Proceeding of ICITS 2022 e-ISSN: 2716-6732
7th International Conference on Information Technology
& Society October 7th & 8th, 2022, Selangor, MALAYSIA

Various Techniques to Protect Templates for Biometric System

Shubham Jain and Peeyush Tomar

Computer Science and Engineering Department, Vidya College of Engineering, Meerut (UP), India 250005

shubhamjain01.sep@gmail.com

Abstract. Biometric identification methods have grown in popularity in recent years. Traditional password and token-based authentication systems are rapidly being replaced by biometric technologies. The two most critical elements to consider when creating biometric systems are security and recognition accuracy. To a considerable extent, biometric authentication based on multimodal fusion can overcome the challenges associated with the existence of unimodal biometrics. However, if a multimodal biometric template is stolen, the consequences are worse, hence it is vital to research template protection techniques for multimodal biometric systems. This paper discusses several template protection systems such as DNA, Cancellable Biometric, Cryptosystem, Hashing, Fuzzy, and Blockchain.

Keywords: Biometric, DNA, Cancellable Biometric, Cryptosystem, Hashing, Fuzzy, Blockchain.

INTRODUCTION

Biometrics are biological measurements that allow us to identify individuals based on physical traits such as retina scanning, fingerprint mapping, and facial recognition. It is the science of identifying people based on biological, anatomical, or behavioral characteristics. A biometric trait must have four main characteristics: It must be universal, which means that most people must have the trait; (ii) it must be distinctive, which means that it must differ from person to person; and (iii) it must be permanent, which means that it must be invariant (regardless of matching criteria) over time; and (iv) These properties make biometrics a dependable answer to person recognition, and biometric features cannot be transmitted, forgotten, guessed, shared, or lost like other ways of personal recognition such as passwords, ID-cards, and so on. The unique biometric identity of each individual is used to replace or supplement password systems for computers, mobile devices, and restricted access secret rooms and buildings. After obtaining and mapping biometric features data, it is saved in the biometric template database to be compared and matched with future efforts at the moment of access. Most systems encrypt this data and store it on the device or on a remote server.

RELATED WORK

The ideal method for protecting biometric templates must satisfy the following require ments: (1) Security system must make it extremely hard to identify between the real patte rn and the fake pattern; (2) if the fake pattern is lost, the administrator can immediately re voke it and introduce a new altered pattern based on the same biometric information; (3)

Diversity: to secure user privacy, if a cancelled biometric pattern is changed by a new te mplate, it should not be linked with any other users; and (4) Diversity. The biological pattern security system strategy may be classified into two parts [2]: (1) The template transform method includes technology to project the user's unique key into the transformation space, making it difficult to recover the original pattern. (2) Helper repository strategy: The template is limited to a passcode, and a security system sketch is generated from the error-correcting code. The cipher template is then put in instead of the original biometric template. We can easily decipher the sketch and recover the pattern by getting a query that is sufficiently close to the registered template.

A DNA molecule's fundamental structure, which is either real or made up, can be viewed of as a string of letters used to carry genetic information. The four fundamental components of DNA are represented by the letters A, C, G, and T (adenine, cytosine, guanine, and thymine). Each letter stands for a base; a base pair is made up of two bases. Four base pair molecules make up one DNA molecule. There are two set criteria for matching base pairs: A-T and C-G [2]. Each pixel in a digital image is known to be represented by an 8-bit binary integer. Binary numbers can be expressed using the letters A, C, T, and G to represent the digits 00, 01, 10, and 11 respectively. This allows a pixel to be encoded into a series of nucleotides. Consider a pixel in a digital image with a grey value of 225; the binary value for 255 is 11100001. As per the DNA Coding rules given in Table I, the binary string corresponding to the nucleotide of gray value 225 is "TGAC". As per the Table I, there are eight coding combinations that can be applied.

