mathbf{W}_{nd}^{(l)}$ and $\mathbf{W}_{eg}^{(l)}$ are learnable matrices of a node path and an edge path; and $\alpha_{uv}^{(l)}$ and $\beta_{uv}^{(l)}$ are a node-level attention value and a edge-level attention value. Note

that n represents the user u or the venue v . To learn user embeddings, if a quantity of layers is an even number, n indicates the user u ; or otherwise, n indicates the venue v .

[0075] It is considered that different neighbors of nodes and edges should have different importance for different target nodes. Therefore, node-level attention and edge-level attention can be introduced. Node-level attention is intended to measure importance of a neighbor node to a target node and aggregate information of the neighbor node. In addition, edge-level attention is intended to measure importance of a neighbor edge to a target node and aggregate edge information. In detail, a score of the node-level (edge-level) attention is obtained by matching an embedding representation of a node n_1 with an embedding representation of a node n_2 or an edge e_{n_1, n_2} :

$$\begin{aligned}\alpha'_{n_1 n_2} &= \mathbf{a}_{attn}^T \cdot \mathbf{W}_{nd}^{attn} \cdot (\mathbf{h}_{n_1} || \mathbf{h}_{n_2}), \\ \beta'_{n_1 n_2} &= \mathbf{b}_{attn}^T \cdot \mathbf{W}_{eg}^{attn} \cdot (\mathbf{h}_{n_1} || g(\mathbf{x}_{n_1 n_2})),\end{aligned}$$

where $\cdot^T$ is transpose, $\mathbf{W}^{attn}$ is used to map a node embedding representation or an edge embedding representation to an attention space, and $\mathbf{a}_{attn}$ ($\mathbf{b}_{attn}$) is used to map a unified embedding representation to an attention fraction.

[0076] An attention weight α_{n_1, n_2} can be obtained by normalizing attention scores on all selected neighbors by using a softmax function:

$$\begin{aligned}\alpha_{n_1 n_2} &= \frac{\exp(\alpha'_{n_1 n_2})}{\sum_{j \in \mathcal{N}_{n_1}^s} \exp(\alpha'_{n_1 j})}, \\ \beta_{n_1 n_2} &= \frac{\exp(\beta'_{n_1 n_2})}{\sum_{j \in \mathcal{N}_{n_1}^s} \exp(\beta'_{n_1 j})}.\end{aligned}$$

[0077] According to an information propagation rule represented by equation (1), a user embedding representation $\mathbf{e}_u^s$ on a code-scanning payment path can be obtained.

Similarly, a user embedding representation $\mathbf{e}_u^f$ on a face-scanning payment path and venue embedding representations $\mathbf{e}_v^f$ and $\mathbf{e}_v^s$ in the two types of heterogeneous relationships can be obtained.

[0078] At 520, modeling is performed on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account by using the second machine learning model to obtain a biometric feature embedding representation used to reflect a similarity between the biometric feature data of the to-be-identified user and the biometric feature data of the target user account.

[0079] In an example, the second machine learning model can be implemented by using a multilayer perceptron (for example, a wide model). When modeling is

performed by using a multilayer perceptron, input features can include features strongly correlated with a current heterogeneous relationship (for example, face-scanning payment), for example, historical face-scanning information of the user and a machine, other association information, and real-time features of current face-scanning payment, such as a face comparison score and location information. The modeling can enhance memorability of a face-scanning behavior while enabling the model to have specific interpretation performance.

[0080] For example, a wide model can be used to separately perform modeling on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account. The wide model is advantageous in a good memory, and can well maintain importance of a biometric feature to user matching. The wide model is a generalized linear model that can be represented as follows:

$$\mathbf{h}_{wide} = W_{wd}\mathbf{x}_{wd} + \mathbf{b}_{wd},$$

where $\mathbf{h}_{wide}$ represents a biometric embedding feature, $\mathbf{x}_{wd}$ represents an original visual feature of the wide model, W_{wd} represents a weight matrix, and $\mathbf{b}_{wd}$ represents a bias vector of the wide model.

