Cryptanalysis of DRPE Using Complex S-Box Based on Linear Canonical Transform

R Girija (girija.srikanth09@gmail.com)
VIT University - Chennai Campus https://orcid.org/0000-0001-6635-7975
H. Singh
The NorthCap University
G. Abirami
SRMIST: SRM Institute of Science and Technology

Research Article

Keywords: Complex S-box, nonlinearity, DRPE, chosen plaintext analysis

Posted Date: April 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-447642/v1

Cryptanalysis of DRPE using complex S-Box based on Linear Canonical Transform

R. Girija[*1], H. Singh[2], G.Abirami[3],*
[1]SCOPE, VIT University, Chennai Campus, India
[2]Department of Applied Sciences, The NorthCap University, Sector 23-A, Gurugram, India
[2]Department of CSE, SRMIST, Kattankulathur, India
**Corresponding author email: girija.srikanth09@gmail.com*

Abstract

During recent decades, double random phase encoding grasped more attention for researchers. To achieve nonlinearity, it had been done with random S-Box. We exhibit this involvement that DRPE system is much vulnerable in the above methodology. Concatenating anything with DRPE needs an imaginary value, wherein s-box unsuccessful in it. Used S-box has been reformed into various sizes. Due to this scenario, S-box values are replicating. So, complex S-box has been employed and proposed size of the s-box is similar to an input image. Numerical simulations have been performed out to validate the practicability and trustworthiness of traditional DRPE system with complex S-box.

Keywords: Complex S-box, nonlinearity, DRPE, chosen plaintext analysis

1. Introduction:

In the past two to three decades, securing the data, images, audio files and video files from intruder plays a foremost task. Even though there are numerous algorithms are existing, it is very difficult to protect the information. A traditional image encryption algorithm delivers poor presentation for small images. This can be easily accomplished by optical cryptography [1]. In the meantime, Refregier and Javidi [2] proposed DRPE and it has practised countless enhancements and enlargements by hosting few parameters such as wavelength, propagation distance, and polarization. Various transforms such as discrete cosine transforms (DCT) [3-6], Fresnel transforms (FrT) [7-12], Gyrator transforms (GT) [13-15], Hartley transforms (HT) [16-18], Fractional Fourier Transforms (FrFT) [19-28] and LCT [29-38] are pooled with DRPE system. These transforms are prepared with symmetric cryptosystem. Symmetric cryptosystem is defenceless to CPA [39], CCA[40] and KPA [41]. In order to defeat these attacks, an asymmetric optical cryptosystem was designed by many researchers and proposed which uses two pair of keys. In order to improve the security concern in DRPE system, in the place of traditional phase masks, there are various other types of masks are used such as deterministic phase masks [42-43], chaotic masks [44-46] etc. Enhancement of DRPE is not only shown on asymmetric cryptosystem, but also adding the nonlinearity factor which is done by random S-Box [47]. S-box is the most important key factor in placing nonlinearity in DRPE system. Proposed Random S-box is in the size of [16 16] and it has been regenerated to size of input image. Due to this values used in S-box are replicating. Moreover, generated S-box is not a complex S-box. In other words, DRPE needs complex system to get merged with any input images.

In this, cryptanalyzing the random S-box and proposing the solution for the DRPE system to add nonlinearity. Elucidation also produced for the random S-box. The parameters for Complex S-box has been checked and validated. Proposed system also holds Linear canonical transforms which also adds the more number of security parameters to our system.

The paper is given as follows:

2. Theoretical Background:

2.1.S-box:

S-Box shows a vibrant role in contemporary cryptosystems [47-50]. Without S-Box, no secured cryptosystem is possible to design in block cipher and stream cipher. Now-a-days, designing of S-box are considered as an important component in image encryption and decryption. The foremost factor for DRPE is Nonlinearity, which is easily supported by S-box. Even though nonlinearity is provided by S-Box, there is a huge ambiguity is available in constructed S-Box. Proposed S-Box is given below:

$$S - Box = rand\{r, c\} \quad (1)$$

$$S - Box = S - box\{M \times N\} \quad (2)$$

Where $rand, r$ and c are a random function, rows and columns respectively. M and N are the size of input images. While investigating the S-box from equation 1 and 2, its size is 16×16, and then it had been resized into the size of the input image. Due to this, values are getting replicated. Moreover, DRPE system mainly deals with complex numbers. But the created S-box, is not matching with complex numbers. Our proposed system overcomes the loopholes of the previous system and concentrated on enactment procedures for instance Non-linearity, Bit-Independence criterion (BIC), Strict Avalanche Criterion (SAC), Differential Probability (DP) and Linear Probability (LP). These parameters are shown in Table 1.

Table 1: S-Box parameters

Parameters	**Values**
Nonlinearity	104.6
Differential Probability	0.057
Linear Probability	0.24
Bit-Independence Criterion	104.67
Strict Avalanche Criterion	0.606

2.2.Linear Canonical Transform (LCT)

LCT is optically instigated by QPS (quadratic phase systems) [51]. LCT is considered as grander case of all the transforms such as Fourier Transform, Fractional Fourier Transform and Fresnel Transforms. The 2-dimensional LCT consists of three

parameters. LCT is considered as based on linear integral transforms and it is completely defined as follows,

$$f'(x,y) = LCT_{\alpha,\beta,\gamma}\{f(x_0,y_o)\} = \exp\left(\frac{-j\pi}{4}\right)\sqrt{\beta}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x_0,y_0)$$

$$\times \exp\{\alpha(x^2+y^2) - 2\beta(x_0x + y_0y) + \gamma(x^2+y^2)\}.dx_0.dy_0 \quad (3)$$

Where $LCT_{\alpha,\beta,\gamma}\{.\}$ represents the LCT transform through three real transform parameters α, β and γ. Two planes, one is called as input plane which is characterized as (x_0, y_0) and the other is transform plane which is mentioned as (x, y). The three transform factors α, β and γ are associated through QPS renovation. Henceforward it is interconnected to the transmission distances d_1, d_2 and the focal length$f$. The real parameters are shown as,

$$\alpha = \frac{d_1 - f}{\lambda[f(d_1+d_2) - d_1d_2]}; \quad (4)$$

$$\beta = \frac{f}{\lambda[f(d_1+d_2) - d_1d_2]}; \quad (5)$$

$$\gamma = \frac{d_2 - f}{\lambda[f(d_1+d_2) - d_1d_2}; \quad (6)$$

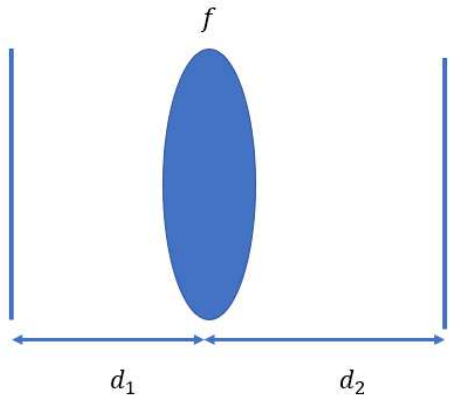


Figure 1. Optical setup of QPS

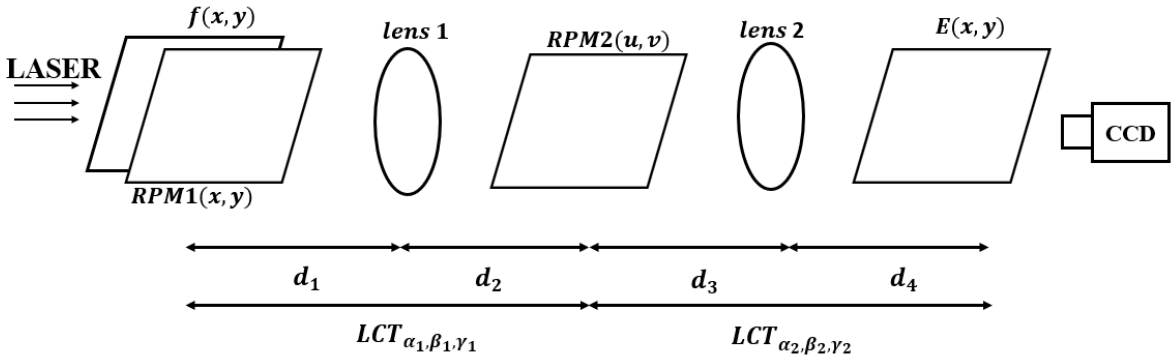


Figure 2. LCT established DRPE system

Beginning from the figure 2, it is undoubtedly agreed, input and transform planes are placed as $d_1$and d_2. The transform planes and output planes are positioned as d_3 andd_4. d_1,d_2, d_3 and d_4 are recognized as distance factors and deliberated as important to QPS. Random phase masks from DRPE system (RPM1 and RPM2) and six parameters of LCT $(\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2)$. So, totally eight parameters are considered as the security space for LCT grounded DRPE system.

3. Proposed Work

   Figure 3 shows the encryption and decryption of proposed system. Let us consider $f(x,y)$ as an input image. It is getting multiplied with first random phase mask $RPM1(x,y)$. In order to overcome the loopholes in [47], complex random S-Box has been created with the size of input image using the following equation.

$$S-box = complex\_rand\{M,N\} \qquad (7)$$

   Where M, N are the size of the input images. In the place of traditional Fourier transform, Linear canonical transforms has been considered in the proposed model with three security parameters $\alpha_1, \beta_1, \gamma_1$.

