“Secure cancellable iris template creation scheme based on modulo operation”

a project report

Submitted by

Kavadi Lasya

Department of Information Technology

National Institute of Technology, Surathkal

Under the guidance of

Dr. M. V. N. K. Prasad

Associate Professor, IDRBT

CERTIFICATE

This is to certify that Ms. ***Kavadi Lasya***, pursuing B.Tech. in Information Technology at National Institute of Technology, Surathkal has done bonafide work on 'Secure cancellable iris template creation scheme based on modulo operation' as a project trainee at Institute for Development and Research in Banking Technology (IDRBT), Hyderabad.

Date: 07-07-2017

Place: Hyderabad

Signature of guide

ACKNOWLEDGEMENT

To find, investigate and to exhibit something new is to wander on an obscure way towards an unexplored destination is a difficult experience unless one gets a genuine light carrier to demonstrate the way. I express my sincere gratitude to my guide **Dr. M. V. N. K. Prasad**, Associate Professor, IDRBT, for his valuable guidance, proper advice and constant cordial support.

I am extremely thankful to Dr. A. S. Ramasastri, Director, IDRBT and all members of IDRBT, Hyderabad for the infrastructural facilities and support.

I express my gratitude to the authors whose work we have consulted and quoted in this work. Finally, I acknowledge the constant inspiration, encouragement and good wishes to all my friends for their cooperation and support.

ABSTRACT

Although biometric recognition systems have overcome all the drawbacks of token-based authentication systems, privacy invasion and security theft issues still persist. Suppose the original biometric data is stored without any morphing, if the data is compromised then it cannot be replaced or issued. To overcome these issues, biometric template is morphed before storing. The morphed template is called cancellable template and it is unlinkable and non-invertible. The cancellable can be easily replaced and reissued. In this paper, we proposed a novel approach of protecting biometric template based on modulo operation. The proposed method utilises consistent bit vector which is generated from pre-aligned IrisCodes. These IrisCodes are generated by applying 1-D Gabor filter on the iris images. To confirm the efficiency of proposed approach experiments are conducted on different iris datasets. By applying proposed cancellable technique, we achieved Equal Error Rate of 1.62% and 2.12% for CASIA-V 1.0 and CASIA V3-internal iris datasets respectively. This proposed methods also satisfies revocability, unlinkability and irreversibility criteria.

Table of Contents

List of Figures

List of Tables

1 Introduction

In conventional identity verification systems, possession tokens or memory based credentials such as PIN numbers, passwords, access cards, etc are used. But they cannot be trusted because passwords can be guessed and cards can be lost or stolen.As an alternative, biometrics have been introduced that exploits behavioral and physiological characteristics of human being as identities.As biometric traits are unique in every human being, the fore mentioned security problems can be overridden.Typical biometric traits are fingerprint, palm print, facial image, iris, etc. Due to its advantages, these biometric recognition systems now a days are replacing the passwords and access cards.

Among all the available biometric traits, eye iris is considered as one of the reliable traits attributed to its stability and uniqueness. The Iris remains stable throughout the life and less susceptible to environment and genetic factors[1].Besides, the entropy of iris patterns is much higher than that of other biometric traits which shows that false matches between different iris images is not likely to happen. Apart from verification, iris can also be used for identification tasks. Daugman, the first person to devise automated iris recognition systems also invented favourite iris representation known as iris codes[1].

For both identification and verification tasks, each user has to initially enroll to the system by storing his/her iris data which is in the form of template(e.g. iris code) is stored in system's database.For authentication purpose, only right person can be identified or verified by the matching of right iris from genuine user with the IrisCode.

Since these IrisCodes contains crucial information of users, these have to be protected from attackers. The exposure of IrisCodes might lead to severe attacks like replay attack and masquerade attack. Once the iris codes are exposed there would be permanent loss of identity because they cannot be reissued or replaces like access cards or PIN. Moreover, by compromising several databases it is possible to cross-match multiple templates which results in user privacy issues.

To address these security ad privacy issues, a subtopic of biometric technology has emerged called Biometric Template Protection(BTP).Instead of storing the original iris templates in

the database, these templates are transformed into protected instances i.e, distorting certain biometric features intentionally and are then stored in the database.These instances should be non-invertible.This technique is called cancellable biometrics. In this paper we focused on cancellable technique to protect the generated IrisCodes.

The attacks such as correlation, hill-climbing [15] occur due to illicit use of biometric data that reduces reliability of the biometric system.In correlation attack information is retrieved from multiple protected templates of same user and correlation is found between them to retrieve original template. In hill-climbing the matching score of a template is iteratively maximized by finding the next optimal step. So to overcome these issues , a biometric system should be able to generate different templates each time to prevent cross-matching. To design any cancellable biometric technique, below four criteria have to be satisfied[2,3]:

1. Revocability: From multiple protected templates it should not be computationally feasible to derive original template. This enables new protected template to be generated, each time when the cancellable technique is applied. The original template can be protected from adversary.

2. Unlinkability: It should be difficult to differentiate if one or more protected templates are derived from the same user's biometric.This prevents cross-matching among different applications.

3. Non-invertible: Even if the protected template stored in the database is exposed, it should be computationally infeasible to get the original template from it which enhances the security of biometric system.

