A Study of Cancellable Fingerprint Template Generation Techniques using cryptography

Partheeba.R[1], Dr.N.Radha[2]

[1]Research Scholar, Dept.of .Computer Science, PSGR Krishnammal College for Women, Coimbatore.
[2]Assistant Professor, Dept.of .Computer Science, PSGR Krishnammal College for Women, Coimbatore.

---***---

Abstract - *Secure Transmission of data needs ensured cryptographic technique with most effective solution. Network Security has become a great threat to the Network Accessible Resources that consists of the policies to prevent and monitor unauthorized access, modification, misuse of a computer network and network-accessible resources. Several numbers of algorithms and techniques were proposed for the secure transmission of data and to protect user's privacy. Secret-key cryptography and public-key cryptography are the two major cryptographic architectures that are defined for the protection of security issues. Secrecy of the cryptographic key holds the security of the system. Thus key management is the main issue in the cryptography. Hence several key generation methods were developed and ensured for privacy over communication. This work brings a study of various techniques used for network security and how biometrics was used for the authentication, key generation purposes and security purposes in the network. The proposed techniques are compared on the basis of the parameters to prove its efficiency.*

Key Words: Symmetric cryptography, Cryptographic key generation, Biometric security, Crypto-biometric system, Network security.

1. INTRODUCTION

Several schemes were proposed to provide efficient protection for the network security. Among them cryptography is the ancient and more protective. Cryptography, the art of writing in secret code has its goal extended beyond merely making data unreadable into user authentication. Secret-key cryptography and public-key cryptography are the two major cryptographic architectures. Secrecy of the cryptographic key holds the security of the system. Therefore, the key issue in cryptography is key management. The key size is a major fact in protection. If the key size is simple and short then it is easy for an attacker to hack. Rather if it long and complex it is difficult to memorize. So any smart card or token can be used. But if the smart card is stolen or the password used for the smart card is guessed then there is no use of it. Then biometrics was integrated with cryptography.

Biometric authentication refers to the use of automatic personal recognition based on the physical and behavioural characteristics of an individual. Biometrics provides greater security and convenience than earlier used identity authentication systems. The biometrics is associated with a particular individual, such that it is not stolen, forgotten, lost or attached. The main problem in a biometric system itself is the security of the unique biometric data, as once it is compromised. The whole authentication system is compromised.

Biometrics and cryptography has the potential to provide a higher assurance of the legal information holder. Here the key management is implemented in case of combining the biometrics of the users. There are many techniques presented to combine biometrics with a cryptosystem, namely biometrics key generation, biometrics key binding and biometrics key release. In a key release mode, key would be released to the users only if the biometric matches. In the key generation mode, the key of a cryptosystem is derived directly from a biometric template. The unique biometrics provides a unique key based on some transform or feature extraction. The key binding mode has a system that binds a cryptographic key with the user's biometrics for enrolment and the key would be retrieved only upon a successful authentication. The modes of a biometric cryptosystem may change based on the difference between biometrics and cryptographic key. The cryptographic system almost depends on an accurate key matching process and does not tolerate a single bit error. But the biometric characteristics are known to be variable and noisy. The biometric sample is always different and it is ok if there is an approximate match under a threshold between the input biometric data to the stored template to make authentication successful. During the past several years, a number of researchers have made efforts on this issue and have attempted to design secure bio-cryptosystems. This paper shows several techniques and discusses their advantages and disadvantages.

2. BACKGROUND STUDY

Yao-Jen Chang et al., [1] proposed a framework in order to generate stable cryptographic keys from biometric data. The work differed from prior work as it had user-dependent transforms to be utilized to generate more compact and distinguishable features of the fingerprint. A longer and stable bit stream was generated as the cryptographic key using the features. More distinguishable features were obtained by cascading two-class classifiers. The feature binarization was extended to be multiple discrete values so that the each feature may contribute multiple bits effectively. However the system lacks overall performance.