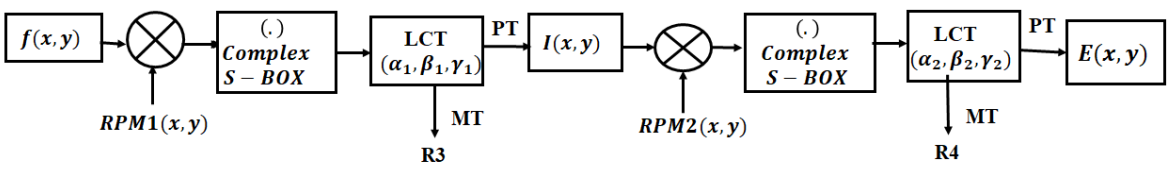


Figure.3. Proposed system-Encryption Process

Intermediate image $I(x,y)$ has been calculated with the following equations.

$$I(x,y) = PT\{LCT(\alpha_1,\beta_1,\gamma_1[f(x,y).*\ RPM1(x,y).*\ Complex\ S-Box]\} \quad (8)$$

$$R3 = MT\{LCT(\alpha_1,\beta_1,\gamma_1[f(x,y).*\ RPM1(x,y).*\ Complex\ S-Box]\} \quad (9)$$

Where PT and MT represents the phase truncation and magnetic truncation respectively. According to the above equations, input image is getting multiplied with first random phase mask and created complex S-Box. The resultant is transformed using linear canonical transforms with three security parameters. The absolution portion is called as $I(x,y)$. $R3$ is denoted as phase portion of equation 9.

Encrypted image is obtained from an intermediate image with the following equations.

$$E(x,y) = PT\{LCT(\alpha_2,\beta_2,\gamma_2[I(x,y).*\ RPM2(x,y).*\ Complex\ S-Box]\} \quad (10)$$

$$R4 = MT\{LCT(\alpha_2,\beta_2,\gamma_2[I(x,y).*\ RPM2(x,y).*\ Complex\ S-Box]\} \quad (11)$$

Intermediate image is multiplied with another random phase mask and complex S-box. The overall product is undergone for the linear canonical transforms with another set of three security parameters. The absolute portion is called as an encrypted image. $R4$ is denoted as phase portion of equation 11. R3 and R4 are also called as decryption keys.

The flow chart for the decryption is given in Figure.4. Cipher image from encryption portion is multiplied with one of the secret key and divide by randomly generated complex S-Box. The product undergoes for the Linear canonical transform using three security parameters $(\alpha_1,\beta_1,\gamma_1)$. After doing this process, $I(x,y)$ is obtained successfully.

$$I(x,y) = LCT(\alpha_1,\beta_1,\gamma_1)\{(E(x,y).*\ R4)./complex\ S-box\} \quad (12)$$

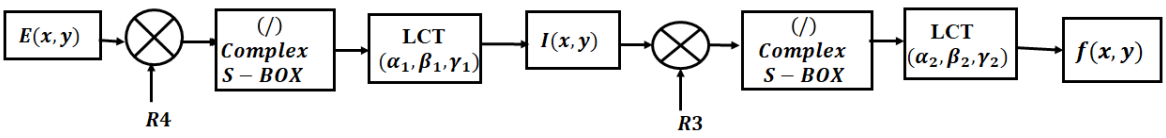


Figure.4. Proposed system-Decryption process

$$f(x,y) = LCT(\alpha_2,\beta_2,\gamma_2)\{(I(x,y).*\ R3)./complex\ S-box\} \quad (13)$$

To obtain the decrypted image back $I(x,y)$is multiplied with another secret key R_3 and divided with complex S-Box. The output undergoes for transformation with another set of three security parameters $(\alpha_2,\beta_2,\gamma_2)$.

4. Simulation results

4.1. Performance Investigation:

The suggested asymmetric cryptosystem has been surveyed by numerous methods such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (CC). MSE, PSNR and CC [52-55] have been computed using the given formulas.

$$MSE = \sum_{x=0}^{256}\sum_{y=0}^{256}\frac{|P(x,y)-P'(x,y)|^2}{256} \quad (14)$$

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right) \quad (15)$$

$$CC = \frac{cov(P(x,y)P'(x,y)}{\sigma(P(x,y)),\sigma(P'(x,y))} \quad (16)$$

Where $P(x,y)$ the plain is image and $P'(x,y)$ is recovered image. cov, σ denotes the co-variance and standard deviation respectively. The computed MSE value from the above equation for 256 × 256 medical image is $9.06 \times 10^{-26.}$ PSNR finds the variance between plain image and recovered image and it is represented in below equation. If the PSNR value is high, it gives the good quality of image. The result of PSNR is 372.21 dB. From the result, it has been clearly observed the value is high, so, it gives the good quality of image. Since all the correct keys given in our system, the value of CC is equal to 1. Table 2 drafts the evaluation results for all the analysis. It has been clearly understood from the table 2; our proposed asymmetric cryptosystem provides better results.

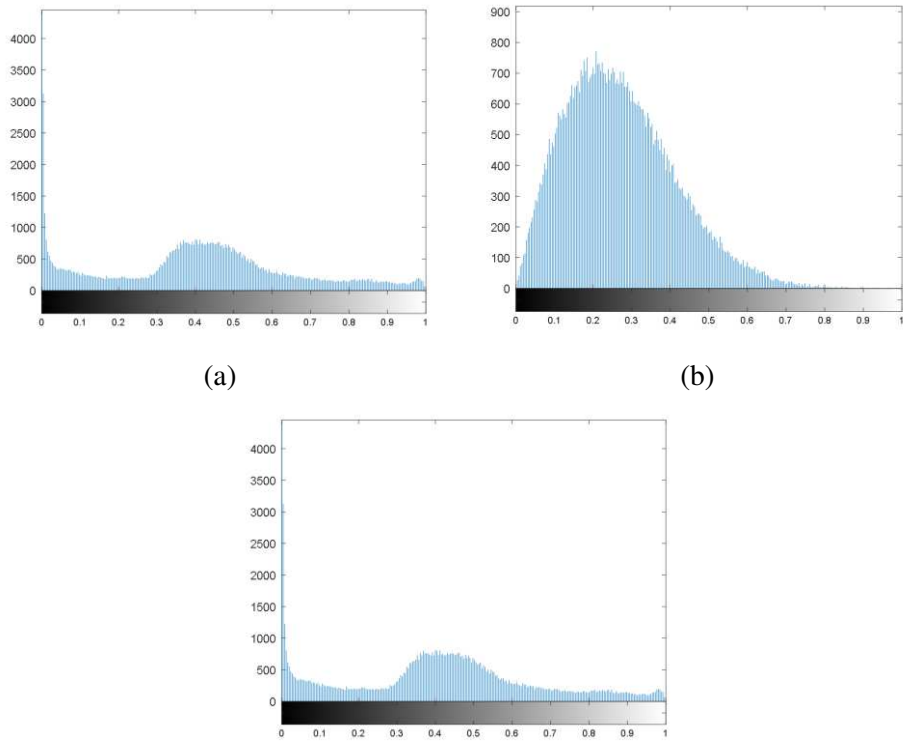
Parameters	H.Singh Scheme [14]	Zamrani scheme [42]	P. Raheja Scheme [52]	Girija Scheme [43]	Girija scheme [47]	Proposed Model
Transform Domain	Gyrator	Fourier	Hybrid multi-resolution Wavelet	Fractional Fourier	Fourier	Linear canonical
Applied Approach	Asymmetric	Symmetric	Asymmetric	Asymmetric	Asymmetric	Asymmetric
Masks	Random masks	Deterministic masks	Random masks	Deterministic masks	Random masks	Random masks

MSE	4.6 $\times 10^{-28}$	7.31 × 10^{-32}	3.10 $\times 10^{-32}$	1.74 $\times 10^{-24}$	7.0488 $\times 10^{-16}$	5.70 $\times 10^{-34}$
PSNR (in db)	310	359.13	Infinite	285.45	178.42	316.12

Table 2: Evaluation results

4.2.Histogram analysis

Histogram is otherwise defined as evaluator for our proposed cryptosystem. To avoid the leakage of information [52-55], histogram of cipher image must be different from histogram of plain image. Figure 5.represents the histogram investigation of offered asymmetric cryptosystem. Figure 5. (a), (b) and (c) represents the plain image, cipher image and recovered image respectively. From the results, it is very clear that histogram of plain image and cipher image are totally different. Suppose, if any attacker attacks the histogram of encrypted image, it is not possible to get any information about plain image.



(a) (b)

(c)

Figure.5. Histogram analysis (a) Plain image (b) Cipher image (c) recovered image

4.3.3 D plot analysis

The efficiency of asymmetric system is checked by 3d plot analysis as indicated in Figure 6. The 3D plot of plain image, encrypted image and recovered image are in Figure 6. (a) (b) and (c) respectively.