4. Accuracy: The recognition performance of biometric system should be maintained high.

To obtain secure biometric template, several different approaches that have been proposed try to encounter the previously mentioned security and privacy issues. Cancellable biometrics [4] is one among them, this employs key-dependent transformation to the raw biometric data. This transformation is non-invertible i.e, original template cannot be derived from cancellable template[5].In the biohashing based cancellable method that was proposed in

[6,7,8] uniformly distributed random sequence is derived using a hash key. All these methods perform well if the tokens used for verification are different for different users. In case of stolen-token issue, the performance degrades. Du et al. [11] proposed a cancellable transformation which is non-invertible based on Gabor features. In this method, cancellable template is derived by combining radial positon information (r) with 64-bit Gabor descriptor. Pillai et al. [10] proposed a method in which iris is divided into different sectors and random projection is applied on each sector. In this method, if the projections applied are subject-specific matching accuracy gets retained. Ouda et al. [9] proposed a method in which verification of a user is based on grouping the blocks which consists of consistent bits in IrisCode. But in case of small block sizes [12], all these approaches are endangered to correlation attacks.

Another way to achieve the security of template is by the use of cryptographic construct. Hao et al. [13] proposed a method in which cryptographic key is derived using the fuzzy commitment scheme from 2048-bit IrisCode. In order to correct the bit errors, this uses Reed-Solomon and Hadamard error. The main drawback of [13] is difficulty to generate exact error-free identifiers with high entropy from noisy biometric features [15]. Dodis et al. [14] proposed a method in which secure fuzzy extractor and sketch schemes are employed. Error tolerant key generation method is used by these schemes. Although they provide security, they do not provide revocability [15].

This paper is organized as follows. Section 2 discusses the Literature review on cancellable iris biometric template. Section 3 discusses our proposed method. Section 4 gives the experimental results and analysis. Section 5 discusses Security analysis. Finally, conclusion is discussed in section 6.

2 Literature Review

From past few years, different approaches have been proposed to deal with various issues of protecting biometric templates by biometric research community. As per literature the approaches can be classified into two types namely, biometric cryptosystem and feature transformation techniques. In the following we shall go through the existing techniques of both types.

Biometric cryptosystems may be further classified two sub categories namely, key generation schemes and key binding schemes. Key generation schemes are used to obtain cryptographic keys directly from user's biometric features. Whereas key binding schemes binds cryptographic keys with biometric features in a way that it is not possible to get back the key unless the true template is produced during authentication. However, due to the introduction of error correction schemes which are necessary for key retrieval the performance of key binding schemes may be affected. It is obvious that even though both schemes offer protection to biometric templates, their main aim is to secure cryptographic keys by using biometric features. In order to attain non-invertibility Dodis et al.[14] applied hash function on error-tolerant biometric input. In this approach two functions are proposed, they are fuzzy extractor and secure sketches. In order to generate a random string fuzzy extractor applies a hash function on biometric input. This random string is used as a key. Unlike fuzzy extractor secure sketch uses this random string to reconstruct the original template. Chang et al.[21] used this method on the fingerprint biometric. Fuzzy commitment is another scheme for biometric cryptosystem proposed by Juels and Wattenberg[16]. In order to generate template this approach applies function the codeword and binary biometric input. To eliminate bit-errors the codeword is prepared with error-correcting codes. The codeword is evaluated for the query biometric data and matched using error-correcting codes at the time of verification. Bringer et al.[22] used this fuzzy commitment scheme [16] with improved error-correcting mechanism. In this approach, a matrix is formed with two different binary Reed-Muller codes. And, a 2-D iterative min-sum decoding is performed to get a 40-bit cryptographic key. Wu et al. [23] proposed an iris cryptosystem based on key generation. The iris feature vector is corrected with Reed-solomon codes. And then a hash function is

applied to generate a cipher key. Reddy and Babu et al.[24] obtained a key using password based transformation to encrypt the fuzzy vault[17].

On the other hand, the primary aim of the cancellable biometrics is to generate many revocable templates from the original template. The different approaches for cancellable biometric given in the literature can be broadly classified into two major primitives, they are biometric salting and non-invertible transforms[18]. Biometric salting associates user-specific auxiliary information with biometric data to generate a "distorted" variant of biometric template as similar to password salting (hardening) in cryptography. A very well-known approach for biometric salting is biohashing which obtains a uniformly distributed random sequence using a hash key [8, 6, 25]. In biohashing, biometric input is varied with token and discretized in binary. The performance of the approaches described in [8, 6, 25] reduces in case of stolen-token scenario. In non-invertible transform based perspective, instead of storing the original biometric, the biometric data is altered using a one-way function and stored into the database to make sure security and privacy of the actual biometric trait. Ratha et al. [4] showed interest on different irreversible methods of generating cancellable template such as grid morphing, block scrambling, Cartesian, polar and surface folding transformation. The transformations can be applied in either the signal domain or the feature domain to get distortion to attain non-invertible, revocability and to avoid cross-matching in stored biometric data among the various databases. Du et al. [11] applied a key on the original iris template which repositions the bit positions to achieve non-invertible.

Du et al. [26] proposed four different non-invertible transforms they are as follows: GRAY-COMBO, BIN-COMBO, GRAY-SALT and BIN-SALT. GRAY-COMBO method executes circular shift operation on Gabor features and random addition of rows. BIN-COMBO uses similar transformation on the iris codes with arbitrary shifting and XOR operation. Arbitrary patterns are added to the Gabor features in GRAY-SALT method and XORed with original iris code in BIN-SALT method. Ouda et al. [3] obtained BioCode by mapping arbitrarily generated seed with biometric features evaluated using biohashing algorithm [6]. These transformations produce lower identification performance for noisy biometric data. Hammerle-Uhl et al. [5] used mapping of permuted blocks with the source texture derived

using wavelet transform [27]. The method [5] was reported with notable performance degradation. Rathgeb et al. [29] suggested block permutation on iris textures to safeguard the iris template. However, they refined the performance by applying bloom filter to produce an alignment-free cancellable iris template. This method suffers against the claim of unlinkability.