TABLE I. DNA Coding Rule

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	10	01	10
G	10	01	01	00	11	10	10	01

TABLE II. DNA Addition Rule

+	**A**	**T**	**C**	**G**
A	A	T	C	G
T	T	G	A	C
C	C	A	G	T
G	G	C	T	A

TABLE III. DNA Subtraction Rule

-	**A**	**T**	**C**	**G**
A	A	C	T	G
T	T	A	G	C
C	C	G	A	T
G	G	T	C	A

The DNA adding and subtracting operations are similar to the conventional algebraic adding and subtracting rules.

The double helix can be seen in DNA adding operation, whereas the DNA subtracting operation does not show the double helix, in Table II and Table III. Here the DNA subtracting operation is taken as the corresponding decryption rule.

Fuzzy vault is a powerful technology that improves the security risk present in the storage of cryptographic keys by integrating the traditional cryptographic protection scheme with biometric authentication. For standalone protection and authentication equipment in the form of system-on-chips (SoC), biometric encryption systems based on fuzzy vault methods are particularly beneficial. However, the current fuzzy vault methods require several computationally demanding operations to make them functional. The fuzzy method's most important and computationally demanding step is the noise generation, or "chaff generation," which creates noise points that obscure the true points inside the vault pattern. By using straightforward algebraic operations, Mohamed et al. [20] introduced a novel chaff generation algorithm that is computationally quick and cost-effective for hardware acceleration. The difficulty of the algorithm, according to the study, is O(n2), which is a significant improvement over the O(n3) complexity of the existing technique. The proposed technique outperforms the sophisticated Clancy's algorithm by a factor of over 130 for the creation of 500 chaff points, according to experiments. The fuzzy vault strategy is now much more likely to be used in a SoC environment with limited resources thanks to the updated chaff generation algorithm.

By combining a cryptography key with the biometric patterns, a biometric cryptosystem secures the biometric patterns. In these kinds of systems, neither the key nor the biometric information is maintained in a database. Only the helper data, which results from fusing the key with the biometric patterns, is stored by biometric systems.

Information regarding the key or biometrics is not included in the helper information. When the actual biometric data is provided, it is used to recover the system key. Systems for system key generation and systems for system key binding are two categories for biometric cryptosystems.

The key is formed and limited with biometric data in the system key binding scheme to create helper information, which is then stored in the database. The system key is produced independently from biometric data in the key binding mechanism. If there is a match between the two sets of biometric data and an error-correction code (ECC) is employed to manage biometric data changes, the system key will be released during the authentication phase. In the system key generation process, a biometric pattern is used to generate the helper information, which is then used to generate the cryptographic system key. This method converts non-uniform binary biometric information into uniform binary strings using a fuzzy separator technique known as a secure sketch (SS) with strong randomness separator. Later cryptographic applications can use these strings as encryption keys. The features template may be turned into a new template via the feature transformation scheme. Bio-hashing and non-invertible transform are the two basic methods for achieving transformation. By projecting the feature vector with the transformation matrix and a binary key, the biometric template is converted into a binary code by code in the bio-hashing method, which then thresholds the individual elements. The confidentiality of the biometric template is maintained by the non-invertible transform technique. In this method, a biometric template is converted into a cancellable template that has no information about the original template. The cancellable template cannot be used to recreate the original template. A new cancellable template will be constructed and change the disfigurement features of the non-invertible transform if the stored template has been attacked. The third strategy is a hybrid that incorporates the first two strategies.

VARIOUS TECHNIQUES

We will first talk about DNA sequence coding, and then we'll talk about biometric systems that use fuzzy, hashing, blockchain, cancellable, and cryptography.

DNA sequence is the actual or fictitious primary structure of a DNA molecule, which uses a chain of letters to carry genetic data.

A unique multimodal biometric template protection technique based on DNA encoding was suggested in reference [2]. The multimodal template is first turned into a DNA sequence by DNA encoding, followed by the generation of a chaotic DNA sequence, the addition of these two DNA sequences, and finally the conversion of the sum of these two DNA sequences into decimal numbers, from which we derive the encrypted template. The experiment's findings, which are presented in this work, demonstrate that the suggested multimodal biometric template protection strategy both assures the security of the multimodal biometric template system and does not impair the biometric system's ability to recognise individuals [2].