[0081] At 530, the embedding representations of the target user account and the first venue in the various heterogeneous relationships and the biometric feature embedding representation are provided for an aggregation layer to predict matchability between the target user account and both of the first venue and the biometric feature data of the to-be-identified user.

[0082] The aggregation layer is configured to aggregate the user embedding representation, the venue embedding representation, and the biometric feature embedding representation. In consideration that different types of nodes, different types of heterogeneous relationships, and biometric feature data have different contributions to different offline identification scenarios, the aggregation layer used can include an aggregation layer that is based on type-level attention. The aggregation layer can aggregate different types of embedding representations according to the following equation:

$$\hat{s}(\mathbf{e}_t) = \tanh(\mathbf{e}_t) \cdot \mathbf{w}_t,$$

$$\text{where } \mathbf{e}_t \in E = \{\mathbf{e}_u^s, \mathbf{e}_u^f, \mathbf{e}_m^s, \mathbf{e}_m^f, \mathbf{h}_{wide}\}.$$

[0083] In addition, a softmax function can further be used to obtain an attention weight of each type of embedding representation:

$$\alpha(\mathbf{e}_t) = \frac{\exp(\hat{s}(\mathbf{e}_t))}{\sum_{\mathbf{e}_0 \in \mathbf{E}} \exp(\hat{s}(\mathbf{e}_0))}.$$

[0084] Then, all types of embedding representations are cascaded, and an MLP is used to project the embedding representations according to equation (2) as a predicted value $\hat{y}_{uvf}$ that is used to reflect matchability between the target user account and both the first venue and the biometric feature data of the to-be-identified user:

$$\hat{y}_{uvf} = \text{MLP}(\|\mathbf{e} \in \mathbf{E}(\alpha(\mathbf{e}) \cdot \mathbf{e})\}). \quad (2)$$

[0085] In some embodiments, the first machine learning model, the second machine learning model, and the aggregation layer can be integrally trained as one model. During model training, a cross-entropy loss function can be used as a total loss function for model training. For example, the total loss function represented below can be used:

$$\mathcal{L} = -\frac{1}{|\text{Tr}|} \sum_{(u,v,f) \in \text{Tr}} y_{uvf} \log(\hat{y}_{uvf}) + (1 - y_{uvf}) \log(1 - \hat{y}_{uvf}),$$

where $y_{uvf} \in \{0, 1\}$ is a real label of a triplet (a user u , a venue v , and a face f), and Tr is a training set.

[0086] In some embodiments, the total loss function for model training can include a loss function for introducing L2 regularization to a model parameter. With this total loss function, overfitting can be avoided, and the overall model can be optimized by using mini-batch random gradient descent.

[0087] FIG. 7 is an example schematic diagram of a user verification process according to some embodiments of this specification.

[0088] As shown in FIG. 7, the first machine learning model such as a graph neural network is used to perform layer-by-layer iteration to obtain the user embedding representations $\mathbf{e}_u^s$ and $\mathbf{e}_u^f$ and the venue embedding representations $\mathbf{e}_v^f$ and $\mathbf{e}_v^s$ on the code-scanning payment path and the face-scanning payment path, and the second machine learning model such as a multilayer perceptron model is used to obtain the face visual feature embedding representation h_{wide} . Then, the user embedding representations $\mathbf{e}_u^s$ and $\mathbf{e}_u^f$, the venue embedding representations $\mathbf{e}_v^f$ and $\mathbf{e}_v^s$, and the face visual feature embedding representation h_{wide} are cascaded and provided to an MLP in the aggregation layer to predict a matching score (that is, a predicted value) of the triple (the user u , the venue v , and the face f).

[0089] FIG. 8 is another example flowchart of a user verification process according to some embodiments of this specification.

