Journal of Harbin Engineering University Vol 44 No. 5
ISSN: 1006-7043 May 2023

Interference Based on Image Encryption in Fractional Fourier Domain Using Symmetric Keys

Himanshu[1], Reena Hooda[2], Vikas Poply[3]
[1]Research Scholar, Indira Gandhi University, Meerpur, Rewari-123401, India
[2]Assistant Professor, Indira Gandhi University, Meerpur, Rewari-123401, India
[3]Assistant Professor, K.L.P. college, Rewari-123401, India
Email id: iithimanshusaini@gmail.com , reenah2013@gmail.com, vikaspoply@gmail.com

Abstract

A Fractional Fourier Transform (FFT), we offer a picture encryption approach that relies here on the intrusion concept and a "phase Truncation" (PT) strategy. The suggested system uses symmetric keys to provide various levels of security while avoiding the silhouette problem. Multiple input images are fractionally Fourier independently converted using a random phase mask (RPM). The resultant spectrum's amplitude truncation (AT) aids in the generation of individual and universal keys, while PT provides two "phase-only masks" (POM) divergent. In two POM optically interact during decryption, resulting in a PT output function. The actual picture is successfully recovered after employing the correct RPM, global key, particular key, and fractional sequences. The proposed method is validated on the computer simulation process of two gray-scale photographs. To know what the best-proposed approach is, we measured the "mean square error" (MSE) around the actual and deciphered pictures. The encrypting and decrypting keys creation in this system are difficult and should be done digitally. An optoelectronic system has been proposed for decryption.

Keywords: Fraction Fourier transform, Encryption, Decryption, Random phase mask, Symmetric key

1. Introduction

Encrypting images with optical information processing provides a significant advantage. Optical techniques have been frequently employed for encrypting images due to their multi-dimensional and parallel processing capabilities. Refregier and Javidi [1] proposed a "random-phase encoding" (RPE) method for encrypting an initial picture to immobile noise. Several strategies have been documented in the literature as a result of this groundbreaking concept. By relocating the RPM distant from the angle of Fourier, Matoba, and Javidi [2] a third dimension was incorporated into the RPM. To provide numerous encryption, a waveform multiplexing approach has been added to the RPE system [3-4]. It has been reported a method for multiplexing encrypted images is based on the changing of an RPM. A solution adaptive control "Gerchberg–Saxton" (GS) algorithm and a PT power in the FFT have also been created to reduce cross-talk in multiple picture encryptions and multiplexing [5]. The FFT has been ramped up using the DRPE technique [6-11]. Which gives further order parameter security and robustness against a variety of strikes?

'Zhang and Wang' [12] offer a means to encode the image using two plain POM optical imaging (OI) interference theories. The gradually changing of masks is computed analytically rather than adopting an iterative technique to encode the actual image into true "phase diffraction elements" (PDEs). The system parameters are set, and two faces can be issued to two individuals for incredibly safe authentication. The encrypted file can only be obtained at the yield surface when both faces are right. However, there is a disadvantage to this method: Just one of the two faces is employed in the verification procedure, and the silhouette of the encrypted picture could still be identified. Because of the POM's equidistant nature by the analytical approach, even if the accurate decryption of an encrypted image is impossible. The Poisson of two POMs must be dispersed at unexpected times switched as a possible solution to this problem [13]. However, this method will raise the system's processing demand. The input picture would perhaps be split into 2 pieces, one is phase part organization and another with amplitude part distributed, according to a distinct approach [14]. Using two separate illumination wavelengths [15] suggested an algorithm for encoding data from two different pictures into three PDEs. The double-step holographic exposure approach [16] was used to develop OI encryption depending on

interference. Kumar et al. [17] suggested incorporating the jigsaw transmogrify it into an involved optical block cipher to solve the silhouette problem. A method for digitally encoding the original image into a single POM using an upgraded GS algorithm and another predetermined RPM is givin in [18]. The optical interference hypothesis has also been used to disguise information recently [19].

The large bulk of the approaches available in the literature is symmetric cryptosystems, which have identical encryption algorithm keys. Asymmetric in fractional parts are free of the difficulty with backdrops for practical use. For the simulation investigation, four grayscale photographs were employed. The proposal's robustness was assessed using the MSE method. The construction of encryption algorithm keys in this safety system is difficult and must be done on a computer digitally. The decoding procedure is straightforward and can be completed using an optoelectronic setup. An optoelectronic system has been proposed for decryption [20].

