Technology Available for Licensing
UB Docket 5922 and 6000

stor
UB Office of Science, Technology Transfer and Economic Outreach

Biometric Convolution:

A method for securing data using multiple biometrics

Biometric presents an accurate method for personal authentication. Biometrics is the science of establishing the identity of an individual through his or her physiological or behavioral characteristics. Fingerprints, face, iris, signature, voice and hand geometry are some of the common biometric modalities. Biometrics, though proven to be more secure and efficient than password protected systems are probabilistic and not all or none like passwords. Even a slight change in the acquisition of the biometric can lead to a totally different hash value, which might not match the stored template. If a biometric template is compromised, it cannot be re-issued since any user has a limited number of biometrics. Another major concern is the possible sharing and misuse of biometric databases between organization and agencies without the user's knowledge. Therefore a method and system is required where the privacy and security of the biometric template is ensured. The system should allow re-enrollment and replacement of biometrics if the original template is compromised.

Biometric convolution: A method for securing data using multiple biometrics

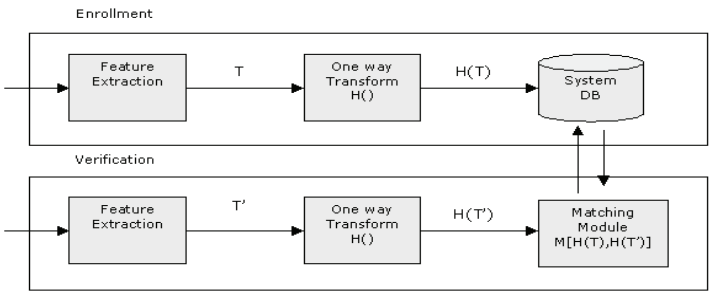
OVERVIEW

Biometric presents an accurate method for personal authentication. Biometrics is the science of establishing the identity of an individual through his or her physiological or behavioral characteristics. Fingerprints, face, iris, signature, voice and hand geometry are some of the common biometric modalities. Although biometrics provides a reliable means of establishing the identity of an individual, it presents its own unique vulnerabilities. Passwords and tokens such as smart cards can be reissued or revoked easily when they are compromised. However, if a biometric template is compromised, it cannot be re-issued since any user has a limited number of biometrics. There are also pertinent issues of privacy when the same biometric is used across several applications or organizations. The major concern is the possible sharing and misuse of biometric databases between organization and agencies without the user's knowledge.

In order to prevent compromise of passwords over the network in password authentication systems, the hashed values of the passwords are transmitted instead of the actual passwords. A hash function is a transformation that takes an input string and returns a value, which is called the hash value. The hash functions can be non-invertible and it is impossible to recover the original from the hash value.

Therefore a method and system is required where the privacy and security of the biometric template is ensured. The system should allow re-enrollment and replacement of biometrics if the original template is compromised. A system that is capable of doing this will be a cancellable biometric system.

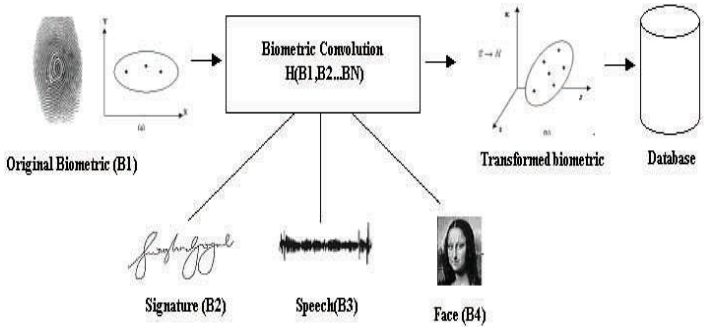
Fig: Cancelable biometric using a non-invertible transformation function



INVENTION

A new system, Biometric convolution is proposed. In this system, biometric is modified using a non-invertible transformation that is derived using another biometric of the individual. Due to the non-invertible nature of the conversion, it is not possible to recover the original biometric even if the template is compromised. This mechanism also allows for the re-issuance and replacement of such templates when required. Another advantage of this technique is that the template representation is not changed in the process allowing us to increase the trustworthiness and security of current systems without altering or replacing existing biometric recognition algorithms.

The most commonly used non-invertible transform is a one-way hash function. In this approach, the password itself is not stored in the database; instead, the result of a one-way hashing function is stored. During verification, the input is hashed and then compared to what is stored in the database. Our approach to cancelable biometrics is to create hashing functions, and perform matching in the hashed space instead of the original. Different transforms can be used in each application to protect the biometric data. Thus, even if the stored biometric is compromised, the person can be re-enrolled simply by changing the transformation.

