Comparison of Privacy Preserving Biometric Schemes

Amrutha S Nair
PG Student
Department of Computer Science & Engineering
Mount Zion College of Engineering

Jeena P Abraham
Assistant Professor
Department of Computer Science & Engineering
Mount Zion College of Engineering

Abstract

Biometric verification is defined as the verification of an individual based on the physical, chemical or behavioral attributes of the person. To protect the biometric data containing privacy information, a number of privacy-preserving biometric schemes (PPBSs).These PPBSs can be classified into Biometric encryption based schemes, Cancelable biometric based schemes, Multi-modal and hybrid based schemes, secure computation (SC) based schemes. There is a comparative study of PPBS and select the best one .On the bases of comparisons select the best PPBS is Biometric encryption based schemes.

Keywords- Biometric encryption, Cancelable biometric, Hybrid based, Multimode, Secure computation

I. INTRODUCTION

Exponential growth of the internet, identity verification becomes an essential part in web-based applications. Traditionally, passwords, identity cards and pin numbers are used for the verification of individuals. But attackers can get access to a system by guessing passwords and pin numbers. Overcome the disadvantages uses biometric verification system. Biometric verification is defined as the verification of a individual based on the physical, chemical or behavioral attributes of the person. To protect the biometric data containing privacy information, a number of privacy-preserving biometric schemes (PPBSs)[1].These PPBSs can be classified into Biometric encryption based schemes, Cancelable biometric based schemes, Multi-modal and hybrid based schemes, secure computation (SC) based schemes. There is a comparative study of PPBS and select the best one.

II. BIOMETRIC ENCRYPTION BASED SCHEMES (BE)

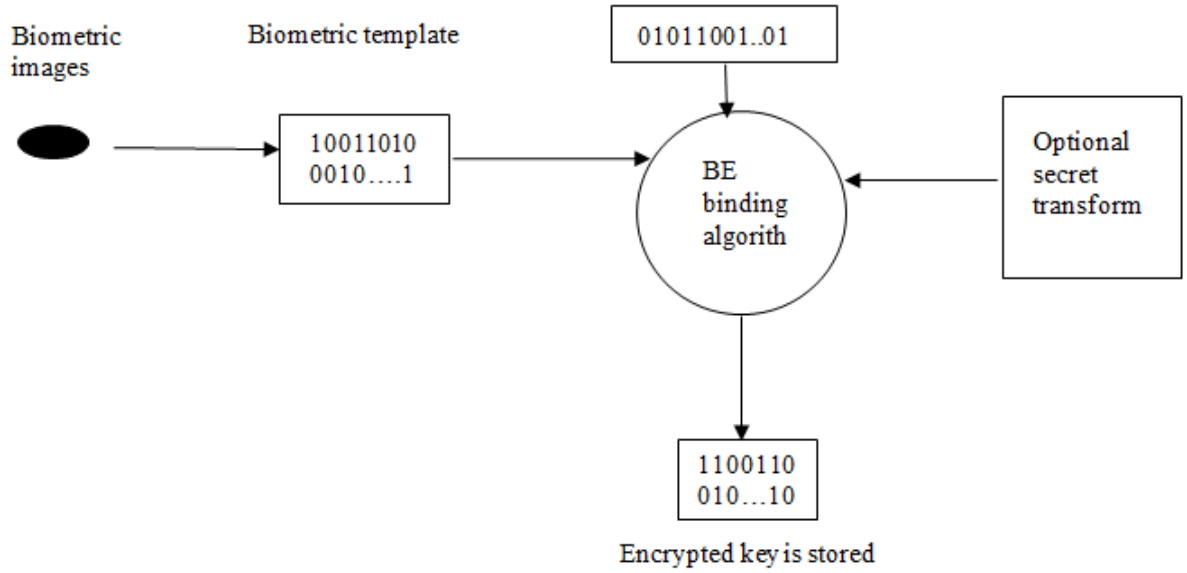
In frame work is including two pats Enrolment and Verification .At the enrolment stage, a user provides a biometric signal as an input. At the verification stage, the received biometric signal, together with the secret key and then produce the helper data. Biometric Encryption (BE) is a group of emerging technologies that securely bind a digital key to a biometric or generate a digital key from the biometric, so that no biometric image or template is stored [2]. What is stored is the BE template otherwise known as a ‘‘bio-metrically encrypted key’’ or ‘‘helper data.’’ As a result, neither the digital key nor the biometric can be retrieved from the stored BE template. BE conceptually differs from other systems that encrypt biometric images or templates using conventional encryption, or store a cryptographic key and release it upon successful biometric authentication. With BE, the digital key is recreated only if the correct biometric sample is presented on verification. The output of BE verification is either a digital key or a failure message. This ‘‘encryption/decryption’’ process is fuzzy because of the natural variability of biometric samples. Currently, available BE system requires that biometric-dependent helper data be stored. Specific privacy concerns with these technologies [8]

