A Chaotic Clifford Attacker Map-based Image Encryption in Double Random Phase Encoding

ABSTRACT

Encryption is the most useful technique used for the security of data during storage and transmission. A well-known encryption scheme called Double Random Phase encoding was introduced by Refregier and Javidi. But due to its linear nature, this scheme has been proven vulnerable against Known plaintext and chosen plaintext attacks. Here in this paper, we propose a chaotic map-based nonlinear encryption scheme that enhances the security of the DRPE encryption scheme for images. Clifford attacker is a non-linear chaotic map that has four parameters and two initial values. This map is highly sensitive to these values. Therefore, these parameters and initial values work as extra secret keys. MATLAB simulation shows that the proposed technique enhances the security level of the DRPE and at the same time has a better immunity to noise and occlusion attacks.

Keywords: Encryption, Chaotic map, DRPE, Clifford attacker map, Sensitivity analysis

1. INTRODUCTION

In the current era of technology, the problem of the security of data has augmented. Most of the data transmitted via the internet are in the form of photos and videos. We always want to secure our data during its transmission. Even though there are a variety of security features available, image encryption is particularly important for protecting data in the form of images. Advanced encryption standards (AES) and data encryption standards (DES) are two types of digital image encryption algorithms that have been created [1,2]. However, digital encryption solutions have drawbacks such as computing complexity, time consumption, and sequence algorithm. These methods may be breakable once high-performance computing devices become available. To overcome these limitations, people all over the world are becoming increasingly interested in optical cryptosystems. As these optical cryptosystems have inherent properties such as large information capacity, parallel processing, low computational complexity, multiple parameters such as wavelength amplitude focal length, which also serves as an extra encryption key, and high speed.

After an optical encryption scheme based on double random phase encoding proposed in [3], optical technologies have become increasingly attractive for the security of information. Random phase masks are employed in both the spatial and Fourier domains to encrypt an input image to stationary white noise in DRPE-based optical schemes. [4,5] demonstrated that the Double Random Phase Encryption technique is resistant to noise introduced into the encrypted image. DRPE-based schemes were further investigated and enhanced by many researchers using different transformations namely fractional Fourier, Fresnel domain, and Hartley transformation [6,7,8,9]. Further, it was found that all these DRPE-based schemes are symmetric and linear. Due to symmetric and linear, cryptoanalysis of these schemes shows that these schemes are vulnerable to some attacks [10,11,12]. To resist these attacks, a nonlinear chaotic map-based encryption scheme was introduced [13,14,15,16,17]. Elshamy et al. [14] developed a system based on the use of a chaotic baker map as a preprocessing layer to allow for pixel randomization, followed by the use of a double random phase encoding layer. To improve the security of the DRPE Scheme, Sharma et al. [16] adopted the 3-D Lorenz system in the Fourier domain. Many other encryption schemes using chaotic maps in different ways to make more secure encryption schemes are discussed in [20,21,22,23].

Chaotic maps have a wide range of applications in the field of cryptography due to their qualities such as uncertainty in prediction, the sensitivity of parameter and beginning values, unpredictable behavior, and many more, Sensitivity of the parameter is a very strong property of chaotic maps, therefore, these parameters can be used as encryption keys. Clifford attacker map is one of the most sensitive chaotic maps which is used in [18,19]. In this paper, we will also use this map for pixel randomization.

In section 2, we discuss the methodology used. The strength of the encryption scheme and robustness against different attacks are discussed in section 3. The paper is concluded in sections 4 and 5 followed by a reference.

2. Material and Methods

2.1 Double Random Phase Encoding:

The DRPE approach proposed in [3] is based on altering an image's intensity distribution. This is accomplished by the use of random phase masks, which result in an encrypted image. We can't decrypt the encrypted image into the original image without any information about the alteration. The input image is first multiplied by a random phase mask (RPM1), after that it is subjected to a Fourier transformation. In the Fourier domain, another random phase mask (RPM2) is applied to the converted image, followed by a second Fourier transformation, yielding into the encrypted image.
Here RPM1 and RPM2 are defined as follows

$$RPM1 = \exp\left(2\pi i m(x, y)\right)$$
$$RPM2 = \exp\left(2\pi i n(x, y)\right)$$

Mathematically, we can write this encryption process as:

$$e(x, y) = FT(FT(I(x, y) * RPM1) * RPM2)$$

Where $I(x, y)$ is the input image and RPM1 and RPM2 are random phase mask 1 and random phase mask 2 respectively. In the decryption procedure, the inverse Fourier transformation of an encrypted image is multiplied by the complex conjugate of the second random phase mask and then the image is subjected to another inverse Fourier transformation. As a result, the output is

$$IFT\left(IFT\left(e(x, y)\right) * abs(RPM2)\right) = I(x, y) * RPM1$$

whose absolute value turns out to be the decrypted image $I(x, y)$.

The elements which are used to encrypt an input image are called encryption keys and the elements which are used to decrypt the encrypted image are called decryption keys. Here RPM1 and RPM2 are encryption keys. The complex conjugate of RPM2 serves as the decryption key,

Diagrammatically, the whole process of encryption and decryptions is shown below:

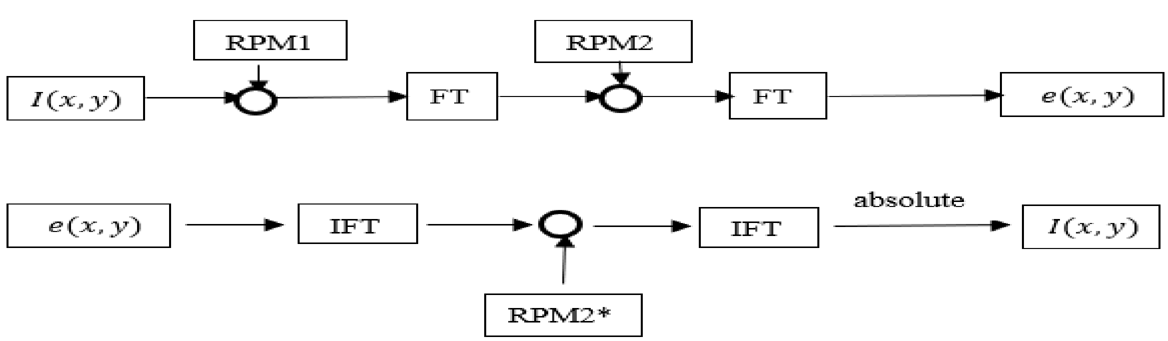


Fig. 1. **Encryption and decryption process of DRPE**

2.2 Clifford attacker map

Clifford attacker map is a two-dimensional chaotic map that generates a sequence of random numbers. This map is used as a tool to enhance the security of the encryption scheme by pixel randomization of the transformed image in the Fourier domain. Mathematically, this map is written as:

$$x_{n+1} = \sin(ay_n) + c\cos(ax_n)$$

$$y_{n+1} = \sin(bx_n) + d\cos(by_n)$$

where a, b, c, d are the parameters and x_0, y_0 are the initial values of this map. These parameters and initial values of this map are highly sensitive. As a result, these values serve as encryption keys in this system. In this paper, the values of parameters a=1.5, b=-1.8, c=1.6, d=0.9 and initial values $x_0 = 0.14$ and $y_0 = 0.15$ are used. The bifurcation diagram of the Clifford map as shown in figure 2 is obtained by taking 66,000 iterations to generate a random sequence of numbers.