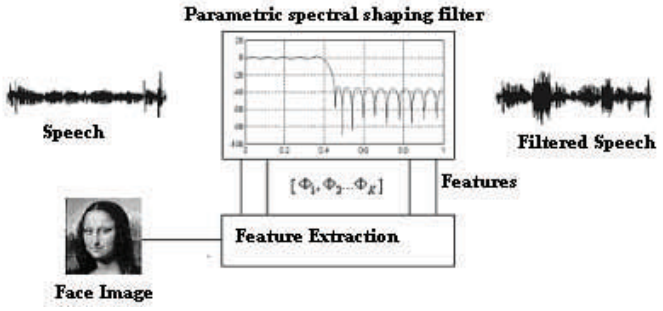


In cancelable biometrics and hashing scheme, the original biometric B1 altered through a non-invertible transform to yield the biometric B1^ = T(B1). altered through a non-invertible transform to yield the biometric (B1,B2….BN). The altered biometric can be obtained by B1^ = T(B1,B2….BN). The transformation can be parameterized by the secondary biometric signals or may use the signal itself to obtain the mapping. The advantage of this approach is that the secondary biometrics that is used to obtain the transformed biometric need not even be stored in the database making the system very secure.

Intellectual Property Division, UB Technology Incubator, Suite 111, 1576 Sweet Home Road, Amherst, NY 14228
Tel: (716) 645-5500 Fax: (716) 645-3436 Web: www.stor.buffalo.edu

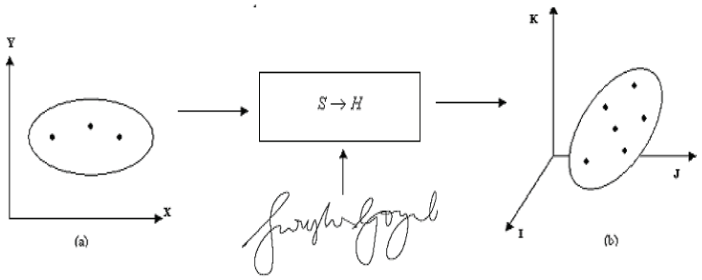
INVENTION

For example, we can combine face and voice data to construct a new cancelable biometric template.



Let speech be the primary biometric data Bs that has to be secured. Let the face biometric Bf be used to generate the unique transfer function. When a user presents for authentication, a one-way secret transformation function T (Bs, Bf, K) is applied to the original voice data Bs to generate the new biometric template B^s, which is henceforth used in all processing. The parameter K may be changed to yield different transformation functions allowing us to re-enroll the users using the same biometrics Bs and Bf. The transformation in the example may be achieved through a parameterized digital filter that alters the frequency content of the original voice signal. The parameters may specify gain at different frequencies and will be based on the eigenface features derived from the feature extraction module.

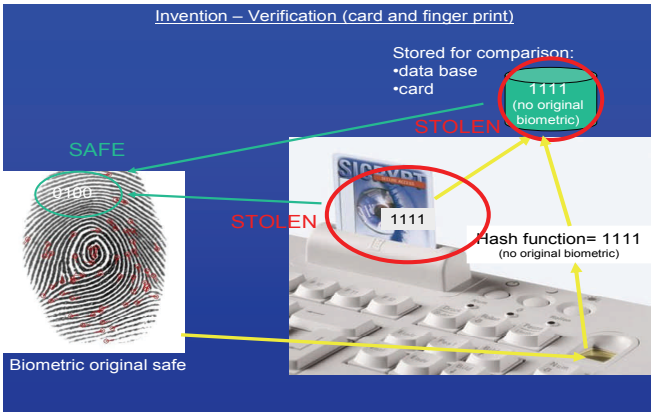
Such a system is robust to minor changes in the filter parameters due to variation in the biometrics Bs, Bf and does not alter the spectral shaping significantly. In order to circumvent such a system, the attacker should have access to a reproduction of the user's biometric Bs, Bf and should also know the secret key K and the details of the transformation function T. Circumventing all these measures is difficult which makes such a system extremely secure and reliable.



