Original Research Article

A Chaotic Clifford Attacker Map based Image Encryption in Double Random Phase Encoding using Fourier Transformation

ABSTRACT

Encryption is the most useful technique used for security of data during storage and transmission. The proposed scheme in this paper will enhance the security of DRPE encryption scheme for images by implementing Clifford attacker map. Clifford attacker is a non-linear chaotic map which has four parameters and two initial values. This map is highly sensitive to these values. MATLAB simulation experiment 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 attack.

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

1. INTRODUCTION

In the current era of technology, the problem of security of data has augmented. Most of the data transmitted like messages photos and videos via internet. We want no one to be able to view our data while it is being transmitted. There are a variety of security features available, but image encryption is particularly important for protecting data in the form of images. Advanced encryption standards (AES) and data encryption standards are two types of digital image encryption algorithms that have been created (DES) [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, which 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 encryptions scheme based on double random phase encoding proposed in [3], optical technologies have become increasingly attractive for 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] and [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 transformation namely fractional Fourier, Fresnel domain, Hartley transformation [6,7,8,9]. Further, it was found that all these DRPE based schemes are symmetric and linear in nature. Due to symmetric and linear,

cryptoanalysis of these schemes shows that these schemes are vulnerable against some attacks [10,11,12]. To further improve the security of DRPE based scheme many researchers done efforts by using different transformations, chaotic maps to make DRPE based schemes nonlinear in nature [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.

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

In section 2, we discuss the methodology used to. The strength of encryption scheme and robustness against different attacks are discussed in section 3. The paper is concluded in section 4 and 5 followed by 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 results 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 which 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 an encrypted image.

Here RPM1 and RPM2 are defines as follows

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

Mathematically, we can write this encryption process as:

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

Where $I(x,y)$, RPM1 and RPM2 are the input image, 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, which serves as the encryption key, and then the image is subjected to another inverse Fourier transformation. As a result, the output is

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

whose absolute value turns out to decrypted image $I(x,y)$. Diagrammatically, the whole process of encryption and decryptions is shown below:

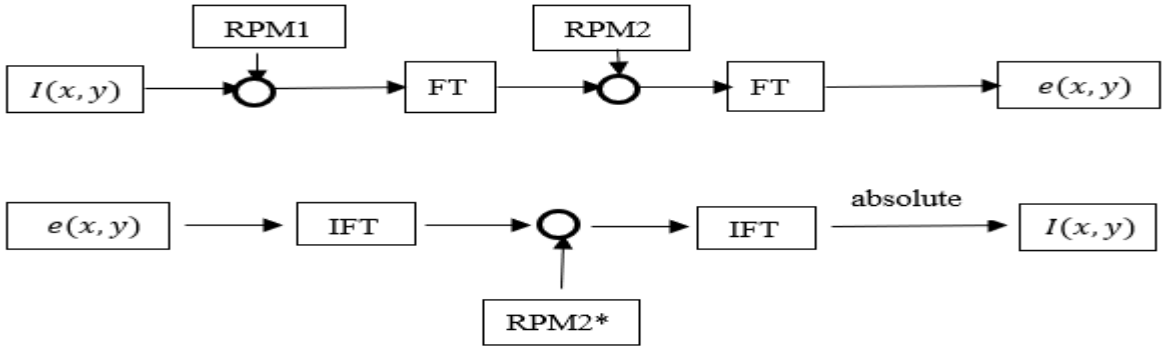


Fig. 1. Flowchart of encryption and decryption process of DRPE

2.2 Clifford attacker map

Clifford attacker map is two-dimensional chaotic map that generates a sequence of random numbers. This map is used as tool to enhance the security of encryption scheme by pixel randomization of transformed image in 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. Graphical picture of the Clifford map as shown in figure 2 is obtained by taking 66000 iterations to generate a random sequence of numbers.

