Hindawi
International Journal of Optics
Volume 2022, Article ID 6165901, 16 pages
https://doi.org/10.1155/2022/6165901

Research Article

A New Highly Secure Optical Image Security Technique Using Gyrator Transform for Image Security-Related Applications

L. Anusree [1] **and M. Abdul Rahiman** [2]

[1]*Department of Electronics and Communication Engineering, LBSITW, Thiruvananthapuram, Kerala, India*
[2]*LBSCST, Thiruvananthapuram, Kerala, India*

Correspondence should be addressed to L. Anusree; anusreelathika@gmail.com

Received 17 November 2021; Revised 26 April 2022; Accepted 23 May 2022; Published 21 June 2022

Academic Editor: Samir K. Mondal

New methods and apparatuses for information security have evolved as a result of the rapid expansion of optical information processing. Security is one of the major issues in digital image transmission because it can deliver very secret information to any corresponding agency such as the military, biomedical, and security agencies. Previously, various techniques are proposed to perform optical image encryption techniques using different transformation and pixel-level techniques. Each work has its advantages and disadvantages in terms of computational complexity, security level, flexibility, quality, and so on. To overcome the security issues present in the previous works, a novel optical image encryption standard is proposed in this paper. This work uses information hiding followed by image encryption using Gyrator Transform (GT) using mean gradient key-based block swapping techniques. The main advantage of this work is that the key generation is dynamic and it depends upon the pixel intensity of 8×8 blocks. Secret information hiding is performed in the Discrete Cosine Transform (DCT) domain to protect the data against noise attacks. To analyze the performance, various evaluation metrics are used to measure the quality of the decrypted image under various distortions such as cropping and rotation. The robustness of information hiding is analyzed using a noise attack on the received image. This work achieved 45.6 dB of Peak Signal-to-Noise Ratio (PSNR) and 0.965 of Structural Similarity Index (SSIM), which is the best when compared to the conventional image encryption standards.

1. Introduction

As network information technology continues to progress at a fast pace, maintaining critical information security is becoming more crucial in the information age. When information is stolen in certain businesses, it has far-reaching ramifications for the victims. Because of advances in information security technology, data may be encrypted to the point that even if it is stolen, an eavesdropper will not be able to decrypt it and therefore prevent certain harms. It is becoming more essential in the field of information security as a result of its great degree of freedom, high resilience, parallel processing capabilities, and rapid speed [1]. Refregier and Javidi originally suggested a Double Random Phase Encoding (DRPE) based on the 4f optical correlator. Various further DRPE-based optical encryption methods for monochrome and color images have been introduced since then [2].

If the two-phase masks disagree significantly, DRPE indicates that the encrypted picture has a stationary normal distribution. Due to its noteworthy benefits, such as huge keyspace and stability in the blindness encryption operation, the DRPE method was later suggested to the Fresnel domain and fractional Fourier domain. Nonetheless, it has two obvious faults that prohibit it from being utilized for an extended period. As a result, a growing number of individuals are concentrating their efforts on developing nonlinear optical encryption methods [3].

Integral imaging is a real three-dimensional (3D) imaging technique that depends on an integrated photographic method that only allows us to capture a series of Two-Dimensional (2D) pictures from a 3D scene using a lenslet

array. These 2D pictures are known as elemental images because they contain information on the direction and brightness of a 3D scene [4].

Several nonlinear processes, including vector operations, natural logarithm operations, and log-polar transforms, are used to encrypt systems to address the linearity issue. Aside from the linearity issue, most encryption algorithms that use the transformed domain produce complex-valued outputs, making the display, transmission, and storage challenges. To reconstruct the original image via holography, the phase information of the final findings should be preserved [5].

The grayscale image is split into 8×8 blocks in this work, and these blocks are converted using the DCT. The input text is converted into ASCII code and converted to binary numbers. Replace Least Significant Bit (LSB) from this concatenated binary number. Apply Inverse Discrete Cosine Transform (IDCT) after performing the reverse quantization method. Then, assemble 8×8 blocks. Finally, apply GT with an angle θ.

The remainder of this work is structured as follows: Section II describes the optical encryption techniques that have been published. Section III discusses the suggested optical encryption technology. Section IV explains the outcome and discussion of the suggested approach, comparative research, and analysis. Finally, Section V explores the conclusion.

2. Literature Survey

Previously, a large number of works were presented to implement the optical encryption approach. These various strategies aim to minimize design complexity by improving the algorithm's architecture. This section contains some of the previously suggested efforts for performing optical encryption implementation.

Le Hong Zhang et al. proposed that optical encryption is based on deep learning and Ghost Imaging (GI), and it is also used as a point-to-face transmission method to reduce the influence of chaotic medium and turbulence on the communication channel. The image is first preprocessed by the Joint Photographic Experts Group (JPEG) to produce a compressed image. Finally, deep learning is being utilized for reconstruction to address the issue of poor image quality following GI transmission, which can improve image resolution [6].

Lina et al. proposed optical encryption-based diffractive imaging depending on the learning-based attacks. An opponent can recover unknown plaintexts from provided ciphertexts using a machine learning assault. End-to-end learning is used in the proposed approach to derive a superior mapping connection between ciphertexts and plaintexts. The suggested learning technique is viable and effective for analyzing the susceptibility of optical encryption systems, as demonstrated by simulations and optical experimental findings [7].

Sara T. Kamal et al. proposed a novel encryption method for both grayscale and color medical pictures. The introduction of a novel splitting the image approach depends on blocks of the image. The image blocks were then jumbled with a zigzag pattern, rotation, and random permutation. The scrambled image is then diffused using a chaotic logistic map. Security and time complexity studies are used to calculate the performance of this technique for encrypting medical images [8].

Tatsuya Chuman and Warit Sirichotedumrong proposed to improve the security of encryption-then-compression (EtC) systems employing JPEG compression. It is proposed to use a block scrambling-based encryption scheme, which allows us to communicate pictures without fear of being intercepted by an entrusted channel provider. A smaller block size and a bigger number of blocks may be used using the proposed technique in contrast to the previous system. Although the original picture has three color channels, photos encrypted using the recommended approach have less color information than the original image since grayscale images are used to encrypt the image. These characteristics help to build defenses against a variety of threats [9].

Kang Yi et al. proposed GI optical encryption and public-key cryptography. The Rivest–Shamir–Adleman (RSA) algorithm of the public key is used to solve the key distribution problem. When there are fewer ciphertexts, the CS technique gives excellent quality plaintext reconstruction. The features of the RSA public-key method are combined with the GI method to provide convenience and security of use for speedy transmission of data. It is very resistant to statistical analysis and repeated attacks, as well as highly resilient. In a nutshell, optical encryption is founded on Compressive Sensing Ghost Imaging (CSGI) and public-key cryptography [10]. Dongdong et al. proposed when various frequencies of quantized DCT (Discrete Cosine Transform) coefficients are used in a JPEG picture, the resultant image will have varying capacities and embedding deformities. As a first step toward reducing overall distorted distortion for the marked image, we select coefficients from frequencies that produce fewer distortions for embedding, and then we employ an advanced block selection strategy to always modify the block that produces the least simulated distortion first until the given payloads have been completely embedded in the marked image and until the overall distorted image has been reduced to zero [11].

It is obvious from the preceding discussion that numerous works have previously been offered to increase the robustness. The primary disadvantages of prior efforts are their poor quality and lack of security. The major purpose of this effort is outlined in the following parts:

(i) The main objectives of this work are as follows:

(ii) To improve the robustness of optical encryption under various complicated noise attacks.

(iii) To enhance the accuracy of the optical encryption method.

(iv) To maintain the image quality without the loss of any data.

(v) To reduce the computational complexity.

3. Proposed Method

In this work, a greyscale image is taken as input and initially converted into 8×8 blocks. Further DCT is applied to each block to shift from spatial to frequency domain. A typical quantization table is used to perform the quantization process by its corresponding constant, which is then rounded down to the closest integer for each coefficient. Following that, the DCT quantized coefficients are scanned in a zigzag pattern according to a preset schedule. The 64 DCT coefficients are organized in each block from the lowest frequency at the top left corner to the highest frequency at the bottom right corner. The low frequencies include the image's most significant visual features, whereas the higher frequencies contain the details. At that time, the input text is converted into ASCII code and converted to binary number. Then the binary number is concatenated with the image binary number. Replace LSB from this concatenated binary number. To convert the frequency domain data to the spatial domain, IDCT is applied after performing a reverse quantization process. All the 8×8 blocks are further assembled to generate a complete encrypted image. To create a scrambled image, Gyrator Transform is used with block swapping technique mean block variance vector as key. To extract secret information, the reverse process is performed with secrete θ key vector on the receiver side. Figure 1 shows the block diagram of the proposed method.