Sunil V. K. Gaddam et al., [2] proposed a fresh methodology for the efficient and secure storage of fingerprint template by generating secured Feature Matrix. The keys for cryptographic techniques for data encryption or decryption was built with the help of cancellable biometric features.This paper proposed a technique to produce cancellable key from fingerprint where the flexibility and dependability of cryptography was enhanced using cancellable biometric features. It employeddistortion of fingerprint in a repeatable fashion and it uses the fingerprint thus obtained. A new fingerprint can be obtained when the old one is stolen, by altering the parameters of the distortion process. However it consumes more time for the process.

Sanjay Kanade et al., [3] proposed an effective protocol to share crypto-biometric keys securely. Another protocol was proposed to generate and share session keys that are being changed for each communication session.Without the need of trusted third party certificates, this protocol achieved mutual authentication between the client and the server. When the user verification was successful, it yields a long key so that it produced a strong link between the user identity and his cryptographic keys. It also facilitated easy online updating of the templates that were cancelable. The protocols were evaluated for biometric verification performance on a subset of the NIST-FRGCv2 face database successfully. However it do not accommodate for multi biometric modalities.

Jagadeesan et al., [4] proposed an efficient approach that was based on multimodal biometrics such as Iris and fingerprint to generate a secure cryptographic key. The security was further enhanced with the difficulty of factoring large numbers. Initially the features, minutiae points and texture properties were extracted from the fingerprint and iris images respectively. After that the extracted features were fused at the feature level to obtain the multi-biometric template. At last, a multi-biometric template was used for generating a 256-bit cryptographic key. However the proposed work had high computational complexity.

Chulhan Lee et al., [5] proposed a new method in order to generate cancelable bit-strings templates from fingerprint minutiae. The proposed method generated cancelable templates where the pre- alignment of fingerprints was not necessary. Main aim was to map the minutiae into a predefined 3 dimensional array that consists of small cells. It also finds out which cells include minutiae in the fingerprint. One of minutiae was chosen as reference minutiae and other minutiae were translated and rotated to map the minutiae into the cells based on the position and orientation of the reference minutiae. Then after the mapping process, the cells in the 3D array were set to 1 if they include more than one minutiae otherwise the cells are set to 0. One Dimensional bit-string was generated and the order of the 1D bit- string was permuted according to the type of reference minutiae. At last, cancelable bit-strings were generated by changing the reference minutia into another minutiae in turn. When the PINs were duplicated the proposed system lacks its efficiency.

Kai Xiet al., [6] presented a bio-cryptographic security protocol for client/server authentication in a secure server. The fingerprint biometric was used in user verification, protected by efficient Public Key Infrastructure (PKI) scheme and Elliptic Curve Cryptography (ECC). Fingerprint information was hidden in the feature vault. This vault is the mixture of legitimate and malicious features of finger print. The proposed protocol provided a secure and trust worthy authentication of remote mobile users over insecure network too.

Chulhan Lee et al., [7] proposed a method to generate cancelable bit-strings from fingerprint minutiae. This proposed method provided a simple mean to generate cancelable templates without the requirement of pre-alignment of fingerprints. The minutiae was matched into a predefined 3 dimensional array of small cells. It also finds which cell includes minutiae.One of minutiae was chosen as reference minutiae and other minutiae were translated and rotated for mapping the minutiae into the cells.The cells in the 3D array was set to 1 after mapping if they include more than one minutiae, otherwise the cells were set to 0. By sequentially visiting the cells, a1D bit-string was generated. At last cancelable bit-strings were generated by changing the reference minutiae into another minutiae in turn.

Wong et al., [8] proposed a low complexity revocable fingerprint template called Multi-line code. The proposed Multi-line code enhances the performance by combining the several single line codes involving the inspection of minutiae distribution along a straight line constructed based on the reference minutiae. Thus the fingerprint template is generated efficiently with better network security providing diversity and revocability. However, the proposed method requires large storage capacity as the template is stored as a real number string.

