

<sup>1</sup> R. Vasuki<sup>2</sup> Dr. K. Ranjith Singh

## Enhanced Image Encryption Scheme for Securing Iris Template using a Novel Hybrid Fractional Fourier DRPE



**Abstract:** - Security becomes more and more necessary as a result of the significant advancements in computers and communications as well as the widespread use of electronic media, particularly in organizations where information is increasingly vital. Earlier methods, like traditional cryptography, employ encryption keys, which are lengthy bit strings that are extremely difficult to memorize. Additionally, it is easily attackable utilizing the brute force attack method. Since biometric traits are always changing and ever-living, biometrics—such as voice, fingerprints, and iris—provide a unique means of identifying an individual and a safe stream cipher in place of more conventional cryptographic approaches. Information security is becoming more and more necessary as information technology advances. The biometric-based encryption technology has advanced quickly to meet demands for increased convenience and security. Among them, iris technology has grown in importance as a subject of study for information security researchers because of the constancy of iris traits and their difficulty being copied. In this paper, the iris portion is extracted from the eye and a novel encryption technique which is a hybrid combination optical cryptography and Fast Fourier transformation is presented. The Idea behind the technique is to extract the iris by means of novel encryption technique. After encryption process, the decryption is performed. The common iris database MMU and IITD is used to conduct the simulation experiment. The results demonstrate that the technique may significantly increase the security of the encryption and decryption process as well as the consistency of iris encryption.

**Keywords:** DPRE-Double phase Random Encoding, FRFT – Fractional Fourier Transform, IFRFT –Inverse FRFT, EFRFT- Encrypted FRFT, DFRFT –Decrypted FRFT.

### I. INTRODUCTION

Information technology is advancing quickly, and so there is the demand for information security transmission and biometric-related technologies. The information characteristics created by human tissue structure, such as the iris, face, fingerprint, voice, DNA, and palm positions, are referred to as human biometrics. The research and development community focused on biometrics-based identification and verification has recently been interested in the human iris. No two irises in the whole human population are same, not even in identical twins or even in the left and right eyes of the same individual. This is because each iris is so unique. Due to their uniqueness, the biological traits of the human body are frequently exploited in identity identification and other domains. The features of the iris are extracted through the application of iris recognition technology. The iris possesses superior qualities in comparison to other human biological traits. For picture encryption, it is more appropriate to enhance the algorithm's security and resilience against attacks. Identity identification technology that utilizes iris feature extraction is receiving more attention from both academic and corporate sectors. It has a broad range of applications and is progressively used in several areas that demand high security, such financial systems and secret operations, among others. Feature extraction is used to filter the target information from the picture so that information processing may be done based on the demands of the user.

There are more security requirements for image encryption. When removing features from deep learning algorithms and using them for picture encryption, iris features work better. It works better to increase encryption security than other biometrics. Traditional iris image encryption technology, which extracts features from iris images using a machine learning algorithm, has certain drawbacks, including difficulty with feature learning and low efficiency. Other issues include high iris image quality, difficulty with image preprocessing, and the requirement to repeat iris image acquisition during the decryption process in order to perform a successful decryption operation.

In this work, a novel iris image encryption algorithm based on is developed, building upon the original approach. Training the sample allows for the realization of the image encryption function. The suggested approach is able to resolve the inconsistency of iris characteristics and enhance the secrecy of the encryption and decryption process, according to simulated studies conducted on iris samples from the public iris database.

<sup>1</sup> Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore

<sup>2</sup> Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore

The following are the details that are discussed and literature survey are discussed in section 2. In section 3 the proposed methodology are discussed. In section 4 Experimental results are discussed. Finally, Section 5 deals with conclusion.

## II. RELATED WORK

Deep learning is used as the feature classification technique and the iris feature is used as the research object to study [1] the iris feature encryption technology. The shared iris database is used to conduct the simulation experiment. The outcomes demonstrate that the technique may significantly increase the security of the encryption and decryption process as well as the consistency of iris encryption. Combining chaotic encryption [2] with iris recognition will result in a more practical and secure iris recognition system. The multi-scale 2D Gabor filter is used in the iris recognition procedure to obtain the iris texture identification code in a single direction alone. The one-way coupled map lattice (OCML) chaotic system is used to produce a pseudo-random number key stream in order to safeguard the identity code during transit. The iris identify code is then encrypted and decrypted using the ciphertext feedback technique. Finally, the iris classification process is done with the Hamming distance. The technology offers a high encryption speed and recognition accuracy, according to experimental data.

