Cancelable biometric template generation based on Log-Gabor filter and Hyperelliptic Curve Cryptography and Neuro fuzzy system

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.

Abstract: For biometric identification systems to be secure and private, the creation of cancelable biometric templates has emerged as a critical field of study. This study suggests a new way to make biometric templates that can be deleted. It does this by using the strength of Log-Gabor filters for feature extraction, the safety of Hyperelliptic Curve Cryptography (HECC), and the accuracy of a neuro-fuzzy system for classification. Log-Gabor filters extract strong phase-based characteristics from iris pictures to achieve high discriminating capacity over a variety of spatial frequencies. We use a lightweight cryptographic approach, HECC, to effectively encrypt the retrieved characteristics and secure the biometric templates against unauthorized access and data breaches. Furthermore, we incorporate a neuro-fuzzy system (NFS) to enhance decision-making by combining the learning capabilities of neural networks with the reasoning flexibility of fuzzy logic. Tests on the benchmark CASIA Iris V4 and IITD iris datasets show that the suggested method achieves safe, reversible, and very accurate biometric authentication with a low false acceptance rate (FAR) and false rejection rate (FRR). In order to meet the demands of both current biometric systems. This hybrid technique provides a secure and efficient solution.

Keywords. Biometrics, cancelable templates, Log-Gabor filters, Hyperelliptic Curve Cryptograph, neuro-fuzzy system.

Introduction

Biometric recognition systems have gained significant attention due to their enhanced security for identification. Irises are one kind of biometric data that are known for their reliability, stability, and improved accuracy for recognising users [1]. Iris recognition is the best option for safe authentication systems because the complex iris patterns don't change over time. High computational costs and vulnerability to security risks like identity theft and data manipulation during communication are two of the many issues that remain with iris-based systems, despite their demonstrated dependability [2]. Iris recognition has received extensive attention due to its high dependability in biometric authentication. Iris pre-processing is the first stage of the iris identification procedure. There are potential privacy concerns with biometric technology. Storing biometric templates in a database exposes them to potential theft. It is now possible to apply the learned iris templates to other applications. A leak of the user's biometric data poses a significant risk to their privacy and security. To prevent data breaches, biometric data must be stored securely. The security component shouldn't reduce biometric efficacy because recognition of biometric templates is an important and computationally intensive activity. This can create secure one-to-many correlations and improve our recognition performance. Decrypted biometric authentication or verification can be achieved using simple biometric encryption methods, which include encrypting biometric characteristics at the transmitter and decrypting them at the receiver. Among the most well-known approaches in this field, Daugman's algorithm has strong iris feature extraction and matching capabilities; it makes use of 2D Gabor filters. Over the years, many researchers have steadily improved the accuracy and processing

time of iris preprocessing methods, as evidenced by [3]. The trade-off between computing complexity and identification accuracy is one of the constraints that traditional iris recognition algorithms still have. Nevertheless, issues like noise resilience and adaptability to different illumination scenarios continue to be major concerns. HECC is an emerging cryptography technique that offers protections comparable to Elliptic Curve Cryptography (ECC) with a much lower computing cost due to increasingly smaller key sizes. Because of its effectiveness in protecting biometric data, HECC is well-suited for systems with limited resources, as shown in [4]. In terms of security and speed, HECC is a better option for real-time authentication systems than more conventional cryptographic algorithms such as RSA and ECC [5]. To further improve security, researchers have recently integrated cryptographic techniques with iris recognition. After using ECC to encrypt iris templates, one study found that iris recognition systems were far more secure and efficient [6]. Combining biometrics and cryptography ensures the biometric template's safety, even in the event of an intercept. When studying the effectiveness of iris recognition systems, researchers often use the IITD and CASIA Iris V4 databases [7]. Researchers used these datasets to create and evaluate secure iris recognition methods in the study [8], establishing them as the de facto standards for evaluating the precision and stability of iris recognition algorithms. Compared to more conventional approaches such as RSA or ECC, Hyperelliptic Curve Cryptography (HECC) provides superior security with much smaller key sizes while being efficient and lightweight [9, 10]. HECC protects biometric data from intrusion during transmission and storage by incorporating it into the template creation process. The number ten. Additionally, we include a neurofuzzy technology to enhance the decision-making process during biometric authentication. Neuro-fuzzy systems use both neural networks and fuzzy logic to combine their learning and reasoning powers. They can handle uncertainty and make classification more accurate in large biometric datasets. Using Log-Gabor filters for feature extraction, HECC for encryption, and neuro-fuzzy systems for decision-making leads to a strong, accurate, and cancelable biometric system that can keep sensitive biometric data safe while still delivering high authentication performance.