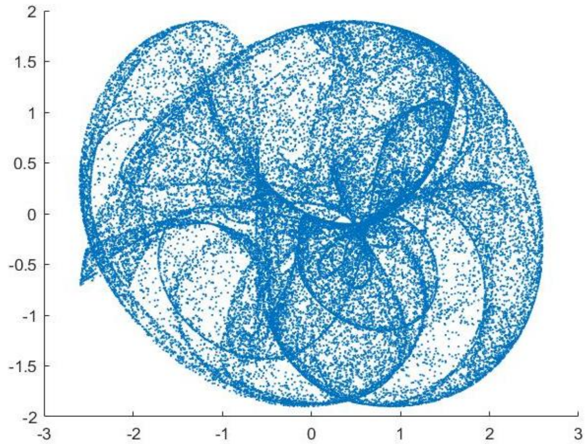


Fig. 2. Bifurcation diagram of Clifford attacker map

2.3 Proposed encryption scheme

The proposed encryption scheme is based on the pixel randomization of the image in the Fourier domain. The following is a description of how the Clifford attacker map is implemented in the DRPE scheme:

1. Consider the MN-pixel input image $I(x, y)$.
2. The first random phase mask RPM1 is implanted in the input image, and Fourier processing is done to it.
3. Divide the previous step's resultant image into smaller blocks and transform each one into a vector format.
4. Using the Clifford attacker map, a sequence of random integers is created and sorted in ascending order.
5. Sort the vector you got in step 3 with the vector you got in step 4.
6. Resize the image MN by reshaping the vector produced in step 5.
7. The resulting image is subjected to the second layer of DRPE in which the obtained image is multiplied by a second random phase mask and further Fourier transform is performed, yielding an encrypted image.
8. The decryption process is the inverse of the encryption process in order to recover the original image from the encrypted image.

Along with the keys used in the DRPE scheme, parameters and initial values of the Clifford attacker map work as both encryption and decryption keys for the proposed scheme. The same is also mentioned in Table 2. The whole process of encryption and decryption of the proposed scheme is displayed in figure 3.

By implementing the proposed encryption scheme on an input image, we get extra security for an encrypted image in comparison to the DRPE scheme. In the DRPE scheme, an attacker can retrieve the second random phase mask RPM2. But in the proposed scheme even if the attacker retrieves RPM2 still he won't be able to retrieve the parameters of the Clifford map which works as an extra security level.

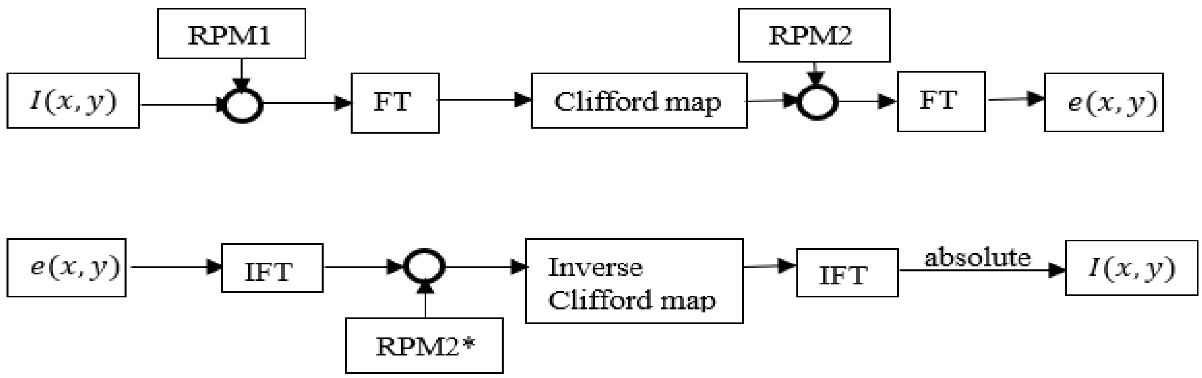
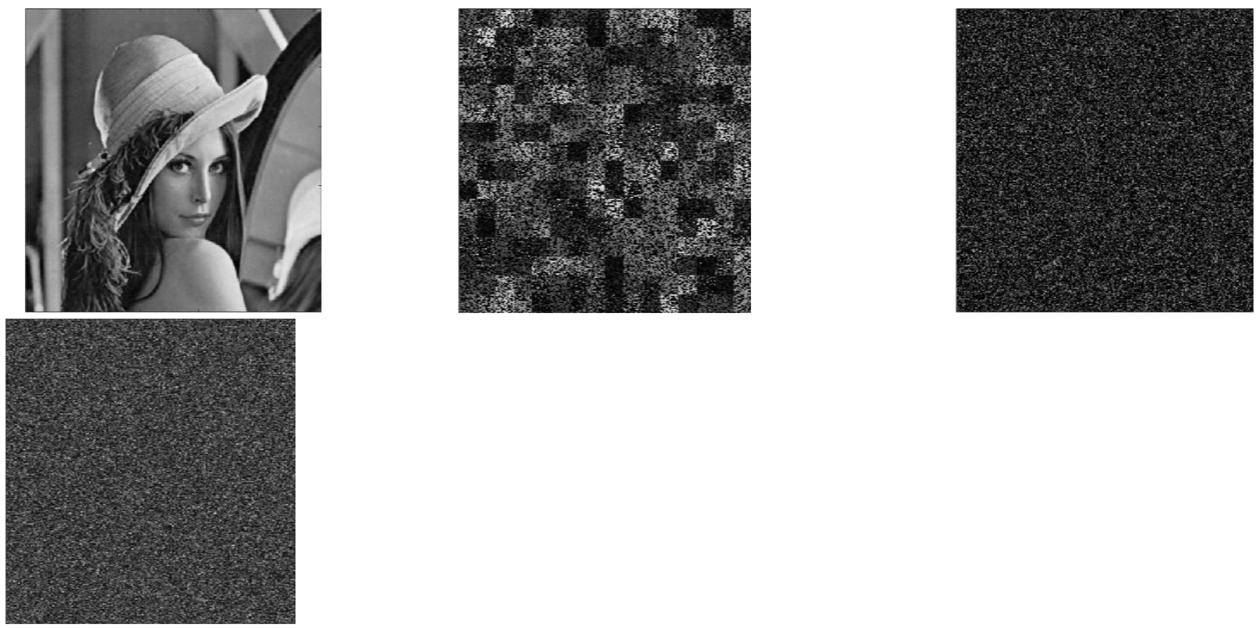
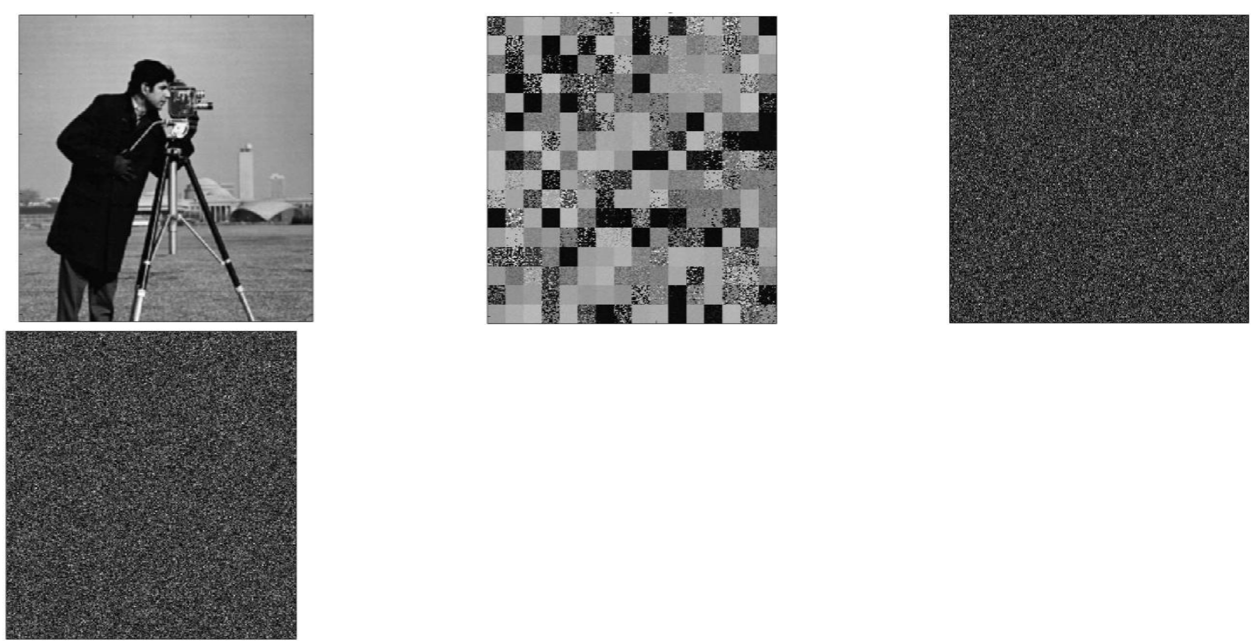