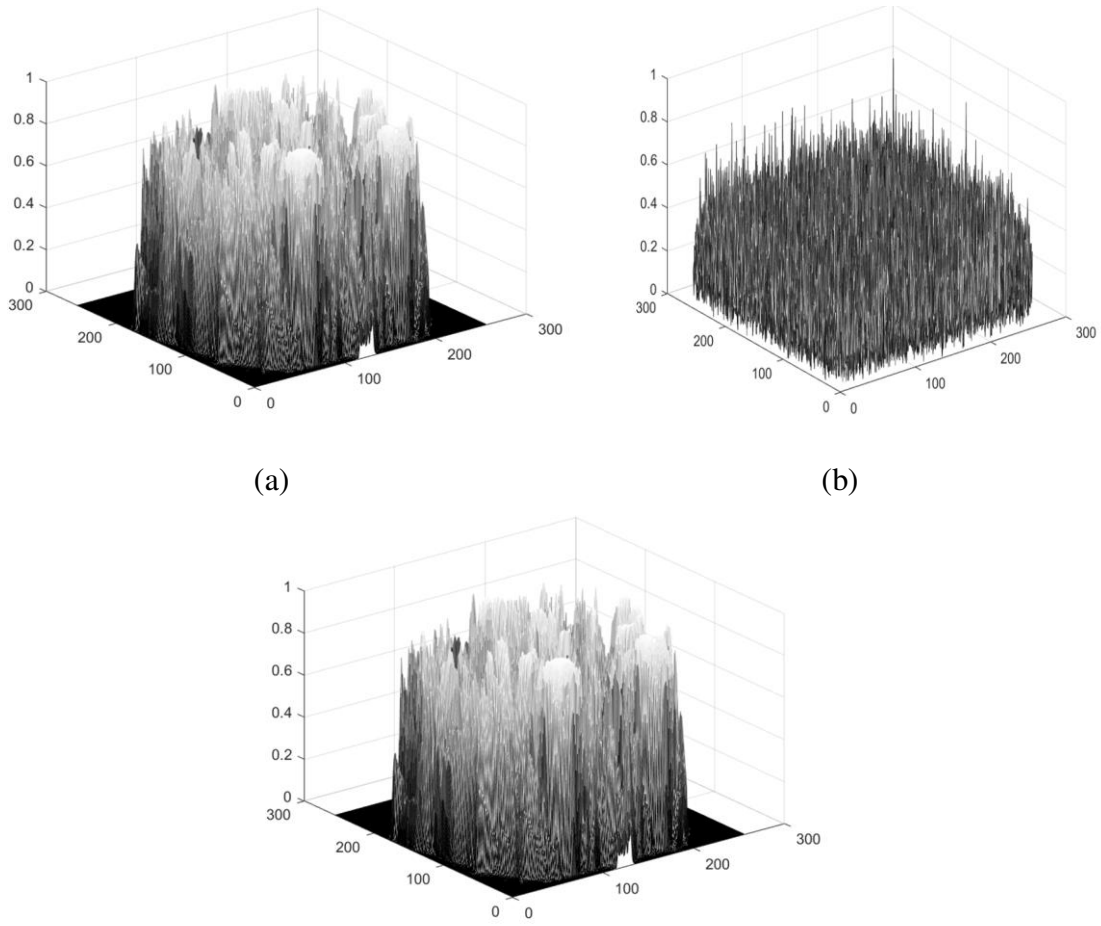


Figure.6. 3D plot analysis (a) Plain image (b) cipher image (c) recovered image

5. DRPE S-Box cryptanalysis

In this segment, conflict of DRPE using S-Box has been checked against various attacks such as occlusion attack, noise attack and chosen plaintext attack in brief.

5.1. Occlusion attack analysis

Occlusion is defined as hiding some portions or overwriting throughout communication. To examine the robustness of an encrypted data, occlusion attack [52-55] has been preferred for this cryptosystem. Figure 7. demonstrates the occlusion analysis. Minimum portion that is 10% on encrypted images are hidden in fig.7. (a) and obtained recovered image is in fig. 7. (b).

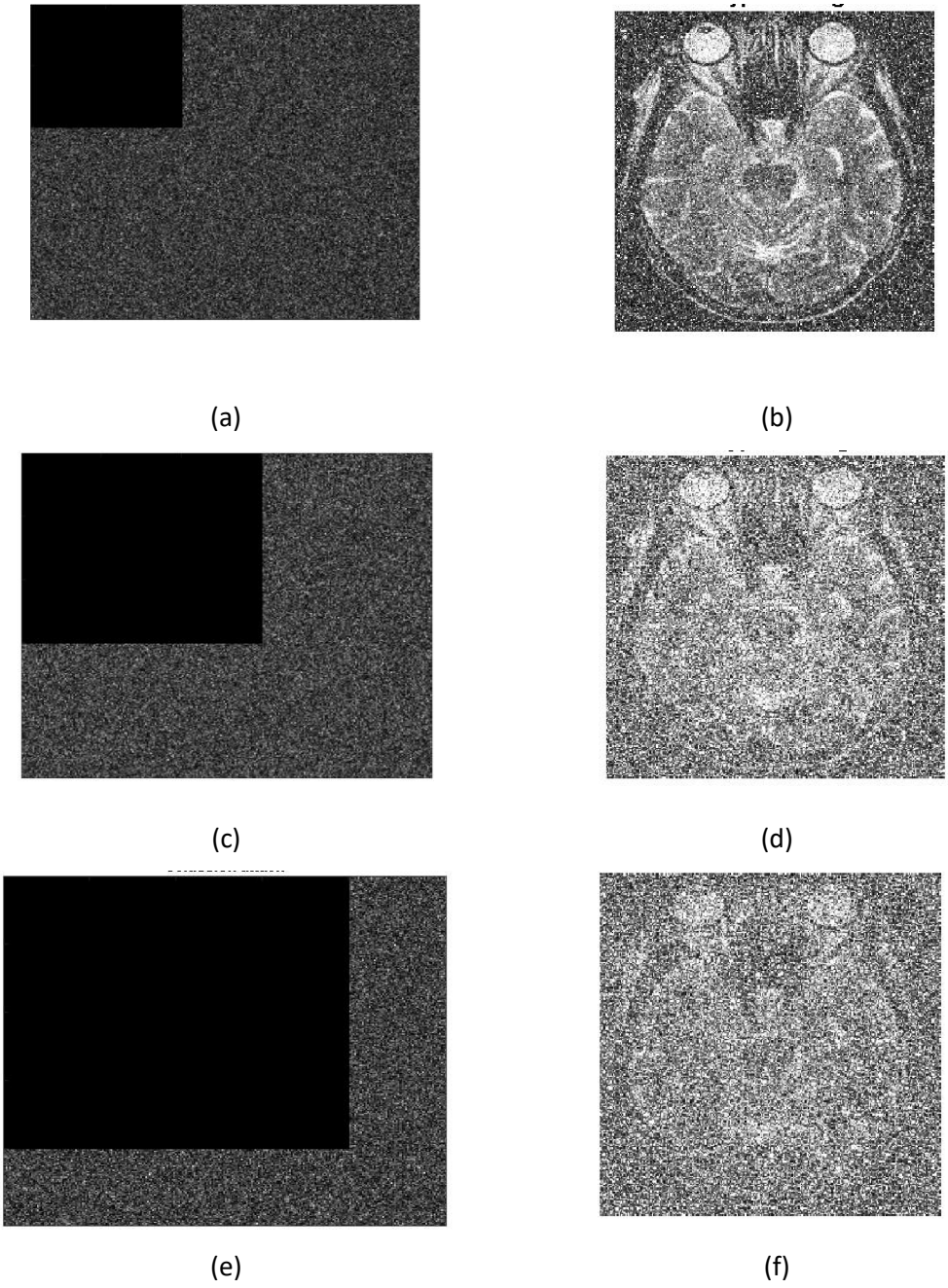
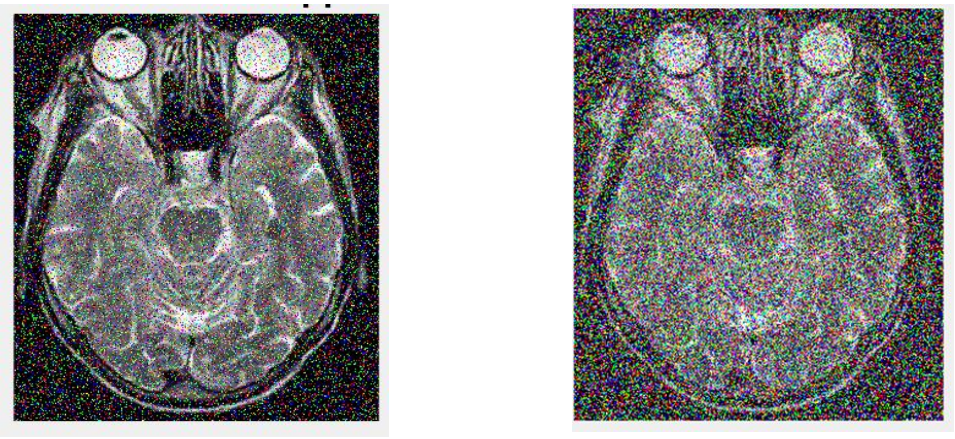


Figure.7. Occlusion analysis (a) 10% are occluded (b) corresponding decrypted image (c) 25% are occluded (d) corresponding decrypted image (e) 75% are occluded (d) corresponding decrypted image.

25% and 75% portion of encrypted images are occluded in (c) and (e) corresponding decrypted images are shown in fig. (d) and (f) respectively. As the data hiding is increasing, it is not possible to recover the image back.

5.2.Noise attack analysis

During transmitting and receiving the signals in channels, there is always a chance for noise distortion. In case, if the level of distortion is high, sometimes, it is not possible to clear picture the recovered image. Hence, it is mandatory to check our proposed system with respect to noise. In figure 8, it has been checked with salt and pepper noise. Figure 8. (a, b) represents the salt and pepper noise with density of 0.2 and 0.9 respectively. It has been observed from the figure 9, as the noise increases, mse value decreases.



