J. Electrical Systems 20-10s (2024): 8507-8516

Eakta Kumari[a*]
Saurabh Mukherjee[a]

Optical Encryption using Unequal Modulus Decomposition and Diffractive Imaging in Fresnel Domain

Abstract- In this paper, a secured cryptosystem based on diffractive imaging encoding and unequal modulus decomposition by using double random phase encoding in Fresnel domain is proposed. First, an input image is encoded using random phase masks and then intensity patterns are generated and after that the resultant is decomposed in two independent phase masks with unequal modulus. Here, unequal decomposition is used for creating one-way effective trapdoor function. As a result, the proposed scheme provide resistance to basic and specific attack proposed by Wang et.al. Numerical simulations are done to demonstrate the validity, feasibility and robustness of the proposed scheme.

Keywords: Unequal modulus decomposition, Double random phase encoding, Fresnel transform, Image encryption.

1.Introduction

In the past decades, optical techniques have made a great progress in the field of securing and validating the information and many of them appeared as an excellent tool. The very well-known optical technique proposed by Refregier and Javidi known as double random phase encoding (DRPE) which encrypts the input image by the usage of two random phase masks which are located in spatial and frequency planes, into a stationary white noise data (Break into two lines).[1], [2], [3]. The DRPE method is implemented in various other domains rather than the Fourier domain such as Fresnel transform, gyrator transform, Hartley transform, fractional Fourier, fractional Hartley, fractional Mellin, Wavelets, Hybrid domains to make advancements in the encryption algorithm [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. But, the DRPE scheme is found to be vulnerable to various attacks such as known-plaintext attack (KPA), chosen-plaintext attack (CPA) and ciphertext only attack (COA) [16], [17], [18]. Due to their linear behaviour, the symmetric cryptosystem are not resistant to cryptographic attacks [17], [19], [20], [21]. To counter these attacks, optical and digital methods were proposed with the variants of DRPE. Researchers proposed and enhanced the asymmetric cryptosystems based on phase truncation and phase reservation operations in various domains [20], [22], [23]. But later on, it was found that the asymmetric cryptosystems are also prone to specific attack [18], [24], [25], [26], [27]. Hence, research has been on track develop a cryptosystem which would resist these types of attacks.

Image encryption scheme proposed by Zhang and Wang which uses the principle of interference [28] shows the advantage of non-iterative scheme and being simple, but it suffers from the silhouette problem. To remove the silhouette problem various methods have been proposed [29], [30]. In a novel approach, to achieve an efficient cryptosystem two waves are superimposed. To achieve the nonlinearity, the scheme makes the use of equal modulus decomposition (EMD) rather than phase-truncated operation in Fourier transform [31], [32]. In EMD based encryption scheme, the input image is split into two complex masks having the same modulus. One is used as private key and the other as cipher text [31], [33], [34], [35], [36], [37]. Later EMD based cryptosystems shows vulnerability to specific cryptographic attack which is based on phase truncation[33], [38], [39]. Here, the modulus of ciphertext is used to retrieve information about the private key. Recently, unequal modulus decomposition (UMD) is proposed [40], [41]. In UMD the modulus of ciphertext and private key is different.

In an effort to develop a strong secure architecture, encryption scheme was proposed using diffractive-imaging based encryption [42]. This scheme possesses improved security against attacks, such as the chosen-plaintext attack, known-plaintext attack and it also offers a simple optical setup. DIBE (Diffractive Imaging Based Encryption) is concise in architecture and provides relatively high security with its nonlinear structure. Due to simple architecture, it has been extensively found applications in encryption and watermarking schemes. However, various attempts to strengthen diffractive imaging based encryption have been reported [43], [44]. Initially it was considered that DIBE was unbreakable against these attacks because of its nonlinearity but Li and Shi proved its vulnerability to CPA [45]. In fact, the applicability of CPA was proved if the attacker has access to the data of input and output planes and also know about the mathematical relation between plaintext and ciphertext. In relation to DIBE, Gong et. al. proposed a modified technique which is not vulnerable to CPA but vulnerable to occlusion attack [46].

Thus, with the aforementioned background of the diffractive-imaging based encryption technique and asymmetric UMD scheme, a new cryptosystem is proposed which resists the vulnerability of the UMD-based method to the special attack. Therewith, the proposed method is also capable of overcoming the vulnerability of diffractive imaging-based encryption [45].

