IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 2, April, 2024, pp. 901-910
Journal homepage: http://iieta.org/journals/ts

Enhanced Security in Biometrics: A Cancelable Multi-Instance Iris Authentication Utilizing Quotient Filter

Gopi Suresh Arepalli*, Pakkiri Boobalan

Department of Information Technology, Puducherry Technological University, Puducherry 605014, India

Corresponding Author Email: gopiarepalli@ptuniv.edu.in

https://doi.org/10.18280/ts.410230

Received: 11 August 2023
Revised: 10 January 2024
Accepted: 18 February 2024
Available online: 30 April 2024

Keywords:
biometric authentication system, privacy-preserving, cancelable biometrics, quotient filter, multi-instance iris

ABSTRACT

Biometric-based authentication systems (BAS) can provide a strong security guarantee regarding the identity of users over traditional authentication systems. The iris of the eye is widely acknowledged as one of the most robust biometrics due to its exceptional performance. Despite this, templates used in traditional iris recognition systems remain unprotected, rendering them highly susceptible to various security and privacy breaches. However, several cancelable biometric schemes being introduced but at the expense of substantially decreased accuracy performance and increased computational time. To address this, we propose a cancelable multi-instance iris authentication system utilizing a quotient filter (CMAQF). The purpose of the quotient filter in CMAQF is to distort the biometric information without compromising the accuracy. Modified local random projection is applied on the fused iris template to generate the reduced template results in less authentication time. Experiments have been conducted on publicly available iris databases to assess the efficiency of CMAQF. The experimental results conclude that CMAQF achieves reasonable performance compared to existing methods, satisfying the properties of irreversibility, diversity, and revocability.

1. INTRODUCTION

Secure access to smart devices, information, and networks relies on a variety of credentials [1]. Historically, tokens or passwords have been the go-to for user authentication. However, remembering passwords can be challenging, and there are numerous methods for unauthorized access to password-protected systems. In contrast, Biometric Authentication Systems (BAS) require the physical presence of the individual, eliminating the need for cards or password memorization [2]. This minimizes the risk of identity loss, forgetfulness, forgery, or duplication [1, 3, 4]. Biometrics offer the advantage of time invariance, making them particularly attractive. Among physiological biometric traits, face, fingerprint, and iris are the most commonly used [2-4]. These modalities possess unique characteristics specific to each individual, ensuring uniqueness, non-repudiation, and permanence [3, 4]. The iris, with its stability and distinctiveness, is particularly favored for different applications in contrast to fingerprint, face, finger vein etc. [5, 6].

The biometric systems with only one biometric trait are called unimodal biometric identification systems. The challenges faced by these systems are robustness against spoofing attacks, high security, and poor recognition [2-4]. The systems with two or more modalities are termed as multimodal biometrics [2]. These systems are very trustworthy, robust, & repellent to spoofing attacks. The multi-instance biometric system uses two or more instances to authenticate the person. The proposed approach comes under multi-instance iris authentication system as it uses the right & left irises of a person for authentication. Iris is the pattern which emerges in the circular area of the eye that encircles the pupil [5]. The iris has high resistance to environmental and genetic constraints for the whole lifetime. Additionally, the recognition system has lesser mismatches because of their randomness in pattern.

A conventional biometric system has two phases: verification and enrollment/registration. In these two phases, the user acquires images. These images are pre-processed to produce a template. During registration, the template produced is known as reference template, & the one obtained at the time of verification is known as probe template [4]. During the enrollment process, the reference template is placed in a database/server. In the server, the probe template is compared against the reference template during the verification phase. Biometric modalities such as facial features, fingerprints, and iris patterns are irreplaceable since each person possesses a unique set. However, one major drawback of BAS is the inability to alter or reissue biometric templates if they are stolen, making them vulnerable to misuse [7]. Accidentally, if these templates are accessed by an unauthorized user, the data becomes unusable and irretrievable due to its distinctiveness and permanence.

Previous research by multiple authors [8-11] has demonstrated the potential reconstruction of an authentic biometric image if the corresponding raw template remains stored in the server. Once compromised, generating new

biometric data becomes impossible due to its inherent permanence, leading to significant security and privacy issues [7, 12]. Consequently, various Biometric Template Protection Schemes (BTPS) have been introduced to address these issues, including cancelable biometrics [13], homomorphic encryption (HE) [14], and bio-cryptosystems [15]. Cancelable biometrics maintain the privacy of biometric templates by utilizing transformed versions instead of the originals during authentication or enrollment phases. These transformed templates are derived through one-way transformations applied to the original template.

However, the limitations like computational complexities with HE schemes [14] and information leakage with Bio-cryptosystems make the researchers explored and identified the cancelable technique as a BTPS [16-19]. We notice a prevalent challenge in many of the current iris template protection methods, such as those referenced in the papers [20, 21] which involves a compromise between security (privacy) and accuracy. This compromise primarily stems from the requirement for strong non-invertibility, which leads to the destruction of structure in the Iris Code, causing unavoidable information loss. However, maintaining sufficient information is essential to uphold performance, as highlighted in the study [22]. Therefore, there is a need to develop a cancelable Iris Code scheme that effectively balances these two criteria. The major contributions of our work are as follows:

1.1 Contributions

1) A cancelable multi-instance iris authentication system (CMAQF) is designed to preserve the privacy of the iris templates. CMAQF uses the concept of a quotient filter to achieve confidentiality.
2) CMAQF derives the secret key directly from the iris codes themselves, distinguishing it from other cancelable approaches.
3) CMAQF yields the projection matrix used in random projection from the iris codes itself as opposed to local random projection.
4) CMAQF aids in mitigating intercept channel and template modification attacks.
5) CMAQF is evaluated on different publicly available iris databases to evaluate its effectiveness.

1.2 Quotient filter

The concept of quotient filter is initiated by the researchers [23] in 2011. This innovative data structure is designed to efficiently manage sets by implementing probabilistic operations such as addition, deletion, and membership testing [23]. In this approach, data, such as a iris, is divided into two sections as illustrated in Eq. (1) and Eq. (2):

- The least significant bits (r)

$$f_r = f \ mod \ 2^r \tag{1}$$

- The most significant bits (q)

$$f_q = \lfloor f/2^r \rfloor \tag{2}$$

The three bits constitute a bucket, all of which are zero at the start: is shifted, is the continuation, and is occupied.