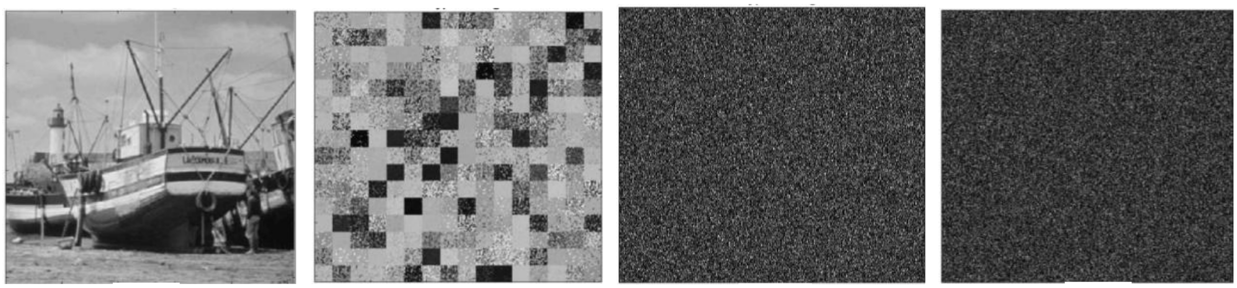
Fig. 3. Encryption and decryption process of the proposed scheme



(a) (b) (c) (d)



(e) (f) (g) (h)



(i) (j) (k) (l)

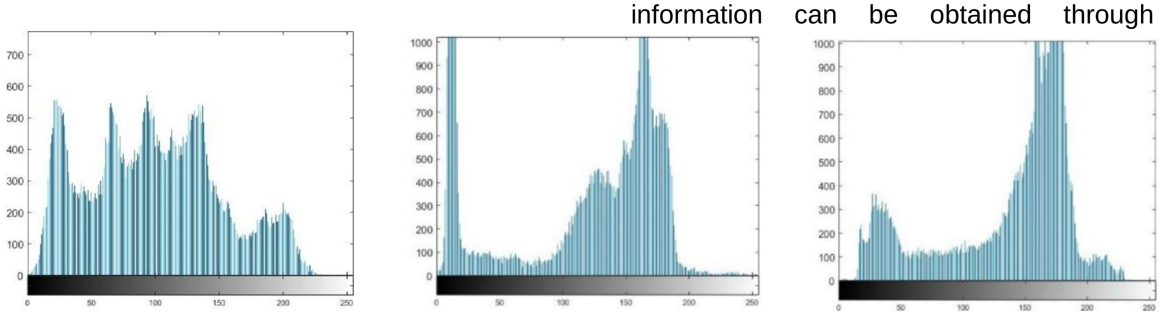
Fig. 4. Scheme validation results; (a,e,i) input images and its encrypted images; (b,f,j) using only Clifford attacker map; (c,g,k) using Double Random Phase Encoding scheme; (d,h,l) using proposed scheme of girl, cameraman and boat respectively.

3. RESULTS AND DISCUSSION

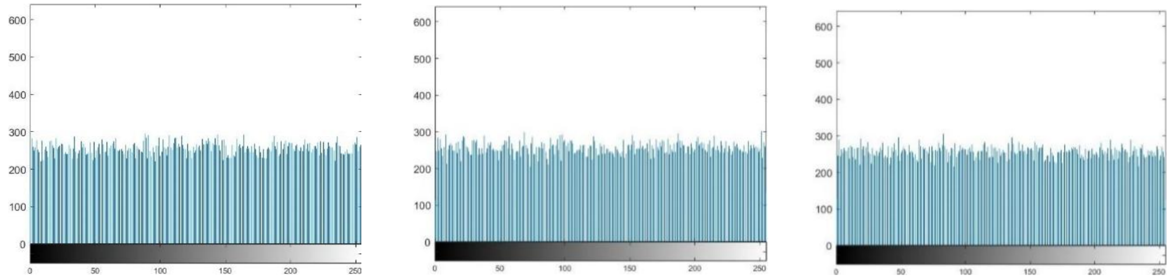
Three grayscale images of a girl, cameraman, and boat with an image size of 256×256 are used to demonstrate the validity of the proposed technique. MATLAB is used to generate the simulation results. In the simulation, the values of parameters of Clifford attacker map a=1.5, b= -1.8, c=1.6, d=0.9 and initial values $x_0 = 0.14$, $y_0 = 0.15$ are used. The validation results of the proposed encryption scheme are shown in figure 4. The validation of the encrypted image is carried out using various statistical analyses like a histogram and 3-D plot analysis, correlation distribution analysis, and information entropy. Later, the sensitivity of parameters is discussed followed by basic occlusion and noise attack.