Zhe Jin et al., [9] presented a protection technique for fingerprint to secure the fingerprint minutiae. Graph-based Hamming Embedding (RGHE) was used such that the generated binary template was protected against inversion by using a minutiae descriptor, as Minutiae Vicinity Decomposition (MVD). It was utilized to get a set of randomized geometrical invariant featuresalong with random projection of the fingerprint. Randomized MVD was then improved by User specific Minutiae Vicinities Collection scheme. Graph-based Hamming Embedding was used to embed the MVD. Binary template has a strong concealment of the minutiae vicinity that protects the location and orientation of minutiae effectively. The matching attributed to bit-wise operationswere also fast.

Zhe Jin et al., [10] proposed a fingerprint template protection technique to secure the fingerprint minutiae. Randomized Graph-based Hamming Embedding (RGHE) was incorporated to generate the binary template that could be strongly protected against inversion. This method adopted a minutiae descriptor, called as Minutiae Vicinity Decomposition (MVD) in order to derive a set of randomized geometrical invariant features along with the random projection in the system. Then discrimination of the randomized MVD was improved by User specific Minutiae Vicinities Collection scheme. It was the embedded into a Hamming space using Graph-based Hamming Embedding technique. There are various advantages in this technique namely, it efficiently protects the location and the orientation of the minutiae points, well preserved discriminability of the MVD, the templates are revocable and it is a fast approach. However the MVD features are highly likely to reveal the minutiae vicinity.

Mengxing Li et al., [11] addressed about the construction of privacy-preserving protocols for securing the fingerprint minutiae based on the combination of garbled circuit and homomorphic encryption. The proposed work promised protection for both template and transaction. The user's private key is used to encrypt the template stored on the server.Template can be updated or revoked by re-encryption technique. In this paper, two hybrid protocols with the combination of homomorphic encryption and garbled circuit were presented to fulfill the minutiae matching. Euclidean distance was utilized as distance measures in one protocol and in the other, city block distance was adopted. Thus the efficient circuits were implemented using the corresponding tasks. The main disadvantage of the system is that in incurs less efficiency at times.

DilaraAkdogan et al., [12] proposed a new secure key agreement protocol where biometrics with unordered set of features was used. The proposed protocol enabled the user and the server to agree on a symmetric key that was generated by the feature points of the user's biometrics only. The proposed protocol did not generate the key randomly or it did not use any random data in the key itself, but it used fingerprints. A threshold-based quantization mechanism was used to group the minutiae in a predefined neighborhood in order to increase the chance of user-server agreement on the same set of minutiae points. The acceptance or the rejection decision was made depending on the calculated similarity score on the common set of minutiae. The cancelable form of template was not used.

Cai Li et al., [13] proposed a new security analysis framework where the information-theoretic approach and computational security were combined. This paper constructed a fingerprint-based Multi Biometric Cryptosystem (MBC) using decision level fusion. The work mainly consists of two parts namely, a newbio-cryptosystem-oriented security analysis framework anda practical fingerprint-based MBCD construction.Hash functions are utilized in the construction of the MBCD to protect each single biometric trait further. However consumes more storage space.

Usha Subramaniam et al., [14] presented a system in which the cryptographic keys aregenerated using biometrics and conventional cryptographic algorithms. By using these keys a shared session key is generated between E-Passport and ES. Since, biometric concept is integrated with the conventional cryptography; this method is used to develop a best authentication system. The proposed method satisfies the following security goals like unique identification, Authenticity of the message,data confidentiality by the shared secure of sessionkey, privacy of the E-Passport holder and Integrity of data guaranteed by signatures. The proposed method can also be used to transmit information securely for real time applications.

Subhas Barman et al., [15] proposed an approach for the generation of the cryptographic key from cancelable fingerprint template of both the sender and the receiver. The Cancelable fingerprint templates of them were securely transmitted to each other using a key-based steganography technique. Thetemplates were combined with concatenation based feature level fusion technique to get a combined template. The Elements of combined template were then shuffled using shuffle key and then the hash of shuffled template generated a unique session key for communication. A revocable key for symmetric cryptography was generated from irrevocable fingerprint and privacy of the fingerprints is protected by the cancelable transformation of fingerprint template in the proposed approach. However it lacks session based cryptographic key.