In this paper first an attack to UMD based cryptosystem is applied and the results shows that information about plaintext is retrieved. Then, a hybrid method is proposed using simple diffractive imaging-based encryption along with unequal modulus decomposition in Fresnel domain. The various Fresnel parameters such as propagation distance and wavelength help to enlarge the key space and are very sensitive to their original values. The remaining paper is

[a]Department of Computer Science, Banasthali Vidyapith, Banasthali,Rajasthan,India- 304022

organized as follows: Section 2 explains about the basic principle behind the UMD and basic definition of Fresnel domain. Section 3 gives explanation about the proposed cryptosystem based on diffractive imaging and UMD. Section 4 is about to discuss the results generated using proposed cryptosystem and attack analysis. In the last section the conclusion about the paper is presented.

2. Theoretical analysis

2.1 Fresnel Transform

The Fresnel transform (FrT) of an input image $f(x,y)$, when it is illuminated by a plane wave of wavelength λ and at a propagation distance z can be written [5-7] as

$$F(u,v) = FrT_{\lambda,z}\{f(x,y)\} = \iint_{-\infty}^{+\infty} f(x,y)\, h_{\lambda,z}(u,v,x,y)\, dxdy, \quad (1)$$

Here, the operator $FrT_{\lambda,z}$ denotes the Fresnel transform with parameters λ(wavelength) and z(distance), and $h_{\lambda,z}$ denotes kernel of the transform which is given by equation 2.

$$h_{\lambda,z}(u,v,x,y) = \frac{1}{\sqrt{i\lambda z}}\, exp\,(i\frac{2\pi z}{\lambda})\, exp\,\{\frac{i\pi}{\lambda z}\,(u-x)^2 + (v-y)^2\} \quad (2)$$

A useful property of the FrT is

$$FrT_{\lambda,z1}\{FrT_{\lambda,z2} f(x)\} = FrT_{\lambda,z1+z2}\{f(x)\} \quad (3)$$

To satisfy the Fresnel approximation, the distance parameters *z1* and *z2* are taken accordingly. In the adjacent planes, the distributions of complex amplitude are determined by a Fresnel transform with respect to propagation distances *z1*, *z2*, and wavelength λ. The propagation distance and wavelength serve as an additional key to the cryptosystem.

2.2 Unequal Modulus Decomposition

The method of decomposing a two-dimensional image into two independent phase masks having unequal phase and amplitude is known as unequal modulus decomposition. As graphically shown in Figure 1, input image $F(u,v)$ is decomposed into two vectors $F1$ and $F2$ having different phase and amplitude. Mathematically, any complex number is composed of two parts one is real and another is imaginary. And in coordinate system it can be expressed as a vector, where on horizontal axis (x-axis) the real part is represented while on vertical axis (y-axis) the imaginary part is represented as shown in Figure 1.

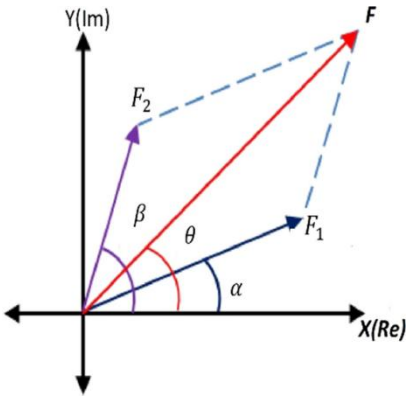

Fig.1 Graphical representation of UMD.

$$F1 = \frac{A\, sin\,(\beta - \phi)}{\sin\,(\beta - \alpha)}\, e^{j\alpha} \quad (4)$$

$$F2 = \frac{A\, sin\,(\phi - \alpha)}{sin\,(\beta - \alpha)}\, e^{\,j\beta} \quad (5)$$

Here, A and ϕ represents the amplitude and phase of image $F(u,v)$ as $A = |F(u,v)|$ and $\phi = arg[F(u,v)]$ and the functions α and β randomly generated in the interval $[0, 2\pi]$.

