A REVIEW ON CANCELABLE BIOMETRIC AUTHENTICATION

Akhila Ashok J[1], Prof. Kanjana G[2]

[1]PG Student, Dept. of Electronics & Communication Engineering, LBSITW, Kerala, India
[2]Assistant Professor, Dept. of Electronics & Communication Engineering, LBSITW, Kerala, India

Abstract - *Biometric authentication automatically compares a user's biometric to a stored biometric template in order to confirm a user's identity. Biometrics has a lot of advantages. Compared to credit cards and passwords, biometrics are constantly associated with a user. So it cannot be restored. Cancelable biometric is a biometric template safety technique. The principle behind cancelable biometrics is that a biometric image of a sample is transformed into another form. It is very difficult to find the original biometric image from the transformed one. The main purpose of this paper is to make a comparative analysis of existing cancelable biometric techniques.*

Key Words: Biometrics, Biometric authentication, Cancelable biometrics, Attack via record multiplicity, Deep learning

1. INTRODUCTION

Biometric refers to a person's behavioral or physical characteristics. The biometrics are believed to be unique to an individual. So biometric generation has been widely used for several applications. Biometric authentication mainly focuses on figuring out or verifying the identity of someone. It suffers from privacy and protection issues. To address this issue, cancelable biometrics is recommended wherein a biometric image of a person is distorted or transformed in such a way that it becomes difficult to achieve the unique biometric image from the distorted one. Some other critical feature of cancelable biometrics is that it may be reissued if compromised.

So that you can save the robbery of biometrics, it's beneficial to alter them via revocable and non-invertible adjustments to provide cancelable biometric templates. The idea of cancelable biometric is to make a biometric template, it can be canceled and be revoked like a password.

Four targets of designing a cancelable biometric scheme are as accompanied:

- Diversity: No identical cancelable functions may be used throughout various programs, therefore a big quantity of protected templates from the identical biometric feature is needed.
- Reusability/Revocability: Trustworthy revocation and reissue inside the event of compromise.
- Non-invertibility: Non-invertibility of template computation to avoid recovery of original biometric statistics.
- Performance: The expression should not decay the recognition performance.

Cancelable biometric has gained a lot of interest in recent times. During this system, rather than storing the original biometric, it's converted using a one way function. The conversion can be applied either in the original form or in the feature form. It absolutely shows that this manner of constructing biometric templates has the preferable properties of cancelable biometric templates. It provides privacy and security since it's computationally delicate to recover the original biometric from a converted one. It prevents cross-matching between databases since each operation uses a distinct metamorphosis. And it doesn't degrade the delicacy of an identical algorithm because the statistical characteristics of features are roughly maintained after metamorphosis.

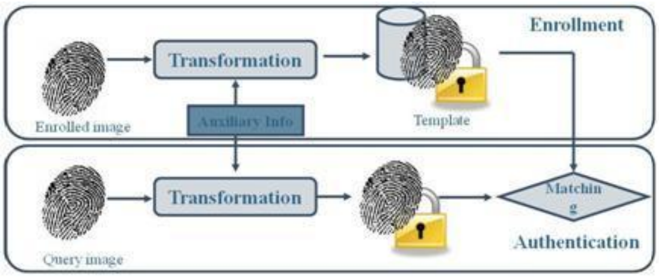

Fig- 1: Cancelable biometric authentication

2. REVIEW OF THE DIFFERENT PAPERS

Ahsan *et al.* proposed an intelligent system for automatic fingerprint identification using feature fusion by gabor filter and deep learning [1]. An intelligent computational approach has been introduced to automatically authenticate fingerprints for personal identification and verification. Gabor filtering technique and deep learning technique has been combined and a feature vector is obtained.

Yang *et al.* proposed a cancelable biometric authentication system based on feature adaptive random projection [2]. The traditional random projection based cancelable template design suffers from many attacks. To address this issue, a feature adaptive random projection based cancelable biometric authentication system has been proposed. Here the projection matrices are generated from one basis matrix. The generated projection matrices are discarded after use.

Arpita Sarkar *et al*. introduced the design of a hybrid approach using a revocable technique and steganographic text color coding technique for fingerprint template protection [3]. In this paper, a step hybrid template safety scheme has been proposed, wherein step one is the introduction of a converted template from the unique template, and the second step is to hide the value of the converted template by making use of the textual content steganography.

