

Claims

1. A method, comprising:
 - obtaining feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user;
 - comparing the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and
 - in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:
 - prompting the to-be-verified user to enter verification data;
 - receiving the verification data entered by the to-be-verified user;
 - comparing the verification data with preset data corresponding to the preset feature point information set; and
 - in the event that the verification data and the preset data are the same, verifying the to-be-verified user, wherein:
 - the first predetermined threshold value relates to a lower degree of match above which the to-be-verified user is deemed to be directly verified; and
 - the second predetermined threshold value relates to an upper degree of match below which the to-be-verified user is deemed to be directly invalidated.
2. The method as described in claim 1, wherein in the event that the degree of match is greater than the first predetermined threshold value, verifying the to-be-verified user.
3. The method as described in claim 1, wherein:
 - the biometric information of the to-be-verified user is determined by at least:
 - collecting, via a user terminal, the biometric information;
 - sending, via the user terminal, a message to a server, the message including the biometric information; and
 - receiving, via the server, the biometric information;

the obtaining of the feature point information from the biometric information comprises extracting, via the server, the feature point information from the biometric information to form the to-be-verified feature point information set;

the comparing of the to-be-verified feature point information set with the preset feature point information sets that were stored in advance comprises comparing, via the server, the to-be-verified feature point information set with the preset feature point information sets that were stored in advance;

the receiving of the verification data entered by the to-be-verified user comprises receiving, via the server, the verification data entered by the to-be-verified user;

the comparing of the verification data with the preset data comprises comparing, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

the verifying of the to-be-verified user comprises verifying, via the server, the to-be-verified user.

4. The method as described in claim 1, wherein:

the biometric information of the to-be-verified user is determined by at least:

collecting, via a user terminal, the biometric information;

the obtaining of the feature point information from the biometric information comprises:

extracting, via the user terminal, feature point information from the biometric information to form the to-be-verified feature point information set;

sending, via the user terminal, a message to a server, the message including the to-be-verified feature point information set; and

receiving, via the server, the to-be-verified feature point information set;

the comparing of the to-be-verified feature point information set with the preset feature point information sets that were stored in advance comprises comparing, via the server, the to-be-verified feature point information set with the preset feature point information sets that were stored in advance;

the receiving of the verification data entered by the to-be-verified user comprises receiving, via the server, the verification data entered by the to-be-verified user;

the comparing of the verification data with the preset data comprises comparing, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

the verifying of the to-be-verified user comprises verifying, via the server, the to-be-verified user.

5. A method, comprising:

obtaining feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user, wherein:

the obtaining of the feature point information from the biometric information comprises extracting, via a server, the feature point information from the biometric information to form the to-be-verified feature point information set; and

the biometric information of the to-be-verified user is determined by at least:

collecting, via a user terminal, the biometric information;

sending, via the user terminal, a message to a server, the message

including the biometric information; and

receiving, via the server, the biometric information;

comparing, via the server, the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

receiving, via the server, verification data entered by the to-be-verified user; and

comparing, via the server, the verification data with preset data corresponding to the preset feature point information set;

in the event that the verification data and the preset data are the same, verifying the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value:

acquiring, via the server, location information of a predetermined positioning terminal of the to-be-verified user;

determining whether the predetermined positioning terminal and the user terminal that collected the biometric information of the to-be-verified user are in a same location; and

in the event that the predetermined positioning terminal and the user terminal are not in the same location, receiving, via the server, the verification data entered by the to-be-verified user, comprising:

comparing, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verifying, via the server, to-be-verified user.

6. The method as described in claim 5, further comprising:

in the event that the predetermined positioning terminal and the user terminal are in the same location, verifying the to-be-verified user.

7. The method as described in claim 5, wherein the message includes location information of the user terminal.

8. The method as described in claim 1, further comprising:

receiving business data entered by the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value, comparing the business data with a preset rule; and

in the event that the business data does not comply with the preset rule:

receiving the verification data entered by the to-be-verified user;

comparing the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verifying the to-be-verified user.

9. The method as described in claim 8, wherein:

the business data includes a spending amount; and

the preset rule corresponds to a spending amount interval determined based on an analysis of historical spending records of the to-be-verified user, the business data being required to fall within the spending amount interval.