[0090] As shown in FIG. 8, at 810, matchability between the target user account and the first venue is determined based on the user behavior relationship heterogeneous graph, and at 820, it is determined whether the target user account matches the first venue. For example, a graph neural network can be used to predict the matchability
5 between the target user account and the first venue based on the user behavior relationship heterogeneous graph, that is, predict a possibility (a probability) that the target user account accesses the first venue. If a result at 820 is a mismatch, at 860, it is determined that the user identification fails.

[0091] If a result at 820 is a match, at 830, matchability between the target user
10 account and the biometric feature data of the to-be-identified user is determined based on the biometric feature data of the target user account and the biometric feature data of the to-be-identified user, and at 840, it is determined whether the target user account matches the biometric feature data of the to-be-identified user. For example, a similarity
15 between the target user account and face visual feature data of the to-be-identified user can be determined based on face visual feature data of the target user account and the face visual feature data of the to-be-identified user. If the similarity is not less than a predetermined threshold, it is determined that the target user account matches the face
visual feature data of the to-be-identified user. If the similarity is less than the predetermined threshold, it is determined that the target user account does not match
20 the face visual feature data of the to-be-identified user.

[0092] If a result at 840 is a match, at 850, it is determined that the user identification succeeds. If a result at 840 is a mismatch, at 860, it is determined that the user identification fails.

[0093] The offline user identification methods according to the embodiments of this
25 specification are described above with reference to FIG. 1 to FIG. 8.

[0094] By using the above-mentioned offline user identification methods, historical venue access information of users is mined to construct a heterogeneous relationship graph between the users and venues. During offline user identification, in addition to performing comparative verification based on biometric features, supplementary
30 verification is further performed to determine, based on the constructed heterogeneous relationship graph, whether a retrieved user account accesses a current venue. To be specific, matchability between an input biometric feature of a user, the retrieved user account, and the current to-be-accessed venue is determined. As such, user identification can be assisted based on offline behaviors and habits of the user, thereby

improving accuracy of offline user identification.

[0095] By using the above-mentioned offline user identification methods, the candidate-user-account local database and the candidate-user-account global database are created and maintained, and the local-global retrieval mechanism is used, thereby
5 improving retrieval efficiency of the target user account. In addition, the candidate-user-account local database is limited to a database created based on biometric feature data of users accessing the venue within a specified time period, so that the created candidate-user-account local database is time-limited, and a size of the candidate-user-account local database can be reduced, thereby further improving the retrieval
10 efficiency of the target user account. In addition, the candidate-user-account local database for each venue is limited to a database constructed based on historical access data at the venue and historical access data at another venue within a range of a given distance from the corresponding venue, so that the created candidate-user-account local database has increasing spatial locality, thereby increasing a retrieval hit rate of the
15 target user account.

[0096] By using the above-mentioned offline user identification methods, modeling is separately performed on graph information and biometric feature data, thereby improving embedding representation efficiency of users, venues, and biometric feature data.

[0097] By using the above-mentioned offline user identification methods, the first machine learning model, the second machine learning model, and the aggregation layer are trained together as an overall model, thereby improving overall identification accuracy of the first machine learning model, the second machine learning model, and the aggregation layer. In addition, by introducing L2 regularization to the total loss
20 function for model training, overfitting can be avoided, and the overall model can be optimized by using mini-batch random gradient descent.

[0098] FIG. 9 is an example block diagram of an offline user identification apparatus 900 according to some embodiments of this specification. As shown in FIG. 9, the offline user identification apparatus 900 includes a biometric feature data acquisition
25 unit 910, a target user account retrieval unit 920, and a user identification unit 930.

[0099] The biometric feature data acquisition unit 910 is configured to obtain biometric feature data of a to-be-identified user at a first venue. For an operation of the biometric feature data acquisition unit 910, refer to the operation described above with
30 reference to 210 in FIG. 2.