Related work

In the field of cancellable biometrics, several researchers have made multiple efforts.
In [11], the authors proposed hyperelliptic curve cryptography (HECC) as a method for improved iris recognition. To optimise feature extraction during iris preprocessing, the technique uses a 2D Gabor filter. HECC, a lightweight cryptographic technique, encrypts the iris template to prevent unauthorised access. The system had a lower rate of false acceptance and rejection when tested with the CASIA Iris V-4 and IITD iris datasets. It was 99.74% accurate, accepted all documents correctly 100% of the time, and took no more than 3 seconds to recognize a person. According to the results, this method is much more effective than the currently popular alternatives. The authors in [12] proposed a new cancelable biometric approach that circumvents these restrictions by not relying on any particular modality. By dividing the biometric feature vector by the distance between several randomly transformed versions of it, this approach produces a cancelable template (a pseudo identifier). To accomplish these modifications, we grouped the feature vector components according to a set of unique random vectors for each user. Since the proposed technique does not save any information about the biometric template and instead generates a cancelable template that only stores the distance values between various random feature vector transformations, template reconstruction is not an option. We test the suggested scheme's identification capabilities using both fingerprint and facial modalities. In an extreme scenario, the Equal Error Rate (EER) for the face is 1.5, and for the fingerprint it is 1.7.

The authors of [13] presented a cancelable multimodal biometric system that uses fingerprints, voiceprints, and face pictures. For verification, they used the voiceprints' Mel frequency cepstral coefficients (MFCCs). Steganography is a technique that uses block-based singular value

decomposition (BSVD) to conceal characteristics taken from voiceprints and insert them into a face picture. We use double random phase encoding (DRPE) as an encryption method to create the final cancelable templates. They enhanced the system's security by using random-phase masks (RPMs) made from fingerprint photos. The verification process involves determining the correlation between the registered and test MFCCs. We use the distribution curves for the real and fake correlations to determine a threshold value, then compare it with the correlation value. The simulation results show that the proposed system performs very well, with equal error rate (EER) values near zero and the area under the receiver operator characteristic curve (AROC) close to one. The suggested system performs well across several areas. The authors of [14] laid out the framework for a trustworthy session key agreement protocol that relies on the creation of a 256-bit session key at the end of each conversation. In order to generate the 256-bit key, every session included recording the left and right thumbs. The cancelable fingerprint biometrics were created using the communicating parties' right thumb impressions. The suggested double hash function generates a 64-bit hash value based on each party's left thumb impressions. Afterwards, using elliptic curve encryption, the two parties exchange hash values and secret values generated from their cancelable biometric data. At the conclusion of the procedure, we combine the secret value and hash value to create the revocable key for the session key agreement protocol. All of this protocol's operations are based on elliptic curve encryption for improved efficiency and security. Under the proposed protocol, unwanted third parties cannot force this group of agreed parties to choose a key. Testing on four separate FVC2002 datasets confirmed that the suggested architecture both protects users' privacy and works well with a wide range of real-time biometric applications.

In [15], the authors introduced a novel method for cancelable facial recognition based on elliptic curve cryptography (ECC). The ECC is an example of an asymmetric (public-key) encryption method. Both the sender and the receiver use a public key and a private key in public-key encryption. The suggested architecture protects the original biometric features from potential attackers by encrypting and distorting them before storing them in the database. They have utilised three sets of face biometric datasets to verify the suggested technique. To evaluate the performance, we assess the ROC curve and correlation scores. The simulation findings demonstrate the efficiency, robustness, and promising outcomes of the suggested technique. The authors of [16] showed a new cancelable biometric template-generating layout that uses selective encryption and DT-CWT fusion. The automated face-segmentation (Viola-Jones) technique uses the input facial biometric to quickly recognise objects. The Viola-Jones algorithm can detect the left and right eyes, nose, and mouth in the input biometric image. The encoder can select either the left or right eye to create an eraseable biometric template. The encoder XORs the chosen eye image with the constructed PRN matrix to generate a starting main picture. For main image encryption, they used Arnold Cat Map (ACM), which scrambles the PRN matrix pixel-by-pixel while preserving the integrity of the pixel values. Finally, they encrypt the ACM jumbled eye images using the Advanced Encryption Standard (AES) technique before storing them in the database. Furthermore, for database storage, the biometric model authentication procedure uses the AES method's PRN and Initial Key (IK) for the same individual. The DT-CWT approach creates the IK by fusing the right eye and right finger. It is necessary to create models for both the right and left eyes in order to prevent damage to only one.

