# New cancelable iris biometric templates protection technique using new prime code

Tawheed Hassan Mohammed Ahmed Alabed
University of Khartoum
**4** PUBLICATIONS **0** CITATIONS

Review article

# New cancelable iris biometric templates protection technique using new prime code

Tawheed Hassan Mohammed Ahmed **Alabed**[1*], Faisal Mohammed **Abdallah**[2], Mohammed Bakri **Bashir**[1], Nazim Osman **Bushara**[1], Abdel Fattah **Awad Elkariem**[3]

*1- Department of Computer Science, Faculty of Computer Science and Information Technology, Shendi University, Shendi, Sudan, *tawalabed@gmail.com*

*2- Department of Computer Science, University of Karary, Khartoum, Sudan*

*3- Information Technology Center, Shendi University, Shendi, Sudan*

**Abstract**

With the increasing application of biometric systems in various applications increased needs a reliable solution to the problem of user authentication. Identity privacy, unlinkability users at different applications; integrity and revocability are the main requirements to designing a biometric system to achieve privacy and security at the biometric system. Due intra users variability at biometric systems authentication create a challenge to protect the biometric template due that variability in the acquired biometric traits and disclosed sensitive information for bad attacker. This paper proposed a new iris biometric templates protection technique using a new prime code cancelable unique code. It has 0.0333 FAR and 0 FRR and TSR 99. 89%.

**Keywords:** Biometric, security, privacy, cancelable, cryptosystem.

## Introduction

Biometric is composed of two wards bio and metric which means “life” and “to measure” [1]. Biometric is known on [2] as the physical and logical unique traits of humans, which differ from one to another person defined as a person's unique identification (ID) [3]. Biometric identification taxonomies as physical or behavioral traits like iris, ear, face, hand, finger, and gaits. In addition to these past taxonomy biometric characteristics generally has three categories inherent, technical and procedural [4]. The inherent biometric characteristics proposed at [5] have four characteristics classified as collectability, universality, permanence and universality. Also, efficiency and getting the accuracy of the extraction and matching of biometrics is a technical characteristics related to the different technical implementations used to build biometric system. at designing a biometric system, the manner in which the biometric is calculated should also not influence its performance [4]. On the performance characteristic, the passport service from United Kingdom in 2005 did trials biometrics, which found that the face recognition rate had get a success rate of 69%, fingerprints access rate of 81% and the iris recognition 96%, which preferred on both men and women [4]. Procedural characteristics are added to the chosen biometric(s) if applied multi-modal biometric solutions or biometric traits may use at many applications which lessing circumvention [6]. Diversity characteristic appearing when we need to applied biometric traits at different application for more than one purpose [7]. Also, the reusability procedure is applied to revoke or reissue the biometric for conciliation [4]. Every biometric system mainly consists of four modules proposed at [8]: first module is the enrollment registers into biometric database system. Here, biometrics reader can scan the biometric characteristic to produce the digital representation. Second module is feature extraction processes which generate a template from input sample to store it in a database or a smartcard issued to the individual. Matching module compares the input with the template to perform identity verification.

The rest of the paper organized as follows: section 2 presents biometric system security and privacy threats. In sections 3 biometric template protections in 4 section new cancelable approaches for iris template protection technique. Lastly concludes the paper at 5.

## Biometrics security and privacy threat

Biometric systems designed mainly to securing the access to information at applications used biometric recognition authentication. There are many advantages of applied biometric systems like having same identification for two users in the biometrics security technology system is nearly zero [9]. Biometric technologies implemented identification execute at security environment make it less prone for users to share access to sensitive data, that because biometric traits cannot be forgotten or stolen. Also, this technique need less effort for execution except DNA/retinal/iris recognition [9]. Building a genuine identification at verification considered as main challenge at designing biometric system recognition [10]. Still many problems hinder the verify this goal present at [11] like noisy data caused by defected sensors and defective physical and unfavorable conditions and all that causes incorrectly matched or rejected. Also intra-class variations problems face building a genuine user, which appeared in case of the different between the data acquired at authentication and the enrollment data generating affect at matching procedure. All these problems consider basis building for many attacking types [12]: attacking at sensor, attacking signal attacking feature extracting module, attacking representation of biometric feature by tampering it. The matcher corrupt and tampering with the stored templates, attacking the channel between the matcher and the stored template to overriding the final decision. The privacy of genuine users requires identity privacy, irreversibility and unlinks ability between different applications. Also, the security requires confidentiality, integrity and renewability or revocability if a threat. Table 1 present the required of privacy, security and present threat which face security and privacy. The

Identity privacy is achieved by saving a process of storing biometric reference data which related with other identity data.

