Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Technology Review: A Fingerprint Privacy Protection Schemes

Ms. Namrata Yesansure
M.tech (CSE) GHRAET, Nagpur University
India

Dr. Anjali Mahajan
Prof. and H.O.D. (CSE) PIET, Nagpur
India

Prof. Rushi Longadge
Asst. Prof. GHRAET, Nagpur
India

Abstract— In recent years use of biometric technologies gains popularity as concern about the privacy and misuse of biometric data increases. Thus protecting biometric data becomes an important issue. The oldest and widely used form of biometric identification is the fingerprints. It has been widely used in both forensic and civilian applications. Though much progress and research has been made in fingerprint authentication systems, the performance of even state-of-the-art recognizer are still low. In addition to this, securing a stored fingerprint template is of paramount importance because once fingerprints are compromised fingerprint cannot be easily revoked. Over the years many template protection schemes have been explored, we made an effort to review existing biometric template protection schemes. The core motive of this paper is to review the various fingerprint privacy protection schemes. This literature also includes vulnerable points in biometric systems and type of fingerprint matching techniques. In our survey, we observed some reliable and robust schemes.

Keywords—Fingerprint, Biometric templates, Virtual identity, Authentication, Minutiae.

I. INTRODUCTION

Now a day's verification is becoming a security mainstay in the modern distributed systems environment. The biometric is a stirring and emerging field of technology that offers solutions in many applications for instance verification, recognition, security monitoring, border control and immigration, financial transactions, law enforcement agencies, retail sales [16]. In authentication systems the fingerprints are the widely used form of biometric identification. As compared with the other biometric features fingerprint-based biometrics is the proven technique and has the largest market shares. Although fingerprint recognition has been studied for many years and many such security techniques have been explored, the performance of even state-of-the-art matcher is still much low. Moreover, traditional encryption techniques are not enough for fingerprint privacy protection as decryption is required before fingerprint matching, which exposes the fingerprint to the adversaries. Thus protecting the privacy of the fingerprint becomes an important issue. In this paper existing fingerprint template protection schemes are discussed. Section 2 highlights the vulnerabilities in a biometric systems. Section 3 describes the fingerprint recognition system and various fingerprint matching techniques. Section 4 describes the various fingerprint template protection schemes. Finally, section 5 includes the concluded review.

II. VULNERABILITIES IN A BIOMETRIC SYSTEM

The cardinal goal of using a biometric system is to provide non-repudiable authentication. Non-repudiation make sure that an individual who accesses a certain resource cannot later deny using it. Authentication suggests that (i) Only authorized users can access the physical or logical resources protected by the biometric systems and (ii) deceivers are prevented from accessing the protected resources [3]. Like any authentication system, the possible vulnerabilities in a biometric system is the leakage of biometric template information. The leakage of this template information to imposters causes a serious security and privacy threat. The reasons for such threat are as follows:

1. Intrusion attack: In this type of attack if an imposter can hack into a biometric database, he can easily obtain the stored biometric template information of authorized person. Once this information has obtained attacker can use this information for gaining unauthorized access to the system either by reverse engineering or replaying the stolen template. For example, as illustrated in finger-1 fingerprint image can be reconstructed from minutiae template.

2. Function creep: An opponent can make use of the biometric template information for unintended purposes thus compromising the user privacy [3].

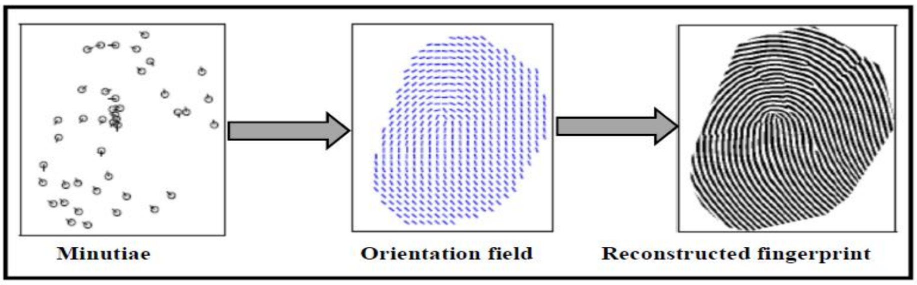

Fig. 1 A fingerprint image reconstruction from minutiae template.