3.1 Histogram and 3-D plot analysis

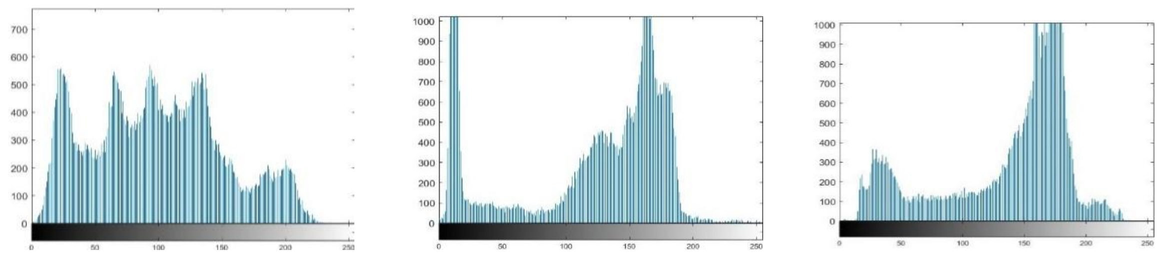
To validate the proposed scheme, histogram analysis has been performed on the input images of the girl, cameraman, and boat. For a better encryption algorithm, the histogram of the encrypted image should be different from the histogram of the original image. Figure (5a-5c) shows the histogram of original images, figure(5d-5f) shows a histogram of encrypted images, and figure (5g-5i) shows a histogram of decrypted images of a girl, cameraman, and boat respectively. It is clear from figure 5 that the histogram of the encrypted image is different from the original image. Pixel values in the histogram of the encrypted image are uniformly distributed i.e., all pixel values have the almost same frequency. Therefore, no statistical information can be obtained through it.



(a) (b) (c)



(d) (e) (f)

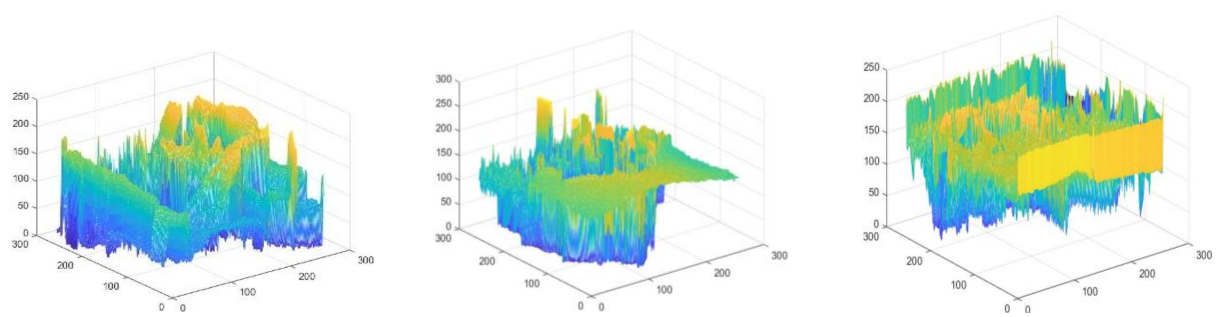


(g) (h) (i)

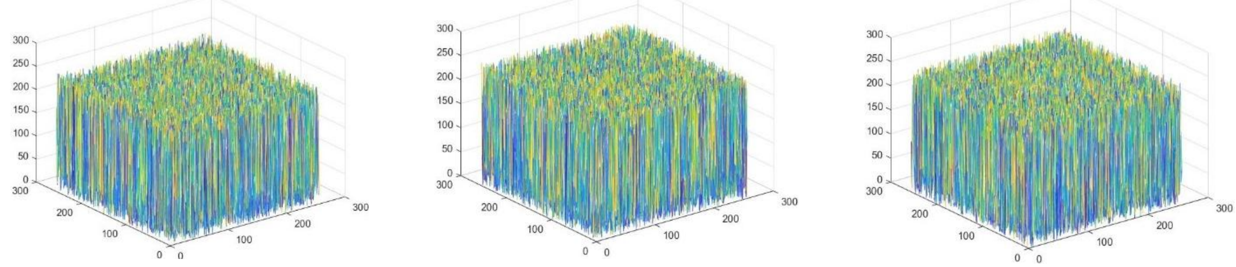
Fig. 5. Histogram of; (a,b,c) input images; (d,e,f) encrypted images; (g,h,i) decrypted images of girl, cameraman and boat respectively.

The presented encryption scheme's efficiency may be evaluated using a 3-D visualization of a girl's image. The 3-D plots of the original images are shown in figure (6a-6c), encrypted images shown in figure (6d-6f), and decrypted images shown in figure (6g-6i) of the girl, cameraman, and boat respectively. Figure 6 clearly shows that the 3-D plot of the encrypted image is randomly dispersed, however, the 3-D plots of the original image and the decoded image are quite similar, demonstrating the effectiveness of the proposed encryption scheme.

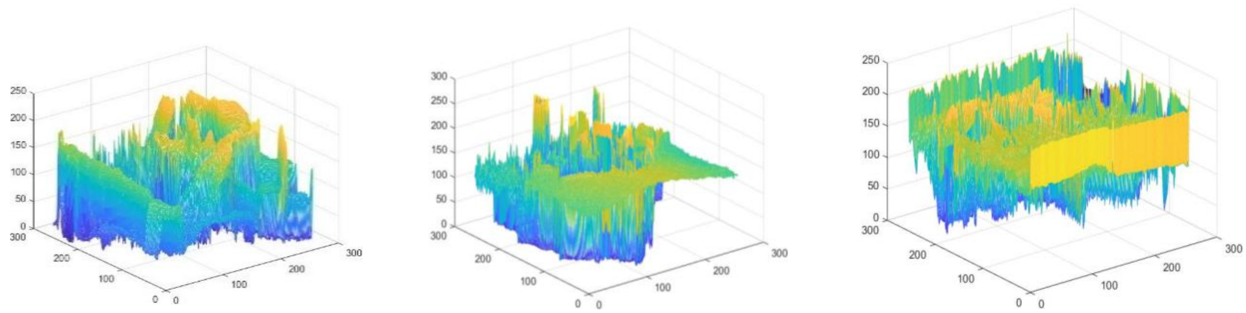
(g) (h)