A multibiometric pictures encryption approach based on Fast Fourier Transform (FFT) and hyperchaotic system is presented [3] to address the issues of low image reconstruction quality and inadequate security in the encryption and transmission of multibiometric images. The multibiometric pictures are first converted from the spatial to the frequency domain using the FFT. Next, the hyperchaotic Lorenz system's starting values are produced. Using the inverse fast Fourier transform, the transform domain is rebuilt in the second phase to produce numerous RGB three-channel colour pictures. Next, we execute confusion and diffusion on each colour channel by combining the two diffusion methods: Galois domain diffusion and additive mode diffusion. Lastly, several colour pictures are created by encrypting the various grayscale images.

This study [4] proposes a revolutionary multimedia encryption method inspired by biometrics. Dual parameter fractional Fourier transform (DP-FrFT), a novel approach to the definition of fractional Fourier transform, is suggested and applied in multimedia encryption for this reason. The fundamental idea of the suggested encryption method is to generate the keys needed for the encryption process after obtaining a bitstream that has been biometrically encoded. This study suggests an effective way to create a bitstream that is biometrically encoded using biometrics and then use that bitstream to create keys. Next, Hessenberg decomposition and nonlinear chaotic map are used to encrypt multimedia data in the DP-FrFT domain. In conclusion, a dependable decryption method is suggested to create original multimedia content from the encrypted material.

In this research [5], we provide an Iterative Fast Fourier Transform (IFFT) based fingerprint image improvement technique. For fingerprint recognition systems to function more efficiently, iterative picture reconstruction methods are crucial. The design of the reconstruction algorithms is crucial to enhancing performance given the rapid rise in fingerprint data volumes. In iterative reconstruction, Fourier-based frequency orientation techniques have the potential to significantly cut down on calculation time. This paper [6] proposes an approach to key generation based on iris biometrics. The iris structure is extracted from the iris images using an edge-preserving filter and an ensemble gradient minimization technique in the first step of the suggested method. Second, the consistent region is chosen using a novel statistical technique once the iris texture data has been normalized. Thirdly, the ensemble local space-filling curve descriptors and their variations are used to create feature vectors. Fourth, neighborhood component analysis and hybrid feature selection are used to create a discriminant feature vector. The discriminant feature vector is then utilized to create a key using an interval-based encoding approach. Our primary contribution is the presentation of a unique authentication system that utilizes an evolutionary encryption technique based on Genetic Algorithms (GAs) in [7]. The first is that rather than starting with a single template, the GA starts its search from a population of templates. Second, the generated first population is exploited by a few statistical operators to produce subsequent populations. Lastly, the ultimate cancelable biometric templates are created by performing the crossover and mutation processes.

This work [8] proposes a new approach for biometric templates using a 2D fractional discrete cosine transform (FrDCT) and a 6D chaotic environment. The  $k$  biometric templates are represented into three groups in this technique. After representation, these three groups are turned into row vectors and scrambled by employing keys generated by the 6D-chaotic system and after that, these row vectors are merged into three matrices. The three

matrices are then split in half horizontally, representing the real and imaginary parts of a complex-valued matrix (CVM) respectively on the left and right halves. Additionally, 2D FrDCT is applied to this CVM. The 2D FrDCT output is divided into three sections. The substitution operation with keys generated by the 6D-chaotic system significantly increases the technique's robustness. The encrypted template in its final form is thus obtained. It is suggested to use a new asymmetric cryptosystem built on the QZ modulation [9]. For the first time, we introduce the QZ technique to modify both the random phase mask and the plain picture. We use the RPM and the input picture as two inputs to the QZ algorithm in our cryptosystem. Two aspects of this work [10] are innovative: first, a new idea of optical image encryption is proposed by integrating the high-dimensional chaotic digital image encryption method into the 4f optical image encryption system; second, a distinct encryption paradigm of real and imaginary images in the frequency domain is proposed, which significantly increases the security of image encryption and transmission. This work [11] presents a unique approach for picture encryption using fractional Fourier transformation and chaotic map. To conduct the FRFT transformation, we first split the picture into blocks and choose the blocks with the highest correlation. Second, the pixel values will be altered using the simple image key. Lastly, the entire image is jumbled using the Baker Map. Fractional Fourier transform (FrFT) and discrete orthogonal Stockwell transform (DOST) [12] are used to build this technique. The right sequence and keys have been used to produce the encrypted picture. Plotting the encrypted histogram and scatter of many photos was done. Next, determine the entropy, encryption time, encryption picture, and original correlation coefficient.