**Table 1.** Security and privacy requirement, threats and attack

| **Security and privacy** | **Biometric system requirement, threats and attack** | | |
|---|---|---|---|
| | Requirement | Threats | Attack |
| Privacy | Identity privacy<br>Irreversibility<br>Unlinkability | Cross match data subjects across different services or applications by comparing biometric references. | Link users between different databases |
| | | Sharing the characteristic and moving beyond its original purpose by using function creep concept. | Function Creep |
| | | Possibility to extract sensitive information from the stored biometric data. | Function Creep |
| Security | Confidentiality<br>Integrity<br>Renewability and revocability | Data capture subsystem attacks, Signal processing subsystem attacks, Comparison subsystem attacks , Storage subsystem attacks<br>Decision subsystem attacks , Transmission and other attacks | Sensor spoofing<br>A coercive attack<br>Trojan horse<br>Tampering with the storage subsystem.<br>Hill climbing attack.<br>Brute force attack |

Also, the finding a linking points between identities data on different application allows this malicious to link data by using biometrics. Also, choosing irreversibility at designing attributes to prevent using biometric for any other purpose. Additionally, biometric reference unlinkable at different applications to stopping tracking and tracing subjects to guarantee that no attacker has a random guessing in determining a related two biometric references. The confidentiality of saved information from unauthorized attackers. Also, protected storage and transmission data which need cryptographic techniques [13]. The integrity at security concern is the property of saving the accuracy and completeness of assets. Moreover, verification will come bad if the integrity of a biometric reference or the results of the various processing subsystems aren’t trusted. Also, users have limited biometric traits, so identity theft renders corresponding biometric references as unusable for future use in risk. So, the renewability and revocability is requirement at security to make ability to cancel and update biometric reference.

**Biometric template protection**

Discretion of confidentiality is main security supporting to ensure information privacy from bad attacker. At enrollment phase biometric data is stored which need to save it securing. Securing procedure need to finding ways to protected it against unauthorized disclosure, eavesdropping, or modification of the data. All that concern built new approaches to protect biometric data which classified at [14] to cryptosystem and feature transform schemes, Fig. 1.

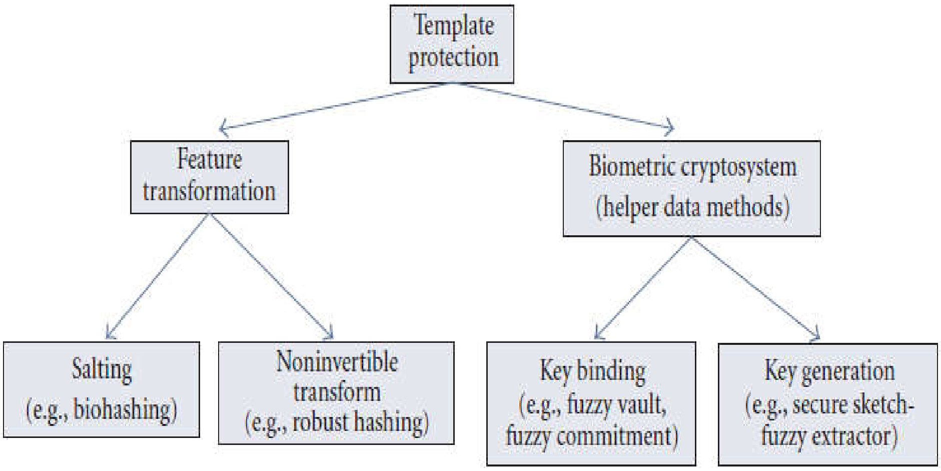
Template protection
Feature transformation
Biometric cryptosystem (helper data methods)
Salting (e.g., biohashing)
Noninvertible transform (e.g., robust hashing)
Key binding (e.g., fuzzy vault, fuzzy commitment)
Key generation (e.g., secure sketch-fuzzy extractor)