- Function creep (i.e., unauthorized secondary uses of biometric data).
- Expanded surveillance, tracking, profiling, and potential discrimination (biometric data can be matched against samples collected and stored elsewhere and used to make decisions about individuals)
- Data misuse (data breach, identity theft, and fraud)
- Negative personal impacts of false matches, non-matches, system errors, and failures (the consequences of system anomalies, especially in large-scale systems, often fall disproportionately on individuals, normally in the form of inconveniences, costs, and stigma)
- Insufficient oversight, accountability, and openness in biometric data systems

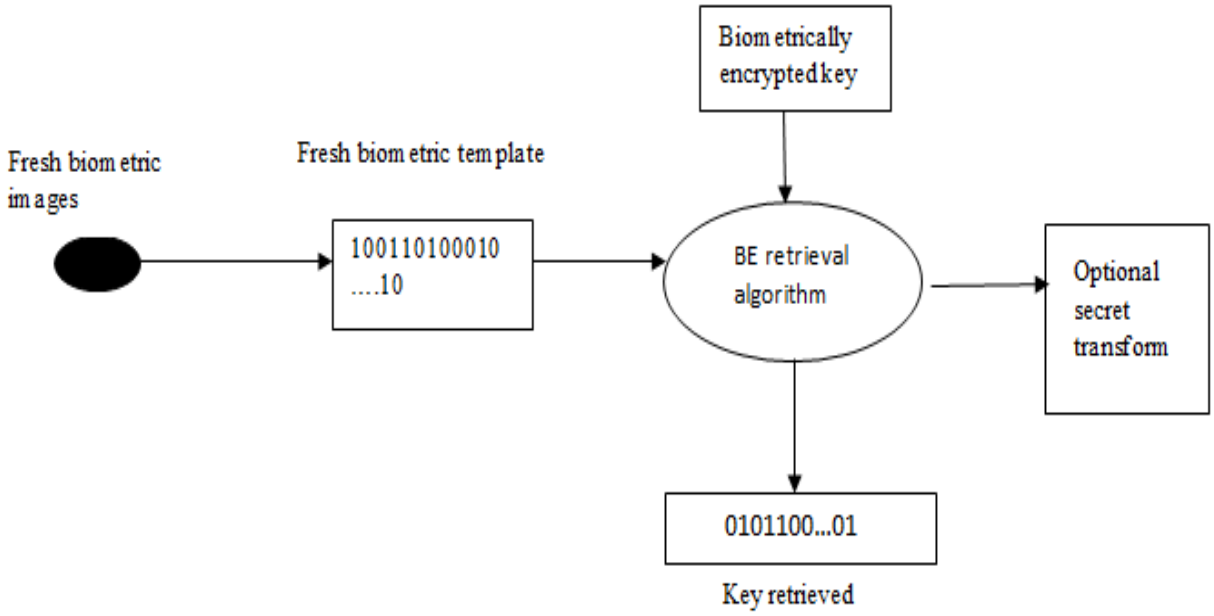
Many BE schemes also store a hashed value of the key. so that a correct key is released from the BE system only if the hashed value obtained on verification is exactly the same. Also, good practice would be not to release the key, but rather, another hashed version of it for any application. This hashed version can in turn serve as a cryptographic key. With this architecture, an attacker would not be able to obtain the original key outside the BE system. Likewise, the biometric image/template should not be sent to a server; the BE verification should be done .Locally in most scenarios. An important part of most BE algorithms is an Error Correcting Code (ECC). ECCs are used in communications, for data storage, and in other systems where errors can occur. Biometric Encryption is a new area for the application of ECC.