(a) (b) (c)



(d) (e) (f)



(g) (h) (i)

Fig. 6. 3-D plot of; (a,b,c) input images; (d,e,f) encrypted images; (g,h,i) decrypted images of girl, cameraman and boat respectively

3.2 Correlation distribution analysis

Correlation distribution analysis is another approach to demonstrate the efficiency of an encryption scheme. In the horizontal, vertical, and diagonal directions, we plotted 5,000 pairs of adjacent pixels from the original image and its encrypted image of the girl at random. Figure (7a-7c) shows that neighboring pixels in the input image are substantially connected in all three directions, whereas adjacent pixels in (7d-7f) of the encrypted image have no correlation. Figure (7g-7i) displays the correlation distribution of the retrieved image which is identical to the input image. The comparison clearly shows that the pixels of the encrypted image has lost any correlation, resulting in a random distribution. A similar comparison of correlation distribution plots can be carried out for cameraman and boat images. As shown in table 1, the correlation coefficient between neighboring pixels from the original image and its encrypted image is computed in the horizontal, vertical, and diagonal directions of the girl, cameraman, and boat images. As a result, the proposed scheme is resistant to statistical attacks.

Table 1. The correlation coefficient between adjacent pixels of the input image and their encrypted images in a horizontal, vertical, and diagonal direction

Image	**Type**	**Horizontal direction**	**Vertical direction**	**Diagonal direction**
Girl image	Input image	0.9706	0.9436	0.9192
	Encrypted image	-0.0014	0.0097	0.0024
Cameraman image	Input image	0.9431	0.9722	0.9030
	Encrypted image	-0.0067	0.0082	0.0056
Boat image	Input image	0.9554	0.9518	0.9331
	Encrypted image	-0.0074	0.0055	0.0025

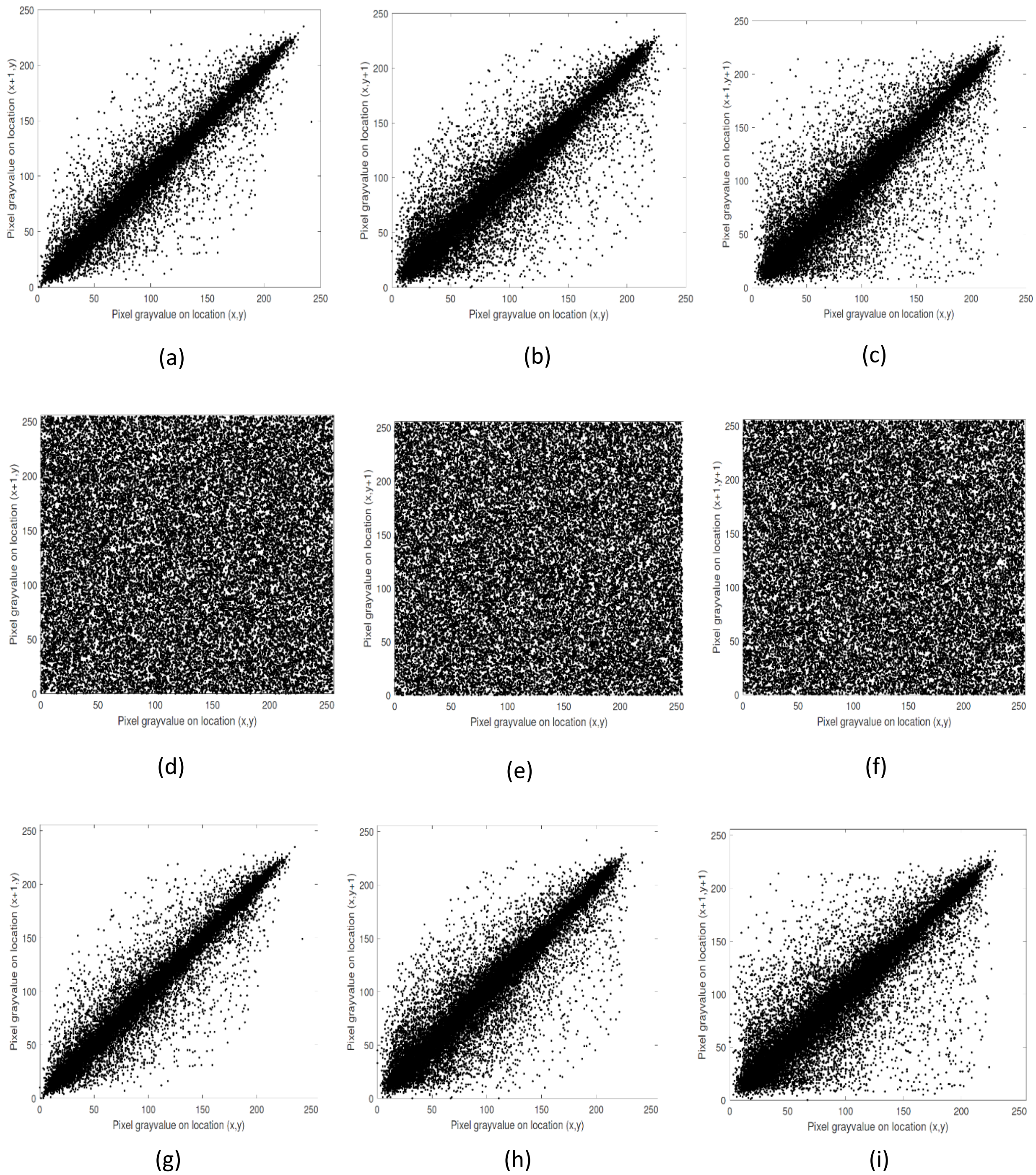


Fig. 7. Correlation distribution plots of pixels of (a-c) input image of girl; (d-f) corresponding encrypted image; (g-i) decrypted image in horizontal, vertical, and diagonal directions respectively.

3.3 Information entropy

The texture of an image can be described using information entropy, which is a statistical measure of unpredictability. The information entropy H(m) of source m, is defined as

$$H(m) = \sum_{k=1}^{256} p(m_k) \log_2 \frac{1}{p(m_k)}$$

Where $p(m_k)$ is the probability of m_k. The entropy of a grayscale image ranges from 0 to 8. The entropy of a grayscale girl, cameraman and boat images are 7.5784, 7.0583 and 7.1622 while its encrypted image using the proposed scheme has an entropy of 7.9956,7.9954 and 7.9956. The result shows that the encrypted image's unpredictability and randomness is increased because its entropy value is extremely close to the grayscale image's maximum value.