Andrew Beng Jin Teoh et al., [16] proposed cancelable biometrics realization with the multi-space random projections. The proposed approach introduces a new template using a set of user-specific random numbers from biometrics data. However, the generic two-factor non invertible mixing process is carried out by linear subspace projection, which is known as Multi-space Random Projections (MRPs). The two-factor authentication system has the advantage of avoiding any attack with a single factor that attempts with a stolen token or fake biometrics that works with the traditional system.

Lee et al., [17] proposed a method for generating cancelable fingerprint templates without requiring alignment of input fingerprint images. While obtaining invariant values the errors may happen. To reduce such errors this method creates changing functions by linear interpolation and the sum of two random number generators whose seeds are user's PIN. This method involves Preprocessing, Minutiae extraction, Calculation of invariant value, Changing functions and Minutia movement and generation of a cancelable template.

Emile J. C. Kelkboom et al., [18] presented a framework for analytically estimating both the genuine and impostor HD pmfs from the analytically estimated bit-error probability. In this approach, the central limit theorem is employed for the real world features and uses PGC framework for modeling. Then for each component has its own channel with the corresponding additive Gaussian noise representing the biometric variability and measurement noise, called the within-class variability. Thus the biometrics performance can be significantly improved.

Jaishanker K. Pillai et al., [19] proposed a biometric of iris recognition using random projections and sparse representations. The proposed unified approach for iris image selection and recognition efficiently handles the common distortions in iris image acquisition like blur, occlusions, and segmentation errors. The incorporation of random projections and random permutations into the proposed method to prevents the compromise of sensitive biometric information of the users.

Li & Jiankun et al., [20] proposed a security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar (P-P) minutiae structures. It provides solution for template/key protection without registration. P-P minutiae structure is used to describe relationships between reference minutiae. To gain the information of original features minutiae matcher algorithm is converted into transformation-invariant feature-applicable version. The proposed vault selects both genuine and chaff features to reduce the decoding time. For security purpose P-P minutiae structure is converted before being encoded into the fuzzy vault.

3. COMPARISON OF METHODOLOGIES

3.1 Comparison based on methods, advantages and disadvantages

This section provides the overall comparison of all the analyzed papers and provides the merits and de-merits listed in a comparison table given below.

Table -1: Comparison based on the techniques

S.NO	TITLE	AUTHORS	METHODS	MERITS	DEMERITS
[1]	Biometric based cryptographic key generation from faces	B.Chen, VinodChandran	Distinguishable feature generation and a stable key generation mechanism.	Feasible and encouraging	Lacks optimal performance.
[2]	Efficient Cancellable Biometric Key Generation Scheme for Cryptography	Sunil VK Gaddam,ManoharLal	Cancellable biometric Crypto System	High Flexibility and dependability	Consumes more time due to the higher response time for key generation
[3]	Generating and sharing biometrics based session keys for secure cryptographic applications	SanjayKanade, DijanaPetrovska-Delacrétaz, and Bernadette Dorizzi	Biometrics based session-key generation and sharing protocol	Revocability, template diversity, and privacy protection	Does not accommodate for multi biometric modalities
[4]	Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature	A. Jagadeesan, T. Thillaikkarasi, K. Duraiswamy	Multimodal biometrics fusion techniques	Better Authentication and security	High computational complexity
[5]	Cancellable fingerprint templates using minutiae-based bit-strings	ChulhanLee, Jaihie Kim	Generatingcancelable bit-strings (templates) from fingerprint minutiae	Highly secure and reduced distortion	When the PINs were duplicated the performance becomes poor.
[6]	A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobilecomputing environment	Kai Xi, Tohari Ahmad, Fengling Han, Jiankun Hu	Public KeyInfrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC) protocols are used for user verification	Secure and trustworthy authentication	Less efficient fingerprint matching schemes
[7]	Fingerprint template protection with minutiae-based bit-string for security and privacy preserving	ZheJin, Andrew Beng Jin Teoh, Thian Song Ong, Connie Tee	Polar Grid based 3-tuple Quantization (PGTQ)	Enhanced security	However, when PINs were duplicated the performance was not highly secure.
[8]	Multi-line code: A low complexity revocable fingerprint template forcancelable biometrics	Wong, W. J., Wong, M. L. D., & Kho, Y. H	Multi-line code	High diversity and revocability	Requires large storage capacity as the template is stored as a real number string
[9]	Non-invertible analysis on Graph-based Hamming Embedding Transform for protecting fingerprint	Zhe Jin, Goi Bok-Min, Andrew Beng Jin Teoh, Yong Haur Tay	Graph based Hamming Embedding (GHE)	Strong concealment, faster	Computational cost is high

