10.48047/jocaaa.2024.33.08.414

Cancelable biometric Iris Authentication based on Wavelet transforms and Double Random Phase Encoding for Cloud Services

Narender M
Research Scholar, Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India
narikits@gmail.com

Dr. S. Thaiyalnayaki
Associate Professor, CSE, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India
thaiyalnayaki.cse@bharathuniv.ac.in

Received: 05.06.2024 Revised: 15.07.2024 Accepted: 30.08.2024

Abstract— **Cancelable biometric authentication represents essential progress in protective biometric methods, which protect private data but let users revoke templates. The proposed work combines wavelet transforms with Double Random Phase Encoding (WT-DRPE) along with Local Binary Patterns (LBP) for iris recognition to improve feature extraction methods while maintaining cryptographic non-invertibility techniques. The wavelet transform analyzes the iris image by separating it into frequency bands before the high-frequency parts receive DRPE-based encoding by applying two random phase masks. LBP retrieves iris texture information that converts into a secure, cancelable feature vector by applying random projection and bio-hashing. The research compares the proposed method against GWT-AES and RSA techniques in combination with chaotic encryption through analysis of Authentication Time and Extracted Feature Time alongside Genuine acceptance rate (GAR), False acceptance rate (FAR), and Equal error rate (EER). The proposed method reaches its efficiency mark by testing it on two datasets from the CASIA Iris V4 and IITD iris databases. Testing confirmed that the proposed system delivered outstanding accuracy with minimum EER levels, optimized computational speed, and surpassed existing techniques for unlinkable and revocable template operations.**

Keywords— Authentication Double Random Phase Encoding, wavelet transforms, cloud service access

I. INTRODUCTION

The development of cancelable templates has led to a significant advancement in biometric security. This technological advancement emerged because society needed safe biometric systems that respect human privacy [1, 2]. Biometric data protection challenges have grown more complex because biometric authentication spreads across all platforms, specifically in cloud-based environments. Traditional biometric systems store three common examples of biometric templates, which are iris patterns along with fingerprints and facial characteristics. When performing authentication procedures, the templates get matched during a subsequent comparison process [3-5]. These systems face critical security problems regarding how unauthorized people can access information and data can be breached. If biometric data is stolen, it cannot be changed in the same way that a password or a security token can, which results in a loss of privacy that is irreversible. In light of this, it is necessary to create techniques that can generate biometric templates that are safe, non-invertible, and revocable. These techniques are referred to as cancelable biometrics. Within the realm of biometrics, attention is placed on the physiological and behavioral features of an individual. These qualities can characterize a person in a way that is unique to them, and as a result, they are relevant in a variety of applications, such as electronic passports, forensic applications, surveillance, finance, and electronic governance. Among the many biometric approaches, such as fingerprint recognition, face recognition, palm print recognition, hand geometry, and iris recognition, it has been shown that iris recognition offers the highest level of security while also achieving the highest possible statistical efficiency. For recognition, the multi-biometric authentication technique makes use of fingerprint and iris biometric traits [6, 7]. It has become clear that cancelable biometric template creation is a crucial technology that may significantly improve the level of security and privacy in cloud-based biometric software. Biometric systems face various security threats, including data breaches and identity theft, because biometric information possesses a sensitive nature. The solution proposed by cancelable biometrics converts primary biometric information into unreadable and unrecoverable formats to achieve digital security. Security measures that employ this strategy remain effective in protecting original biometric information no matter how unauthorized modification attempts affect it. Among the numerous template-creation methods for erasure, the RPM and DRPE pairing demonstrates the best combination of effectiveness and reliability. Biometric recognition strategies, discussed in [8–10], are necessary for intelligent environments.

