AUTHORIZED ANONYMOUS AUTHENTICATION

DESCRIPTION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of provisional application number 60/437,416, filed in the United States Patent Office on December 31,.2002.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not Applicable.

TECHNICAL FIELD:

[0003] This invention generally relates to processing data and, more particularly, to enabling an authorized submission and authentication of certain biometric data in a confidential manner.

BACKGROUND OF THE INVENTION:

[0004] Biometric data (e.g., DNA, fingerprints, retinal scans, voiceprints or other data corresponding with a physical representation of a natural person) is, and will continue to be, utilized in a variety of situations. For example, biometric research and testing has been and will likely continue to be utilized to: (a) provide greater understanding, and increase the likelihood, of curing physical challenges, (b) provide evidence supporting or undermining claims alleged in legal proceedings, (c) create greater specificity and accuracy with respect to certain archeological discoveries, and (d) using a template (e.g., a sample, abstract or other electronic or digitized system which enables sufficient parameters through an algorithmic mathematical reduction to compensate for a less than constant input or output), authenticate a natural person, such as prior to access into secure systems or facilities.

[0005] However, the increased use of biometric data has raised several privacy and ethical issues. Such issues include, without limitation: (a) using human subjects for potentially speculative results, (b) extrapolating the results of biometric testing beyond the reasonable scope of the tests, (c) establishing a framework within

which to cause or increase discrimination against protected classes, and (d) using and disclosing personally identifiable information beyond the scope of any use authorized by the natural person providing the information and/or relevant privacy laws.

[0006] Some current systems use data emanating from one or a combination of the following to authenticate a natural person: (a) something the natural person knows (e.g., passwords, pass-phrases, log-on numbers), (b) something the natural person possesses (e.g., plastic ID cards, tokens), (c) a physical representation of the natural person (e.g., biometrics) and (d) a behavioral representation of the natural person (e.g., keystroke cadence). Some of the means are less reliable than others and combining various means may prove to be more reliable and provide higher certainty against any identity fraud.

[0007] Some current systems use a reversible cryptographic algorithm (e.g., encryption or encoding or other algorithm which can be reversed to the original data, such as using decryption or decoding) in association with biometric data using a template. A template is used because most biometric data changes based upon several factors, such as illness, stress, hygiene or extraction variables. For example, an authentication system may use a fingerprint of the natural person during an enrollment process to prepare a corresponding fingerprint template. Thereafter, the system may capture biometric data corresponding to the fingerprint (which is subject to collection variability or even physical changes, such as burns, blisters, scratches, or dirt, which causes the resulting data to be inconsistent as compared to earlier captured fingerprint data) and compare the captured fingerprint data to the fingerprint template in determining whether to authenticate the natural person. Depending upon the parameters (e.g., statistics, patterns or other factors) of the system and the template, the natural person identity is authenticated or rejected. The reversible cryptographic algorithm is used with the template for confidentiality purposes (e.g., while the data is in transit), but the original biometric data can be reversed and analyzed to determine whether the parameters of the system and/or the template are appropriate.

[0008] Some current systems (e.g., NT or Unix) use an irreversible cryptographic algorithm (e.g., a one-way function, such as MD-5 or other algorithm having the effect of a one-way function, such as using a reversible cryptographic algorithm and destroying the corresponding decryption key) in conjunction with password storage to authenticate the natural person, such as prior to access to a secure

system. Using the irreversible cryptographic algorithm minimizes the possibility of disclosing all stored passwords should the system or password file be compromised. Furthermore, the irreversible cryptographic algorithm requires a constant input because any change in the input, such as a space, will cause a different result when processed through the irreversible cryptographic algorithm.

[0009] However, no current system, in association with a template or otherwise, utilizes the biometric data in association with the irreversible cryptographic algorithm, whether or not the biometric data is used in combination with any other means, such as a personal key.

