Techniques for Privacy Preservation

Aswini Prasad
PG Student
Department of Communication Engineering
Mount Zion college of engineering

Abstract

A form of biometrics, also called Biometric Encryption or BioCryptics, in which the proves is protected against the misuse of template data by a dishonest verifier. Biometric identification requires that a verifier searches for matches in a data base that contains data about the entire population. This introduces the security and privacy threat that the verifier who steals biometric templates from some (or even all) persons in the data base can perform impersonation attacks. When a private verification system is used on a large scale, the reference data base has to be made available to many different verifiers, who, in general, cannot be trusted. Information stolen from a data base can be misused to construct artificial biometrics to impersonate people. Creation of artificial biometrics is possible even if only part of the template is available. To develop an insight in the security aspects of biometrics, one can distinguish between verification and private verification. In a typical verification situation, access to the reference template allows a malicious verifier to artificially construct measurement data that will pass the verification test, even if the prover has never exposed herself to a biometric measurement after the enrollment. In private verification, the reference data should not leak relevant information to allow the verifier to (effectively) construct valid measurement data. Such protection is common practice for storage of computer passwords. When a computer verifies a password, it does not compare the password typed by the user with a stored reference copy. Instead, the password is processed by a cryptographic one-way function F and the outcome is compared against a locally stored reference string F(y). So y is only temporarily available on the system hardware, and no stored data allows calculation of y. This prevents attacks from the inside by stealing unencrypted or decrypt able secrets. Biometric verification is defined as the verification of a individual based on the physical, chemical or behavioural 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- Bio Cryptic, privacy-preserving biometric schemes, biometric encryption, cancellable biometric, hybrid based, multimode, secure computation

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance .Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice ,Some researchers have coined the term behavior metrics to describe the latter class of biometrics. More traditional means of access control include token-based identification systems, such as a driver's license or passport and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information 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 enrolment stage, a user provides a biometric signal as an input. The important features of the biometric signal are extracted using a feature extraction module. We denote the extracted biometric features set by x. In order to protect the privacy of biometric data, x will not be stored in a database. Instead, x is processed in certain ways to produce the so-called helper data, denoted by v. The helper data v is stored in a database and plays an essential role at the verification stage. This process should be designed in such a way that it is almost impossible to retrieve x from v, which greatly protects the privacy of biometric data. In these PPBSs, only the biometric sample is required to perform identity verification at the verification stage. On the other hand, some PPBSs employ a secret key sk , in different manners, to further enhance the protection of biometric data privacy. In some cases, the altered version of the secret key h(sk) is also stored in the database. In PPBSs, where secret key is used in and the secret key are needed at the verification stage. At the verification stage, the received biometric signal, together with the secret key in the case of two factor verification schemes, is used to extract the biometric features and then produce the helper data. We denote the biometric feature set and helper data obtained at the verification stage by x 0 and v 0 , respectively. Based on the similarity between v 0 and its counterpart v obtained at the enrolment stage and stored in the database, one decides whether a legitimate user or an adversary is present. In some schemes, at the verification stage, a secret key s 0 k is generated from the received biometric signal and the stored helper data. Then the altered version of the generated secret key h(s 0 k) is obtained. For verification, h(s 0 k) and its counterpart h(sk) are compared. It defined three metrics to compare the similarity between two binary vectors: Hamming distance metric, set difference metric and edit difference metric. 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. 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.