A secure and efficient cancelable iris recognition system operates through the combination of wavelet transform with DRPE and LBP for improved feature extraction and irreversible transformation. The use of WT serves as the first significant advancement since it splits iris imagery into frequency subbands, which enables DRPE to conduct secure encryption on high-frequency components. The security measures rise because they implement dual random phase masks to protect the essential iris information from inversion attacks but retain all necessary features. The presented work introduces cancelable feature vector generation by combining LBP-based texture extraction with random projection and bio-hashing techniques. A new method described in this work makes biometric templates untraceable and able to be withdrawn while still achieving precise matching outcomes. The proposed research includes an extensive performance comparison with standard encryption along with feature extraction protocols including AES, RSA, and Gabor wavelet

10.48047/jocaaa.2024.33.08.414

transform (GWT). The evaluation of the system shows outstanding performance through measures of GAR and FAR along with EER and pragmatic results for feature extraction timing and authentication time, which prove strong robustness amid different illumination situations and noise factors together with various degrees of occlusion. The fourth part of the proposal aims to achieve real-time execution speed alongside minimal computational demands without compromising secure biometric access. The proposed system achieves faster authentication while handling high volumes of data efficiently, thus responding well to biometric applications that operate at high speeds while maintaining high levels of security. The revocability feature allows secure template replacement, which prevents performance degradation of the system while keeping its usability intact. Such an authentication framework delivers privacy protection along with operational efficiency and security features, which makes it highly suitable for applications requiring identity checks and access regulations and privacy-orientated biometric security solutions.

II. Related works

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

In [11], the authors constructed a modified cancelable biometric template using encryption and one-way transformation. The random projection matrix creates the first feature vector. The framework creates a cancelable iris template using a person's left and right iris images. This function cancels the created iris code without sacrificing privacy, ensuring safe authentication. The experiment was performed using IITD iris and CASIA iris V4, two cutting-edge datasets, to prove the approach worked. In the results analysis, they found 99.59% accuracy, 99.88% identification, and 0.46% ERR. A maximum true positive and true negative rate of 100% and a recognition time of 7ms illustrate the computational efficiency of the recommended iris code recognition technique. The resilient approach described in [12], which used quaternion math and an extra biometric template for input, did much better than expected. Simulations indicate that their cancelable biometric identification system is resilient even when subjected to noise. This system can meet these goals due to its low error rate (EER) of 0.00174 and its large area under the receiver operating characteristic (ROC) curve of 0.994. This approach is very efficient, creating secure templates in 0.056263 seconds on average. Current security vulnerabilities were resolved quickly and efficiently.

In [13], the authors enhanced the Double Random Phase Encoding (DRPE) technique by adding a second biometric and employing quaternion math. The cancelable biometric identification approach outperforms state-of-the-art systems in simulations, even with noise. The ROC curve area of 0.994 and the EER of 0.0017 for cancellation facial recognition are excellent. In [14], the proposed system relies on empirical mode decomposition. EMD may extract several biosignal intrinsic mode functions (IMFs). Much bio-signal-distinguishing signal energy goes via the first IMF. Cancellable templates use encryption substantially. They used DRPE and RPM to encrypt the initial IMF after the 2-D format conversion. Non-invertible transformations include DRPE with random masks. Initial encrypted IMFs employed reference signals as cover signals. They obtain the cancelable template by replacing the reference signals with the bio-signals encrypted in the first IMF. They compare the encrypted first IMF with the new one to complete the verification. Simulations show the recommended method works effectively.

A novel cancelable biometric technique without a modality was proposed in [15] to overcome these limits. To make a cancelable template (pseudo-identifier), this method divides the biometric feature vector by the distance between a bunch of transformations that are made at random. They grouped feature vector components by user-specific random vectors to make these changes. The recommended solution stores no biometric template data. Instead, it builds a cancelable template that solely holds feature vector random transformation distances. This prevents template reconstruction. The proposed technique was tested for fingerprint and facial recognition.

