International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

A Survey on Biometric Template Protection

Laxmi Menaria*[1], Kalpana Jain[2]

*[1]Department of Computer Science and Engineering, College of Technology and Engineering, Udaipur, Rajasthan, India
[2]Assistant Professor, Department of Computer Science and Engineering, College of Technology and Engineering, Udaipur, Rajasthan, India

ABSTRACT

Biometric authentication offers most reliable approach to person authentication. This authentication approach is based on the 'what you are' security measure. However, biometric templates are vulnerable to different types of attacks and any data leakage cause privacy risks. Unlike passwords, stolen biometric data cannot be revoked or reissued hence biometric templates must be protected and any leakage of biometric information must be prevented. This paper surveys various biometric template protection schemes.

Keywords : Biometric Template Protection, Biometric Cryptosystem, Cancelable Biometrics, Bloom Filter, Honey Template.

I. INTRODUCTION

Biometric authentication is a technique which recognized a person based on his physiological or behavioural traits. The behavioural traits include *signature, voice, DNA* and physiological traits include *fingerprint, palm print, face, Iris, hand geometry* [1]. There are five major components in a generic biometric authentication system: sensor, feature extractor, template database, matcher and decision module (Figure 1). Sensor is the interface between the user and the biometric authentication system, it is used to scan the biometric trait of the user. Feature extraction module extracts the feature set from the scan biometric traits. In some cases, the feature extractor is preceded by a quality assessment module which determines whether the scanned biometric trait is of sufficient quality for further processing. Biometric systems have two stages *enrollment* and *verification* stage [2]. At enrollment, biometric sample of a new user is stored in the database as a template (X_T). During authentication, the matcher compares the biometric template (X_Y) presented by user with the stored template (X_T). According to score outputted by matcher, decision module takes decision. If $S(X_{T,}$ XQ) >= t then authentication claim is true otherwise it is false, here S represents the score of comparison and t represents the threshold value used by decision module. Biometric system works in two modes: (i) *verification mode* (one to one comparison) - In this mode biometrics can be used to verify a person's identity. (ii) *Identification mode* (one to many comparison) - In this mode biometrics can be used to determine a person's identity, even without that person's knowledge [1].

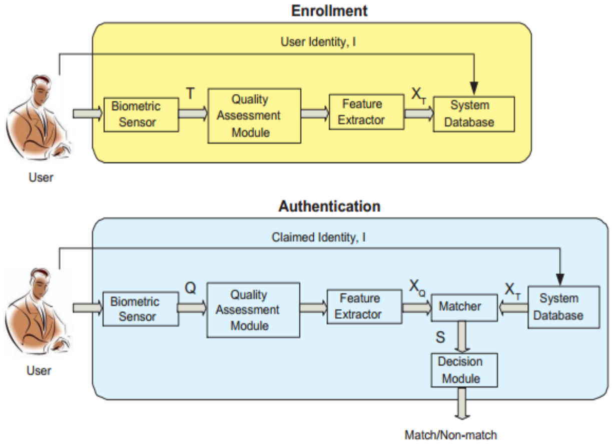

Figure 1: Biometric system enrollment and authentication stages [2]

Biometrics are very sensitive personal information and tightly linked with a person, any information leakage cause severe security risks hence any information leakage related to biometric data must be prevented. The stolen biometric data can be used in spoof attacks,

CSEIT1722303 | Received : 16 April 2017 | Accepted : 24 April 2017 | March-April-2017 [(2)2: 995-999]

replay attacks, *function creep* [3] or cross matching in which biometric template is used in application other than the registered application.

To prevent such types of attacks, various types of biometric template protection schemes are proposed in previous researches. In biometric template protection, the original biometric sample of user is not stored in the database, instead a secure template is stored which is obtained after applying biometric template protection schemes (BTPS). These stored templates include protected biometric information and other values such as helper data. The international standard ISO/IEC 24745 [4] gives two types of properties for the biometric template protection:

> *Irreversibility:* It should not be possible to reconstruct a biometric sample from protected template which is positively authenticated by the biometric system.
>
> *Unlinkability:* If a same user is enrolled in different applications then on given protected template of these applications it should not be possible to determine that this template belong to same subject.

A biometric template protection scheme must satisfy these two properties with no recognition performance degradation.

This survey is organized as follows: a brief introduction to categories of BTPS is presented in section 2. A review on biometric cryptosystem (section 3) and Cancelable biometrics (section 4) is given. In section 5, the recently proposed BTPS based on honey template and bloom filter is discussed and lastly, Section 6 concludes this survey.

