IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-10, Oct 2019 E-ISSN: 2347-2693

Fingerprint Template Protectionsthrough Various Pattern Transformation Approaches: A Review

K.Kanagalakshmi[1*], Joycy K.Antony[2]

[1] Dept. of Computer Science, Kamalam College of Arts and Science, Tamil Nadu, India
[2]Dept. of Computer Science, Nehru Arts And Science College, Tamil Nadu, India

DOI: https://doi.org/10.26438/ijcse/v7i10.107110 | Available online at: www.ijcseonline.org

Accepted: 09/Oct/2019, Published: 31/Oct/2019

***Abstract*:-**Biometric Templates are majorly used as an authentication and identification metric of a person in different industries. The Biometric templates are generated through various mechanisms like key, index and transformation based. This paper focuses on a study of fingerprint Biometric and various existing pattern transformation approaches based on fingerprint.

Keywords: Biometrics, Cancellable Templates, Fingerprint.

I. INTRODUCTION

Biometric is a statistical measurement of the physical and behavioural features of a human. It can be used to secure the system and to authenticate and identify a person.The fingerprint is one of the accepted biometric methods used to verify human being. Fingerprint recognition system is the most significant biometric technique. Dr .E.Chandraet al (2011). (1) affords consistent means of biometric verification due to features noise removal, Universality, Distinctiveness, Permanence and Accuracy. It is the technique of identifying an individual and it can be used different applications, such as, medical records, criminal investigation, detection, verification, and cloud computing, communication.Fingerprint detection involves the location and resolution of the unique characteristics of the fingerprint. The fingerprint is collected of various 'ridges' and 'bifurcation', which forms the basis of the loops, arches and swirls on the fingertip as in fig.1.The ridges and bifurcation contain different kinds of breaks and discontinuities known as 'minutiae'. It is from these minutiae that the unique features are located and resolute. There are two types of minutiae points: ridge and valley pointspresented Handbook of Fingerprint Recognition (2003) (2).

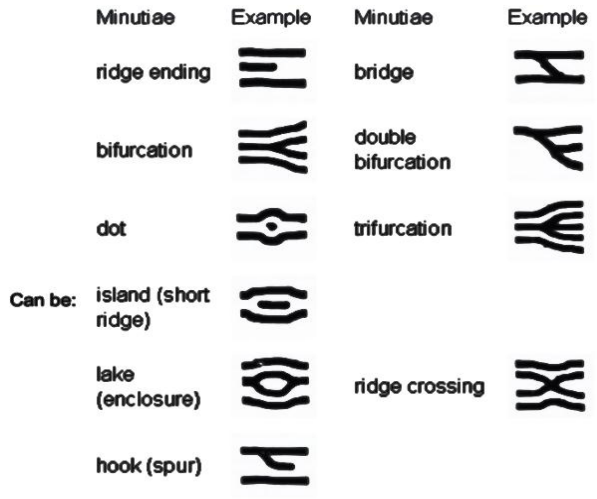

Figure 1 Minutiae features

The key terms of the fingerprint biometrics are as follows:

1. Ridge endings - a ridge that ends abruptly
2. Ridge bifurcation - a single ridge that divides into two ridges
3. Short ridges, island or independent ridge - a ridge that commences, travels a short distance and then ends
4. Spur - a bifurcation with a short ridge branching off a longer ridge
5. Crossover or bridge - a short ridge that runs between two parallel ridges

Now-a-days cancellable fingerprint templates are used for security, authentication and identification purposes. The rest of the paper comprises 3 sections. Section-2 gives a review of the existing template protection schemes. In section-3, a comparative study has been given. Section-4 concludes the study.

II LITERATURE REVIEW ON FINGERPRINT PROTECTION TECHNIQUES

Cavoukian, and Ann, (2012). (3) While biometric technology provides various advantages, there exist some major problems like changeability and privacy. Biometric data reflect the user's physiological or behavioural

characteristics. If the storage of the biometric templates is obtained by an adversary, the user's privacy may be compromised. The biometric templates should be stored in a format such that the user's privacy is preserved.

Sadhya et al (2016). (4) To deal with this, a number of research works have been proposed in recent years. These techniques can be categorized into two main classes such as Biometric cryptosystems and Template transformation.

Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen.Template transformation techniques modify the biometric template with user specific key or twisted logics such that it is difficult to recover the original template from the transformed template.

Alex C. Kot et al. [2013], (5) proposed the fingerprint combination for privacy protection in which two different fingerprints were combined to produce a new virtual identity and finally stored in database. proposed fingerprint reconstruction algorithm. A fake fingerprint image is reconstructed from a stolen combined fingerprint template; there are possibilities that the hacker can crack traditional systems. Minutiae points are found based on amplitude and frequency and the reconstructed fingerprint is used by the attacker to rebuild.The spirals from the partial fingerprint image and the fingerprint can be reconstructed intuitively. by reconstructing a fingerprint it might be faked, which causes enormous problems to the security systems.