Different levels of attacks in the biometric systems [12] are as follows; Entry Level Attack, Resubmitting previously stored digitized Biometric Signals, Overriding the feature sets chosen by the attacker, Tampering with Biometric features representation, Corrupting the Matcher, Tampering with stored Template , Attacking the channel between the stored template and the matcher, Overriding the final decision. Among all the attacks, the stored template and the matcher attacks are affected severely by image reconstruction techniques. Jianjang Feng and Anil Jain [15] proposed a method to reconstruct an image from minutiae to phase. Sheng Li and Alex Kot [14], Alder [21], Raffaele Chappelli[19], Arun Ross et al. [18] and Hill [22] also discovered a technique to reconstruct the original template from the stored minutia template.

III. **FINGERPRINT RECOGNITION SYSTEM**

Everyone is known to have unique, immutable fingerprints. For authentication purpose, fingerprint template is extracted from fingerprint images and saved into the central repositories. The fingerprint recognition system composed of following stages: fingerprint enrolment, verification and fingerprint identification. The goal of verification is to prevent multiple individuals from accessing the same identity and it is typically used for positive recognition. Fingerprint verification is technique used to verify the authenticity of one person by his fingerprint. During the identification stage, the system recognizes a person by searching the templates of all the users in the database for a match. The stages verification and identification both makes use of certain schemes for fingerprint matching this is exhibited in the following subsection.

A] Techniques for Fingerprint Matching

Various fingerprint matching techniques discussed in literature [13] are as follows:

- *Minutiae based technique:* Most of the fingerprint authentication systems are based on Minutiae. Minutia based techniques represent the fingerprint by its local ridge characteristics, like ridge endings and bifurcations. This approach is the mainstay of the current available fingerprint authentication systems has been fiercely studied.

- *Image Based Techniques:* This is an advanced and newly emerging method for fingerprint recognition. Image based techniques try to do matching based on the global features of a whole fingerprint image. Image based technique is useful to solve some stubborn problems of the minutiae based approach.

IV. **FINGERPRINT TEMPLATE PROTECTION SCHEMES**

Most of the existing techniques exploit the key or token for the fingerprint privacy protection, which creates the troublesomeness. They may also be open to attacks when both the key or token and the protected fingerprint are stolen. Several approaches have been proposed in the literature to protect biometric templates from revealing important information.

Teoh et al. [5] propose a biohashing approach in which the inner products between the user’s fingerprint features and a tokenized pseudorandom number (i.e. the key) is computed. The accuracy of this approach primarily depends on the key or token, which assumed to be never shared or stolen[20].

Ratha *et al* [6] propose to generate cancelable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is guided by a key, which will usually lead to a reduction in matching accuracy. The work in [5] and [6] are shown to be exposed to intrusion and linkage attacks when both the key and the transformed template are stolen [17].

Sheng Li and Alex Cot [7] imperceptibly hide the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the secured thinned fingerprint are stolen.

There are some schemes [1],[2],[4] and [8]–[11] that are able to protect the privacy of the fingerprint without using a key. These schemes provide security to the biometric template by creating a virtual identity. A virtual identity is the one created by the Biometric system that acts as an interface between the *system* and the *physical person*. Virtual identity is created by mixing features acquired from two or more biometric template which is then stored into the database instead of original template. For example as shown in figure-2 the virtual identity is created by combining features extracted from two fingerprints.

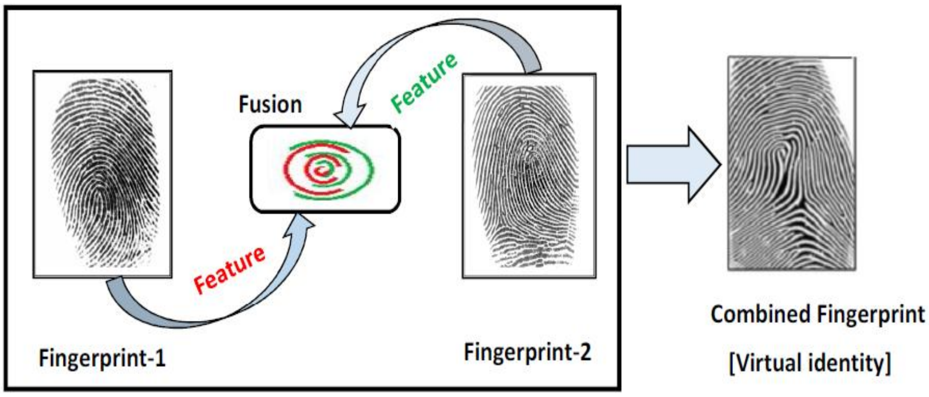

Fig.2 Virtual identity creation by combining features acquired from two fingerprints.