### III. METHODOLOGY

There are two more types of encryption: partial encryption and full encryption. A piece of a picture is encrypted while the remainder of the image is left unaltered in partial encryption [13]. The entire encrypted image is presented in an asymmetric format [14]. Symmetric or asymmetric keys are employed in the studies [15] to lock the simple image. Symmetric encryption is used when both encryption and decryption use the same key. Asymmetric encryption uses a pair of public and private keys in place of a single key. The use of fractional transforms is highlighted in this study as an alternative to the various known picture encryption approaches. For Image encryption this paper highlights the use of Fractional transforms. The key used during the encryption procedure determines the image's level of protection. Researchers utilize mathematical keys in the majority of situations, but they are easily traceable. Hence, biometrics might be employed in the encryption process as a backup key. Biometric keys are preferred over mathematical keys because two distinct individuals cannot share the same traits and remain untraceable. Biometrics [16] such as iris, face, fingerprint, handwritten signature, palm print, voice, DNA, ECG, and others can be utilized as keys in the encryption process. The proposed approach uses fractional transforms in conjunction with a scrambling procedure to produce image encryption.

#### 3.1 Fractional Fourier Transform:

The Input image from the iris dataset is given. The Fractional Fourier transform is applied to input image. The fractional transform is a linear transformation that can convert images into any intermediate domain because its definition is the  $n$ th power;  $n$  does not have to be an integer. The fractional Fourier transform expression for a single dimension is as follows:

$$F_V \int_{-\infty}^{\infty} f(t)M_v(t, u)dt \quad (1)$$

The **Two-dimensional** Fractional Fourier transform with orders  $p_1$  and  $p_2$  is defined as follows

$$U_2(x_2, y_2) = F^{\alpha, \beta} \{U_1(x_1, y_1)\} \quad (2)$$

FRFT includes more parameters than the usual Fourier transform, including fractional orders and scaling factors in the x- and y-axes. These parameters can be used in addition to the FRFT when it comes to picture encryption. Keys to strengthen security in addition to the random phase mask. We will repeatedly use FRFT in an iterative manner to further enhance security performance. **Again,** apply the Inverse Fourier transform function to the output image obtained by FRFT. The IFRFT is a mathematical tool that performs the conversion of frequency domain signal to time domain signal.

Encryption Algorithm:

The iris detection encryption algorithm **uses** the FRFT model to extract the features of the iris image after performing preprocessing operations such as normalization on the gathered iris image dataset. After key generation using the extracted feature vector, the key and the original image's pixel value are subjected to the FRFT procedure.

Algorithm:

Step 1: Read the Input Image.

Step 2: Convert the Color Image into Gray scale Image.

Step 3: The Image is resized to the power of 2.

Step 4: Normalization is applied to the image with the pixel (0,1).

Step 5: Apply FRFT to the normalized image.

Step 6: The Original Encrypted Image is obtained by applying scaling operation on the transformed image.

Decryption Algorithm:

The image is encrypted by the encrypting side, and then the decryption process is carried out. The following steps can be used to describe the decryption process:

Step 1: Input the encrypted image and normalize it to [0,1].

Step 2: Apply IFRFT to the input image.

Step 3: Decrypted image is obtained.

Step 4: Scaling is performed to image to obtain the original size of an image.

Step 5: Finally original, encrypted and decrypted image is obtained.

### 3.2 Double Phase Random Encryption:

Optical cryptography, which encrypts hidden images into visual patterns, presents itself as a potent platform for information security. Utilizing optical cryptography from MMU and the IITD database, a solution for encryption is proposed. If the encryption method withstands outside attacks on images, it is deemed effective.