3. Proposed Cryptosystem

3.1 Encryption procedure

The encryption part of the proposed cryptosystem mainly consists of composition of three main steps:
(1) Applying the single diffractive imaging-based encryption on the input image
(2) Bonding of random phase mask on the intermediate image obtained from the first step and in the last step
(3) Unequal modulus decomposition is applied and finally the encrypted image is obtained.

Step 1: In order to describe the proposed scheme, a schematic diagram of the optical image encryption based on diffractive imaging is shown in Figure 2. Here, I stands for the initial image which is taken for the encryption, $R1, R2$ and $R3$ represents random phase masks, which are independent and randomly chosen in between $[0, 2\pi]$. A

monochromatic plane wave of wavelength λ is illuminated in the system. The complex wavefront just before the phase mask $R2$ is represented as:

$$A(\eta, \xi) = FrT\{I(x, y)R1(x, y); \lambda; d1\} \quad (6)$$

Using the same base, the diffraction pattern recorded on the CCD camera is mathematically represented as:

$$I1(u, v) = |FrT[FrT\{FrT\{I(x, y)R1(x, y); d1\}R2(\eta, \xi); z2\}R3(p, q); z3]|^2 \quad (7)$$

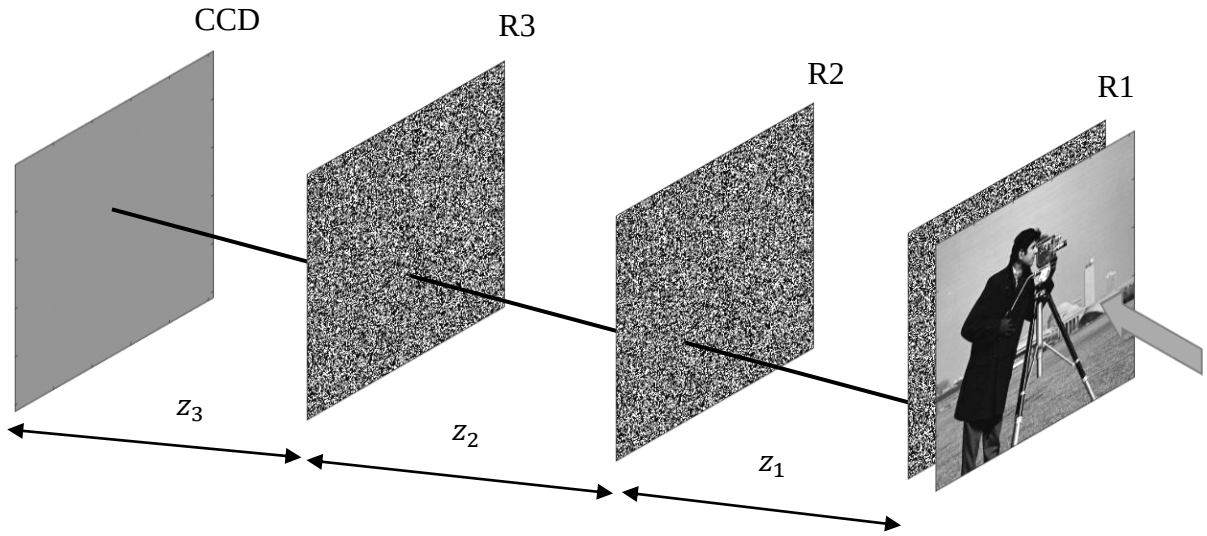

Fig. 2 A schematic setup used for diffractive imaging based optical image encryption.

Here, $||$ denotes a modulus operator and $I1(u, v)$ is captured as the ciphertext which is an intermediate image for the proposed scheme which is supplied to the next step.

Step 2: In double random phase encoding two independent phase masks are used. Now, the intermediate image obtained from the diffractive imaging step goes under the DRPE procedure. The intensity pattern obtained from first step i.e., $I1(u, v)$ is multiplied with first random phase mask and then Fresnel propagated and in the same manner then the resultant image is multiplied with second random phase mask and propagated to get the resultant image as shown in the below equation:

$$I2(p, q) = FrT\{FrT\{I1(u, v)RPM1(u, v)\}\, RPM2(m, n)\} \quad (8)$$

where RPM1 and RPM2 denotes the random phase mask one and two respectively.