Materials and Methods

The proposed “Iris 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.

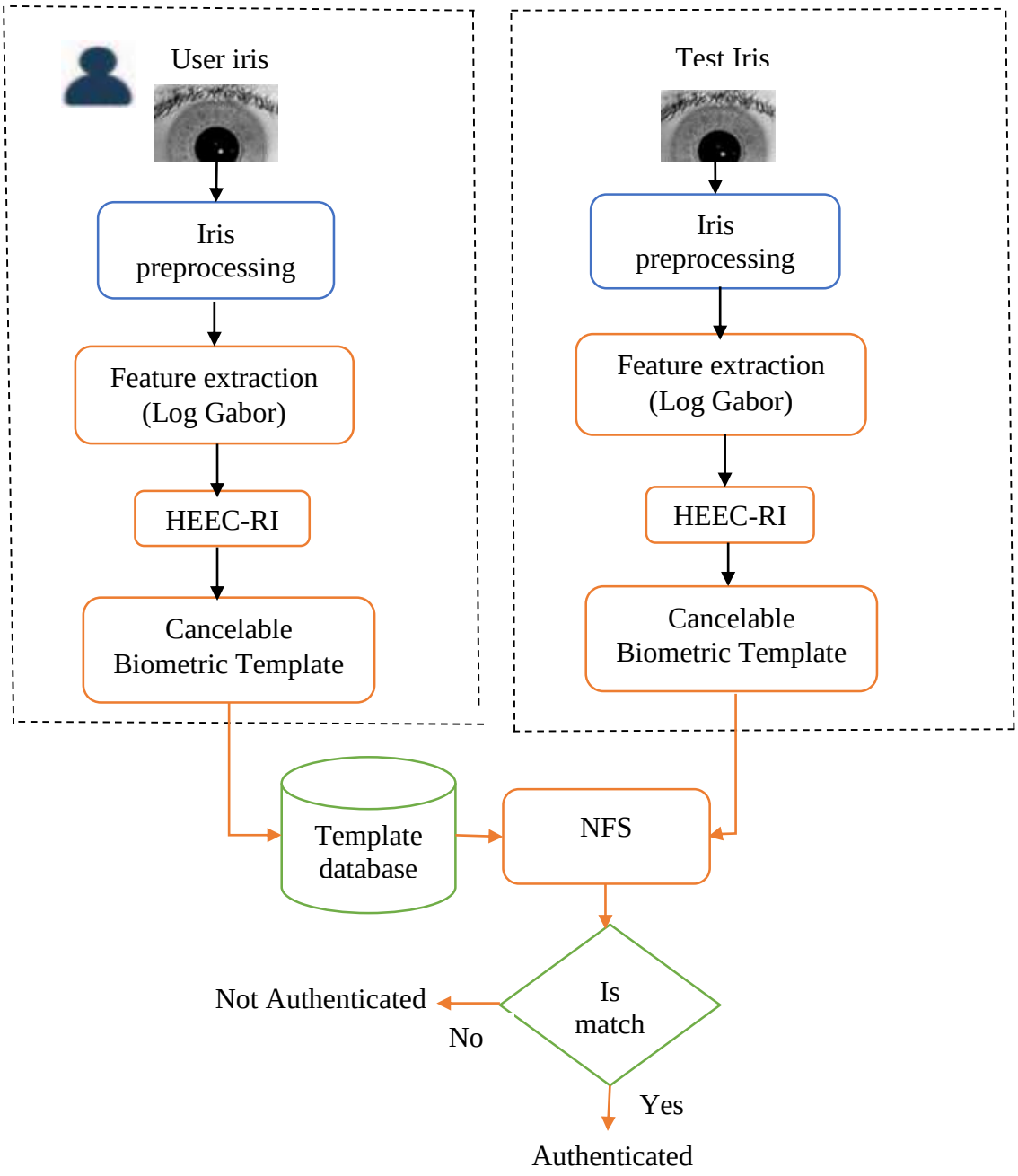

Figure 1: Block diagram of Iris authentication system.

The iris preprocessing is an important first step in the proposed cancelable template generation. During iris preprocessing, we remove noise from the original template and transform it into a normalised iris image. The Log-Gabor filter approach achieves perfect feature extraction from normalised iris images. The HECC method takes the preprocessing step's output as its input. The HECC-RI method generates a secure cancelable iris template, whereas neuro fuzzy system can achieve the template match as mentioned in latter sections.