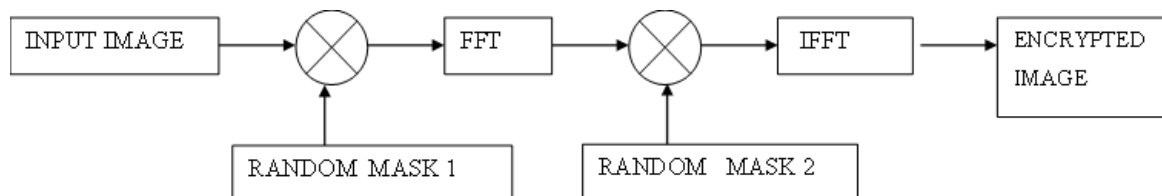


Fig 1. Encryption Block Diagram for DRPE.

Double random phase encoding (DRPE) is one of the method used for Optical Encryption. The work of Refregier and Javidi [17], where two random-phase functions in fractional Fourier domains are employed to encrypt input plain images into stationary white noise, is the source of DRPE-based picture encryption. Image encryption has been demonstrated by Hennelly and Sheridan [18] as random shifting in the fractional Fourier domain. The DRPE approach has been generalized in the fractional Fourier domain by Unnikrishnan [19]. Optical processing-based applications make extensive use of and exploration of the DRPE architecture. The DRPE system has been successfully extended to various linear canonical transformations (LCTs) domains, and the academic community has been actively investigating ways to further improve its security. The fig 1 shows encryption block diagram for double random phase encoding. Two statistically independent random phase-keys and two Fourier transforms are used to encode the primary input picture X to stationary white noise. Two keys are positioned, one in the Fourier domain and the other in the input domain.

ALGORITHM FOR DPPE:

Step 1: Input the Iris Image from the Dataset.

Step 2: Input the First and Second Random Mask along with the input image.

Step 3: Encrypted image is produced as output.

The Decryption process is the inverse of DPRE.

3.3 Proposed **HFRFDRPE** (Hybrid Fractional Fourier **DPRE**):

The fig 2 shows the overall architecture of the proposed system HFRFDRPE based encryption from the eye that is extracted by Iris. It shows the hybrid combination fractional fourier transform and double random phase.

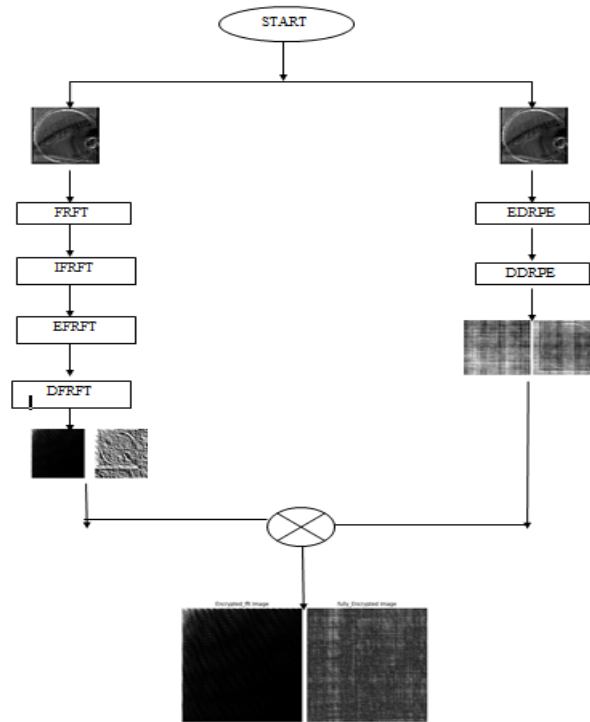


Fig 2 ARCHITECTURE OF HFRFDRPE

The steps for the proposed algorithm are as follows:

- Step 1: Input the gray scale iris image.
- Step 2: Apply FRFT to the input iris image.
- Step 3: Transformed FRFT iris image is obtained.
- Step 4: Apply IFRFT to the FRFT transformed iris image.
- Step 5: Generate Random mask for the Input Image.
- Step 6: Encryption is applied by means of hybrid combination of FRFT and DPRE.
- Step 7: Encrypted Image is finally obtained.
- Step 8: Repeat the same steps for Decryption.

IV. PERFORMANCE METRICS:

The original image is scrambled and cannot be recognized by anyone, which is the meaning of the security. A proposed encryption strategy aims to increase security by generating a key using the combination of DPRE and FRFT transform angles, which adds an extra degree of freedom. The proposed algorithm is performed on the experimental analysis with PSNR, SSIM, FRR, FAR.

