Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Cancelable Biometric Iris Authentication System Based On Random Projection Matrix And Double Random Phase Encoding For Cloud Services

Narender. M[1], Dr. S. Thaiyalnayaki[2]

[1] Research Scholar, Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India.
[2] Associate Professor, CSE, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India.

In conventional authentication techniques, biometric identification has overshadowed major security issues. Biometric recognition is continually growing with the advent of higher accuracy and lower computing devices, increasing the need for authentication. Cancelable biometric template generation is a pivotal approach for enhancing security and privacy in biometric systems. This paper presents a novel method that combines Random Projection (RP) matrix and Improved Double Random Phase Encoding (IDRPE) to generate secure, non-invertible biometric templates. The RP matrix is utilized to minimize the biometric feature vector's dimensionality while maintaining its discriminative properties, thereby enhancing privacy through non-invertible transformation. The IDRPE technique is then applied to encrypt the transformed feature vector, further securing the biometric data by introducing additional randomness and non-linearity. To confirm the efficacy of the proposed technique, the experimental procedure is carried out on two CASIA Iris V4 and IITD iris datasets. The integration of these two techniques ensures that the generated biometric templates are both cancelable and resistant to various security threats, making them highly suitable for cloud-based biometric authentication systems. From the results the proposed work, has lower EER 0.42% with less computational time of 6ms.

Keywords. Biometrics, cancelable templates, Random Projection matrix, Double Random Phase Encoding.

Introduction

Cancelable biometric template generation is a critical advancement in the field of biometric security, addressing the increasing need for privacy-preserving and secure biometric systems [1, 2]. As biometric authentication becomes more prevalent, particularly in cloud-based environments, the challenges associated with securing sensitive biometric data have intensified. Traditional biometric systems store biometric templates, such as iris patterns, fingerprints, or facial features, in databases for later comparison during authentication processes [3-5]. However, these systems face significant security risks, including potential data breaches and unauthorized access. If biometric data is compromised, it cannot be replaced like a password or a security token, leading to permanent privacy loss. This necessitates the development of methods that can generate secure, non-invertible, and revocable biometric templates, known as cancelable biometrics. The physiological and behavioral characteristics of a person are focused in biometrics. These characteristics can uniquely define the person in and hence applicable in various uses which includes E-Passport, forensic applications, surveillance, financial, and e-governance.

Among the numerous biometric techniques like fingerprint recognition, face recognition, palm print recognition, hand geometry and iris recognition, iris recognition has been shown to provide a high degree of security with optimal statistical efficiency. The multi-biometric authentication strategy uses fingerprint and iris biometric features for recognition [6, 7]. Cancelable biometric template generation has emerged as a pivotal technology for enhancing security and privacy in cloud-based biometric systems. Traditional biometric systems are susceptible to various security threats, including data breaches and identity theft, which can have severe impacts given the sensitivity of biometric data. Cancelable biometrics offers a robust solution by transforming the original biometric data into a secure, non-reversible format. This approach ensures that even if the transformed data is compromised, the original biometric data remains protected. Among the various techniques for generating cancelable biometric templates, the combination of Random Projection Matrix (RPM) and Double Random Phase Encoding (DRPE) stands out for its efficacy and robustness. The importance of the application of biometric recognition in smart environments is discussed in [8–10]. This approach ensures that the security and privacy of the individual are maintained, even in the event of a data breach. Among the various techniques for generating cancelable biometric templates, the combination of Random Projection (RP) matrix and Improved Double Random Phase Encoding (IDRPE) has emerged as a promising solution due to its robustness and flexibility.

In this paper, the integration of Random Projection Matrix and Improved Double Random Phase Encoding provides a comprehensive solution for generating cancelable biometric templates. The RP matrix is applied first to reduce the dimensionality of the biometric feature vector and ensure non-invertibility. This transformed feature vector is then encrypted using IDRPE, adding a robust layer of security by introducing significant randomness and complexity into the template. The combination of these techniques results in a cancelable biometric template that is both secure and efficient.

Related work

Several attempts have been made by various researchers in the area of cancellable biometrics.