Step 3: In the next step unequal modulus decomposition is applied on the resultant image and we get final encrypted image and private key.

$$[P1, P2] = UMD_{\alpha,\beta}\big(I2(p, q)\big) \quad (9)$$

The values of α and β are generated randomly in the interval $[0, 2\pi]$ and they are used for decomposing $I2$ in two vectors $P1$ and $P2$. Here, $P1$ is the obtained encrypted image and $P2$ is saved as private key which is stored for later use. The steps of the encryption algorithm in form of flowchart are shown in figure 3.

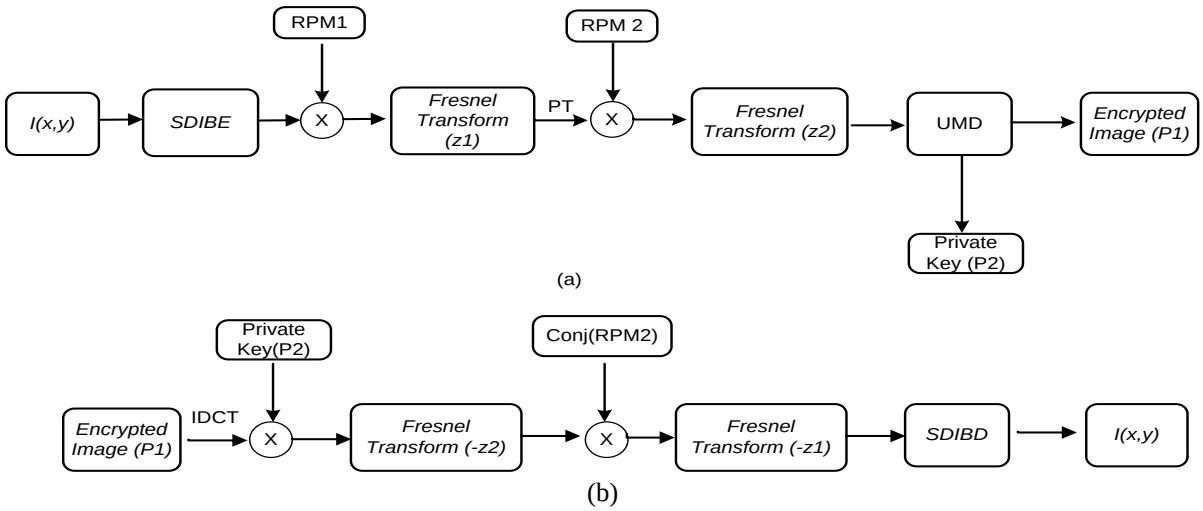

Fig. 3 Flowchart of the proposed scheme (a) encryption; (b) decryption process.

3.2 Decryption procedure

In the decryption process of the proposed cryptosystem involves following steps:

1. Firstly, multiplication operation is applied on the ciphertext obtained $P1$ and the private key $P2$.
2. The result obtained is Fresnel propagated with distance $-z2$ or we can say that apply inverse Fresnel propagation with $z2$ propagation distance.
3. After that, conjugate of second random phase mask is multiplied with the resultant and again Fresnel propagated with distance $-z1$.
4. Then, apply the iterative decryption process for the diffractive imaging as proposed by Qin et.al. [43].

The iterative procedure involves two cycles: cycle A and cycle B; the flowchart for these two cycles is shown in Figure. 4 and 5.

Cycle A: First, an initial estimation for $n = 1$ of the plaintext $T_n(x, y)$ is taken for the initialization and propagated in forward direction to the CCD plane as shown below:

$$U_n(u, v) = FrT[FrT\{FrT\{T_n(x, y)R1(x, y); d1\}R2(\eta, \xi); z2\}R3(p, q); z3] \quad (10)$$

After that the square root of the intensity pattern is used to update the $U_n(u, v)$.

$$\overline{U_n(u, v)} = \frac{I1(u, v)^{\frac{1}{2}} U_n(u, v)}{|U_n(u, v)|} \quad (11)$$

Thereafter, this obtained amplitude is propagated in reverse direction to the input plane and the obtained intensity is shown as:

$$\overline{T'_n(x, y)} = \left|FrT\left[FrT\{FrT\{\overline{U_n(u, v)}; -z3\}R3^*(p, q); -z2\}R2^*(\eta, \xi); -z1\right]\right|^2 \quad (12)$$