A. Advantages

- There is no retention of biometric image or conventional biometric template, and they cannot be recreated from the stored helper data.
- They are capable of multiple identifiers: a large number of BE templates for the same biometric can be created for different applications.
- The BE templates from different applications cannot be linked.
- The BE template can be revoked.
- They can be easily integrated into conventional cryptosystems, as the passwords are replaced with longer digital keys, which do not have to be memorized.
- They provide improved authentication and personal data security through a stronger binding of user biometric and system identifier.
- The BE systems are inherently protected from substitution attack, tampering, Trojan horse attack, overriding Yes/No response, and less susceptible to masquerade attack.
- They are suitable for large-scale applications, as the databases will store only untraceable, yet sufficient, information to verify the individual's claim.



(a) Enrollment



(b) Verification

Fig. 1: High level diagram of a Biometric Encryption process in a key binding mode, a) Enrollment b) Verification

In the key binding mode, a randomly generated secret key and the biometric features are combined monolithically using cryptographic framework. In other words, the secret key is encrypted using biometric features. The biometrically encrypted data (which is the helper data in this context) and the hash value of the secret key are stored. At the verification end, the secret key is retrieved using the stored biometrically encrypted data and the received biometric signal. During the verification process, the hash value of the retrieved secret key is compared with the stored hash value of the secret key. Fuzzy commitment scheme During enrollment, commit (bind) a code word w of an error-correcting code C using a fixed length biometric feature vector x as the witness. Given a biometric template x, the fuzzy commitment (or the helper data) consists of h(w) and x ¡ w, where h is a hash function . During verification, the user presents a biometric vector x0. The system subtracts x ¡ w stored in the database from x0 to obtain w0 = w + ±, where ± = x0¡x. If x0 is close to x, w0 is close to w since x0¡x = w0¡w. Therefore, w0 can now be decoded to obtain the nearest code word which would be w provided that the distance between w and w0 is less than the error correcting capacity of the code C. Reconstruction of w indicates a successful match.

B. Advantages

This approach is tolerant to intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated code word.

III. BE TECHNOLOGIES

A. Mytec1

This is the first BE scheme [1]. It was developed using optical processing, but can also be implemented digitally. The key is linked to a predefined pattern, s(x), which is a sum of several delta-functions. Using s(x) and a fingerprint, f(x), one can create a filter, H(u) ¼ S(u)/F(u), in Fourier domain (S(u) and F(u) are the Fourier transforms of s(x) and f(x)). It is difficult to obtain either S(u)orF(u)from the stored filter H(u). On verification, if a correct fingerprint, F'(u) □ F(u), is applied to the filter, it will reconstruct a correct output pattern, s'(x) □ s(x) so that the key will be regenerated from the locations of the output correlation peaks. Unfortunately, this scheme turned out to be impractical in terms of providing sufficient accuracy and security.

B. Mytec2

This is the first practical BE scheme [9]. Unlike Mytec1, it retains phase-only parts of S(u) and F(u) in the filter, H(u). The phase of S(u) is randomly generated, but not stored anywhere. As a result, the output pattern, c(x), is also random. The key, normally 128 bit long, is linked to c(x) via a lookup table and ECC. The filter, H(u), the lookup table, and the hashed key are stored in the helper data.

C. ECC Check Bits

This scheme, which was originally called ''private template,'' is a secure sketch.

D. Biometrically Hardened Passwords

A password that the user types or says is fused with a key (via a secret sharing scheme) extracted from a biometric component, thus hardening the password with the biometrics. The technique was made adaptive by updating a ''history file'' (which is, in fact, helper data) upon each successful authentication.

E. Fuzzy Commitment

A biometric template must be in the form of an ordered bit string of a fixed length. A key is mapped to an (n,k,d) ECC code word of the same length, n, as the biometric template. The codeword and the template are XOR-ed, and the resulting n-bit string is stored into helper data along with the hashed value of the key. On verification, a fresh biometric template is XOR-ed with the stored string, and the result is decoded by the ECC. If the code word obtained coincides with the enrolled one (this is checked by comparing the hashed values), the k-bit key is released. If not, a failure is declared.

F. ECC Syndrome

In this spinoff of the Fuzzy Commitment scheme, a so-called ECC syndrome of (n-k) size is stored in the helper data.