3.1. DCT. DCT is frequently used in digital compression techniques such as JPEG. DCT is used in the image encryption process [12]. DCT may alter the distribution of pixel values over an entire picture to produce a random output pattern. Another argument for adopting DCT is that it is specified in the real number field. Thus, with this encryption, output data can be encoded using real numbers [13, 14].

The input gray image is split into 8×8 blocks. Every block undergo the encryption process with DCT in equation (1):

$$\mathrm{U_k(x,y)} = \frac{\mathrm{c(x)c(y)}}{4} \sum_{\mathrm{m=0}}^{7} \sum_{\mathrm{n=0}}^{7} \mathrm{u_k(m,n)} \cos\left(\frac{(2\mathrm{m}+1)\mathrm{x}\pi}{16}\right) \cos\left(\frac{(2\mathrm{n}+1)\mathrm{y}\pi}{16}\right),$$
$$\text{with } \mathrm{c(e)} = \begin{cases} \dfrac{1}{\sqrt{2}}, & \mathrm{e} = 0, \\ 1, & \mathrm{e} = 0, \end{cases} \tag{1}$$

where $U_k(x, y)$ is the outcome of DCT in the position (x, y), while $u_k(m, n)$ is the initial image pixel value in the (m, n) position before being transformed to DCT.

Decompression is used to recover the compression result utilizing DCT by applying the Inverse Discrete Cosine Transform function through equation (2):

$$u_k(m,n) = \frac{1}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} c(x)c(y)U_k(x,y) \cos\left(\frac{(2m+1)x\pi}{16}\right) \cos\left(\frac{(2n+1)y\pi}{16}\right),$$
$$\text{with } c(e) = \begin{cases} \dfrac{1}{\sqrt{2}}, & e = 0, \\ 1, & e = 0, \end{cases} \tag{2}$$

where $u_k(m, n)$ is the IDCT result in the (m, n) position, while $U_k(x, y)$ is the DCT result in the (x, y) position.

3.2. Quantization. Higher compression rates can be achieved with vector quantization, a block-based efficiency picture compression coding technique. If the simple picture does not closely match, the rebuilt image has visible blocking artifacts [15, 16].

The codebook $y = \{y_j\}_{j=1}^{m}$ in vector, and quantization can be generated by equation (3):

$$\min \sum_{i=1}^{n} d_i; \quad d_i = \min E\left(x_i, y_j\right), \quad (i \le j \le m), \tag{3}$$

where $x = \{x_i\}_{i=1}^{n}$ is the training sample set and $E(x_i, y_j)$ is a suitable metric distance function.

After that, the DCT results were quantified. The DCT findings were divided by chrominance and luminance matrix for quantification. The quantization results were read indirectly and converted into sequences in the form of blocks, with each block generating a sequence of 64 lengths [17].

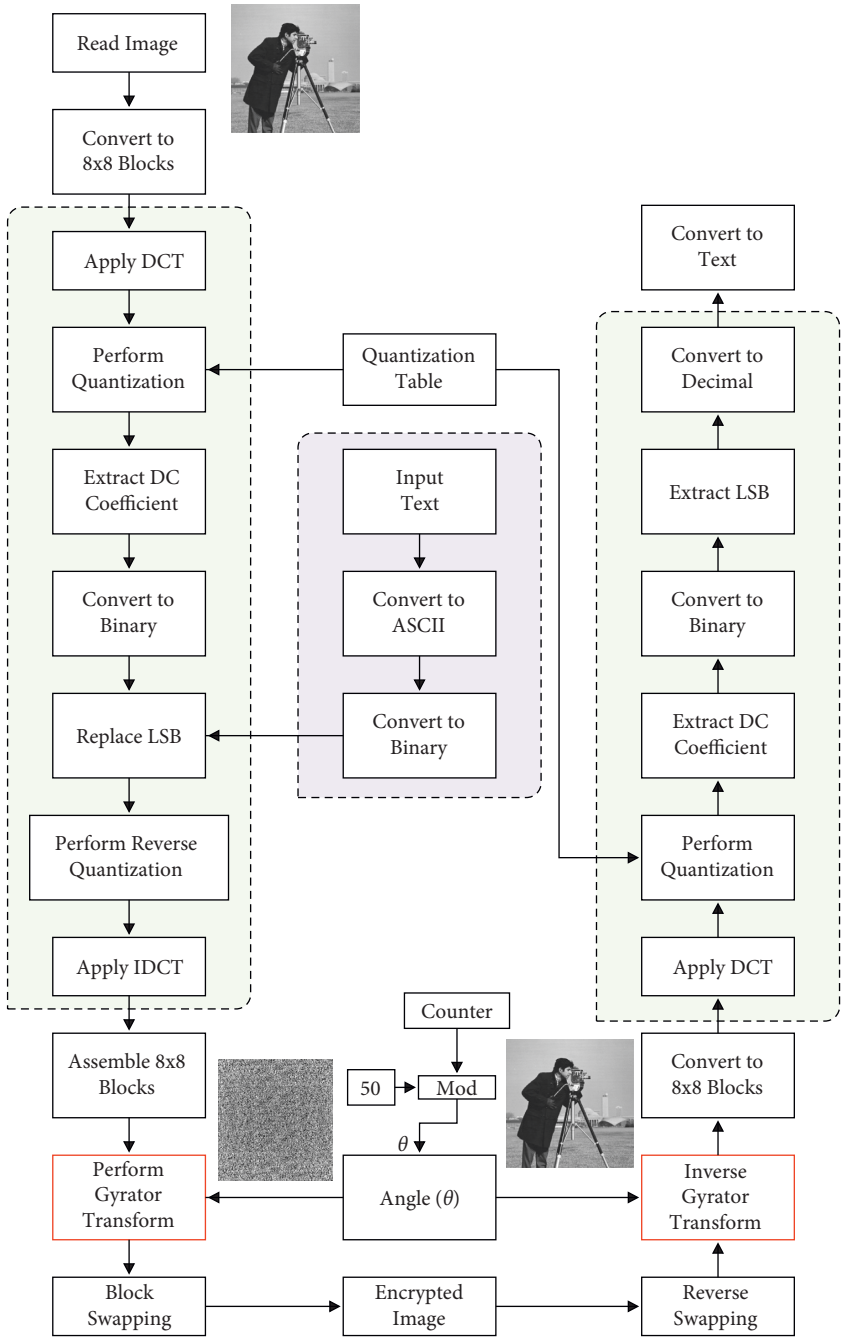


Figure 1: Block diagram of the proposed method.

3.3. Gyrator Transform. GT is a 2D complex field function linear canonical transform that is commonly used to create rotation in the position-spatial frequency plane [18]. For the input image f (x, y), the definition of GT at α can be explained in equation (4):

$$F(u,v) = GT^{\alpha}[f(x,y)](u,v) = \frac{1}{|\sin\ \alpha|}\int\int f(x,y)\times\ \exp\left[\frac{i2\pi(xy+uv)\cos\ \alpha-(xv+yu)}{\sin\ \alpha}\right]\mathrm{d}x\mathrm{d}y, \tag{4}$$

where (x, y) and (u, v) are input and output plane coordinates and α is the rotation angle. Some of GT's characteristics are comparable to those of FRFT. GT is a function that is both periodic and additive [19, 20]. The

rotation angle α between two generalized lenses is formed by two convergent thin cylindrical lenses [21]. The inverse GT is GT with an opposite rotation angle [22]. The image encryption process is performed based on gyrated transform with different theta values. Theta value is calculated using equation (5):

$$\begin{aligned} \theta_m &= m\%50 \\ \text{for } m &= 1 \text{ to } N. \end{aligned} \tag{5}$$

3.4. Mean Difference Key-Based Block Swapping. The block swapping method ensures a two-tier secured shield [23]. Figure 2 shows the proposed block swapping method. After the GT, split the real and imaginary number of GT complex values, and then calculate the mean value of the real number. Mean value calculation is performed by using an 8×8 block size. To create the dynamic key for different images, the successive difference of the mean array is calculated further to perform the block swapping process. Negative and zero differences are considered as "0," and positive differences are considered as "1." Then, the "0" value blocks are swapped into the imaginary number blocks, and imaginary number blocks are swapped into real numbers blocks. It is explained in equations (6) and (7).