**Figure 1.** Categorization of template protection schemes [14]

***Biometric cryptosystem approach***

This scheme designed to protect biometric template to ensure information privacy from bad attacker which presented on [15]. The key cryptography at this approach developed by using features from biometric template or generating key directly from templates. Here, a helper data is generally taken from public biometric template information's [16]. The method of collecting or generating this information determine the type of key cryptosystem approach, which taxonomies as key generation and key binding [14]. The security and unique information amount determine security level [14]. The binding procedure at key binding scheme implement to create a new biometric template which containing a secret key on the biometric data. On the [17] cryptographic algorithms is used to applied the binding procedure. So, complexity of the key binding and storing it securely consider basic challenges on this aspect. The bit replacement process to hiding key on biometric template consider as a main procedure [18]. So that to release some bits from biometric template and replaced it by key. Fuzzy commitment scheme, fuzzy vault and shielding functions [19] consider as a techniques using this approach.

The evaluation of biometric template protection approaches done by using concepts of false reject rate (FRR) and false accept rate (FAR) [20]. It measures the probability of person wrongly identified as another one. Also, the amount of overlap between two distributions can calculated them by normalized area between 0 and the separation point, κ, to determine false accept rate in the inter-class distribution. Also, FRR determined by normalized area between the separation point, κ, and 1 in the intra-class distribution. The iris template protected using fuzzy commitment scheme in [21], [22], [23], [24], [25] evaluated by FRR 0.47%, 5.62%, 6.65%, 4.64% and 4.92%. Also, at [26] implement fuzzy vault for iris too which get 0% FRR. Face template protection applied fuzzy commitment scheme in [27] and [28] evaluated as 7.99% and 0.47%. in addition to that, implement this approach too at fingerprint on [29], [23], [27] and [30] evaluated as 0.9%, 2.73%, 7.99% and 4.92%. Also using FAR for [31], [32], [33], [34], [35], [36] evaluated as 0%, 0.24%, 0.01%, 0%, 0% and 0%. EER evaluated [37] as 2.1%. Moreover fingerprint protected using fuzzy vault at [38] evaluated as genuine acceptance rate = 90%.

However, the cryptographic key will be retrieved from the same location in a template each time a different user is authenticated by the system. Thus, if attacker find the location of bit, he specify the key and reconstructed the embedded binding key from any identifies users' templates. If an attacker had access to the enrollment program then he could determine the locations of the key by enrolling several people in the system using identical keys for each enrollment. Key generation approach is extract hashing value or get cryptographic key directly from the biometric data [39]. They are implemented either as secure sketches or fuzzy extractors. The method used for key generation depends largely on the nature or structure of the biometric data [14]. biometric reference used to generating a helper data which stored as updateable key or hash value extracted directly from a reference biometric data [40]. This approach applied to protect face at [41] evaluated as 7.69%. In addition, it applied too at [42] and [43] to protect fingerprint with 3.81% and 4.5% EER (equal error rate). However, there are challenges at in biometric the natural of extracted feature from biometric and algorithm of matching affect by acquisition variations in biometric identifier representation which generated by key generation [44]. The threat of applied biometric cryptosystem approach to protect biometric template by gaining illegitimate accesses to protected data, information, facilities or services [7]. The illegitimate accesses done by attacker which make a risk at security and privacy present at Table 1 to find locations of secret key bit always can easy compromised cross matching across different services. Also, sharing the characteristic and moving beyond its original purpose by using function creep concept which is new concept define as a wide widening use of a biometric system technology beyond the designation objective for which it was intended which threat the privacy [1] generally done by administrator or system users to bad done.

