

CLAIMS:

1. A method for authorizing access to one or more secured computer resources, the method comprising:

storing an obfuscated reference biometric vector at an authentication computing device, the obfuscated reference biometric vector previously obfuscated from a reference biometric vector using a similarity-preserving obfuscation at a client computing device;

receiving an obfuscated authentication biometric vector, the obfuscated authentication biometric vector previously obfuscated from an authentication biometric vector using the similarity-preserving obfuscation at the client computing device;

testing a similarity of the obfuscated reference biometric vector and the obfuscated authentication biometric vector at the authentication computing device; and

based on the similarity being within an authentication threshold, communicating an authentication authorization from the authentication computing device to the client computing device to grant access to the one or more secured computer resources,

wherein the similarity-preserving obfuscation uses a received authentication credential as a seed for a random number generator to generate a sequence of transformations.

2. The method of claim 1, wherein the similarity-preserving obfuscation is a deterministic obfuscation.

3. The method of claim 2, wherein the similarity-preserving obfuscation is a deterministic vector rotation.

4. The method of claim 3, wherein testing the similarity of the obfuscated reference biometric vector and the obfuscated authentication biometric vector includes calculating a cosine angular distance between the obfuscated reference biometric vector and the obfuscated authentication biometric vector.

5. The method of claim 2, wherein the similarity-preserving obfuscation is a deterministic Euclidean transformation.

6. The method of claim 5, wherein testing the similarity of the obfuscated reference biometric vector and the obfuscated authentication biometric vector includes calculating an

L2 norm between the obfuscated reference biometric vector and the obfuscated authentication biometric vector.

7. The method of claim 1, wherein the received authentication credential is a password.

8. The method of claim 1, wherein the received authentication credential is a device identifier.

9. The method of claim 1, wherein the received authentication credential is a biometric identifier.

10. A method of granting access to one or more secured computer resources, the method comprising:

obfuscating a reference biometric vector into an obfuscated reference biometric vector using a similarity-preserving obfuscation at a client computing device;

sending the obfuscated reference biometric vector from the client computing device to an authentication computing device;

measuring an authentication biometric identifier at the client computing device;

transforming the authentication biometric identifier into an authentication biometric vector at the client computing device;

obfuscating the authentication biometric vector into an obfuscated authentication biometric vector using the similarity-preserving obfuscation at the client computing device;

sending the obfuscated authentication biometric vector from the client computing device to the authentication computing device; and

based on receiving an authentication authorization from the authentication computing device, granting access to the one or more secured computer resources, the authentication authorization previously determined at the authentication computing device based on a similarity of the obfuscated reference biometric vector and the obfuscated authentication biometric vector being within an authentication threshold,

wherein the similarity-preserving obfuscation uses a received authentication credential as a seed for a random number generator to generate a sequence of transformations.

11. The method of claim 10, wherein the reference biometric vector is transformed from a reference biometric identifier measured at the client computing device.

12. The method of claim 10 or 11, wherein the similarity-preserving obfuscation is deterministic vector rotation.

13. The method of claim 10, wherein the similarity-preserving obfuscation is a deterministic Euclidean transformation.

14. The method of any one of claims 10 to 13, wherein the authentication biometric identifier is a sensed human fingerprint.

15. The method of any one of claims 10 to 13, wherein the authentication biometric identifier is a sensed human iris.

16. The method of any one of claims 10 to 13, wherein the authentication biometric identifier is a sensed human face.

17. The method of any one of claims 10 to 13, wherein the authentication biometric identifier is a sensed human voice.

18. A method of authorizing access to one or more secured computer resources, the method comprising:

obfuscating a reference biometric vector into an obfuscated reference biometric vector using a similarity-preserving obfuscation;

obfuscating an authentication biometric vector into an obfuscated authentication biometric vector using the similarity-preserving obfuscation;

testing a similarity of the obfuscated authentication biometric vector and the obfuscated reference biometric vector; and

based on the similarity being within an authentication threshold, authorizing access to the one or more secured computer resources,

wherein the similarity-preserving obfuscation uses a received authentication credential as a seed for a random number generator to generate a sequence of transformations.