(a) (b)

Figure.8. Salt and pepper analysis (a) with the density of 0.2 (b) with the density of 0.9

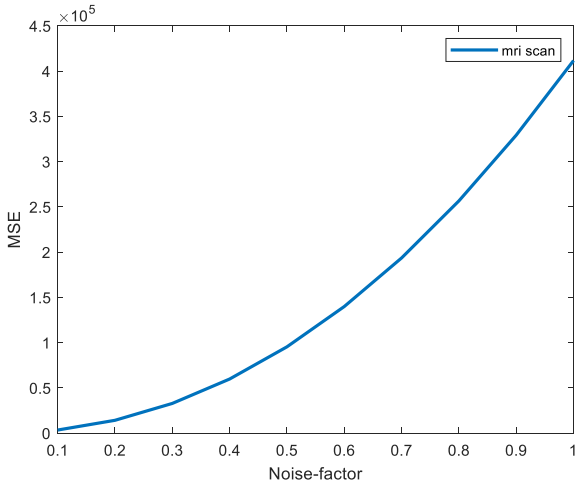


Fig. 9. Noise plot

5.3.Chosen plaintext analysis

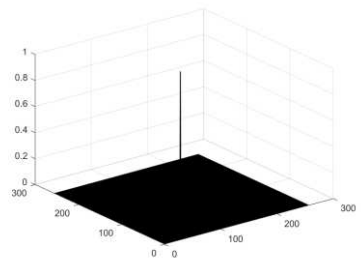
In CPA, attacker has the plain image and scheme. With respect to these, he will try the cipher image. Normally, DRPE is highly vulnerable to CPA. If an attacker chooses Dirac delta function [56] which is shown in the below equation,

$$\delta(x,y) = \begin{cases} 1, & x = 0 \; and \; y = 0 \\ 0, & otherwise \end{cases}$$

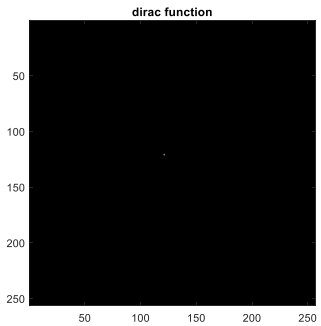
Dirac delta function is to be considering single nonzero pixel at the centre of the image and all the other values are zero. In order to perform Chosen plaintext analysis, created Dirac delta function is considered as plain image and cipher image calculation is given in the equation.

$$DRPE_{cpa} = \{ifft(fft[\delta(x,y).* RPM1(x,y).* RPM2(x,y)]\}$$

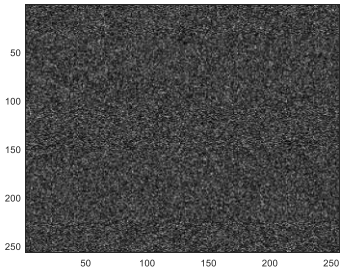
From the above equation, second secret key is easily obtained by $drpe_{cpa.}$Figure 9 shows the CPA analysis of DRPE system.



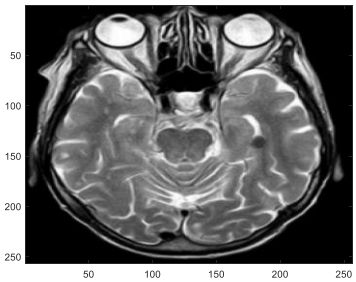
(a)



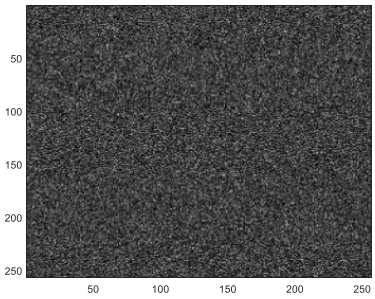
(b)

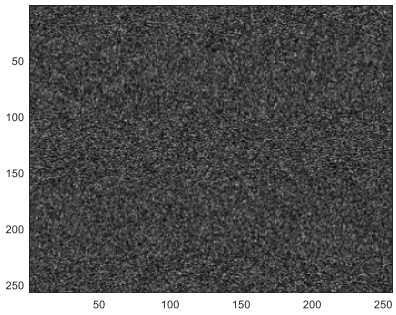


(c)



(d)



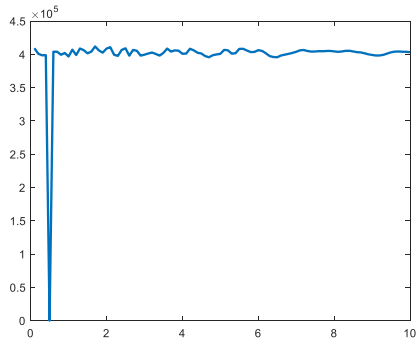


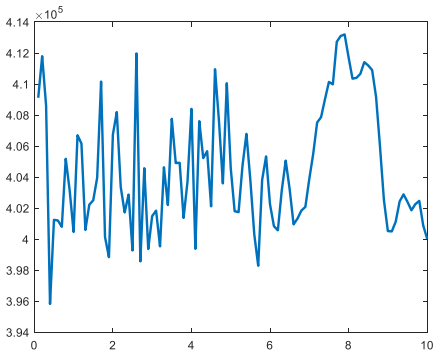
(e) (f)

Figure.10. (a) Dirac delta function (b) 3D plot of Dirac delta function; (c) DRPE encrypted image with CPA; (d) decrypted image of DRPE with CPA (e) encrypted image based on complex S-box (f) decrypted image of DRPE with CPA

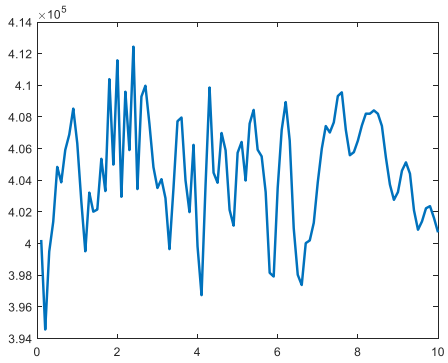
5.5 Sensitivity Analysis:

The proposed system has been checked with sensitivity analysis [52-55] . It means, how much the system is sensitive even there is a small difference. Then only when attacker tries with all possibilities, he should not able to get back the image. Figure shows the clear picture about sensitivity analysis. LCT has three security parameters; until unless attacker gets all three parameters, he is not possible for cracking. So, analysis made w.r.t LCT. Figure 11. (a) represents the plot of medical image when all the security parameters are correct. Figure 11. (b) denotes the all wrong parameters Figure 11. (c) Indicates one correct parameter and other two wrong parameters. Figure 11. (d) Represents only one wrong parameter. Hence, even attacker gets only one parameter, he is not capable to pull through the image. So, our proposed system is highly sensitive and provides best results.

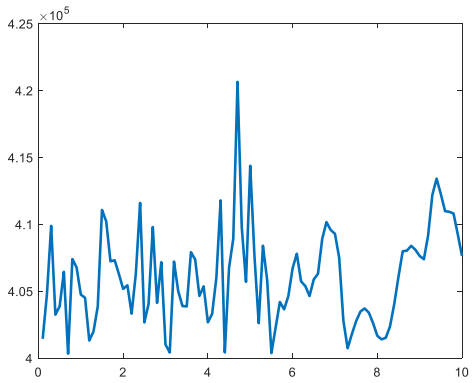




(a) (b)



(c)



(d)

Fig.11 (a) All three are correct parameters (b) All three are wrong parameter (c) Two are wrong parameters (d) only one wrong parameter.

Performance Analysis

The proposed complex S-Box based asymmetric cryptosystem is instigated in MATLAB R2020b and the rapidity is tested on Intel(R) core(TM) i5-7200 CPU @ 2.5–2.71 GHz, 8 GB RAM successively Windows 10. The time duration for the proposed system execution is 0.534 seconds.

Conclusion

Since, DRPE is in need of nonlinearity; the foremost important block to support nonlinearity is S-box. Creation of random S-box and embedded in DRPE is already done. The size of the random S-box is small and it replicates the values in order to match with the plain image. Moreover, the created S-box is not consisting of complex values. The cryptanalysis has been performed and a new approach has been specified and given as proposed asymmetric cryptosystem. Numerical analysis such as histogram, occlusion, noise attack and sensitivity analysis has been done for the proposed asymmetric cryptosystem. The transform used for proposed system is LCT with three security parameters. These three security parameters also play a vital role for the robustness of our system. Hence, the proposed asymmetric cryptosystem provides better results in comparison with other DRPE systems.

Declaration of Competing Interest

The authors declare no conflict of interest.

References

[1] Javidi, B., Carnicer, A., Yamaguchi, M., Nomura, T., Pe´rezCabre´, E., Milla´n, M. S., et al. (2016). Roadmap on optical security. Journal of Optics, 18(8), 083001.

[2] Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. *Optics letters*, *20*(7), 767-769.

[3] Abuturab, M. R. (2012). Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding. *Optics and Lasers in Engineering*, *50*(10), 1383-1390.

[4] Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., & Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications*, *284*(1), 123-128.

[5] Starchenko, A. P. (2011). Using the discrete cosine transformation to construct a hologram for the task of embedding hidden watermarks. *Journal of Optical Technology*, *78*(3), 176-179.

[6] Abuturab, M. R. (2012). Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding. *Optics and Lasers in Engineering*, *50*(9), 1209-1216.

