What is claimed is:

1. A biometric recognition method, comprising:
Step A: receiving biometric data;
Step B: performing a random transformation of low-bit data in received biometric data;
Step C: randomly selecting one or more filtering algorithms to pre-process randomly transformed biometric data; and
Step D: performing identity verification based on the pre-processed biometric data.

2. The method according to claim 1, wherein the step of "performing a random transformation of low-bit data in received biometric data" comprises: performing a random transformation of lowest bits in the biometric data, and wherein the step of "performing a random transformation of lowest bits in the biometric data" comprises any one of the following:
setting the lowest bits of the biometric data all to 0;
setting the lowest bits of the biometric data all to 1;
randomly re-arranging the lowest bits of the biometric data; and
randomly generating the lowest bits of the biometric data.

3. The method according to claim 1, wherein the identity verification based on the pre-processed biometric data is performed in the Step D to obtain a first comparison result, and the method further comprises:
repeating execution of the Steps B to D to obtain a second comparison result; and
directly performing identity verification based on received biometric data to obtain a third comparison result.

4. The method according to claim 3, further comprising:
comparing the first comparison result, the second comparison result and the third comparison result for consistency; and
feeding back the first comparison result when the first comparison result, the second comparison result and the third comparison result are consistent.

5. The method according to claim 4, further comprising:
feeding back a recognition process anomaly when the first comparison result, the second comparison result and the third comparison result are inconsistent; and
adding a corresponding data collection terminal to a blacklist.

6. The method according to claim 1, wherein the biometric data includes facial image data, and wherein the biometric data further includes a timestamp, and the method further comprises between the Steps A and B:
decrypting the biometric data to obtain the facial image data and the timestamp; and
feeding back an anomaly when a difference between system time and the timestamp does not meet requirements.

7. The method according to claim 6, further comprising between the Steps A and B:
detecting a facial position in the facial image data when the difference between the system time and the timestamp meets the requirements.

8. The method according to claim 7, further comprising between the Steps A and B:
adding an adversarial sample to the facial position, the adversarial sample devised to counteract action of a negative adversarial sample added at the data collection terminal, wherein the negative adversarial sample is a negative value of the adversarial sample, wherein the adversarial sample is pre-generated by performing a backpropagation training on a generator based on facial recognition results.

9. A biometric recognition server, comprising:
a receiving device to receive biometric data;
a low-bit random filter to randomly transform low-bit data in received biometric data;
a preprocessor to randomly select one or more filtering algorithms to pre-process randomly transformed biometric data; and
an identity verification device to perform identity verification based on pre-processed biometric data.

10. The server according to claim 9, wherein the low-bit random filter is configured to randomly transform lowest bits in the biometric data, and wherein the low-bit random filter is configured to perform any one of the following:
set the lowest bits of the biometric data all to 0;
set the lowest bits of the biometric data all to 1;
randomly re-arrange the lowest bits of the biometric data; and
randomly generate the lowest bits of the biometric data.

11. The server according to claim 9, further comprising:
a recognition decision device to compare multiple recognition results for consistency and to feed back the results when all the recognition results are consistent.

12. The server according to claim 11, wherein the recognition decision device is further configured to:
feed back a recognition process anomaly when the recognition results are inconsistent; and
add the corresponding data collection terminal to a blacklist.

13. The server of claim 9, wherein the biometric data includes facial image data, and wherein the biometric data further comprises a timestamp, and the server further comprising:
a decryption device to decrypt the biometric data to obtain the facial image data and the timestamp; and

a verification device to feed back an anomaly when a difference between system time and the timestamp does not meet requirements.

14. The server of claim 13, wherein the verification device is further configured to:
detect a facial position in the facial image data when the difference between the system time and the timestamp meets the requirements.

15. The server of claim 14, wherein the verification device is further configured to:
add in the facial position an adversarial sample for counteracting action of a negative adversarial sample added at the data collection terminal, wherein the negative adversarial sample is a negative value of the adversarial sample, wherein the adversarial sample is pre-generated by performing a backpropagation training on a generator based on facial recognition results.

16. A client for use in conjunction with the server according to claim 15, comprising:
a facial data collection device to collect facial image data; and
an embedding device to embed a negative adversarial sample in a facial position.

17. The client of claim 16, wherein the embedding device is configured to:
detect the facial position based on the facial image data;
embed the negative adversarial sample in the facial position; and
send a processed facial image and a timestamp in an encrypted manner.

18. A method for generating an adversarial sample using a biometric recognition server as claimed in any one of claims 9 to 15, comprising:
Step A: constructing an adversarial generative network comprising a generator and a discriminator;
Step B: generating noise information with the generator, and adding the noise information to real facial image data to obtain generated facial data;
Step C: recognizing the generated facial data with a facial recognition model;
Step D: performing a backpropagation training on the generator based on recognition results;
Step E: repeating the Steps B to D until the facial recognition model produces an erroneous recognition result; and
Step F: determining the noise information corresponding to the erroneous recognition result as an adversarial sample.

19. A computer storage medium comprising instructions, wherein the instructions, when running, implement the method as claimed in any one of claims 1 to 8.

20. A computer program product comprising a computer program, wherein the computer program, when executed by a processor, implements the method as claimed in any one of claims 1 to 8.