International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

Review Paper on Biometric Template Security

Sudhi G. K.
M.Tech Image Processing
College of Engineering Chengannur
Kerala, India

Smitha Dharan
HOD, Dept. of Computer Engg.
College of Engineering Chengannur
Kerala, India

Manjusha Nair S
Assistant Professor
College of Engineering Chengannur
Kerala, India

***Abstract*—An accurate authentication plays a main job in secure communication. Conventional personal authentication methods were based on passwords and identity documents which fails to meet the performance and security of several important applications like E-commerce, banking, health care and many other fields where critical authentication is needed. The biometric authentication system works on features like fingerprint, voice and Iris. But the direct storage of fingerprint details he said that to the identity of the user which raises various privacy concerns. To address these problems various techniques have been introduced in recent years. These techniques have been introduced as a template protection mechanism to improve the confidentiality of the template. All this issues made the biometric authentication a highly desirable technique. Biometric Cryptosystems represents the emerging technologies in the biometric template protection schemes to address these threats. Biometric Cryptosystems is the combination of biometric with cryptography. In this literature review several aspects of biometric template generations and the security of the generated template are explained.**

***Keywords*— Biometric; Template, Security; Biometric Cryptosystems.**

I. INTRODUCTION

Biometrics is the discipline of achieving the authenticity of a user by his various attributes like behavioural features. The biometric is very relevant in our modern society. The key duty of an authentication system is the establishment of a user's authenticity.

There were many traditional ways of authentication such as knowledge-based and token to based mechanisms, but these representation of identities can be lost easily and the passwords can be guessed or manipulated easily. The only way was to set a complex password, but the chances of forgetting the password is high.

The identity management systems works on the process of authenticating a person's identity and give access t that particular user. The importance of such systems are to prevent intruders from accessing confidential data from protected environment.

The use of cryptography provides security to confidential data. The user can access the data by using a private key. But the length of the cryptographic key make it very hard to remember the password whenever it is required. The disadvantage of this method is that the security of the system improves as the password becomes stronger. Some users provide simple passwords as they will not be able to remember strong passwords. These behaviours make the data at high risk.

All these situations made the biometric authentication a highly desirable technique. In a biometric authentication system, the cryptographic key is protected with the help of biometric traits. For this the user only needs to enter the biometric sample. Whenever the sample is matched with the already stored one, we can say that a successful authentication is done. So, the user is not needed to recollect passwords. In this literature review various biometric cryptosystems are reviewed. The review concentrated mostly on fingerprint and iris data.

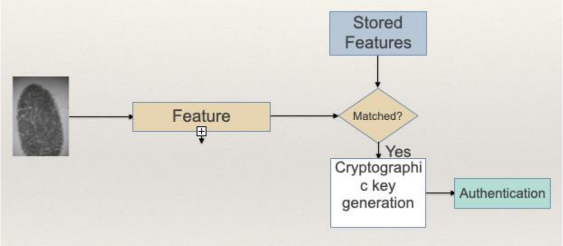

Fig. 1 shows the formation of a Hazy image

This figure shows the basic working of a biometric cryptosystem. The authentication is done by giving the biometric trait as an input to the system. If it matches, the key is released.

II. RELATED WORKS

Biometric system is the branch of science that identifies the person based on his or her psychological or behavioural characteristics such as fingerprint, palm print, palm vein, face, iris, gait, writing style and voice. Protection of template is one of main problem in biometric authentication system. The confidentiality of biometric template is observed as a an important property because heisted images are reprocessed by pirates.

To prevent these security threats, incorporation of biometrics and cryptography helps to evolve a novel technology known as biometric cryptosystems.

The first step in biometric crypto system is the generation of biometric features. The template generation of fingerprint includes binarization, segmentation, thinning and minutiae detection. Binarization is the method of transforming greyscale image into binary image and it helps to improve the contrast between values and ridges in an image. Segmentation is the process of eliminating unwanted edges of the fingerprint image. The main objective of segmentation is to extract the region of interest. The morphological operation of thinning is done to extract the fingerprint features and to eliminate that unnecessary noise. Once the thinning is done then the minutiae regions are extracted. The feature extraction of Iris includes that iris segmentation and normalization. Iris segmentation is used to distinguish the nearness of a circular shape in a given image. The normalization phase is to take a fixed size of the image in order to allow comparison by transforming the iris region.