II. CATEGORIES OF BTPS

According to ISO/IEC 24745 standard [4], the protected template contains two element *pseudonymous identifier (PI)* and *auxiliary data (AD).* PI represents the protected information of biometric template. AD is used to regenerate the PI at verification time. BTP schemes are categorized into two parts depending on how these two elements are generated: (i) *Biometric cryptosystems (BCSs)* (ii) C*ancelable biometrics* (figure 2). In biometric cryptosystems either key is extracted from the biometric template or it is bind with the biometric template [5]. In BCSs some public information called helper data [2] is derived from the biometric sample and stored in database. During authentication, helper data is used to reconstruct the key from input biometric data and comparisons are performed indirectly by validating keys. Depending on how helper data is generated BCSs are categorized as *Key generation* and *key binding* schemes [2]. In key binding scheme, a secret key binds with the biometric template to obtain the helper data. In key generation scheme, helper data is extracted from the biometric template and key is generated from the helper data and input biometric template. (ii) In C*ancelable biometrics* biometric sample is transformed using a transformation function and this transformed template is stored in the database [6]. User specific parameters (keys or password) are used to derive the parameters of transformation function. During authentication, comparison of biometric template is performed in the transformed domain. Depending on the characteristics of the transformation function, the cancelable biometrics scheme can be further categorized as *salting* and *non-invertible transform*. In salting, the transformation function is non-invertible, if an attacker gains access to user-specific parameters and biometric template, he can recover the original biometric template hence the key or passwords must be kept secret. In non-invertible transform, a one way function is applied to biometric data and it is computationally hard to recover a transformed template even if the key or password is known.

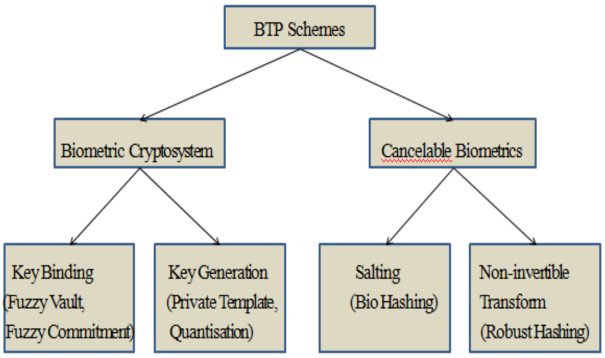
BTP Schemes
Biometric Cryptosystem
Cancelable Biometrics
Key Binding (Fuzzy Vault, Fuzzy Commitment)
Key Generation (Private Template, Quantisation)
Salting (Bio Hashing)
Non-invertible Transform (Robust Hashing)

Figure 2: Categories of biometric template protection schemes

III. BIOMETRIC CRYPTOSYSTEMS

In fuzzy vault scheme [7], the biometric data is hidden by polynomial and error correcting codes. In this scheme, a secret key is secured using an unordered feature set ‘A’ extracted from biometric sample. This secured key generates vault. If another set ‘B’, which is used to unlock vault, is largely overlap with set A, then vault is unlocked. The fuzzy vault scheme is applied to fingerprint [8], in which 128 bits key is used to generate vault. Wu et al. [9] proposed the fuzzy vault scheme for face. Fuzzy commitment scheme [10] is based on error correcting codes. In this scheme, an error correcting codeword ‘c’ and a witness ‘x1’ is used, where witness ‘x1’ is biometric data. The helper data is formed by (x1-c) and hash value of c (h(c)). This helper data is stored in the database. At verification, witness ‘x2’ is presented, which is used to reconstruct the codeword ‘c’ by subtracting (x1-c) from ‘x2’. A successful reconstruction of codeword c shows successful authentication.

Davida et al. [11] proposed the private template scheme, which was applied to iris. In this scheme, biometric template itself is used as a secret key. Helper data which are error correction check bits, are used for correcting the erroneous bits of a given iris code. Rathgeb and Uhl [12] proposed the quantization scheme, which has been applied to iris and generating 128 bits keys. The quantization scheme process feature vectors out of several enrolled samples and derive appropriate intervals for each feature element. These feature intervals are encoded and used as helper data. At authentication, to generate hash or key, biometric characteristics are measured and mapped into the previously defined intervals.

IV. CANCELABLE BIOMETRICS

In BioHashing approach secret tokens are blended with biometric data to derive a distorted biometric template. At authentication secret user-specific tokens have to be presented to generate biometric hashes. Kong et al. [13] presented an implementation of BioHashing, which was applied to face. In robust hashing [14] biometric data is secured by applying non invertible (one way) transformation. For generating different transformation of data, polynomials generated by template are used. This scheme uses cryptographic hashes for providing the diffusion property.