[7] Wang, Q., Guo, Q., Lei, L., & Zhou, J. (2013). Multiple-image encryption based on interference principle and phase-only mask multiplexing in Fresnel transform domain. *Applied optics*, *52*(28), 6849-6857.

[8] Wang, Q., Guo, Q., & Zhou, J. (2013). Multiple-image encryption using polarized light encoding and the optical interference principle in the Fresnel-transform domain. *Applied optics*, *52*(36), 8854-8863.

[9] Rajput, S. K., & Nishchal, N. K. (2014). Fresnel domain nonlinear optical image encryption scheme based on Gerchberg–Saxton phase-retrieval algorithm. *Applied optics*, *53*(3), 418-425.

[10] Matoba, O., & Javidi, B. (1999). Encrypted optical memory system using three-dimensional keys in the Fresnel domain. *Optics Letters*, *24*(11), 762-764.

[11] Situ, G., & Zhang, J. (2004). Double random-phase encoding in the Fresnel domain. *Optics Letters*, *29*(14), 1584-1586.

[12] Hwang, H. E., & Han, P. (2006). Fast algorithm of phase masks for image encryption in the Fresnel domain. *JOSA A*, *23*(8), 1870-1874.

[13] Rodrigo, J. A., Alieva, T., & Calvo, M. L. (2007). Gyrator transform: properties and applications. *Optics express*, *15*(5), 2190-2203.

[14] Singh, H., Yadav, A. K., Vashisth, S., & Singh, K. (2014). Fully phase image encryption using double random-structured phase masks in gyrator domain. *Applied optics*, *53*(28), 6472-6481.

[15] Singh, H., Yadav, A. K., Vashisth, S., & Singh, K. (2015). Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane. *Optics and Lasers in Engineering*, *67*, 145-156.

[16] Chen, L., & Zhao, D. (2006). Optical image encryption with Hartley transforms. *Optics letters*, *31*(23), 3438-3440.

[17] Singh, P., Yadav, A. K., & Singh, K. (2017). Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. *Optics and Lasers in Engineering*, *91*, 187-195.

[18] Girija, R., & Singh, H. (2019). Triple-level cryptosystem using deterministic masks and modified

gerchberg-saxton iterative algorithm in fractional Hartley domain by positioning singular value decomposition. *Optik*, *187*, 238-257.

[19] Qin, W., & Peng, X. (2009). Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys. *Journal of Optics A: Pure and Applied Optics*, *11*(7), 075402.

[20] Lu, D., & Jin, W. (2011). Color image encryption based on joint fractional Fourier transform correlator. *Optical Engineering*, *50*(6), 068201.

[21] Unnikrishnan, G., Joseph, J., & Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional Fourier domain. *Optics letters*, *25*(12), 887-889.

[22] Nishchal, N. K., Joseph, J., & Singh, K. (2003). Fully phase encryption using fractional Fourier transform. *Optical Engineering*, *42*(6), 1583-1588.

[23] Liu, S., Mi, Q., & Zhu, B. (2001). Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. *Optics Letters*, *26*(16), 1242-1244.

[24] Hennelly, B., & Sheridan, J. T. (2003). Optical image encryption by random shifting in fractional Fourier domains. *Optics letters*, *28*(4), 269-271.

[25] Liu, S., Yu, L., & Zhu, B. (2001). Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. *Optics Communications*, *187*(1-3), 57-63.

[26] Tao, R., Xin, Y., & Wang, Y. (2007). Double image encryption based on random phase encoding in the fractional Fourier domain. *Optics Express*, *15*(24), 16067-16079.

[27] Singh, N., & Sinha, A. (2008). Optical image encryption using fractional Fourier transform and chaos. *Optics and Lasers in Engineering*, *46*(2), 117-123.

[28] Zhao, J., Lu, H., Song, X., Li, J., & Ma, Y. (2005). Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique. *Optics Communications*, *249*(4-6), 493-499.

[29] Huang, Z. J., Cheng, S., Gong, L. H., & Zhou, N. R. (2020). Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. *Optics and Lasers in Engineering*, *124*, 105821.

[30] Healy, J. J. (2017). Simulating first order optical systems—algorithms for and composition of discrete linear canonical transforms. *Journal of Optics*, *20*(1), 014008.

[31] Zhao, L., Muniraj, I., Healy, J. J., Malallah, R. E., Cui, X. G., Ryle, J. P., & Sheridan, J. T. (2017, May). 2D non-separable linear canonical transform (2D-NS-LCT) based cryptography. In *Holography: Advances and Modern Trends V* (Vol. 10233, p. 102331B). International Society for Optics and Photonics.

[32] Wei, D., Wang, R., & Li, Y. M. (2016). Random discrete linear canonical transform. *JOSA A*, *33*(12), 2470-2476.

[33] Guo, C., Muniraj, I., & Sheridan, J. T. (2016). Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems. *Applied optics*, *55*(17), 4720-4728.

[34] Hennelly, B. M., & Sheridan, J. T. (2005). Fast numerical algorithm for the linear canonical transform. *JOSA A*, *22*(5), 928-937.

[35] Kumar, P., Joseph, J., & Singh, K. (2016). Double random phase encoding based optical encryption systems using some linear canonical transforms: Weaknesses and countermeasures. In *Linear canonical transforms* (pp. 367-396). Springer, New York, NY.

[36] Pei, S. C., & Huang, S. G. (2015). Fast discrete linear canonical transform based on CM-CC-CM decomposition and FFT. *IEEE Transactions on Signal Processing*, *64*(4), 855-866.

[37] Wu, J., Liu, W., Liu, Z., & Liu, S. (2015). Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings. *Optics Communications*, *338*, 164-167.

[38] Zhao, L., Healy, J. J., & Sheridan, J. T. (2015). Constraints on additivity of the 1D discrete linear canonical transform. *Applied optics*, *54*(33), 9960-9965.

[39] Peng, X., Wei, H., & Zhang, P. (2006). Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Optics letters*, *31*(22), 3261-3263.

[40] Carnicer, A., Montes-Usategui, M., Arcos, S., & Juvells, I. (2005). Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. *Optics letters*, *30*(13), 1644-1646.

[41] Qin, W., & Peng, X. (2009). Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys. *Journal of Optics A: Pure and Applied Optics*, *11*(7), 075402.

[42] Zamrani, W., Ahouzi, E., Lizana, A., Campos, J., & Yzuel, M. J. (2016). Optical image encryption technique based on deterministic phase masks. *Optical Engineering*, *55*(10), 103108.

[43] Girija, R., & Singh, H. (2018). A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition. *Optical and Quantum Electronics*, *50*(5), 1-24.

[44] Liansheng, S., Bei, Z., Xiaojuan, N., & Ailing, T. (2016). Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. *Optics Express*, *24*(1), 499-515.

[45] Abuturab, M. R. (2018). Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition. *Optics & Laser Technology*, *98*, 298-308.

[46] Girija, R., & Singh, H. (2018). Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional Fourier transform. *3D Research*, *9*(3), 1-20.

[47] Girija, R., & Singh, H. (2018). Enhancing security of double random phase encoding based on random S-Box. *3D Research*, *9*(2), 1-20.

[48] Devaraj, P., & Kavitha, C. (2016). An image encryption scheme using dynamic S-boxes. *Nonlinear Dynamics*, *86*(2), 927-940.

[49] Farwa, S., Muhammad, N., Shah, T., & Ahmad, S. (2017). A novel image encryption based on algebraic S-box and Arnold transform. *3D Research*, *8*(3), 1-14.

[50] Liu, H., Kadir, A., & Gong, P. (2015). A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. *Optics Communications*, *338*, 340-347.

[51] Unnikrishnan, G., & Singh, K. (2001). Optical encryption using quadratic phase systems. *Optics Communications*, *193*(1-6), 51-67.

[52] Rakheja, P., Singh, P., & Vig, R. (2020). An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain. *Optics and Lasers in Engineering*, *134*, 106177.

[53] Maan, P., & Singh, H. (2018). Non-linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain. *3D Research*, *9*(4), 1-12.

[54] Yadav, P. L., & Singh, H. (2018). Optical double image hiding in the fractional Hartley transform using structured phase filter and Arnold transform. *3D Research*, *9*(2), 1-19.

[55] Girija, R., & Singh, H. (2019). An asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain. *Multimedia Tools and Applications*, 1-19.

[56] Kumari, E., Singh, P., Mukherjee, S., & Purohit, G. N. (2020). Analysis of triple random phase encoding cryptosystem in Fresnel domain. *Results in Optics*, *1*, 100009.