In [11], the authors used an encryption function and a one-way transformation function to build a modified cancelable biometric template. Here, the random projection matrix generates the initial feature vector. Next, used Double Random Phase Encryption (DRPE) in the FFT domain to construct an encrypted cancelable iris code. Using a person's left and right iris images, the suggested framework constructs a single cancelable iris template. This function ensures secure authentication by allowing the cancellation of the generated iris code without compromising privacy. They conducted the experiment on two state-of-the-art datasets, IITD iris and CASIA iris V4, to confirm the effectiveness of the suggested technique. They observed an encouraging 99.59% accuracy, a 99.88% identification rate, and a 0.46% equal error rate (ERR) in the results analysis. With a maximum true positive and true negative rate of 100% and a recognition time of 7ms, the suggested method has also shown its computational efficiency in recognizing the iris code. In [12], the authors used the robust technique using quaternion mathematics and an auxiliary input biometric template, they achieve performance levels that are remarkable and beyond prior norms. Simulation tests show that the cancelable biometric identification method they introduced performs quite well, remaining durable even when exposed to noise. This cancelable face recognition system does a good job of meeting these goals, with an equal error rate (EER) of 0.00174 and a significant area under the receiver operating characteristic (ROC) curve of 0.994. On average, each secure template created takes just 0.056263 seconds, demonstrating the incredible efficiency of the solution. This demonstrates the swift and efficient resolution of current security issues. In [13], the authors improved the performance of the Double Random Phase Encoding (DRPE) algorithm by adding a second biometric as an extra input and using quaternion math in the suggested method. The proposed cancelable biometric recognition method outperforms the state-of-the-art methods in simulation tests, even in the presence of noise. This is especially true when it comes to cancelable face recognition, where the results show an impressive ROC curve area of 0.994 and an equally impressive EER of 0.0017.

In [14], the authors introduced a unimodal cancelable biometric system. The suggested system evaluates bio-signals, which are biometric signals like voiceprints, electroencephalography, and electrocardiography. A key component of the suggested system is the empirical mode decomposition (EMD). EMD allows for the extraction of a variety of intrinsic mode functions (IMFs) from a biosignal. Much of the bio-signal-distinguishing signal energy travels via the first IMF. Cancellable template creation relies heavily on the encryption technique. They used DRPE and its RPM to encrypt the first IMF after the 2-D format conversion. A non-invertible transformation may be DRPE with its random masks. The first encrypted IMF used a reference signal as a cover signal. However, to obtain the cancelable template, we substitute the bio-signal's encrypted first IMF for the reference signal's first IMF. To complete the verification procedure, we compare the encrypted versions of the previously stored first IMF with the new first IMF. The suggested solution performs well, according to the simulation results. To evaluate the suggested system, we explored various measures. In [15], the authors suggested a new cancelable biometric approach that does not rely on any particular modality to circumvent these restrictions. This method generates a cancelable template (pseudo identifier) by dividing the biometric feature vector by the distance between several randomly produced transformations. To accomplish these modifications, they grouped the feature vector components according to a set of unique random vectors for each user. The suggested method doesn't store any information about the biometric template. Instead, it creates a cancelable template that only stores the distance values between the random transformations of the feature vector. This makes it impossible to reconstruct the template. They tested the suggested scheme's recognition performance for both fingerprint and face modalities.

Materials and Methods

The proposed “fingerprint authentication system” contains enrolment process and verification process (see Figure 1). The enrollment process creates and stores a user's template in order to register them, while the verification process generates a query user's template in order to compare it with the enrolled user.

