IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-2, Issue-7 E-ISSN: 2347-2693

Fingerprint Privacy Protection Techniques: A Comparative Study

Aafa J S*
Dept. of CSE
SCT College of Engineering
Trivandrum, Kerala
aafa.1161@gmail.com

Soja Salim
Dept. of CSE
SCT College of Engineering
Trivandrum, Kerala
sojasalim@gmail.com

www.ijcseonline.org

Received: 20 /06/ 2014 Revised: 30/07/ 2014 Accepted: 24 /07/ 2014 Published: 30 /07/ 2014

Abstract— Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. But they are vulnerable to attacks and fake fingerprints can be generated to login into the system anonymously. With the widespread applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint. This paper reviews some of the existing techniques which protect the privacy as well as security of the fingerprint systems.

Keywords: Minutiae, Security, Protection, Privacy

INTRODUCTION

Biometric authentication [1] is an automated system in which an individual's identity is confirmed by testing a behavioral characteristics or a physiological trait such as fingerprint, iris, face, signature etc. Behavioral characteristics are mostly influenced by controllable actions and less controllable psychological factors. One's signature, keystroke dynamics or voice comes under the behavioral characteristics. Major issue associated with these biometric templates is that it should be updated each time it is used since behavioral characteristics change over time. Behavior-based biometric is less expensive and less threatening to users. However, physiological traits offer higher security and accuracy to users. Biometric traits prevent theft or fraud because it is unique to each individual. A password or personal identification number can be easily lost, forgotten or stolen while a biometric template cannot be. There are lots of devices that provide access to users by scanning user's physiological or behavioral characteristics. These devices are used in several computer rooms, research labs, vaults, ATM, blood banks and military installations. Biometric traits currently in use are fingerprint, iris, face, palm and finger vein and voice pattern.

Among these, fingerprint recognition system [2] is heavily used and actively studied biometric technology. A fingerprint consists of number of ridges and valleys on its surface. Ridges are upper layer skin segment while valleys are lower layer segments. Ridges are collectively called minutiae points which consist of ridge endings and bifurcations. The uniqueness of an individual is characterized by pattern of ridges. However, the compromise of stored template is a vulnerability to fingerprint authentication system. Fake fingerprints can be made by an adversary by using the stolen templates thereby entered into the system. Both intrusion attack and linkage attack can be practiced in fingerprint biometric systems [3]. So ensuring the privacy and security of biometric system is necessary in order to gain public trust and acceptance thereby promoting the wide spread use of fingerprint authentication systems. The major requirements of biometric template protection are:

Irreversibility: It should be computationally difficult to recover the original template from the protected biometric template and at the same time it should be easy to construct the protected template.

Unlinkability: Based on the same biometric information different versions of protected templates can be constructed. However, protected templates should not allow cross-matching.

A number of techniques have been developed to improve the privacy and security of fingerprint templates. There are hardware based and software based solutions. This paper reviews the various software based techniques that were proposed to ensure the privacy of fingerprint templates.

REVIEW OF TECHNIQUES

A. Biohashing

In biohashing techniques [4], before the fingerprint template is stored in the database, it is combined with a constant string. The technique has significant advantages than solely biometric systems in the sense that it has zero equal error rate and it makes a clear separation between genuine and imposter users. Hence the technique allows the elimination of false accept rates without suffering from increased occurrence of false reject rates. The work in [4] introduces a novel two factor authentication approach in which the fingerprint feature is combined with user specified tokenized random number or data to generate a unique compact code for each user. Two processes are carried out discretization and wavelet Fourier–Mellin transform (FMT). The discretization is performed by iterating inner product between the pseudo-random number and the wavelet Fourier–Mellin transform (FMT) fingerprint feature, and finally deciding each bit on the sign based on the predefined threshold. Direct mixing of pseudo-random number and biometric data—BioHashing is an extremely efficient mechanism with which to incorporate physical tokens, such as smart card, USB token etc. thereby resulting in two factors (token + biometrics) credentials via tokenised randomisation. Hence, it protects against biometric fabrication without adversarial knowledge of the randomisation or equivalently possession of the corresponding token. Tokenised discretisation also enables straightforward revocation via token replacement, and furthermore, biohashing has significant functional advantages over solely biometrics i.e. zero equal error rate (EER) point and eliminate the occurrence of FAR without overly imperil the FRR performance.

B. Biometric Key Generation

Several techniques [5] [6] were introduced which uses the concept of key generation. The enrolled fingerprint template is transformed to a key and the key is stored instead of the template. During authentication a key is generated from the input template by using the same function that was used during enrolment. The keys are compared using any matching algorithm.