Figures

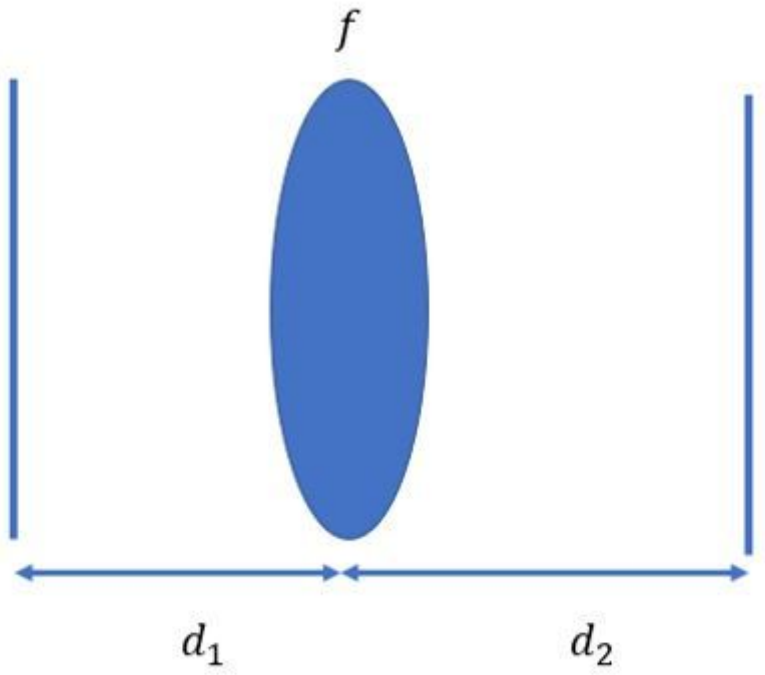


Figure 1

Optical setup of QPS

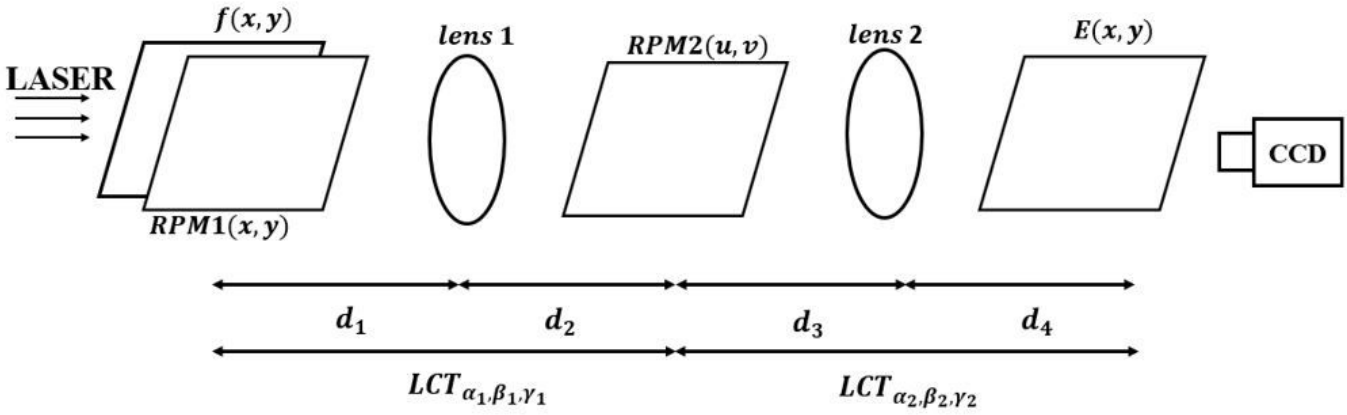


Figure 2

LCT established DRPE system

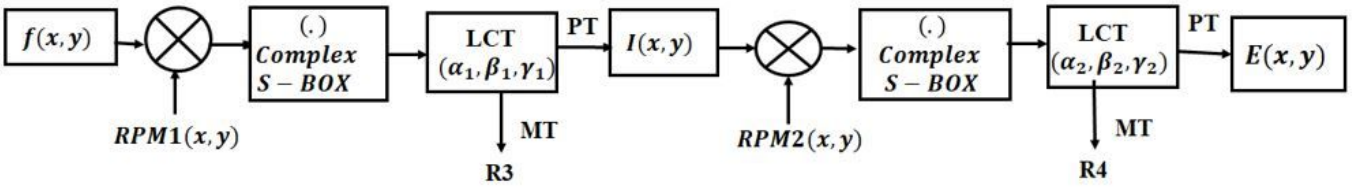


Figure 3

Proposed system-Encryption Process

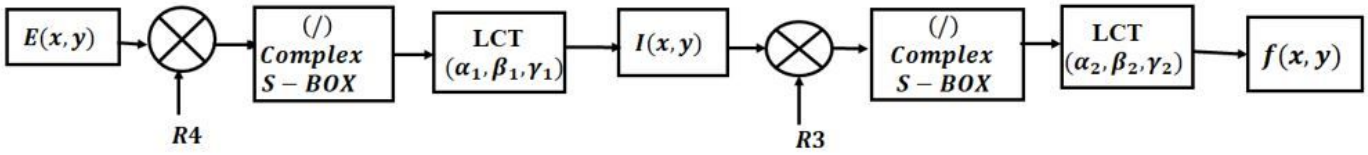


Figure 4

Proposed system-Decryption process

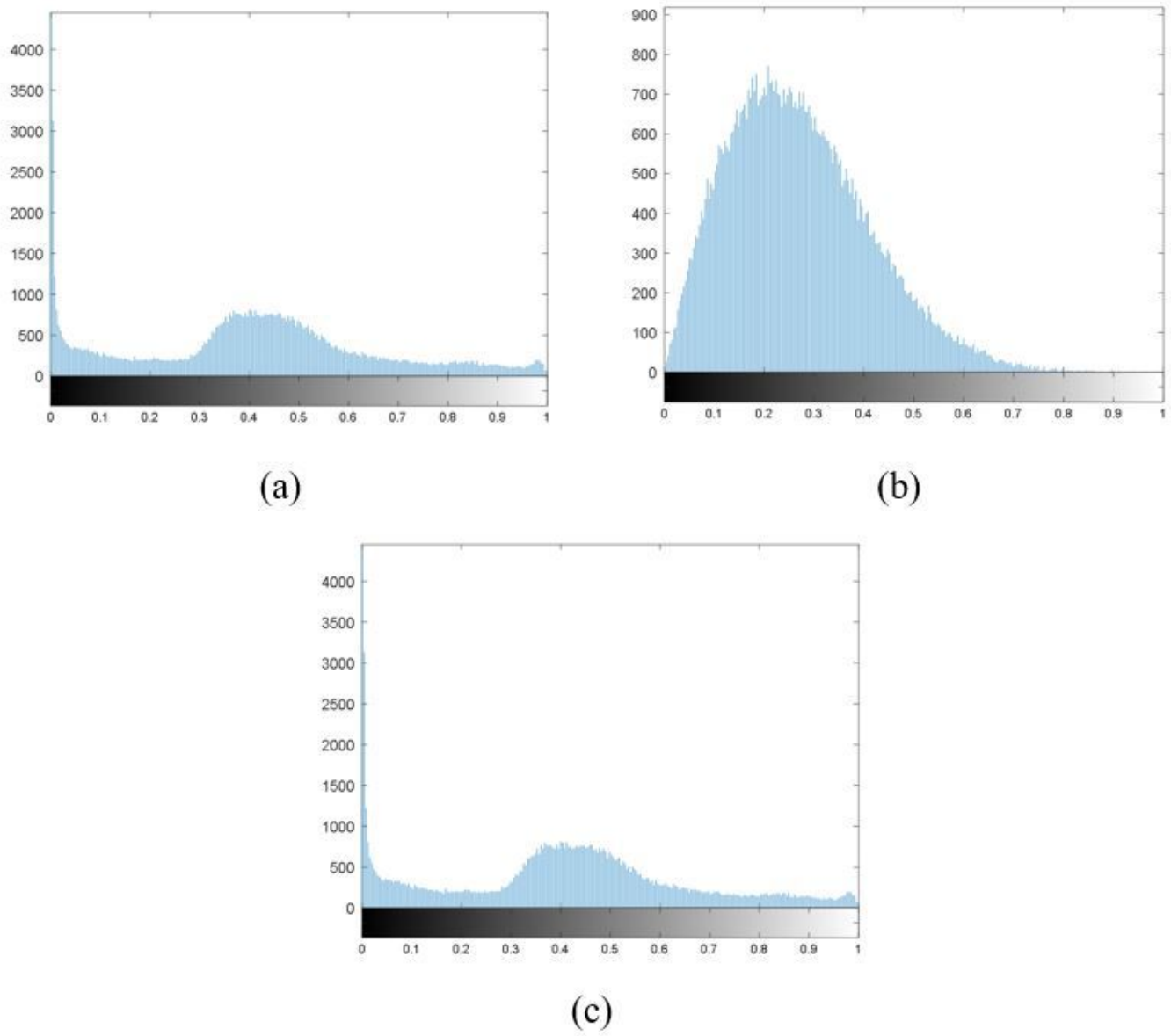


Figure 5

