Biometric Template Protection Scheme-Cancelable Biometrics

Vinit Kumar Gunjan, Puja S. Prasad and Saurabh Mukherjee

Abstract Biometric template is actually digital representation of the biometric features that are extracted by applying different algorithms on the captured images of different types of biometric modalities. This digital information is stored in a biometric database for identification and authentication purposes. The objective of this paper discussed about cancelable Biometric template protection scheme. The idea behind cancelable biometrics is intentionally and repeatedly alteration of biometric features in such a way so that the data or biometric features will be protected.

Keywords Cancelable biometrics · Non-invertible transform · Invertible transform · Bio hashing · Template

1 Introduction

Biometric recognition is one of the most demanding authentication process these days and act as access control systems as well as modern identity management. As due to the personal and permanent link between individuals and their biometric traits, it become very vulnerable to different types of attack. Exposure of already register biometric information to opponents can seriously compromise biometric privacy as well as security. Research have been going on for finding different methods for biometric template protection over the last two decades. As biometrics is a dominant tool against disclaimer and has been broadly used in numerous authentication systems [1]. The features obtained from biometric are primarily incontrovertible, and it results in compromise of permanent biometric data once it is stolen. Number of protection

V. K. Gunjan (✉)
CMRIT, Hyderabad, India
e-mail: vinitkumargunjan@gmail.com

P. S. Prasad
GCET, Hyderabad, India
e-mail: puja.s.prasad@gmail.com

S. Mukherjee
Banasthali Vidyapith, Banasthali, Rajasthan, India

A. Kumar and S. Mozar (eds.), *ICCCE 2019*, Lecture Notes in Electrical Engineering 570, https://doi.org/10.1007/978-981-13-8715-9_48

scheme are already on research in which one is cancelable biometrics. The main concept of cancelable biometric is that like password it can be cancelled and revoked and remain unique for every application.

Mobile biometrics has also come with new practice of risks. Number of different service providers like bank, financial organizations are now introduced biometric authentication in their apps [2, 3]. They use the concept of integrating fingerprint or face recognition to authenticate customers so that user access their services. But one of the most important concern is that the biometric data is movement of biometric data between user and the bank which creates an issue of compromising of the biometric data [4]. Another important concern is that the image capturing device used on mobile devices is very small in size so as well as low quality to take all the feature appropriately. For example, fingerprint recognition on mobile devices uses partial fingerprint recognition algorithm. The sensor itself is so tiny that it cannot accommodate the whole fingertip. These risks with mobile biometrics can only be mitigated with continuous research and development [5].

One of the main concern of cancelable biometrics is that it needs storage for the distorted biometric template which actually offer very high privacy level by permitting multiple biometric templates to be linked with the same biometric sample [6]. This has one advantage of non-linkability of user's biometric data kept across numerous databases.

Cancelable biometric is one of the major category including biometric cryptosystem for biometric template protection scheme [7, 8]. As cancelable feature is compromised, the distortion features are changed and this biometric is mapped to a new template and used afterwards (Fig. 1).

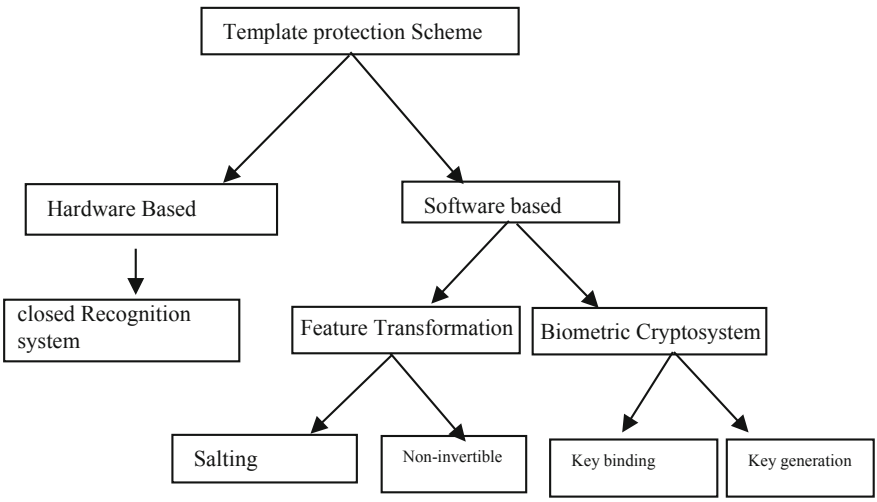

Fig. 1 Types of biometric template protection scheme

Template protection schemes generally categorized as Helper data based schemes also called biometric cryptosystems and feature transformation called cancelable biometrics [9]. Both of these schemes has to meet two main requirements-