C. Biometric Cryptosystem

Biometric cryptosystem is a new technique which combines biometrics and cryptography [7] [8], and is popularly known as crypto-biometric systems. The system is also called helper data-based system. The integration of biometrics and cryptography is broadly carried out in two distinct steps. In case of biometrics-based key generation, a biometric matching amid an input biometric signal and a registered template is utilized in the release of the secret key. In biometrics resetting is very much complicated. One of the huge merits of the biometric data over time is its uniformity which is also the demerit at the same instant. In case of any conventional techniques that uses credit card, smart card etc it is possible to issue a new one, if it is lost. But it is impossible to substitute the biometric characteristics and it is fully evident since it is not feasible to provide a person with a fresh biometric feature once it is stolen. In a biometric cryptosystem, a secure sketch is derived from the enrolled biometric template and stored in the system database instead of the original template.

Biometric cryptosystems are classified into two classes based on how helper data is generated: key binding schemes and key generating schemes. In key binding schemes, the key or helper data is obtained by binding a chosen key to the biometric template. At authentication, keys are generated from the helper data by applying a key retrieval algorithm [9]. Fuzzy commitment scheme [10], fuzzy vault scheme [11], shielding functions [12] are various approaches to this technique. While in key generating schemes, the helper data is obtained only from the biometric template. Keys are generated from the helper data and a given biometric template [13]. Various approaches to this technique are private template scheme [14] and quantization schemes [15].

Once the key and decrypted template is stolen then the original fingerprint template can be constructed. This problem can be solved by the approach called cancellable biometric. This procedure uses a predefined transform and thus provides the intended and repeatable distortion of a biometric signal.

D. Cancellable biometrics:

Cancellable biometric transforms [16] are designed in a way that it should be computationally hard to recover the original biometric data. The technique is also called feature transformation. Two main categories of cancellable templates are non-invertible transforms and biometric salting. In non-invertible transforms, biometric data are obtained by applying a non-invertible function. The advantage of applying this technique is that potential imposters are not able to construct the entire biometric data even if transform is compromised. However, applying non-invertible transforms mostly results in a loss of accuracy. Poor performance is caused by the fact that transformed biometric templates are difficult to align in order to perform a proper comparison and in addition information is reduced. Biometric salting usually denotes transform of biometric templates which are selected to be invertible. Invertible transform of biometric feature vector elements represent an approach to biometric salting even if biometric templates have been extracted in a way that is not feasible to reconstruct the original biometric signal. As a consequence parameters have to be kept secret. If user-specific transforms are applied, the parameters of the transform have to be presented at each authentication. Imposters are able to recover the original template in case the transform parameters are compromised.

E. On mixing fingerprint features

In this technique, the various features of multiple fingerprints are combined to produce a new identity [17]-[18]. The two fingerprints are combined either in the image level or at feature level. Combination at the feature level [17] combines the continuous and spiral component of two different fingerprints to generate a new identity. The continuous component represents the orientation of the fingerprint image while spiral component represents the minutiae positions of the fingerprint image. The ridge flow of a fingerprint can be represented as a 2-D Amplitude and Frequency Modulated signal. This phase is then decomposed into continuous and spiral component. A remote fingerprint system maintains a small set of preselected auxiliary fingerprints corresponding to multiple fingerprints. During enrolment local machine decomposes the fingerprint into continuous and spiral component. To ensure the privacy of the fingerprint image in the local system, the remote system transmits the fingerprints in the auxiliary set and the local machine searches through the received fingerprints to locate a “compatible” fingerprint based on the continuous component of enrolled fingerprint which is then decomposed into continuous component and mixed with spiral component of enrolled fingerprint. The new mixed template is enrolled in the remote system database. During authentication, when the subject presents a sample of the left index finger, it is decomposed and its continuous component is used to search through the fingerprints in the auxiliary set from the remote fingerprint system to determine the most “compatible” fingerprint. In the local machine, the spiral component of enrolled template is mixed with the continuous component retrieved from the remote machine to generate a mixed fingerprint, which is then compared against the database entry. The work in [18] explores the possibility of combining minutiae points pertaining to two different fingerprints to get a new identity.