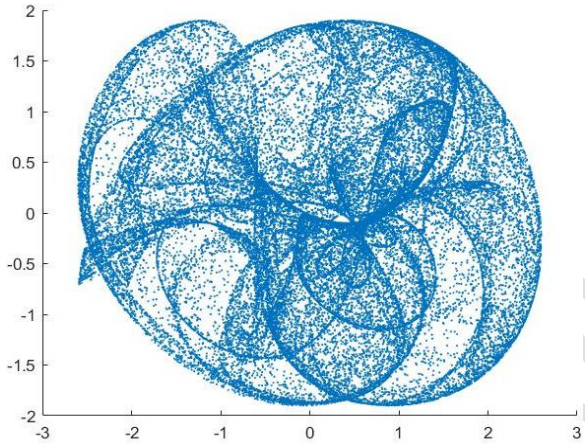


Fig. 2. Graphical picture of Clifford attacker map

2.3 Proposed encryption scheme

The proposed 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, which entails multiplying it by a second random phase mask and applying the Fourier transform once more, resulting in 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.

Flowchart of whole process of encryption and decryption of the proposed scheme displayed in the figure 3.

By implementing the proposed encryption scheme on an input image, we get extra security of encrypted image in comparison of DRPE scheme. In DRPE scheme, an attacker can retrieve the second random phase mask RPM2 but in the proposed scheme he still not able to retrieve the parameters of Clifford map which works as an extra security level.

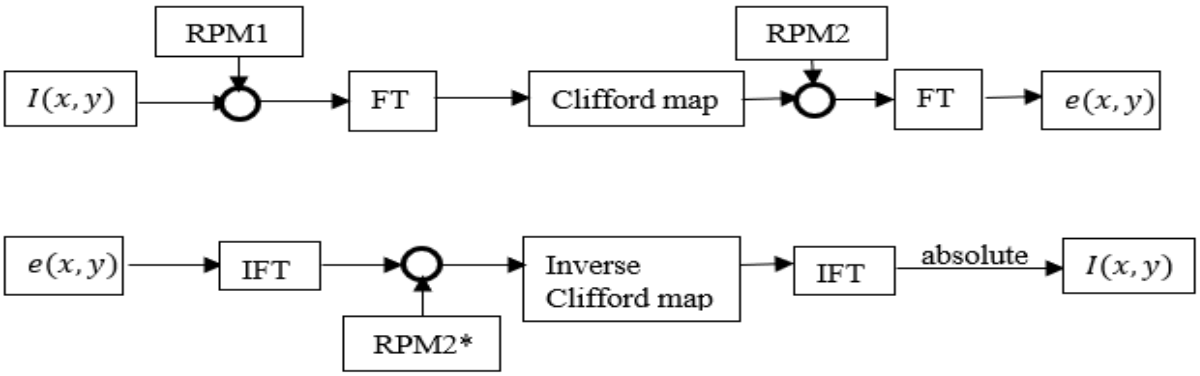
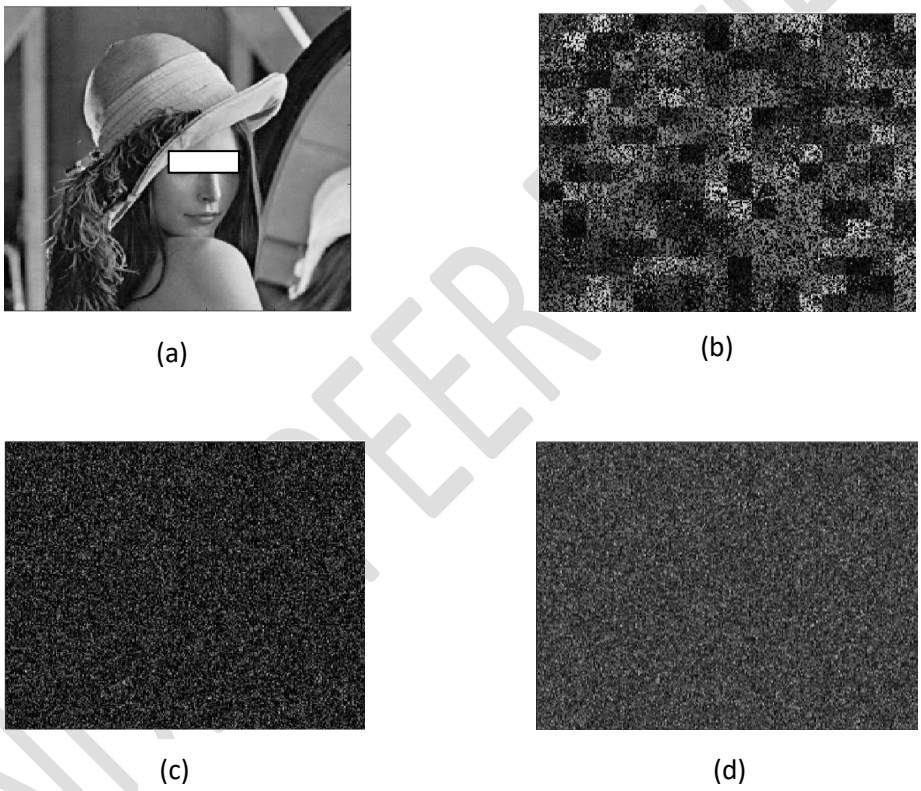