### *Cancelable biometric approach*

The feature transform of biometric template known as cancelable biometric template protection scheme which introduced in [12]. The main goal from create this approach is to make biometric template differ by different application. It consists of an intentional, repeatable distortion of a biometric trait based on a chosen transform. In this scheme, used a function to generate protected biometric templates and the parameter of the function is used as the key [45], and transformed biometric template can be cancelled like passwords [46]. The security of biometrics using this scheme by protects user-specific sensitive data by both intentional and systematic distortion of the extracted biometric features [47][48]. At this approach a transformation function is applied to the unprotected biometric template during enrollment, thus transforming it into a protected template to be stored in the database. The transformation function is typically governed by random parameters employed as key or a password. During verification, the same transformation function is applied to the query features using the same key/password and the matching between query and template occurs in the transformed space. Privacy and security are enhanced by using different distortions for multi different services and the true biometrics are never stored on the authentication server [8]. In addition to that cancelable approach can be used to resist attacks at template database. This approach achieve uniquely feature at any application, however there are a challenge at registration, intra-user variation tolerance, and entropy retention and transformation functions design [49]. According to characteristics of the transformation function, this category can be further divided in salting, where user specific "extra" information is added to the existing biometric template (reminiscent to password "salting" methods) [50], and non-invertible transform approaches, where a one-way function is applied to the considered templates [49].

The salting approach is one type of cancelable biometric template protection scheme, which depend on transformation of features by applied a robust transformation function 'F' on biometric template [14]. The security level here is based on saving the key or password securely. At enrollment phase, password P of the user and pseudorandom string S are concatenated before hashing H (P+S) and the hash value stored in the database securely [49]. This approach applied to protect face at [50], [51], [52], [53] and [54] evaluated as 0.001, 16, 10.915, 0 and 2.11 EER. Also, it applied to protect fingerprint [55] EER= 0.65%. Moreover, it applied to protect iris at [56], [57] and [58] with EER = 2.59, 1.3, and 2.3.

Noninvertible approach is a second type of cancelable which secured biometric template by applying a noninvertible transformation function to it. It is a one-way function, F, easy to compute, hard to convert in polynomial time [14]. This scheme applied to protect fingerprint at [59], [60], [61], [62] and [63] evaluated by computed EER = 13, 3.9, 9, 3.5, and 2.27. In addition, it applied to protect face too at [64] with EER = 3.34. Moreover, iris template protected using this approach at [65], [66] and [67] which evaluated as 0.2, 1.016 and 2.0 EER.

However it is a good cancelable scheme but tradeoff between discriminability (similarity structure) and non invertible of transformation function in that transformation function should preserve similarity structure of feature set from same user should have high similarity in the transformed space and features from different users should be different after transformation. Noninvertible classified into [54]: Geometric transform, robust hashing or bio hashing, random projections, biometric filter and random permutation.

The threat in applied this concept is also the danger of function creep by administrator person attacking by collect biometric samples of users for abuse exception or collusion. Tampering with presentation the biometric features implement by attacking storage subsystem by using the data from the sensor and replaced it with a different fraudulent features [9]. A Trojan horse attacking executed at feature vector to produces under some specific condition a pre-selected feature [2] to replace module of feature extractor with Trojan horse virus at a given time. This attacking known as an executable code which gets features recorded and sent to a server specified by the Trojan. It used as a zombie biometric modular to allow launch cyber attacks throw internet. Attacking throw sending random template to biometric system described in [5] as hill-climbing. Output of its application is recorded score of matching and continues this procedure until exceeded decision threshold score. The brute-force attack performed by sending real biometric templates to matcher module and continued until the system accepts wrongly one as corresponding to the template from the user's account under attack [6].

## New proposed iris template protection using new prime code cancelable technique

It considered as a new technique used cancelable concept to protect iris template against threats. It consists of four main steps. At the first step, Daugman model for iris applied to getting a normalization iris with size of 9600 bit. In the second step, implementation new prime code. Last step at this new cancelable approach is hashing a prime output code. Here the new iris code will be secured rather than general iris template. Step four is the matching phase, where two iris codes will be compared and a similarity score is computed. These steps are shown schematically in Fig. 2.