The original template in the experiment possesses the properties of face and palmprint. Using the PolyU palmprint repository and ORL repository, the facial characteristic and palmprint features are mined with PCA and merged like f p qi = + to provide the modal image of the system. The main criteria for calculating the performance of a recognition algorithm are the False Match Rate (FMR) and False Nonmatch Rate (FNMR). The algorithm's total performance is determined by its equal error rate (EER). According to the experiment's findings, the original algorithm's and the proposed one's EERs are both 3.5%.

In a multi-biometric authentication, Sujitha et al. [3] used the fuzzy vault approach as the security system of palm prints and fingerprint features. Users will be documented using the biometric connected and shed on polynomial during the registration or encoding process. The chaff points would be merged with the new vectors when this vector designs a secret key to create the vault. During the authentication (decryption) phase, the reverse encoding (encryption) technique could be used, yielding a false accept rate (FAR) value of 0.02 at polynomial degree 14. A fuzzy vault was suggested by Baghel et al. [4] as a way to protect the features and characteristics. By integrating the actual vault place with noise points, they were capable of improving the fuzzy vault. The enroll template and authentication template were aligned using principal component analysis (PCA). The FVC2002 DB1 dataset with polynomial degree = 9 yielded 0.28 and 4.55 for FAR and equal error rate (EER), respectively, while the FVC2002 DB2 dataset with polynomial degree = 10 yielded 0.06 and 4.79 for FAR and EER, respectively, and the FVC2004 DB1 dataset with polynomial degree = 10 yielded 1.77 and 17.35 for FAR and EER, respectively.

Reference [1] authors suggested utilizing different k-lengths to analyze the performance of the system. Recurrent neural networks (RNNs), which are built on top of convolutional neural networks, are used to extract touch traits from raw touch information (CNN). The touch template is subject to the FCS for the purpose of the template security system, and helper data is kept in the system storage area as opposed to the touch-gesture template. Two different touch datasets, the Touchalytics dataset and the BioIdent dataset, were used to compute the suggested system. The prime outcomes were produced with a key length of k = 98 and n = 255; for the Touchalytics dataset, the FAR was 0.00 and the FRR was 0.5754, whereas for the BioIdent dataset, the FAR was 0.006 and the FRR was 0.5499. The FCS demonstrates its strength in dynamic authentication security systems.

To secure the finger vein patterns, Kirchgasser et al. [5] created a cancellable template system security technique based on index-of-maximum (IoM) hashing. To remove the finger vein feature, they employ six methods: Gabor filter (GF), isotropic undecimated wavelength transform (IUWT), maximum wavelength curvature (MWC), principal curvature (PC), repeated line tracking trait (RLT), and broad line detector feature (WLD). When utilizing the PC trait selection strategy on the UTFVP datasets, the major outcome was EER = 0.81.

Jindal et al. [6] combined the FCS methods of biometric cryptosystems with transform-based approaches to provide a novel hybrid method for securing the facial template biometrics system. For all of the photos, they used the VGG-Face architecture to draw out face patterns and translate the features to binary code. Following that, the cryptographic hash (SHA3-512) algorithm is applied to the binary code and feature vector to generate a 512-bit cryptographic hash that is saved in the database. For the PIE datasets, the significant result was an EER of 0.15% ± 0.03%.

Yang et al. [22] created a new cancelable fingerprint template using random projection. Because of the decorrelation algorithm's properties, the developed template can defend against attacks via record multiplicity (ARM). In the meantime, the approach's proposed Delaunay triangulation-based local structure mitigates the unfavorable impact of nonlinear distortion on matching performance. Some novel proposals for improving protection and recognition performance included the use of multimodal cancelable biometric systems. Later, Yang et al. [7] proposed an unique multimodal cancelable biometric system that combines the fingerprint trait and the finger-vein trait to achieve excellent recognition accuracy and security. The partial discrete Fourier transform is employed in this upgraded system to give non-invertibility and revocability.