[0100] The target user account retrieval unit 920 is configured to retrieve a target user account from a candidate-user-account database based on the obtained biological feature data. For operations of the target user account retrieval unit 920, refer to the operations described above with reference to 220 in FIG. 2 and FIG. 3.

5 **[0101]** The user identification unit 930 is configured to determine, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user to perform user identification. For operations of the user
10 identification unit 930, refer to the operations described above with reference to 230 in FIG. 2 and FIG. 4 to FIG. 8.

[0102] FIG. 10 is an example block diagram of a target user account retrieval unit 1000 according to some embodiments of this specification. In the example of FIG. 10, the candidate-user-account database includes a candidate-user-account local database and a candidate-user-account global database. As shown in FIG. 10, the target user
15 account retrieval unit 1000 includes a local retrieval module 1010 and a global retrieval module 1020.

[0103] The local retrieval module 1010 is configured to retrieve the target user account from a corresponding candidate-user-account local database of the first venue
20 based on the obtained biometric feature data.

[0104] The global retrieval module 1020 is configured to retrieve the target user account from the candidate-user-account global database based on the obtained biometric feature data in response to a failure in retrieving a matched target user account from the candidate-user-account local database.

25 **[0105]** In an example, the user identification unit is configured to predict the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account.

30 **[0106]** FIG. 11 is an example block diagram of a user identification unit 1100 according to some embodiments of this specification. As shown in FIG. 11, the user identification unit 1100 includes a first embedding representation generation module 1110, a second embedding representation generation module 1120, and a prediction module 1130.

[0107] The first embedding representation generation module 1110 is configured to perform modeling on the target user account and the first venue by using a first machine learning model based on the user behavior relationship heterogeneous graph to obtain embedding representations of the target user account and the first venue in various heterogeneous relationships. For an operation of the first embedding representation generation module 1110, refer to the operation described above with reference to 510 in FIG. 5.

[0108] The second embedding representation generation module 1120 is configured to perform modeling on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account by using a second machine learning model to obtain a biometric feature embedding representation used to reflect a similarity between the biometric feature data of the to-be-identified user and the biometric feature data of the target user account. For an operation of the second embedding representation generation module 1120, refer to the operation described above with reference to 520 in FIG. 5.

[0109] The prediction module 1130 is configured to provide the embedding representations of the target user account and the first venue in the various heterogeneous relationships and the biometric feature embedding representation for an aggregation layer to predict matchability between the target user account and both of the first venue and the biometric feature data of the to-be-identified user. For an operation of the prediction module 1130, refer to the operation described above with reference to 530 in FIG. 5.

[0110] FIG. 12 is another example block diagram of a user identification unit 1200 according to some embodiments of this specification. As shown in FIG. 12, the user identification unit 1200 includes a first matching module 1210, a second matching module 1220, and a user identification module 1230.

[0111] The first matching module 1210 is configured to determine matchability between the target user account and the first venue based on the user behavior relationship heterogeneous graph. For an operation of the first matching module 1210, refer to the operation described above with reference to 810 in FIG. 8.

[0112] The second matching module 1220 is configured to determine matchability between the target user account and the biometric feature data of the to-be-identified user based on the biometric feature data of the target user account and the biometric feature data of the to-be-identified user. For an operation of the second matching

module 1220, refer to the operation described above with reference to 830 in FIG. 8.

[0113] The user identification module 1230 is configured to determine, in response to that the target user account matches both the first venue and the biometric feature data of the to-be-identified user, that the user identification succeeds; and determines, in response to that the target user account does not match at least one of the first venue and the biometric feature data of the to-be-identified user, that the user identification fails.

[0114] The offline user identification method and the offline user identification apparatus according to some embodiments of this specification are described with reference to FIG. 1 to FIG. 12 above. The above-mentioned offline user identification apparatus can be implemented by hardware, software, or a combination of hardware and software.

