CLAIMS

1. A method for identifying identity information, comprising:

acquiring user data, the user data comprising identity information and account information of a user;

establishing an association relationship between account information and identity information that are bound in the user data, and establishing an association relationship between two pieces of account information having common features in the user data; and

determining a risk value of target identity information in the user data according to the established association relationships, and determining, according to the determined risk value, whether the target identity information has a risk of being used fraudulently,

wherein the establishing an association relationship between account information and identity information that are bound in the user data, and establishing an association relationship between two pieces of account information having common features in the user data comprises:

establishing a relationship diagram corresponding to the user data, the relationship diagram comprising an identity node for representing identity information in the user data and account nodes for representing account information in the user data, wherein there is a connection line between an account node and the identity node that are bound, and there is a connection line between two account nodes having common features; and

wherein among paths connecting a first account node and a second account node in the relationship diagram, a path comprising the fewest connection lines is used as the shortest path between the first account node and the second account node; and accordingly, the determining a risk value of target identity information in the user data comprises:

counting, in the established relationship diagram, the number of the shortest paths where a target identity node representing the target identity information is located, and counting the total number of the shortest paths in the relationship diagram, and

determining a ratio of the number of the shortest paths where the target identity node is located to the total number of the shortest paths as the risk value of the target identity information.

2. The method according to claim 1, wherein the two pieces of account information having common features comprises at least one of the following:

the two pieces of account information having an interaction behavior;

the two pieces of account information being bound to the same object; and

the two pieces of account information being logged-in on the same device.

3. The method according to claim 1, wherein the determining whether the target identity information has a risk of being used fraudulently comprises:

comparing the determined risk value with a specified threshold, and if the determined risk value is greater than the specified threshold, determining that the target identity information has a risk of being used fraudulently.

4. The method according to claim 1, wherein after determining whether the target identity information has a risk of being used fraudulently, the method further comprises:

extracting account information bound to the target identity information from the user data if the target identity information has a risk of being used fraudulently, and screening suspicious account information out from the account information bound to the target identity information.

5. The method according to claim 4, wherein the screening suspicious account information out from the account information bound to the target identity information comprises:

determining, for current account information in the account information bound to the target identity information, an authentication device corresponding to the current account information; and

counting the quantity of accounts authenticated in the authentication device, and if the counted quantity is greater than or equal to a specified quantity threshold, determining the current account information as suspicious account information.

6. An apparatus for identifying identity information, comprising:

a data acquisition unit configured to acquire user data, the user data comprising identity information and account information of a user;

an association relationship establishing unit configured to establish an association relationship between account information and identity information that are bound in the user data, and establish an association relationship between two pieces of account information having common features in the user data; and

an identifying unit configured to determine a risk value of target identity information in the user data according to the established association relationships, and determine, according to the determined risk value, whether the target identity information has a risk of being used fraudulently,

wherein the association relationship establishing unit comprises:

a relationship diagram establishing module configured to establish a relationship diagram corresponding to the user data, wherein the relationship diagram includes an identity node for representing identity information in the user data and account nodes for representing account information in the user data, wherein there is a connection line between an account node and the identity node that are bound, and there is a connection line between two account nodes having common features, and

wherein among paths connecting a first account node and a second account node in the relationship diagram, a path comprising the fewest connection lines is used as the shortest path between the first account node and the second account node; and correspondingly, the identifying unit comprises:

a shortest path counting module configured to, in the established relationship diagram, count the number of the shortest paths where a target identity node representing the target identity information is located, and count the total number of the shortest paths in the relationship diagram; and

a ratio calculation module configured to determine a ratio of the number of the shortest paths where the target identity node is located to the total number of the shortest paths as the risk value of the target identity information.

7. The apparatus according to claim 6, wherein the identifying unit comprises:

a threshold comparison module configured to compare the determined risk value with a specified threshold, and if the determined risk value is greater than the specified threshold, determine that the target identity information has a risk of being used fraudulently.

8. The apparatus according to claim 6, wherein the apparatus further comprises:

a suspicious account screening unit configured to extract account information bound to the target identity information from the user data if the target identity information has a risk of being used fraudulently, and screen suspicious account information out from the account information bound to the target identity information.

9. The apparatus according to claim 8, wherein the suspicious account screening unit comprises:

an authentication device determining module configured to, for current account information in the account information bound to the target identity information, determine an authentication device corresponding to the current account information; and

an authentication quantity counting module configured to count the quantity of accounts authenticated in the authentication device, and if the counted quantity is greater than or equal to a specified quantity threshold, determine the current account information as suspicious account information.

10. An apparatus for identifying identity information comprising a memory and a processor, wherein the memory is configured to store a computer program, and when executed by the processor, the computer program implements the method according to any of claims 1 to 5.