- 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

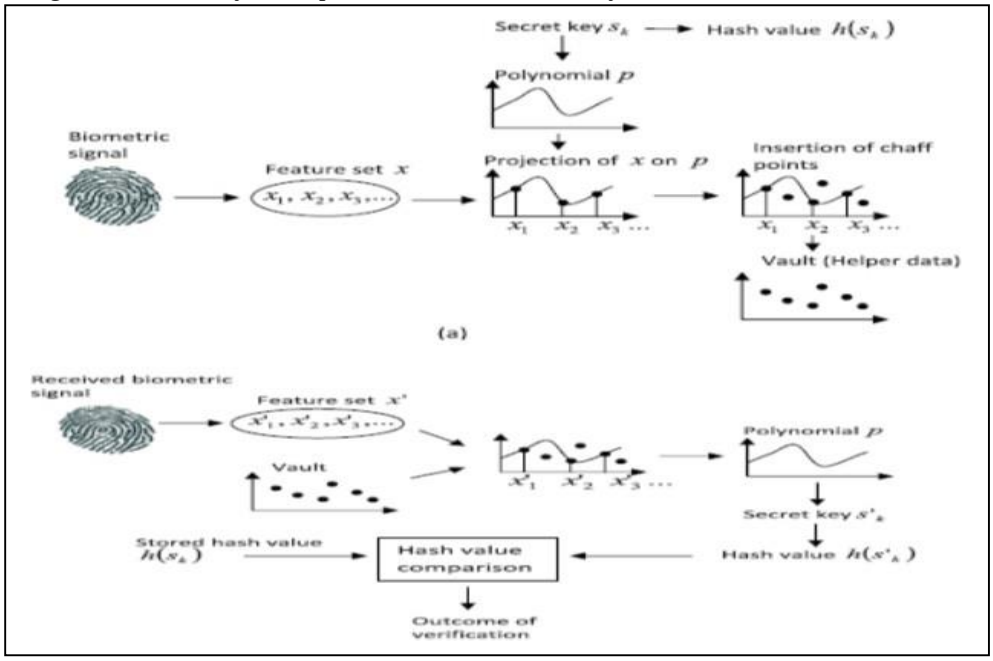

Fig. 1: Key Binding Mode using fuzzy Walt

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.

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.

B. Possible applications of BE

- Biometric boarding cards for travel
- Drug prescriptions
- Three-way check of travel documents
- Identification, credit, and loyalty card systems
- Consumer biometric payment systems
- Remote authentication via challenge-response scheme
- Access control (physical and logical)
- Personal encryption products

III. CANCELABLE BIOMETRIC BASED SCHEMES

A bio hashing process consists of two steps. In the first step, a pre-processing is carried out on the biometric feature set in order to make the biometric feature invariant to small variations in the input biometric signal. For example, in the case of face biometrics, Fourier-Mellon transform can be used to make the feature vector invariant to geometric variations such as rotation and translation. In the second step, a user specific secret key is used to generate a random vector. Then, a bio hash value is generated by comparing the inner product of the generated random vector and the feature vector extracted against a predefined threshold. Fig. 4 shows the block diagram of generating bio hash value. At the verification end, by following the process used at the enrolment stage, a bio hash value can be generated from the received biometric signal and the secret key given by the user. Afterwards, the verification is done by comparing the newly computed bio hash value with the stored bio hash value. Some representative PPBSs based on bio hashing can be found. 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.

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.

IV. MULTI-MODAL AND HYBRID BASED SCHEMES

It combines two biometric traits, e.g., ear and face, face and fingerprint, etc. help deal with problems like intra-class variability, inter-class similarity, data quality and sensitivity to noise. Solving or moderating these problems in return improves verification accuracy. By combining diverse biometric traits in different ways, various multi-modal based PPBSs have been developed. The PPBS combines fingerprint and voice using fuzzy logic. The face and online handwritten signature were combined using linear discriminant analysis. To ensure that the significant features were used in a balanced manner, a genetic algorithm with modified fitness function was utilized. Nadheen et al. employed principle component analysis to extract features from ear and iris, and the extracted biometric features were jointly exploited using the score level fusion 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].

A. 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 OR gates. In SC based PPBSs using holomorphic encryption, the biometric feature set is encrypted using holomorphic encryption via a public key. 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. During the verification phase, the biometric feature set of the received biometric signal is extracted and then encrypted using the public key. Verification is conducted by comparing the similarity, by means of a distance matrix, between the received encrypted feature set and the stored encrypted feature set. A privacy-preserving comparison protocol is used to determine whether the distance is below a threshold or not and only the verification system knows the threshold. Due to the usage of holomorphic encryption, the similarity between the biometric signals used in enrolment and verification processes is reflected in their encrypted counterparts. This is vital as the biometric feature sets used in enrolment and verification processes are not going to be identical due to noise and misalignments.

V. 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.*

VI. 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	*Homomorphic and garbled circuit.*

VII. 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 vbyearwoodGProtection of Privacy in BiometricDataSchool of Information Technology, Deakin University, HJGeelong, VIC 3220, AustraliaCorresponding author: Y. F)
[2] JHandbook 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 andprivacy 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 biometricidentification 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 ofCryptography and Security. New York, NY, USA: Springer, 2009.