2. Multiple Image Symmetric Cryptosystem in the FRT Domain

A PT operation is included in the FT. It simply means that the "Fourier spectrum's amplitude" is preserved when the phase part is shortened. The amplitude component of the spectrum has been shortened in AT, leaving just in the phase portion [21-22]. FFT as a classical Fourier Transform into a general form was introduced as an aspect of mathematics as Namias is first and foremost in many applications of optics [23]. We need a new tune to analyze a time frequency in which FFT will play a good role. Which is the optical implementation of the FFT that was given by Mendlovic and Ozaktas in 1993, Which is used a lot in the optical field. FFT gives us more freedom in doing image encryption and in increasing the size of the key [24].

We will use FFT on a plane image I(x) as follows: [25]

$$\mathrm{Fp\{I(x)\}(u)} = \int_{-\infty}^{+\infty} k_p(x,u)I(x)dx \quad (1)$$

Where K_p (x,u) is the kernel function and is expressed as

$$KP(x,u) = \begin{cases} T\exp\left[i\pi(x^2 cot\emptyset - 2xu\ csc\emptyset + u^2 cot\emptyset)\right] & p \neq n\pi; \\ \delta(x-u), & p = 2n\pi \\ \delta(x+u), & p = (2n+1)\pi. \end{cases} \quad (2)$$

Here,

$$T = \frac{\exp\left[-i\left(\pi\, sgn\frac{\emptyset}{4} - \frac{\emptyset}{2}\right]\right.}{\sqrt{|sin\emptyset|}} \quad (3)$$

where $\emptyset = p\pi/2$. FFT is an integral transform which is the setup of linear and optical. We get some important property from FFT. FFT two dimension is a simple extension of one dimension which we represent as [26-29]

$$F^{\alpha 1,\alpha 1}\{I(x,y)\}(u,v)\alpha = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} K_{\alpha 1,\alpha 2}(x,y;u,v)f(x,y)dxdy \quad (4)$$

Where

$$K_{\alpha 1,\alpha 2}(x,y;u,v) = K_{\alpha 1}(x,u)K_{\alpha 2}(y,v) \quad (5)$$

3. Mean Squared Error

The difference between our actual picture and the decrypted picture is the "mean square error" ('MSE'), which we use to assess image quality. The closer the MSE number gets to zero, the higher the visual effects [30-31]. MSE assesses the most common and easiest distortion; the less our MSE measurement, the better the result [32-33]. MSE is given by the formula

$$MSE = \frac{1}{S*P}\sum_{l=0,m=0}^{S-1,P-1}[I(l,m) - K(l,m)]^2 \quad (6)$$

The S and P in it are our image width and length what came is our received image I(l,m) and K(l, m) are our initial image, l and m are our rows and columns which are of the received image and input image respectively.

4. The proposed scheme

The proposed scheme is divided into two parts: Encryption and Decryption process.

4.1. Encryption process

Fig. 1 depicts the block diagram of the proposed technique. To obtain the complex intermediate

image, each passage of an input picture is transformed into another phase picture with amplitude coupling masking before being FFT. The amplitude portion is then bonded with an RPM, this is the initial secret key.

Step 1: Transfer Every picture is transformed into a phase image, then bound with RAM before applying the FFT, which is expressed mathematically as:

I=FFT{exp(iπI).*RAM}
(7)

Step 3: The FFT component is then saved as the decryption's private key. The red component's equations are presented below, and the same processes apply to the others Images as well.

Key1=FFT{exp(iπI).*RAM}
(8)

g=FFT{exp(iπI).*RAM}
(9)

Step 4: A RPM is then attached to the portion (g), & after the FFT apply once more to act as a second private key (key2).