Here, * denotes the conjugate operation and then a low pass filtering operation is applied and estimated plaintext is computed as

$$\overline{T_n(x, y)} = LPFilter\left[\overline{T'_n(x, y)}\right] \quad (13)$$

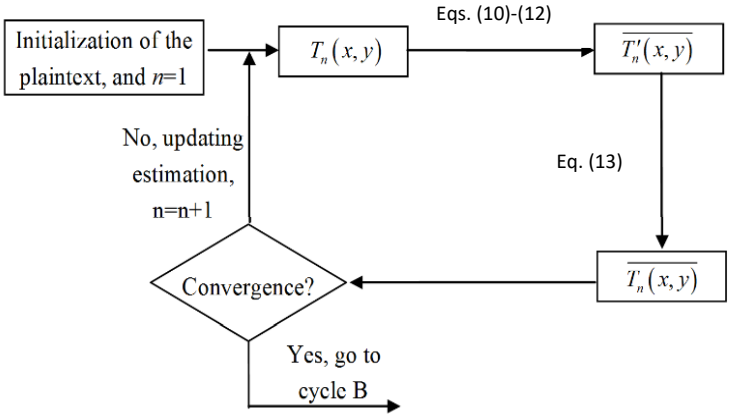

Fig. 4. Flow chart for illustrating cycle A.

Now, $\overline{T_n(x, y)}$ is taken as the new substitute of $T_n(x, y)$. This procedure from equation 10-13 will continue until the iterative error computed between $T_{n-1}(x, y)$ and $T_n(x, y)$ is less than the preset threshold value which is computed using eq. 14.

$$Error_1 = \sum [|T_n(x, y)| - |T_{n-1}(x, y)|]^2 \quad (14)$$

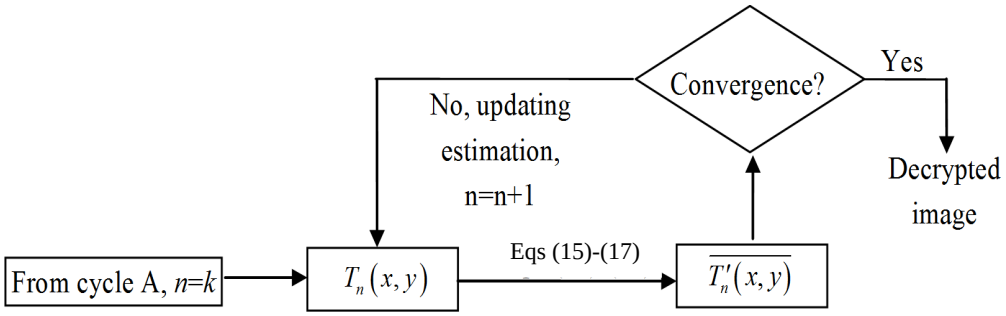

Fig. 5. Flow chart for illustrating cycle B.

Cycle B: On fulfilling the convergence condition i.e., error less than threshold value, iteration procedure of cycle A is stopped and the iterative procedure of cycle B starts. Suppose the cycle A terminated at $n = k$, now $T_n(x, y), n = k$ is taken as the new estimated plaintext for cycle B and in the same manner to that of equation 10 the estimated plaintext is propagated to the CCD plane as given in equation 15.

$$U_n(u, v) = FrT[FrT\{FrT\{T_n(x, y)R1(x, y); d1\}R2(\eta, \xi); z2\}R3(p, q); z3] \quad (15)$$

Now, the intensity pattern $I1(u, v)$ serves as the support constraint in real part of $U_n(u, v)$.

$$\overline{U_n(u, v)} = \frac{I1(u, v)^{\frac{1}{2}} U_n(u, v)}{|U_n(u, v)|} \quad (16)$$

Thereafter, $\overline{U_n(u, v)}$ is back propagated to the input plane and the obtained intensity is computed as:

$$\overline{T'_n(x, y)} = \left|FrT\left[FrT\{FrT\{\overline{U_n(u, v)}; -z3\}R3^*(p, q); -z2\}R2^*(\eta, \xi); -z1\right]\right|^2 \quad (17)$$

Then, $\overline{T'_n(x, y)}$ will be used in place of $T_n(x, y)$ and this iterative procedure continues until the computed value of $Error2$ is not larger than the preset threshold value. When the terminated condition meets, the iterative procedure is stopped and $\overline{T'_n(x, y)}$ is taken as the decrypted image.