G. Fuzzy Vault

This is, probably, the only BE scheme that is fully suitable for unordered data with arbitrary dimensionality, such as fingerprint minutiae. A secret message (i.e. a key) is represented as coefficients of a polynomial in a Galois field, for example, GF(216). In the most advanced version, the 16-bit x-coordinate value of the polynomial comprises the minutia locations and the angle, and the corresponding y-coordinates are computed as the values of the polynomial on each x. Both x and y numbers are stored alongside with chaff points that are added to hide real minutiae. On verification, a number of minutiae may coincide with some of the genuine stored points. If this number is sufficient, the full polynomial can be reconstructed.

IV. SIMPLE HASH FUNCTION USING BIOMETRIC AUTHENTICATION

A. Requirements of a Hash Function

The purpose of a Hash function is to produce a „fingerprint" of a file, message, or block of data. To be useful for authentication applications, a hash function H must have the following properties:

- H can be applied to a block of data of any size
- H produces a fixed length output.
- H(M) is relatively easy to compute for any given message M, making both hardware and software implementations practical
- For any given value h, it is computationally infeasible to find M such that H (M) =h. This is known as one way property.
- For any given message M, it is computationally infeasible to find Y ≠ M such that H (Y) = H(M)

B. Simple hash Function

All hash functions operate using the following general principles. The input is viewed as a sequence of n bit blocks. The input is processed one block at a time to produce n bit Hash function. One of the simplest hash functions is the bit – by- bit exclusive OR of every block. This operation produces a simple parity for each bit position and is known as longitudinal redundancy check. In our work, we have proposed the use of centroids values and singular values as hash values for the authentication of Biometric Templates. This hash values are of smaller size than the original image. Every image will have its unique hash value.

C. K-means based Hash Value for Authentication

K-means is one of the simplest unsupervised learning algorithms that solve the well-known clustering problem. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed a priori. The steps for generating Hash values using K means approach are

- Place k points into the space represented by the objects that are being clustered. These points represent initial group centroids.
- Assign each object to the group that has the closest centroid.
- When all objects have been assigned, recalculate the positions of the k centroids
- Arrange the centroids as N_1 N_2 N_3… N_k. If there are 8 clusters, there will be 8 centoids vales.
- These k centroids will be stored in password protected MySQL server

D. SVD based Hash Value for Authentication

The singular value decomposition of image A is a decomposition of the form A = UDVT Where A is m x n matrix; U and V are orthogonal matrices. D is a diagonal matrix of singular values; the singular values appear in descending order along the main diagonal of D. The singular values are obtained by taking the square root the of Eigen values of AAT and ATA. Hence the image A can be represented as The U and V vector are calculated as the Eigen vectors of AAT and ATA respectively. The square roots of the Eigen values are the singular values along the diagonal of the matrix D. Since our signature is resized to 128 x 256, we get a total of 128 singular values out of which we consider the first few values as hash values. 0 ..... 3 2 1 … n

- Find out the singular values of the templates.
- Consider the top „k" singular values.
- These k singular values will be stored as the reference hash values

V. CANCELABLE BIOMETRIC BASED SCHEMES

Cancelable Biometrics (CB) consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain .To prevent impostors from tracking subjects by cross-matching databases it is suggested to apply different transforms for different applications[5]. Two main categories of CB are distinguished.

A. Non-Invertible Transforms

In these approaches biometric data is transformed applying a non-invertible function .In order to provide updatable templates parameters of the applied transforms are modified. The advantage of applying non-invertible transforms is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. However, applying non-invertible transforms mostly implies a loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align (like in BCSs) in order to perform a proper comparison and, in addition, information is reduced.

B. Biometric Salting

Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. Any invertible transform of biometric feature vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal. As a consequence, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform (which can be seen as a secret

seed have to be presented at each authentication. Impostors may be able to recover the original biometric template in case transform parameters are compromised, causing a potential performance decrease of the system in case underlying biometric algorithms do not provide high accuracy without secret transforms.