3 Proposed Scheme

In this section, the method that has been adopted to generate secure cancellable iris templates is presented. The tasks performed are shown in Figure 1. First, IrisCodes are generated from iris images. Rotation-Invariant IrisCodes are obtained by shifting IrisCodes. These rotation-invariant IrisCodes are transformed to row vectors. In the following step, the consistent bits are identified and consistent bit vectors are constructed. Modulo operation is then applied on the consistent bit vector to reduce its size and get reduced bit vector.

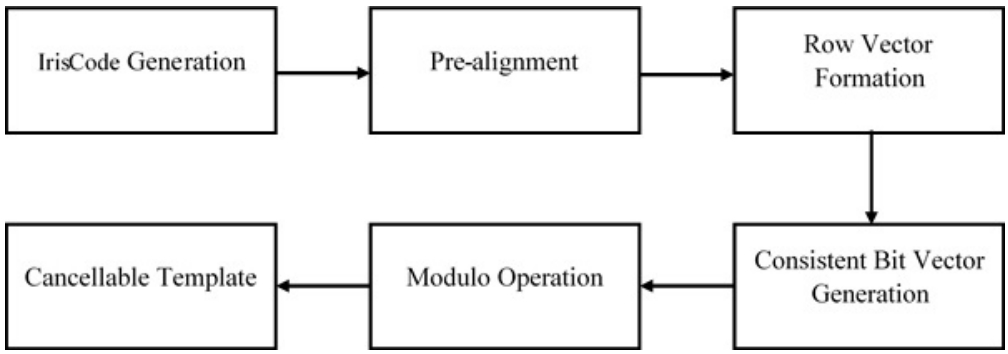

Figure 1: Block Diagram of Proposed Scheme.

3.1 IrisCode generation

The iris code generation technique used in this paper is adopted from [20].For the eye image, segmentation technique which is followed by normalization and image enhancement is done. Segmentation technique is applied to extract iris region from iris images by eliminating noise like eyelids, eyelashes. Daugman algorithm is used in our approach that detects iris and pupil circles. From each iris image, first iris boundary is detected and pupil boundary is then identified from the previously detected iris boundary instead of from the whole image because pupil is located within iris region i.e Daugman's integrodifferential operator is used to segment iris and pupil boundaries. Parabolic curve parameter is used instead of circle parameters to detect eyelids. Due to different imaging and illumination variations, the radial size of pupil can change accordingly. So, iris region is normalized using rubber sheet model of Daugman to get rid of these variations.This unwraps iris region into fixed dimension array

of size 64×256. Each one-dimensional vector is then convoluted with 1-D log Gabor to get complex iris Gabor-features of size 64×256. Each complex iris Gabor-features are then phase quantized to 2 bits to get IrisCode I $\{0,1\}$ $m1 \times m2$, where m1=64 and m2=512 which is total of 32768 bits.

3.2 Pre-alignment

Due to the head tilt of a person during acquisition, the rotational inconsistencies occur. There is possibility for poor intra class jaccard distance even for genuine subject which causes performance degradation. These are addressed by pre-alignment which is done before row vector formation by shifting each of the IrisCode by ± 16 i.e, shifting 16 columns left and right one at a time which yields 32 shifted iris instances and one original IrisCode. Jaccard distances are calculated between each of the 32 iris instances and the original iriscode of the same sample. The one with the least jaccard distance is best Iris instance which is further utilized to form row vector which is then used for consistent bit identification instead of enrolling it. In order to apply pre-alignment, we consider S samples from each subject. The value of S is determined in Section 4.1. In case of verification, the verifiable template is shifted ± 16 and minimum jaccard distance Iris instance is chosen.

3.3 Row vector formation

For ease in computation, the best IrisCode of each sample is transformed into row vector. It is easy to apply any transformation on 1-D vector instead of 2-D matrix because we need to traverse only in one direction. This row vector (R_v) of each sample is formed by merging next row to the previous one as shown in Eq.(1) :

$$R_v[k + l \times cols] = IrisCode(k, l) \tag{1}$$

For example, the IrisCode of 3×3 is transformed to 1×9 row vector as shown in the Figure 2.

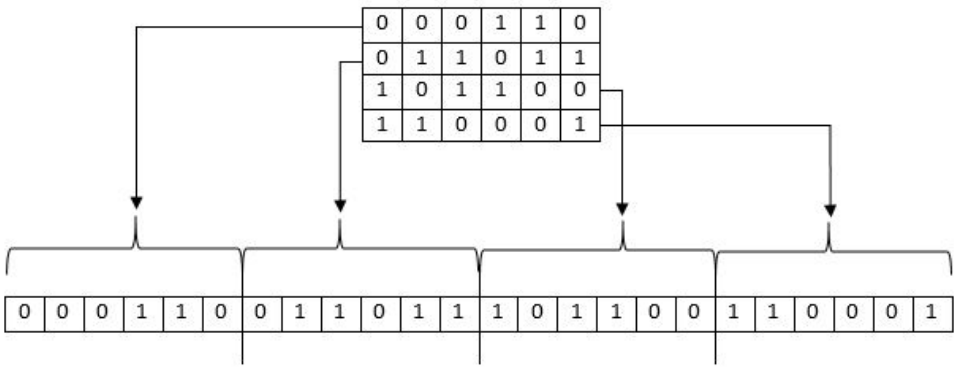

Figure 2: Example of row vector formation.