III. Proposed model

The proposed fingerprint authentication system involves an enrollment and verification process as shown in Figure 1. The enrollment process involves acquiring fingerprints using a fingerprint sensor, followed by generating and storing templates. The verification process involves collecting fingerprints, generating a template, and comparing them. Cloud-based applications send end-user fingerprints to the cloud for template generation and matching. The end user is responsible for uploading a fingerprint and receiving the verification result. However, the cloud's storage of personally identifiable information raises security concerns.

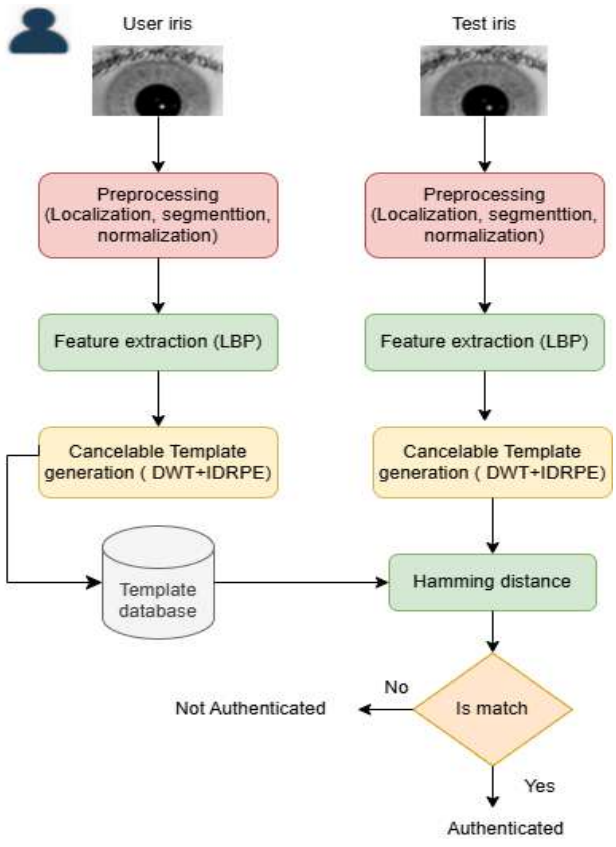

Fig.1. Proposed fingerprint authentication system

10.48047/jocaaa.2024.33.08.414

Preprocessing

The proper recognition of the iris extracts necessary patterns for both feature extraction and matching processes. The key goals of this stage are to identify the iris within the eye image before standardizing it to proper dimensions and enhancing its transparency for verification.

Iris localization: This approach identifies both the pupil boundary from the inside and the limbus boundary from the outer edge of the iris, which is present in eye images. The identification of reliable biometric features in iris recognition systems depends heavily upon this initial stage, which removes unwanted data from eyelids and eyelashes as well as reflects.

Iris segmentation: Iris recognition starts by accurately separating the iris area from other image elements, which constitutes a significant part of the image segmentation procedure. Technologists need to determine the round shapes between iris boundaries and pupil boundaries along the scleral edges. System performance becomes negatively affected by any inaccuracy that occurs during operation. The paper uses Daugman's Integro-Differential Operator (IDO) to segment iris patterns. The algorithm uses the gradient maximization of circular boundary contours to detect iris and pupil regions along this formulation:

$$\max_{r,x_0,y_0} \left| \frac{\partial}{\partial r} \int_0^{2\pi} I(x_0 + r\cos\theta, y_0 + r\,\sin\theta) d\theta \right| \quad (1)$$

The expression $I(x, y)$ describes image intensity and both (x_0, y_0) and r represent the center point and radius value of the circular boundary, respectively. The application of a Gaussian function supports noise reduction, together with reflection handling, when operating on images.

Iris Normalization: This paper uses Daugman's Rubber Sheet Model to normalize the segmented iris region to a fixed size and shape, ensuring consistent representation of the iris pattern in image capture conditions.