Yanikoglu and Kholmatov [11] first proposed the concept combining two different fingerprints into a new identity. In this approach the new identity is created by combining the minutiae locations extracted from the two fingerprints. Thus new identity protects the original minutiae locations of each fingerprint. However, this approach involves remedy: it is easy for attacker to identify such new identity because as compare to original fingerprint new identity contains many more minutiae locations.

E. Camlikaya et al. [10], proposes the concept of multi-model biometric system which preserves privacy and increases accuracy. This technique combines two different biometrics into a new identity, by extracting the minutiae positions from a fingerprint and the artificial points generated from the voice to produce a new identity. In this work, the EER are shown to be under 2% according to the experimental results.

Ross and Othman [8],[9] and [2]combine two different fingerprints into a single new identity in the image level. In this, the mixing fingerprint process starts with the decomposition of each fingerprint into two different components viz., the continuous component and the spiral component based on the fingerprint FM-AM model [14]. After some alignment, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint, as a result new virtual identity is created which is named as a mixed fingerprint. This mixed fingerprint have several benefits. For example (i) this technique could be utilized in multi-finger authentication system because by using this approach it is possible to mix images of thumb and the index finger of single person, or index finger of two different persons. (ii) Mixing fingerprint can be used to generate large set of virtual identities, which can be used to obscure the original identities of individuals or be used for large-scale evaluation of algorithm. In addition to above merits their work in [2] adds one more feature to mixing fingerprint which is the template can be reset if the mixed fingerprint is compromised (i.e. generate a cancelable fingerprint).

Compared with the work in [10],[11] which is a feature level technique, an image level based fingerprint combination techniques [8],[9] and [2] has two advantages: (i) it is difficult for the attacker to discriminate a mixed fingerprint from the original fingerprints, and (ii) existing fingerprint matching algorithms are applicable for matching two mixed fingerprints. However, approach in [8] and [9] produces a visually unrealistic mixed fingerprint due to the variations in the orientation and frequency between the two different fingerprints, and the approach in [2] produces a new entity that bear resemblance to plausible fingerprint image. Their experimental results [9] show that the EER of matching two mixed fingerprints is about 15% when two different fingerprints are randomly chosen for creating a mixed fingerprint. If the two different fingerprints are carefully chosen according to a compatibility measure, the EER can be reduced to about 4%.

Li and Cot [1],[4] explored a feature level based technique for fingerprint privacy protection by combining two fingerprints into a new identity. The discovered technique creates a new identity by combining the minutiae location extracted from the one fingerprint and directions extracted from another fingerprint. Thus the original minutiae positions and orientation of first and second fingerprint respectively can be protected in the new identity (i.e. virtual identity) Compared with the work in [8]-[11] and [2] these fingerprint combination technique has following advantages: (i) Combined fingerprint achieves a lower error rate than the mix fingerprint.(ii) Compared with feature level based technique [10],[11] this techniques able to create a new identity which is difficult to be distinguished from the original minutiae template. (iii) It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates. (iv) Compared with the image level based techniques [8], [9] and [2] this technique creates a new virtual identity which performs better for randomly chosen two different fingerprint. However, this approach involves one shortfall, that is generating a combined fingerprint would cost more time than creating a mixed fingerprint because of the fingerprint reconstruction.

V. **CONCLUSION**

The robustness and reliability of the any authentication system against attacks is depends the way the system provides privacy to the individuals sensitive or confidential data. This paper reviewed various fingerprint template protection schemes their advantages and remedies. This paper also highlights some schemes that provide security to the template by creating virtual identity that are more secure than traditional techniques that makes use of key or token for the fingerprint privacy protection. Moreover, this paper also discussed fingerprint recognition system and types of fingerprint matching techniques. In our literature we have also addressed some open to attack points in biometric authentication system.