BRIEF DESCRIPTION OF THE DRAWINGS:

[0010] FIGURE 1 is a functional block diagram of the system in accordance with the invention; and

[0011] FIGURE 2 is a flowchart of the system block in FIGURE 1.

DETAILED DESCRIPTION OF THE INVENTION:

[0012] While this invention is susceptible of embodiment in many different forms, there is shown in the drawing, and will be described herein in detail, a specific embodiment thereof with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and is not intended to limit the invention to the specific embodiment illustrated.

[0013] A data processing system 10 for processing data is illustrated in Figures 1-2. The system 10 includes at least one conventional computer 12 having a processor 14 and memory 16. The memory 16 is used both for storage of the executable software to operate the system 10 as well as for storage of the data in a database and random access memory. However, the software can be stored or provided on any other computer readable medium, such as a CD, DVD or floppy disc. The computer 12 receives inputs from a plurality of sources 181 - 18n.

[0014] The system 10 performs an enrollment process (i.e., process to receive and verify data corresponding with a natural person, such as in association with employment, a facility, a system and/or a privileged program like a frequent traveler program or a loyalty club program) 20 and an authentication process (i.e.,

process to receive and compare data to authenticate or reject the natural person and allow or reject the association with the employment, facility, system and/or other privileged program) 22. The enrollment process 20 and the authentication process 22, as further illustrated below, enables the natural person to authorize an authentication of the natural person's identity in an anonymous manner utilizing, at a minimum, biometric data and cryptographic algorithms.

[0015] The enrollment process 20 includes steps wherein the system 10: (a) receives a first biometric data from the natural person (e.g., segments of the natural person's DNA using developments in DNA sequencing, such as Polymerase Chain Reaction techniques, or facial scan data that can be embodied in a template) that is distinctive to the natural person and, independently and/or by generating one or more variants corresponding with actual or potential changes in the first biometric data, causes a result that can be processed through an irreversible cryptographic algorithm ("Enrollment Biometric Data") which, in some circumstances (e.g., circumstances wherein the natural person, laws, ethical considerations or other issues prefer that the Enrollment Biometric Data is not saved in any manner), is processed through a first irreversible cryptographic algorithm, in step 24, (b) receives a first personal key (e.g., a password, pass phrase, token, behavioral representation, a separate biometric, or other representation of the natural person's authorization) ("Enrollment Personal Key"), which is processed through a cryptographic algorithm (e.g., either the first irreversible cryptographic algorithm, a secondary irreversible cryptographic algorithm, or a reversible cryptographic algorithm) in highly confidential circumstances, in step 26, (c) identifies or assigns a primary key (e.g., an alphanumeric or numeric value corresponding with the natural person, such as an identification number) to the natural person ("Primary Key") in step 28, (d) combines (e.g., strung together, re-organized in a standard way, constant data introduced in a standard way, or other means to combine) the Enrollment Biometric Data and the Enrollment Personal Key ("Combined Data")in step 30, (e) processes the Combined Data through a second irreversible cryptographic algorithm (which can be the first irreversible cryptographic algorithm), sometimes after adding salt (i.e., additional data used to pad, modify, skew, or coat) to the Combined Data, causing the resulting data ("Processed Combined Data") to be undecipherable and irreversible (e.g., pre-image resistant), in step 32, (f) associates the Primary Key with the Processed Combined

Data ("Associated Processed Data") and eliminates all storage or trace of the Enrollment Biometric Data, Enrollment Personal Key and Combined Data, in step 34, and (g) transfers/stores the Associated Processed Data in a repository ("Repository") 38 in step 36.

[0016] For example, if the enrollment process 20 is in association with a trusted traveler program, the enrollment process 20 includes the step wherein the system receives the first biometric data (e.g., a DNA segment, retinal scan, facial image, or other biometric data) from a traveler and, in circumstances where the first biometric data is not constant, generates the one or more variants from the first biometric data (e.g., actual or potential changes in the DNA segment, retinal scan, facial image, or other biometric data), forming the Enrollment Biometric Data, which enables processing through the irreversible cryptographic algorithm (e.g., the Enrollment Biometric Data can be processed through the irreversible cryptographic algorithm and, in the event that the first biometric data changes thereafter, the one or more variants generated can be used, independently or by simulating fuzzy logic, to later authenticate the natural person). The enrollment process 20, in certain circumstances (e.g., to minimize concern regarding the storage of the passenger's DNA in a decipherable format), processes the Enrollment Biometric Data through the first irreversible cryptographic algorithm.