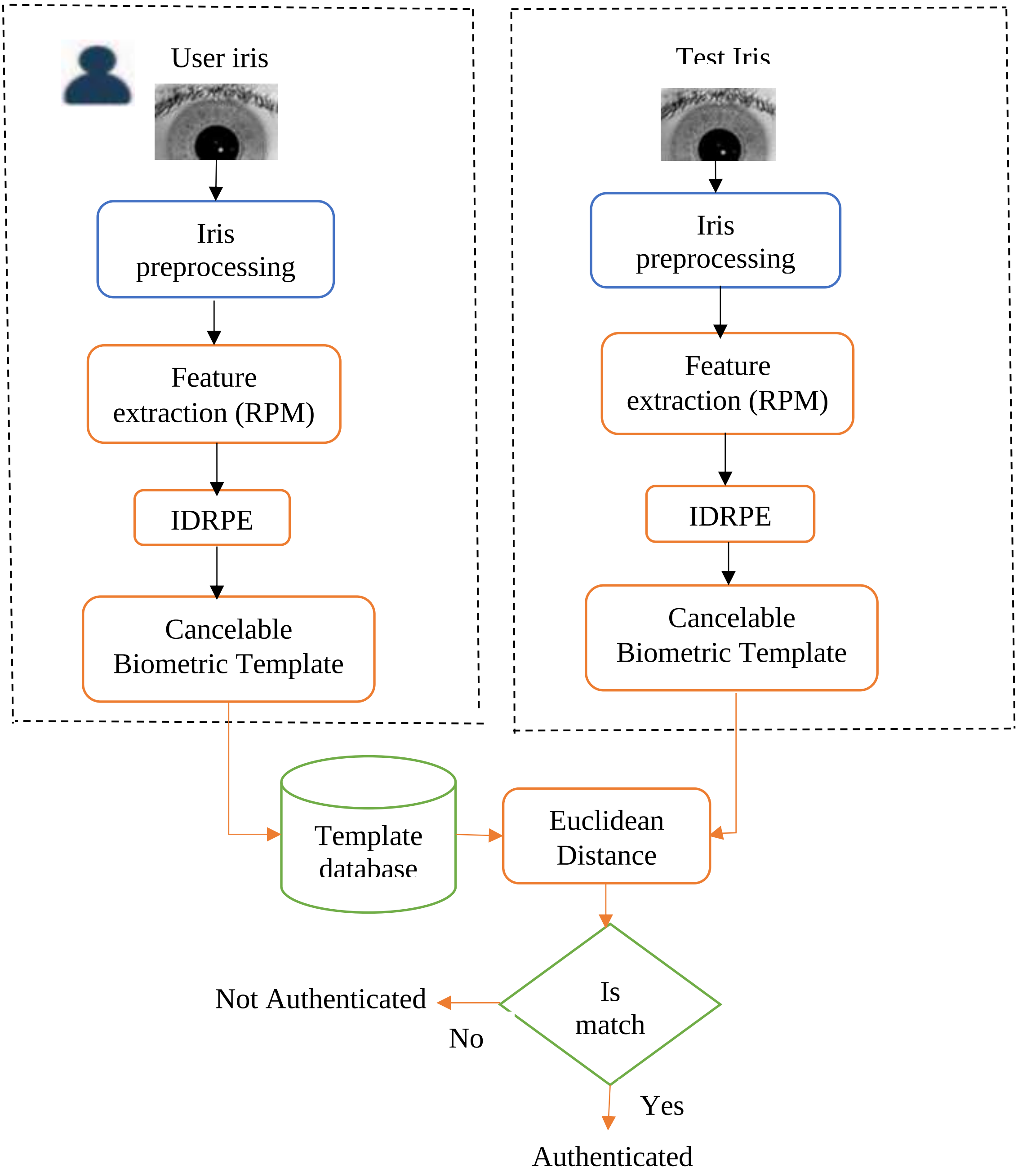


Figure 1: Bock diagram of fingerprint authentication system.

Typically, the enrollment process involves acquiring fingerprints using a fingerprint sensor, followed by the generation and storage of templates. Typically, the verification process includes collecting fingerprints, generating a template, and then comparing the two. Applications running on the cloud first send end-user fingerprints to the cloud to generate, store, and match templates. The end user is responsible for taking a fingerprint, uploading it to the cloud, and receiving the verification result. The fact that the cloud stores personally identifiable information (such as fingerprints) raises security concerns.

Iris preprocessing

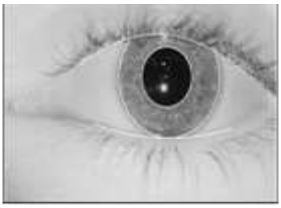
This is a crucial step in the overall process of iris recognition, which ensures that the iris patterns are accurately captured and prepared for feature extraction and matching. The main goals of iris preprocessing are to locate the iris region within the eye image, normalize the iris to a consistent format, and enhance the quality of the image to facilitate reliable recognition.

Image Acquisition: The first step is to capture a high-quality image of the eye using specialized cameras. The quality of the captured image plays a significant role in the subsequent preprocessing steps and the overall accuracy of the iris recognition system.

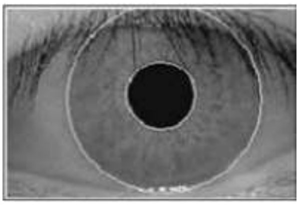
Iris Localization: The process of iris localization entails locating the iris borders within the ocular image. Accurately differentiating the iris's pupil from its sclera is important. This study employs the coarse-to-fine localization approach. A few black areas make up an image's threshold at the coarse stage. Equation (1) describes the suggested method, which uses three-tiered threshold systems based on histogram analysis. Thanks to the provided threshold approach, the suggested method works well over a wide range of intensity levels. See Figure 2 for the localized iris image.

$$\text{Threshold} = \begin{cases} 120: \sum_{j=155}^{260} d_j < 0.80\,\text{MN} \\ 60: \sum_{j=0}^{j=100} d_j < 0.35\text{MN} \\ 90: \text{Otherwise} \end{cases} \tag{1}$$

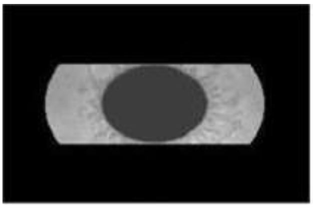
where d_j indicates the histogram based on the pixel intensity j. M and N represent the number of rows and columns in the iris image respectively.



a) Original iris image



b) Iris localization



c) Iris Segmentation

Figure 2: Iris Localization and segmentation

Perform grayscale closing, choose an appropriate threshold based on Equation (1) and convert gray image with a threshold into the binary image. Minimize the reflection effects. Obtain the pupil region by labeling the connected parts. Make the pupil center as the initial centroid point. Find the starting point for the coarse stage, then resize the iris image to a quarter size. Make marks in the 10 by 10-pixel area. Look only within the iris' borders; avoid scanning all the way around. Find the starting point that defines the intersection of two vectors.