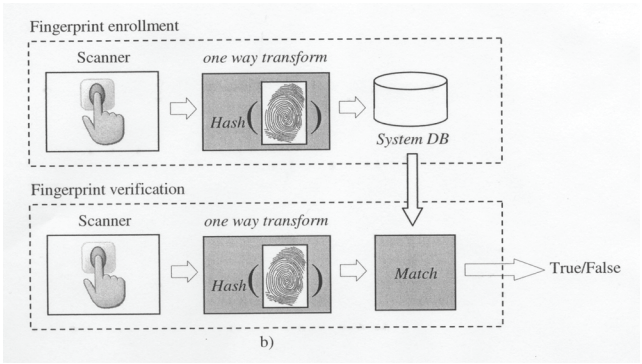
Hashing (a) Original minutiae in Cartesian space (b) Mapping into Hash space

Assume that two fingerprints originating from one finger differ by scale and rotation. Thus the set of minutia points of one fingerprint image can be obtained from the set of minutia points of another fingerprint image by scaling and rotating.

This algorithm gives a system for hashing biometric information by representing minutia on the biometric as space and direction and using those points as the inputs of the hash function. Only the hashed function of the minutia points is stored or transmitted so there is no way to get the original biometric from the database. If the database is compromised, a new set of points and a new hash function can be made without compromising the entire biometric



Summarizing, we have got a secure hashed representation of the fingerprint and a technique to create hash using localized information. The matching algorithm which matches based on localized information, we have a method to make biometric revocable by changing the hash function and further secure the hash by using s second factor.



Technology Available for Licensing
UB Docket 5922and 6000

UB Office of Science, Technology Transfer and Economic Outreach

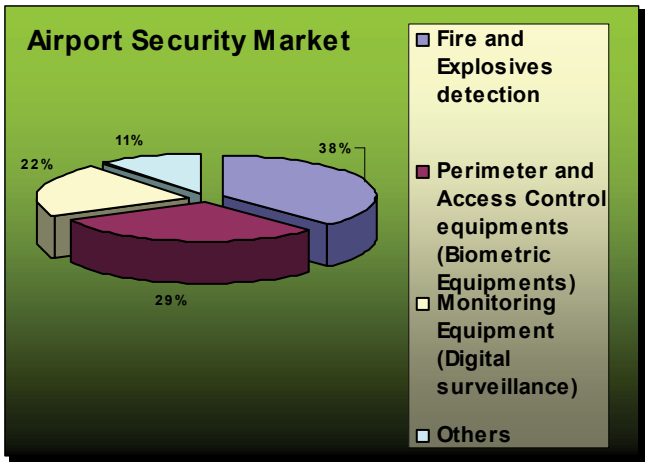
Biometric Convolution:
A method for securing data using multiple biometrics

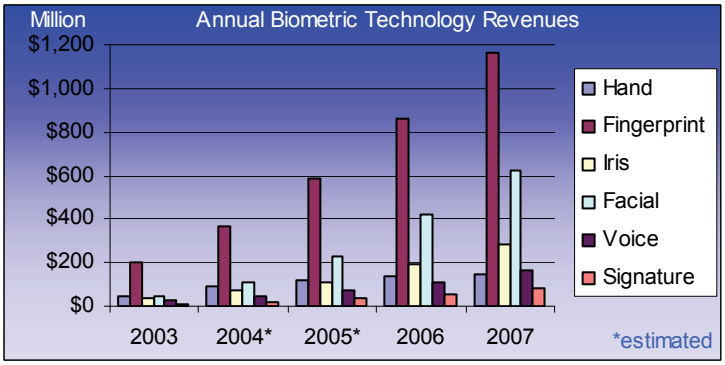
ADVANTAGE

This technique presents several advantages over existing methods.
(i) Since the transformation is derived using another biometric, external transformation parameters or the second biometric need not even be stored in the database. This makes it even more difficult to compromise the templates
(ii) When a biometric of one individual closely resembles that of another, it can lead to false positives in the recognition process. However the chances of multiple biometrics of different individuals being identical is statistically insignificant. By utilizing a personal but statistically independent process to modify the original biometric implies that the false accept rates will be reduced, increasing the accuracy of existing matching algorithms.

MARKET

Markets that have recently embraced biometric technologies include transportation/immigration services, healthcare, government, prisons, and financial services. The following figure shows the share of biometrics in the Airport Market





INTELLECTUAL PROPERTY

Provisional application filed with USPTO covering all claims.

CONTACT PERSON

Rupal Desai
Commercialization Manager
UB Office of Technology Transfer and Licensing
UB Technology Incubator, Suite 111
Baird Research Park
1576 Sweet Home Road
Amherst, NY 14228
Tel: (716) 645 - 5500
Fax: (716) 645 - 3436
Email: rdesai@buffalo.edu

PRIMARY INVENTOR

Dr. Venu Govindaraju
Department of Computer Science and Engineering
University at Buffalo