REFRENCES

[1] S. Li, A. C. Kot,” Fingerprint Combination for Privacy Protection”, *IEEE Transactions on Information Forensics and security, Vol. 8, No. 2, February 2013.*

[2] A. Othman, A. Ross, “On Mixing Fingerprints”, *IEEE Transactions on Information Forensics and security, Vol. 8, No. 1, January 2013.*

[3] A. K. Jain, K. Nandakumar and A. Nagar,” Fingerprint Template Protection: From Theory to Practice”, *Appear in Security and Privacy in Biometrics, P. Campisi (ed.), Springer, 2012.*

[4] 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.*

[5] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, “Biohashing: Two factor authentication featuring fingerprint data and toke1nized random number,” *Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.*

[6] 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.*

[7] S. Li and A. C. Kot, “Privacy protection of fingerprint database,” *IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.*

[8] 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.*

[9] 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.*

[10] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, “Multi-biometric templates using fingerprint and voice,” *Proc. SPIE, vol. 69440I, pp.69440I-1–69440I-9, 2008.*

[11] B. Yanikoglu and A. Kholmatov, “Combining multiple biometrics to protect privacy,” *in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.*

[12] E. Chandra and K. Kanagalakshmi,”Cancelable Biometric Template Generation and Protection Schemes: a Review,” *3rd Int. Cof. Electronics computer technology Vol. 5, 10.1109/5941948,2011.*

[13] R. Bansal, P. Sehgal and P. Bedi,”Minutiae Extraction from Fingerprint Images- a Review,” *in Proc.IJCSI,Vol.8, Issue 5, No3, September 2011.*

[14] S. Li and A. C. Kot, “Attack using reconstructed fingerprint,” *in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.*

[15] J. Feng and A. K. Jain, “Fingerprint reconstruction: From minutiae to phase,” *IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp.209–223, Feb. 2011.*

[16] Md. R. Islam, Md. S. sayeed and A. Samraj,”Technology Review: Image Enhancement, Feature Extraction and Template Protection of a Fingerprint Authentication System,” *Journal of Applied Sciences 10(14):1397-1404, 2010.*

[17] A. Nagar, K. Nandakumar, and A. K.Jain,“Biometric template transformation:A security analysis,” *in Proc. SPIE, Electron. Imaging,Media Forensics and Security, San Jose, Jan. 2010.*

[18] Arun Ross, Jidnya Shah and Anil K. Jain, “From Template to Image: Reconstructing Fingerprints from Minutiae Points” , *IEEE Transactions on Pattern analysis and Machine Intelligence, Vol.29,No. 4, April 2007.*

[19] Raffaele cappelli, Alessandra Lumini, Dario, and Davide Maltoni,“ Fingerprint Image Reconstruction from Standard Template”, *IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29,no. 9, Sepember 2007.*

[20] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of biohashing and its variants,” *Pattern Recognit., vol. 39, no. 7, pp.1359–1368, 2006.*

[21] A. Adler, “Can images be regenerated from biometric templates?”, *In Biometrics consortium conference, (Airlington, VA), Sept. 2003.*

[22] G.Davida, Y. Frankel, and B. J. Matt, “On enabling secure applications through offline biometrics identification,” *in Proc. Symp. Privacy and Security, 1998, pp. 148–157.*

AUTHORS BIOGRAPHY

Ms. Namrata M. Yesansure, received the B. E. degree in Information Technology from Yeshwantrao Chavan College of Engineering, Nagpur, India, in 2009. She is currently pursuing M.Tech in Computer Science & Engineering from G. H. Raisoni Academy Of Engineering and Technology, Nagpur. Her research interests include Biometric template protection, Pattern recognition and Image Processing.
nm.yesansure@gmail.com

Dr. Anjali Mahajan, currently working as Professor and Head in Department of Computer Science and Engineering, PIET, Nagpur, completed her B.E. in Computer Science and Engineering from Government College of Engineering, Amravati in the year 1994, M.Tech from Sant Gadge Baba Amravati University in the year 2002 and Ph.D. from Sant Gadge Baba Amravati University in 2010. Dr. Mahajan has to her credit thirteen publications in International Journals and 29 publications at the International conferences and 5 publications in National Conferences. She is a member of IEEE, LM of CSI, and LM of ISTE. Dr. Mahajan areas of interest are Parallel Computing, Advanced Operating systems, Digital Image Processing & Soft computing systems. armahajan@rediffmail.com

Mr. Rushi Longadge, received the Bachelor of Engineering degree in Information Technology from North Maharashtra University, Jalgon, India, in 2010 and Master of technology in Computer Science & Engineering from G.H. Raisoni College of Engineering, Nagpur. Mr. Rushi Longadge, currently working as Asst. Professor in Department of Computer Science & Engineering, G. H. Raisoni Academy Of Engineering and Technology, Nagpur. His Reaserch areas are Data Minig, Machine Learning and Image Processing.
rushilongadge@gmail.com