Iris segmentation: The iris recognition process involves a crucial step of accurately isolating the iris region from the rest of the eye image. Proper segmentation is essential because any inaccuracies can lead to errors in subsequent steps like feature extraction and matching, ultimately affecting the performance of the iris recognition system. The first step in segmentation is to locate the boundaries of the iris. This involves identifying the circular boundaries between the iris and the pupil (inner boundary) and between the iris and the sclera (outer boundary). The pupil is typically the darkest part of the eye image. In this paper Hough Transform is used to identify the circular boundary of the pupil. The resulting circle is determined by its center and radius, and after locating the pupil, the outer boundary of the iris is detected.

Iris Normalization: After segmentation, the iris region is normalized to a fixed size and shape to compensate for variations in pupil size and camera distance. In this paper we use Daugman's Rubber Sheet Model. This model remaps the segmented iris region from Cartesian coordinates to a dimensionless polar coordinate system, where the radius of the iris is scaled to a constant value. This process ensures that the iris pattern is consistently represented, regardless of the conditions during image capture.

Feature Extraction

One of the modernized approaches for generating feature vector is random projection. Random Projection matrix (RPM) is a powerful dimensionality reduction technique that preserves the structural integrity of the data while significantly reducing its dimensionality. By projecting the high-dimensional biometric feature vectors onto a lower-dimensional subspace using a randomly generated matrix, RP effectively minimizes the risk of overfitting and enhances computational efficiency. The use of a random projection matrix ensures that the transformation is non-invertible, thereby adding a layer of security to the biometric template. The transformation is defined as:

$$y \in Rx \qquad (2)$$

where $x \in R^n$ is the original biometric feature vector. $R \in R^{m \times n}$ is the random projection matrix, where $m < n$. $y \in R^m$ is the transformed feature vector. The matrix R is typically generated with entries sampled from a Gaussian distribution $\mathcal{N}\left(0, \frac{1}{m}\right)$, ensuring that the distances between vectors are approximately preserved.

By projecting normalized iris onto a randomly generated subspace, the feature extraction step produces a first-level cancelable iris template. Various sectors make up the top half of the normalized iris. The concatenation unit is the end product of merging all the sectors using the random projection matrix. Because it is closer to the pupil border, the upper half of the iris is less susceptible to noise degeneration than the lower half. The suggested technique uses the top portion of the iris to enhance identification rate while preventing noise degradation. Algorithm 1's random projection process culminates in the generation of a perfect cancelable feature vector. Figure 3 shows the flow of the random projection strategy.

Algorithm: 1 Generation of cancelable feature vector 1
Input : Upper half iris image
Output : Cancelable Feature vector 1

Process:
Step 1 : Read upper half iris image
Step 2 : Convert the iris image into different sectors
Step 3 : Generate different blocks on iris sectors
Step 4 : Extract two dimensional Gabor features
Step 5 : Apply random projection to each Gabor feature
Step 6: Generate a cancelable feature vector on the concatenation.

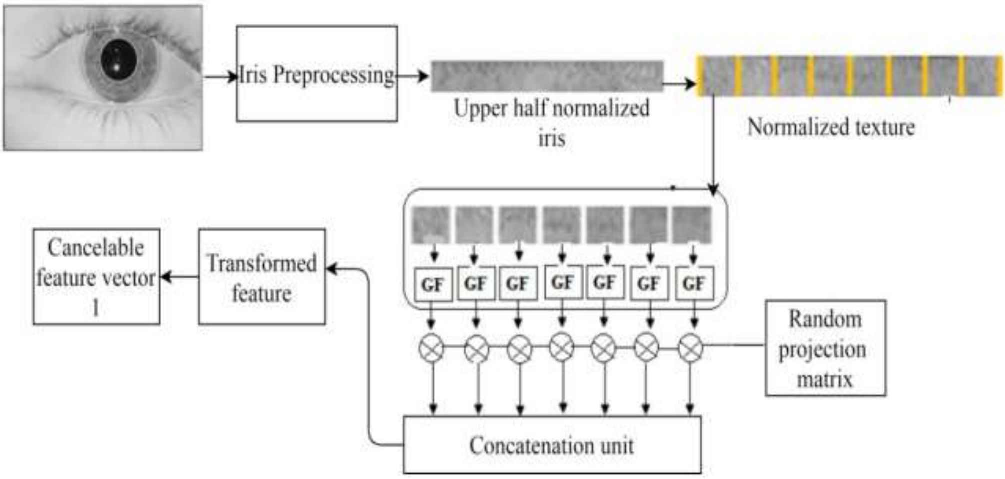


Figure 3: Generation of cancelable feature vector using RPM

Cancelable Template generation

In Figure 4, we can see the results of the IDRPE-based template generation process. This process involves enrollment and verification. In the previous step, two random keys, P_1 and P_2, were input to FFT. During the enrolling phase, we generate the cancelable feature vector 1 using the left iris and Algorithm 1. Subsequently, $P_1(u, v)$ and the cancelable feature vector 1 enter the FFT. We re-encode the FFT output and $P_2(x, y)$ from the user's right iris in the FFT domain to generate a cancelable iris template. The verification phase entails repeating the enrollment phase's steps until we create the cancelable iris template. We use hamming distance to compare the newly created cancelable template with the one we obtained from the application database.