	minutiae				
[10]	A non-invertible randomized graph-based hamming embedding for generating cancellable fingerprint template	Zhe Jin, Meng-Hui Lim, Andrew Beng Jin Teoh, and Bok-Min Goi	Randomized Graph-based Hamming Embedding (RGHE)	Effectively protects the location and orientation of minutiae, fast approach, template is revocable.	MVD features are highly likely to reveal the minutia vicinity,
[11]	Minutiae Matching with Privacy Protection Based on the Combination of Garbled Circuit and Homomorphic Encryption	MengxingLi, QuanFeng, Jian Zhao, Mei Yang, Lijun Kang, Lili Wu	privacy-preserving protocols of fingerprint minutiae based on the garbled circuit and homomorphic encryption	Improves Security and privacy	Less efficient
[12]	Secure key agreement using pure biometrics	DilaraAkdogan, DuyguKaraoglanAltop, Albert Levi	hash functions and threshold mechanisms	Highly robust, low error rates.	The templates generated were not cancelable.
[13]	A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion	Cai Li, Jiankun Hu, Josef Pieprzyk, Willy Susilo	Biometric cryptosystems,entropy-based security analysis of finger print based cryptosystems.	Stronger Security and efficient authentication accuracy	Consumemuch computer storage.
[14]	A Biometric Based Secure Session Key Agreement using Modified Elliptic Curve Cryptography	UshaSubramaniam, KuppuswamiSubbaraya	Public Key Infrastructure (PKI) and radio frequency identification technologies	Enhanced Security	Validation of session key is not performed
[15]	Cancelable biometrics realization with multispace random projections	Andrew Beng Jin Teoh & Chong Tze Yuang	Two-factor cancelable biometric formulation	Avoids single factor attack	Feature extraction needs further enhancements
[16]	Alignment-free cancelable fingerprint templates based on local minutiae information	Lee, C., Choi, J. Y., Toh, K. A., Lee, S., & Kim, J	Alignment-free cancelable Fingerprint templates	Achieves reproducibility and non-invertibility	Stealing & misuse of user's PIN can increase the false accept rate
[17]	Binary biometrics: An analytic framework to estimate the performance curves under gaussian assumption	Emile J. C. Kelkboom, Gary Garcia Molina, Jeroen Breebaart, Raymond N. J. Veldhuis, Tom A. M. Kevenaar, and Willem Jonker	Binary Biometrics	Optimum estimation of the class variability enhancing authentication	False acceptance due to dependence between the feature components and corresponding bits
[18]	Secure and robust iris recognition using random projections and sparse representations	Jaishanker K. Pillai, Vishal M. Patel, Rama Chellappa, and Nalini K. Ratha	Unified approach for iris image selection and recognition using random projections and sparse representations	Efficiently handles common distortions Better matching performance	Consumes more memory and computation requirements
[19]	A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures	Cai Li, and Jiankun Hu	Alignment-free fuzzy vault-based fingerprint cryptosystem	Improved recognition accuracy	Brute force attack is not detected due to logically rigorous and thorough security analysis
[20]	Fingerprint-based crypto-biometric system for network security	SubhasBarman, DebasisSamanta, SamiranChattopadhyay	Concatenation Based Feature Level Fusion Technique	Highly secure and robust.	Feasibility of the approach for attacks other thankey attacks,replay attack, man-in-middle attacks has to be analyzed