Key2=FFT(g.*RPM)
(10)

E= FFT(g.*RPM)
(11)

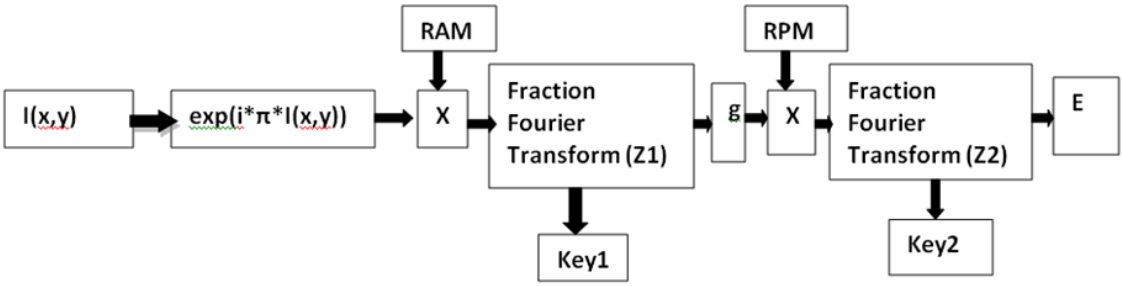

Fig.1. Block diagram for optical image encryption based on AT and PT in the FFT domain. (AT: amplitude truncation, PT: phase truncation).

4.2 Decryption process

In the Decoding algorithm, the encrypted file is padded with zeros to preserve size, as seen in Fig. 2.

Step 1: Zeros are used to fill in the gaps in the data, in the received encrypted picture (E), restoring the image to its original size.

Step 2: The second private key is then concatenated, and the FFT with reverse propagation distance is performed. Following that, the first secret key is merged, followed by a reverse FFT, and finally produces the original image (I).

I=FFT{FFT(E_R.*key2).*key1}
(12)

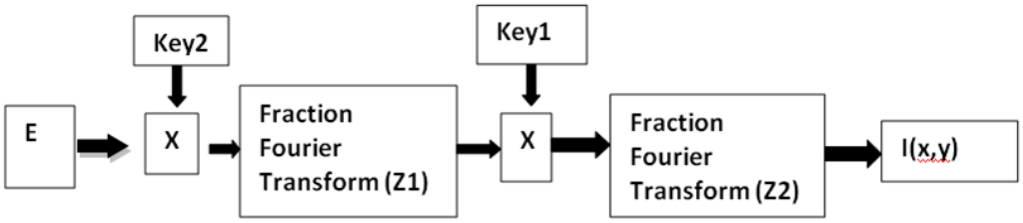

Fig. 2. Block diagram for decryption based on amplitude truncation and phase truncation in FFT domain.

4.3 Simulation Results

The initial image is shown in Fig. 3, and show histogram of input is in Fig. 4. Histograms are considered as the basis for a number of spatial domain techniques. Histograms play an important role in the enhancement of digital photographs. Histograms are used to display image information in a more understandable visual way. The frequency of intensity levels that occur in an image is described by the histogram [34].

a b

Fig. 3. Gray-scale input images to be used for encryption. Images of (a) Lena and (b) Cameraman

The FFT is based here on the image's amplitude, with the phase part serving as an additional secret key to show encrypted images Fig. 5.