[0017] The system 20 then receives the Enrollment Personal Key and processes the Enrollment Personal Key through the cryptographic algorithm, which can be the first irreversible cryptographic algorithm, the second irreversible cryptographic algorithm, or the reversible cryptographic algorithm (e.g., if the corresponding decryption key is destroyed, the reversible cryptographic algorithm effectively becomes the secondary irreversible cryptographic algorithm).

[0018] Still using the example of the trusted traveler program, the system 20 then identifies and/or assigns the Primary Key (e.g., an alphanumeric value that can be known or unknown to the passenger), and processes the Primary Key through the cryptographic algorithm. The trusted traveler system then combines the Enrollment Biometric Data and the Enrollment Personal Key (not the Primary Key) forming the Combined Data.

[0019] The trusted traveler system then adds salt to the Combined Data and processes the salted Combined Data through the second irreversible cryptographic

algorithm (which can be the first irreversible cryptographic algorithm) forming the Processed Combined Data. For example, prior to, or part of, processing the Combined Data through the second irreversible cryptographic algorithm, the salt is added to the Combined Data and the Processed Combined Data would include irreversible and undecipherable data.

[0020] The trusted traveler program then associates the Primary Key with the Processed Combined Data forming the Associated Processed Data and transfers and/or stores the Associated Processed Data in the Repository.

[0021] All or part of the process in the enrollment process 20 may be performed by various applications and equipment, depending upon the relevant confidentiality and security requirements. For example, the process may be embodied as the following, at a minimum: (a) an installed software application on the source system or (b) a box unit that self-destroys the unit upon any tampering, such as an IBM 4758 cryptographic co-processor.

[0022] The location of the Repository 38 is less critical because the Enrollment Biometric Data, the Enrollment Personal Key and the Combined Data cannot be deciphered, reversed or decrypted from the Associated Processed Data. However, the Associated Processed Data may be used for comparison purposes.

[0023] The authentication process 22 includes steps wherein the system 10: (a) receives a second biometric data and generates one or more secondary variants (which can be the one or more variants and/or the first biometric data if the first biometric data changed in a manner that the one or more secondary variants causes a result that can be processed through the first irreversible cryptographic algorithm) ("Authentication Data") in step 40 and, consistent with the confidentiality circumstances in the enrollment process, processes the Authentication Data through the first irreversible cryptographic algorithm (i.e., the same first irreversible cryptographic algorithm used in the enrollment process in step 24), (b) receives a second personal key, which if received pursuant to the natural person's authorization, is the Enrollment Personal Key ("Authentication Personal Key"), and, also consistent with the confidential circumstances in the enrollment process, processes the Authentication Personal Key through the cryptographic algorithm, in step 42, (c) identifies a second primary key (e.g., if the second primary key identified is not the Primary Key, the system can reject the natural person identity initially)

("Authentication Primary Key") in step 44, (d) combines the Authentication Data and the Authentication Personal Key ("Combined Authentication Data") in step 46, (e) processes the Authentication Data through the second irreversible cryptographic algorithm (i.e., the same second irreversible cryptographic algorithm used in the enrollment process in step 34) after adding the salt to the Combined Authentication Data, causing the resulting data ("Processed Authentication Data") to be undecipherable and irreversible, in step 48, (f) associates the Authentication Primary Key with the Processed Authentication Data ("Associated Authentication Data"), eliminating all storage or trace of the Authentication Data, Authentication Personal Key and Combined Authentication Data, in step 50, and (g) transfers the Associated Authentication Data to the Repository 38 for comparison in step 52.