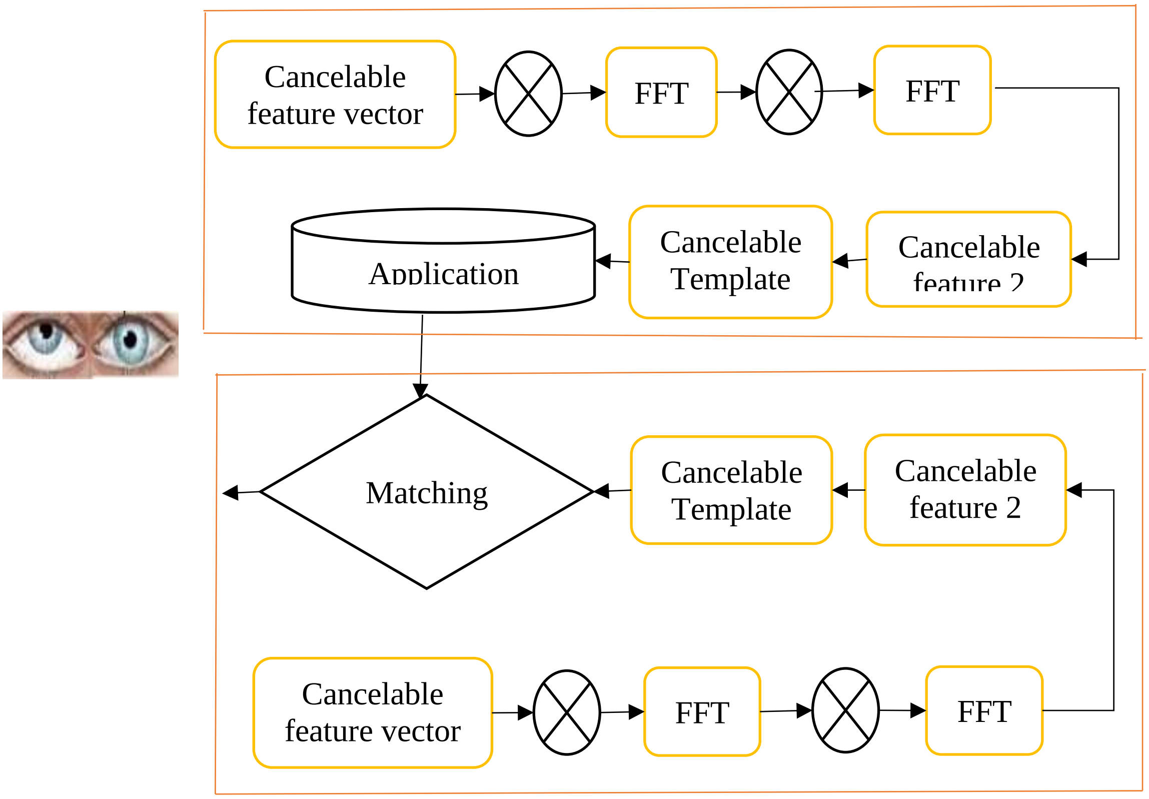


Figure 4: Cancelable template generation based on IDRPE

Improved Double Random Phase Encoding (IDRPE)

This is an optical encryption technique that employs two random phase masks to encrypt the biometric data. The process involves performing a Fourier transform on the biometric image, multiplying the result by a random phase mask, applying an inverse Fourier transform, and then repeating these steps with a second random phase mask. This multi-stage encryption process ensures that the biometric data is securely transformed and non-reversible, thereby safeguarding it against unauthorized access.

Apply the Fourier Transform to the original image and multiply the Fourier-transformed image by a random phase mask

$$I(x,y) = \mathcal{F}\{I(x,y) = I(u,v)\} \qquad (3)$$

$$P_1(u,v) = e^{j\phi_1(u,v)}$$

$$I_1(u,v) = I(u,v)P_1(u,v) \qquad (4)$$

Apply the Inverse Fourier Transform then apply a nonlinear transformation (e.g., a sigmoid function) to the result:

$$I_1(x,y) = \mathcal{F}^{-1}\{I_1(u,v)\} \qquad (5)$$

$$I_2(x,y) = \sigma\{I_1(x,y)\} \qquad (6)$$

Multiply this result by another random phase mask $P_2(x,y) = e^{j\phi_2(x,y)}$

$$I_3(x,y) = I_2(x,y)\ P_2(x,y) \qquad (7)$$

Apply a Fourier Transform to obtain the encrypted image

$$I_{IDRPE}(u,v) = \mathcal{F}\{I_3(x,y)\} \qquad (8)$$

Matching process

Iris feature matching is a crucial step in the iris recognition process, where the extracted features of an iris image are compared against stored templates to determine identity or verify an individual. During the matching process, the iris code of the captured iris image (probe) is compared against the stored iris codes (templates) in the database. The comparison is typically performed using a hamming distance metric. The Hamming distance is defined as:

$$HD = \frac{1}{N}\sum_{i=1}^{N}(a_i \oplus b_i) \qquad (9)$$

where a_i and b_i are the corresponding bits in the probe and template iris codes, N is the total number of bits, and $\oplus$ denotes the XOR operation. A lower Hamming distance indicates a higher similarity between the iris codes.