Here, N is the number of blocks. θ_m is the angle for the mth block.

$$s_r(m) = \begin{cases} s_i(m), & \text{if key}(m) = 1, \\ s_r(m), & \text{if key}(m) = 0, \end{cases} \tag{6}$$

$$s_i(m) = \begin{cases} s_r(m), & \text{if key}(m) = 1, \\ s_i(m), & \text{if key}(m) = 0. \end{cases} \tag{7}$$

Figure 3 shows the results obtained for the key generation process. Figure 3(a) shows the mean value obtained for each block. Here, the x-axis shows the block number for the corresponding image blocks. Figure 3(b) shows the successive difference of mean value concerning block number. Generated key data concerning the mean value difference can be shown in Figure 3(c).

4. Results and Discussion

This section ran a series of simulations to show that the proposed encryption method is both legitimate and effective. This work is done by MATLAB R2020b using a computer with CPU Intel (R) Core (TM) i5-3320M CPU @ 2.60 GHz, and 2 GB of RAM.

4.1. Dataset. In this work, the dataset images with size 256×256 gray image-standard test images are encrypted and decrypted, as presented in Figure 4. Cameraman, Lena, pout, mandrill, pepper, CT scan, X-ray, and house images are used in this work. A standard test image is a digital image file that is used by many different organizations to evaluate image processing and image compression methods on the same data set of pixels. Different laboratories are able to compare findings both visually and numerically since they are utilizing the same set of standard test images. Table 1 shows the dataset description.

4.2. PSNR. The PSNR is the proportion of the signal's maximum potential strength to the power of completely corrupted input [24]. PSNR is expressed as equation (8):

$$\text{PSNR} = 20 \cdot \log_{10} MAX_{PY} - 10 \cdot \log_{10} MSE, \tag{8}$$

where MAX_{PY} represents a maximum image pixel value.

4.3. Correlation Coefficient (CC). The CC is a graphical representation of a type of correlation, which is a statistical relationship between these two variables [25]. The variables may be two columns from a given set of data or two components of a quantitative probability distribution with a good distribution represented in equation (9):

$$CC(K,k) = \frac{M\{[K - M(K)][k - M(k)]\}}{M\left\{[K - M(K)]^2\right\} M\left\{[k - M(k)]^2\right\}}. \tag{9}$$

Here, K and k represent the plain image and decrypted image.

4.4. SSIM. SSIM is a perspective paradigm that treats image loss as a perceived shift in structural details while often integrating core visual effects, including the intensity of light masking and intensity masking concepts [26], shown in equation (10):

$$\text{SSIM}(i,j) = \frac{\left(2k_i k_j + r1\right)\left(2l_{xy} + r2\right)}{\left(k_i^2 + k_j^2 + r1\right)\left(l_i^2 + l_j^2 + r2\right)}. \tag{10}$$

4.5. Mean Square Error (MSE). The MSE measures an estimator's consistency; it is often nonnegative, with values closest to zero being greater [27]. The distinction between the original and decrypted images is represented in MSE depicted in equation (11):

$$\text{MSE} = \frac{1}{Px^* Px} \sum_{i=1}^{Px} \sum_{j=1}^{Px} |\hat{I}(i,j) - I(i,j)|^2. \tag{11}$$

4.6. Root-Mean-Square Error (RMSE). The RMSE is used to calculate the residuals' standard deviation. Residuals are a metric about how far apart the data points are from the regression line; RMSE is expressed in equation (12):

$$\text{RMSE} = \sqrt{\overline{E - K}}, \tag{12}$$

where E is the expected value and K are known results.

4.7. Mean Absolute Error (MAE). MAE is a statistical assessment of error among matched data representing the same phenomenon. Comparisons of predicted versus

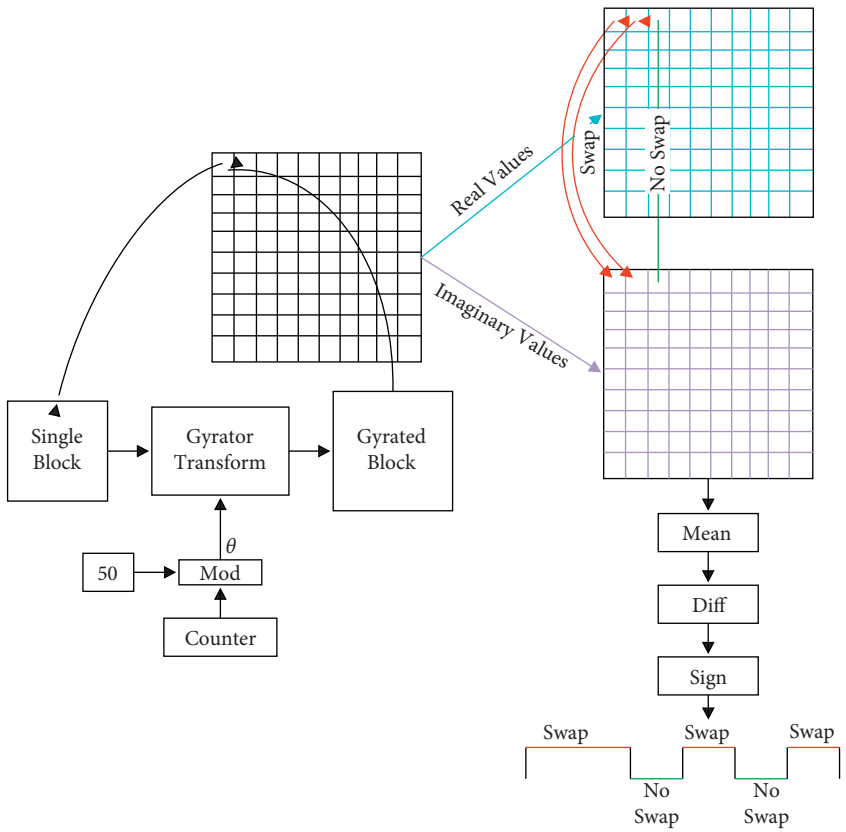


Figure 2: Proposed block swapping method.

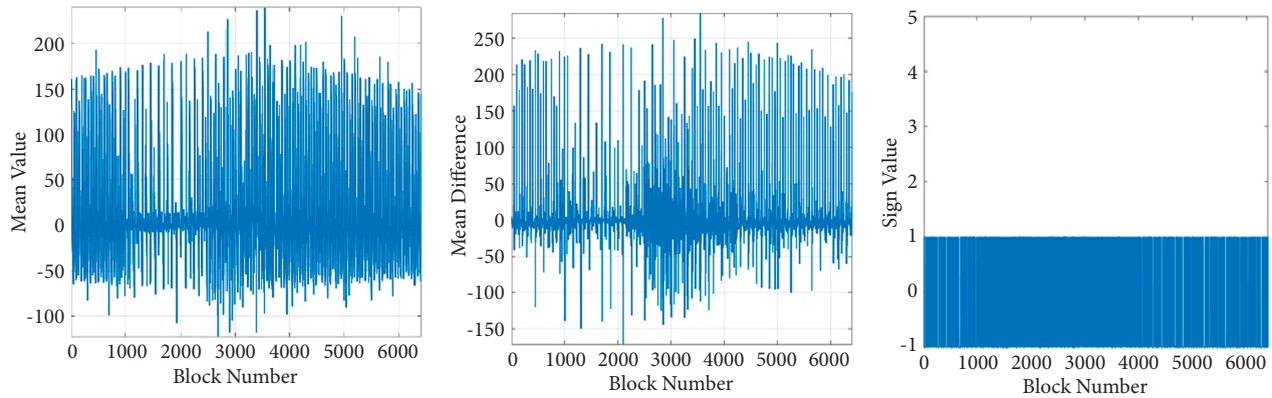


Figure 3: Mean key-based block swapping. (a) Mean block value. (b) Mean difference. (c) Sign of difference.

observed future time versus starting time and one measuring technique versus another are shown in equation (13):

$$\mathrm{MAE} = \frac{\sum_{I=1}^{N} |Y_I - X_I|}{N}. \tag{13}$$

4.8. Perception-Based Image Quality Evaluator (PIQE). Calculate the PIQE score for an image and the distorted images that go with it. Display the results along with the image that corresponds to them. Determine the PIQE score of an image that has been altered by blocking artifacts and Gaussian noise.