PSNR:

Peak signal-to-noise ratio (PSNR) is the ratio of an image's maximum potential power to corrupting noise's ability to degrade the image's representation quality. It is measured in Decibels.

$$PSNR = 20 \log_{10} \left( \frac{L-1}{RMSE} \right) \quad (3)$$

SSIM (Structural Similarity Index Measure):

A standardized metric called SSIM is used to determine how comparable the original and decrypted images are structurally. Its variation ranges from [-1, 1]. There is no similarity between the photos if the value is around -1. The degree of similarity between the photos is at its highest when the value is near 1. The phrase that is used is:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + D_1)(2\sigma_{xy} + D_2)}{(\mu_x^2 + \mu_y^2 + D_1)(\sigma_x^2 + \sigma_y^2 + D_2)} \quad (4)$$

False acceptance rate and error rejection rate (FAR, FRR):

The false acceptance rate (FAR) is the likelihood that the original image can be correctly decrypted using the incorrect key. The likelihood that the original image cannot be properly decrypted with the correct key is known as the false rejection rate, or FRR.

V. EXPERIMENTAL ANALYSIS:

The proposed method is experimented by the performance metrics is shown in table 1 and the graphs are tabulated below and are shown in Fig 3.a and 3.b.

Table I: Performance Report of our proposed method

METHODS	VALUES
PSNR	28
SSIM	0.002
FAR	0.5
FFR	0.33
ENTROPY	5.68

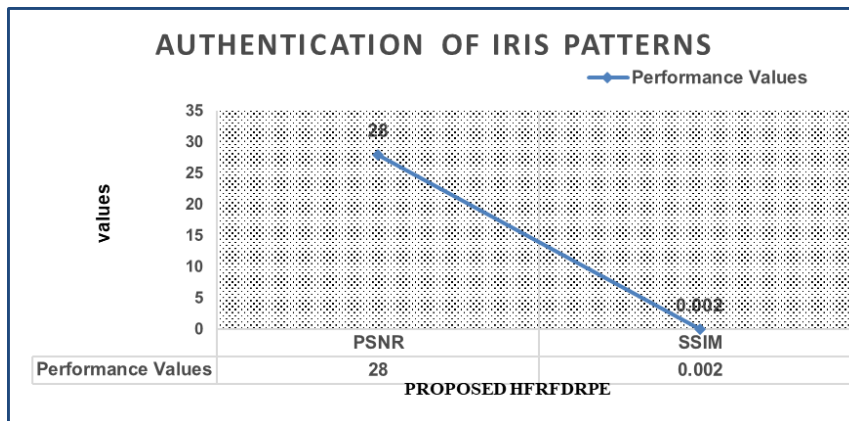


Fig 3.a Performance Graph of PSNR and SSIM

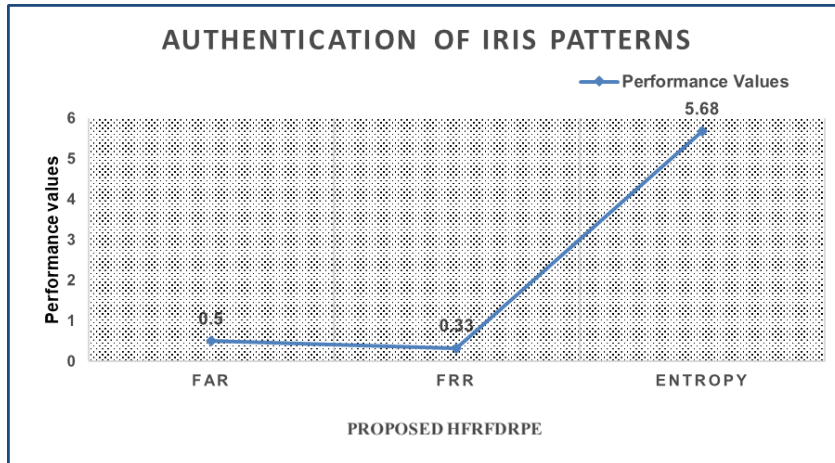


Fig 3.b Performance graph of FAR, FFR, ENTROPY

The performance of several iris identification methods is presented in Table 2. It displays the False Acceptance Rates (FAR), False Rejection Rates (FRR), the recognition obtained using various techniques. The table shows that, in terms of processing time, our suggested solution has fared better than the methods that are already in use. FRR:

Table 2: Performance comparison of different methodologies.