10. A method, comprising:
 - obtaining feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user;
 - comparing the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and
 - in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:
 - receiving verification data entered by the to-be-verified user;
 - comparing the verification data with preset data corresponding to the preset feature point information set;
 - in the event that the verification data and the preset data are the same, verifying the to-be-verified user;
 - receiving business data entered by the to-be-verified user;
 - in the event that the degree of match is greater than the first predetermined threshold value, comparing the business data with a preset rule; and
 - in the event that the business data does not comply with the preset rule:
 - receiving the verification data entered by the to-be-verified user;
 - comparing the verification data with the preset data corresponding to the preset feature point information set; and
 - in the event that the verification data and the preset data are the same, verifying the to-be-verified user, wherein:
 - the business data is a spending amount;
 - the preset rule corresponds to a mean or average spending value determined based on an analysis of historical spending records of the to-be-verified user; and
 - the business data is to be less than a multiple of the mean or average spending value.
11. A system, comprising:
 - at least one processor configured to:

obtain feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user;

compare the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

prompt the to-be-verified user to enter verification data;

receive the verification data entered by the to-be-verified user;

compare the verification data with preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verify the to-be-verified user, wherein:

the first predetermined threshold value relates to a lower degree of match above which the to-be-verified user is deemed to be directly verified; and

the second predetermined threshold value relates to an upper degree of match below which the to-be-verified user is deemed to be directly invalidated;

and

a memory coupled to the at least one processor and configured to provide the at least one processor with instructions.

12. The system as described in claim 11, wherein in the event that the degree of match is greater than the first predetermined threshold value, verify the to-be-verified user.

13. The system as described in claim 11, wherein:

the biometric information of the to-be-verified user is determined by at least:

collect, via a user terminal, the biometric information;

send, via the user terminal, a message to a server, the message including the biometric information; and

receive, via the server, the biometric information;

the obtaining of the feature point information from the biometric information comprises extract, via the server, the feature point information from the biometric information to form the to-be-verified feature point information set;

the comparing of the to-be-verified feature point information set with the preset feature point information sets that were stored in advance comprises compare, via the server, the to-be-verified feature point information set with the preset feature point information sets that were stored in advance;

the receiving of the verification data entered by the to-be-verified user comprises receive, via the server, the verification data entered by the to-be-verified user;

the comparing of the verification data with the preset data comprises compare, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

the verifying of the to-be-verified user comprises verify, via the server, the to-be-verified user.

14. The system as described in claim 11, wherein:

the biometric information of the to-be-verified user is determined by at least:

collect, via a user terminal, the biometric information;

the obtaining of the feature point information from the biometric information comprises:

extract, via the user terminal, feature point information from the biometric information to form the to-be-verified feature point information set;

send, via the user terminal, a message to a server, the message including the to-be-verified feature point information set; and

receive, via the server, the to-be-verified feature point information set;

the comparing of the to-be-verified feature point information set with the preset feature point information sets that were stored in advance comprises compare, via the server, the to-be-verified feature point information set with the preset feature point information sets that were stored in advance;

the receiving of the verification data entered by the to-be-verified user comprises receive, via the server, the verification data entered by the to-be-verified user;

the comparing of the verification data with the preset data comprises compare, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

the verifying of the to-be-verified user comprises verify, via the server, the to-be-verified user.

15. A system, comprising:

at least one processor configured to:

obtain feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user, wherein:

the obtaining of the feature point information from the biometric information comprises extract, via a server, the feature point information from the biometric information to form the to-be-verified feature point information set; and

the biometric information of the to-be-verified user is determined by at least:

collect, via a user terminal, the biometric information;

send, via the user terminal, a message to a server, the message including the biometric information; and

receive, via the server, the biometric information;

compare the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

receive, via the server, verification data entered by the to-be-verified user;

compare, via the server, the verification data with preset data

corresponding to the preset feature point information set;

in the event that the verification data and the preset data are the same, verify the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value:

acquire, via the server, location information of a predetermined positioning terminal of the to-be-verified user;

determine whether the predetermined positioning terminal and the user terminal that collected the biometric information of the to-be-verified user are in a same location; and

in the event that the predetermined positioning terminal and the user terminal are not in the same location, receive, via the server, the verification data entered by the to-be-verified user, comprising:

compare, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verify, via the server, to-be-verified user; and

a memory coupled to the at least one processor and configured to provide the at least one processor with instructions.