Histogram analysis (a) Plain image (b) Cipher image (c) recovered image

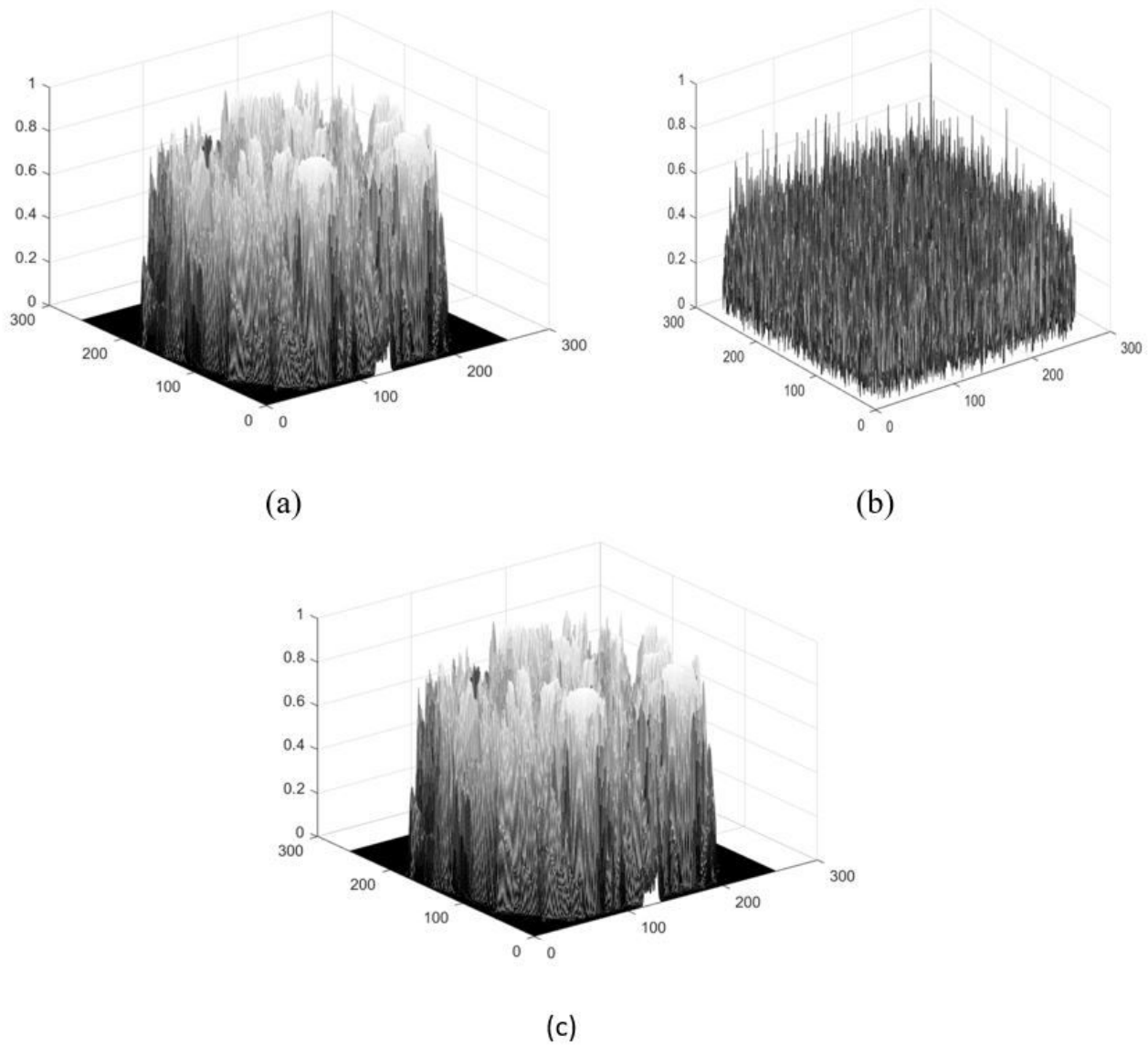


Figure 6

3D plot analysis (a) Plain image (b) cipher image (c) recovered image

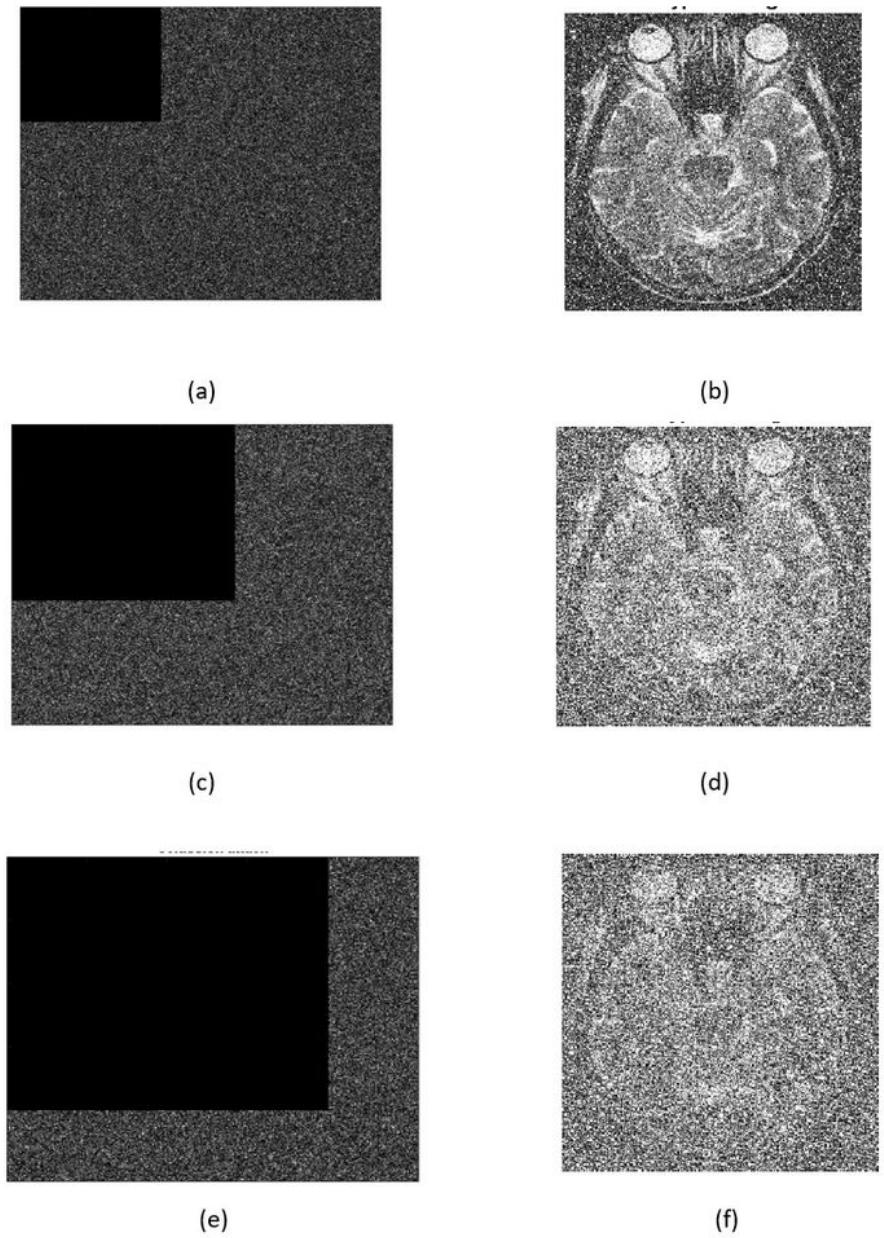


Figure 7

Occlusion analysis (a) 10% are occluded (b) corresponding decrypted image (c) 25% are occluded (d) corresponding decrypted image (e) 75% are occluded (d) corresponding decrypted image.