S. No	METHOD NAME	FAR
1	Proximity Searchable Encryption [20]	0.10
2	Secure ATM [21]	0
3	CHT and Absolute Differencing [22]	0.1
4	PROPOSED HFRFDRPE	0.33

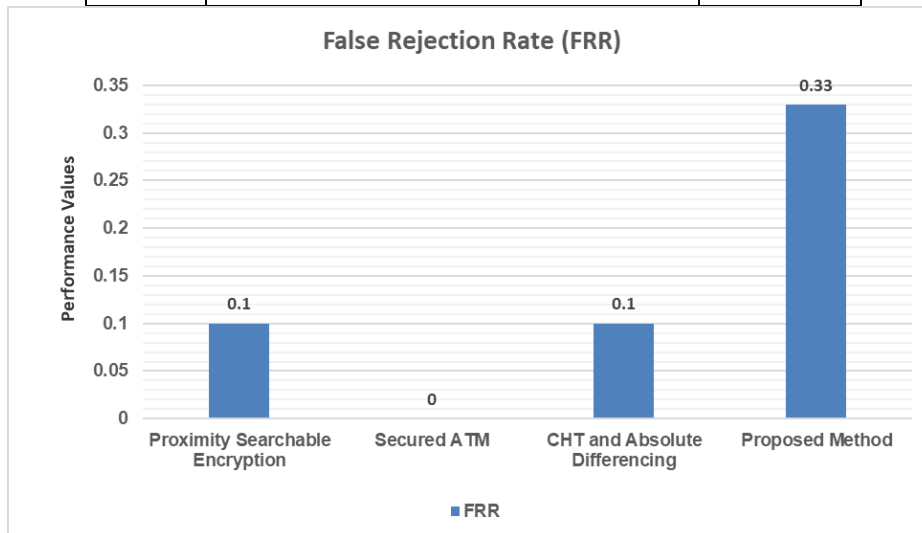


Fig 4. Performance graph of our proposed method of FRR with various methods

FAR:

Table 3: Performance comparison of different methodologies.

S. No	METHOD NAME	FAR
1	Block-based error correction - An improved approach [23]	10.2
2	Secure ATM [21]	5



3	CHT and Absolute Differencing with PCA [22]	8.9
4	PROPOSED HFRFDRPE	0.5

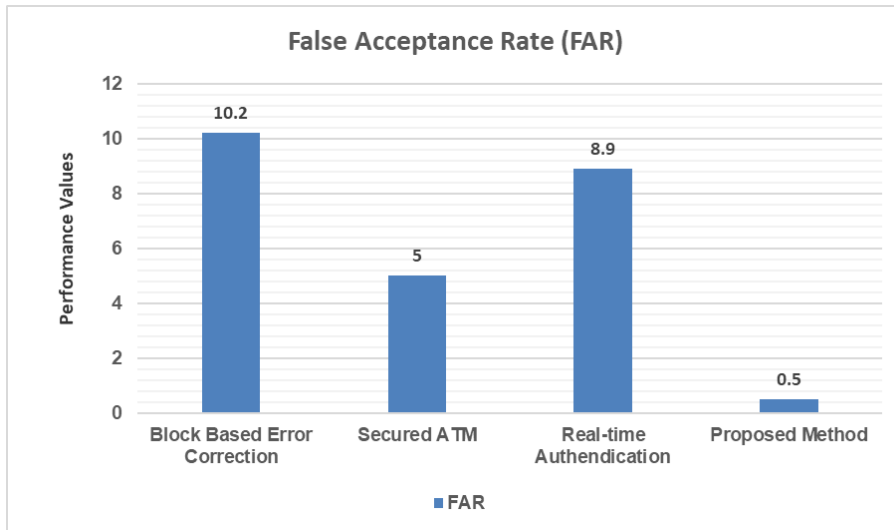

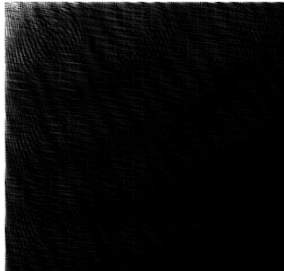
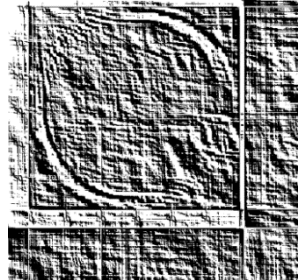