3.4 Consistent bit identification

After generating row vector for all the best IrisCodes of each sample, consistent bits are extracted to form consistent bit vector.This consistent bit vector is of same dimension as the row vector. Consistent bits are those which are less likely to change. The consistent bit vector is formed by aligning all the row vectors of 4 samples of each subject, taking the average of bits in each row index of 4 samples and comparing with threshold value. The impact of inconsistent bits on the performance is presented in Hollingsworth et al. [28]. It is explained that probability (pb) of the bit flip only affects False Reject Rate (FRR) but not False Accept Rate (FAR) performance. To improve FRR performance we tested our method with different values of pb. The bits in the best IrisCodes are secured using probability constraint.The bits with higher probability of occurrence in various samples of the same subject are collected in consistent bit vector (C_v).

In our method, the bit in the row vectors of various samples of same subject with the probability of occurrence greater than or equal to threshold value (pb_{th}) is taken into account as defined in Eq. (2):

$$C_v(j) = \begin{cases} 1, & \text{if } pb(j) < pb_{th}. \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

where pb(j) is the probability of j^{th} bit in samples of the particular subject.

The consistent bit vector formation is as shown in Figure 3:

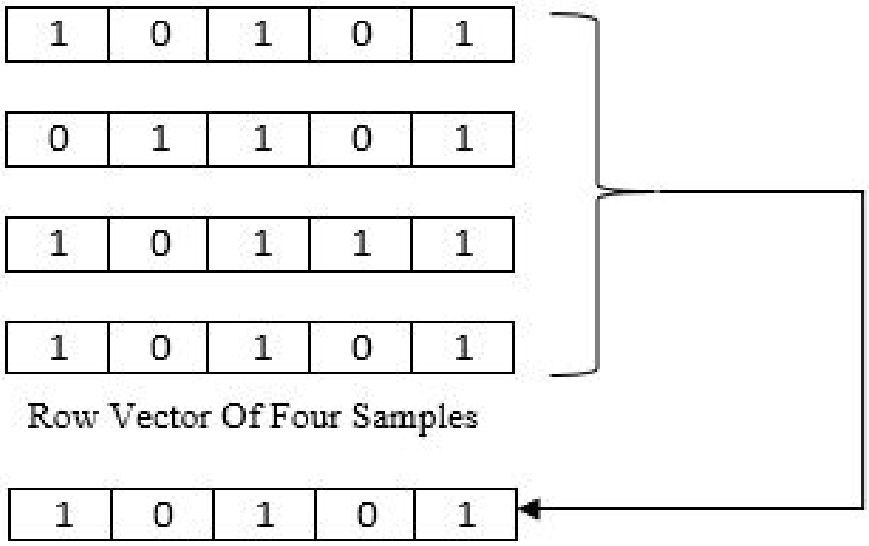

Figure 3: Example of consistent bit vector formation with pb_{th}=0.5

In our experiment, we have considered 4 samples to test the effect of pb_{th} on the value of ERR and the results obtained are reported in Table 1.From the table, it is proved that masking out inconsistent bits with pb_{th}=0.5 improves the accuracy of recognition firmly.

Table 1- EER for different values of pb_{th}

pb_{th}	ERR
0	49.44
0.25	4.34
0.5	1.62
0.75	3.12
1	23.09

3.5 Modulo Operation

In order to achieve many-to-one mapping in our approach, we applied Modulo Operation to the index j of the consistent bit vector C_v(j) i.e., jmodI, with I being a positive integer and I<L where L is length of C_v(j). Then the elements of C_v(j) are mapped to a new(Shortened) vector Sd_v(n) as in Eq.(3):

$$B_c(n) = B_c(j), \quad n = jmodI \quad where \quad j = 0, 1, ..., L-1. \tag{3}$$

The size of Sd_v(n) is 1×I.

Note: The parameter I in (3) is user and application specific, which means that for different applications it can be set to different values. By varying the value of I, different shortened vectors Sd_v(n) in (3) can be generated for the same user in different applications even though all these shortened vectors are generated from the same features.

3.6 Matching

The shortened vector (Sd_v) generated from 4 samples of each subject is the cancellable template and is stored in the database. The remaining 5th sample of each subject is used for verification. This 5th sample is converted into row vector and Modulo Operation is applied with the same value of I. This generates shortened vector (Sv_v) of same size as (Sd_v) i.e, 1×I. This (Sd_v) is used for verification. The dissimilarity between the Enrolled cancellable template (Sd_v) and Verifiable template (Sv_v) is measured using L2-norm as shown in (4)

$$||N||_p = (\sum_{i=1}^{n} |N_i|^p)^{1/p}, \quad p = 2 \tag{4}$$

This gives GAR and FAR values which are plotted to obtain ROC curve.

4 Experimental results and analysis

For the evaluation of accuracy, CASIA v3-internal [20]and CASIA-V 1.0 [19]databases are used. CASIA v3-internal dataset[20] consists of 1685 iris images from 337 users (classes).CASIA-V 1.0 dataset[19] consists of 756 iris images from 108 users. In our experiment, right eye images and left eye images are considered as different subjects for CASIA v3-internal dataset[20] because iris patterns differ for right and left eyes. The subjects which consists of at least 5 iris images are considered.The experiment is then performed on 338 subjects which consists of 165 subjects of right eye iris images and 173 subjects of left eye iris images.Out of 5 iris images considered,randomly selected 4 iris images are used to form one iris cancellable template which is enrolled and remaining 1 iris image is used for verification.