3.2 Comparison based on Parameters

Various Techniques for Cancellable fingerprint template generation were studied and their processes were compared based on the merits and demerits incurred. Each of the work has an advantage of its own. The techniques incur knowledge about the fingerprint based authentication techniques and also provide knowledge for the development of more advanced techniques. Table 2 infers that the parameters list primarily includes False Rejection Ratio (FRR), False Acceptance Ratio (FAR), and Equal Error Rate (EER).

Table -2: Comparison based on Error rates

Authors	**Method**	**FAR**	**FRR**	**EER**
B.Chen et al.,[1]	Distinguishable feature generation and a stable key generation mechanism.	0.045 %	0.05 9%	5%
Sanjay Kanade et al.,[3]	Biometrics based session-key generation and sharing protocol	0%	5.6%	-
Chulhan Lee et al., [5]	Generating cancellable bit-strings (templates) from fingerprint minutiae	1%	-	10. 3%
Kai Xi et al.,[6]	Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography(ECC) protocols are used for user verification	11%	3%	5.4 %
Zhe Jin et al.,[7]	Polar Grid based 3-tuple Quantization (PGTQ)	0.5%	-	-
Wong et al.,[8]	Multi-line code	0	2%	-
Zhe Jin et al.,[10]	Randomized Graph-based Hamming Embedding (RGHE)	4.36%	2%	1%
Mengxing Li et al.,[11]	privacy-preserving protocols of fingerprint minutiae based on the garbled circuit and homomorphic encryption	0.01%	-	0.0 45 %
Dilara Akdogan et al.,[12]	Hash functions and threshold mechanisms	3%	3%	0.5 7%
Cai Li et al.,[13]	Biometric cryptosystems, entropy-based security analysis of finger print based cryptosystems.	0.001 %	0.07 4%	-
Andrew Beng Jin Teoh et al.,[15]	Two-factor cancellable biometric formulation	-	-	18 %
Lee, C et al.,[16]	Alignment-free cancelable Fingerprint templates	-	-	3.4 %
Emile J. C. Kelkboom et al.,[17]	Binary Biometrics	-	-	0.1 5%
Jaishanker K. Pillai et al.,[18]	Alignment-free fuzzy vault-based fingerprint Cryptosystem	0.28%	10%	5.2 8%
Subhas Barman et al.,[20]	Concatenation Based Feature Level Fusion Technique	0	-	0.0 02 %

From table 1 and 2, it is inferred that the Fingerprint-based crypto-biometric system for network security [15] is efficient in all aspects such as reduced error rate and also the FAR and FRR rates depend on the EER rate which is too small and also had least running time of 2 seconds.

4. CONCLUSION

In this study, the performances of various Cancellable Fingerprint Template Generation techniques were discussed and the techniques were compared based on their merits and demerits. The study focussed on understanding the template generation techniques in order to enhance the network security. The studied techniques are compared interms of error rates from which it can be found that the Fingerprint-based crypto-biometric system for network security is highly efficient. Though the Fingerprint-based crypto-biometric system has minimum error rate and running time, still there is scope for enhancement. In future, specific concentration should be given on including improved key generation approaches using reduced false detection concepts.

REFERENCES

[1] Chen, B., & Chandran, V. (2007). Biometric based cryptographic key generation from faces. In IEEE 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394-401).

[2] Gaddam, S. V., & Lal, M. (2010). Efficient Cancellable Biometric Key Generation Scheme for Cryptography. *IJ Network Security*, vol.*11*, no.2, pp.61-69.