Fig. 3. Flowchart of encryption and decryption process of proposed scheme



(a) (b)

(c) (d)

Fig. 4. Scheme validation results; (a) input image and its encrypted image; (b) using only Clifford attacker map; (c) using Double Random Phase Encoding scheme; (d) using proposed scheme

3. RESULTS AND DISCUSSION

A grayscale image of girl with a size of 256×256 is 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. Proposed scheme validation results are shown in figure 4. The validation of encrypted image carried out using various statistical analysis like histogram and 3-D plot analysis, correlation distribution analysis and information entropy. Afterthat, 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 image of Lena. For better encryption algorithm, the

histogram of the encrypted image should be totally different from the histogram of the original image. Figure (5a-5c) shows the histogram of original, encrypted and decrypted image. It is clear from the figure 5 that histogram of encrypted image is totally different from the original image. Pixel values in the histogram of encrypted image are uniformly distributed i.e., all pixel values have almost same frequency. Therefore, no statistical information can be obtained through it.

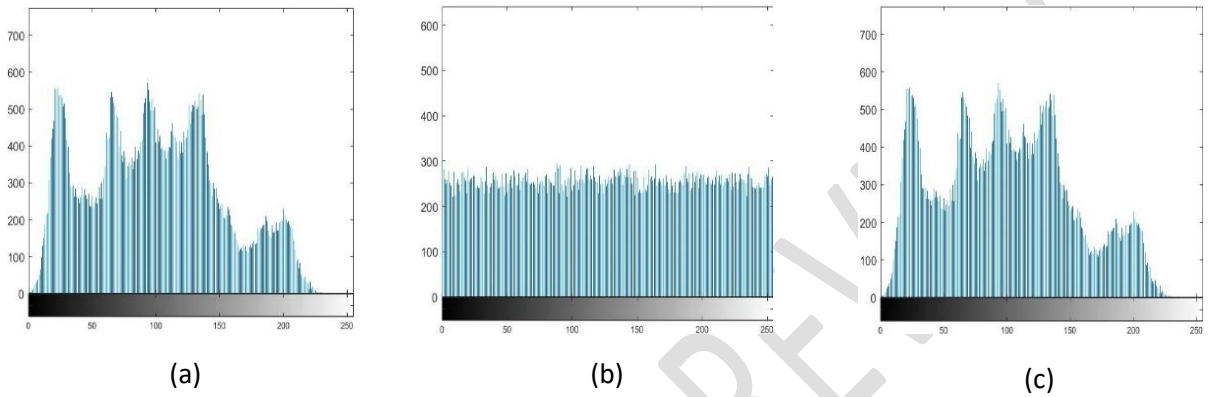


Fig. 5. Histogram of; (a) input image; (b) encrypted image; (c) decrypted image

The presented encryption scheme's efficiency may be evaluated using a 3-D visualization of girl's image. The 3-D plot of the original image, encrypted image, and de-crypted image are shown in figure (6a-6c). The 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.