[0024] For example, returning to the trusted traveler program, the authentication process 22 includes circumstances wherein the passenger or an authenticator (e.g., a natural person at a check-in station or a computer system without any human interface) wants to authenticate the passenger's enrollment in the trusted traveler program. The passenger (if the passenger authorizes authentication) provides to the authenticator the second biometric data (which may be the same value as the first biometric data if the first biometric data is constant), the first personal key (i.e., the Authentication Personal Key prior to any processing through the cryptographic algorithm) and some data to enable the system to identify the first primary key (i.e., the Authentication Primary Key). The second biometric data and the first personal key are then processed through the authentication process, associated with the first personal key and compared with the data stored in the Repository.

[0025] Furthermore, the data that could be used to identify the primary key in the trusted traveler program can be a frequent flyer number, a confirmation code or some other data for the system to identify the passenger. Thereafter, the salt is added to the Combined Authentication Data (e.g., in the same manner as the enrollment process) and the salted Authentication Data is associated with the Authentication Primary Key.

[0026] Once the Associated Authentication Data reaches the Repository 38, the system within the Repository 38 would compare the Associated Authentication Data with the database of other enrollment data in a cryptographic format in step 54. Based upon the comparison, the system within the Repository 38 would determine

whether there was a match (e.g., independently and/or by simulating fuzzy logic wherein the system identifies a match, such as when the use of the variants cause predominant matches) in step 56 and provide a response confirming authentication in step 58 or indicating no authentication in step 60.

[0027] Returning to the example of the trusted traveler program, depending upon the parameters identified by the system and by simulating fuzzy logic, the system in the Repository 38 can confirm a match, even if the value of the first biometric data does not match the value of the second biometric data if, based upon certain matches by and between the one or more variants and the one or more secondary variants.

[0028] When a match exists in the trusted traveler program example, the system indicates a confirmation signal and the passenger is confirmed as an authenticated enrollee of the program. When no match exists, the system indicates a rejection signal and the passenger may be denied the benefits of the trusted traveler program and additional steps would be taken in accordance with the program rules. In the interim, given the irreversible nature of the data in the Repository 38, the data in the Repository 38 would be meaningless to any intruder or person desiring to scan or review the data, thus addressing the difficult problem associated with an inside threat or outside intruder.

[0029] All or part of the process in the authentication process 22 may be embodied within various applications and equipment, depending upon the relevant confidentiality and security requirements. For example, the process may be embodied as the following, at a minimum: (a) an installed software application on the source system or (b) a box unit that self-destroys the unit upon any tampering, such as an IBM 4758 cryptographic co-processor.

[0030] From the foregoing, it will be observed that numerous variations and modifications may be effected without departing from the spirit and scope of the invention. It is to be understood that no limitation with respect to the specific apparatus illustrated herein is intended or should be inferred. It is, of course, intended to cover by the appended claims all such modifications as fall within the scope of the claims.

WHAT IS CLAIMED IS:

1. A method for processing data comprising:

receiving a first biometric data and a first personal key;

processing the first biometric data and the first personal key through an irreversible cryptographic algorithm to form a first processed data;

receiving a second biometric data and a second personal key;

processing the second biometric data and the second personal key through the irreversible cryptographic algorithm to form a second processed data;

comparing the second processed data to the first processed data; and

generating a signal pertaining to the comparison of the second processed data to the first processed data.

2. The method of claim 1 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

3. The method of claim 1 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm.

4. The method of claim 1 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

5. The method of claim 1 further comprising adding salt to the first biometric data and the first personal key.

6. The method of claim 1 further comprising processing the first personal key through a cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

7. The method of claim 1 further comprising associating a first primary key to the first processed data.

8. The method of claim 1 further comprising associating a second primary key to the second processed data.

9. The method of claim 1 wherein receiving the first biometric data and the first personal key occurs during an enrollment process.