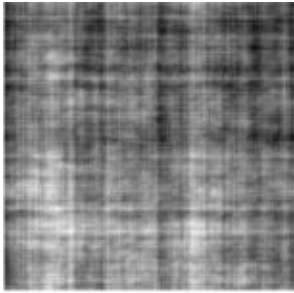
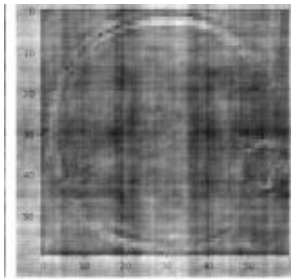


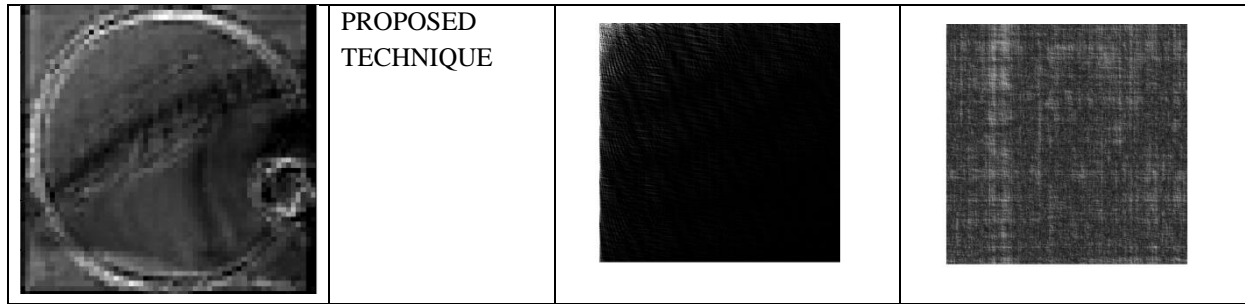
Fig 5. Performance graph of our proposed method of FAR with various methods.

Visual evaluation of encryption process- original images, encrypted images and decrypted images are represented in Table 5.

Table 5: Tabular Form of Original Image, Encrypted and Decrypted image

ORIGINAL IMAGE	METHODS	ENCRYPTED IMAGE	DECRYPTED IMAGE
	FRFT		
	DPRE		





VI. DATASET USED

The two different **datasets** are used for this encryption technique. They are MMU (Multimedia University Iris Dataset) and IITD (Indian Institute of Technology Dataset).

MMU:

It Contains 460 images from 46 images with few empty files.

IITD:

It Contains 224 images that is collected from different students and different staffs from IIT Delhi.

## VII. CONCLUSION

The secret to successful encryption and decoding in cryptography is the key. Information security is contingent upon key security. The assault of malicious key sharing and repudiation is too strong for the conventional image encryption technique. To achieve information encryption, the key is produced based on the user's biometrics and then applied to the appropriate picture encryption technique. The biological traits that are amenable to encryption should possess traits such as singularity, consistency, non-aggression, and so forth. In addition to meeting the aforementioned specifications, the iris possesses robust anti-attack capabilities, rich feature information, and exceptional encryption potential. Iris image encryption has grown to be a significant area of image encryption and is crucial to the field. The iris is used as the study object in this paper, and an image encryption and decryption method based on iris characteristic is achieved. An algorithm for extracting iris features through combination of FRFT and DRPE has been established. The collected features are applied to the processing of image encryption and decryption, and an impartial assessment of the suggested technique is conducted. The public iris database's simulation results demonstrate that the suggested strategy is capable of achieving image encryption.