[0115] FIG. 13 is an example schematic diagram of an offline user identification apparatus 1300 implemented based on a computer system according to some embodiments of this specification. As shown in FIG. 13, the offline user identification apparatus 1300 can include at least one processor 1310, a storage (for example, a non-volatile storage) 1320, a memory 1330, and a communications interface 1340, and the at least one processor 1310, the storage 1320, the memory 1330, and the communications interface 1340 are connected together by using a bus 1360. The at least one processor 1310 executes at least one computer-readable instruction (to be specific, the above-mentioned element implemented in a software form) stored or encoded in the storage.

[0116] In an embodiment, computer-executable instructions are stored in the storage, and when executed, the computer-executable instructions enable the at least one processor 1310 to obtain biometric feature data of a to-be-identified user at a first venue; retrieve a target user account from a candidate-user-account database based on the obtained biometric feature data; and determine, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user to perform user identification, where the user behavior relationship heterogeneous graph is constructed based on historical venue access data of user accounts.

[0117] It should be understood that, when executed, the computer-executable instructions stored in the storage enable the at least one processor 1310 to perform the

above-mentioned operations and functions described with reference to FIG. 2 to FIG. 12 in the embodiments of this specification.

[0118] According to an embodiment, a program product such as a machine-readable medium (for example, a non-transient machine-readable medium) is provided. The machine-readable medium can have instructions (to be specific, the above-mentioned elements implemented in a software form). When executed by a machine, the instructions enable the machine to perform the above-mentioned operations and functions described with reference to FIG. 2 to FIG. 12 in the embodiments of this specification. Specifically, a system or an apparatus equipped with a readable storage medium can be provided, and software program code for implementing the functions in any of the above-mentioned embodiments is stored in the readable storage medium, so that a computer or a processor of the system or the apparatus reads and executes the instructions stored in the readable storage medium.

[0119] In this case, the program code read from the readable medium can implement the functions in any of the above-mentioned embodiments. Therefore, the machine-readable code and the readable storage medium that stores the machine-readable code form a part of the present invention.

[0120] Embodiments of the readable storage medium include a floppy disk, a hard disk, a magneto-optical disc, an optical disc (for example, a CD-ROM, a CD-R, a CD-RW, a DVD-ROM, a DVD-RAM, a DVD-RW, or a DVD-RW), magnetic tape, a non-volatile memory card, and a ROM. Alternatively, the program code can be downloaded from a server computer or a cloud over a communications network.

[0121] According to an embodiment, a computer program product is provided, where the computer program product includes a computer program, and when the computer program is executed by a processor, the processor is enabled to perform the above-mentioned operations and functions described with reference to FIG. 2 to FIG. 12 in the embodiments of this specification.

[0122] A person skilled in the art should understand that variations and modifications can be made to the embodiments disclosed above without departing from the essence of the present invention. Therefore, the protection scope of the present invention shall be subject to the appended claims.

[0123] It should be noted that not all steps and units in the above-mentioned processes and system structural diagrams are mandatory, and some steps or units can be ignored according to an actual requirement. An execution sequence of the steps is not fixed, and

can be determined as needed. The apparatus structure described in the above-mentioned embodiments can be a physical structure, or can be a logical structure. In other words, some units may be implemented by the same physical entity, or some units may be implemented by multiple physical entities or implemented jointly by some components in multiple independent devices.

[0124] In the above-mentioned embodiments, the hardware units or modules can be implemented by using a mechanical method or an electrical method. For example, a hardware unit, module or processor can include a permanent dedicated circuit or logic (for example, a dedicated processor, FPGA, or ASIC) to complete corresponding operations. The hardware unit or processor can further include programmable logic or a programmable circuit (for example, a general-purpose processor or another programmable processor), so that software can perform temporary settings to complete corresponding operations. Specific implementations (mechanical methods, dedicated permanent circuits, or temporarily set circuits) can be determined based on cost and time considerations.