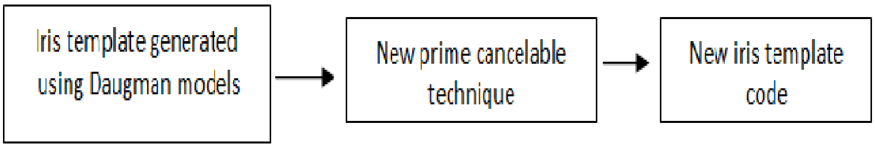
Iris template generated using Daugman models
New prime cancelable technique
New iris template code

**Figure 2.** New cancelable iris template protection technique

***Iris template generation***

Depending on Daugman model to generate iris template many steps constructed this model [68] begin with segmentation, normalization and encoding features which shown on Fig. 2 to generate 9600 bit. At this paper we implement model on cassia v1[69] and taking exactly a normalize iris image which used as input to this cancelable technique.

***Prime iris code***

After input a normalization iris image as 2D image to this new cancelable technique a prime pixel value generated. After that, output value passed to 512 hashes [70].

***Matching***

The matching procedure is evaluation the similarity of two iris representations. At this paper we implement Hamming distance [71]. At this paper constructed distance score matrix between training sample and testing for exactly person. With the CASIA V1' data set unique inter-class comparisons are possible. Also, hamming distance values are calculated. On the evaluation intra variability, distance score matrix between training sample and testing for different person constructed. With the CASIA V1'data set unique intra-class comparisons are possible. In other words hamming distance values are calculated.

**Experimental analysis**

The performance of proposed new cancelable technique which built a new iris code. It has been tested on CASIA V1 iris datasets. Performance comparison is done using FAR (false acceptance rate), FRR (false rejection rate) and computed EER (equal error rate). According to statistical theory, the mean Hamming distance for comparisons between inter-class iris templates will be 0.5. This is because, if truly independent, the bits in each template can be thought of as being randomly set, so there is a 50% chance of being set to 0 and a 50% chance of being set to 1. Therefore, half of the bits will agree between two templates, and half will disagree, resulting in a Hamming distance of 0.5 [72]. Due to this, the mean Hamming distance for inter-class template comparisons will be slightly lower than 0.5, since the lowest Hamming distance out of several comparisons between shifted templates is taken. As the number of shifts increases, the mean Hamming distance for inter-class comparisons will decrease accordingly. After that, compute false accepts rate and compute false reject rate. In addition, we decided to take 4 samples in class for training and 3 samples for testing. Suitable threshold value is 0.6 because it has 0.0333 FAR and 0 FRR and TSR 99. 89%.

The output from this new iris template protection security technique is 512 bit which is from SHA512. This hash function is one way known as message summary or compression function takes the enter variable length and converts it into a binary sequence of a fixed length. If we want to analyze it, breaking the hash algorithm is equivalent to finding a collision in the hash algorithm. We just need to find an output of the hash function that is equal to the hash of a valid password (thus "collision"). Finding a collision using a birthday attack takes O(2^(n/2)) time, where n is the output length of the hash function in bits. Also, SHA-2 has an output size of 512 bits, so finding a collision would take O(2^256) time. Given there are no clever attacks on the algorithm itself. The 2^256 actually computations which would take

2^240 * 2^-2 = 2^238 ~ 10^72s ~ 3.17 * 10^64 years Even calling this millions of years is improbably.

On the other hand, if we compared a proposed technique on CASIA V1iris database, found that it is quite challenging to compare different biometric template protection technique on CASIAV1dataset against them in a fair manner because the protection of iris template has not standard experimental protocol reported on [1].

**Table 2.** Comparative analysis of biometric template protection technique

| Paper | Technique | Result |
|---|---|---|
| [23] | Key binding using fuzzy commitment (Min-sum decoding) | FRR = 6.65<br>FAR =0 |
| [73] | Key binding using fuzzy vault (Multiple features from multiple local regions shift matching) | FAR=0.0235 |
| [56] | Salting methods | FAR = 1.43;<br>FRR = 3.75 EER = 2.59 |
| [56] | Random secret integration | FAR = 1.43% FRR =3.75%<br>EER = 2.59% |
| [74] | Fuzzy commitment | FRR=3.75%<br>FAR=0.0% |
| [75] | Cryptography | EER = 3.68% |

At Table 2, a comparative analysis on different biometric template protection implement on CASSIA V1. Authors of [23] and [73] authors applied cryptosystem approach but the threat here is key binding bit location may retrieve when cross matching data subjects across different services or applications by comparing biometric references or function creep. In addition to that, some [56] proposed a salting method called S-iris encoding to protect a template but if key is compromised, attacker had access to biometric data that may make reject for user who has a right to access. At [74] the helper data are generated by using XOR operation between (1) random key k which encoder using reed-solomon and (2) iris code. However, it more secure but if attackers know the protected template and secret key, it will be unsafe. Author of [75] proposed an encryption approach for iris technique using encryption using advanced encryption standard (AES) to make biometric more secure but possible to use reconstructed secret to retrieve original biometric data from secure template.