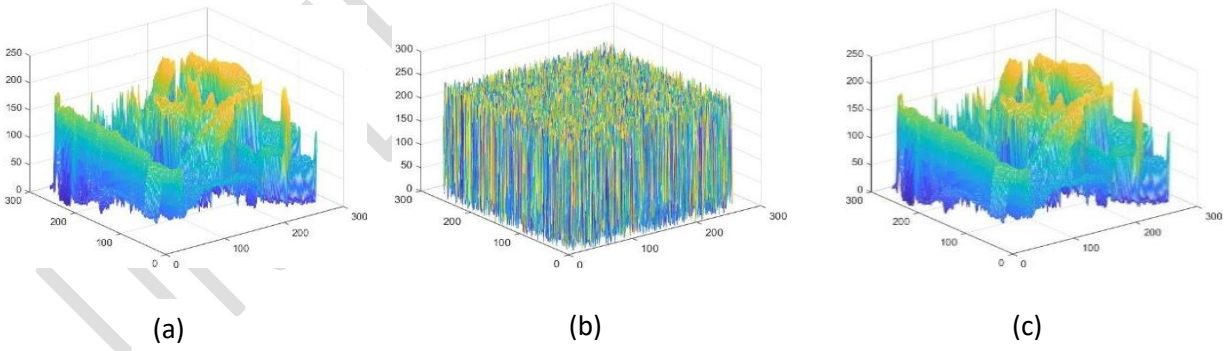


Fig. 6. 3-D plot of; (a) input image; (b) encrypted image; (c) decrypted image

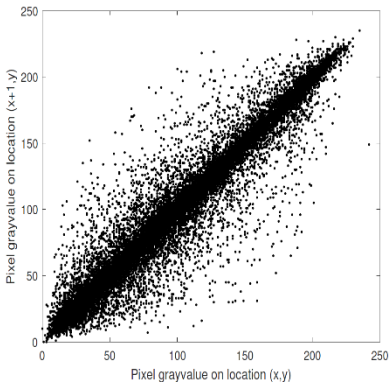
3.2 Correlation distribution analysis

Correlation distribution analysis is another approach to demonstrate the efficiency of an encryption scheme. In the horizontal, vertical, and diagonal directions, we plotted 5000 pairs of adjacent pixels from the original image and its encrypted image 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 encrypted image have no correlation. Figure (7g-7i) displays the correlation distribution of the retrieved image which is identical to input image. The comparison clearly shows that the pixels of the encrypted image have lost any correlation,

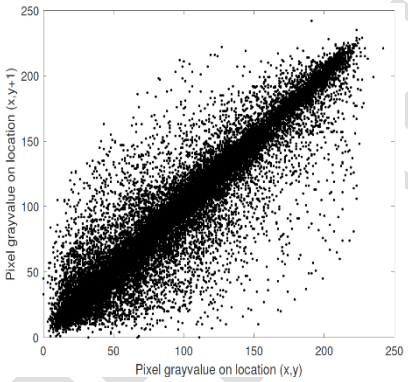
resulting in a random distribution. As shown in the table 1, the correlation coefficient between neighboring pixels from the original image and its encrypted image is computed in the horizontal, vertical and diagonal directions of the girl image. As a result, the proposed scheme is resistant to statistical attacks.

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

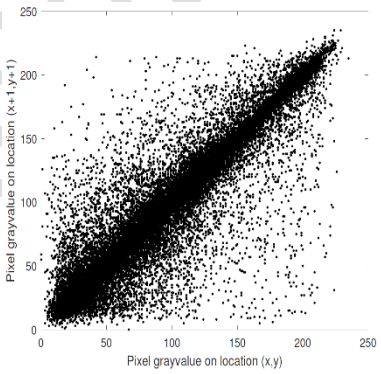
Image	Type	Horizontal direction	Vertical direction	Diagonal direction
Girl image	Input image	0.9706	0.9436	0.9192
	Encrypted image	-0.0014	0.0097	0.0024