[0125] The specific implementations illustrated above with reference to the accompanying drawings describe example embodiments, but do not represent all embodiments that can be implemented or fall within the protection scope of the claims. The term "example" used throughout this specification means "used as an example, an instance, or an illustration" and does not mean "preferred" or "advantageous" over other embodiments. For the purpose of providing an understanding of the described technologies, specific implementations include specific details. However, these technologies can be implemented without these specific details. In some instances, well-known structures and apparatuses are shown in block diagrams to avoid causing difficulties in understanding the concepts of the described embodiments.

[0126] The above-mentioned descriptions of the present disclosure are provided to enable any person of ordinary skill in the art to implement or use the present disclosure. Various modifications made to the present disclosure are clear to a person of ordinary skill in the art. In addition, the general principles defined in this specification can also be applied to other variants without departing from the protection scope of the present disclosure. Therefore, the present disclosure is not limited to the examples and designs described in this specification, but is consistent with the widest scope of principles and novelty features that conform to this specification.

CLAIMS

What is claimed is:

1. An offline user identification method, comprising:
obtaining biometric feature data of a to-be-identified user at a first venue;
5 retrieving a target user account from a candidate-user-account database based on the obtained biometric feature data; and
determining, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and
10 the biometric feature data of the to-be-identified user to perform user identification, wherein the user behavior relationship heterogeneous graph is constructed based on historical venue access data of user accounts.
2. The offline user identification method according to claim 1, wherein the determining, based on a user behavior relationship heterogeneous graph, the biometric
15 feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user comprises the following:
predicting the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model
20 based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account.
3. The offline user identification method according to claim 2, wherein the predicting the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model
25 based on the user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account comprises the following:
performing modeling on the target user account and the first venue by using a first machine learning model based on the user behavior relationship heterogeneous graph
30 to obtain embedding representations of the target user account and the first venue in various heterogeneous relationships;
performing modeling on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account by using a second machine learning

model to obtain a biometric feature embedding representation used to reflect a similarity between the biometric feature data of the to-be-identified user and the biometric feature data of the target user account; and

providing the embedding representations of the target user account and the first venue in the various heterogeneous relationships and the biometric feature embedding representation for an aggregation layer to predict matchability between the target user account and both of the first venue and the biometric feature data of the to-be-identified user.

4. The offline user identification method according to claim 3, wherein the first machine learning model comprises a graph neural network, and the second machine learning model comprises a multilayer perceptron model.

5. The offline user identification method according to claim 4, wherein the graph neural network comprises an attention mechanism-based graph neural network.

6. The offline user identification method according to claim 3, wherein the aggregation layer comprises an attention mechanism-based aggregation layer.

7. The offline user identification method according to claim 3, wherein the first machine learning model, the second machine learning model, and the aggregation layer are trained integrally as one model.

8. The offline user identification method according to claim 7, wherein a total loss function for training of the model comprises a cross-entropy loss function.

9. The offline user identification method according to claim 7, wherein a total loss function for training of the model comprises a loss function for introducing L2 regularization to a model parameter.

10. The offline user identification method according to claim 1, wherein the determining, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user comprises the following:

determining matchability between the target user account and the first venue based on the user behavior relationship heterogeneous graph;

determining matchability between the target user account and the biometric feature data of the to-be-identified user based on the biometric feature data of the target user account and the biometric feature data of the to-be-identified user; and

determining, in response to that the target user account matches both the first venue

and the biometric feature data of the to-be-identified user, that the user identification succeeds.

11. The offline user identification method according to claim 1, wherein the candidate-user-account database comprises a candidate-user-account local database and
5 a candidate-user-account global database; and

the retrieving a target user account from a candidate-user-account database based on the obtained biometric feature data comprises the following:

retrieving the target user account from a corresponding candidate-user-account local database of the first venue based on the obtained biometric feature data; and

10 retrieving the target user account from the candidate-user-account global database based on the obtained biometric feature data in response to a failure in retrieving a matched target user account from the candidate-user-account local database.