## References

[1] Ashok J, Shivashankar V, Mudiraj P. 2010. An overview of biometrics. *Int J Comput Sci Eng* 2: 2402–2408.

[2] Jain AK, Ross A, Prabhakar S. 2004. An introduction to biometric recognition.*Trans Cir systems Vid Technol* 14: 4–20.

[3] Le C, Jain R. 2009. A survey of biometrics security systems. EEUU. Washington University in St. Louis.

[4] van de Haar H, van Greunen D, Pottas D. 2013. The characteristics of a biometric. *Information Security for South Africa* 1–8.

[5] Gokulkumari G, Lakshmi A. 2011. Study of effects and perceptual analysis in implementing biometric authentication. *Eur J Sci Res* 61: 42–254.

[6] Manivannan S, Padma E. 2011. Comparative and analysis of biometric systems. *Int J Comput Sci Eng* 3: 2156–2162.

[7] Lalithamani N, Soman K. 2009. Irrevocable cryptographic key generation from cancelable fingerprint templates: An enhanced and effective scheme. *Eur J Sci Res* 31: 372–387.

[8] Ambalakat P. 2005. Security of biometric authentication systems. Available online: https://pdfs.semanticscholar.org/e1d7/7b951c55d7d1f322d1f96942daa77ec6c4ee.pdf.

[9] Tistarelli M, Nixon M. 2009. Advances in biometrics: 3rd international conferences, ICB 2009, Alghero, Italy, Proceedings ( Lecture notes in computer science, 5558. Springer.

[10] Schneier B. 1999. The uses and abuses of biometrics. *Comm ACM* 42: 136–136.

[11] Matyas V, Riha Z. 2003. Toward reliable user authentication through biometrics. *Secur Priv* 1: 45–49.

[12] Ratha NK, Connell JH, Bolle RM. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM sys J* 40: 614–634.

[13] Breebaart J, Yang B, Buhan-Dulman I, Busch C. 2009. Biometric template protection. *Datenschutz und Datensicherheit-DuD* 33: 299–304.

[14] Jain AK, Nandakumar K, Nagar A. 2008. Biometric template security. *EURASIP J adv Sig Pro*: 1–17.

[15] Cavoukian A, Stoianov A. 2007. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy: Information and privacy commissioner, Ontario.

[16] Vetro A, Memon N. 2007. Biometric system security. in Tutorial presented at 2nd International conference on biometrics, Seoul, South Korea.

[17] Rathgeb C, Uhl A, Wild P. 2012. Iris biometrics: from segmentation to template security 59: Springer Science & Business Media.

[18] Nair J, Kumari R. 2015. A review on biometric cryptosystems. *Int J Latest Trends Eng Technol* 6: 46–53.

[19] Jegede A, Udzir N, Abdullah A, Mahmod R. 2017. *S*tate of the art in biometric key binding and key generation schemes. *Int J Commun Netw Inf Secur* 9: 333–344.

[20] Daugman J. 2000. Biometric decision landscapes. University of Cambridge, Computer Laboratory.

[21] Hao F, Anderson R, Daugman J. 2006. Combining crypto with biometrics effectively. *Trans Comput* 55: 1081–1088.

[22] Bringer J, Chabanne H, Cohen G, Kindarji B, Zemor G. 2007. Optimal iris fuzzy

sketches. First international conference on biometrics. *Theo Appl Sys*.

[23] Bringer J, Chabanne H, Cohen G, Kindarji B, Zemor G. 2008. Theoretical and practical boundaries of binary secure sketches. *Trans Inf Forens Secur* 3: 673–683.