$$Error_2 = \sum \left[\left|\overline{T'_n(x, y)}\right| - \left|\overline{T'_{n-1}(x, y)}\right|\right]^2 \quad (18)$$

4. Simulations and Results

The proposed scheme is numerically simulated on the MATLAB platform (R2016a). Simulations results have been studied to check the feasibility, robustness and security of the proposed method for a number of images. But results have been shown only for the image of Cameraman of size 256×256 pixels. The provided input image of Cameraman is subjected to the first part of encryption process where the diffractive intensity patterns are recorded in Fresnel domain which is followed by bonding with the phase masks and then finally the unequal modulus decomposition is applied. During this process, the Fresnel parameters $\lambda = 632.8nm$ and the propagation distances $z1 = 10mm, z2 = 20mm$ and $z3 = 30mm$ are taken into consideration.

The input image, the encrypted image, generated private key and the retrieved image are shown in Figure 6.

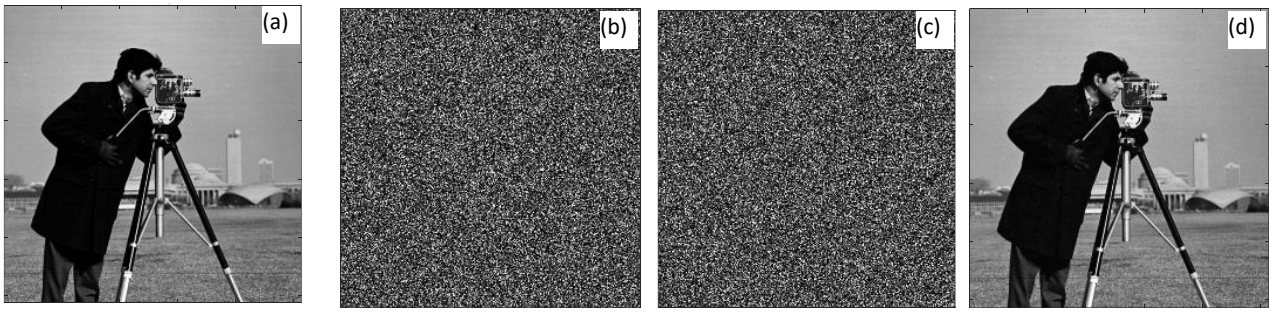

Fig. 6 Validation results for the proposed scheme (a) input image of cameraman (b) private key; (c) corresponding encrypted image; (d) decrypted image

The evaluate the performance of proposed architecture and quality of the decrypted image, various statistical metrics such as peak signal to noise ratio (PSNR), correlation coefficient (CC) and mean square error (MSE) are used which are computed using the formula:

$$CC = \frac{\sum_{p=1}^{M}\sum_{q=1}^{N}\left|(I_{inp}(p,q) - \overline{I_{inp}(p,q)})(I_{rec}(p,q) - \overline{I_{rec}(p,q)})\right|}{\sqrt{\sum_{p=1}^{M}\sum_{q=1}^{N}(I_{inp}(p,q) - \overline{I_{inp}(p,q)})^2}\sqrt{\sum_{p=1}^{M}\sum_{q=1}^{N}(I_{rec}(p,q) - \overline{I_{rec}(p,q)})^2}} \quad (19)$$

where $\overline{I_{inp}(p,q)}$ and $\overline{I_{rec}(p,q)}$ gives the mean value of input image and recovered image respectively.

$$MSE = \frac{1}{M \times N}\sum_{p=1}^{M}\sum_{q=1}^{N}\left|I_{inp}(p,q) - I_{rec}(p,q)\right|^2 \quad (20)$$

herein $M \times N$ denotes the number of pixels.

$$PSNR = 10 \times \log_{10}\frac{255^2}{MSE} \quad (21)$$

Table 1 : MSE, PSNR, and CC between input and retrieved images.

Statistical Measure	Values
MSE	$1.2226e^{-4}$
$PSNR$	200.9361
CC	0.9990

4.1 Information Entropy

Information entropy for the proposed scheme is analysed. Entropy computes [47] the content of the image. The level of randomness, disorder, the uncertainty of an image, quantified by the entropy. The value of information entropy for a grayscale image falls in between the interval $[0, 8]$. The maximum value of entropy of an image computes the high level of randomness. The entropy of encoded image is 7.7236. More the entropy value tends towards the maximum value, it indicates that the encoded image does not reveal any clue about the input image.