PERFORMANCE OF TECHNIQUES

The performance of biometric systems is generally evaluated based on three factors: False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (ERR) [20]. Usually conventional biometric systems response with YES or NO for acceptance while biometric cryptosystems require generation and retrieval of 100% correct keys. FRR of biometric cryptosystem refers to the rate of incorrect keys generated by the system untruly or the percentage of incorrect keys given to genuine users while FAR denotes the rate of correct keys generated by the system untruly or the percentage of correct keys given to non-genuine users. FRR and FAR intersect at a point as score distribution overlap and this defines the ERR of the system. Studies shows that there is a decrease in recognition performance for biometric cryptosystems as when compared to biometric systems [21]. This is because within biometric cryptosystems, at comparison the template cannot be aligned properly. Moreover, experiments report an FAR $\leq 2^{-k}$ and FRR of ~3.3% for biometric cryptosystems where k denotes the maximum length of cryptographic key. In majority of the proposed approaches based on cancellable biometrics, template alignment is non-trivial and transforms applied are non-invertible. Some of the approaches related to biometric salting report an increase in performance in case of user specified transforms. Because in case of user specific transforms, two factor authentication is achieved thereby resulting in an increase in security while it doesn't guarantee any effect in the accuracy of authentication. Performance is evaluated based on stolen-token scenario. If the scenario is ignored, performance can be untruly gained. Biometric key generation algorithms usually lack accuracy in matching. Fingerprint mixing by using only the minutiae information pertaining to two different fingerprints shows an ERR of 2.1%.

SECURITY OF TECHNIQUES

In biometric cryptosystems, key length plays an important role in security. Increase in key length may minimize the probability that secret keys are guessed [22]. Privacy leakage is another factor that affects the security of biometric cryptosystems. Identity theft can be avoided by minimizing privacy leakage. In case of cancellable biometrics, if user specified transforms are used, the transform is compromised during inter-class comparisons. Moreover, secret token doesn't guarantee any higher level of security. Security is analyzed on the basis of irreversibility and unlinkability. For irreversibility i.e., to generate the original fingerprint template by inverting the applied transform, the feature transformation function has to be analyzed in detail. If block permutation is used to generate cancellable template then computational effort to reconstruct the original template can be estimated. For achieving unlinkability the amount of applicable parameters should be limited. The security of biometric key generation algorithms depends on the cryptographic algorithm used to generate the key. In the case of fingerprint mixing approach, it may be difficult for the attacker to distinguish between the new identity and original fingerprint.

CONCLUSION

With respect to design goals, the discussed approaches provide significant advantages to improve the security of fingerprint recognition systems, enabling reliable authentication at an high security level. One fundamental issue affect most of the techniques is alignment of minutiae points which may affect the matching performance. For cancellable biometrics, optimization of transformations and alignment of transformed template should be done in order to enhance the recognition performance. Fingerprint combination provides a better security since it fuse the features of two different fingerprints into a new identity. The new identity doesn't reveal the information of both fingerprints.

REFERENCES

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

[2] D.Maltoni, D.Maio, A.K.Jain, and S.Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, 2003.

[3] B. Schneier, "The uses and abuses of biometrics", *Comm. ACM*, vol. 42, no. 8, pp. 136, Aug. 1999.

[4] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.

[5] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in *Proc. 7th Int. Conf. Inform. Assurance and Security (IAS)*, Dec. 5–8, 2011, pp. 262–266.

[6] Y Dodis, R Ostrovsky, L Reyzin, A Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Proc Eurocrypt **2004**, 523–540 (2004)

[7] M Upmanyu, AM Namboodiri, K Srinathan, CV Jawahar, Efficient biometric verification in encrypted domain. ICB '09: Proc of the Third Int Conf on Biometrics, 899–908 (2009).

[8] C Soutar, GJ Tomko, GJ Schmidt, Fingerprint controlled public key cryptographic system. US Patent, 5541994 (1996)

[9] AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008)

[10] A Juels, M Wattenberg, A fuzzy commitment scheme. 6th ACM Conf on Computer and Communications Security, 28–36 (1999)

[11] A Juels, M Sudan, A fuzzy vault scheme. Proc 2002 IEEE Int Symp on Information Theory, 408 (2002)

[12] J-P Linnartz, P Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates. Proc 4th Int Conf Audio- And Video-Based Biometric Person Authentication, 393–402 (2003)

[13] AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008)

[14] G Davida, Y Frankel, B Matt, On enabling secure applications through off-line biometric identification. Proc of IEEE, Symp on Security and Privacy, 148–157 (1998)

[15] H Feng, CC Wah, Private key generation from on-line handwritten signatures. Inf Manag Comput Secur **10**(18), 159–164 (2002)

[16] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach.Intell.*, vol. 29, no. 4, pp. 561–72, Apr. 2007.

[17] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in *Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO)*, Barcelona, Spain, Aug. 29–Sep. 2, 2011.

[18] A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.