Iris preprocessing

Ensuring the accuracy of iris pattern collection and preparation for feature extraction and matching is an essential part of the iris recognition process. Finding the iris area within the iris image, standardizing the iris to a uniform format, and improving the image quality to enable dependable detection are the primary objectives of iris preprocessing.

Iris Localization: The first step in iris localization is to find the edges of the iris in the eye picture. We must accurately distinguish the sclera and pupil of the iris. Finding the pupil's center and radius allows for localization. Using a suitable threshold value, we calculate a pupil with low pixel intensity. This paper employs the coarse-to-fine localization method. At the coarse level, an image's threshold consists of a few black patches.

Iris segmentation: Correct segmentation is critical for feature extraction and matching in iris identification, which requires precisely separating the iris area from the rest of the iris image. Find the inner (circular) border between the iris and the pupil and the outer (circular) boundary between the iris and the sclera. This is the first step in determining the iris's boundaries. In most eye images, the darkest area is the pupil. We can find the center and radius of the pupil using the Hough transform, which together define its circular border.

Iris Normalization: In this study, we use Daugman's Rubber Sheet Model to normalise the segmented iris area to a constant size and shape. This model accounts for fluctuations in pupil size and camera distance. The model changes the segmented iris area from a Cartesian to a dimensionless polar coordinate system. This makes sure that the iris pattern is always shown the same way, no matter how the picture was taken.

Log-Gabor filters: Iris identification is highly effective due to their ability to record a wide range of spatial frequencies while maintaining phase information. Log-Gabor filters, unlike conventional Gabor filters that rely on Gaussian functions, enable improved frequency selectivity and precise feature extraction. It is possible to characterize a Log-Gabor filter in terms of either space or frequency. This is what the formula entails:

$$G(f) = exp\left(-\frac{log^2\left({}^{f}/_{f_0}\right)}{2.log^2(\sigma_f)}\right) \quad (1)$$

where f is the frequency, f_0 is the center frequency of the filter, σ_f is the standard deviation of the filter in the frequency domain, controlling the bandwidth of the filter.

To better capture higher frequencies, log-Gabor filters differ from conventional Gabor filters in that they guarantee zero DC response or no energy at zero frequency. It is common practice to apply these filters at various angles in order to glean directional data. We can express the filter's orientation adjustment as follows:

$$G(\theta) = exp\left(\frac{(\theta - \theta_0)^2}{2.\sigma_\theta^2}\right) \quad (2)$$

where θ is the orientation of the filter, θ_0 is the preferred orientation, σ_θ is the angular spread, determining how selective the filter is for a specific orientation.

The Log-Gabor filter combines the radial and angular components in the frequency domain. This equation illustrates a frequency- and orientation-selective Log-Gabor filter.

$$G(f,\theta) = exp\left(-\frac{log^2\left(f/f_0\right)}{2.log^2(\sigma_f)}\right).exp\left(\frac{(\theta-\theta_0)^2}{2.\sigma_\theta^2}\right) \quad (3)$$

While conventional Gabor filters have a straightforward analytical shape in the space domain, log-Gabor filters do not. The inverse Fourier transform applied to the frequency domain filter $G(f,\theta)$ may be used to calculate their spatial domain response, however. Using this information, we can calculate the spatial domain response of the filter, which is $g(x,y)$.

$$g(x,y) = F^{-1}\big(G(f,\theta)\big) \quad (4)$$

where F^{-1} denotes the inverse Fourier transform.

HECC-RI approach

This method uses the real and imaginary components of the curve to convert the biometric iris data into a cancelable template using Hyperelliptic Curve Cryptography (HECC). It provides security and revocability by breaking down the iris feature vector into various parts, preventing direct storage of the original biometric data. If we compromise on an existing template, we can use an alternative transformation to create a new cancelable template.

We denote the extracted iris feature vector from the iris image as F_{iris}. We can extract the features using Log-Gabor filters. We will use this feature vector to create a secure cancelable template called F_{iris}.

$$F_{iris} = [f_1, f_2, \ldots\ldots, f_n] \quad (5)$$

where $f_i \in \mathbb{R}$ are the extracted features

A hyperelliptic curve C of genus g over a finite field F_q is defined by the equation:

$$C: y^2 + h(x)y = f(x) \quad (6)$$

where $h(x)$ and $f(x)$ are polynomials over F_q, the degree of $f(x)$ is $2g+1$ for a genus g curve.