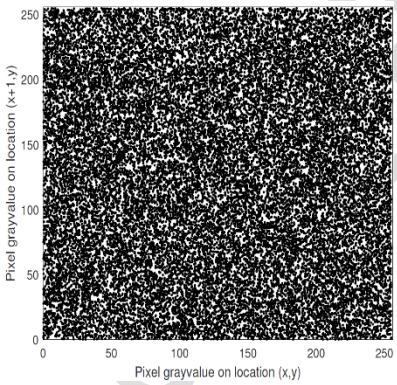
(a)



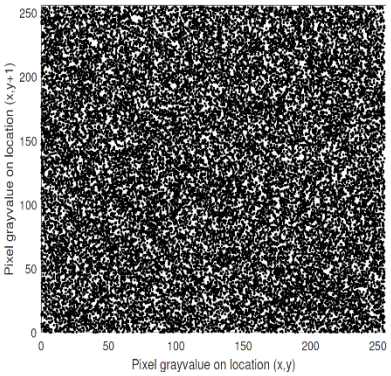
(b)



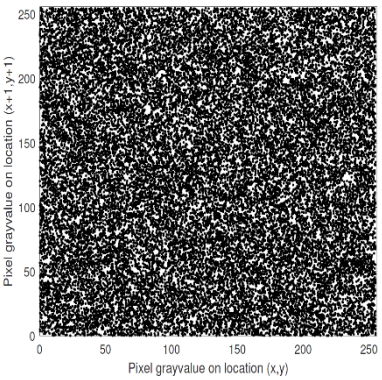
(c)



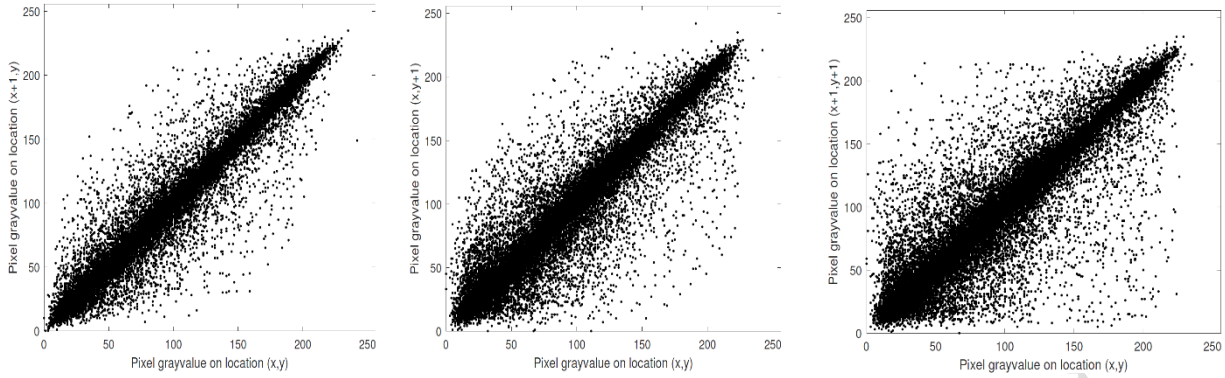
(d)



(e)



(f)



(g) (h) (i)