(i) **Irreversibility**: Reconstruction of original biometric template should be computationally hard from the already saved reference data or we say protected template, but it would be easy to make the protected biometric template.
(ii) **Unlinkability**: From the same biometric data different version of biometric template created called renewability but cross matching should not have allowed.

2 Cancelable Biometric

Cancelable biometric alters are the result of systematically and intentional distortion of biometric features in order to shield subtle user biometric data. The transform biometric aimed in a way that it should be computationally very hard to recuperate the original biometric data [10, 11]. The main strength (individuality) of biometric features or characteristics should not be reduced when applying transforms while on the other hand transforms should be tolerant to intra-class variation (Fig. 2) [9].

Correlation of numerous transformed templates essentially not disclose any evidence about the distinctive biometrics (unlinkability) [12]. As soon as transformed biometric compromised, transformation parameters are changed, and the corresponding biometric template is updated. There are two key technique of transformation in order to protect from imposter and to make more robust biometric template scheme.

A. Non-invertible Transform-Non-invertible function are applied to construct the transform biometric template. Main benefits of smearing non-invertible function

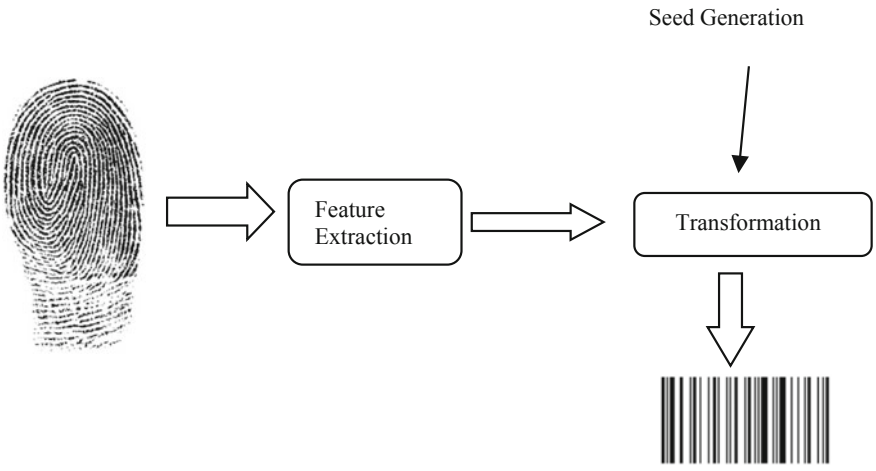

Fig. 2 Seed generation and transformation for biometric template protection

are potential imposter as well as not able to rebuild original biometric data once biometric datasets compromised. One of the disadvantage of non-invertible transform is it reduces accuracy of the overall system. Performance of the system reduces as less information regarding biometric feature are there for comparison.

B. Invertible Transform- Also called biometric salting. It involves transformation of biometric template using invertible function which means biometric template is transformed into original form. As a result, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform have to be presented at each authentication [13, 14]. If the transform parameters are compromised the impostors may be able to recover the original biometric template which result a possible performance decrease of the system in case primary biometric algorithms do not deliver high correctness without undisclosed transforms.

3 Invertible Transforms

Biometric Salting comes under Invertible transformation. Biometric salting is very much alike to password salting used in cryptography. It consists of random bits R_b which is combine with secret key K and it is taken as input factor (Fig. 3) [9].