2. RELATED WORKS

Khodadoust et al. [16] suggested a biometric authentication system utilizing finger-vein, fingerprint, and finger-knuckle-print. The efficiency of the system is more and it is user friendly as the system uses only finger as a biometric trait. Lee et al. [17] employs an XOR decryption, encryption & proposed a token-less cancellable biometric system. Dargan and Kumar [24] proposed a survey paper on various unimodal and multimodal biometric system. They clearly mentioned the different feature extraction techniques, classifiers considered, and datasets considered by various authors. Zhong et al. [25] proposed an approach using palm print and hand vein modalities. The authors used biometric graph matching to retrieve the features & considered Support vector machine (SVM) to determine about the genuineness of the user. Walia et al. [18] suggested a multi-modal authentication system using face, fingerprint, and iris traits. A novel feature-level fusion technique was introduced using adaptive graph in their approach which counters the presentation attack. Vijay and Indumathi [19] use the ear, finger vein, and iris traits to propose a multi-modal system. In their approach, authors use a score level fusion and for comparison, deep belief network is considered. Heidari and Chalechale [26] examined the finger knuckle print and the fingernail of three fingers. They employed the transfer learning technique using AlexNet. Cloud mechanism was utilized by Vidya and Chandra [27] for authentication. They employed the Entropy Based Local Binary Pattern method to increase accuracy by refining the feature extraction method. Talreja et al. [28] opted for iris and face as biometric traits for authentication. Initially, the features are retrieved from the iris and face utilizing deep learning, known as deep feature extraction. These features were then fused & subjected to cryptographic hash for security, forming a feature vector. Face, iris, and fingerprint were examined by Gayathri and Malathy [29] for extracting features using various approaches. For authentication, Hammad et al. [30] utilized ECG and fingerprint traits. They initially retrieved features with CNN. Peng et al. [31] suggested a biometric authentication system by incorporating finger knuckle, fingerprint, finger shape, and finger vein as biometric traits.

Format-preserving encryption is used by Bansal and Garg [32] and proposed a privacy-preserving authentication system. Authors tested their approach on both multi-modal and unimodal biometric datasets and proved that their system is efficient when contrasted against conventional techniques. Kumar and Manisha [33] introduced a method for creating a cancellable biometric template utilizing Random Walk. The resultant template is evaluated against the actual template using metrics such as root mean square error and correlation coefficient. This approach is examined on gray and color datasets available publicly to check the performance. A hybrid encryption framework depending on Rubik's cube algorithm is proposed by Helmy et al. [34]. The face biometric, iris, and fingerprint traits are considered in their approach. The findings indicate that this system effectively tackled certain security and robustness issues associated with cancelable templates. Compared to existing methods, this proposed approach is deemed reliable. Manisha and Kumar [35] developed a cancellable template utilizing the Chinese Reminder Theorem and random permutations.

Lee et al. [36] devised a cancelable iris protection, facilitating swift template comparisons and enhancing authentication efficiency. Moreover, it attains the

Unlinkability property. Siddhad and Khanna [37] introduced a cancelable template optimized for low-end devices via the Max-min threshold. This technique yields a template merely 25% of the original size, enabling expedited authentication. The authors verified the effectiveness of their approach across various scenarios including general, stolen tokens, and changeable templates. Vallabhadas and Sandhya [38] developed a privacy-preserving biometric authentication system by utilizing the concepts of Homomorphic encryption and local random projection. Their technique attains a fair performance besides preserving the privacy of the user. A deep learning based multi-modal cancelable biometric system is suggested by Abdellatef et al. [39]. Authors considered face and iris in their approach. If the old template is compromised, this system automatically generates a new cancelable biometric template. Helmy et al. [40] presented a novel hybrid encryption framework leveraging the Rubik's Cube method. They encrypted various images simultaneously with RC6 as well as AES algorithms to enhance diffusion. The output from stage 1 feeds into stage 2, where a chaotic algorithm introduces permutation. This innovative approach achieves improved robustness and efficiency.

While existing works utilizing Homomorphic Encryption (HE) schemes achieve enhanced privacy for biometric templates, they suffer from prolonged computational time. Similarly, prior efforts based on cancelable biometrics fail to ensure a balanced trade-off between security, accuracy, and speed. Therefore, the Cancelable Multi-Instance Iris Authentication System (CMAQF) is suggested to uphold the privacy of iris templates while minimizing authentication time. Unlike conventional methods, CMAQF selects the application secret key directly from the user's biometrics instead of relying on random selection. Similarly, to enhance the security of traditional random projection methods and eliminate user involvement in selecting the projection matrix, CMAQF directly selects the projection matrix from the user's biometrics.

3. CANCELABLE MULTI-INSTANCE IRIS AUTHENTICATION USING QUOTIENT FILTER (CMAQF)

Table 1. List of variables considered in CMAQF

Variable	Meaning
R	Fused Reference Template
Q	Fused Query Template
n	Number of bits in a block considered in Section 3.2
R_P	Reference transformed fused template
Q_P	Query transformed fused template
m	Number of blocks considered in Section 3.2
A_{sk}	Randomly chosen j^{th} slot from the original iris code (Application secret key).
L'_R	Reduced Reference template subsequently employing LRP
L'_Q	Reduced Query template after applying local random projection

CMAQF is the first multi-instance privacy-preserving biometric verification system using the concept of a quotient filter. The architecture of CMAQF is depicted in Figure 1. The variables used in CMAQF are mentioned in Table 1. The cloud server, & the client device are the two entities considered in CMAQF. CMAQF comprises of four modules i.e., 1) Fused template creation, 2) Local Random projection (LRP)utilizing inversive congruential generator, 3) Cancelable template generation, and 4) Distance computation between the protected templates respectively. CMAQF considers that the cloud server performs the computations genuinely. The steps of CMAQF in the enrollment phase and verification phase are described in Table 2 and Table 3.

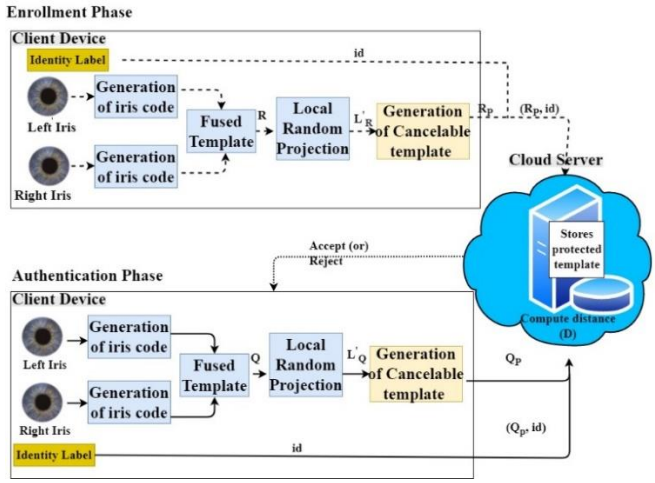


Figure 1. Block diagram of CMAQF

Table 2. Steps involved in enrollment phase

Enrollment Phase	
Client Device	**Cloud Server**
1. Obtains the reference left & right images of eye from the user. 2. Generates the iris code of size 1*10240, 1*10240 from the right & left irides utilizing the University of Salzburg tool kit (USIT) [41]. Produces the fused reference template (R) from the generated iris codes by appending one to the other. 3. Employs the LRP on R to obtain L'_R as explained insection 3.2. 4. Produces the reference transformed fused template (R_P) as illustrated in Section 3.3. 5. Sends the reference transformed fused template and user's identity label to the cloud server.	6.Stores (R_P, id).