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

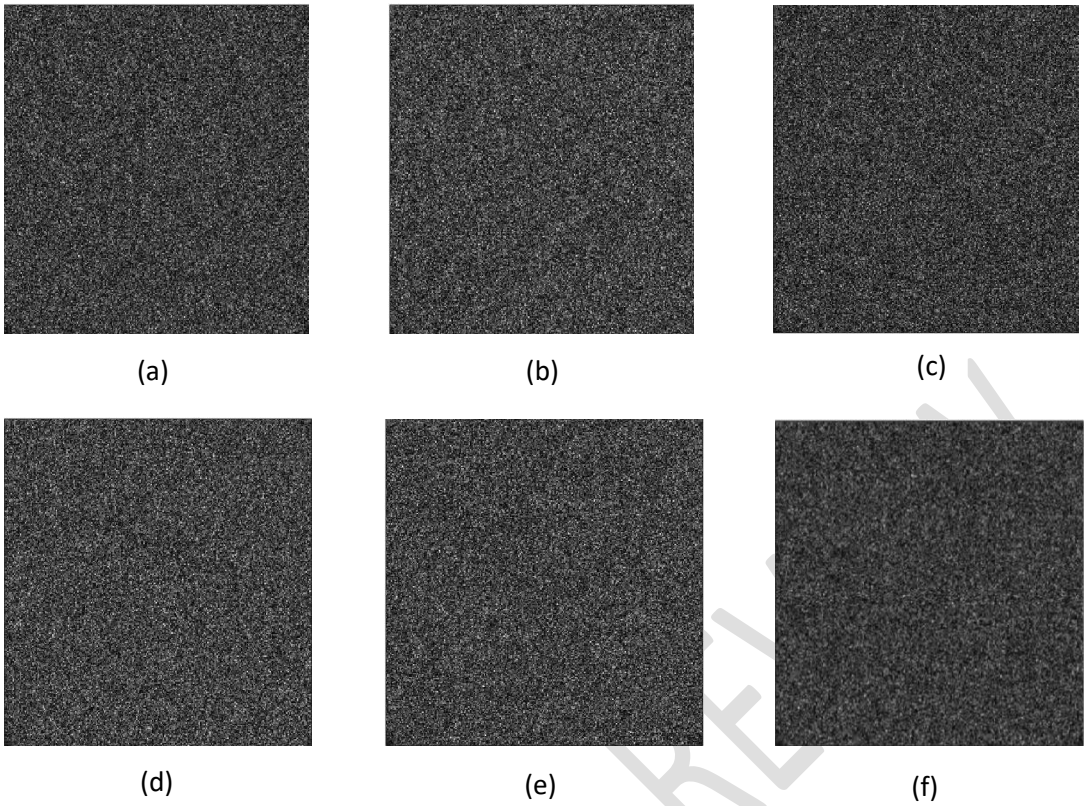
$$H(m) = \sum_{k=1}^{256} p(m_k) \log_2 \frac{1}{p(m_k)}$$

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 Lena image is 7.5784, while its encrypted image using the proposed scheme has an entropy of 7.9956. The result shows that the encrypted image's unpredictability and randomness 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, use of Clifford map enables the scheme to have six additional secret keys as compared to DRPE to strengthen the proposed scheme and strength can be tested by analyzing the sensitivity of secret key. The results of the sensitivity of parameters and initial values of Clifford attacker map are shown in figure 8. From the figure 8 it is observed that the decrypted image obtained by slight change in parameter and initial values is completely unrecognizable. The key is sensitive at least up to fourteen decimal places of each parameter and initial value. Figure 9 shows the result when we use RPM2 in decryption process in place of conjugate of RPM2.

The sensitivity of parameters and initial values of parameters of Clifford attacker map is also demonstrated against variation in the parameters and initial values of this map in terms of CC plots. Figure 10 explored the CC between original and retrieved image of 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 cleared from the figure 10 that the value of CC=1 obtained only for the zero deviation that is only for correct value of the parameter otherwise it is very close to zero for slight deviation. Extremely sensitive nature of parameters of Clifford attacker map demonstrates the robustness of proposed scheme.



(a) (b) (c)

(d) (e) (f)

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=0.139999999999999 is used instead of x_0=0.14; (f) incorrect initial value y_0=0.1499999999999999 is used instead of y_0=0.15.