Shahzad *et al.* proposed an alignment- free cancelable fingerprint templates with dual protection [4]. Many existing cancelable fingerprint templates suffer post transformation performance deterioration and also the attacks via record multiplicity(ARM). An alignment-free cancelable fingerprint template with dual protection has been proposed, which consists of the window- shift XOR model and the partial discrete wavelet transform. It works just for the minutia descriptor kind of fingerprint template.

Gaurav Varma *et al.* proposed a digital holographic based cancelable biometric for personal authentication [5]. The realization of cancelable biometrics is presented by using an optoelectronic approach, during which an optically recorded hologram of the fingerprint of an individual is numerically reconstructed. The user specific fingerprint features are often extracted from the reconstructed fingerprints using feature extraction.

Barman *et al.* proposed a fingerprint based crypto-biometric system [6]. In this paper, a cryptographic key of both sender and receiver will be generated from a cancelable fingerprint template. Cancelable fingerprint templates of every sender and receiver are securely transmitted to each other through the utilization of a key based steganography. Each template is mixed and generates a blended template.

Kanagalekshmi k *et al.* proposed a novel complex conjugate phase transform technique for cancelable and irrevocable biometric template generation for fingerprints [7]. Here, a reciprocated magnitude and complex conjugate phase transform is proposed for the generation of a cancelable biometric template.

Maiorana *et al.* proposed the Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system[8]. In this paper a protected on- line based signature - based authentication system has been proposed.

Table- 1: Comparison of Review Paper

Year & Reference	Technique	Advantages	Disadvantages
2021 [1]	Gabor filter and deep learning	Alignment free technique	More time complexity
2021 [2]	Feature adaptive random projection	Overcome the limitations of traditional random projection based cancelable template design	Only concentrated on the minutiae pair feature descriptor
2021 [3]	Steganographic text color coding	Good for data hiding	Applicable only for small messages
2021 [4]	Hybrid	More secure	Time complexity
2016 [5]	Digital holographic	Holograms can be easily captured	More complex
2015 [6]	Crypto-biometric	Easy to implement	High computational complexity
2012 [7]	Complex conjugate phase transform	Low false acceptance rate	Low performance
2011 [8]	Bioconvolving	Transformed template is same as that of the original template	Applicable only for multi biometric scenario

3. CONCLUSION

Cancelable biometrics is a biometric template protection method. Biometrics is a useful concept and it has a number of advantages. The biometric traits cannot be lost or forgotten compared to passwords. However their use raises several privacy and security concerns, especially in their storage. So to overcome this issue, cancelable biometric techniques have been chosen. This work is a summary of different cancelable biometric approaches.

ACKNOWLEDGEMENT

We would like to thank the Director of LBSITW and the Principal of the institution for providing the facilities and support for our work.

REFERENCES

[1] Ahsan M, Based MA, Haider J, Kowalski M. An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning. Computers & Electrical Engineering. 2021 Oct 1;95:107387.

[2] Yang W, Wang S, Shahzad M, Zhou W. A cancelable biometric authentication system based on feature-adaptive random projection. Journal of Information Security and Applications. 2021 May 1;58:102704.

[3] Sarkar A, Singh BK. Design of a hybrid approach using a revocable technique and steganographic text color coding technique for fingerprint template protection. Multimedia Tools and Applications. 2021 May;80(13):20641-70.

[4] Shahzad M, Wang S, Deng G, Yang W. Alignment-free cancelable fingerprint templates with dual protection. Pattern Recognition. 2021 Mar 1;111:107735

[5]Verma G, Sinha A. Digital holographic-based cancellable biometric for personal authentication. Journal of Optics. 2016 Mar 24;18(5):055705.

[6] Barman S, Samanta D, Chattopadhyay S. Fingerprint-based crypto-biometric system for network security. EURASIP Journal on Information Security. 2015 Dec;2015(1):1-7.

[7] Kanagalakshmi K, Chandra E. Novel Complex Conjugate-Phase Transform technique for cancelable and irrevocable biometric template generation for fingerprints. International Journal of Computer Science Issues (IJCSI). 2012 Jul 1;9(4):426.

[8] Maiorana E, Campisi P, Neri A. Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In2011 IEEE International Systems Conference 2011 Apr 4 (pp. 495-500). IEEE.