In 2013, Rathgeb et al. [15] introduced cancelable biometrics based on Bloom filters, which has been applied to different biometric characteristics. Bloom filters are data structures which are used in membership queries. In [15] bloom filter based protection scheme has been applied to iris. In this scheme bloom filters are used to obtain alignment free cancelable iris biometric data. This bloom filter based protection provides irreversibility and unlinkability properties. In this scheme, unlinkability is provided by application specific secret values and irreversibility is provided by mapping multiple codewords to an identical position. In [16] bloom filter based biometric template protection scheme has been applied to face, which generate the irreversible facial template while maintaining the system recognition performance. In this protection scheme, Local Gabor Binary Pattern Histogram Sequence (LGBPHS) algorithm is used to extract the facial features. Rathgeb et al. [17] extended the scheme of [15] to achieve biometric template protection, data compression and efficient identification. Biometric template protection is obtained by irreversible transformation of template. Biometric data compression is obtained by transforming the template to a limited size of bloom filter. Efficient identification is obtained by alignment free transformations which reduce the identification response time. In [18] authors presented an implementation of cancelable multibiometrics. In this scheme bloom filter-based transforms are applied in order to mix binary iris biometric templates at feature level, where iris-codes are obtained from both eyes of a single subject. This scheme provides the irreversibility and unlinkability security requirements. Rathgeb et al. [19] proposed the multi-biometric template protection scheme based on face and iris. In this scheme, template protection is provided by mixing the bloom filter based transformed features of face and iris. This protection scheme provides the irreversibility property. In [20] bloom filter based transformation has been applied to fingerprint and address the challenges of variable size and length of fingerprints. In this scheme, before generating binary sample a pre- alignment is done which select the minutiae points inside a particular area. In [21] authors proposed an irreversible fingerprint template creation technique using minutiae relation code (MRC) and bloom filters. MRC consists of a set of vector-represented relation information between arbitrary minutiae, which enables to create a useful fingerprint template by handling boarder minutiae and isolated minutiae efficiently. Bloom filters are used to realize the irreversibility feature. In [22] security analysis of schemes proposed in [15, 17] shows that these schemes does not achieve unlinkability property.

In [23] security analysis is performed with non-uniformity and variability between captures and it is shown that protection scheme proposed in [15] leaked protected data. To overcome these security issues, Gomez-barrero et al. [24] proposed a new scheme which provides an improved security framework for analysis of the unlinkability and irreversibility properties. In this proposed scheme, to prevent cross matching attacks, authors re-design the original bloom filter based template protection scheme and use an additional processing step, which is referred to as *structure preserving feature rearrangement*. This new scheme has been applied to the face corpus and it is shown that the proposed scheme maintains the biometric performance of the unprotected system and achieves the cross matching resistance.

V. HONEY TEMPLATE BASED BTPS

Honey templates are used to enable the detectability of leaked template and to prevent masquerade attacks. The idea of honey template is taken from the ‘’honeyword’’ [25] approach which is used to detect the leakage of stored password. In this approach, hashes of false passwords (honeywords) are stored with the hash of real password (sugarword).

In 2015, Yang et al. [26] proposed honey template based template protection scheme to detect the biometric template database leakage. In this protection scheme, machine learning based classification algorithms are used to generate the sugar and honey templates. Unlike password, biometric data once compromised cannot be renewed, hence to provide renewability property hash based BTPS scheme is required in honey template based protection scheme. In [27] the honey template based protection scheme was applied to face. Martiri et al. [28] proposed a general biometric template protection scheme based on honey template and bloom filters. This scheme has been applied to publicly available BioSecure Multimodal database and provides unlinkablity, irreversibility security requirements and prevents the masquerade attacks.

VI. CONCLUSION

In this paper a survey of biometric template protection schemes (BTPS) and categories of BTPS (biometric cryptosystems and cancelable biometrics) is presented. These biometric template protection schemes provide the irreversibility, unlinkability properties of security and preventing the cross matching attacks. Honey template based biometric template protection scheme adds an extra layer of protection to prevent the masquerade attacks.

VII. REFERENCES

[1]. Jain, A.K., Ross, A., Prabhakar, S.: ‘An introduction to biometric recognition’, IEEE Trans. Circuits Syst. Video Technol., 2004, 14, pp. 4–20

[2]. Jain, A.K., Nandakumar, K., Nagar, A.: ‘Biometric template security’, EURASIP J. Adv. Signal Process., 2008, pp. 1–17

[3]. A. K. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[4]. ISO/IEC JTC1 SC27 Security Techniques, ISO/IEC 24745:2011: ‘Information technology – security techniques – biometric information protection, International Organization for Standardization, 2011, 14

[5]. Uludag, U., Pankanti, S., Prabhakar, S., et al.: ‘Biometric cryptosystems: issues and challenges’, Proc. IEEE, 2004, 92, (6), pp. 948–960