Dr. E. Chandra et al. [2014], (6) proposedashift based estimation for fingerprint enhancement. It is a technique that retrieves the preliminary orientations from the fingerprint. After obtaining the clustered candidates, final direction is determined. The proposed algorithm is poor and inefficient in terms of latency and speed.

S. Li et al. [2011]. (10) proposed an architecture that provides security to fingerprints, in which the fingerprint privacy is done in enrolment without using any key. This makes it a tough deal for the hacker to differentiate the original fingerprint template from the saved template. Even if the combined minutiae template is stolen, the hacker will not be able to obtain the properties of the complete fingerprint thus overcoming the existing fingerprint privacy protection techniques. The algorithm is still not up to the inferiority mark, thus resulting in slow speed and low quality latent.

A. Othman et al. [2011], (13) proposed avisual cryptography for biometric privacy that makes use of cryptography for imparting confidentiality of biometric information such as fingerprint images, face images, iris codes. The planned approach stores the fingerprint in non-recoverable format. Without pixel expansion VCS is developed. Now there does not exist any such scheme where accidental noisy images are produced.The algorithms proposed earlier are based on keys that ensure fingerprint security. However, if the keys are stolen, it makes the protection system insecure.

E.Liu et al. [2016], (15) and Josef Strom proposed a bio-hashing approach in which pseudo random numbers and minutiae features extracted from the fingerprint are made use of. The key which is being made use of should not be revealed to increase the protection criteria.

Ratha.N.Ket al. [2007], (12) suggested by generating a cancellable fingerprint template by employingtransformations, on the features extracted, that are non- recoverable. The resulting transformed template is encrypted with a key and an irreversible template is obtained. If the key and the resultant template are hacked, [7] and [16] prove worthless.

T. H. Nguyen et al [2015] (8) suggested by executing fuzzy fault logic on the minutiae features in which the key-inversion attack was used. (13) the works in hides the identity of the user who has a thinned fingerprint image by making use of keys. When the thinned fingerprint template and the key is revealed, the user identity can be easily hacked. Only few protection techniques are available without making use of keys.In matching applications, two separate databases are required in order to perform computations or work in it. The works in a new identity is obtained after combining the features or images of left and right fingerprints.Minutiae features from two fingerprints are obtained and are combined.

Dr. E. Chandra et al. (2011), (9) the new identity noiseremoval and performance evaluation mixture of existing minutiae features and new minutiae positions. The attacker can identify the new template because of the presence of a number of new minutiae features. After experimenting with the fingerprint database, EER is found to be 2.1%.

Z. Jin et al. (2016), (5) a new technique is proposed where artificial minutiae points are inserted into the fingerprint template by means of voice input. Thus a new template is generated after inserting these artificial minutiae points.After experimentation, EER is found to be less than 2%.In, image level combination of two fingerprints is proposed. Firstly, spiral and continuous components of each fingerprint is separated with respect to FM-AM model.This proposed SNL makes use of techniques such as inter-mixing; swapping, simulated key insertion followed by tree based shuffling mechanism to provide new virtual identity.The matching algorithm combines transformations for alignment purposes and a threshold based mapping approach to calculate a similarity score. The implementation results show very low error rate with FMR of 0.5 % and FNMR of 0.3 % .

III. SUMMARY OF THE LITERATURE SURVEY

The summary of the literature review is given table 1. It furnishes the techniques, problems addressed and limitations of the technique.

Table 1 Summary of the literature survey

S.No.	Author & Title	Technique used	Problem Addressed	Limitations
1	Sheng Li, (2013) , Fingerprint Combination for Privacy Protection	Fingerprint combination	New virtual identity Low error rate	Limited privacy protection Features of original template completely revealed in the new identity-information leakage
2	D. M. Sabah et al (2018), Implementation of Secure Biometric System Based on Energy properties of Fingerprint image to select Blocks for Data Hiding Algorithm	Data hiding	Better data hiding techniques by embedding user's private information	Poor performance
3	S. M. T. Toapanta et al (2018) Algorithms for Efficient Biometric Systems to Mitigate the Integrity of a Distributed Database	Bio convolving and HMM	Non invertible transforms	Security depends on hardness of transformations applied
4	X. Dong et al (2018), A Generalized Approach for Cancellable Template and Its Realization for Minutia Cylinder-Code	MCC representation	Accurate Better privacy protection	Invertible
5	B. Yan et al (2017), A novel public key encryption model based on transformed biometrics	Public key cryptography	Applicable to multiple biometrics	Involves more computations
6	B. O. Mohammed and and S. M. Shamsuddin (2018), Feature level Fusion for Multi-biometric with identical twins	Feature level fusion framework and fuzzy commitment	Higher security	Poor feature fusion Multimodal database management
7	Z. Li et al (2019) Improvement for distortion resistance of Delaunay triangulation net-based fingerprint templates	Delaunay quadrangle based structure	Improved security	Uncertainty due to rotation and translation

IV CONCLUSION

This paper made an attempt to review the existing biometric base template generation technique. Pros and cons of the techniques have been reviewed.