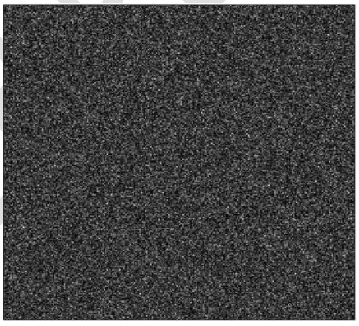
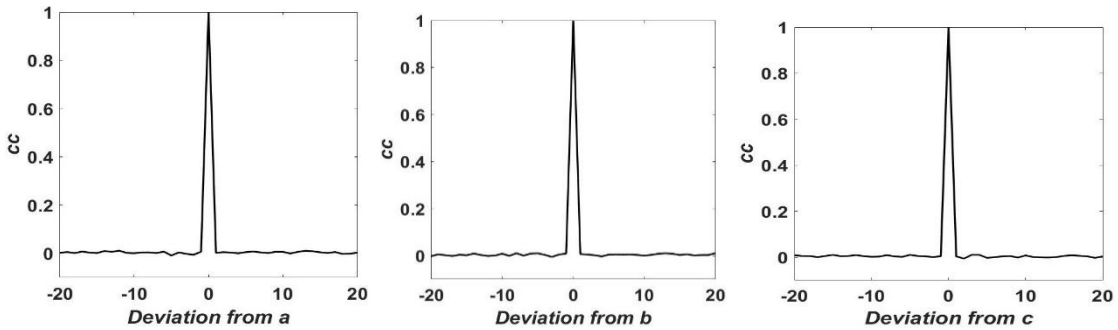


Fig. 9. Decrypted image using RPM2 in place of conjugate of RPM2.



(a) (b) (c)

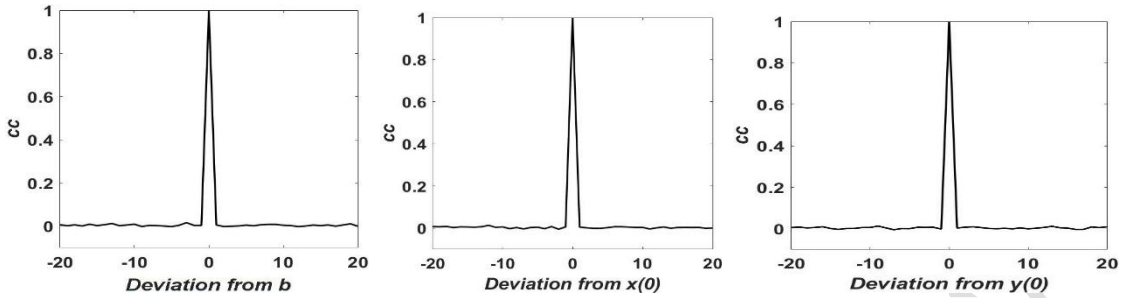


Fig. 10. Correlatio(d) ficient versus incorrect (e) tion value of the parame (f) b, c, d and initial value x_0, y_0 of Clifford attacker map.