Table 3. Steps involved in verification phase

Authentication Phase	
Client Device	**Cloud Server**
1. Obtains the probe right and left eye images of the user. 2. Generates the iris code of size 1*10240, 1*10240from the right & left iridesusing the USIT [41]. The iris codes are concatenated to obtain Q. 3. Apply the LRP on Q to obtain L'_Q as explained in section 3.2. 4. Produces the probe transformed template (Q_P) as	

explained in Section 3.3. 5. Sends the probe transformed fused template and user's identity label to the cloud server.	
	6. Obtains the probe transformed fused template for the associated *d* and calculates the distance between R_P and Q_P. 7. Compares the computed result witha threshold.

3.1 Creation of fused template

A fused template is obtained in this section from the acquired right & left eye images of the user. The iris codes of size 20X512 are formed from the obtained right and left iris individually using the USIT [41]. A 1X10240 row vector is obtained from the 20X512. Subsequently, the right iris code is concatenated to the left iris code, resulting in a fused template with dimensions of 1X20480. This fused template then serves as the input for the subsequent module to reduce the size of the fused template.

3.2 Local random projection using inversive congruential generator (L'_{rp})

The random projection (RP) is one of the prominent technique considered by many of the researchers in their works either to diminish the biometric template size or to preserve the privacy of the user. Let the projection matrix is denoted using M_r, feature vector is denoted using X. The traditional RP can be described using the Eq. (3).

$$L_{rp} = X * M_r \tag{3}$$

In the traditional RP, the user considers the projection matrix (M_r) randomly from the user. In the traditional RP, the user randomly chooses M_r. In our approach, we enhance security and streamline the process by automatically selecting the M_r from the user's biometric features, eliminating the need for user intervention. This method not only bolsters security but also reduces the size of the iris template, leading to a decrease in authentication time. The steps involved to generate L'_{rp} are mentioned below:

Step 1: The template generated in section 3.1 is splitted into *p* blocks. Each block comprises of *m* bits.

$$Y=Y_1||Y_2|| \ldots ||Y_i|| \ldots ||Y_p$$

Step 2: The j^{th} slot of Y i.e., Y_j where j Ɛ [1, p] is considered to obtain $M_r' = rand\ (X_j, j)$.

Step 3: Theinversive congruential generator (https://en.wikipedia.org/wiki/Inversive_congruential_generator) [42] is used to generate the *rand* (X_j, j).

Step 4: The M_r' is multiplied with each slot of *Y* to obtain L'_{rp} as described in Eq. (4).

$$L'_{rp} = X_j * M'_r \tag{4}$$

Table 4 outlines the Equal Error Rate (EER) obtained for different sizes of compressed templates in the untransformed system and for the original iris template of size 1X20480. We can infer from Table 4 that there is an increase in the EER of size 2240 obtained after applying L'_{rp} when compared to the original iris template. Consequently, CMAQF employs this 2240-bit template for subsequent processing steps.

Table 4. EER values of original iris template and obtained iris templates of different sizes after applying L'_{rp}

Size of R/Q	EER	Size After L'_{rp}	EER
20480	0.31	13440	0.96
		8960	0.64
		4480	0.39
		2240	**0.24**
		1120	0.45

3.3 Generation of cancelable template

The projected template obtained in Section 3.2 is of dimension 1X2240. The steps to be followed to generate the cancelable template are illustrated in Algorithm 1. Algorithm 1 takes the modified local random projection L'_{rp} and application secret key A_{sk} as input and produces the transformed or cancelable template as an output. Unlike the other works, CMAQF considers the j^{th} slot binary vector from the original iris code as an application secret key. The binary vector is represented in the decimal and considered as A_{sk}. Initially, $L'_{rp}$is represented in the binary form. It is splitted into *m* blocks consisting of *n* bits each. A matrix (*M*) of size *n X m* is generated by writing the bits of each block column-wise as shown in Figure 2. Let *Z* be the decimal representation of the primary diagonal of *M*using the Eq. (5).

$$Z= (diag\ (M))_{10} \tag{5}$$

Now, compute the number of ones, and the sum of indices of one's in every column *i* of *M* and store in N_i, S_i using Eq. (6).

$$\begin{aligned} &N_x\text{=Number of set bits (1's) in } x^{th} \text{ column of } M. \\ &S_x\text{=Sum of indexes of set bits (1's) in } x^{th} \text{ column of } M. \end{aligned} \tag{6}$$

where, *x* varies from 1 to *m*.

The vector *T* is obtained by adding N_i with Z, and S_i with A_{sk} using Eq. (7).

$$\begin{aligned} T_i&=N_i+Z \\ T_{i+1}&=S_i+A_{sk} \\ i &\text{ Ɛ } [1, m] \end{aligned} \tag{7}$$

A few bits of *T* are extracted to get the final transformed template *Y*.

Algorithm 1 Generation of Cancelable Template

Input : Template obtained after L'_{rp} (X_{10}), Application Secret Key (A_{sk})

Output : Transformed fused template (Y_{10})

1. Represent X in binary form (each number is represented with the maximum number of bits in L'_{rp}).
2. Divide X into *j* blocks, each of size *k*.
3. A matrix M of size k X j is generated by writing the bits of each block in column wise as shown in Figure 2.
4. Compute Z= $(diag\ (M))_{10}$.

5. for $x \leftarrow 1$ to m
6. N_x= Number of set bits in x[th] column of M.
7. S_x= Sum of indexes of set bits in x[th] column of M.
8. $x \leftarrow x+1$
9. end for
10. $t \leftarrow 1$
11. for j←1:2:2m do
12. $T_j = N_t+Z$.
13. $T_{j+1} = S_t+A_{sk}$.
14. $t \leftarrow t+1$
15. end for
16. Y=Extract few bits from T.