D. Chitra et al. [1] put forward a Fuzzy vault system which has key binding method and can make up for intra class variation in the data. The process is executed by using the minutiae points of the fingerprint image. The fuzzy vault system is a cryptographic method with a key to encode a polynomial function. *Wendy P. H. et al.* [7] also proposed a template protection approach using fuzzy vault scheme. In a key binding crypto system a helper data is obtained by binding the biometric data with the key. The system proposed by D. Chitra et al. consists of various functions called preprocessing, pre-alignment and minutiae extractions, fuzzy vault and verification. The fingerprint needs to be preprocessed in-order to detect the minutiae point. So some feature extractions are done on the fingerprint such as image enhancement, binarization, segmentation and thinning. Once the preprocess have completed the minutiae points are extracted. The minutiae extraction has performed by a technique called crossing number (CN), which is popular and commonly used. The fuzzy vault make a one way hash function for encryption process. Intra class variations can be held by this encryption. The fuzzy vault system relies on Galois field ($GF(2^{16})$) for constructing the vault. In-order to recover the secret key the vault decoding process reconstruct the polynomial.

Babak P. G. et al. [2] introduced a euclidean-distance based fuzzy commitment scheme for biometric security. The method used a key binding approach by assisting a helper data with any attempt to recreate the key. The scheme usually consists of a function F to commit a codeword c and witness x. The codewords are used for error correction. The fuzzy commitment method has been applied to iris data. The two components for commitments are offset and hash of the codeword. F is constructed by the help of hash. In authentication stage it recreates the codeword and the result of the hash function should match with the hash which is stored. Another scheme is also proposed by *Babak P. G. et al*.[2]. In this the number of the lattice points are increased by a more compact sphere packing and by changing the direction of the packing. Here the attacker has to identify the intersection of the translated line on which all feasible feature vectors are located and the lattice points in the path of the data to maximise the secured lattice points. *S Chauhan et al.* [9] proposed an improved fuzzy commitment scheme. The scheme has five modules namely encoder module, feature extraction module, data base module, ECC decoder module and comparator module. Encoding operation is performed by error correction encoder module. The comparator module decides whether the authentication is successful or not by the comparison of hash value of the key obtained and the stored hash value.

M Seo et al. [3] proposed the creation of a biometric based key derivation function. The BB-KDF consists of two algorithms.(1) the public parameter generation algorithm and (2) the deterministic algorithm (KDF). Biometric such as fingerprint and face is represented as real number vector. A biometric vector is unique to each user and hence it is used as the idea of a user. The privacy is guaranteed by BB-KDF. The key derived by the BB-KDF is secure. Fuzzy extractor has been widely used to generate keys from biometric information. In BB-KDF scheme, every user can generate a key with the help of a public parameter and the users on biometric vector. In the construction non-adaptive PRF is used to uniformly distribute the inputs source of a hash function. The security of the BB-KDF is ensured by stating that only a public parameter is revealed and it consists of a threshold vector, and a PRF and its key and a hash function. The public parameter doesn't have any relation to the user's biometric vectors and hence it is not possible to extract any meaningful biometric information in it.

Randa F. S. et al. [4] proposed a cancellable iris recognition method with the help of comb filter. The 2D Gabor filter is used as local band-pass filter. Gabor filter localizes the frequencies in an image with some optimal joint localization rather than Fourier transform that only indicates spatial frequencies in an image. The iris code is generated using the coarse-to-fine algorithm for segmentation. To make the scheme insensitive to the threshold value, morphological processing are done. Daugman operator is used for building the circles of both pupil and iris region. Log Gabor filter is used to mine the properties. The iris templates are disfigured intentionally with the multi-passband comb filter. The generated deformed templates are used at the stage of biometric verification. The comb filter resembles a comb as if places equally spaced zeroes with the shape of magnitude responds. Comb filters have the ability to pass or eliminate some frequencies.