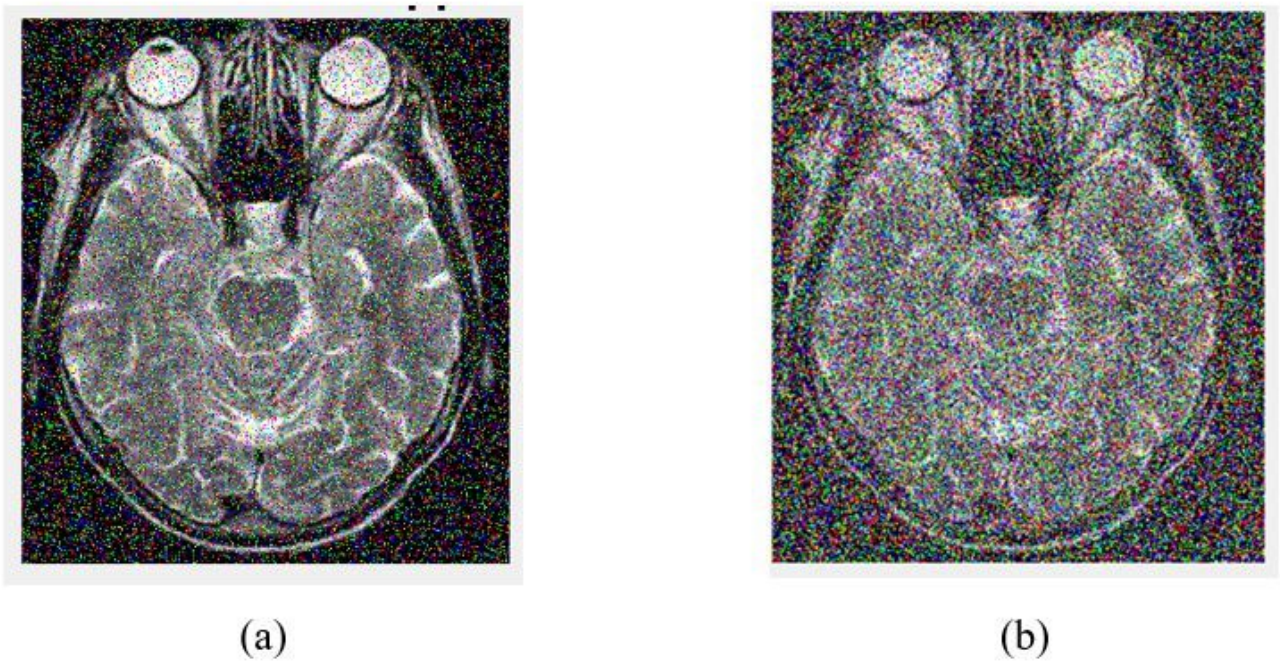


Figure 8

Salt and pepper analysis (a) with the density of 0.2 (b) with the density of 0.9

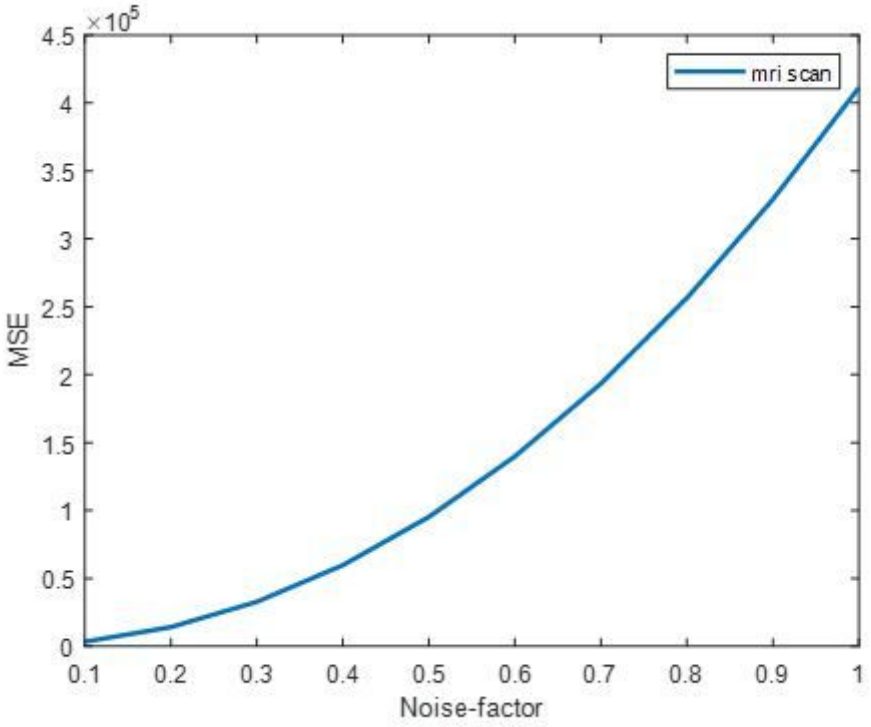


Figure 9

Noise plot

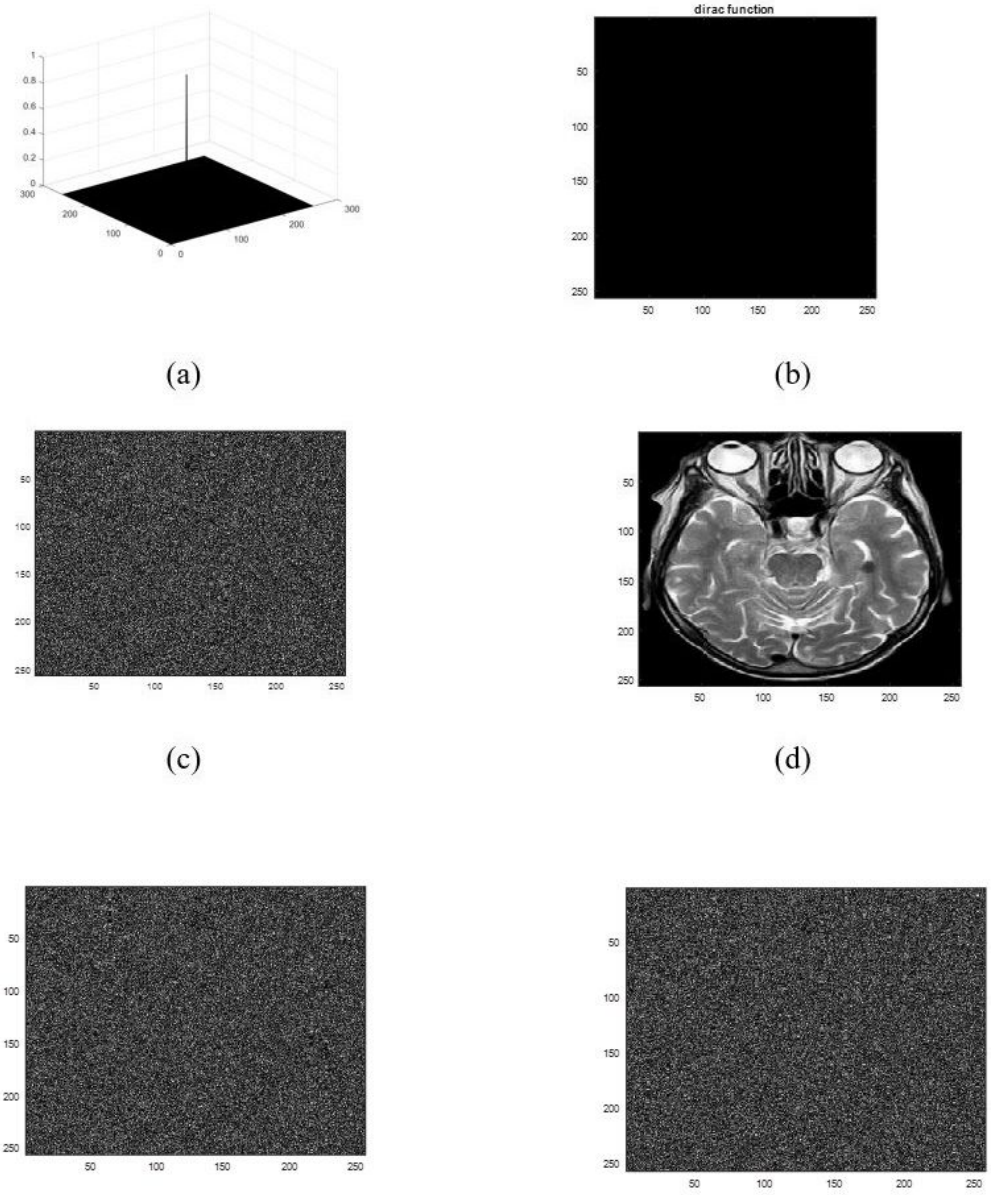


Figure 10

(a) Dirac delta function (b) 3D plot of Dirac delta function; (c) DRPE encrypted image with CPA; (d) decrypted image of DRPE with CPA (e) encrypted image based on complex S-box (f) decrypted image of DRPE with CPA

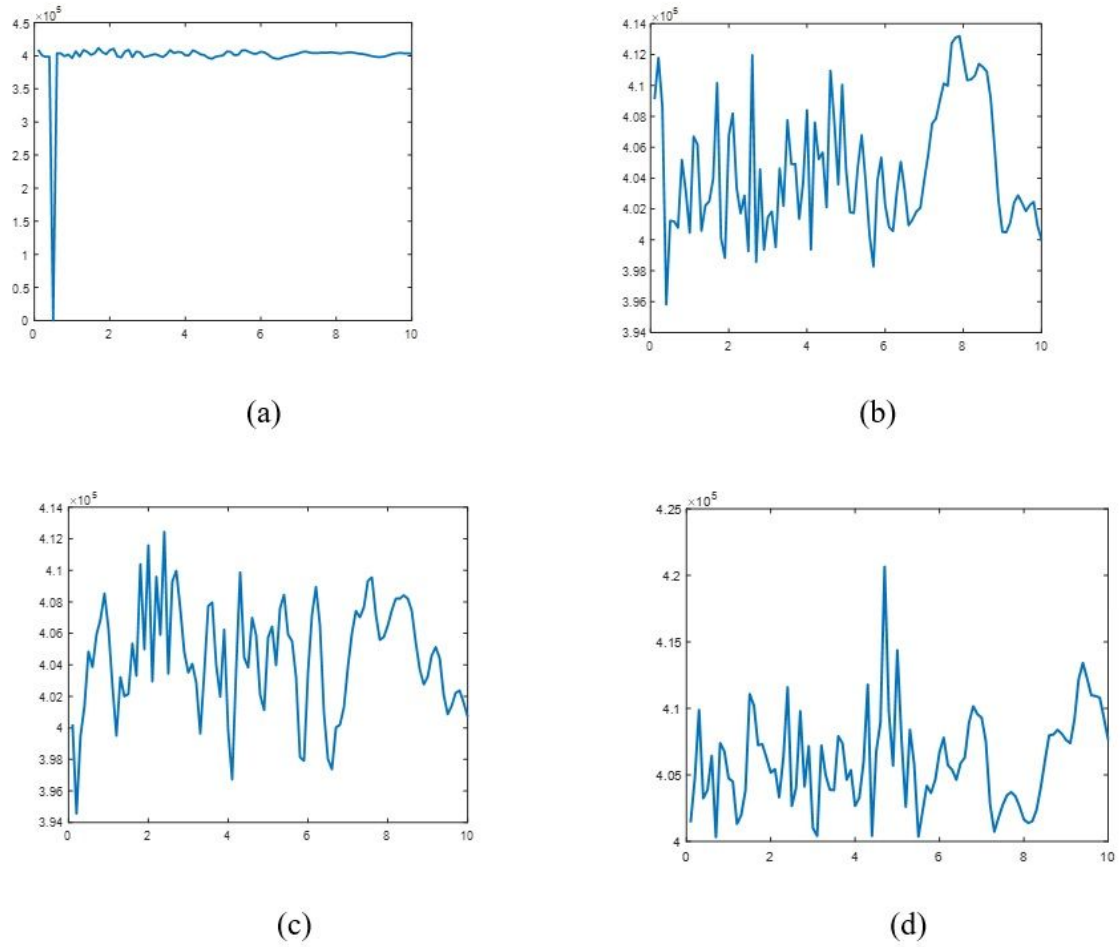


Figure 11

(a) All three are correct parameters (b) All three are wrong parameter (c) Two are wrong parameters (d) only one wrong parameter.