4.9. Blind/Referenceless Image Spatial QUality Evaluator (BRISQUE). BRISQUE compares the output image to a default model computed from original images with similar aberrations. A lower score denotes higher perceptual quality. Using the default model, compute the BRISQUE score for an original image and its deformed copies.

Table 2 shows the better comparative performances of CC, PSNR, and MSE compared with previous works. This

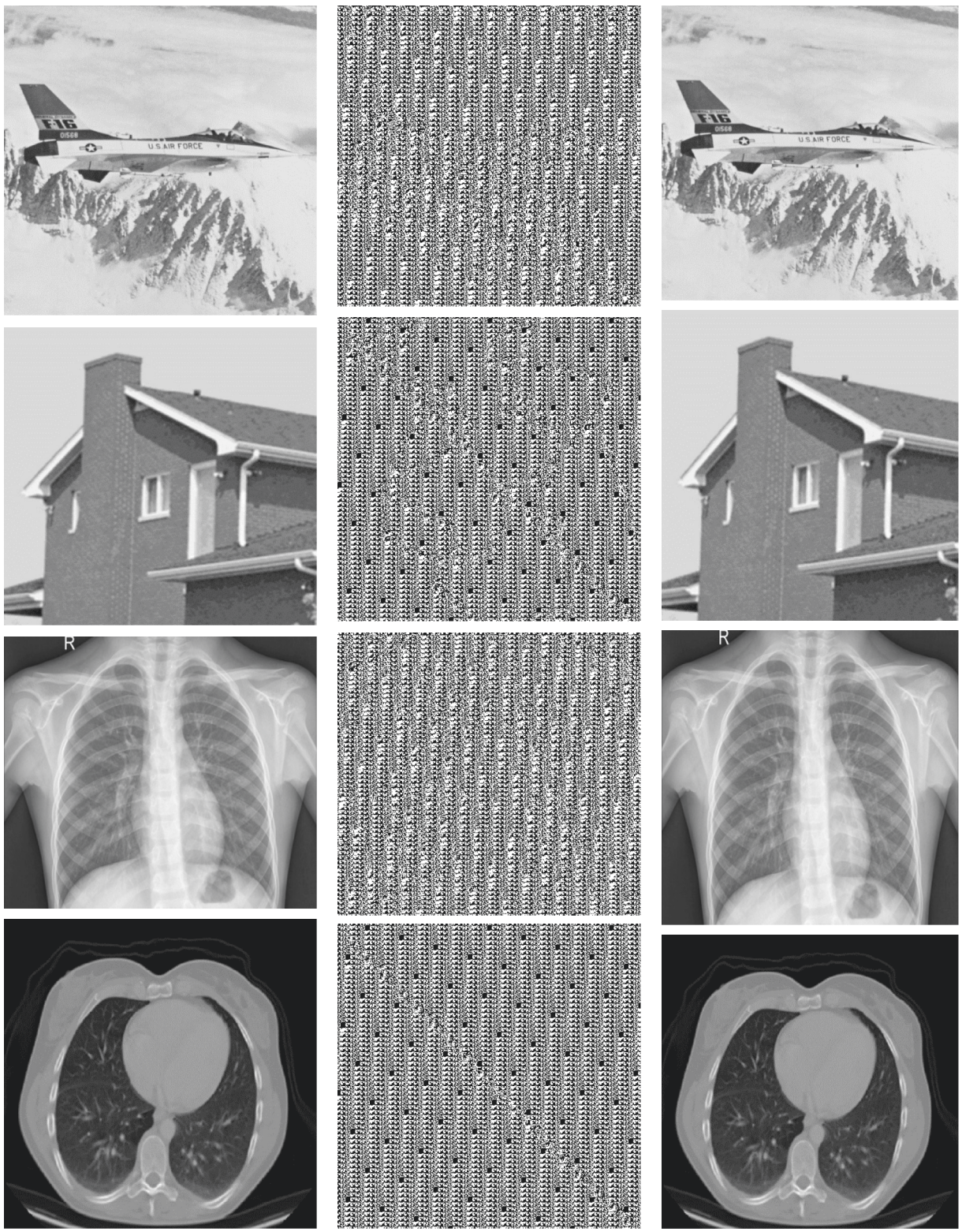


Figure 4: (a) Input sample images. (b) Encrypted images. (c) Decrypted images.

work has enhanced CC, PSNR, and lower MSE compared to other previous methods. GI has 0.02 of CC, 46.25 of PSNR, 0.37 of MSE, 0.63 of SSIM, 0.67 of MAE, and 0.076 of RMSE. Double Phase Encryption (DPE) gives 0.19 of CC, 49.29 of PSNR, 0.42 of MSE, 0.79 of SSIM, 0.49 of MAE, and 0.145 of RMSE. Diffractive Imaging (DI) returns 0.14 of CC, 36.78 of

Table 1: Dataset description.

Dataset	Name of the dataset	Number of images
[24]	Standard dataset	17
	Leaf Shapes	10
	FG-NET Facial Aging	50
	JAFFE	125
	FacialExpression	
[25]	CT images	8057
	X-ray images	9544

Table 2: Comparative performance of previous works.

Method	CC	PSNR	MSE	SSIM	MAE	RMSE
GI [1]	0.02	46.25	0.37	0.63	0.67	0.076
DPE [2]	0.19	49.29	0.42	0.79	0.49	0.145
DI [7]	0.14	36.78	0.024	0.46	0.17	0.13
GS [9]	0.64	39.4	0.076	0.83	0.35	0.19
CGI [23]	0.46	49.53	0.035	0.73	0.16	0.095
This work	0.99	28.53	0.0056	0.99	0.015	0.056

PSNR, 0.024 of MSE, 0.46 of SSIM, 0.17 of MAE, and 0.13 of RMSE. Grayscale (GS) has 0.64 of CC, 39.4 of PSNR, 0.076 of MSE, 0.83 of SSIM, 0.35 of MAE, and 0.19 of RMSE. Computational Ghost Imaging (CGI) has 0.46 of CC, 49.53 of PSNR, 0.035 of MSE, 0.73 of SSIM, 0.16 of MAE, and 0.095 of RMSE. Finally, this work has 0.99 of CC, 28.53 of PSNR, 0.0056 of MSE, 0.99 of SSIM, 0.015 of MAE, and 0.056 of RMSE.

Figure 5 shows the comparative performance like CC, MSE, SSIM, MAE, and RMSE of the proposed method. Figure 6 shows the comparative performance of CC based on the noise density.

Figure 7 shows the performance comparison for encryption: (a) MSE, (b) PSNR, (c) SSIM, (d) RMSE, (e) CC, and (f) MAE based on the rotation angle in degree with different images such as Cameraman, Lena, mandrill, and pout. Figure 8 depicts the performance comparison of encryption: (a) MSE, (b) PSNR, (c) SSIM, (d) MAE, (e) RMSE, (f) PIQE, (g) BRISQE, and (h) CC based on distortion with Cameraman, Lena, mandrill, and pout. When compared to other images, Cameraman images have a high CC value.

The ability to recreate a plain picture with a pleasing aesthetic appearance should be provided by a successful encryption method if an encrypted image is smeared by noise or loses some data during transmission. Figure 9 shows the performance of the decrypted picture after being blurred by Salt and Pepper noise at densities of 0.005, 0.01, 0.015, and 0.02, as well as the performance of the encrypted image after being blurred.