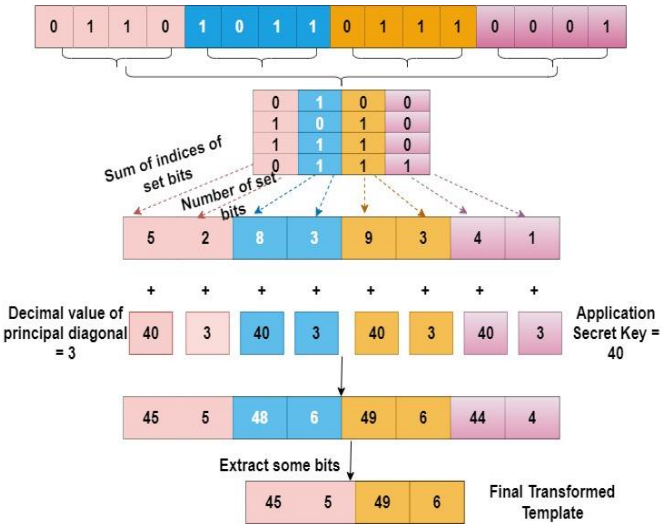


Figure 2. An example of cancelable template generation in CMAQF

Example: The process to generate the cancelable template with an example is shown in Figure 2. We considered a 16-bit binary template to explain the process with an example. This template is obtained by representing the L'_{rp} (decimal vector) in binary form. The 16-bit template is split into 4 blocks each of 4 bits. A 4X4 binary matrix is formed from the 1X16-bit template as shown in Figure 2. The primary diagonal bits are considered and computed Z=3. The number of set bits and the sum of indices of set bits for each column are computed (N_1=2, N_2=3, N_3=3, N_4=1; S_1=5, S_2=8, S_3=9, S_4=1). A vector T is formed with S_i and N_i. In the example, we considered an application secret key A_{sk}=40 (Chosen from the user's iris data). A_{sk} and Z are added to the S_i and N_i to get T= (45, 5, 48, 6, 49, 6, 44, 4). Few bits are extracted from T to obtain the final transformed template Y= (45, 5, 49, 6).

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Details of databases and experimental setup

CMAQF is tested on IITD [43] (DB2), CASIA-V3-Interval (http://www.cbsr.ia.ac.cn/IrisDatabase.htm) (DB1), and SDUMLA-HMT [44] (DB3) databases to inspect its efficiency. Table 5 depicts the summary of the total number of subjects and samples. As CMAQF requires both the irises of a user to authenticate him/her. So, we considered only 208, 115, and 106 subjects from DB2, DB1, DB3 databases which have minimum 5 samples of left and right irises. Hence, we utilize these subjects for our experiments while excluding others from consideration. Out of 5 samples, one sample is used during the enrollment phase and another sample is used during the authentication phase.

The experiments of CMAQF are implemented on a Windows 10 operating system with Intel Core i5 7[th] Gen processor and 16GB Random Access Memory.

Table 5. Summary of databases considered in CMAQF

Database	Number of Subjects	Number of Samples	Number of Subjects Considered
DB1	249	2639	115
DB2	225	2250	208
DB3	106	1060	106

4.2 Performance analysis

Table 6 presents a comparison of the Equal Error Rate (EER) calculated between transformed and untransformed templates of different sizes. Based on the data in Table 6, three key observations can be made:

1) The performance of right or left iris alone is less when compared to the performance of the fused template.

2) There is a slight increase in the EER of a fused compressed template in the transformed system when compared to the EER of a fused compressed template in an untransformed system.

3) There is a minimal reduction in the performance of the fused compressed template in the transformed system when compared to the fused template in the transformed system. But, it can be inferred from Table 7 that there is an increase in the performance in terms of computational time.

The comparison of EER between Compressed Untransformed Fused (CUF), Compressed Transformed Fused (CTF), Uncompressed Untransformed Fused (UUF), & Uncompressed Transformed Fused (UTF) templates are mentioned in Table 7. UUF template indicates the templates without transformation and before applying L'_{rp}. CUF template indicates the template without transformation & after applying L'_{rp}, UTF template represents the template with transformation and before applying L'_{rp}, and CTF template represents the templates with transformation & after applying L'_{rp}. We can observe from Table 7 that there is a degradation in the performance in terms of EER between the UUF and CTF templates in CMAQF.

Table 6. EER obtained in untransformed and transformed templates of CMAQF. FCLRP-Fused Template after applying L'_{rp}, ALI-Alone Left Iris, CT-Fused Template, ARI-Alone Right Iris

Database	Untransformed System				Transformed System	
	ALI	ARI	CT	FCLRP	CT	FCLRP
DB1	3.26	4.41	0.31	0.24	0.25	0.15
DB2	4.41	4.15	0.86	0.78	0.81	0.43
DB3	2.10	1.28	0.13	0.05	0.11	0.04