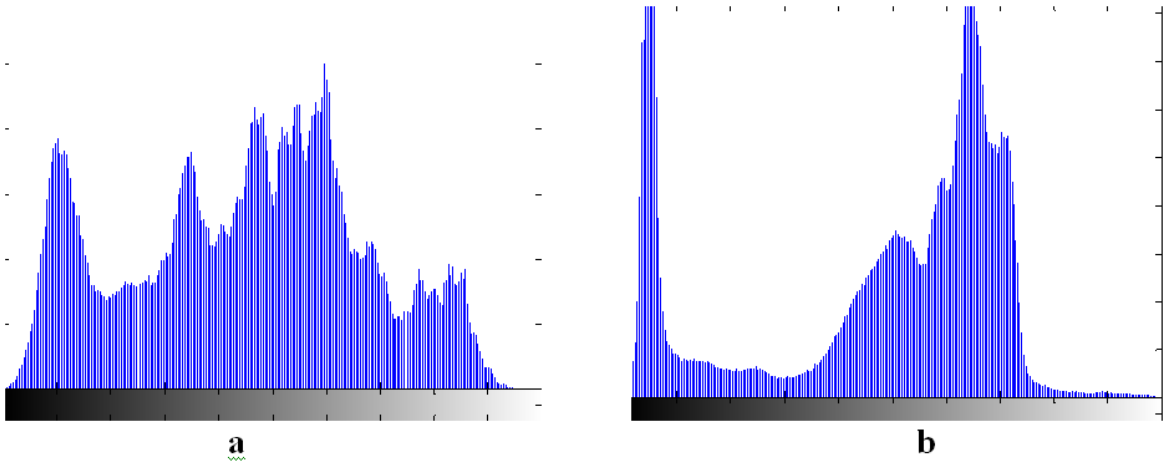

Fig. 4. Histograms for input Images of (a) Lena and (b) Cameraman

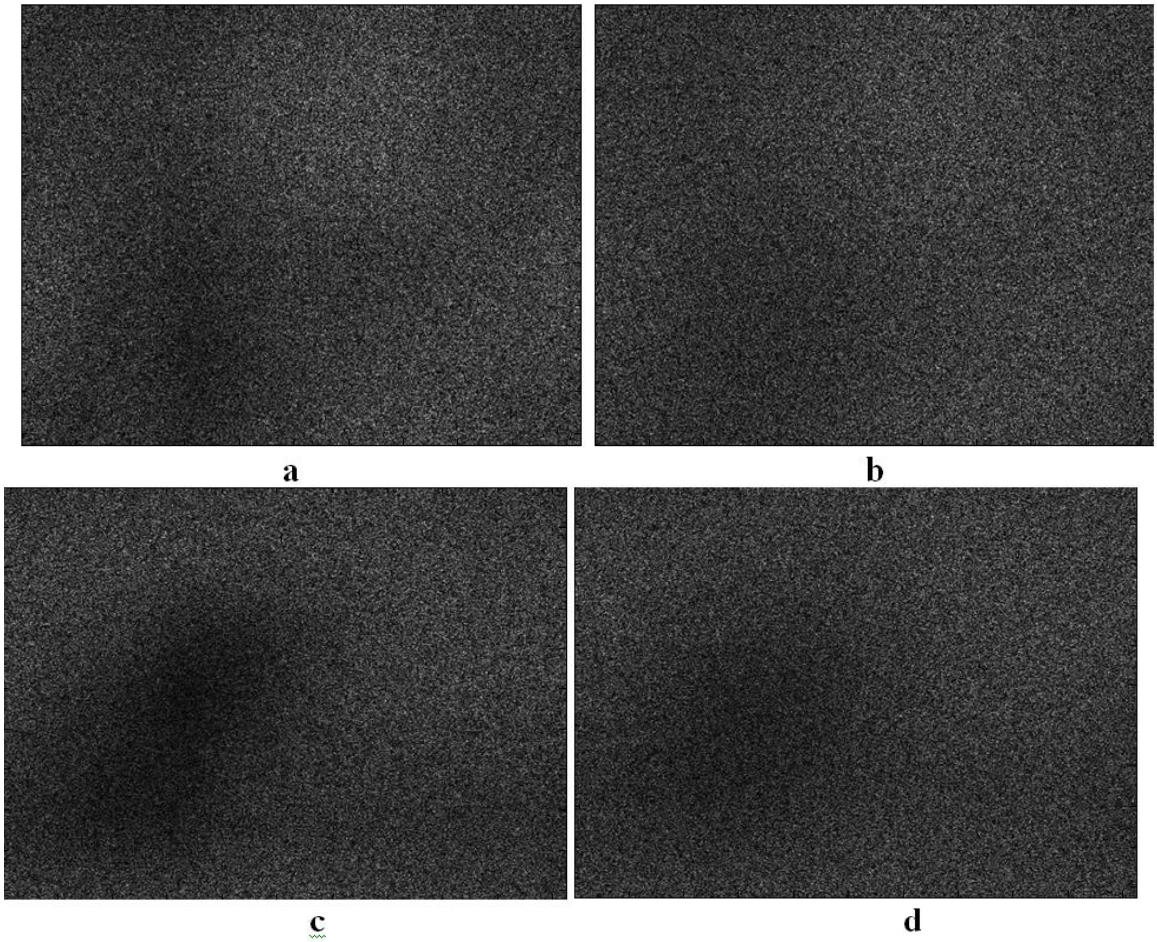

Fig. 5 (a) Encrypted image Lena after adding PM1 (b) Encrypted image Cameraman after adding PM1 (c) Encrypted image Lena after adding PM2 (d) Encrypted image Cameraman after adding PM2.