## REFERENCES

- [1] Li, X., Jiang, Y., Chen, M., & Li, F. (2018). Research on iris image encryption based on deep learning. *EURASIP Journal on Image and Video Processing*, 2018(1), 1-10.
- [2] Yang, L., Fei, L. Y., Dong, Y. X., & Yan, H. (2010, June). Iris recognition system based on chaos encryption. In *2010 International Conference on Computer Design and Applications (Vol. 1, pp. V1-537)*. IEEE.
- [3] Ding, C., Xue, R., & Niu, S. (2023). Multibiometric Images Encryption Method Based on Fast Fourier Transform and Hyperchaos. *International Journal of Bifurcation and Chaos*, 33(07), 2350084.
- [4] Bhatnagar, G., & Wu, Q. J. (2014). Biometric inspired multimedia encryption based on dual parameter fractional fourier transform. *IEEE transactions on systems, man, and cybernetics: systems*, 44(9), 1234-1247.
- [5] Cui, D., Shu, L., Chen, Y., & Wu, X. (2013, August). Image encryption using block based transformation with fractional Fourier transform. In *2013 8th International Conference on Communications and Networking in China (CHINACOM)* (pp. 552-556). IEEE.
- [6] Dash, P., Pandey, F., Sarma, M., & Samanta, D. (2023). Efficient private key generation from iris data for privacy and security applications. *Journal of Information Security and Applications*, 75, 103506.
- [7] Kumar, D., Joshi, A. B., Singh, S., Mishra, V. N., Rosales, H. G., Zhou, L., ... & Singh, S. (2021). 6D-chaotic system and 2D fractional discrete cosine transform based encryption of biometric templates. *IEEE Access*, 9, 103056-103074.
- [8] Shen, Y., Tang, C., & Lei, Z. (2023). A double random phase encoding-based asymmetric cryptosystem using QZ modulation. *Journal of Optics*, 52(1), 189-196.
- [9] Tao, L., Liang, X., Wu, Z., Han, L., & Zhu, J. (2023). Plaintext Related Optical Image Hybrid Encryption Based on Fractional Fourier Transform and Generalized Chaos of Multiple Controlling Parameters. *Journal of Grid Computing*, 21(1), 17.

- [10] Wu, W., & Wang, Q. (2023). Block image encryption based on chaotic map and fractional fourier transformation. *Multimedia Tools and Applications*, 82(7), 10367-10395.
- [11] Ranjan, R., & Thakur, A. (2023). Image encryption using discrete orthogonal Stockwell transform with fractional Fourier transform. *Multimedia Tools and Applications*, 82(12), 18517-18527.
- [12] Khashan OA, Zin AM, Sundararajan EA (2014) Performance study of selective encryption in comparison to full encryption for still visual images. *Journal of Zhejiang University SCIENCE C* 15(6):435–444.
- [13] Wang XY, Yang L, Liu R, Kadir A (2010) A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics* 62(3):615–621.
- [14] Chandra S, Paira S, Alam SS, Sanyal G (2014) A comparative survey of symmetric and asymmetric key cryptography. *International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 83–93.
- [15] Jain A, Flynn P, Ross AA (2007) *Handbook of biometrics*. Springer Science & Business Media, Berlin Heidelberg.
- [16] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt Lett.* (1995) 20:767–9. doi: 10.1364/OL.20.000767
- [17] Hennelly B, Sheridan JT. Optical image encryption by random shifting in fractional Fourier domains. *Opt Lett.* (2003) 28:269–71. doi: 10.1364/OL.28.000269
- [18] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt Lett.* (2000) 25:887–9. doi: 10.1364/OL.25.000887.
- [19] Cachet, C., Ahmad, S., Demarest, L., Hamlin, A., & Fuller, B. (2022, May). Proximity searchable encryption for the iris biometric. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (pp. 1004-1018).
- [20] Parika Jain, Palak Garg, Shreya Asthana, Shristi, Meharban Ali (2019). Secured ATM System Using Iris Recognition Technique . *Eur. Chem. Bull.* 2023, 12(Special Issue 1), 1661-1670.
- [21] Hafeez H, Zafar MN, Abbas CA, Elahi H, Ali MO. Real-Time Human Authentication System Based on Iris Recognition. *Eng.* 2022; 3(4):693-708. <https://doi.org/10.3390/eng3040047>.
- [22] Moi, S. H., Yong, P. Y., Hassan, R., Asmuni, H., Mohamad, R., Weng, F. C., & Kasim, S. (2022). An improved approach of iris biometric authentication performance and security with cryptography and error correction codes. *JOIV: International Journal on Informatics Visualization*, 6(2-2), 531-539.