4.10. The Histogram Analysis. Figure 10 depicts the greyscale histograms of (a) Cameraman, (b) Lena, (c) mandrill, and (d) pout and their encrypted picture based on a statistical analysis of the original image and the encrypted image. When the histograms are compared, it is observed that the original image's pixel values are focused on a few values, but

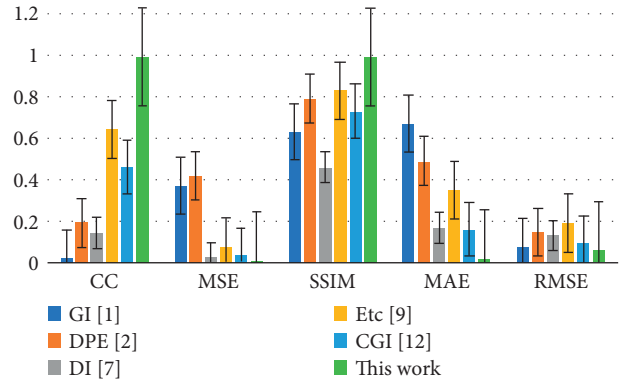


Figure 5: Comparative performance of the proposed method.

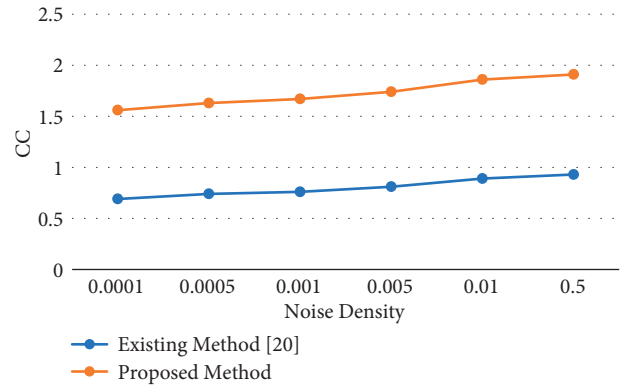


Figure 6: Comparative performance of CC.

the distribution of the encrypted image's pixel values is more uniform.

This work used Cameraman, Lena, mandrill, and pout standard images. Variance of input, encrypted, and decrypted images are measured to evaluate the performance. For better performance, a less value of histogram variance should be obtained. As shown in Table 3, this work obtained less histogram variance when compared to [23, 24]. Also, the input and output histogram values should match.

4.11. Key Sensitivity Analysis. Image encryption technique is sensitive to the initial values of the secret key. Key sensitivity analysis of the image coding technique was done. Table 4 shows the key sensitivity analysis performance of original and encrypted images. Here, key sensitivity, CC, SD, arithmetic mean, and MSE are evaluated. Key sensitivity for various images ranges from 0.6 to 0.7. Also, the CC value for the encrypted image is evaluated for different images. Less CC between input and encrypted images shows the highest performance. Similarly, SD, mean, and MSE values are evaluated as shown in Table 3.

Table 5 shows the performance of computation time for various images. The computation time for encryption and decryption varies concerning pixel deviation and texture pattern.

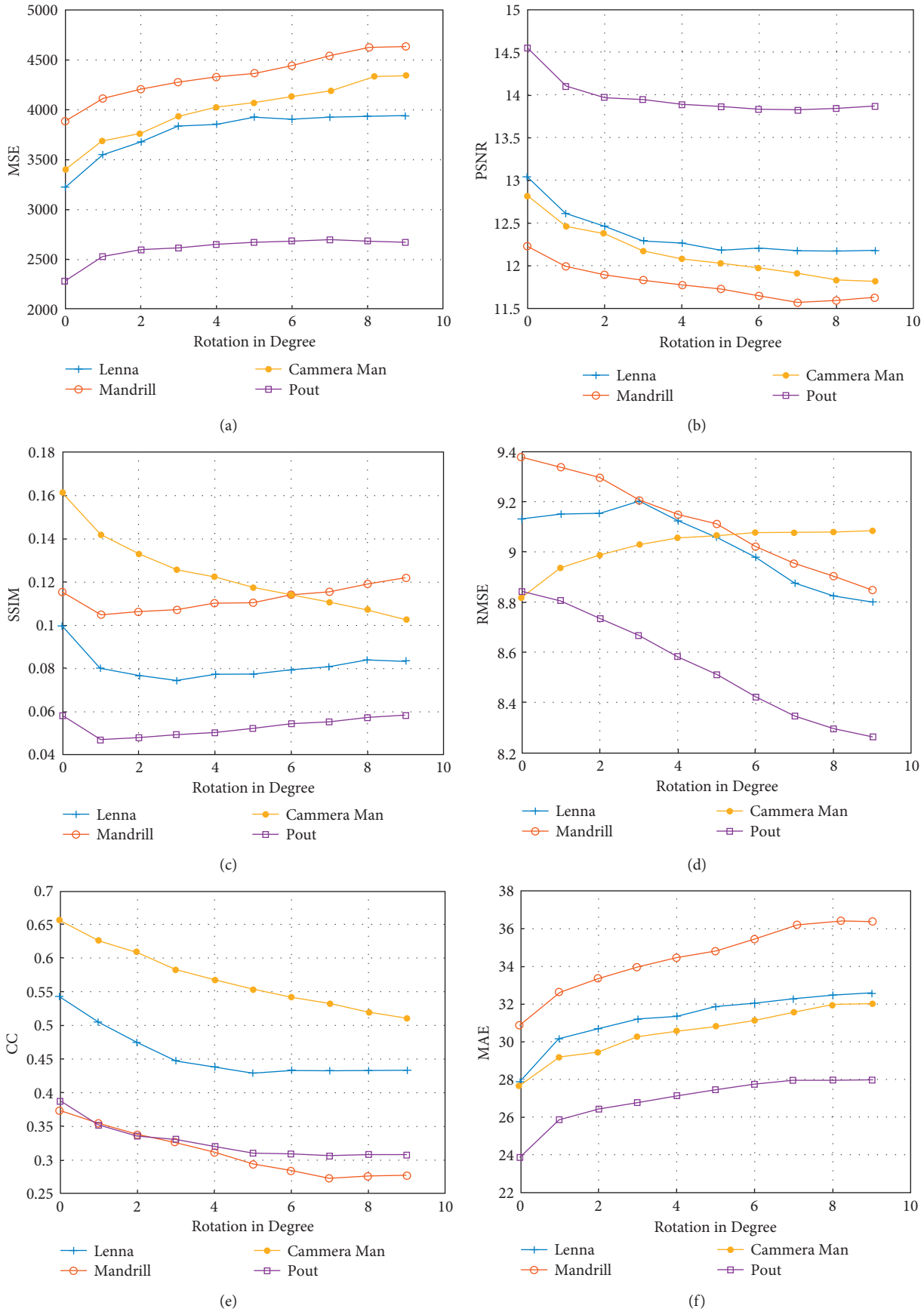


Figure 7: Performance comparison: (a) MSE, (b) PSNR, (c) SSIM, (d) RMSE, (e) CC, (f) and MAE based on rotation in degree.