REFERENCES

[1] Dr. E. Chandra, K. Kanagalakshmi . (2011). Noise Elimination in Fingerprint Image Using Median Filter. Int. J. Advanced Networking and Applications (0975 – 8887) Volume: 02, Issue: 06, Pages: 950-955.

[2] Fingerprint Analysis and Representation (2003). In: Handbook of Fingerprint Recognition. Springer Professional Computing. Springer, New York.

[3] Cavoukian, Ann. "Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era." Privacy protection measures and technologies in business organizations: aspects and standards. IGI Global, 2012. 170-208.

[4] Sadhya, Debanjan, and Sanjay Kumar Singh. "Privacy preservation for soft biometrics based multimodal recognition system." Computers & Security 58 (2016): 160-179.

[5] Z. Jin, M. Lim, A. B. J. Teoh, B. Goi and Y. H. Tay, "Generating Fixed-Length Representation From Minutiae Using Kernel Methods for Fingerprint Authentication," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 10, pp. 1415-1428, Oct. 2016.

[6] Dr. E. Chandra, K. Kanagalakshmi. (2014, March). Novel Shift-Phase Transformation based Cancelable and Irrevocable Biometric Template Generation for Fingerprints. International Journal of Computer Applications (0975 – 8887) Volume 89 – No 20.

[7] Jianjiang Feng, Jie Zhou, Proposed, "Orientation Field Estimation for Latent Fingerprint Enhancement" IEEE Trans, pattern anal, and machine intelligence, Vol. 35, no. 4, pp. 925-939, April 2013.
[8] T. H. Nguyen, Y. Wang, Y. Ha and R. Li, "Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints," in IET Biometrics, vol. 4, no. 1, pp. 29-39, 3 2015.
[9] Dr. E. Chandra, K. Kanagalakshmi. (2011, April) "Performance evaluation of filters in noise removal of fingerprint image," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 117-121
[10] Li.S. and KotA. C., "Privacy protection from fingerprint database," IEEE Signal Process. Let., Vol. 18, no. 2, pp. 115–118, Feb. 2011.
[11] L. Ghammam, M. Barbier and C. Rosenberger, "Enhancing the Security of Transformation Based Biometric Template Protection Schemes," 2018 International Conference on Cyberworlds (CW), Singapore, 2018, pp. 316-323.
[12] RathaN. K., ChikkerurS., ConnellJ. H., and BolleR. M., "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach.Intell., Vol. 29, no. 4, pp. 561–72, Apr. 2007.
[13] RossA. and OthmanA., "Mixing fingerprints for template security and privacy," Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.
[14] Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, Fingerprint Combination for Privacy Protection IEEE Transactions on information forensics and security, Vol. 8, no. 2, pp. 350-360, February 2013.
[15] E. Liu and K. Cao, "Minutiae Extraction From Level 1 Features of Fingerprint," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1893-1902, Sept. 2016
[16] D. M. Sabah, D. A. A. Majeed and H. S. Hatem, "Implementation of Secure Biometric System Based on Energy properties of Fingerprint image to select Blocks for Data Hiding Algorithm," 2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT), Baghdad, Iraq, 2018, pp. 48-50
[17] S. M. T. Toapanta, A. A. C. Cruz, L. E. M. Gallegos and J. A. O. Trejo, "Algorithms for Efficient Biometric Systems to Mitigate the Integrity of a Distributed Database," 2018 International Conference on Computer, Information and Telecommunication Systems (CITS), Colmar, 2018, pp. 1-5
[18] X. Dong, Z. Jin and K. Wong, "A Generalized Approach for Cancellable Template and Its Realization for Minutia Cylinder-Code," 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Honolulu, HI, USA, 2018, pp. 908-915.
[19] B. Yan and L. You, "A novel public key encryption model based on transformed biometrics," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, 2017, pp. 424-428.
[20] B. O. Mohammed and S. M. Shamsuddin, "Feature level Fusion for Multi-biometric with identical twins," 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, 2018, pp. 1-6.
[21] Z. Li, W. Lei and W. Zhang, "Improvement for distortion resistance of Delaunay triangulation net-based fingerprint templates," in IET Biometrics, vol. 8, no. 5, pp. 325-331, 9 2019.