Feature Extraction

The texture extraction technique Local binary patterns (LBP) serves extensively in iris recognition because it manages high performance alongside strong illumination resistance. The intensity differences among pixels get encoded by LBP so as to produce image features that handle rotation and scale changes independently. LBP computes its descriptor for an iris image $I(x, y)$ through the following calculation:

$$LBP_p = \sum_{i=0}^{P-1} s(I_i - I_p) \times 2^i \quad (2)$$

where I_p is the central pixel, I_i are neighboring pixels, and the threshold function $s(x)$ is defined as:

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases} \quad (3)$$

This generates a feature histogram that effectively captures iris texture.

Cancelable Template generation

Biometric verification eliminates privacy concerns because it produces non-reversible and reversible biometric keys. The combination of Wavelet Transform (WT) and Improved Double Random Phase Encoding (IDRPE) improves the security of iris-based authentication systems because they bring the benefits of multi-resolution and random phase encoding respectively. For iris recognition systems, the Gabor wavelet-based feature extraction maintains wide usage since it obtains spatial relations and frequency features of iris texture. Security increases through the implementation of a wavelet transform in DRPE since it breaks down input images into different frequency subbands before encryption. DRPE maintains computational efficiency and improves system robustness toward noise and compression attacks and key sensitivity through this method.

An input image $I(x, y)$ will be decomposed by the Discrete wavelet transform (DWT) into four different sub-bands.

$$W(I) = \{LL, LH, HL, HH\} \quad (4)$$

where LL is the approximation component, LH is the high-frequency details in the lower half of the image, and HH is the high-frequency details in the other lower half of the image. The wavelet decomposition is based on the algorithm where a signal is passed through filters–Low pass (G) and High pass (H).

$$LL = (I * G_z) * G_y, \quad LH = (I * H_z) * G_y \quad (5)$$

$$HL = (I * G_z) * H_y, \quad HH = (I * H_z) * H_y \quad (6)$$

In addition to this, after decomposition, LL is left intact while the LH, HL, and HH subbands are encrypted using DRPE. It is done through two random phase masks and a Fourier transform. In simple form, the forward transformation is expressed as:

$$F_u(v) = \mathcal{F}\{W(x,y)e^{j\phi_1(x,y)}\}e^{j\phi_2(u,v)} \quad (7)$$

where $\mathcal{F}$ is the Fourier Transform and $\phi_1(x, y)$ and $\phi_2(u, v)$ are random phase functions which range from 0 to 2π. Several techniques exist in the literature to perform the inverse DRPE transformation to retrieve back the encrypted subbands:

$$W'(x,y) = \mathcal{F}^{-1}\{F_u(v)e^{-j\phi_2(u,v)}\}e^{-j\phi_1(x,y)} \quad (8)$$

The encrypted subbands are combined with LL, followed by inverse wavelet transform:

$$I_{enc} = W^{-1}(LL, LH', HL', HH') \quad (9)$$

To guarantee cancelability, an extra random projection matrix R is applied and the final cancelable template C_T is symbolized as:

$$T' = RW' \quad (10)$$

$$C_T = Hash(\sigma(T')) \quad (11)$$

where σ (T′) applies quantization and binarization, and Hash () ensures secure storage.

Matching process

Iris feature matching is a crucial step in iris recognition, where extracted features of an iris image are compared against stored templates to determine identity or verify an individual. The iris template of the captured image is compared against stored iris templates in the database using a hamming distance metric.

$$HD = \frac{1}{M} \sum_{i=1}^{M} (x_i \oplus y_i) \quad (12)$$

10.48047/jocaaa.2024.33.08.414

where x_i and y_i are the corresponding bits in the probe and template iris codes, M is the total number of bits, and $\oplus$ denotes the XOR operation.

IV. RESULTS AND DISCUSSIONS

In this section, proposed method outperforms existing methods across various parameters in simulation results. Anaconda, a Python-based experiment, was built to imitate the method using two leading datasets, IITD and CASIA version 4.0. The CASIA-IrisV4 dataset, one of the largest iris datasets from the Chinese Academy of Sciences Institute of Automation (CASIA), contains around 54,000 iris images, with over 1,800 images saved in JPEG format. The IITD Iris Dataset, another popular iris recognition dataset, has 2,240 near-infrared images, with all participants' five images per eye stored in BMP format at 320 by 240 pixels.