3.4 Secret-key sensitivity analysis

If an image encryption technique has highly sensitive secret keys and has a vast key space to avoid brute force attacks, it is said to be ideal. The parameters and initial values of the Clifford attacker map, as well as RPM2 of DRPE, serve as secret keys in this scheme. In this scheme, the use of the Clifford map enables the scheme to have six additional secret keys as compared to DRPE to strengthen the proposed scheme. Its strength can be tested by analyzing the sensitivity of the secret key. The results of the sensitivity of parameters and initial values of the Clifford attacker map using the girl image as input image are shown in figure 8. From figure 8 it is observed that the decrypted image obtained by a slight change in parameter and initial values is completely unrecognizable. The key is sensitive to at least up to fourteen decimal places of each parameter and initial value. Figure 9 shows the result when we use RPM2 in the decryption process in place of the conjugate of RPM2.

The sensitivity of parameters and initial values of parameters of the Clifford attacker map is also demonstrated against variation in the parameters and initial values of this map in terms of correlation coefficient (CC) plots. Figure 10 explored the correlation coefficient between the original and retrieved image of the girl while slight (10a) deviation in the parameter a, (10b) deviation in b, (10c) deviation in c, (10d) deviation in d, (10e) deviation in x_0, (10f) deviation in y_0 up to order 10^{-15}. It is clear from figure 10 that the value of CC=1 was obtained only for the zero deviation which means the correct value of the parameter. CC is very close to zero even for a slight deviation in parameter. The extremely sensitive nature of the parameters of the Clifford attacker map demonstrates the robustness of the proposed scheme. Similar sensitivity analysis can also be done using cameraman and boat images.

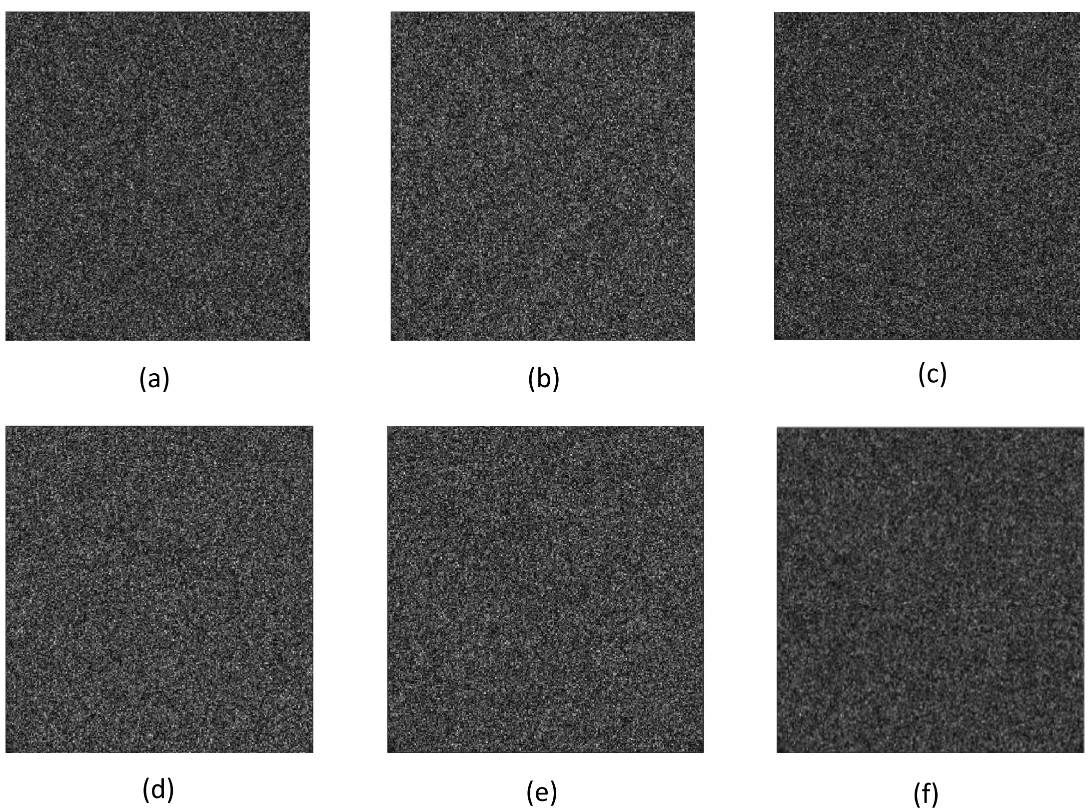


Fig. 8. Decrypted image of girl; (a) incorrect parameter a=1.499999999999999 is used instead of a=1.5; (b) incorrect parameter b=-1.7999999999999999 is used instead of b= -1.8; (c) incorrect parameter c=1.5999999999999999 is used instead of c= 1.6; (d) incorrect parameter

d=0.8999999999999999 is used instead of d=0.9; (e) incorrect initial value x_0=0.1399999999999999 is used instead of x_0=0.14; (f) incorrect initial value y_0=0.1499999999999999 is used instead of y_0=0.15.

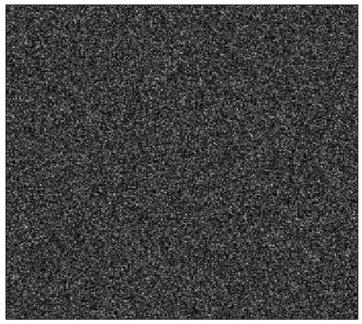


Fig. 9. Decrypted image using RPM2 in place of the conjugate of RPM2.