10. The method of claim 1 wherein receiving the second biometric data and the second personal key occurs during an authentication process.
11. The method of claim 1 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data.
12. The method of claim 11 wherein issuing a confirmation signal allows access to a facility.
13. The method of claim 11 wherein issuing a confirmation signal allows access to a system.
14. The method of claim 1 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data.
15. The method of claim 1 further comprising storing the first processed data in a database.
16. The method of claim 15 wherein the database includes a plurality of first processed data.

17. A method for processing data comprising:

receiving biometric data and a personal key;

processing the biometric data and the personal key through an irreversible cryptographic algorithm to form a processed data; and

comparing the processed data to secondary data.

18. The method of claim 17 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

19. The method of claim 17 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

20. The method of claim 17 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

21. The method of claim 17 wherein receiving the biometric data and the personal key occurs during an authentication process.

22. The method of claim 17 further comprising associating a primary key with the biometric data and the personal key.

23. The method of claim 17 wherein the secondary data includes a secondary biometric data and a secondary personal key.

24. The method of claim 23 wherein the secondary biometric data and the secondary personal key is received during an enrollment process.

25. The method of claim 17 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data.

26. The method of claim 25 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data.

27. The method of claim 25 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data.

28. The method of claim 25 wherein generating a signal allows entry into a facility when the processed data matches the secondary data.

29. The method of claim 25 wherein generating a signal allows entry into a system when the processed data matches the secondary data.

30. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method for processing data comprising:

receiving a first biometric data and a first personal key;

processing the first biometric data and the first personal key through an irreversible cryptographic algorithm to form a first processed data;

receiving a second biometric data and a second personal key;

processing the second biometric data and the second personal key through the irreversible cryptographic algorithm to form a second processed data;

comparing the second processed data to the first processed data; and

generating a signal pertaining to the comparison of the second processed data to the first processed data.

31. The computer readable medium for performing the method of claim 30 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

32. The computer readable medium for performing the method of claim 30 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm.

33. The computer readable medium for performing the method of claim 30 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

34. The computer readable medium for performing the method of claim 30 further comprising adding salt to the first biometric data and the first personal key prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

35. The computer readable medium for performing the method of claim 30 further comprising processing the first personal key through a reversible cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

36. The computer readable medium for performing the method of claim 30 further comprising associating a first primary key to the first processed data.

37. The computer readable medium for performing the method of claim 30 further comprising associating a second primary key to the second processed data.

38. The computer readable medium for performing the method of claim 30 wherein receiving the first biometric data and the first personal key occurs during an enrollment process.

39. The computer readable medium for performing the method of claim 30 wherein receiving the second biometric data and the second personal key occurs during an authentication process.

40. The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data.

41. The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a facility.

42. The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a system.

43. The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data.

44. The computer readable medium for performing the method of claim 30 further comprising storing the first processed data in a database.

45. The computer readable medium for performing the method of claim 44 wherein the database includes a plurality of first processed data.

46. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method for processing data comprising:

receiving biometric data and a personal key;

processing the biometric data and the personal key through an irreversible cryptographic algorithm to form a processed data; and

comparing the processed data to secondary data.

47. The computer readable medium for performing the method of claim 46 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

48. The computer readable medium for performing the method of claim 46 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

49. The computer readable medium for performing the method of claim 46 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

50. The computer readable medium for performing the method of claim 46 wherein receiving the biometric data and the personal key occurs during an authentication process.

51. The computer readable medium for performing the method of claim 46 further comprising associating a primary key with the biometric data and the personal key.

52. The computer readable medium for performing the method of claim 46 wherein the secondary data includes a secondary biometric data and a secondary personal key.

53. The computer readable medium for performing the method of claim 52 wherein the secondary biometric data and the secondary personal key is received during an enrollment process.

54. The computer readable medium for performing the method of claim 46 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data.

55. The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data.

56. The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data.

57. The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a facility when the processed data matches the secondary data.

58. The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a system when the processed data matches the secondary data.