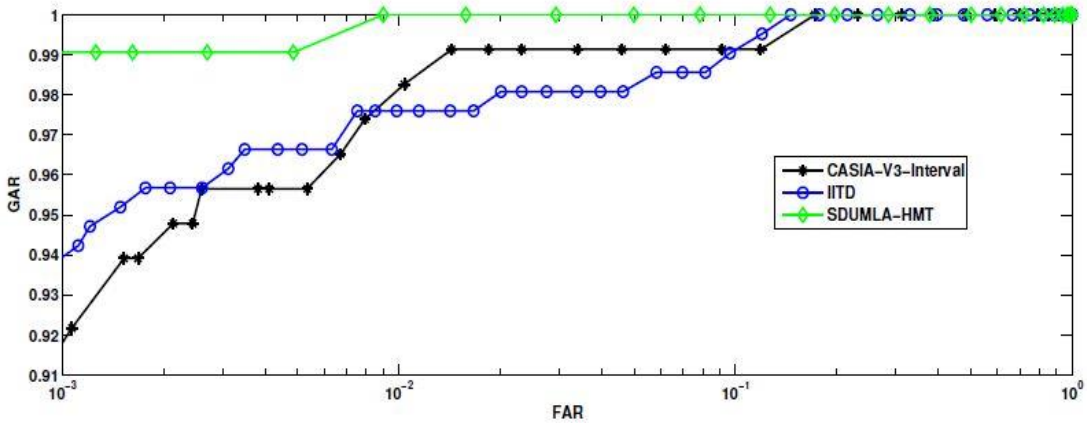
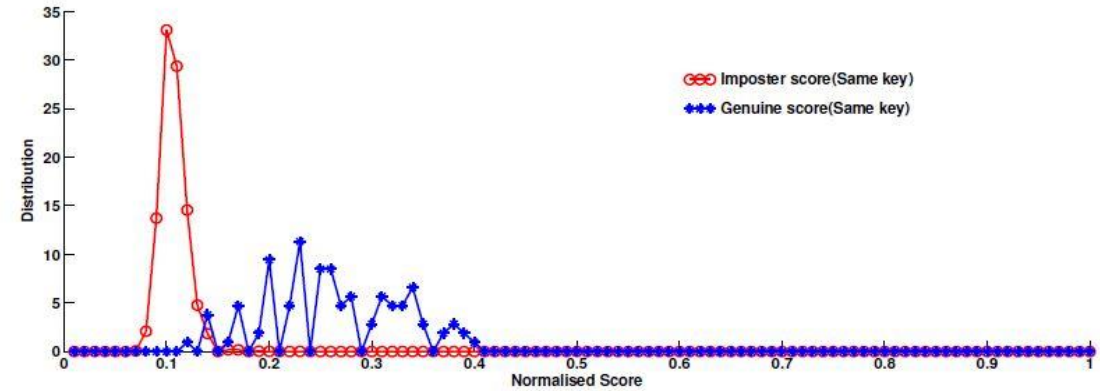
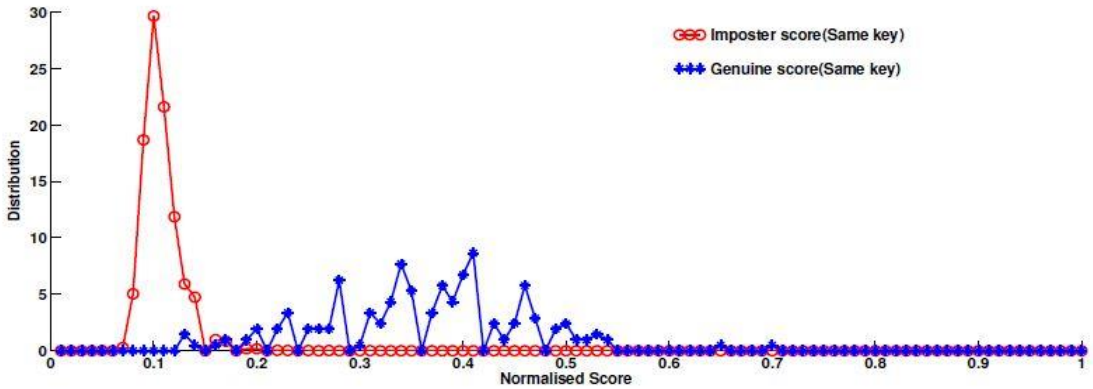


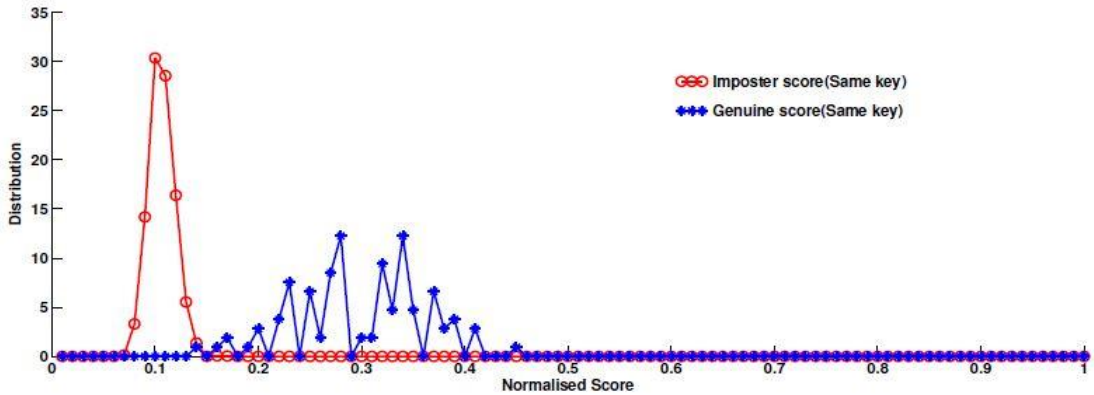
Figure 3. ROC curve of CMAQF for DB1, DB2, DB3



(a)



(b)



(c)

Figure 4. Genuine & Impostor distributions of CMAQF for (a) DB1, (b) DB2 (c) DB3 databases

Table 7. Baseline comparison. ALI-Alone Left Iris, ARI-Alone Right Iris

Database	Template Type	Template Size	Time (in Secs)	EER (in %)
DB1	ALI	10240	0.096	3.26
	ARI	10240	0.096	4.41
	UUF template	20480	0.186	0.31
	CUF template	2240	0.098	0.24
	UTF template	20480	0.871	0.25
	CTF template	2240	0.102	0.15
DB2	ALI	10240	0.523	4.41
	ARI	10240	0.523	4.15
	UUF template	20480	0.613	0.86
	CUF template	2240	0.528	0.78
	UTF template	20480	1.723	0.81
	CTF template	2240	0.595	0.43
DB3	ALI	10240	0.0856	2.10
	ARI	10240	0.0856	1.28
	UUF template	20480	0.0972	0.13
	CUF template	2240	0.0945	0.05
	UTF template	20480	0.6945	0.11
	CTF template	2240	0.0963	0.04

Table 8. Results of GAR and FAR at different values of threshold for DB2 database

Threshold	FAR	FRR	GAR (in %)
0	0	1	0
0.1	0	0.95	0.05
0.15	0.01	0.91	0.09
0.2	0.08	0.86	0.14
0.3	0.232	0.83	0.17
0.4	0.34	0.78	0.22
0.5	0.37	0.61	0.39
0.6	0.41	0.54	0.46
0.65	0.55	0.42	0.58
0.70	0.58	0.38	0.62
0.80	0.61	0.25	0.75
0.82	0.651	0.209	0.791
0.84	0.79	0.15	0.85
0.86	0.91	0.083	0.917
0.90	1	0.033	0.67
0.95	1	0.0087	0.9913
1	1	0.0053	0.947

At the same time, a fair performance in terms of authentication time is achieved for CTF templates. The Receiver Operating Characteristic (ROC) curve of the CMAQF scheme for DB1, DB2, DB3 databases is depicted in Figure 3. The genuine and imposter distribution for DB1, DB2, DB3 databases are shown in Figure 4. We can observe from Figure 4, that the two scores are well separated. The values of GAR (Genuine Accept Rate: 1-FRR), FAR (False Accept Rate), FRR (False Reject Rate) at different threshold values for IITD database is depicted in Table 8. It can be inferred from Table 6 that FAR increases and FRR decreases which indicates the efficiency of the CMAQF. The EER $(\frac{FAR+FRR}{2})$=0.43 value is obtained at threshold value = 0.82.

4.3 Security analysis of CMAQF

The requirements of biometric template protection schemes must be contented to guarantee the privacy of the fused iris templates.