C. Open Issues and Challenges

One fundamental challenge, regarding both technologies, represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within both technologies, i.e. alignment of obscured templates without leakage is highly non-trivial. While for some biometric characteristics (e.g. iris) alignment is still feasible, for others (e.g. fingerprints) additional information, which must not lead to template reconstruction, has to be stored. Within conventional biometric systems align-invariant approaches have been proposed for several biometric characteristics. So far, hardly any suggestions have been made to construct align-invariant BCSs or CB. practical error correction codes are designed for communication and data storage purposes such that a perfect error correction code for a desired code length has remained evasive (optimal codes exist only theoretically under certain assumptions.

VI. MULTI-MODAL AND HYBRID BASED SCHEMES

In multi-model combining two biometric traits, e.g. face and fingerprint etc. Hybrid based including both biometric encryption and cancelable biometrics scheme. A fuzzy extractor uses error correction code to recover a uniform random string with the assistance of helper data [1].

VII. SC BASED SCHEMES

SC based PPBSs can achieve higher level of privacy and verification accuracy as they utilize well-established encryption algorithms. They client and server engage in a biometric verification process but not reveal to each other any biometric data. Biometric feature set is encrypted using holomorphic encryption via a public key [3]. The public key is only used for encryption and it cannot be employed for decryption. The encrypted biometric feature set is stored in a data base .In a biometric based verification system, a large amount of helper data corresponding to different users is often stored in the database .If the system wants, it can track or monitor a user's activity with respect to verification. Then using garbled circuit, it allows the evaluation of binary circuits, such as the circuits made up by AND and OR gates.

VIII. COMPARISONS OF PPBS BASED ON STORAGE

PPBSs	*STORAGE*
1) Biometric encryption based schemes	*Secret key hash value is combined with discrete features of biometric data.*
2) Cancelable biometric based schemes	*Biohash value stored.*
3) Multi-modal and hybrid based schemes	*Two biometric trails are stored.*
4) Secure computation(SC) based schemes	*Encrypted biometric features are stored.*

IX. COMPARISONS OF PPBS BASED ON USING METHODS

PPBSs	*METHODS*
1) Biometric encryption based schemes	*Fuzzy vault and fuzzy extractor*
2) Cancelable biometric based schemes	*Bio hashing and Non-invertible transform.*
3) Multi-modal and hybrid based schemes	*Fuzzy extractor*
4) Secure computation(SC) based schemes	*Holomorphic and garbled circuit.*

X. CONCLUSION

The biometric encryption based schemes are better than other PPBS.A discrete feature set is extracted from the original biometric signal and a secret key is combined with the biometric feature set through a binding algorithm. The resulting representation and the hash value of the key are stored in the database but the biometric feature set and the key are discarded. Binding should be performed in a secure way such that neither the key nor the biometric information can be retrieved, even when the stored data is compromised. In the verification process, if the presented biometric signal is sufficiently close to the stored biometric data.

REFERENCES

[1] Iynkaran natgunanathan, abid nmehmood, yong xiang, (Senior dmember, IEEE),gleb beliakov, gsenior member, ieee), and john vbyearwood Protection of Privacy in Biometric Data School of Information Technology, Deakin University, HJGeelong, VIC 3220, AustraliaCorresponding author: Y. F)
[2] Handbook of Biometrics. A. K. Jain, P. Flynn, and A. A. Ross, New York,GNY, USA: Springer, 2008.

[3] R. Belguechi, E. Cherrier, V. BNAlimi, P. Lacharme, and C. BNAn Overview on Privacy BNPreserving Biometrics. Rijeka, Croatia: InTech,2011.
[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, ``Enhancing security and privacy in biometrics-basedVauthentication systems," IBM Syst. J., Bvol. 40,no. 3, pp. 614_634, Apr.2001
[5] C. Rathgeb and A. Uhl, ``A survey on biometric cryptosystems and cancelable biometrics' 'EURASIP J. Inf. Secur., p. 3, Sep. 2011
[6] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, ``Secure biometrics:Concepts, authentication architectures and challenges," IEEE Signal Process. Mag., vol. 30, no. 5, pp. 51_64, Sep. 2013.
[7] J. Bringer, H. Chabanne, and A. Patey, ``Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," IEEE Signal Process. Mag., vol. 30, no. 2, pp. 42_52, Mar. 2013.
[8] A. Cavoukian and A. Stoianov, ``Biometric encryption," Encyclopedia of Cryptography and Security. New York, NY, USA: Springer, 2009.