12. The offline user identification method according to claim 11, wherein each candidate-user-account local database comprises a candidate-user-account database
15 constructed based on historical access data at a corresponding venue and historical access data at another venue within a range of a given distance from the corresponding venue.

13. The offline user identification method according to claim 1, wherein the biometric feature data comprises visual feature data of face information.

20 14. An offline user identification apparatus, comprising:

a biometric feature data acquisition unit, configured to obtain biometric feature data of a to-be-identified user at a first venue;

a target user account retrieval unit, configured to retrieve a target user account from a candidate-user-account database based on the obtained biometric feature data; and

25 a user identification unit, configured to determine, based on a user behavior relationship heterogeneous graph, the biometric feature data of the to-be-identified user, and biometric feature data of the target user account, matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user to perform user identification, wherein the user behavior relationship heterogeneous
30 graph is constructed based on historical venue access data of user accounts.

15. The offline user identification apparatus according to claim 14, wherein the user identification unit predicts the matchability between the target user account, the first venue, and the biometric feature data of the to-be-identified user by using a machine learning model based on the user behavior relationship heterogeneous graph,

the biometric feature data of the to-be-identified user, and the biometric feature data of the target user account.

16. The offline user identification apparatus according to claim 15, wherein the user identification unit comprises the following:

5 a first embedding representation generation module, configured to perform modeling on the target user account and the first venue by using a first machine learning model based on the user behavior relationship heterogeneous graph to obtain embedding representations of the target user account and the first venue in various heterogeneous relationships;

10 a second embedding representation generation module, configured to perform modeling on the biometric feature data of the to-be-identified user and the biometric feature data of the target user account by using a second machine learning model to obtain a biometric feature embedding representation used to reflect a similarity between the biometric feature data of the to-be-identified user and the biometric feature data of
15 the target user account; and

 a prediction module, configured to provide the embedding representations of the target user account and the first venue in the various heterogeneous relationships and the biometric feature embedding representation for an aggregation layer to predict matchability between the target user account and both of the first venue and the
20 biometric feature data of the to-be-identified user.

17. The offline user identification apparatus according to claim 14, wherein the user identification unit comprises the following:

 a first matching module, configured to determine matchability between the target user account and the first venue based on the user behavior relationship heterogeneous
25 graph;

 a second matching module, configured to determine matchability between the target user account and the biometric feature data of the to-be-identified user based on the biometric feature data of the target user account and the biometric feature data of the to-be-identified user; and

30 a user identification module, configured to determine, in response to that the target user account matches both the first venue and the biometric feature data of the to-be-identified user, that the user identification succeeds.

18. The offline user identification apparatus according to claim 14, wherein the candidate-user-account database comprises a candidate-user-account local database and

a candidate-user-account global database; and

the target user account retrieval unit comprises the following:

a local retrieval module, configured to retrieve the target user account from a corresponding candidate-user-account local database of the first venue based on the

5 obtained biometric feature data; and

a global retrieval module, configured to retrieve the target user account from the candidate-user-account global database based on the obtained biometric feature data in response to a failure in retrieving a matched target user account from the candidate-user-account local database.

10 19. An offline user identification apparatus, comprising:

at least one processor;

a storage coupled to the at least one processor; and

a computer program stored in the storage, wherein the at least one processor executes the computer program to implement the offline user identification method

15 according to any one of claims 1 to 13.

20. A computer-readable storage medium, wherein the computer-readable storage medium stores executable instructions, and when the instructions are executed, a processor is enabled to perform the offline user identification method according to any one of claims 1 to 13.

20 21. A computer program product, comprising a computer program, wherein the computer program is executed by a processor to implement the offline user identification method according to any one of claims 1 to 13.