The partial Hadamard transform was proposed by the authors of reference [8] as an effective non-invertible transformation for securely protecting binary biometric representations in the construction of cancelable biometrics. When this non-invertible transform is performed to the DFT of binary biometric representations, the resulting templates are complex vectors that cannot be converted to the original binary vectors. The suggested technique is notable for its ability to keep the stochastic gap between all binary vectors after the transformation. This stochastic gap maintenance property has been theoretically demonstrated and experimentally validated. The proposed partial Hadamard transform creates cancelable fingerprint templates that meet all of the requirements for revocability, diversity, non-reversibility, and performance. The designed cancelable innovative templates outperform state-of-the-art approaches that also include system security in the binary biometric representations in terms of matching efficiency.

Yang et al. [9] proposed using the cancelable fuzzy vault system to encrypt the Delaunay triangular group based on fingerprint features. Cancellable transformation is produced using polar transformation. Because the transformation unit is a triangle rather than a single minutia, the system is less vulnerable to biometric uncertainty. Alam et al. [10] improved biometric cryptosystem system by combining conventional Discrete Fourier Transformation (DFT) with innovative random projection based cancelable approach to better biometric system security. The suggested technique employs traditional DFT and random projection to build polar grid-based biometric features, which are then used to generate non-reversible system security templates. Furthermore, a bit-toggling approach is employed to introduce noise into the created template in order to improve template system security.

In reference [11], authors created alignment-free cancelable fingerprint system security templates using a revolutionary blind system identification technique. The quantized pair-minutiae vectors used to create the unique binary string, which must be safeguarded, are used as the input for the suggested algorithm's frequency samples. It is suggested to protect the frequency samples of the binary string, which are treated as the source input, by opposing or dissatisfying the identifiability conditions so that they cannot be obtained from the output complex vector results. This is motivated by the identifiability of the source signals in blind system identification (transformed template). In all identifiability circumstances, the suggested transformation in the algorithm is irreversible.

The approach proposed by [19] converts a real-valued feature vector into an index code in such a way that the pairwise-order measure in the hashed code is highly linked with the rank similarity measure. This type of ranking-based hashing has two important advantages: (1) it is resistant to noises/disturbances in numerical values; and (2) it provides extremely nonlinear embedding based on rank correlation statistics. The former is concerned with accuracy performance while minimizing numeric noises/disturbance, whereas the later provides strong non-reversible translation from Euclidean to Rank space via nonlinear feature embedding, resulting in firmness in inversion while preserving accuracy performance. The experiment results show that the benchmark FVC2002 and FVC2004 fingerprint databases perform rather well in terms of accuracy. The study justifies its resistance to preimage attack, inversion, and brute force in order to meet the revocability and unlikability criteria of cancellable biometrics.

The authors of reference [17] proposed a trained biometric recognition system in a distributed architecture based on block chain technology to allow fault tolerant access. The main advantage of this proposed strategy is that tampering with one component of a biometric system alerts the entire system and aids in the quick identification of any potential faults. Authors [17] demonstrated that the suggested approach provides system security to both the learning model and the entire biometric template during experiments in several biometric modalities.

In a "system security-trust model," it is easier to trust a community than a specific individual because decisions are made only when most of the community agrees. It is one of the benefits of adopting a dispersed architecture for biometric template matching. [17] Inspired by this, the authors of reference [17] created a template, auto-correcting, and tamper-proof parameter block chain-based architecture for biometric recognition. The suggested learning model can safeguard several phases of the biometrics identification pipeline, notably feature extraction, matching, and template storage, as demonstrated by studies on face and fingerprint modalities, demonstrating the efficacy of the proposed approach. Cryptographic computations, particularly symmetric key decryption, and encryption, are computationally intensive activities, therefore computation time is a critical limitation. These operations provide irrefutable system security but take time to compute.