Results and Discussion

This section details the final output of the suggested method. The simulation results showed that, in comparison to the current methods, the suggested method is more efficient across a variety of parameters. We simulate the suggested technique by building Anaconda using the Python programming language. The computer hardware requirements for the experiment include an Intel Core i5 CPU and 6 GB of RAM. This experiment utilizes two well-known state-of-the-art datasets: IITD and CASIA version 4.0. When studying iris recognition, the CASIA-IrisV4 dataset is crucial. This iris dataset, created by the Institute of Automation (CASIA) of the Chinese Academy of Sciences, is one of the most extensive ones currently accessible. The CASIA-IrisV4 collection includes more than 54,000 iris pictures. The collection includes more than 1,800 people's iris photographs. The collection saves all photos in JPEG format, with sizes ranging from 640x480 pixels in several sections. Yet another well-known dataset for iris identification research is the IITD (Indian Institute of Technology, Delhi) Iris Dataset. There are 2,240 near-infrared photos in the IITD Iris collection. The dataset contains 224 subjects, each with five images per eye, and all images are saved in BMP format with a resolution of 320 by 240 pixels.

Table 1. Performance assessment of proposed work on CASIA iris dataset.

No. of Iris Samples	**FAR (%)**	**FRR (%)**	**TPR (%)**	**TNR (%)**	**EER (%)**
100	0.12	0.12	100	100	1.22
500	0.24	0.18	100	100	1.31
1000	0.38	0.28	99.32	99.34	1.38
1500	0.48	0.35	98.47	98.21	1.46
2000	0.55	0.42	98.22	98.33	1.51

We used the suggested cancelable method to examine 2000 iris samples from the CASIA dataset. With this dataset, the highest possible TPR and TNR are both 100%. There is a maximum allowable ratio of 0.55% for FAR and 0.42% for FRR. An EER of at least 1.22. Figure 5 shows the graphical depiction of the FAR and FRR from the CASIA dataset.

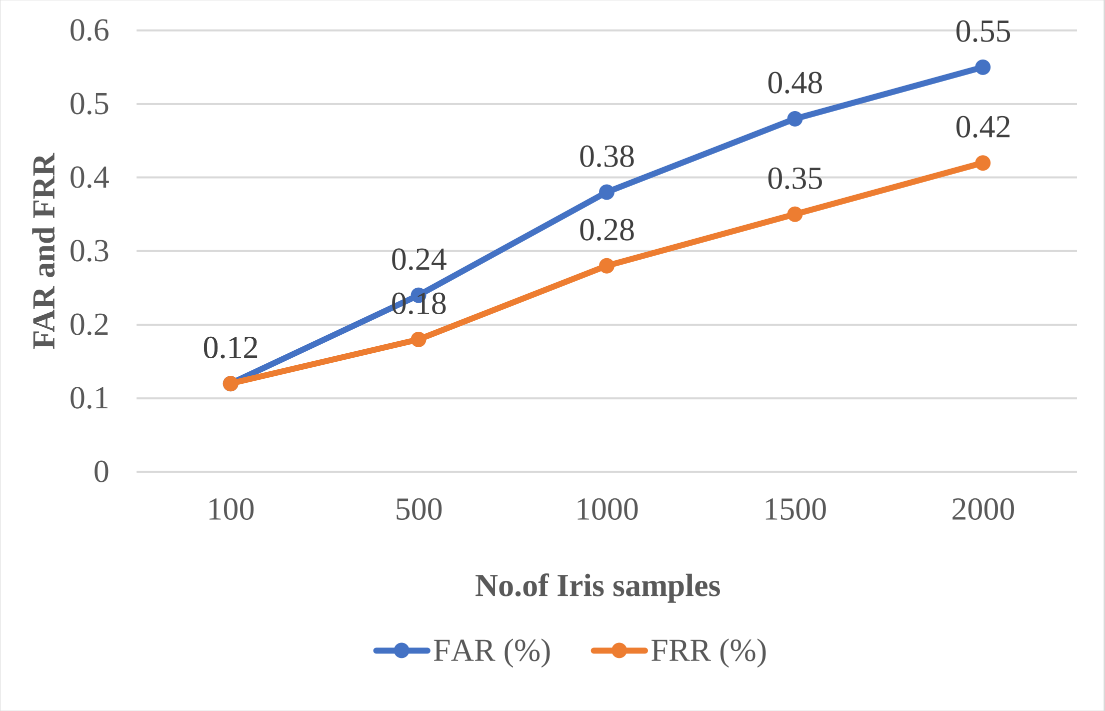


Figure 5: Plot of FAR and FRR for CASIA iris dataset

Table 2. Performance assessment of proposed work on IITD iris dataset.