[24] Rathgeb C, Uhl A. 2009. Systematic construction of iris-based fuzzy commitment schemes. International conference on biometrics, Springer.

[25] Rathgeb C, Uhl A. 2010. Adaptive fuzzy commitment scheme based on iris-code error analysis. 2nd European workshop on visual information processing.

[26] Rathgeb C, Wagner J, Tams B, Busch C. 2015. Preventing the cross-matching attack in Bloom filter-based cancelable biometrics. 3rd International workshop on biometrics and forensics.

[27] Ao M, Li SZ. 2009. Near infrared face based biometric key binding. International conference on biometrics. Springer.

[28] Lu H, Martin K Bui F, Plataniotis K, Hatzinakos D. 2009. Face recognition with biometric encryption for privacy-enhancing self-exclusion. 16th International conference on digital signal processing.

[29] Teoh AJ, Kim J. 2007. Secure biometric template protection in fuzzy commitment scheme. *IEICE Elec Exp* 4: 724–730.

[30] Imamverdiyev Y, Teoh AJ, Kim J. 2013. Biometric cryptosystem based on discretized fingerprint texture descriptors. *Exp Sys Appl* 40: 1888–1901.

[31] Uludag U, Jain A. 2006. Securing fingerprint template: Fuzzy vault with helper data. Conference on computer vision and pattern recognition workshop.

[32] Nandakumar K, Jain AK, Pankanti S. 2007. Fingerprint-based fuzzy vault: Implementation and performance. *trans Info Fore Sec* 2: 744–757.

[33] Nagar A, Nandakumar K, Jain AK. 2008. Securing fingerprint template: Fuzzy vault with minutiae descriptors. 19th International conference on pattern recognition.

[34] Nguyen TH, Wang Y, Ha Y, Li R. 2015. Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints. *IET Biomet* 4: 29–39.

[35] Tams B, Merkle J, Rathgeb C, Wagner J, Korte U, Busch C. 2015. Improved fuzzy vault scheme for alignment-free fingerprint features. International conference of the biometrics special interest group.

[36] Bansal D, Sofat S, Kaur M. 2015. Fingerprint fuzzy vault using Hadamard transformation. International conference on advances in computing, communications and informatics.

[37] Nandakumar K. 2010. A fingerprint cryptosystem based on minutiae phase spectrum. IEEE International workshop on information forensics and security.

[38] Mehmood R, Selwal A. 2020. Polynomial based fuzzy vault technique for template security in fingerprint biometrics. *Int Arab J Info Technol* 17: 926–934.

[39] Dodis Y, Ostrovsky R, Reyzin L, Smith A. 2008. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J Comput* 38: 97–139.

[40] Bodo A. 1994. Method for producing a digital signature with aid of a biometric feature. *Ger patent DE* 42: 908.

[41] Nguyen TT, Dang T, Truong Q, Nguyen D. 2019. Secure biometric-based remote authentication protocol using Chebyshev polynomials and fuzzy extractor. arXiv preprint arXiv:1904.04710.

[42] Hong-wei L, Yao W. 2012. A new fuzzy fingerprint vault using multivariable linear function based on lorenz chaotic system. IEEE International conference on computer science and automation engineering.

[43] Yang W, Hu J, Wang S. 2014. A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement. *Trans Info For Secu* 9: 1179–1192.

[44] Uludag U, Pankanti S, Prabhakar S, Jain k. 2004. Biometric cryptosystems: issues and challenges. *Proceed IEEE* 92: 948–960.

[45] Patel VM, Ratha NK, Chellappa R. 2015. Cancelable biometrics: A review. *Sig Pro Mag* 32: 54–65.

[46] Kaur H, Khanna P. 2016. Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multi Tool Appl* 75: 16333–16361.

[47] Rathgeb C, Uhl A. 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J Info Secu*1: 1–25.

[48] Belguechi R, Cherrier E, Alimi V, Lacharme P, Rosenberger C. 2011. An overview on privacy preserving biometrics. *Recent Appl Biomet* 65–84.

[49] Ratha NK. Chikkerur S, Connell J, Bolle R. 2007. Generating cancelable fingerprint templates. *Trans patt anal Mach Intell* 29: 561–572.