For genus $g=2$, this simplifies to:

$$C: y^2 + h(x)y = f(x) \quad (7)$$

with polynomials $h(x)$ and $f(x)$ of degree 1 and 5, respectively. The extracted iris feature vector F_{iris} is mapped to a divisor D on the curve, which consists of real and imaginary components.

The divisor D on a hyperelliptic curve can be decomposed into its real part and imaginary part where the real part corresponds to the positions of points on the curve and the imaginary part corresponds to the values at those positions. mathematically, a divisor D is represented as:

$$D = D_{re} + iD_{im} \quad (8)$$

where D_{re} represents the real part (positions of points), D_{im} represents the imaginary part (values at those points).

For an iris feature vector F_{iris}, map the features to a divisor such that:

$$D_{re} = [x_1, x_2, \dots, x_n] \quad (9)$$

where x_i corresponds to the positions on the curve (real part).

$$D_{im} = [y_1, y_2, \dots, y_n] \quad (10)$$

where y_i corresponds to the values of the function at those positions (imaginary part).

Cancelable Template generation

Applying a transformation to create a cancelable template follows the feature vector's mapping to the hyperelliptic curve *C* as a divisor *D*. Using a random transformation matrix *T*, we transform the real and imaginary components of the divisor independently.

$$\widehat{D}_{re} = T_{re}.D_{re} \quad (11)$$

$$\widehat{D}_{im} = T_{im}.D_{im} \quad (12)$$

where T_{re} and T_{im} are random transformation matrices for the real and imaginary parts, respectively.

The transformed divisor $\widehat{D}$ represents the cancelable template:

$$\widehat{D} = \widehat{D}_{re} + i\widehat{D}_{im} \quad (13)$$

We implement HECC to guarantee the cancelable template's security. The encryption process uses scalar multiplication on the hyperelliptic curve's Jacobian.

Scalar multiplication of the converted divisor, $\widehat{D}$, and the scalar private key, *k*, yields the encrypted template *C*.

$$C = k.\widehat{D} \quad (14)$$

We can safely store or share this encrypted cancelable template *C* without fear of compromising the original biometric data.

Matching process

Iris feature matching, which involves comparing an image's extracted characteristics to pre-stored templates. Finding out whether two iris feature vectors belong to the same person and classifying the retrieved iris characteristics are the primary objectives. The Adaptive Neuro-Fuzzy Inference System (ANFIS) is a neuro-fuzzy system that combines a fuzzy inference system with a neural network to learn fuzzy rules in an adaptive manner.

"If feature f_i is close to feature f_i' (from the template), then match degree is high."

Typically represented as Gaussian functions, they explain the membership of each input feature to a fuzzy collection. The NFS receives labelled data during training, where each input represents a pair of iris feature vectors (F_{query}, $F_{template}$), derived from the query and the stored templates. By minimizing the matching error, the neural network component optimizes fuzzy membership functions and the rule base.

A matching score indicates how similar the query iris is to the template. The threshold can identify two iris images from the same user:

$$Match\ score = ANFIS\ output\left(F_{query}, F_{template}\right) \quad (15)$$

Results and Discussion

This section describes the end result of the proposed method. Across a range of parameters, the simulation results demonstrated that the proposed strategy outperformed the present methods. By constructing Anaconda in Python, we are able to mimic the proposed method. For this experiment, you'll need a PC with 8 GB of RAM and an Intel Core i5 processor. The IITD and CASIA version 4.0 datasets are two famous state-of-the-art examples used in this investigation. We used the above terms to figure out if the suggested method would work by looking at things like accuracy, the true negative rate (TNR), the equal error rate (EER), the false acceptance rate (FAR), the true positive rate (TPR) [17–19], and the false rejection rate (FRR).

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

No. of Iris Samples	FAR (%)	FRR (%)	TPR (%)	TNR (%)	EER (%)
100	0.10	0.10	100	100	1.18
500	0.22	0.16	100	100	1.28
1000	0.36	0.22	99.13	99.12	1.32
1500	0.42	0.33	98.12	98.13	1.41
2000	0.45	0.38	98.08	98.02	1.47

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 0.45% for FAR and 0.38% for FRR. An EER of at least 1.18. Figure 2 shows the graphical depiction of the FAR and FRR from the CASIA dataset.