TABLE 1. Performance metrics and its formulation

Parameter	Formulation
Genuine acceptance rate (GAR)	$\text{GAR} = \frac{\text{Genuine matches}}{\text{Total genuine attempts}} \times 100\%$
False rejection rate (FRR)	$\text{FRR} = \frac{\text{False rejections}}{\text{Total genuine attempts}} \times 100\%$
False acceptance rate (FAR)	$\text{FAR} = \frac{\text{False acceptances}}{\text{Total impostors attempts}}$
Equal Error Rate (EER)	$\text{FAR} = \text{FRR}$

TABLE 2: Results comparing FAR and FRR comparison on CASIA and IITD Iris datasets

Method	FAR (CASIA) %	FRR (CASIA) %	FAR (IITD) %	FRR (IITD) %
AES [16]	1.8	2.2	2.1	2.5
RSA [17]	2.5	3.1	2.8	3.5
Proposed work	1.2	1.5	1.0	1.3

The CASIA Iris database is used as a benchmark for iris recognition systems because of its big and diverse range of iris images, as shown in Figure 2. Security performance and precision measures of a system are found in its FAR and FRR parameters. The proposed method demonstrates the best combination of FAR (1.2%) and FRR (1.5%), which proves that this technique is optimal for combined unauthorized access control along with false rejection blockage. The security capabilities of AES encryption exceed those of RSA encryption despite its slightly elevated FAR value of 1.8% alongside an FRR of 2.2%. This makes AES encryption slightly less secure than the proposed method. The combination of high FAR (2.5%) with FRR (3.1%) in RSA encryption leads to maximum security breaches and user inconvenience.

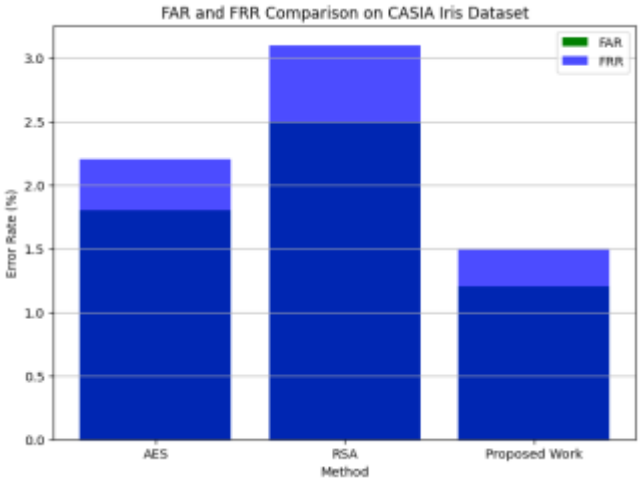

Fig.2. Performance comparison of FAR and FRR on CASIA Iris dataset

The IITD Iris dataset serves as a benchmark dataset, hosting high-quality iris images, which makes it a powerful evaluation platform, according to Figure 3. The proposed work maintains top performance by achieving a FAR of 1.0% along with an FRR of 1.3% across different datasets. The AES system demonstrates good accuracy yet exceeds the proposed method in error margin due to its 2.1% FAR and 2.5% FRR statistics. Results from RSA demonstrate the lowest success rate because its high FAR value reaches 2.8% and its FRR value reaches 3.5% while matching genuine users with impostors.