Irreversibility Analysis: The raw template cannot be obtained from the transformed template. In CMAQF, the irreversibility is achieved in two phases, 1) During the Local Random Projection using inversive congruential generator 2) Generation of cancelable template. The fused reference transformed template is stored in the cloud server during the enrollment phase. Similarly, the fused probe transformed template is sent to the cloud server during the authentication phase. The cloud server calculates the hamming distance on the transformed templates itself. It is observed that from section 3.3, given a transformed template *Y*, it is difficult for an intruder to guess A_{sk} as well as *Z*. Also, it is not clear how many values are extracted and from which positions the values are considered. As a result, it is infeasible for an intruder to acquire the raw iris codes. Hence, the irreversibility property is satisfied in CMAQF.

Revocability Analysis: The proposed cancelable method must be able to produce a different template if the old template gets compromised. Rather than acquiring the new templates from the users, CMAQF generates the new template by changing two parameters: 1) Considered slot during the generation of random projection matrix. The change in considering the slot of bits results in different application specific key as well. 2) Extraction of bits in the last step of Algorithm 1. As a result, CMAQF achieves the revocability.

Unlinkability Analysis: The transformed templates generated in different applications must not have any correlation. The parameters like A_{sk} and the permutation of extraction of few bits in the last step generates different uncorrelated transformed templates.

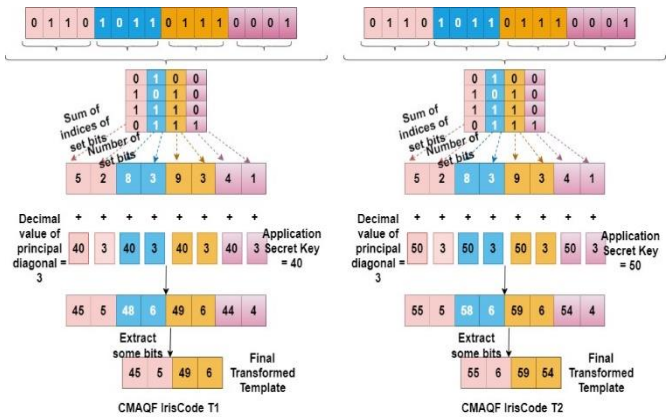


Figure 5. An example of CMAQF illustrating prevention of cross-matching attack

Cross-matching Attack: Figure 5 illustrates how the CMAQF overcome the cross-matching attack among various organizations. Our proposed technique has the ability to produce diverse transformed templates from a user's original template. This capability serves as a deterrent against cross-matching assaults. As shown in Figure 5, if a template is compromised then the new template (which is different from

the original one) can be generated by changing the application specific key (chosen from the user's iris data). Additionally, in Figure 5, we considered the same template (binary form) in both the cases. But if the M_r' is changed (in Section 3.2), there will be a change in the template as well leads to a different transformed template.

Stolen-token Attack: To mitigate stolen template or stolen token attacks in biometric systems, pseudo impostor scores can serve as an effective countermeasure. In a stolen token attack, where an intruder achieves unauthorized access to template or token for fraudulent authentication, pseudo impostor scores offer a solution. These scores are synthetic or artificial representations generated specifically for comparison purposes during authentication, without revealing the original biometric data. To demonstrate how CMAQF addresses the stolen-token attack, we utilized 100 subjects from the DB2 database. The first left and right iris sample in DB2 database is considered and generated 10 different transformed templates with the help of different keys. This resulted in the generation of 100*(1*100) =10000 pseudo-impostor scores. Figure 6 illustrates the distributions of Impostor, Genuine, and Pseudo-impostor scores for the DB2 database. Figure 6 highlights that the pseudo-impostor and impostor scores exhibit close proximity, while the pseudo-impostor and genuine scores demonstrate differentiation. This observation indicates that the newly generated transformed templates, each associated with 100 different application-specific keys, exhibit distinctiveness despite originating from the same iris.

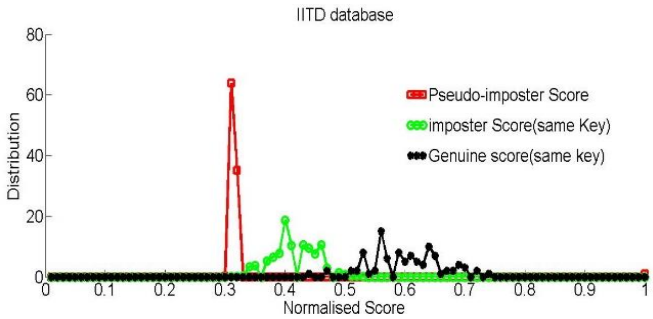


Figure 6. Impostor, Genuine, and Pseudo-impostor Score distributions for DB2 database

4.4 Comparison of equal error rate

Table 9. EER analysis of CMAQF with state-of-the-art works

Database	Method	EER (in %)
IITD	Punithavathi et al. [45]	3.3
	Morampudi et al. [46]	0.88
	Gomez-Barrero et al. [47]	0.7
	Mahesh Kumar et al. [48]	0.88
	Sadhya and Raman [49]	1.4
	Morampudi et al. [50]	0.86
	CMAQF	0.43
CASIA-V3-Interval	Sadhya and Raman [49]	0.105
	Punithavathi et al. [45]	1.9
	Morampudi et al. [46]	0.39
	Lai et al. [51]	0.54
	Mahesh Kumar et al. [48]	0.13
	Dwivedi et al. [52]	0.43
	Morampudi et al. [50]	0.31
	CMAQF	0.15
	Kamalskar et al. [53]	2.5947
SDUMLA-HMT	Gad et al. [54]	0.3
	Mahesh Kumar et al. [48]	0.0002
	Morampudi et al. [46]	0.28
	Morampudi et al. [50]	0.13
	CMAQF	0.04

Table 7 illustrates the baseline comparison (alone left iris, alone right iris and combination of both) of CMAQF. The fair performance is achieved in CMAQF for DB1, DB2 and DB3 databases. Table 9 presents a comparison of CMAQF's EER with other methods. Notably, CMAQF showcases competitive performance in terms of EER when compared to select approaches listed in Table 9. While certain works Mahesh Kumar et al. [48] exhibit improved EER, they require more time for authentication. Additionally, the separability measures such as Kolmogorov-Smirnov (KS), and d-prime test are also evaluated for CMAQF. The d-prime value of CMAQF for DB1, DB3 and DB2 databases are 3.767, 4.9287, and 3.4953. The KStest value of CMAQF for DB1, DB3 and DB2 databases are 0.9797, 0.9934, and 0.9695.