O. C. Abikoye et al. [5] proposed a template generation using steganography and cryptography. The study combines cryptography and a steganographic approach called least significant bits to solve the problem of attacking and hacking biometric templates. Once the image is preprocessed it is split into two segments namely A & B. Segment was encrypted with Twofish algorithm to produce a cipher image a while segment B is encrypted with 3DES to produce cipher B. The template is generated by hough transform, iris normalization and iris feature extraction using Log Gabor filter. The 3DES algorithm has a key dimension of 64 bits and block dimension of 64 bits. Once both the cipher images are obtained they combined together to get cipher image C. The cipher image is embedded into a cover image using LSB. The embedding is done by change and substitute the LSB of the cover image with each bit of two ciphers one by one. The stego image is stored and retrieved whenever the template is requested by genuine user. Anjali *A. S. et al. [10]* proposed a DWT based approach for steganography using biometrics. It embeds a confidential data on skin as it is not visible to human visual system.

G. Panchal et al. [6] proposed an approach to finger print biometric based cryptographic key generation. The work proposes a cryptographic key generation based on finger print features. The minutiae points, delta points and core points are extracted from the finger print image. Once these points are identified the straight line attributes are calculated. The image is segmented into small blocks for this purpose and then all points inside a block are connected to the points inside the neighbouring blocks. These features are combined together to generate a bio-crypto key. The feature vector has been passed through reed-solomon encoder to generate a codeword. This codeword is concatenated with the bio-crypto key and stored separately. *G Panchal et al.* [8] also proposed a biometric based cryptography for digital data security without any key storage. The feature extraction identify the finger print alignment, which has the advantage that it is able to accurately rotate the finger print image.

I. CONCLUSION

Biometric Cryptosystems have gained importance in identity management systems which is used widely on banking, hospital and many other situations where security is mandatory. This paper contains an abstract view on various methods proposed in recent years on biometric template protection. The survey took a look at the various methods for biometric cryptosystems. The various methods discussed in the paper can be implemented based on the needs.

ACKNOWLEDGMENT

We would like to thank our Director of IHRD and the Principal of our institution for providing us the facilities and support of our work. We express our heartfelt gratitude to Jyothi R.L., Asst. Professor in dept. Computer science of our institution for providing timely advice and valuable suggestions to complete our work.

REFERENCES

[1] D. Chitra and V. Sujitha, “Security analysis of prealigned fingerprint template using fuzzy vault scheme,”Cluster Comput vol.22, pp.12817–12825, 2019.

[2] B. P. Gilkalaye, A. Rattani and R. Derakhshani, "Euclidean-Distance Based Fuzzy Commitment Scheme for Biometric Template Security," 7th International Workshop on Biometrics and Forensics (IWBF), Cancun, Mexico, pp. 1-6,2019.

[3] M Seo, J H Park, Y Kim, S Cho, D H Lee, J Y Hwang, "Construction of a New Biometric-Based Key Derivation Function and Its Application", Security and Communication Networks, vol. 2018, pp.14, 2018.

[4] Soliman, R.F., Amin, M. & Abd El-Samie, F.E. “Cancellable Iris recognition system based on comb filter,” Multimed Tools Appl vol. 79, pp.2521–2541, 2020.

[5] Abikoye, Oluwakemi & Ojo, Umar & Bamidele, Awotunde & Ogundokun, Roseline, "A safe and secured iris template using steganography and cryptography,” Multimedia Tools and Applications. vol. 79, 2020.

[6] G. Panchal, D. Samanta, “A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security,” Computers & Electrical Engineering vol. 69, pp.461-478, 2018.

[7] W. Ponce-Hernandez, R. Blanco-Gonzalo, R. Sanchez-Reillo and J. Liu-Jimenez, "Template protection approaches: Fuzzy Vault scheme,” International Carnahan Conference on Security Technology (ICCST), pp. 1-5, 2019.

[8] Panchal, G., Samanta, D. & Barman, S. “Biometric-based cryptography for digital content protection without any key storage”, Multimed Tools Appl. vol. 78, pp.26979–27000, 2019.

[9] Chauhan, S., Sharma, A. Improved fuzzy commitment scheme. Int. j. inf. tecnol. (2019).

[10] A. A. Shejul and U. L. Kulkarni, "A DWT Based Approach for Steganography Using Biometrics," International Conference on Data Storage and Data Engineering, pp.39-43, 2010.