For inter-class comparison scores, each iris cancellable template is matched with every iris template of other classes. Hence CASIA v3-internal dataset results in a total of 56616 imposter scores and CASIA-V 1.0 results in a total of 5778 imposter scores. For intra-class comparison scores, each iris cancellable template is matched with remaining iris templates of the same class. Hence CASIA v3-internal results in a total of 337 genuine scores and CASIA-V 1.0 results in a total of 108 genuine scores.To evaluate the performance of recognition, Equal error rate(EER) i.e, the rate at which false rejection rate(FRR) and false acceptance rate(FAR) are equal in Receiver Operating Characteristic (ROC) curve is used. Genuine Accept Rate (GAR) is also calculated as GAR=1-FRR. ROC curve is obtained by plotting GAR against FAR. The experiment is conducted for different parameter values. The average value of the results is reported in paper.

4.1 Performance Evaluation

The proposed method uses three parameters to generate different cancellable templates. The parameters are number of samples considered for pre-alignement (S), threshold value taken in consistent bit vector identification (pb_{th}), the positive integer (I) considered in modulo operation. We highlight impact of these parameters on the performance of the proposed method. CASIA-V 1.0 [19] dataset is used to validate the parameters.

4.1.1 Effect of number of samples used in pre-alignment (S) and threshold value (pb_{th})

Before row vector formation, each IrisCode generated from the iris images are shifted circularly by ±16 bits and the best IrisCode among them is chosen by calculating jaccard distance with the original IrisCodes of the same subject to avoid rotational inconsistencies. To achieve this, we consider S number of samples from each subject of CASIA-V 1.0 [19] dataset and apply pre-alignment which is followed by consistent bit vector that considers different values of threshold (pb_{th}).Modulo Operation is then applied on consistent bit vector. To validate the parameters S and pb_{th}, we conducted number of experiments with different values of S=2,3..,6 and p=0.33,0.5...0.83 and performance is calculated with respect to EER. The results are shown in Table 1 for S=4 of CASIA-V 1.0 [19] . It has been observed that EER value decreases with the increase in S. So, we considered S=4 in our method. Taking S=4, we get pb_th=0.25,0.5,0.75,1 by experimenting with all the four pb_th values it is observed that EER value is low for pb_th=0.5.

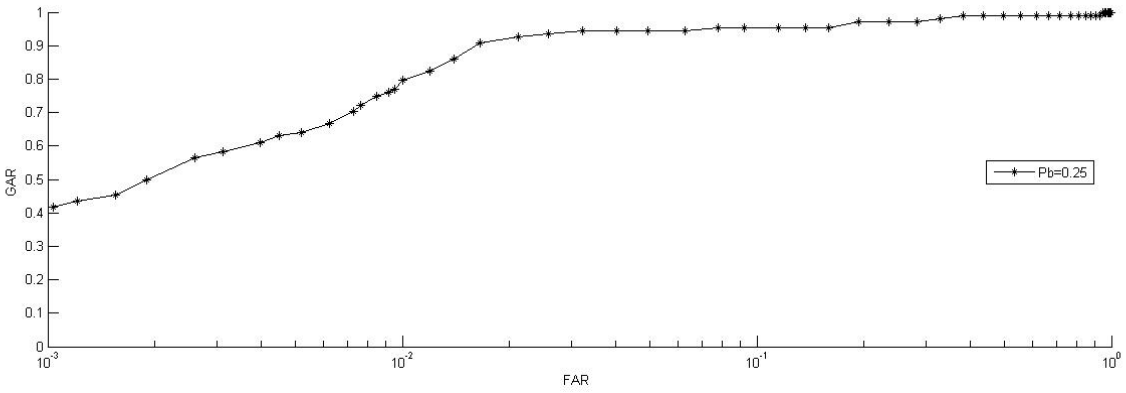

Figure 4: ROC curve for V=4, pb_{th}=0.25 of CASIA-V 1.0

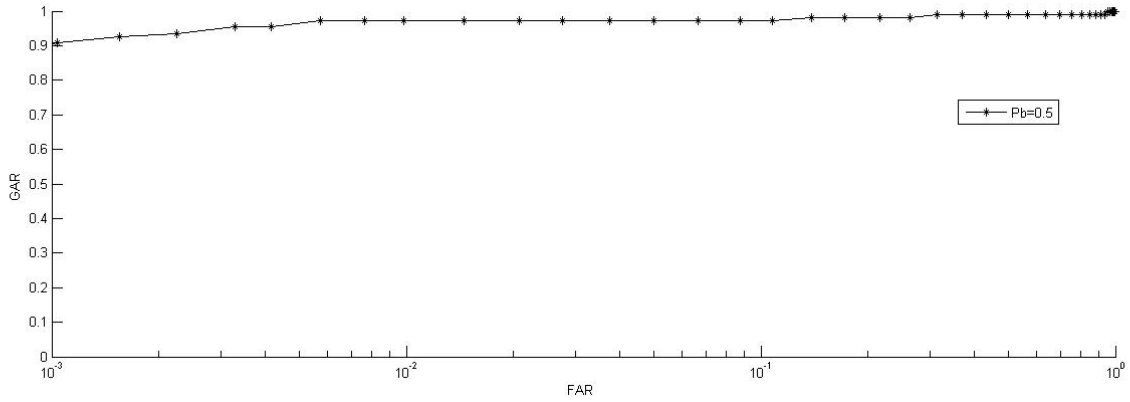

Figure 5: ROC curve for V=4, pb_{th}=0.50 of CASIA-V 1.0

4.1.2 Effect of positive integer (I) in modulo operation

After obtaining consistent bit vectors for each subject, modulo operation is applied on it. This generates a vector of reduced size. The modulo operation is applied to the index j of the consistent bit vector C_v(j) i.e., jmodI, this value of I can be randomly selected. This means that each consistent bit vector can be reduced to any random size which is less than size of C_v(j). To validate the parameter I, number of experiments with different values of I=20,000, 25,000,...32,000 are conducted and performance is calculated with respect to EER. The results are shown in Table 2. It has been observed that EER value is low for I=20,000 in our method.