Inverse Fourier transform with reverse propagation distances images shown in Fig. 6 and decrypted images histogram shown in Fig. 7.

Fig. 6. Decrypted images obtained after the use of all correct keys; (a) Lena and (b) Cameraman.

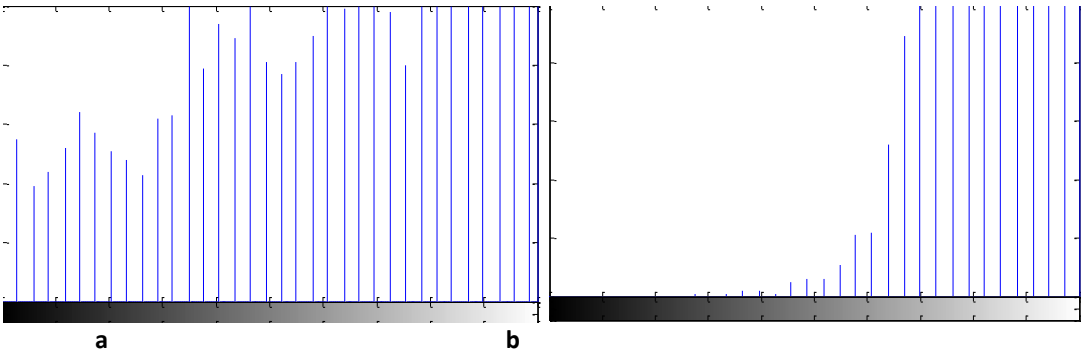

Fig. 7. Histograms' for Decoded Images of (a) Lena & (b) Cameraman

From Fig. 4 (a-b) and Fig.7(c-d), it is clear that the histograms of original images and recovered images are different. But we have recovered the image after applying correct keys with less MSE Furthermore, we cannot draw any static calculation from these histograms.

Working with FFT on images to get the different values of MSE shown in Table 1 and the graph below Fig .8 to show the MSE V/s fraction order.

Table 1: Computed results of MSE at different Fraction Order

SR. NO.	Fraction Oder(A)	Fraction Oder(B)	MSE(I1)	MSE(I2)
1	0.8	0.05	38.4848	98.8187
2	0.8	0.1	8.191	21.0322
3	0.8	0.15	3.0722	7.8887
4	0.8	0.2	1.4442	3.7084
5	0.8	0.25	0.764	1.9618
6	0.8	0.3	0.4332	1.1124
7	0.8	0.4	0.1556	0.3995
8	0.8	0.5	0.0593	0.1522
9	0.8	0.6	0.0224	0.0575
10	0.8	0.7	0.0081	0.0207
11	0.8	0.8	0.0027	0.007