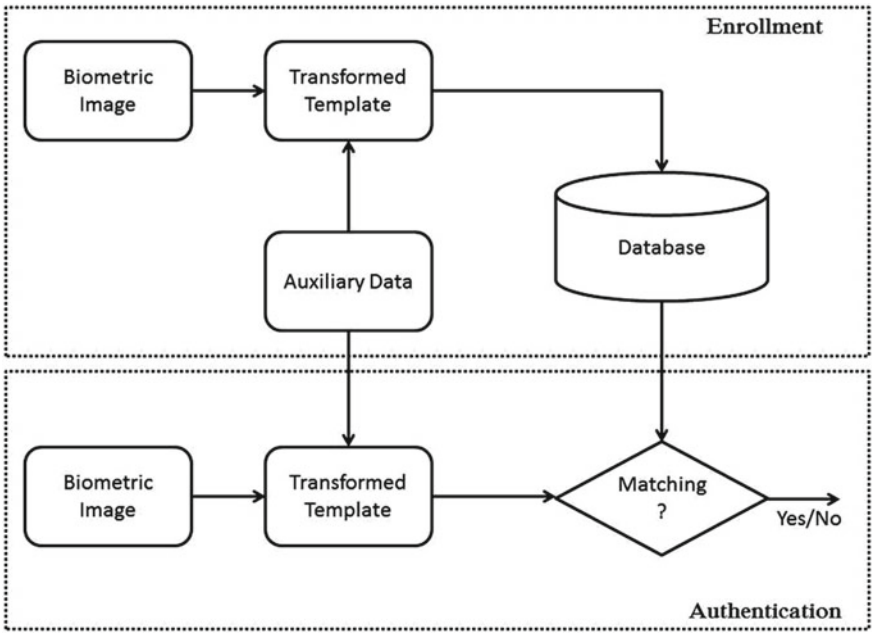

Fig. 3 Biometric salting

The output is repeatedly stored as Hash $H(R_b + K)$ as template. In this process Distorted Biometric template is obtained by combining user specific independent input factor with the biometric data, by using biometric salting process [2]. This data is invertible in nature so it easily revoked and changed so it requires maximum security protection.

Biohashing is one of the example of biometric salting which uses random projection [7, 12].

In this a random matrix R having size $a * b$ is generated in which Gram-Schmidt process of orthonormalization is carried to make b column orthonormal and finally extracted feature vector is projected with the threshold value. This techniques are used with many modalities like speech, face, fingerprint. But the performance of the Bio hash degrades when the token is stolen. For this reason, bio hashing is basically a quantized under-determined linear equation which would be partially solved using pseudo-inverse operation.

Teoh and Chong proposed Multistage random projection was also there that address the problem of performance of stolen token in both theoretical and experimental analysis [15].

Lumini et al. perform Bio Hashing under different threshold value for Stolen token scenarios by fusing the scores [16]. Different researcher works on biometric salting scheme on different biometric features. In one of the technique which uses feature vectors of face image extracted from Principal Component Analysis and Independent Component Analysis from a face image and these are then normalized and then permuted using token-derived permutation. Once it was compromised, by changing permutation matrix new feature vector can be generated.

4 Non-invertible Transform

Non-invertible transformation process involves many-to-one function. The function F is used to modify an unrefined biometric data purposely into a new type within the framework of signal space. The function F has act as main agent that transform the biometric template into non-invertible form which is reused and have diverse in nature. As f does not have directly deals with raw biometrics, the main benefit of this technique is that F does not need to be kept secret.

An understanding of non-invertible transform was first discussed Ratha et al. in which biometric fingerprint data is altered by a sequence of three non-invertible transformation functions. The three transformation functions are based on Polar, Cartesian