Table 2- EER for different values of I

I	ERR
20000	1.62
25000	1.82
30000	2.15
32000	2.2

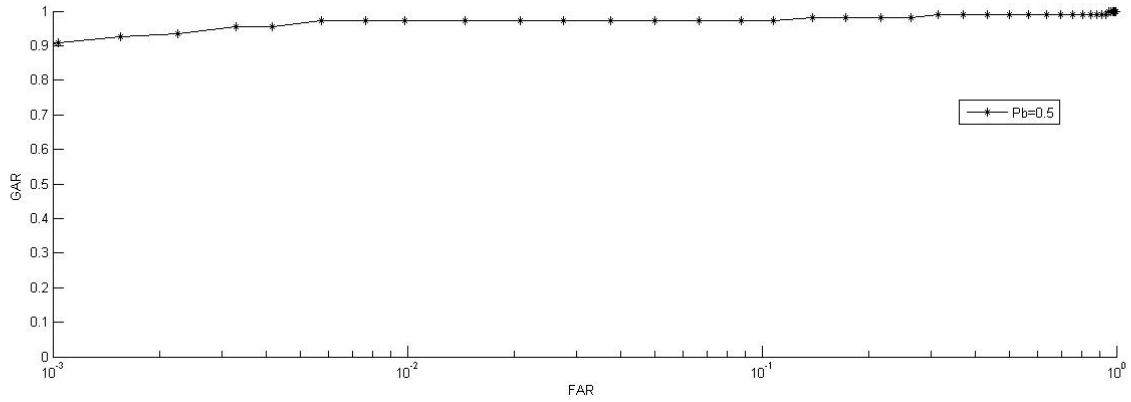

Figure 6: ROC curve for I=20000 of CASIA-V 1.0

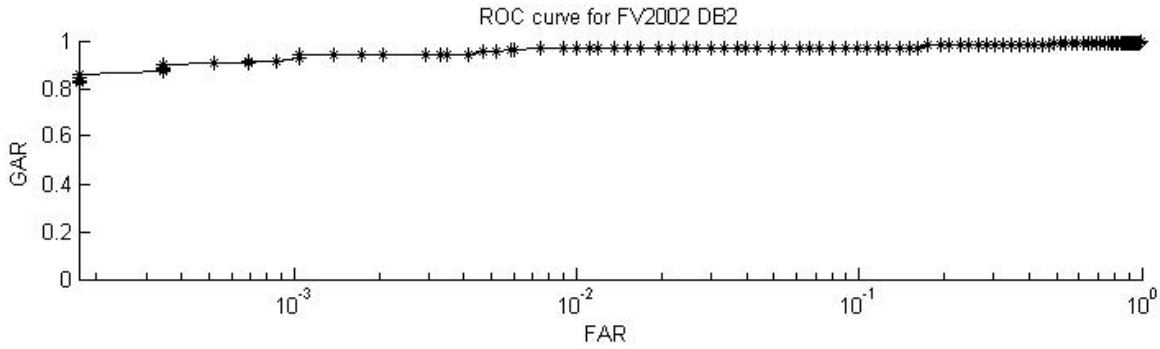

Figure 7: ROC curve for I=25000 of CASIA-V 1.0

4.2 Comparison with and without cancellable technique

In our method, first we obtained genuine and imposter scores for original (unprotected) IrisCode. Then query template is matched with stored template in the transformed domain. The EER values of original and cancellable templates are shown in Table 4 for different datasets. The results reported in the table shows that the performance is degraded by 0.32% for CASIA v3-internal and by 1.52% for CASIA-V 1.0 respectively. This shows that performance degradation is low for transformed template.ROC curves for CAsIA-V 1.0 and CASIA v3-internal is shown in Figure 8.

Dataset	EER	
	Without cancellable transformation	With cancellable transformation
CASIA-V 1.0	0.1	1.62
CASIA-V3-Internal	1.8	2.12