5. CONCLUSION

The limitations inherent in traditional authentication systems can be effectively addressed through the implementation of a biometric authentication system (BAS). Maintaining privacy is a critical consideration in BAS due to its irreversible nature. To address this concern, this article introduces a cancelable multi-instance iris authentication system (CMAQF), aimed at safeguarding the privacy of biometric templates. In CMAQF, the confidentiality of iris templates is ensured through the use of a quotient filter. Furthermore, a modified local random projection technique is employed on the fused iris template to generate reduced templates, resulting in quicker authentication times. The efficacy of CMAQF is evaluated through experimentation with various databases. The experimental findings demonstrate that CMAQF surpasses existing methods in terms of both efficiency and accuracy.

CMAQF assumes the server performs the computations genuinely. The compromising of the server leads to false accept or false reject. So, a system has to be developed in the future that works fine even in the malicious server setting.

REFERENCES

[1] O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12): 2021-2040. https://doi.org/10.1109/JPROC.2003.819611

[2] Jain, A.K., Bolle, R., Pankanti, S. (Eds.). (2006). Biometrics: Personal identification in networked society. Springer Science & Business Media, Vol. 479.

[3] Jain, A.K., Ross, A., Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1): 4-20. https://doi.org/10.1109/TCSVT.2003.818349

[4] Jain, A., Bolle, R., Pankanti, S. (1996). Introduction to biometrics. Springer US, pp. 1-41. https://doi.org/10.1007/0-306-47044-6_1

[5] Daugman, J. (2009). How iris recognition works. The essential guide to image processing. The Essential Guide to Image Processing, USA: Elsevier. Academic Press,

715-739.
[6] Delac, K., Grgic, M. (2004). A survey of biometric recognition methods. In Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine, Zadar, Croatia. IEEE, pp. 184-193.
[7] Prabhakar, S., Pankanti, S., Jain, A.K. (2003). Biometric recognition: Security and privacy concerns. IEEE Security & Privacy, 1(2): 33-42. https://doi.org/10.1109/MSECP.2003.1193209
[8] Mai, G., Cao, K., Yuen, P.C., Jain, A.K. (2018). On the reconstruction of face images from deep face templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 41(5): 1188-1202. https://doi.org/10.1109/TPAMI.2018.2827389
[9] Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., Ortega-Garcia, J. (2013). Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. Computer Vision and Image Understanding, 117(10): 1512-1525. https://doi.org/10.1016/j.cviu.2013.06.003
[10] Cappelli, R., Maio, D., Lumini, A., Maltoni, D. (2007). Fingerprint image reconstruction from standard templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(9): 1489-1503. https://doi.org/10.1109/TPAMI.2007.1087
[11] Venugopalan, S., Savvides, M. (2011). How to generate spoofed irises from an iris code template. IEEE Transactions on Information Forensics and Security, 6(2): 385-395. https://doi.org/10.1109/TIFS.2011.2108288
[12] Ratha, N.K., Connell, J.H., Bolle, R.M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3): 614-634. https://doi.org/10.1147/sj.403.0614
[13] Patel, V.M., Ratha, N.K., Chellappa, R. (2015). Cancelable biometrics: A review. IEEE Signal Processing Magazine, 32(5): 54-65. https://doi.org/10.1109/MSP.2015.2434151
[14] Acar, A., Aksu, H., Uluagac, A.S., Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (Csur), 51(4): 1-35. https://doi.org/10.1145/3214303
[15] Rathgeb, C., Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1): 1-25. https://doi.org/10.1186/1687-417X-2011-3
[16] Khodadoust, J., Medina-Pérez, M.A., Monroy, R., Khodadoust, A.M., Mirkamali, S.S. (2021). A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print. Expert Systems with Applications, 176: 114687, https://doi.org/10.1016/j.eswa.2021.114687
[17] Lee, M.J., Teoh, A.B.J., Uhl, A., Liang, S.N., Jin, Z. (2021). A tokenless cancellable scheme for multimodal biometric systems. Computers & Security, 108: 102350. https://doi.org/10.1016/j.cose.2021.102350
[18] Walia, G.S., Jain, G., Bansal, N., Singh, K. (2019). Adaptive weighted graph approach to generate multimodal cancelable biometric templates. IEEE Transactions on Information Forensics and Security, 15: 1945-1958. https://doi.org/10.1109/TIFS.2019.2954779
[19] Vijay, M., Indumathi, G. (2021). Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications. Journal of Information Security and Applications, 58: 102707. https://doi.org/10.1016/j.jisa.2020.102707
[20] Hämmerle-Uhl, J., Pschernig, E., Uhl, A. (2009). Cancelable iris biometrics using block re-mapping and image warping. In International Conference on Information Security, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 135-142. https://doi.org/10.1007/978-3-642-04474-8_11
[21] Rathgeb, C., Breitinger, F., Busch, C. (2013). Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In 2013 International Conference on Biometrics (ICB), Madrid, Spain, pp. 1-8. https://doi.org/10.1109/ICB.2013.6612976
[22] Nagar, A., Nandakumar, K., Jain, A.K. (2010). Biometric template transformation: A security analysis. In Media Forensics and Security II. SPIE, 7541: 237-251. https://doi.org/10.1117/12.839976
[23] Quotient filter: https://www.gakhov.com/articles/quotient-filters.html, accessed on 10 January 2024.
[24] Dargan, S., Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143: 113114. https://doi.org/10.1016/j.eswa.2019.113114
[25] Zhong, D., Shao, H., Du, X. (2019). A hand-based multi-biometrics via deep hashing network and biometric graph matching. IEEE Transactions on Information Forensics and Security, 14(12): 3140-3150. https://doi.org/10.1109/TIFS.2019.2912552
[26] Heidari, H., Chalechale, A. (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. Expert Systems with Applications, 191: 116278. https://doi.org/10.1016/j.eswa.2021.116278
[27] Vidya, B.S., Chandra, E. (2019). Entropy based Local Binary Pattern (ELBP) feature extraction technique of multimodal biometrics as defence mechanism for cloud storage. Alexandria Engineering Journal, 58(1): 103-114. https://doi.org/10.1016/j.aej.2018.12.008
[28] Talreja, V., Valenti, M.C., Nasrabadi, N.M. (2020). Deep hashing for secure multimodal biometrics. IEEE Transactions on Information Forensics and Security, 16: 1306-1321. https://doi.org/10.1109/TIFS.2020.3033189
[29] Gayathri, M., Malathy, C. (2021). Novel framework for multimodal biometric image authentication using visual share neural network. Pattern Recognition Letters, 152: 1-9. https://doi.org/10.1016/j.patrec.2021.09.016
[30] Hammad, M., Liu, Y., Wang, K. (2018). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. IEEE Access, 7: 26527-26542. https://doi.org/10.1109/ACCESS.2018.2886573
[31] Peng, J., Abd El-Latif, A.A., Li, Q., Niu, X. (2014). Multimodal biometric authentication based on score level fusion of finger biometrics. Optik, 125(23): 6891-6897. https://doi.org/10.1016/j.ijleo.2014.07.027
[32] Bansal, V., Garg, S. (2022). A cancelable biometric identification scheme based on bloom filter and format-preserving encryption. Journal of King Saud University-Computer and Information Sciences, 34(8): 5810-5821. https://doi.org/10.1016/j.jksuci.2022.01.014
[33] Kumar, N., Manisha. (2022). CBRW: A novel approach for cancelable biometric template generation based on 1-D random walk. Applied Intelligence, 52(13): 15417-