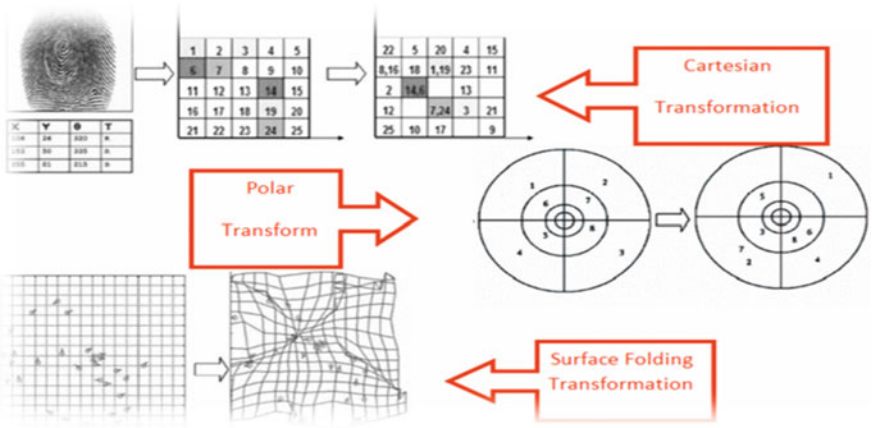

Fig. 4 Cancelable templates from different transforms (adopted from [9])

and surface folding transformation of the minutiae positions. The fingerprint minutia is arranged into rectangular grid in Cartesian transformation, with reference to positions of singular points. In polar transformation image is arrange into polar sectors and is similar to the Cartesian transformation. A mixture of 2D electric potential field and 2D Gaussians distributions are used in surface transformation to translate the minutiae points (Fig. 4).

5 Conclusion

Biometric Technology is one of the authentication techniques that uses different biometric feature for authentication of a person. It grows exponentially during last decades. As biometric is permanently associated with person there is more concern towards security of biometric template. In this paper we discuss about different biometric template protection scheme. One scheme is related to cryptography and other is related to the transformation techniques also called cancelable biometric. We also discuss different invertible and non-invertible transformation techniques. Salting or bio hashing algorithm are also applied in different biometric features for their protection. In this paper we also discuss the effect of performance of the biometric system after applying different protection mechanism. One of the future scope is to develop a non-invertible function for biometric feature transformation that assure non-invertibility requirements as well as performance.

References

1. Prasad PS, Devi BS, Reddy MJ, Gunjan VK (2018) A survey of fingerprint recognition systems and their applications. In: International conference on communications and cyber physical engineering 2018. Springer, Singapore, pp 513–520
2. Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 2011(1):3
3. Ratha N, Connell J, Bolle RM, Chikkerur S (2006) Cancelable biometrics: a case study in fingerprints. In: IEEE 18th international conference on pattern recognition (ICPR'06), vol 4, pp 370–373
4. Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. EURASIP J Adv Signal Process 1(2008):113
5. Prasad PS (2016) Efficient secure authentication using multi biometric cryptosystems
6. Bringer J, Chabanne H, Kindarji B (2008) The best of both worlds: applying secure sketches to cancelable biometrics. Sci Comput Program 74(1–2):43–51
7. Kong A, Cheung KH, Zhang D, Kamel M, You J (2006) An analysis of Bio Hashing and its variants. Pattern Recogn 39(7):1359–1368
8. Zuo J, Ratha NK, Connell JH (2008) Cancelable iris biometric. In: IEEE 2008 19th international conference on pattern recognition, pp 1–4
9. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572
10. Connie T, Teoh A, Goh M, Ngo D (2005) Palmhashing: a novel approach for cancelable biometrics. Inf Process Lett 93(1):1–5
11. Ang R, Safavi-Naini R, McAven L (2005) Cancelable key-based fingerprint templates. In: Australasian conference on information security and privacy. Springer, Berlin, Heidelberg, pp 242–252
12. Teoh AB, Ngo DC (2006) Biophasor: token supplemented cancellable biometrics. In: IEEE 2006 9th international conference on control, automation, robotics and vision, pp 1–5
13. Prasad PS, Baswaraj D (2018) Iris recognition systems: a review. In: International conference on communications and cyber physical engineering 2018. Springer, Singapore, pp 521–527
14. Prasad PS, Devi BS, Preetam R (2018) Image enhancement for fingerprint recognition using Otsu's method. In: International conference on communications and cyber physical engineering 2018. Springer, Singapore, pp 269–277
15. Chin CS, Jin AT, Ling DN (2006) High security iris verification system based on random secret integration. Comput Vis Image Underst 102(2):169–177
16. Teoh AB, Yuang CT (2007) Cancelable biometrics realization with multispace random projections. IEEE Trans Sys Man Cybern Part B (Cybern) 37(5):1096–1106