Table 4: Baseline Comparison

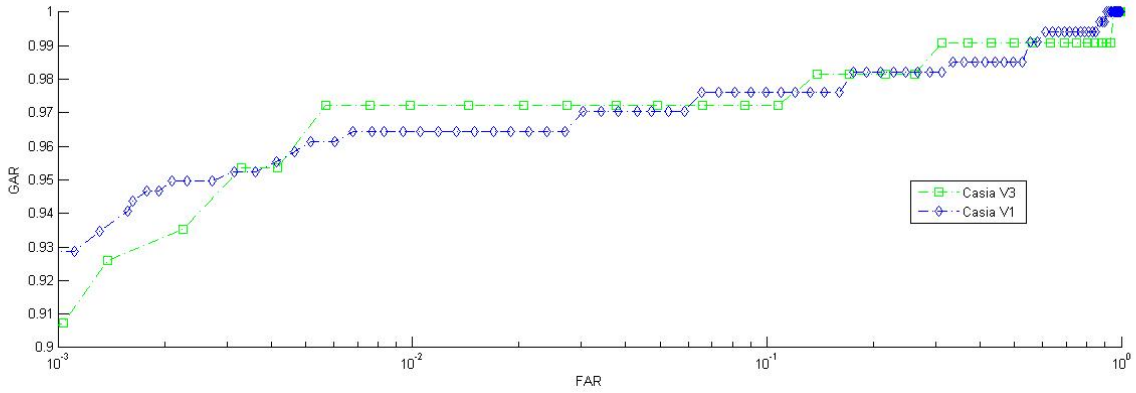

Figure 8: ROC curves for CASIA-V 1.0 and CASIA v3-internal

4.3 Comparison with existing approaches

We observed the performance of our proposed method for different parameters and found the best accuracy to be EER = 1.62 % for parameters pb_th=0.5, V=4 and I=20,000. The objective of all the methods proposed in [5,9,27,11,22,23,24] is similar to our work.

CASIA-V 1.0 [19] is used in the approaches of [22, 23] and CASIA-V3-Interval [20] is used in the approaches of [24, 5, 9, 27]. The summary of results of our proposed method and existing approaches are reported in Table 5. From Table 5, we observe that the best result obtained in existing literature is EER = 0.84 for CASIA-V3-Interval [20], whereas our method gives EER of 1.62 and 2.12 for CASIA-V1.0 [19] and CASIA-V3-Interval [20] respectively.

Methods	EER		Remarks
	CASIA-V 1.0	CASIA-V3-Interval	
Wu et al. [23]	5.55/0 FRR/FAR	–	BC (Hash encoding with error-correcting codes)
Reddy and Babu et al. [24]	–	9.8/0/FRR/FAR	Hardened fuzzy vault
Bringer et al. [22]	6.65/0/FRR/FAR	–	Fuzzy commitment scheme, EER very high
Ouda et al. [3]	–	1.3	Non-invertible transformation
Hammerle-Uhl et al. [6]	–	1.3	Block transformation
Hammerle-Uhl et al. [27]	–	0.84	EER 0.76 for partial dataset
Rathgeb et al. [29]	–	2.6	Non-invertible transformation
Proposed method	1.62	2.12	Non-invertible transformation

Table 5: Performance comparison between proposed method and existing method of cancellable iris template generation

5 Security Analysis

As discussed in Section 1, cancellable biometric system has to satisfy all the security constraints. In this section, the analysis of non-invertible, revocability and unlinkability are discussed to show that our approach satisfies schemes of template protection by preserving recognition accuracy. The analysis of various known attacks against templates is also presented.

5.1 Non-invertible analysis

Non-invertible refers to compuatational hardness in recovering original IrisCode from the transformed one. In our method, none of the parameter is stored. Hence, an attacker would need to learn the complete procedure to get chance of compromising security of the template. Acquiring the consistent bit vector of any subject is as severe as recovering original IrisCode itself because it contains information of the most significant bit. Therefore, probability constraint is applied to evaluate the consistent bit vector. Moreover, in the modulo operation many to one mapping occurs which makes attacker difficult to identify the original IrisCode. This ensures that Non-invertible property is preserved.

5.2 Revocability analysis

The cancellable technique should be designed in such a way that numerous cancellable templates are to be generated from same iris and each of them should differ from one another to prevent cross-matching across various applications. If the previously stored template is compromised, the new template generated should not correlate even if they are generated from the same biometric data. By varying the value of I in modulo operation numerous templates can be generated but we have considered random 100 templates from this combination and pseudo-imposter distribution is obtained by matching 100 templates with the original enrolled template. The pseudo-imposter distribution for various values of I is taken. It shows that variance and mean for pseudo-imposter distribution is far from the genuine distribution and near to the imposter distribution. This shows that the templates generated

from same iris pattern are uncorrelated. Hence, revocability can be preserved.

5.3 Unlinkability analysis

Numerous cancellable templates generated from same iris differ from one another to prevent cross-matching across various applications. To evaluate this, we take different values of I in modulo operation for different many to one mappings. By taking different values of I, we generate different templates for a particular subject which can be distinguished from original template which means that same user can enroll different templates for different physical applications without cross-matching. This validates property of unlinkability.

5.4 Correlation Attack

To prevent correlation attack, our proposed method uses different values of I in the modulo operation to generate different templates for various applications. Even if the attacker is able to get two templates of the same user he could not link i^{th} bit in the two templates because they are derived using different values of I. It is possible that bits in the derived template are permuted and then multiplied with some random sequence before storing it in the database. If this random sequence is dependent on I i.e, for I=20,000 random sequence consists of 20,000 bits which is computationally hard to find for an imposter.

5.5 Hill Climbing Attack

The main idea of hill climbing attack is to examine the matching score of verifiable template with the stored one and consecutively provide different verifiable templates as input to increase the matching score. This process is stopped when there is no improvement in matching score. In our method, we have considered consistent bit vector for each subject after transformation all the IrisCodes of each sample to row vector.Consistent bits are those which are less likely to change.For example, we have four IrisCodes 0010, 0101, 0100 and 0110 the consistent bit vector we get is 0100. To launch hill climbing attack, attacker has to know position of consistent bits. To obtain desired score for verification, attacker has to match all the possible bit vectors.