15435. https://doi.org/10.1007/s10489-022-03215-x
[34] Helmy, M., El-Rabaie, E.S.M., El-Dokany, I., Abd El-Samie, F.E. (2023). A novel cancellable biometric recognition system based on Rubik's cube technique for cyber-security applications. Optik, 285: 170475. https://doi.org/10.1016/j.ijleo.2022.170475
[35] Manisha, Kumar, N. (2022). CBRC: A novel approach for cancelable biometric template generation using random permutation and Chinese Remainder Theorem. Multimedia Tools and Applications, 81(16): 22027-22064. https://doi.org/10.1007/s11042-021-11284-2
[36] Lee, M.J., Jin, Z., Liang, S.N., Tistarelli, M. (2022). Alignment-robust cancelable biometric scheme for iris verification. IEEE Transactions on Information Forensics and Security, 17: 3449-3464. https://doi.org/10.1109/TIFS.2022.3208812
[37] Siddhad, G., Khanna, P. (2022). Max-min threshold-based cancelable biometric templates for low-end devices. Journal of Electronic Imaging, 31(3): 033025. https://doi.org/10.1117/1.JEI.31.3.033025
[38] Vallabhadas, D.K., Sandhya, M. (2022). Securing multimodal biometric template using local random projection and homomorphic encryption. Journal of Information Security and Applications, 70: 103339. https://doi.org/10.1016/j.jisa.2022.103339
[39] Abdellatef, E., Soliman, R.F., Omran, E.M., Ismail, N.A., Elrahman, S.E.A., Ismail, K.N., Rihan, M., Amin, M., Eisa, A.A., El-Samie, F.E.A. (2022). Cancelable face and iris recognition system based on deep learning. Optical and Quantum Electronics, 54(11): 702. https://doi.org/10.1007/s11082-022-03770-0
[40] Helmy, M., El-Shafai, W., El-Rabaie, E.S.M., El-Dokany, I.M., Abd El-Samie, F.E. (2022). A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications. Optik, 258: 168773. https://doi.org/10.1016/j.ijleo.2022.168773
[41] Rathgeb, C., Uhl, A., Wild, P., Hofbauer, H. (2016). Design decisions for an iris recognition sdk. Handbook of Iris Recognition, 359-396. https://doi.org/10.1007/978-1-4471-6784-6_16
[42] Eichenauer-Herrmann, J. (1992). Inversive congruential pseudorandom numbers: A tutorial. International Statistical Review/Revue Internationale de Statistique, 167-176. https://doi.org/10.2307/1403647
[43] Kumar, A., Passi, A. (2010). Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognition, 43(3): 1016-1026. https://doi.org/10.1016/j.patcog.2009.08.016
[44] Yin, Y., Liu, L., Sun, X. (2011). SDUMLA-HMT: A multimodal biometric database. In Biometric Recognition: 6th Chinese Conference, CCBR 2011, Beijing, China, December 3-4, 2011. Springer Berlin Heidelberg. Proceedings, 6: 260-268. https://doi.org/10.1007/978-3-642-25449-9_33
[45] Punithavathi, P., Geetha, S., Sasikala, S. (2017). Generation of cancelable iris template using bi-level transformation. In Proceedings of the 6th International Conference on Bioinformatics and Biomedical Science, pp. 94-100. https://doi.org/10.1145/3121138.3121185
[46] Morampudi, M.K., Prasad, M.V., Raju, U.S.N. (2020). Privacy-preserving iris authentication using fully homomorphic encryption. Multimedia Tools and Applications, 79: 19215-19237. https://doi.org/10.1007/s11042-020-08680-5
[47] Gomez-Barrero, M., Rathgeb, C., Li, G., Ramachandra, R., Galbally, J., Busch, C. (2018). Multi-biometric template protection based on bloom filters. Information Fusion, 42: 37-50. https://doi.org/10.1016/j.inffus.2017.10.003
[48] Mahesh Kumar, M., Prasad, M.V., Raju, U.S.N. (2020). BMIAE: Blockchain-based multi-instance iris authentication using additive ElGamal homomorphic encryption. IET Biometrics, 9(4): 165-177. https://doi.org/10.1049/iet-bmt.2019.0169
[49] Sadhya, D., Raman, B. (2019). Generation of cancelable iris templates via randomized bit sampling. IEEE Transactions on Information Forensics and Security, 14(11): 2972-2986. https://doi.org/10.1109/TIFS.2019.2907014
[50] Morampudi, M.K., Prasad, M.V., Raju, U.S.N. (2021). Privacy-preserving and verifiable multi-instance iris remote authentication using public auditor. Applied Intelligence, 51(10): 6823-6836. https://doi.org/10.1007/s10489-021-02187-8
[51] Lai, Y.L., Jin, Z., Teoh, A.B.J., Goi, B.M., Yap, W.S., Chai, T.Y., Rathgeb, C. (2017). Cancellable iris template generation based on indexing-first-one hashing. Pattern Recognition, 64: 105-117. https://doi.org/10.1016/j.patcog.2016.10.035
[52] Dwivedi, R., Dey, S., Singh, R., Prasad, A. (2017). A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping. Computers & Security, 65: 373-386. https://doi.org/10.1016/j.cose.2016.10.004
[53] Kamlaskar, C., Deshmukh, S., Gosavi, S., Abhyankar, A. (2019). Novel canonical correlation analysis based feature level fusion algorithm for multimodal recognition in biometric sensor systems. Sensor Letters, 17(1): 75-86. https://doi.org/10.1166/sl.2019.4013
[54] Gad, R., Talha, M., Abd El-Latif, A.A., Zorkany, M., Ayman, E.S., Nawal, E.F., Muhammad, G. (2018). Iris recognition using multi-algorithmic approaches for cognitive internet of things (CIoT) framework. Future Generation Computer Systems, 89: 178-191. https://doi.org/10.1016/j.future.2018.06.020