12	0.8	0.9	0.001	0.0026
13	0.8	0.95	0.0007	0.0018

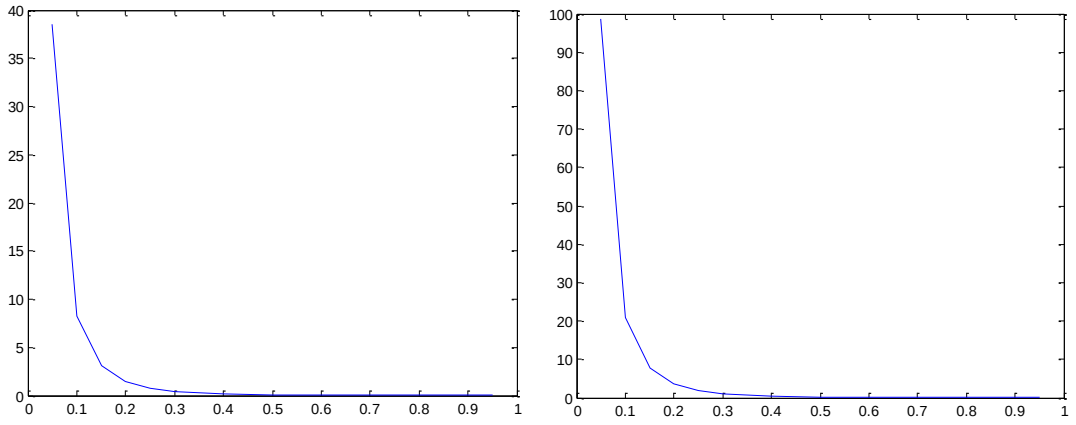

Fig .8 MSE value graphs a and b for Images Lena and the Cameraman

5. Conclusion

Finally, based on the optical interference concept, we offer a unique technique for multiple-image encryption employing symmetric keys in the FFT domain. The suggested methodology is not recurrent, and it addresses the interference technique's underlying silhouette problem. The usage of FFT expands the keyspace, which improves the cryptosystem's security. For several images, the suggested approach provides different degrees of security for different orders. The approach includes specific keys, global keys, a collection of the RPM, a collection of FFT orders, and empirically generated two POM, M1, and M2, to be utilized with optical interference. It has been recommended that the proposed decryption mechanism be implemented optically. To evaluate the proposed scheme's performance, the MSE between the initial and after process retrieved “images” was measured. MSE of two original and recovered images decreases with increasing fraction order. Lastly, findings from a computer simulation with two independent gray-scale images confirm the proposed idea of a multiple picture encryption scheme is better. Also, we investigate that no structural data is observed from the histogram of the original and recovered image.

References

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, no. 7, p. 767, 1995, doi: 10.1364/ol.20.000767.

[2] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” *Opt. Lett.*, vol. 24, no. 11, p. 762, 1999, doi: 10.1364/ol.24.000762.

[3] G. Situ and J. Zhang, “multiple-image encryption by wavelength multiplexing,” *Opt. Lett.*, vol. 30, no. 11, p. 1306, 2005, doi: 10.1364/ol.30.001306.

[4] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encryption-decryption via lateral shifting of a random phase mask,” *Opt. Commun.*, vol. 259, no. 2, p. 532, 2006, doi: 10.1016/j.optcom.2005.09.027.

[5] H.-E. Hwang, H. T. Chang, and W.-N. Lie, “Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain,” *Opt. Lett.*, vol. 34, no. 24, p. 3917, 2009, doi: 10.1364/ol.34.003917.

[6] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” *Opt. Lett.*, vol. 25, no. 12, p. 887, 2000, doi: 10.1364/ol.25.000887.

[7] B. Hennelly and J. T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” *Opt. Lett.*, vol. 28, no. 4, p. 269, 2003, doi: 10.1364/ol.28.000269.

[8] N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Opt. Lasers Eng.*, vol. 46, no. 2, pp. 117–123, 2008, doi: 10.1016/j.optlaseng.2007.09.001.

[9] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photonics*, vol. 1, no. 3, p. 589, 2009, doi: 10.1364/aop.1.000589.

[10] X. Hu, Y. Diao, X. Zheng, Z. Qu, F. Zhou, and Z. Hu, "Isolation and characterization of simple sequence repeat loci in Miscanthus floridulus and their potential use as markers in related species," *Biomass and Bioenergy*, vol. 46, no. 16, pp. 801–804, 2012, doi: 10.1016/j.biombioe.2012.07.003.

[11] N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," *Opt. Commun.*, vol. 284, no. 3, pp. 735–739, 2011, doi: 10.1016/j.optcom.2010.09.065.

[12] Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.*, vol. 33, no. 21, p. 2443, 2008, doi: 10.1364/ol.33.002443.

[13] Y. Zhang, B. Wang, and Z. Dong, "Enhancement of image hiding by exchanging two phase masks," *J. Opt. A Pure Appl. Opt.*, vol. 11, no. 12, pp. 5–9, 2009, doi: 10.1088/1464-4258/11/12/125406.

[14] Y. Han and Y. Zhang, "Optical image encryption based on two beams' interference," *Opt. Commun.*, vol. 283, no. 9, pp. 1690–1692, 2010, doi: 10.1016/j.optcom.2009.12.060.

[15] C.-H. Niu, X.-L. Wang, N.-G. Lv, Z.-H. Zhou, and X.-Y. Li, "An encryption method with multiple encrypted keys based on interference principle," *Opt. Express*, vol. 18, no. 8, p. 7827, 2010, doi: 10.1364/oe.18.007827.

[16] D. Weng, N. Zhu, Y. Wang, J. Xie, and J. Liu, "Experimental verification of optical image encryption based on interference," *Opt. Commun.*, vol. 284, no. 10–11, pp. 2485–2487, 2011, doi: 10.1016/j.optcom.2011.01.039.