6 Conclusion

A method for generation of cancellable iris biometric templates has been proposed which is tested using CASIA-V1.0 and CASIA-V3 interval database. This proposed method generates transformed IrisCodes or cancellable templates by applying modulo operation on the consistent bit vector obtained for each subject. From the cancellable template that is generated it is difficult to regenerate original IrisCode. In our approach, IrisCode for each sample is generated using 1-D Log-Gabor filter. All the generated IrisCodes are prealigned by shifting the bits circularly and converted to row vectors. Then consistent bits are identified in each of the row vector and one consistent bit vector is generated for each subject. Many one mapping is achieved by applying modulo operation on these consistent bit vectors. We tested our proposed method with CASIA-V 1.0 and CASIA V3-Interval iris database and performed a detailed analysis with respect to all taken parameters. It is proved from the results, that our method is able to provide 1.6% EER value for CASIA-V 1.0 and 2.12% EER value for CASIA V3-Interval and also handle all the security and revocable issues.

References

[1] J. Daugman, How iris recognition works, IEEE Trans. Circuits Syst. Video Technol. 14 (1) (2004) 21–30.

[2] A.B.J. Teoh, A. Goh, D.C.L. Ngo, Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs, IEEE Trans. Pattern Anal. Mach. Intell. 28 (12) (2006) 1892–1901.

[3] K. Nandakumar, A.K. Jain, Biometric template protection: bridging the performance gap between theory and practice, IEEE Signal Process. Mag. 32 (5) (2015) 88–100.

[4] N. Ratha, J. H. Connell, R. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40 (3) (2001) 614–634.

[5] J. Hammerle-Uhl, E. Pschernig, A. Uhl, Cancelable iris biometrics using block re-mapping and image warping, in: P. Samarati, M. Yung, F. Martinelli, C. Ardagna (Eds.), Information Security, Vol. 5735 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 135–142.

[6] A. B. Teoh, Y. W. Kuan, S. Lee, Cancellable biometrics and annotations on biohash, Pattern Recognition 41 (6) (2008) 2034–2044.

[7] Z. Jin, B.-M. Goi, A. Teoh, Y. H. Tay, A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template, Security and Communication Networks 7 (11) (2014) 1691–1701.

[8] L. Nanni, S. Brahnam, A. Lumini, Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system, Electronics Letters 47 (15) (2011) 851–853.

[9] O. Ouda, N. Tsumura, T. Nakaguchi, Tokenless cancelable biometrics scheme for protecting iris codes, in: 20th International Conference on Pattern Recognition (ICPR), 2010, pp. 882–885.

[10] J. Pillai, V. Patel, R. Chellappa, N. Ratha, Sectored random projections for cancelable iris biometrics, in: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), 2010, pp. 1838–1841.

[11] E. Y. Du, K. Yang, Z. Zhou, Key incorporation scheme for cancelable biometrics, Journal of Information Security 2 (4) (2011) 185–194.

[12] O. Ouda, N. Tusmura, T. Nakaguchi, Securing bioencoded iriscodes against correlation attacks, in: IEEE International Conference on Communications, 2011, pp. 1–5.

[13] J. Duagman, R. Anderson, F. Hao, Combining crypto with biometrics effectively, IEEE Transaction on Computers 55 (9) (2006) 1081–1088.

[14] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, in: Advances in Cryptology - EUROCRYPT 2004, Vol. 3027 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2004, pp. 523–540.

[15] A. K. jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP J. Adv. Signal Processing (2008) 113:1–113:17.

[16] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: Proceedings of the 6th ACM Conference on Computer and Communications Security, ACM, New York, NY, USA, 1999, pp. 28–36.

[17] A. Juels, M. Sudan, A fuzzy vault scheme, in: IEEE International Symposium on Information Theory, 2002, pp. 408–.

[18] C. Rathgeb, A. Uhl, A survey on biometric cryptosystems and cancelable biometrics, EURASIP Journal on Information Security 2011 (1).

[19] Casia iris image database version 3.0. URL:http://www.cbsr.ia.ac.cn/Databases.htm

[20] Casia iris image database 1.0. URL:http://www.cbsr.ia.ac.cn/Databases.htm

[21] E.-C. Chang, S. Roy, Robust extraction of secret bits from minutiae, in: Proceedings of the 2007 International Conference on Advances in Biometrics, ICB'07, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 750–759.

[22] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, G. Zemor, Theoretical and practical boundaries of binary secure sketches, IEEE Transactions on Information Forensics and Security 3 (4) (2008) 673–683.

[23] X. Wu, N. Qi, K. Wang, D. Zhang, A novel cryptosystem based on iris key generation, in: Fourth International Conference on Natural Computation, Vol. 4, 2008, pp. 53–56.

[24] E. Reddy, I. Ramesh Babu, Performance of iris based hard fuzzy vault, in: 8th International Conference on Computer and Information Technology Workshops, 2008, pp. 248–253.

[25] A. T. B. Jin, T. Connie, Remarks on biohashing based cancelable biometrics in verification system, Neurocomputing 69 (1618) (2006) 2461–2464.

[26] J. Zuo, N. Ratha, J. Connell, Cancelable iris biometric, in: 19th International Conference on Pattern Recognition, 2008, pp. 1–4.

[27] J. Hammerle-Uhl, E. Pschernig, A. Uhl, Cancelable iris-templates using key-dependent wavelet transforms, in: International Conference on Biometrics (ICB), 2013, pp. 1–8.

[28] K. Hollingsworth, K. Bowyer, P. Flynn, The best bits in an iris code, IEEE Transactions on Pattern Analysis and Machine Intelligence 31 (6) (2009) 964–973.

[29] C.Rathgeb, C.Busch, Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters, Computers & Security 42(2014)1-12