Experiments are carried out to determine the new model's efficiency and system security utilizing both face and fingerprint modalities. The results of face identification were reported utilizing subsets of the CMU Multi-PIE Face Database and the Multiple Encounters Database (MEDS-II). The findings of fingerprint identification were published on a subset of the CASIA fingerprint database. Using a pre-trained CNN network, the VGG-Face model is used as the feature extractor, with each layer modelled as a block of the chain. The blocks' parameters include biases, kernels, and the activation function for the convolution layers, pool size for the max-pooling layers, and weights, biases, and the activation function for the deep layers, which use the Python implementation of Shamir's secret sharing to implement the key sharing matrix. Face, fingerprint, and heartbeat identification were performed by comparing the gallery and probe security system templates using the two-distance metrics first Cosine similarity and second Euclidean distance.

The authors of reference [18] investigated specific factors by constructing a smart contract on Ethereum (public blockchain) for biometric template storage, the cost-performance of which was tested by adjusting the complexity of state-of-the-art schemes for handwritten signature and facial biometrics. Experiments using a prominent paradigm in biometric research, such as deep learning techniques and databases, are being reported. As a result, simple techniques for data storage in blockchain, both direct and hash-based, can be used to constrain biometric template storage utilizing cutting-edge biometric

approaches. Using a blockchain technique based on Merkle trees [8] demonstrates a reasonable cost-performance tradeoff.

Exploring the unique biometric system viability based on block chain, focused on storage of biometric security system templates that have been about critical cost-performance tradeoffs such as transaction execution time, economic cost, and biometric performance. Discussing Ethereum's main storage schemes and putting in place a smart contract to estimate storage costs. The results show that real biometric systems are not appropriate when using straightforward schemes such as direct storage of biometric security templates on-chain or direct data hashing, but when Merkle trees is implemented as an intermediate data structure, storage costs become fixed regardless of the total volume of data to store and execution time for writing operations is reduced to 10 to 15 seconds while read operations or security template retrieval is obtained in 10 to 15 seconds. This demonstrates that the integration of biometrics with public blockchains or Ethereum is feasible, both economically and in terms of performance, utilizing two case studies of state-of-the-art technologies and protocols in face and signature biometrics.

To protect iris and fingerprint security system templates, Macek et al. [12] used two schemes: cancellable system template (non-invertible transforms) and key generation. The key is derived from the iris biometric property and then hashed before being saved in the system storage. The fingerprint characteristic is used to construct the cancellable system template. The prime results produced with a key length of 192 had a FAR of 0% and a FRR of 5.75%.

Hoang et al. [13] and Elrefaei et al. [14] used FCS to defend a gait template system in their behavior biometric template security system. The binary key is created at random and then encoded to a codeword using the BCH encoding technique. The key hash code will then be computed. The template will then be safeguarded by employing a hash function to attach the cryptographic key to the biometric template. The database stores the helper information for authentication. The result showed that FAR is 0.0%, while FRR varies for different key lengths. For key length equal to 139, FRR is 16.18%, for key length equal to 71, FRR is 20.59%, and for key length equal to 50, FRR is 14.91% [14]. For key lengths of 50, FAR and FRR were 0% for the CMU MoBo dataset, while for key lengths of 45, FAR and FRR were 0% for the CASIA A database [14]. Furthermore, Nagakrishnan et al. [15] developed a new biometric template security system methodology based on the DNA encoding method and chaotic mapping in speech-based authentication systems to safeguard a person's voice template. A person's voice is utilized to derive Mel frequency cepstral coefficient (MFCC) properties, which are subsequently clustered to reduce memory gaps. Using the AVSpoof database, the system accuracy was 97%. Furthermore, Zhi et al. [16] propose protecting a touch stroke template with a cancelable template protection approach based on learning IoM hashing. The IoM hashing transforms the template into indices of the greatest values selected from a set of random projections of the original template characteristics. Using the Touchalytics dataset and a custom trait extraction technique. By using intra-session scenario, the primary result was EER = 9.50 with a length of m = 30.

CONCLUSION

This study provides a complete review of biometric system assaults and alternative approach mechanisms for fingerprint-based biometric systems. Twenty research publications on biometric security systems are evaluated, analyzed, and examined. In light of recent system threats, this paper examines and summaries some recent research results for template protection. Despite improvements in identification accuracy and current breakthroughs in biometric template security systems, there are still a few open loop flaws.