[3] Kanade, S., Petrovska-Delacrétaz, D., & Dorizzi, B. (2010). Generating and sharing biometrics based session keys for secure cryptographic applications. In *2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, pp. 1-7.

[4] Jagadeesan, A., Thillaikkarasi, T., & Duraiswamy, K. (2010). Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. *International Journal of Computer Applications*, vol.*2*, *no.*6, pp.16-26.

[5] Lee, C., & Kim, J. (2010). Cancellable fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications*, vol.*33*, *no*.3, pp.236-246.

[6] Xi, K., Ahmad, T., Han, F., & Hu, J. (2011). A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. *Security and Communication Networks*, vol.*4*, *no*.5, pp.487-499.

[7] Jin, Z., Teoh, A. B. J., Ong, T. S., & Tee, C. (2012). Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. *Expert systems with applications*, vol.*39*, no.6, pp.6157-6167.

[8] Wong, W. J., Wong, M. L. D., & Kho, Y. H. (2013). Multi-line code: A low complexity revocable fingerprint template for cancellable biometrics. *Journal of Central South University*, vol.*20*, *no*.5, pp.1292-1297.

[9] Jin, Z., Bok-Min, G., Teoh, A. B. J., & Tay, Y. H. (2014). Non-invertible analysis on Graph-based Hamming Embedding Transform for protecting fingerprint minutiae. In IEEE *2014 International Conference on Electronics, Information and Communications (ICEIC)*, pp. 1-2.

[10] Jin, Z., Lim, M. H., Teoh, A. B. J., & Goi, B. M. (2014). A non-invertible randomized graph-based hamming embedding for generating cancellable fingerprint template. *Pattern Recognition Letters*, vol.*42*, pp.137-147.

[11] Li, M., Feng, Q., Zhao, J., Yang, M., Kang, L., & Wu, L. (2014). Minutiae Matching with Privacy Protection Based on the Combination of Garbled Circuit and Homomorphic Encryption. *The Scientific World Journal*, DOI= http://dx.doi.org/10.1155/2014/525387

[12] Akdoğan, D., Altop, D. K., & Levi, A. (2015). Secure key agreement using pure biometrics. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 191-199.

[13] Li, C., Hu, J., Pieprzyk, J., & Susilo, W. (2015). A new bio-cryptosystem-oriented security analysis framework and implementation of multi-biometric cryptosystems based on decision level fusion. *IEEE transactions on Information Forensics and Security*, vol.*10*, *no*.6, 1193-1206.

[14] Subramaniam, U., & Subbaraya, K. (2015). A Biometric Based Secure Session Key Agreement using Modified Elliptic Curve Cryptography. *International Arab Journal of Information Technology (IAJIT)*, vol.*12*, *no*.2, pp.155-162.

[15] Teoh, A. B. J., & Yuang, C. T. (2007). Cancelable biometrics realization with multispace random projections. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol.*37*, *no*.5, pp.1096-1106.

[16] Lee, C., Choi, J. Y., Toh, K. A., Lee, S., & Kim, J. (2007). Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol.*37*, *no*.4, pp.980-992.

[17] Kelkboom, E. J., Molina, G. G., Breebaart, J., Veldhuis, R. N., Kevenaar, T. A., & Jonker, W. (2010). Binary biometrics: An analytic framework to estimate the performance curves under gaussian assumption. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol.*40*, *no*.3, pp.555-571.

[18] Pillai, J. K., Patel, V. M., Chellappa, R., & Ratha, N. K. (2011). Secure and robust iris recognition using random projections and sparse representations. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.*33*, *no*.9, pp.1877-1893.

[19] Li, C., & Hu, J. (2016). A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures. *IEEE Transactions on Information Forensics and Security*, vol.*11*, *no*.3, pp.543-555.

[20] Barman, S., Samanta, D., & Chattopadhyay, S. (2015). Fingerprint-based crypto-biometric system for network security. *EURASIP Journal on Information Security*, vol.*2015*, *no*.1, pp.1-17.