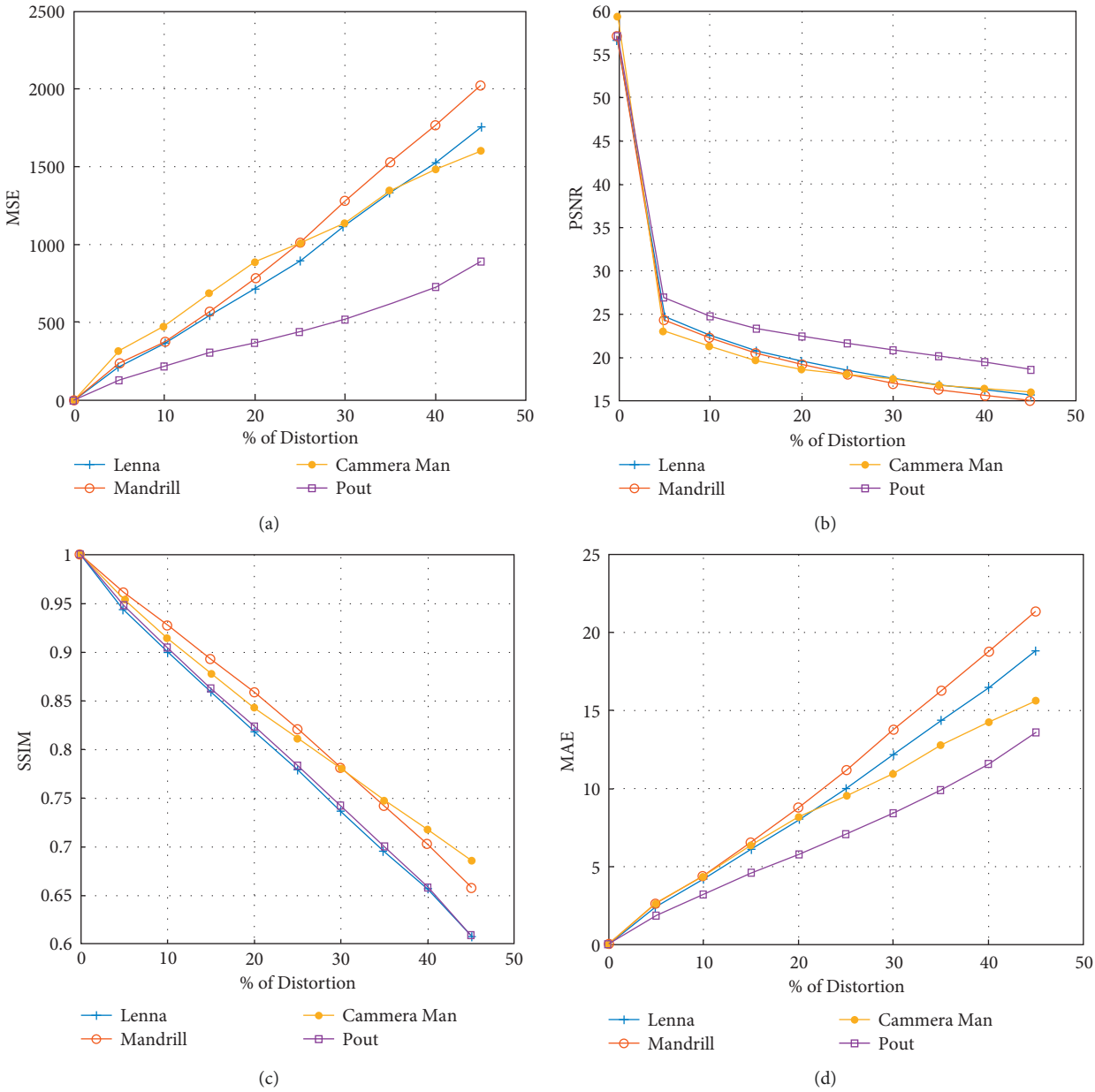


Figure 8: Continued.

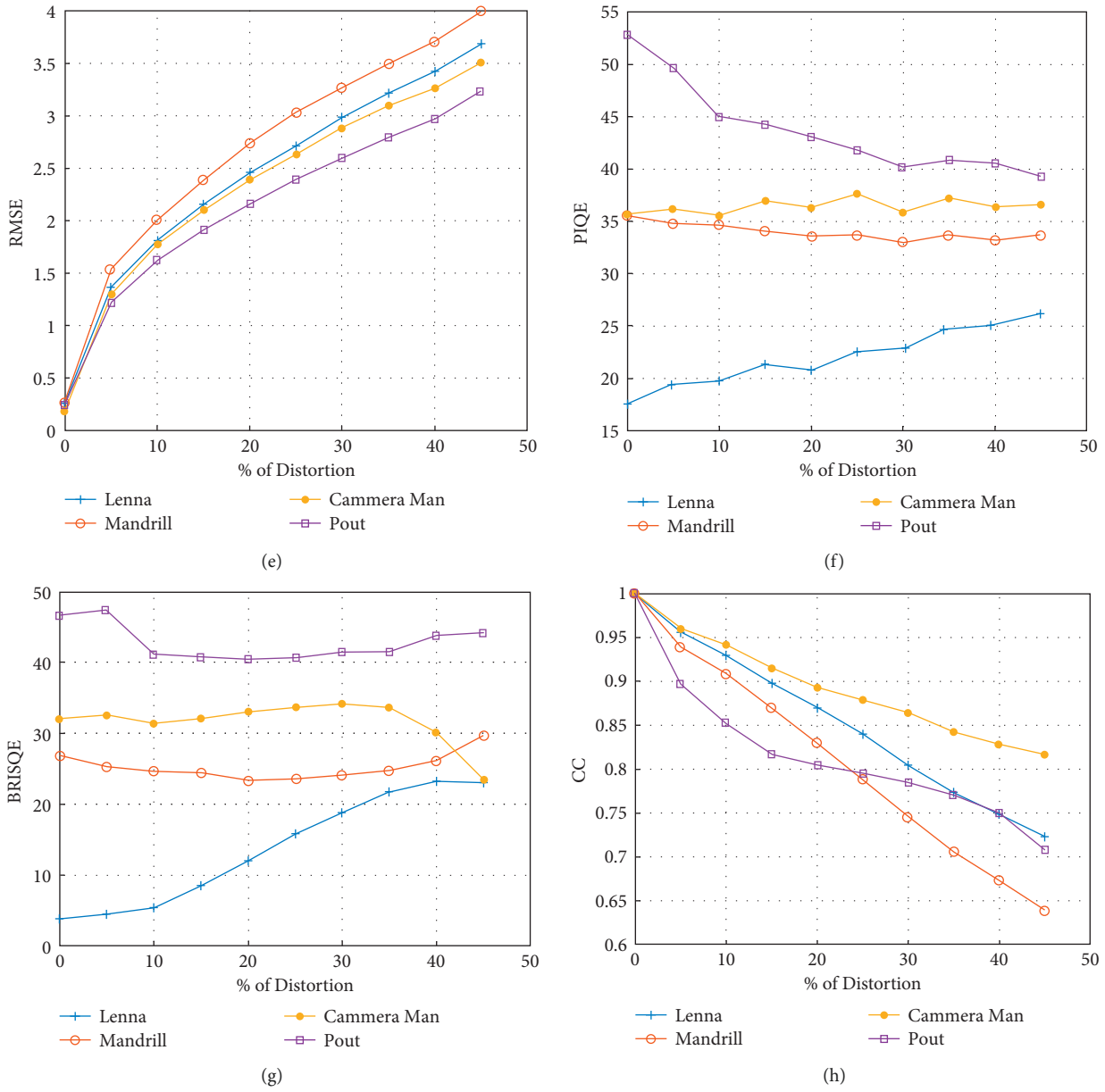


Figure 8: Performance comparison: (a) MSE, (b) PSNR, (c) SSIM, (d) MAE, (e) RMSE, (f) PIQE, (g) BRISQE, and (h) CC based on distortion.

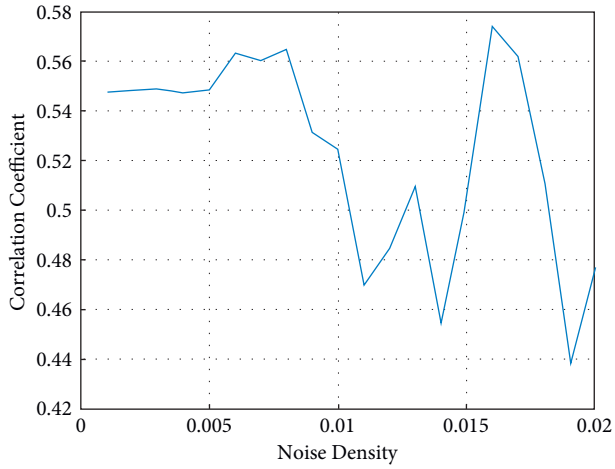
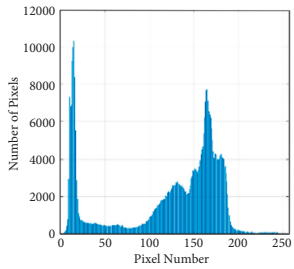
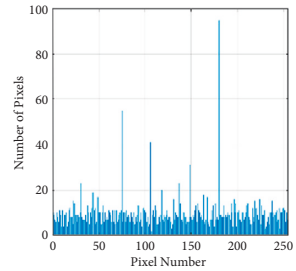
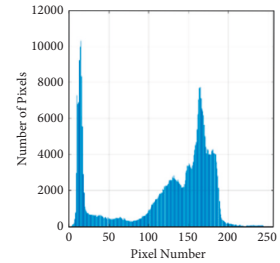


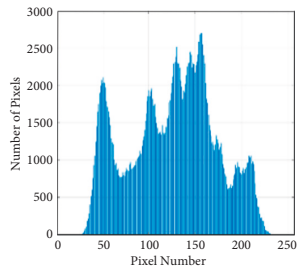
Figure 9: Performance comparison based on noise density.