[6]. Ratha, N., Connell, J., Bolle, R.: ‘Enhancing security and privacy in biometrics-based authentication systems’, IBM Syst. J., 2001, 40, (3), pp. 614–634

[7]. Juels, A., Sudan, M.: ‘A fuzzy vault scheme’, Des. Codes Cryptogr., 2006, 38, (2), pp. 237–257

[8]. Nandakumar, K., Jain, A.K., Pankanti, S.: ‘Fingerprint-based fuzzy vault: implementation and performance’, IEEE Trans. Inf. Forensics Sec., 2007, 2, pp. 744–757

[9]. Wu, Y., Qiu, B.: ‘Transforming a pattern identifier into biometric key generators’. Proc. Int. Conf. on Multimedia and Expo, ICME, 2010, pp. 78–82

[10]. A. Juels and M. Wattenberg, “A Fuzzy Commitment Scheme,” in Proceedings of Sixth ACM Conference on Computer and Communications Security, Singapore, November 1999, pp. 28-36

[11]. Davida G, Frankel Y, Matt B, “On the relation of error correction and cryptography to an off line biometric based identication scheme”, Proc of

WCC99, Workshop on Coding and Cryptography 1999, 129-138

[12]. Rathgeb C, Uhl A: An iris-based interval-mapping scheme for biometric key generation. Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09 2009.

[13]. Kong, A., Cheunga, K.-H., Zhanga, D., et al.: 'An analysis of BioHashing and its variants', Pattern Recognit., 2006, 39, (7), pp. 1359–1368

[14]. Y. Sutcu, H. T. Sencar, and N. Memon, "A Secure Biometric Authentication Scheme Based on Robust Hashing," in Proceedings of ACM Multimedia and Security Workshop, New York, USA, August 2005, pp. 111–116.

[15]. Rathgeb, C., Breitinger, F., Busch, C.: 'Alignment-free cancelable iris biometric templates based on adaptive bloom filters'. Proc. Int. Conf. On Biometrics, ICB, 2013, pp. 1–8

[16]. Gomez-Barrero, M., Rathgeb, C., Galbally, J., et al.: 'Protected facial biometric templates based on local Gabor patterns and adaptive bloom filters'. Proc. Int. Conf. on Pattern Recognition, ICPR, 2014, pp. 4483–4488

[17]. Rathgeb, C., Breitinger, F., Busch, C., et al.: 'On the application of bloom filters to iris biometrics', IET Biometrics, 2014, 3, (1), pp. 207–218

[18]. Rathgeb, C., Busch, C.: 'Cancelable multi-biometrics: mixing iris-codes based on adaptive bloom filters', Comput. Sec., 2014, 42, (0), pp. 1–12

[19]. Rathgeb, C., Gomez-Barrero, M., Busch, C., et al.: 'Towards cancellable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris'. Proc. Int. Workshop on Biometrics and Forensics, IWBF, 2015, pp. 1–7

[20]. Li, G., Yang, B., Rathgeb, C., et al.: 'Towards generating protected fingerprint templates based on bloom filters'. Proc. Int. Workshop on Biometrics and Forensics (IWBF), 2015

[21]. Abe, N., Yamada, S., Shinzaki, T.: 'Irreversible fingerprint template using minutiae relation code with bloom filter'. Proc. Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS), 2015

[22]. Hermans, J., Mennink, B., Peeters, R.: 'When a bloom filter is a doom filter: security assessment of a novel iris biometric'. Proc. Int. Conf. of the Biometrics Special Interest Group, BIOSIG, 2014

[23]. Bringer, J., Morel, C., Rathgeb, C.: 'Security analysis of bloom filter-based iris biometric template protection'. Proc. Int. Conf. on Biometrics, ICB, 2015, pp. 527–534

[24]. Gomez-Barrero, M., Rathgeb, C., Galbally, J., et al.: 'Unlinkable and irreversible biometric template protection based on bloom filters', Inf. Sci., 2016, 370–371, pp. 18–32

[25]. Juels, A., Rivest, R.L.: 'Honeywords: Making password-cracking detectable'. Proc. ACM SIGSAC Conf. on Computer and Communications Security, 2013, pp. 145–160.

[26]. Yang, B., Martiri, E.: 'Using honey templates to augment hash based biometric template protection'. Proc. Int. Workshop on Secure Identity Management in the Cloud Environment (SIMICE), 2015

[27]. Martiri, E., Yang, B., Busch, C.: 'Protected honey face templates'. Proc. BIOSIG, 2015

[28]. Martiri, E., Gomez-Barrero, M., Yang, B., Busch, C.: 'Biometric template protection based on bloom filter and honey template'.IET Biometrics, 2017,6,(1),pp.19–2