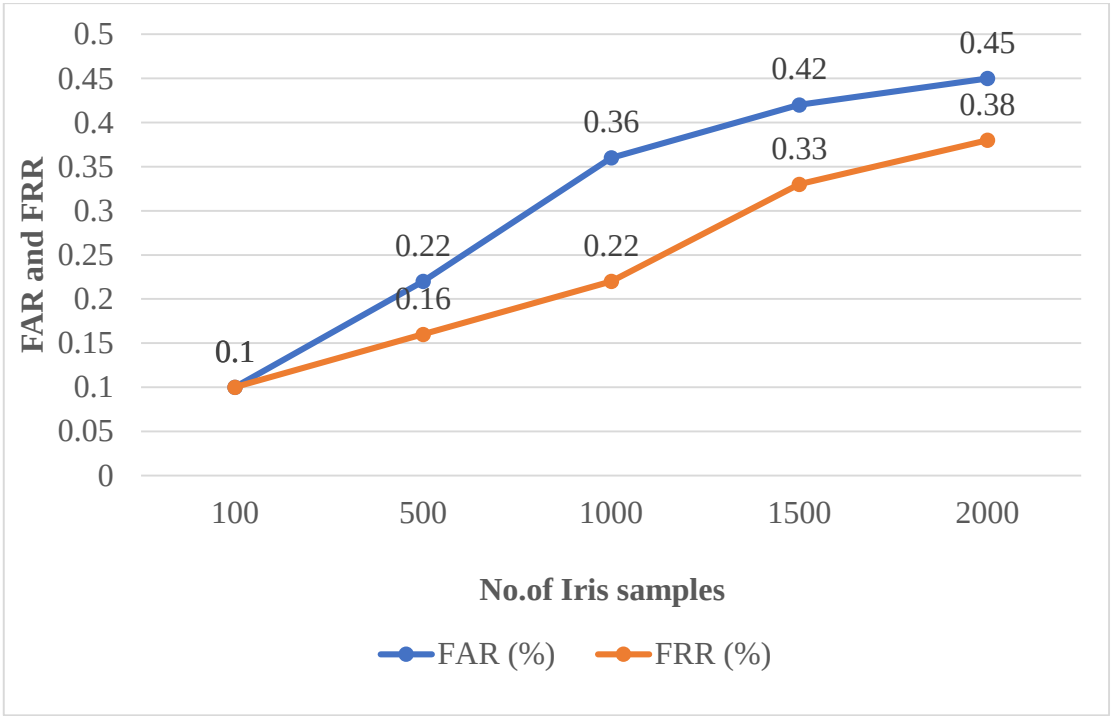

Figure 2: Plot of FAR and FRR for CASIA iris dataset

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	1.08
500	0	0	100	100	1.19
1000	0.22	0.20	99.22	99.18	1.28
1500	0.32	0.28	98.33	98.21	1.32
2000	0.42	0.36	98.22	98.12	1.36

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 0.42% and 0.36%, respectively. For 100 iris samples, the minimal EER is around 1.08. Figure 3 shows the graphical depiction of the FAR and FRR from the CASIA dataset.