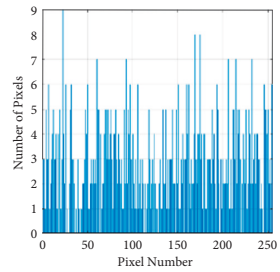



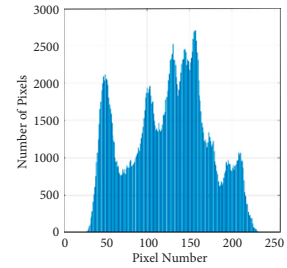
HV = 110970


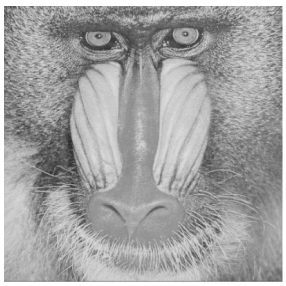
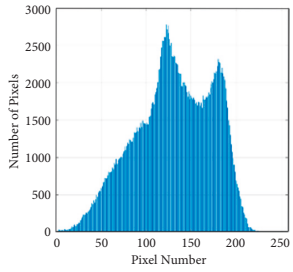
HV = 325.23


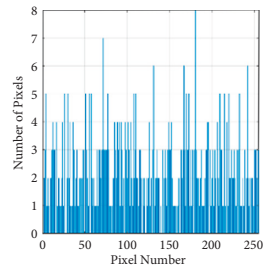
HV = 110970

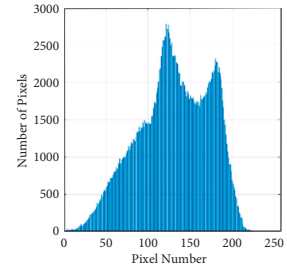


HV = 633400


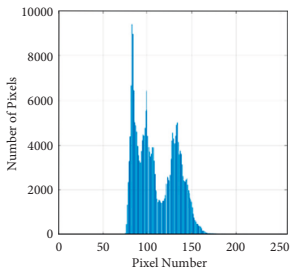
HV = 653.32


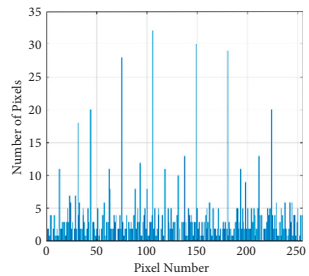
HV = 633400



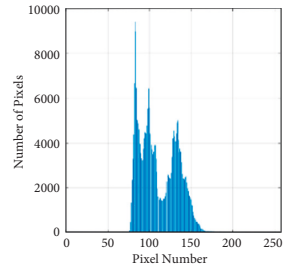
HV = 569847


HV = 562.12


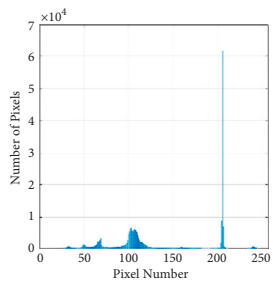
HV = 569847

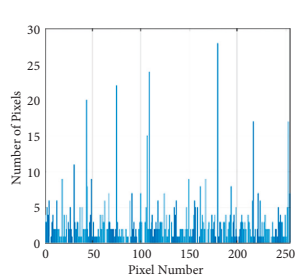


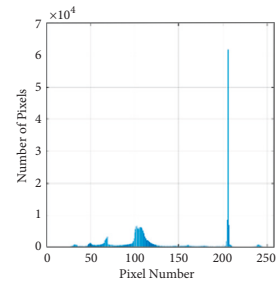
HV = 452036


HV = 562.12


HV = 452036



HV = 394671


HV = 347.13


HV = 394671

(a) Continued.

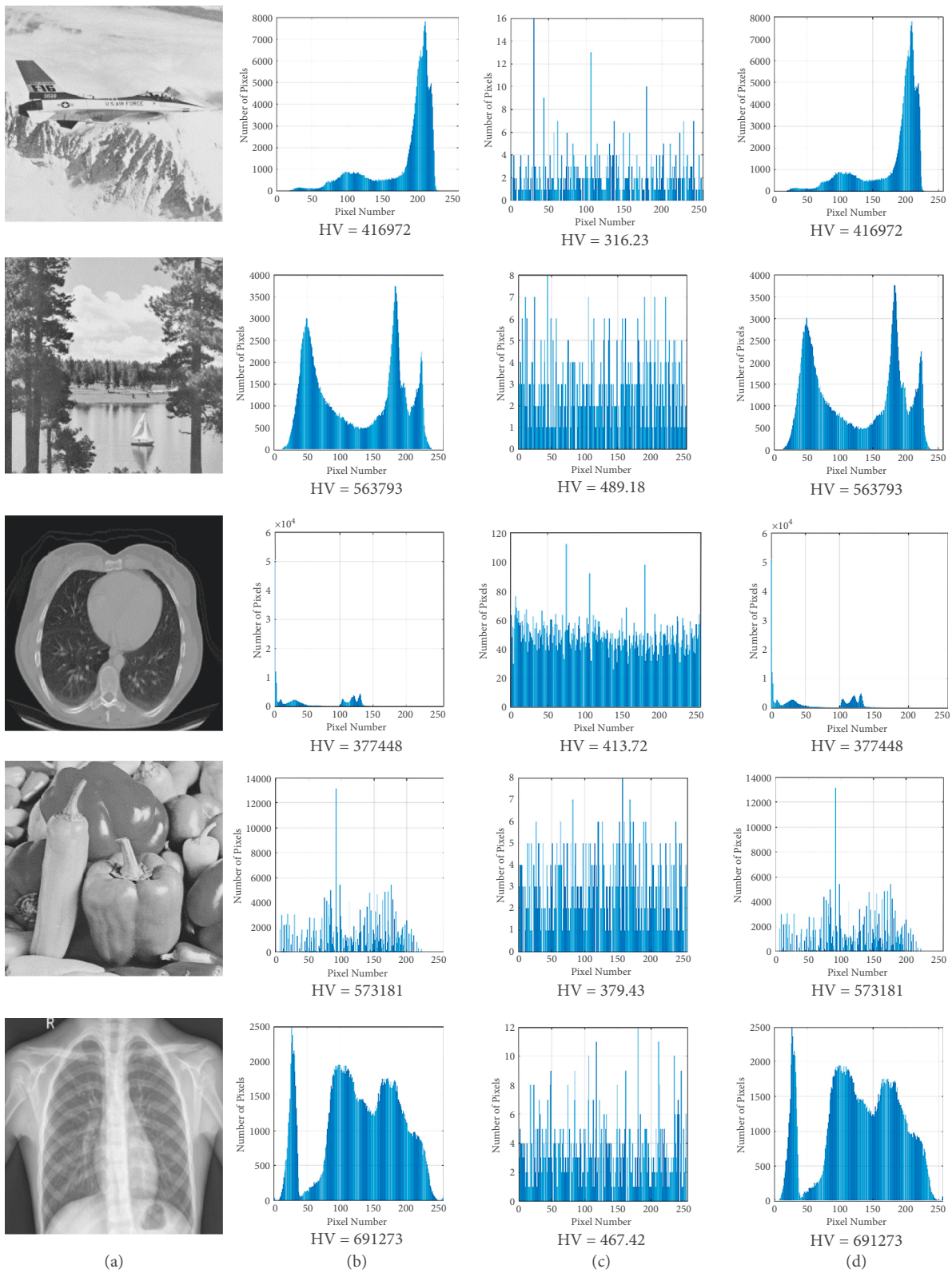


Figure 10: (a) Input image, (b) input histogram, (c) encrypted image histogram, and (d) output image and histogram.

Table 3: Histogram variance.