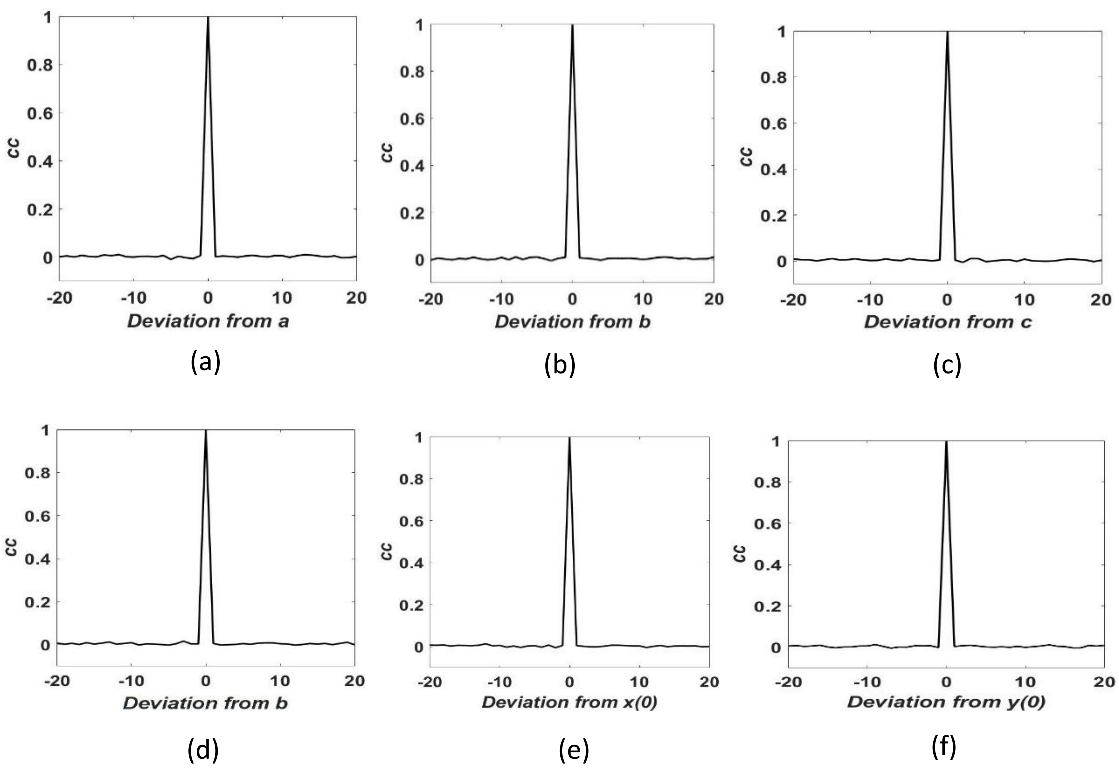


Fig. 10. Correlation coefficient versus incorrect deviation value of the parameters a, b, c, d and initial value x_0, y_0 of Clifford attacker map.

3.3 Occlusion attack analysis

On the encrypted image of the girl, an occlusion attack is carried out by obscuring 20%, 40%, and 60% of the encrypted image as shown in figure (11a-11c) respectively. Then, using the proposed decryption procedure, this occluded image is decoded. As can be seen in figures (11d-11f), the quality of the encrypted image degrades as the area of the occluded component grows larger, although the image is still recognizable as up to 60% occluded. Similarly, outputs of the occlusion attack were obtained from cameraman and boat images. As a result, the technique can withstand a broader spectrum of occlusion attacks.

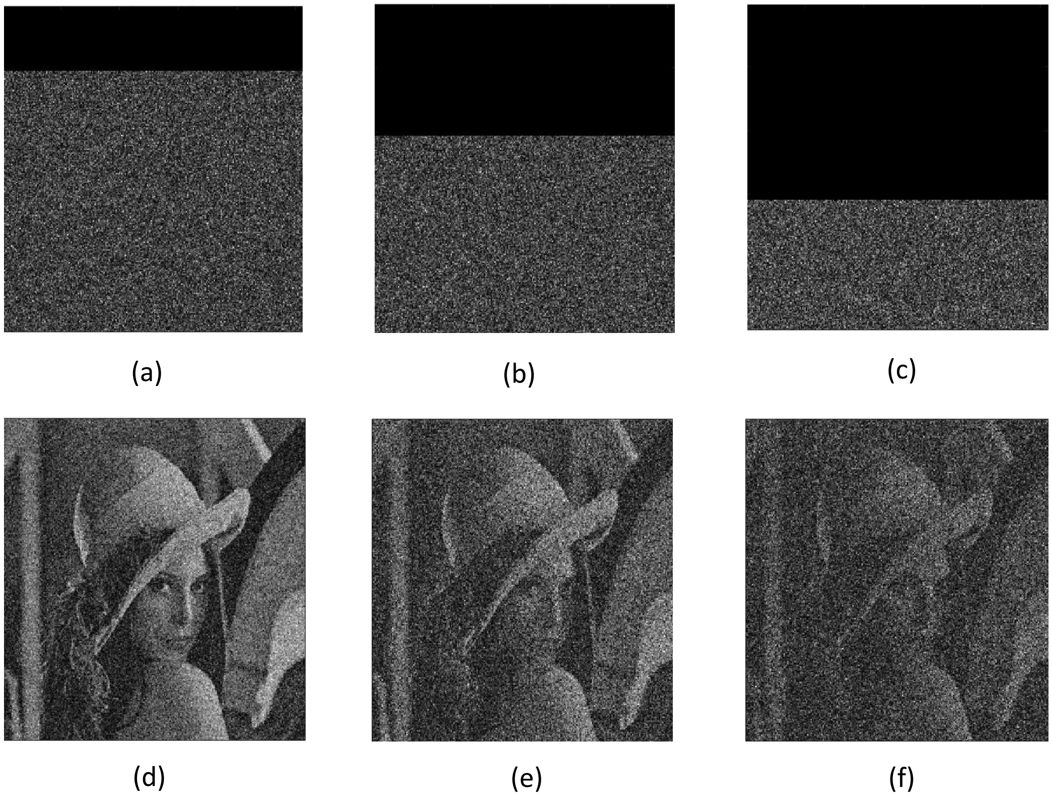


Fig. 11. Encrypted image with occluded part; (a-c) 20%, 40% and 60%; (d-f) their corresponding decrypted image.

3.3 Noise attack analysis

In this subsection, the proposed technique is tested to check its ability to endure the noise attack. The noise of strength 'k' is added to the encrypted image E_n according to the formula

$$E_0 = E_n(1 + kG)$$

Where E_0 is the noise-affected encrypted image and G is the Gaussian noise with mean zero and variance 1. The retrieved images of the girl are shown in figure (12a-12c) when the encrypted image is affected by noise with increasing noise strength k. The clarity of the decrypted image has reduced, but it is still discernible.

Fig. 12. Decrypted image with noise strength (a) k=3; (b) k=6; (c) k=9

3. Comparison of the proposed scheme with existing schemes

Statistical techniques such as the correlation coefficient, mean square error, and peak signal-to-noise ratio can be used to assess the quality of the decrypted image obtained throughout the decryption process. The correlation coefficient is given by

$$CC = \frac{cov\left(I_o(x,y), I_r(x,y)\right)}{\sigma\left(I_o(x,y)\right)\sigma\left(I_r(x,y)\right)}.$$

where, cov denotes covariance and σ denote standard deviation, while $I_0(x,y), and\ I_r(x,y)$

denote the original and retrieved image pixel values, respectively.

The mean square error is calculated as follows:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}|I_0(x,y) - I_r(x,y)|^2$$

The peak signal to noise ratio is given by the following expression

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right)$$

The efficiency of the proposed scheme is also evaluated by comparing it with existing similar symmetric linear or nonlinear techniques such as Elshamy et al. [15], Sharma et al. [16], Clifford System Based scheme, Refrigier and Javidi [3], based on a number of keys, Permutation procedure employed, applied strategy, correlation coefficient, entropy, MSE, and PSNR. It is clear from the comparison results as shown in Table 2 that the proposed technique has vast key space, and can be evaluated optically or digitally. The proposed technique is highly sensitive to the parameters of the Clifford attacker map and shows robustness against various attacks like noise attacks, occlusion attacks, brute force attacks, etc.