No. of Iris Samples	**FAR (%)**	**FRR (%)**	**TPR (%)**	**TNR (%)**	**EER (%)**

100	0	0	100	100	1.12
500	0	0	100	100	1.26
1000	0.24	0.22	99.21	99.21	1.32
1500	0.36	0.32	98.32	98.11	1.38
2000	0.45	0.40	98.12	98.05	1.41

The IITD dataset provides 2000 iris samples for examination using a suggested cancelable technique. With this dataset, the highest possible TPR and TNR are both 100%. Both the FAR and the FRR have maximum values of 0.40% and 0.45%, respectively. For 100 iris samples, the minimal EER is around 1.12. Figure 6 shows the graphical depiction of the FAR and FRR from the CASIA dataset.

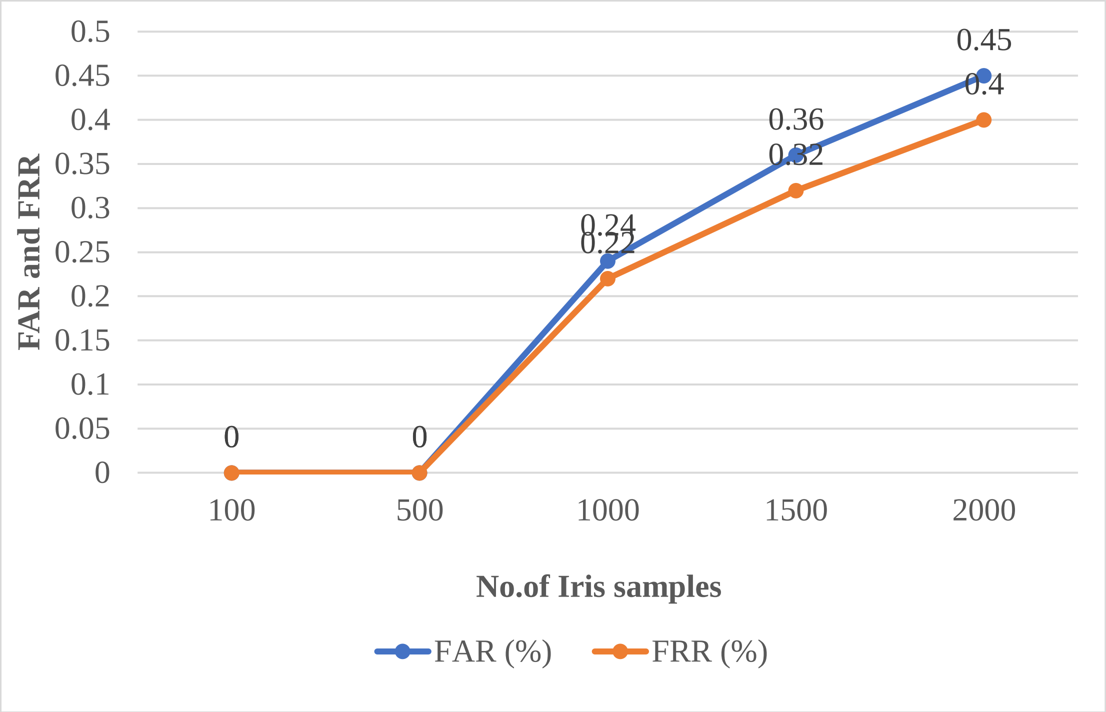


Figure 6: Plot of FAR and FRR for IITD iris dataset.

In biometric systems, EER is often the most crucial parameter to take into account for any cancelable scheme. In Table 3, we can see how the suggested scheme's EER compares to the current methods.

Table 3 Comparison of EER and accuracy of cancelable (RPM+IDRPE) with existing schemes

Methods	**Dataset used**	**Algorithm used**	**EER in (%)**
Kaur et al. (2018) [16]	IITD	Random distance	0.60

Soliman et al. (2018) [17]	CASIA V3	Modified logistic map	1.17
Sadhya et al. (2019) [18]	CASIA V3	Randomized bit sampling	1.4
Ghammam et al. (2020) [19]	CASIA	Index of max hashing	1.47
Khaur et al. (2020) [20]	CASIA	Random distance	0.96
Proposed work	CASIA and IITD Iris Dataset	RPM+IDRPE	0.40

We detail the performance of the suggested method by comparing it with the most advanced cancelable biometric systems. The results show that the suggested strategy reduces computing time by 6 ms while maintaining a lower EER of 0.40%. The suggested strategy demonstrates an improved accuracy of 99.61% while maintaining a reduced EER rate. The suggested system's increased performance with reduced execution time enhances its computational efficiency.