[50] Teoh AB, Goh A,. Ngo DC. 2006. *R*andom multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *Trans Patt Anal Mach Intell* 28: 1892–1901.

[51] Teoh AJ, Yuang CT. 2007. Cancelable biometrics realization with multispace random projections. *Trans Sys Man Cyber Part B (Cybernetics)* 37: 1096–1106.

[52] Kim Y, Toh K-A. A 2007. Method to enhance face biometric security. First IEEE international conference on biometrics: *Theo Appl Sys*.

[53] Wang Y, Plataniotis K. 2007. Face based biometric authentication with changeable and privacy preservable templates. *Biometrics Symposium*, IEEE.

[54] Teoh AB, Kuan YW, Lee S. 2008. Cancellable biometrics and annotations on biohash. *Patt Recog* 41: 2034–2044.

[55] Teoh AB, Ngo DC. 2006. Biophasor: Token supplemented cancellable biometrics. 9th International conference on control, automation, robotics and vision.

[56] Chin CS, Jin AB, Ling DC. 2006. High security iris verification system based on random secret integration. *Comput Vision Image Understan* 102: 169–177.

[57] Ouda O, Tsumura N, Nakaguchi T. 2010. Bioencoding: A reliable tokenless cancelable biometrics scheme for protecting iriscodes. *Trans Inform Sys* 93: 1878–1888.

[58] Ouda O, Tsumura N, Nakaguchi T. 2010. Tokenless cancelable biometrics scheme for protecting iris codes. 20th International conference on pattern recognition 882–885.

[59] Yang H, Jiang X, Kot AC. 2009. Generating secure cancelable fingerprint templates using local and global features. 2nd IEEE International conference on computer science and information technology, Beijing, China.

[60] Zhe J, Jin AB. 2011. Fingerprint template protection with minutia vicinity decomposition. International joint conference on biometrics. Washington, DC.

[61] Ahmad T, Hu J, Wang S. 2011. Pair-polar coordinate-based cancelable fingerprint templates. *Patt recog* 44: 2555–2564.

[62] Wang S, Hu J. 2012. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping approach. *Patt Recog* 45: 4129–4137.

[63] Das P, Karthik K, Garai BC. 2012. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Patt Recog* 45: 3373–3388.

[64] Moujahdi C, Ghouzali S, Mikram S, Rziza M, Bebis G. 2012. Spiral cube for biometric template protection. International conference on image and signal processing 235–244.

[65] Hämmerle-Uhl J, Pschernig E, Uhl A. 2009. Cancelable iris biometrics using block re-mapping and image warping. 12th International conference on information security. Pisa Italy. DOI:10.1007/978-3-642-04474-8_11

[66] Rathgeb C, Uhl A. 2010. Secure iris recognition based on local intensity variations. International conference image analysis and recognition, Springer.

[67] Farberbock P, Kaaser D, Pschernig E, Uhl A. 2010. Transforming rectangular and polar iris images to enable cancelable biometrics. *Image Anal Recog* 276–286.

[68] Daugman J. 2004. How iris recognition works. *IEEE Trans Circuits Syst Vid Technol* 14: 21–30.

[69] Sciences CA. CASIA Iris image database (version 1.0) Institute of Automation.

[70] National Institute of Standards and Technology 2015. Secure hash standard. Federal information processing standards publications FIPS PUB 180–184.

[71] Rai H. Anamika Y. 2014. Iris recognition using combined support vector machine and Hamming distance approach. *Exp Sys Appl* 41: 588–593.

[72] Masek L. 2003. Recognition of human iris patterns for biometric identification. University of Western Australia.

[73] Lee YJ, Park K, Lee S, Bae K, Kim J. 2008. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Trans Sys Man Cyber B (Cybernetics)* 38. 1302–1313.

[74] Adamovic S, Milosavljevic M, Veinovic M, Sarac M, Jevremovic A. 2016. Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. *IET Biomet*. 6: 89–96.

[75] Moi SH, Abdul Rahim N, Saad P, Sim P, Zakaria Z, Ibrahim S. 2009. Iris biometric cryptography for identity document. International conference of soft computing and pattern recognition, Malacca, Malaysia.DOI: 10.1109/SoCPaR.2009.149