Table2. Comparison of the proposed scheme with existing schemes

	Elshamy et al. [15]	**Sharma et al. [16]**	**Refrigier and Javidi [3]**	**Clifford System-Based scheme**	**Proposed scheme**
Number of keys	RPM+ additional layer using Arnold's cat map	RPM+ 9 keys	RPM	6 keys	RPM + 2 initial values and 4 parameters of Clifford attacker map
Permutation procedure employed	Yes	Yes	No	Yes	Yes
Applied strategy	Digital or optical	Digital or optical	Digital or optical	Optical	Digital or optical
The correlation coefficient between input and encrypted image	-0.0011	Not evaluated	-0.0064	-0.0516	-0.0050
Entropy	Not evaluated	7.7460	7.9853	7.5784	7.9956
MSE	8.91×10^{-28}	Not evaluated	3.1334×10^{-27}	0	2.9808×10^{-27}
PSNR	318	10.2918	313	∞	314

4. CONCLUSION

The current paper introduces a novel grayscale image encrypting technique. For pixel scrambling in the Fourier domain, the approach employs the Clifford attacker map. Two random phase masks RPM1 and RPM2 are used, one in the spatial domain and the other in the Fourier Domain. Through simulation in MATLAB, the proposed scheme is validated on images of a girl, cameraman, and boat as shown in figure 4. For a good encryption scheme, the value of the information entropy of the encrypted image should be high while the correlation coefficient and mean square error value between the original and encrypted image should be low. A comparison with different algorithms was conducted which shows the value of information entropy increases from 7.9853 in DRPE to 7.9956 in the proposed scheme whereas the correlation coefficient and mean square error between the original and encrypted image decreases from -0.0064 in DRPE to -0.0050 in the proposed scheme and

3.1334 $\times 10^{-27}$ in DRPE to 2.9808 $\times 10^{-27}$ in the proposed scheme respectively. Its efficacy is assessed using statistical methods like histogram, 3-D plot, and correlation distribution analysis which shows more randomness occurs in encrypted images which are obtained using the proposed scheme. Sensitivity analysis also revealed that the new technique is quite sensitive to Clifford map parameters. As a result, these parameters work as extra encryption keys. Hence security level of the original image increases. Due to its nonlinear behavior, known plaintext and chosen plaintext attacks are not applicable. The scheme also demonstrates its endurance to occlusion and noise attacks.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCE

1. Daemen, J. and Rijmen, V. (2001). Reijndael: The advanced encryption standard. Dr. Dobb's Journal: Software Tools for the Professional Programmer, Vol. 26(3): 137–139.
2. Davis, R. (1978). The data encryption standard in perspective. IEEE Communications Society Magazine, Vol. 16(6): 5–9.
3. Refregier, P. and Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. Optics Letter, Vol. 20(7): 767.
4. Javidi, B., Sergent, A., Zhang, G., and Guibert, L. (1997). Fault tolerance properties of a double phase encoding encryption technique. Opt. Eng., Vol. 36: 992–998.
5. Goudail, F., Bollaro, F., Javidi, B. and Réfrégier, P. (1998). Influence of a perturbation in a double phase-encoding system. J. Opt. Soc. Amer. A, Vol.15: 2629–2638.
6. Unnikrishnan, G., Joseph, J. and Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional fourier domain. Optics letter, Vol. 25(12): 887–889.
7. Situ, G. and Zhang, J. (2004). Double random-phase encoding in the Fresnel domain.Optics Letters, Vol. 29(14): 1584-1586.
8. Chen, L. and Zhao, D. (2006). Optical image encryption with Hartley transforms. Opt. Lett., Vol. 31**:** 3438–3440.
9. Nishchal, N.K., Joseph, J. and Singh, K. (2003). Fully phase encryption using fractional fourier transform. Optical Engineering, Vol. 42(6): 1583–1588.
10. Peng, X., Zhang, P., Wei, H. and Yu, B. (2006). Known-plaintext attack on optical encryption based on double random phase keys. Optics Letters, Vol. 31(8): 1044–1046.
11. Carnicer, A., Montes-Usategui, M., Arcos, S. and Juvells, I. (2005). Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett., Vol. 30: 1644–1646.
12. Peng, X., Wei, H. and Zhang, P. (2006). Chosen-plaintext attack on lensless double-random phase encoding in the fresnel domain. Optics letter, Vol. 31(22): 3261–3263.
13. Sharma, N., Saini, I., Yadav, A. and Singh, P. (2017). Phase image encryption based on 3D Lorenz chaotic system and double random phase encoding. 3D Research, Vol 8: 39.
14. Elshamy, A.M., Rashed, A.N., Mohamed, A.E.N.A., Faragalla, O.S.,Mu, Y., Alshebeili, S.A. and Abd El- Samie, F. (2013). Optical image encryption based on chaotic baker map and double random phase encoding. Journal of Lightwave Technology, Vol. 31(15): 2533–2539.
15. Elshamy, A.M., El-Samie, A., Fathi, E., Faragallah, O.S., Elshamy, E.M., El-sayed, H.S., El-zoghdy, S., Rashed, A.N., Mohamed, A.E.N.A. and Alhamad, A.Q. (2016). Optical image cryptosystem using double random phase encoding and arnold's cat map. Optical and Quantum Electronics, Vol. 48(3): 1–18.
16. Sharma, N., Saini, I., Yadav, A. and Singh, P. (2017). Phase-image encryption based on 3d-lorenz chaotic system and double random phase encoding. 3D Research, Vol 8(4): 1–17.
17. Singh, N. and Sinha, A. (2008). Optical image encryption using fractional fourier transform and chaos. Optics and Lasers in Engineering, Vol. 46(2): 117–123.
18. Giesl, J., Behal, L. and Vlcek, K. (2009). Improving chaos image encryption speed. International journal of future generation communication and networking, Vol. 2(3): 23–36.
19. Kanafchian, M. and Fathi-Vajargah, B. (2017). A novel image encryption scheme based on clifford attractor and noisy logistic map for secure transferring images in navy. International Journal of e-Navigation and Maritime Economy, Vol. 6: 53–63.
20. Rakheja, P., Singh, P., Vig, R. and Kumar R. (2020). Double image encryption scheme for iris tem- plate protection using 3D Lorenz system and modified equal modulus decomposition in hybrid transform domain.

Journal of Modern Optics Apr., Vol. 67(7): 592–605.
21. Tobria, A., Yadav, S. and Singh, P. (2020). Cryptosystem Based on Triple Random Phase Encoding with Chaotic Henon Map. In book: Proceedings of International Conference on Data Science and Applications: 73-84.
22. Rakheja, P., Vig, R., and Singh, P. (2020). Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition. Opt. Quant. Electron, Vol. 52(2): 103.
23. Yadav, S. and Singh, P. (2022). A novel chaotic Umbrella map and its application to image encryption. Optical and Quantum Electronics: 54.