Conclusion

In this paper, a cancelable template generation is proposed based on RPM and IDRPE. The method not only ensures that the original biometric data cannot be reconstructed from the generated templates but also provides flexibility in managing biometric data, such as template revocation and reissue. The successful integration of these techniques demonstrates their potential for deployment in cloud-based biometric authentication systems, where security and privacy are paramount. This method uses two random masks as keys obtained from the iris of the users. The result shows that the proposed method provides better result in terms of maximum TPR and TNR of 100%. The optimal EER obtained from the proposed approach is 0.42% with higher accuracy of 99.46%. Future work will explore the application of this method to other biometric modalities and further optimize its performance for real-time use.

References

[1] Helmy, Mai. (2024). Proposed cancelable biometrics system based on hybrid optical crypto-steganography audio framework for cyber security applications. Multimedia Tools and Applications. 1-26. 10.1007/s11042-024-18232-w.

[2] Wang, Min & Wang, Song & Hu, Jiankun. (2022). PolyCosGraph: A Privacy-Preserving Cancelable EEG Biometric System. IEEE Transactions on Dependable and Secure Computing. PP. 1-15. 10.1109/TDSC.2022.3218782.

[3] V. Pujari, R. Patil, and S. Sutar, “Research Paper On Biometrics Security,” in Contemporary Research In India, Emerging Advancement and Challenges In Science, Technology And Management, 2021.

[4] U. Gawande, Y. Golhar, and K. Hajari, “Biometric-based security system: issues and challenges,” in Intelligent Techniques in Signal Processing for Multimedia Security, Springer, 2017.

[5] B. Guelta, R. Tlemsani, S. Chouraqui, and M. Benouis, "An improved behavioral biometric system based on gait and ECG signals," International Journal of Intelligent Engineering and Systems, vol. 12, no. 6, pp. 147–156, 2019.

[6] Rajasekar, V., Premalatha, J. & Sathya, K. Multi factor signcryption scheme for secure authentication using hyper elliptic curve cryptography and biohash function. Bull. Polish Acad. Sci. Tech. Sci. 68(4), 923–935 (2020).

[7] Galterio, M. G., Angelic, S. S. & Hayajneh, T. A review of facial biometrics security for smart devices. Computers 7(3), 37 (2018).

[8] Menon, V., Jayaraman, B. & Govindaraju, V. Enhancing biometric recognition with spatiotemporal reasoning in smart environments. Pers. Ubiquit. Comput. 17(5), 987–998 (2013).

[9] Ryo, O., & Yasushi, Y. Smart Device-based Multimodal Biometric Authentication with the Function for Environment Recognition. In Proceedings of international symposium on computing and networking (CANDAR), IEEE Book Series: International Symposium on Computing and Networking 495–498 (2015).

[10] De Marsico, M., Mecca, A. & Barra, S. Walking in a smart city: investigating the gait stabilization effect for biometric recognition via wearable sensors. Comput. Electr. Eng. 80, 106501 (2019).

[11] Rajasekar, Vani & Premalatha, J. & Sathya, K. (2021). Cancelable Iris template for secure authentication based on random projection and double random phase encoding. Peer-to-Peer Networking and Applications. 14. 1-16. 10.1007/s12083-020-01046-6.

[12] Nasr, Mahmoud & Piórkowski, Adam & Abd El-Samie, Fathi. (2024). Quaternion double random phase encoding for privacy-preserving cancelable biometrics. Multimedia Tools and Applications. 10.1007/s11042-024-18621-1.

[13] Nasr, Mahmoud & Piórkowski, Adam & Abdelaziz, Mohamad & Abd El-Samie, Fathi. (2023). Cancelable Biometric System Based on the Quaternion Implementation of Double Random Phase Encoding. 1-7. 10.1109/ICEEM58740.2023.10319630.

[14] Salama, Gerges & El-Shafai, Walid & El-Gazar, Safaa & Omar, Basma & Hassan, A. & El-Samie, Fathi & Hussein, Aziza. (2023). Efficient Implementation of Double Random Phase Encoding and Empirical Mode Decomposition for Cancelable Biometrics. 10.21203/rs.3.rs-2644446/v1.

[15] S P, Ragendhu & Thomas Kallivayalil, Tony & Emmanuel, Sabu. (2024). Cancelable Biometric Template Generation Using Random Feature Vector Transformations. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3366456.

[16] Kaur, H & Khanna, P 2018, "Random distance method for generating unimodal and multimodal cancelable biometric features‟, IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 709-719.

[17] Soliman, RF, Amin, M & Abd El-Samie, FE 2018, "A double random phase encoding approach for cancelable iris recognition‟, Optical and Quantum Electronics, vol. 50, no. 8, pp.1-12.

[18] Sadhya, D & Raman, B 2019, „Generation of cancelable iris templates via randomized bit sampling‟, IEEE Transactions on Information Forensics and Security, vol. 14, no. 11, pp. 2972-2986.

[19] Ghammam, L, Karabina, K, Lacharme, P & Atighehchi, K 2020, "A cryptanalysis of two cancelable biometric schemes based on index-of max hashing‟, IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2869-2880.

[20] Kaur, H & Khanna, P 2020, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing‟, Future Generation Computer Systems, vol. 102, pp. 30-41.