Algorithms	Images	Original	Encrypted	Decrypted
This work	Cameraman (512 × 512)	110970	325.23	110970
	Mandrill (512 × 512)	569847	562.12	569847
	Lena (512 × 512)	633400	653.32	633400
	Pout (512 × 512)	452036	235.23	452036
	Avg. of 650 images (512 × 512)	509632	250.12	509632
[23]	Lena	633400	1026.23	633400
[26]	Lena	452036	1065.69	452036

Table 4: Performance of original and encrypted image.

	Key sensitivity analysis	CC	Standard deviation (SD)	Mean	MSE
Cameraman	0.7	0.003	0.83	2.13	0.23
Mandrill	0.6	0.009	0.74	7.45	0.42
Lena	0.8	0.002	0.79	1.12	0.84
Pout	0.6	0.0018	0.81	3.45	0.79

Table 5: Performance of computational time.

	Encrypted image (sec)	Decrypted image (sec)	Total time (sec)
Cameraman	15	44	59
Mandrill	35	61	96
Lena	12	54	66
Pout	23	38	61

Table 6: Chi-square test analysis.

Algorithms	Images	X^2_{test}
This work	Cameraman	230.25
	Mandrill	231.65
	Lena	230.12
	Pout	230.55
[23]	Lena	236
[26]	Lena	252.47

Table 7: Performance of original and encrypted image for all images.

Key sensitivity	HV			CC	SD	Mean	MSE	RMSE	PSNR
	Original	Encrypt	Decrypt						
0.6	369741	325.23	369700	0.010	0.96	4.15	0.72	0.97	83.71
0.7	128567	562.12	128498	0.017	0.38	7.45	0.64	0.75	80.46
0.8	759814	653.32	759804	0.020	0.71	3.72	1.20	1.98	75.01
0.9	317896	235.23	317896	0.008	0.91	2.17	0.98	0.57	98.15

4.12. Chi-Square Test. Table 6 shows the Chi-square test analysis for various images and various techniques. Here, the security level of encrypted images can be evaluated by using Chi-square values. Fewer values of Chi-square values give a better security level. In this work, the proposed work provides high Chi-square values when compared with previous works [23, 26].

Table 7 shows the performance of original and encrypted images for all images. The key sensitivity of 0.6 achieves 369741 of original image, 325.23 of encrypted image, and 369700 of decrypted image for HV and 0.010 of CC, 0.96 of standard deviation, 4.15 of mean, 0.72 of MSE, 0.97 of RMSE, and 83.71 of PSNR. The key sensitivity of 0.7 gets 128567 of original image, 562.12 of encrypted image, and 128498 of decrypted image for HV, 0.017 of CC, 0.38 of standard deviation, 7.45 of mean, 0.64 of MSE, 0.75 of RMSE, and 80.46 of PSNR. The key sensitivity of 0.9 has 317896 of original image, 235.23 of encrypted image, 317896

of decrypted image for HV, 0.008 of CC, 0.91 of standard deviation, 2.17 of mean, 0.98 of MSE, 0.57 of RMSE, and 98.15 of PSNR.

5. Conclusions

This study suggested an optical encryption technique in the GT domains utilizing DCT and quantization in the field of information security. It provided a novel notion of the GT encryption method coupled with image encryption. Block-level GT is applied in this work to perform the image encryption process. Secret information hiding is performed in the DCT domain. To save the data from noise attacks, the binary bits are inserted into the DC coefficients of the 8×8 DCT blocks. To improve the security level of encryption, dynamic angle values are used with means gradient difference-based techniques. This work improves the performance in terms of quality and security level. This work achieved an average of 45.6 dB PSNR and 0.965 of SSIM for various images.

Data Availability

The data that support the findings of this study are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The research and publication of this paper were funded by LBSCST.

References

[1] L. Zhang, X. Yuan, K. Wang, and D. Zhang, "Multiple-image encryption mechanism based on ghost imaging and public key cryptography," *IEEE Photonics Journal*, vol. 11, no. 4, pp. 1–14, 2019.

[2] W. Zamrani, A. Esmail, A. Nawfel, E. G. Hassan, and S. Tayeb, "Optical double phase encryption and spreading technique applied to color image," in *Proceedings of the 2016 15th Workshop on Information Optics (WIO)*, IEEE, Barcelona, Spain, November 2016.

[3] Y. Qin, Q. Gong, and Z. Wang, "Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme," *Optics Express*, vol. 22, pp. 21790–21799, 2014.

[4] M. Z. LiXiaowei, M. Zhao, X. Yan et al., "Optical encryption via monospectral integral imaging," *Optics Express*, vol. 25, no. 25, p. 31516, 2017.

[5] L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie, "An asymmetric color image encryption method by using deduced gyrator transform," *Optics and Lasers in Engineering*, vol. 89, pp. 72–79, 2017.

[6] L. Zhang, R. Xiong, J. Chen, and D. Zhang, "Optical image compression and encryption transmission-based ondeep learning and ghost imaging," *Applied Physics B*, vol. 126, no. 1, p. 18, 2020.

[7] L. Zhou, Y. Xiao, and W. Chen, "Vulnerability to machine learning attacks of optical encryption based on diffractive imaging," *Optics and Lasers in Engineering*, vol. 125, Article ID 105858, 2020.

[8] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.

[9] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for jpeg images," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1515–1525, 2018.

[10] K. Yi, Z. Leihong, and Z. Dawei, "Optical encryption based on ghost imaging and public key cryptography," *Optics and Lasers in Engineering*, vol. 111, pp. 58–64, 2018.

[11] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Processing*, vol. 148, pp. 41–47, 2018.

[12] M. J. Saeed, "A new technique based on chaotic steganography and encryption text in DCT domain for color image," *Journal of Engineering Science & Technology*, vol. 8, no. 5, pp. 508–520, 2013.

[13] Y. Liang, G. Liu, N. Zhou, and J. Wu, "Color image encryption combining a reality-preserving fractional DCT with chaotic mapping in HSI space," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 6605–6620, 2016.

[14] Y. Liang, G. Liu, N. Zhou, and J. Wu, "Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion," *Journal of Modern Optics*, vol. 62, no. 4, pp. 251–264, 2015.

[15] L. Sui, M. Xu, C. Huang, A. Adhikari, A. Tian, and A. Asundi, "Multiple-image encryption by space multiplexing based on vector quantization and interference," *OSA Continuum*, vol. 1, no. 4, p. 1370, 2018.

[16] M. H. Shirafkan, A. Ehsan, and J. Vahidi, "An image steganography scheme based on discrete wavelet transform using lattice vector quantization and reed-solomon encoding," in *Proceedings of the 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, IEEE, Barcelona, Spain, November 2015.

[17] J. Chen, Z. L. Zhu, L. B. Zhang, Y. Zhang, and B. Q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 2018.

[18] H. Chen, C. Tanougast, Z. Liu, W. Blondel, and B. Hao, "Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform," *Optics and Lasers in Engineering*, vol. 107, pp. 62–70, 2018.

[19] M. R. Abuturab, "Multiple information encryption by user-image-based gyrator transform hologram," *Optics and Lasers in Engineering*, vol. 92, pp. 76–84, 2017.

[20] H. Chen, Z. Liu, C. Tanougast, F. Liu, and W. Blondel, "A novel chaos based optical cryptosystem for multiple images using DNA-blend and gyrator transform," *Optics and Lasers in Engineering*, vol. 138, Article ID 106448, 2021.

[21] L. Sui, M. Xu, and A. Tian, "Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain," *Optics and Lasers in Engineering*, vol. 91, pp. 106–114, 2017.

[22] Y. Wei, A. Yan, J. Dong, Z. Hu, and J. Zhang, "Optical image encryption using QR code and multilevel fingerprints in gyrator transform domains," *Optics Communications*, vol. 403, pp. 62–67, 2017.

[23] S. Sun, Y. Guo, and R. Wu, "A novel plaintext-related image encryption algorithm based on stochastic signal insertion and block swapping," *IEEE Access*, vol. 7, pp. 123049–123060, 2019.
[24] https://www.imageprocessingplace.com/root_files_V3/image_databases.htm.
[25] https://www.kaggle.com/datasets/ssarkar445/covid-19-xray-and-ct-scan-image-dataset.
[26] L. Wang, S. Zhao, W. Cheng, L. Gong, and H. Chen, "Optical image hiding based on computational ghost imaging," *Optics Communications*, vol. 366, pp. 314–320, 2016.
[27] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324–332, 2017.