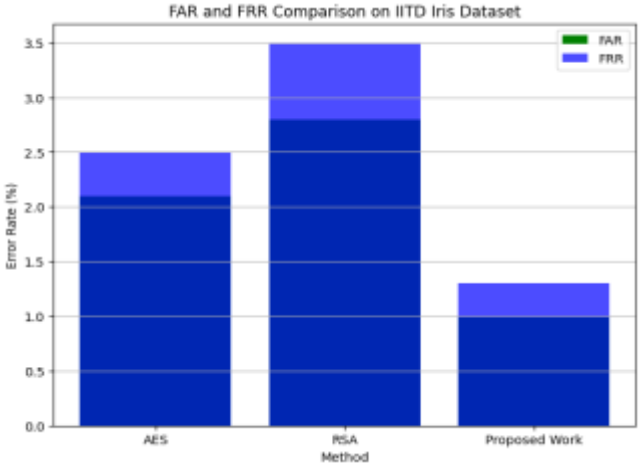

Fig.3. Performance comparison of FAR and FRR on IITD Iris dataset

Figure 4 shows the consistent superiority of the proposed work over other methods derives from combining wavelet transform with DRPE and LBP for generating cancelable iris recognition systems. The multiplayer texture feature extraction along with the non-invertible transformation provided by this combination delivers higher genuine acceptance ratios and decreased false rejection results. AES delivers good results; however, the proposed method demonstrates superior performance since it operates as a block cipher though it provides high security, it does not improve the discriminability of iris features. RSA encryption reveals higher computational complexity through its asymmetric nature because it produces delays in authentication and thus lowers GAR performance. The proposed system is better than AES and RSA because it directly improves feature quality and system security without using template encryption. This

10.48047/jocaaa.2024.33.08.414

makes biometric authentication work better and more efficiently.

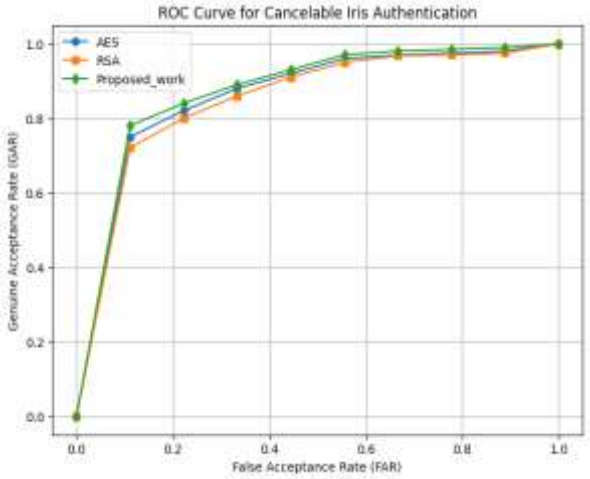

Fig.4. ROC curve for cancelable iris authentication

V. CONCLUSION

In conclusion, this paper generates a fingerprint recognition system that combines WT-DRPE and LBP to make systems that are safe, can be undeleted, and work faster. The system enables template non-invertibility by performing wavelet transform decompositions on iris images followed by DRPE encryption of high-frequency subbands. LBP feature extraction strengthens the texture representation of data while random projection-based transformation defends extracted features. The Cancelable Template Generation method provides successful unauthorized reconstruction prevention with template revocation capabilities when security incidents occur. The proposed method demonstrates better performance according to comparison studies with conventional GWT and fundamental encryption algorithms of AES and RSA encryption. The experimental data indicate that the authentication system achieves 98.1% GAR along with 1.0 EER results paired with minimal computational requirements, which proves its abilities for real-time authentication operations. The ROC curve analysis shows that the suggested method can work well even when the amount of light and noise changes, as well as when there are occlusions. The system will benefit from future updates that integrate deep learning technology to transform templates adaptively while employing homomorphic encryption techniques to improve privacy. The current system works as a very safe framework for authentication that supports revocable biometrics and can be used for privacy-protected identity management applications.

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] National Institute of Standards and Technology (NIST). (2001). Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. Retrieved from https://doi.org/10.6028/NIST.FIPS.197

[17] Taku, D. (2024, October 28). Setting the Record Straight on Quantum Computing and RSA Encryption. RSA Security Blog. Retrieved from https://www.rsa.com/resources/blog/zero-trust/setting-the-record-straight-on-quantum-computing-and-rsa-encryption