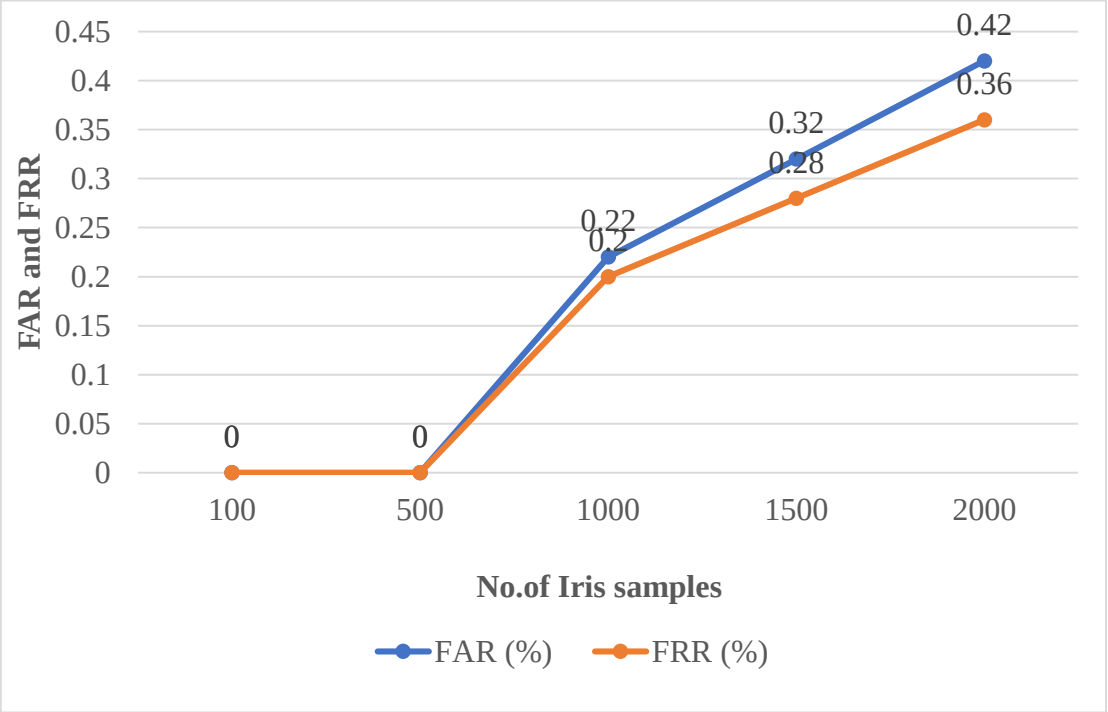

Figure 3: Plot of FAR and FRR for IITD iris dataset.

Comparison of Accuracy and Recognition rate of Proposed Method with Existing Methods.

Table 3 shows the EER, and accuracy of proposed method on both CASIA Iris and IITD iris datasets. The recognition time of proposed method is specified in seconds. The comparison denotes that methodology with fuzzy logic has less error rate and more optimal. The performance metric of the proposed scheme is compared with the state-of-art existing scheme in view of accuracy and maximum TAR as shown in Table 4.

Table 3: Performance parameters of proposed method on both iris datasets.

Method	Dataset	EER	Accuracy	Recognition time (sec)
Proposed method without NFS	CASIA Iris	3.2%	99	2.9
	IITD iris	3.2%	99	2.9
	CASIA Iris	2.2%	99.12	2.6

Proposed method with NFS	IITD iris	2.2%	99.14	2.6

Table 4 Comparison of accuracy of cancelable with existing schemes

Methods	**Dataset used**	**Algorithm used**	**Accuracy (%)**
Deepanshu kumar et al. [20]	MMU	DWT+DCT	80
Mohamed Abdolahi et al. [21]	CASIA	Fuzzy logic	97.5
Fernando et al. [22]	CASIA V3	2D Gabor	99
Mohamed Hamaz Abed [23]	CHUK iris	DWT and cosine	98
Proposed method without NFS	CASIA and IITD iris	Log-Gabor + HECC	99
Proposed method without NFS	CASIA and IITD Iris	Log-Gabor + HECC+NFS	99.13

We detail the performance of the suggested method by comparing it with the most advanced cancelable biometric systems. The results show that the proposed method is having highest accuracy of 99.13% The suggested strategy demonstrates an improved accuracy of 99.13% while maintaining a recognition rate of 2 sec. The suggested system's increased performance with reduced execution time enhances its computational efficiency.

Conclusion

This study presents a novel method for creating deleteable biometric templates. It combines the best parts of neurofuzzy systems, log-gabor filters, and Hyperelliptic curve cryptography (HECC). When used for feature extraction, Log-Gabor filters provide strong phase information, which in turn makes iris templates stand out more. HECC encrypts the biometric data, ensuring robust security and protection against attacks while maintaining computational performance. By addressing uncertainty and optimizing decision-making, a neurofuzzy system enhances classification performance even more. While keeping template revocability and security in mind, the experimental findings demonstrate that the suggested system attains remarkable accuracy with minimal false acceptance and rejection rates. The results demonstrate that the suggested approach provides superior results when considering a maximum TPR and TNR of 100%. With an improved accuracy of 99.13%, the suggested method yields an ideal EER of 0.36%. This combination of techniques has enormous potential for the development of future secure biometric systems; it solves important privacy and security concerns by securing sensitive biometric data while still allowing for reissue in the event of a breach.

References

[1] Daugman, J. (2004). How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21-30. https://doi.org/10.1109/TCSVT.2003.818350.

[2] Zhou, Z., Du, Y., & Pan, Y. (2012). A robust iris recognition system based on structure adaptive hybrid features. Neurocomputing, 99, 333-340. https://doi.org/10.1016/j.neucom.2012.07.019

[3] Masek, L., & Kovesi, P. (2003). MATLAB source code for a biometric identification system based on iris patterns. School of Computer Science and Software Engineering, The University of Western Australia.