3.3 Occlusion attack analysis

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

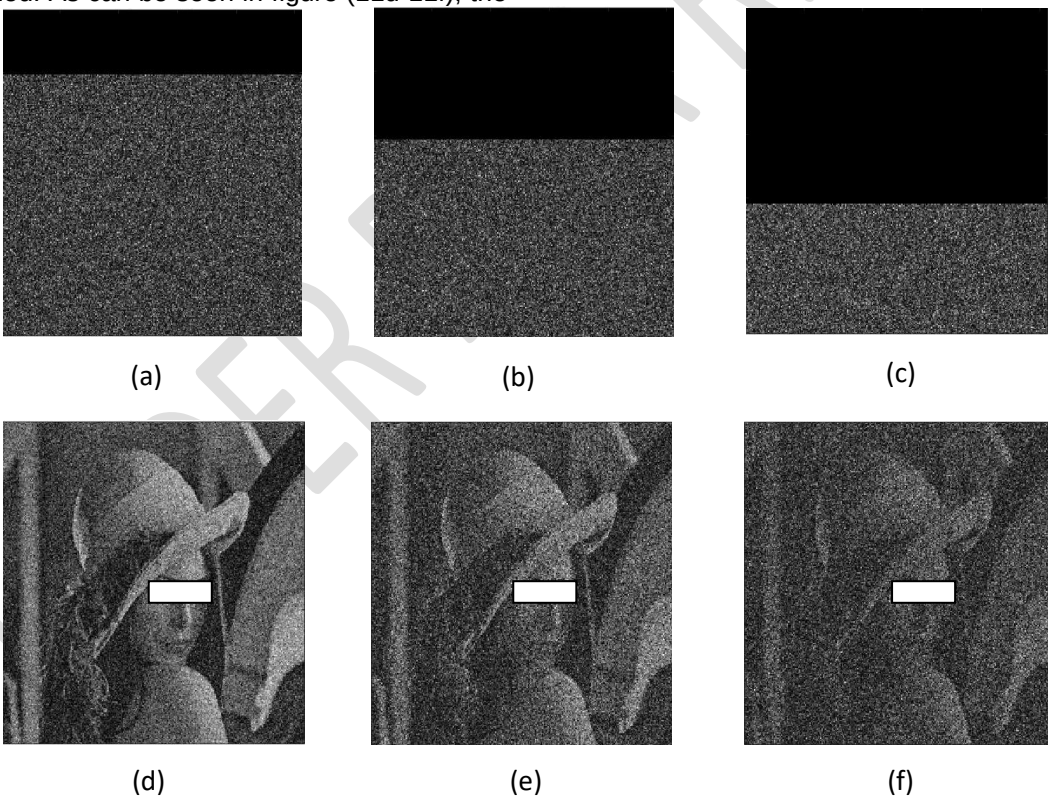


Fig. 11. Encrypted image with occluded part; (a-c) 20%, 40% and 60%; (d-f) their corresponding decrypted image.

3.3 Noise attack analysis

In this subsection, the proposed technique is tested to check its ability to endure noise attack. 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 Gaussian noise with mean zero and variance 1. The retrieved images of 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.

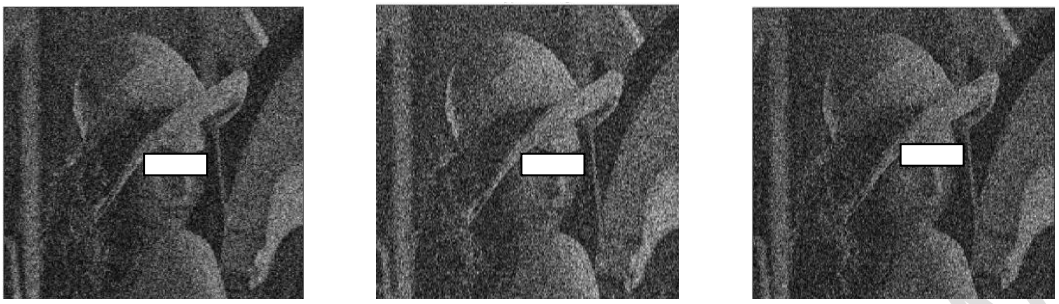


Fig. 12. Decrypted image with noise strength (a) k=3; (b) k=6; (c) k=9

3. Comparison of 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

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

where, cov denotes covariance and σ denotes 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:

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

PSNR is given by the following expression

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

The efficiency of proposed scheme is also evaluated by comparing it with existing similar symmetric linear or nonlinear techniques such as Elshamy et al.[], Sharma et al.[], Refrigier and Javidi [], Clifford System Based scheme, based on number of keys, Permutation procedure employed, applied strategy, correlation coefficient, entropy, MSE and PSNR. It is clear from the comparison results shown in Table \ref{table2} that the proposed technique has vast key space, can be evaluated optically or digitally. the proposed technique is highly sensitive to the parameters of Clifford attacker map and shows robustness against various attacks like noise attack, occlusion attack and brute force attack etc.

Table2. Comparison of 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

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 are used, one in the spatial domain and the other in the Fourier Domain. Through simulation in MATLAB, the proposed scheme was validated on an image of Lena. A comparison with different algorithms was conducted to demonstrate the proposed scheme's superior performance. Its efficacy is assessed using statistical methods like histogram, 3-D plot, and correlation distribution analysis. Sensitivity analysis reveals that the new technique is quite sensitive to Clifford map parameters. The scheme also demonstrates its endurance to occlusion and noise attacks.

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.