[17] P. Kumar, J. Joseph, and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Appl. Opt.*, vol. 50, no. 13, pp. 1805–1811, 2011, doi: 10.1364/AO.50.001805.

[18] B. Yang, Z. Liu, B. Wang, Y. Zhang, and S. Liu, "Optical stream-cipher-like system for image encryption based on Michelson interferometer," *Opt. Express*, vol. 19, no. 3, p. 2634, 2011, doi: 10.1364/oe.19.002634.

[19] S. Yuan, S. X. Yao, Y. H. Xin, and M. T. Liu, "Information hiding based on the optical interference principle," *Opt. Commun.*, vol. 284, no. 21, pp. 5078–5083, 2011, doi: 10.1016/j.optcom.2011.07.015.

[20] P. Trigonometric and C. Map, "SS symmetry Product Trigonometric Chaotic Map," 2022.

[21] X. Wang and D. Zhao, "Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain," *Opt. Commun.*, vol. 284, no. 1, pp. 148–152, 2011, doi: 10.1016/j.optcom.2010.09.034.

[22] W. Qin, "Universal and special keys based on phase-truncated Fourier transform," *Opt. Eng.*, vol. 50, no. 8, p. 080501, 2011, doi: 10.1117/1.3607421.

[23] P. Fitzpatrick, "Asymmetric Cryptography," *Irish Math. Soc. Bull.*, vol. 0020, no. 24, pp. 21–31, 2021, doi: 10.33232/bims.0020.21.31.

[24] H. C. Lin, Y. C. Ye, B. J. Huang, and J. L. Su, "Bearing vibration detection and analysis using enhanced fast Fourier transform algorithm," *Adv. Mech. Eng.*, vol. 8, no. 10, pp. 1–14, 2016, doi: 10.1177/1687814016675080.

[25] D. R. Jariwala and B. Patel, "Accelerating Fast Fourier Transformation using Image Processing Techniques," vol. 7, no. 4, pp. 10767–10771, 2017.

[26] T. Belabed, S. Jemmali, and C. Souani, "FFT implementation and optimization on FPGA," *2018 4th Int. Conf. Adv. Technol. Signal Image Process. ATSIP 2018*, no. 1, pp. 1–6, 2018, doi: 10.1109/ATSIP.2018.8364454.

[27] I. Journal, O. F. Engineering, I. Of, and F. F. T. Algorithm, "International journal of engineering sciences & research technology implementation of fft algorithm," vol. 6, no. 5, pp. 206–211, 2017, doi: 10.5281/zenodo.573508.

[28] G. G. Kumar, S. K. Sahoo, and P. K. Meher, *50 Years of FFT Algorithms and Applications*, vol. 38, no. 12. Springer US, 2019. doi: 10.1007/s00034-019-01136-8.

[29] U. Oberst, "The fast Fourier transform," *SIAM J. Control Optim.*, vol. 46, no. 2, pp. 496–540, 2007, doi: 10.1137/060658242.

[30] U. Sara, M. Akter, and M. S. Uddin, "Image

Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[31] F. Memon, M. Ali Unar, and M. Sheeraz, "Image Quality Assessment for Performance Evaluation of Focus Measure Operators," *Mehran Univ. Res. J. Eng. Technol.*, vol. 34, no. 4, pp. 389–386, 2015, [Online]. Available: http://publications.muet.edu.pk/research_papers/pdf/pdf1147.pdf

[32] P. Sharma, S. Sharma, and A. Goyal, "An MSE (mean square error) based analysis of deconvolution techniques used for deblurring/restoration of MRI and CT Images," *ACM Int. Conf. Proceeding Ser.*, vol. 04-05-March-2016, no. February 2019, 2016, doi: 10.1145/2905055.2905257.

[33] D. Asamoah, E. Ofori, S. Opoku, and J. Danso, "Measuring the Performance of Image Contrast Enhancement Technique," *Int. J. Comput. Appl.*, vol. 181, no. 22, pp. 6–13, 2018, doi: 10.5120/ijca2018917899.

[34] H. Kaur and N. Sohi, "A Study for Applications of Histogram in Image Enhancement," The International Journal of Engineering and Science (IJES),vol. 2, no. 1, p. 59, 2017, doi: 10.9790/1813-0606015963.