[4] Duquesne, S., & Ezerman, M. F. (2015). On the security of cryptosystems based on hyperelliptic curves. Journal of Cryptographic Engineering, 5(4), 241-255. https://doi.org/10.1007/s13389-014-0091-4

[5] Scott, M., Costello, C., & Kachisa, E. (2009). Efficient algorithms for pairing-based cryptosystems. Cryptography and Coding, 231-244. https://doi.org/10.1007/978-3-642-10433-6_18

[6] Kumar, R., Verma, H., & Rajesh, M. (2014). A study on elliptic curve cryptography and its applications. International Journal of Computer Applications, 94(4), 25-29.

[7] 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.2009.08.006

[8] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011, 3. https://doi.org/10.1186/1687-417X-2011-3.

[9] Koblitz, N. (1989). Hyperelliptic cryptosystems. Journal of Cryptology, 1(3), 139-150. https://doi.org/10.1007/BF00669333

[10] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2007). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614-634. https://doi.org/10.1147/sj.403.0614

[11] Rajasekar, Vani & Premalatha, J. & Sathya, K. (2020). Enhanced Biometric Recognition for Secure Authentication Using Iris Preprocessing and Hyperelliptic Curve Cryptography. Wireless Communications and Mobile Computing. 2020. 1-15. 10.1155/2020/8841021.

[12] 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.

[13] Salama, Gerges & el-Gazar, Safaa & Nassar, Rana & El-Shafai, Walid & Khalaf, Ashraf A. M. & El Banby, Ghada & Hamed, Hesham & Abd El-Samie, Fathi. (2022). Efficient multimodal cancelable biometric system based on steganography and cryptography. Iran Journal of Computer Science. 6. 10.1007/s42044-022-00115-8.

[14] Sarkar, Arpita & Singh, Binod. (2021). A multi-instance cancelable fingerprint biometric based secure session key agreement protocol employing elliptic curve cryptography and a double hash function. Multimedia Tools and Applications. 80. 1-31. 10.1007/s11042-020-09375-7.

[15] Eltaieb, Rania & El Banby, Ghada & El-Shafai, Walid & Abd El-Samie, Fathi & Abbas, Alaa. (2023). Efficient implementation of cancelable face recognition based on elliptic curve cryptography. Optical and Quantum Electronics. 55. 10.1007/s11082-023-04641-y.

[16] Ayoup, Ahmed & Khalaf, Ashraf A. M. & Raddady, Al & Abd El-Samie, Fathi & El-Shafai, Walid & Eldin, Salwa. (2022). Cancelable Multi-Biometric Template Generation Based on Dual-Tree Complex Wavelet Transform. Intelligent Automation and Soft Computing. 33. 1289-1304. 10.32604/iasc.2022.024381.

[17] Soliman, R.F.; Ramadan, N.; Amin, M.; Ahmed, H.H.; El-Khamy, S.; Abd El-Samie, F.E. Efficient cancelable Iris recognition scheme based on modified logistic map. Proc. Natl. Acad. Sci. India Sect. A Phys. Sci. 2020, 90, 101–107.

[18] Drozdowski, P.; Garg, S.; Rathgeb, C.; Gomez-Barrcro, M.; Chang, D.; Busch, C. Privacy-preserving indexing of Iris-codes with cancelable Bloom filter-based search structures. In

Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 2360–2364.

[19] Bendib, I.; Meraoumia, A.; Haouam, M.Y.; Laimeche, L. A New Cancelable Deep Biometric Feature Using Chaotic Maps. Pattern Recognit. Image Anal. 2022, 32, 109–128.

[20] D. Kumar, M. Sastry, and K. Manikantan, "Iris recognition using contrast enhancement and spectrum-based feature extraction," in 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), pp. 1–7, Pudukkottai, India, 2016.

[21] A. Mohamed, M. Majid, and J. Mehdi, "Multimodal biometric system fusion using fingerprint, iris with fuzzy logic," International Journal of Soft Computing and Engineering, vol. 2, no. 6, 2013.

[22] B. Fernando, M. Glasston, L. Eduardo, H. C. Paulo, and A. Gaurda, "Exploring the scalability of multiple signatures in iris recognition using GA on the acceptance of frontier earch," in 2017 IEEE Congress on Evolutionary Computation (CEC), pp. 1843–1847, San Sebastian, Spain, 2017.

[23] M. H. Abed, "Iris recognition model based on principal component analysis and two levels Haar wavelet transform," Case study CUHK and UTIRIS databases, pp. 485–500, Journal of college of education, 2017.