16. The system as described in claim 15, wherein the at least one processor is further configured to:

in the event that the predetermined positioning terminal and the user terminal are in the same location, verify the to-be-verified user.

17. The system as described in claim 15, wherein the message includes location information of the user terminal.

18. The system as described in claim 11, wherein the at least one processor is further configured to:

receive business data entered by the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value, compare the business data with a preset rule; and

in the event that the business data does not comply with the preset rule:

receive the verification data entered by the to-be-verified user;

compare the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verify the to-be-verified user; and

a memory coupled to the at least one processor and configured to provide the at least one processor with instructions.

19. The system as described in claim 18, wherein:

the business data includes a spending amount; and

the preset rule corresponds to a spending amount interval determined based on an analysis of historical spending records of the to-be-verified user, the business data being required to fall within the spending amount interval.

20. A system, comprising:

at least one processor configured to:

obtain feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user;

compare the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

receive verification data entered by the to-be-verified user;

compare the verification data with preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verify the to-be-verified user;

receive business data entered by the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value, compare the business data with a preset rule; and

in the event that the business data does not comply with the preset rule:

receive the verification data entered by the to-be-verified user;

compare the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verify the to-be-verified user, wherein:

the business data is a spending amount;

the preset rule corresponds to a mean or average spending value determined based on an analysis of historical spending records of the to-be-verified user; and

the business data is to be less than a multiple of the mean or average spending value; and

a memory coupled to the at least one processor and configured to provide the at least one processor with instructions.

21. A computer program product being embodied in a tangible non-transitory computer readable storage medium and comprising computer instructions for:

obtaining feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user;

comparing the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

prompting the to-be-verified user to enter verification data;

receiving the verification data entered by the to-be-verified user;

comparing the verification data with preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verifying the to-be-verified user, wherein:

the first predetermined threshold value relates to a lower degree of match of above which the to-be-verified user is deemed to be directly verified; and

the second predetermined threshold value relates to an upper degree of match below which the to-be-verified user is deemed to be directly invalidated.

22. A computer program product being embodied in a tangible non-transitory computer readable storage medium and comprising computer instructions for:

obtaining feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user, wherein:

the obtaining of the feature point information from the biometric information comprises extracting, via a server, the feature point information from the biometric information to form the to-be-verified feature point information set; and

the biometric information of the to-be-verified user is determined by at least:

collecting, via a user terminal, the biometric information;

sending, via the user terminal, a message to a server, the message

including the biometric information; and

receiving, via the server, the biometric information;

comparing, via the server, the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

receiving, via the server, verification data entered by the to-be-verified user; and

comparing the verification data with preset data corresponding to the preset feature point information set;

in the event that the verification data and the preset data are the same, verifying the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value:

acquiring, via the server, location information of a predetermined positioning terminal of the to-be-verified user;

determining whether the predetermined positioning terminal and the user terminal that collected the biometric information of the to-be-verified user are in a same location; and

in the event that the predetermined positioning terminal and the user terminal are not in the same location, receiving, via the server, the verification data entered by the to-be-verified user, comprising:

comparing, via the server, the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verifying, via the server, to-be-verified user.

23. A computer program product being embodied in a tangible non-transitory computer readable storage medium and comprising computer instructions for:

obtaining feature point information based at least in part on biometric information collected from a to-be-verified user to form a to-be-verified feature point information set, the to-be-verified feature point information set identifying the to-be-verified user;

comparing the to-be-verified feature point information set with preset feature point information sets that were stored in advance; and

in the event that a degree of match between the to-be-verified feature point information set and a preset feature point information set is less than a first predetermined threshold value, and is greater than a second predetermined threshold value:

receiving verification data entered by the to-be-verified user;

comparing the verification data with preset data corresponding to the preset feature point information set;

in the event that the verification data and the preset data are the same, verifying the to-be-verified user;

receiving business data entered by the to-be-verified user;

in the event that the degree of match is greater than the first predetermined threshold value, comparing the business data with a preset rule; and

in the event that the business data does not comply with the preset rule:

receiving the verification data entered by the to-be-verified user;

comparing the verification data with the preset data corresponding to the preset feature point information set; and

in the event that the verification data and the preset data are the same, verifying the to-be-verified user, wherein:

the business data is a spending amount;
the preset rule corresponds to a mean or average spending value determined based on an analysis of this historical spending records of the to-be-verified user; and
the business data is to be less than a multiple of the mean or average spending value.