We highlight a few research challenges and future prospects in the following sections: i.) Deep learning approaches have enhanced the performance of biometric systems across a wide range of biometric modalities, including facial recognition. Deep learning approaches are expected to be useful tools for latent fingerprint matching. However, the employment of deep learning algorithms may result in biometric system alerts due to the vulnerabilities of those deep learning techniques. ii.) The security challenges caused by a wide range of attacks at various stages of a biometric system (e.g., spoofing, DoS, and so on) investigated for a standard biometric system are also applicable to any biometric system on different platforms, such as fingerprint scanner electronic gadgets. In today's environment, cellphones, which are nearly universally used, constitute a viable platform for the use of biometric features. However, cellular biometrics confront additional hurdles because smartphone typically have limited processing capabilities and battery. As a result, designing light-weight, secure, and reliable algorithms for mobile biometrics systems may be major research subjects. iii. The trade-off between security system and identification accuracy in fingerprint template security system is still a concern. Aside from further study, more robust and different characteristics, and better transformation functions, multi-biometrics in template security schemes are likely to represent the path forward and require much farther investigation.

TABLE IV. Performance comparison of various protection technique

Category	Type of Biometric	Year	Database / Dataset	Best Performance
Dynamic touch gesture	Fuzzy	2022	Touchalyticts dataset	FAR= 0.00 FRR= 0.5754
			Bioldent dataset	FAR= 0.00 FRR= 0.5279
DNA Coding for multimodal system	DNA Coding	2017	ORL Database (facial)	EER=3.6%
			PolyU Palmprint Database	
Fuzzy to secure fingerprint pattern	Fuzzy	2012	FVC2002 DB1	FAR=0.38 EER=4.60 polynomial degree 9
			FVC2002 DB2	FAR=0.16 EER=4.89 polynomial degree 10
			FVC2004 DB1	FAR=1.57 EER=18.35 polynomial degree 10
Security system approach based on IoM hasing	Cancellable biometric	2020	UTFVP Dataset	EER=0.52
Face template protection design	Cryptosystem biometric	2018	PIE Dataset	EER=0.25%± 0.01%
Defeat the attacks via record multiplicity (ARM) through the	Cancellable Biometric	2019	FVC2002 DB1	EER=5.75%
			FVC2002 DB2	EER=4.71%
			FVC2002 DB3	EER=10.22%
			FVC2004 DB 2	EER=12%

feature decorrelation algorithm design				
Cancelable multi-biometric system based on fingerprint and finger-vein	Cancellable Biometric	2018	MD-A MD-B	EER=0.45% EER=0.67%
A partial Hadamard transform approach	Cancellable Biometric	2018	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3 FVC2004 DB2	EER = 1.6% EER = 2% EER = 5.2% EER = 13.3%
A minutiae-based fuzzy vault with cancellability by applying a polar transformation to each Delaunay triangle group	Cancellable biometric	2013	FVC2002 DB1, DB2	FAR=0.38%FRR = 19% FAR=2.25%FRR = 8%
Bit-toggling strategy to inject noise into the proposed fingerprint template	Cancellable biometric	2018	FVC2002 DB1, DB2, DB3 FVC2004 DB1, DB2, DB3	EER=1% EER=2.07% EER=6.11% EER=15.44% EER=9.15% EER=9.28%
A blind system identification template approach	Cancellable Biometric	2016	FVC2002 DB1 FVC2002 DB2 FVC2002 DB3	EER=4% EER=3% EER=8.5%
Machine vision gait-based biometric design	Cryptosytem and fuzzy	2019	CMU MoBo dataset CASIA A dataset	FAR=0.0% FFR=0.00% (key length=50) FAR=0.0% FFR=0.00% (key length=48)
Touch-Stroke Template Protection	IoM hasing	2019	Touchanalytics datasets	EER=9.60

REFERENCES

1. Asrar Bajaber, and Lamiaa Elrefaei, “Biometric Template Protection for Dynamic Touch Gestures Based on Fuzzy Commitment Scheme and Deep Learning,”
2. Jinjin Dong, Xiao Meng, Meng Chen, and ZhifangWang, “Template Protection Based on DNA Coding For multimodal biometric recognition,” 4th ICSAI 2017.

3. Sujitha & D. Chitra "A Novel Technique for Multi Biometric Cryptosystem Using F.0.0uzzy Vault," Journal of Medical System. 2019, 43, 1–9.
4. Vivek Singh Baghel, Surya Prakash & Ity Agrawal, "An enhanced fuzzy vault to secure the fingerprint security system templates." Multimed. Tools Appl. 2021, 80, 33055–33073
5. Simon Kirchgasser, Christof Kauba, Yen-Lung Lai, Jin Zhe, and Andreas Uhl, "A. Finger Vein Template Protection Based on Alignment-Robust Feature Description and Index-of-Maximum Hashing," IEEE Trans. Biom. Behav. Identity Sci. 2020, 2, 337–349.
6. Arun Kumar Jindal, Srinivas Chalamala, and Santosh Kumar Jami, "Face Template Protection using Deep Convolutional Neural Network," IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, UT, USA, 18–22 June 2018.
7. Yang Wencheng,,Wang Song,,Hu Jiankun,,Zheng Guanglou,, and Craig Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," Pattern Recogn. 2018, 78, 242–251.
8. Song Wang, Guang Deng,, and Jiankun Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint security system templates containing binary biometric representations," Pattern Recogn. 2017, 61, 447–458.
9. Wencheng Yang, Jiankun Hu, and Song Wang, "A Delaunay triangle group based fuzzy vault with cancellability," 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, 16–18 December 2013; pp. 1676–1681.
10. Badiul Alam, Zhe Jin, Wun-She Yap, and Bok-Min Goi, "An alignment-free cancelable fingerprint template for bio-cryptosystems," J. Netw. Comput. Appl. 2018, 115, 20–32.
11. Song Wang, and Jiankun Hu, "A blind system identification approach to cancelable fingerprint security system templates," Pattern Recogn. 2016, 54, 14–22.
12. N. Maˇcek, B. Đordevi´c, J. Gavrilovi´c, and Lalovi´c, "An Approach to Robust Biometric Key Generation System Design," Acta Polytech. Hung. 2015, 12, 43–60.
13. T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," Int. J. Inf. Secur. 2015, 14, 549–560.
14. L.A. Elrefaei, and A.M. Al-Mohammadi, "Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme," J. King Saud Univ. Comput. Inf. Sci. 2019.
15. R. Nagakrishnan, and A. Revathi, "A robust cryptosystem to enhance the security system in speech based person authentication," Multimed. Tools Appl. 2020, 79, 20795–20819.
16. J. Zhi, S.Y. Ooi, and A.B.J. Teoh, "Learning-Based Index-of-Maximum Hashing for Touch-Stroke Template Protection," 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Suzhou, China, 19–21 October 2019.
17. Akhil Goel, Akshay Agarwal, Mayank Vatsa, Richa Singh, and Nalini Ratha, "Securing CNN Model and Biometric Template using Blockchain" IEEE 2020.
18. Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana and Ruben Vera-Rodriguez, "Biometric Template Storage with Blockchain: A First Look into Cost and Performance Tradeoffs,"
19. Zhe Jin, Jung Yeon Hwang, Soohyung Kim, Sangrae Cho, Yen-Lung Lai1, and Andrew Beng Jin Teoh, "A Cancellable Ranking Based Hashing Method for Fingerprint Template Protection"

20. Mohamed Khalil-Hani, Muhammad N. Marsono, and Rabia Bakhteri "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," Future Generation Computer Systems Volume 29, Issue 3, March 2013, Pages 800-810
21. Yang Wencheng,,Wang Song,,Hu Jiankun,,Zheng Guanglou,, and Craig Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review" 2019
22. Wencheng Yang, Jiankun Hu, Song Wang, and Qianhong Wu "Biometrics based Privacy-Preserving Authentication and Mobile Template Protection," Wirel. Commun. Mobile Comput. 2018, 2018, 17.