4.2 Statistical Attack Analysis

The histogram is a statistical attack, which gives the relation between the gray level of image and image frequency. For a good encryption scheme, the pixels of an encrypted image are uniformly distributed. To check the efficacy of the proposed cryptosystem, the histogram attack is analyzed for grayscale input image of Cameraman of size 256×256 pixels. Figure 7 shows the histogram and 3D plot of grayscale image. It is clear from the Figure 7(b) that the encoded image histogram is entirely different from input and retrieved image histogram and it tells no clue about the input image. The same results are revealed from the 3D plot analysis that is the plot of encoded image as shown in Figure 7(d) is quite random which does not disclose any data about the input image and the 3D plots of input and decoded image are same.

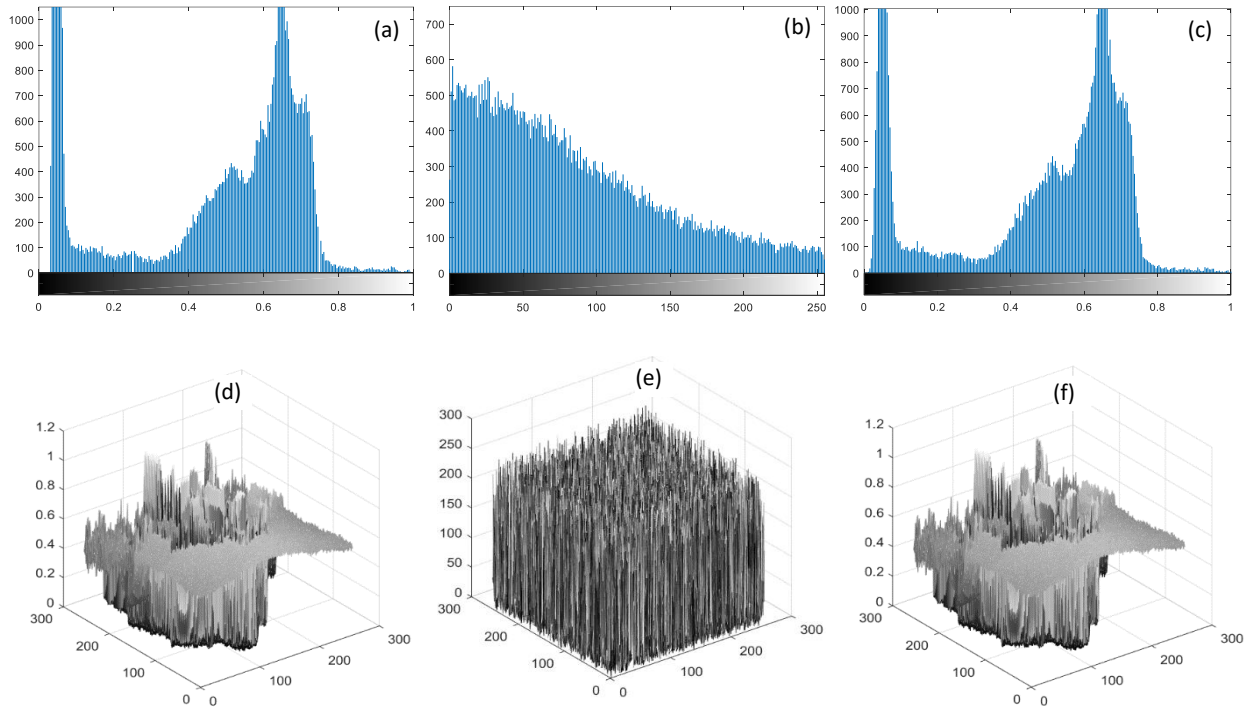

Fig. 7 Histogram analysis of (a) grayscale input image; (b) encrypted image; (c) corresponding decrypted image; 3D plot analysis of (d) grayscale input image; (e) encrypted image; (f) decrypted image.

4.3 Correlation distribution analysis

Correlation distribution analysis is another way to show the performance of an encryption algorithm. In this case, we have plotted the 8000 pixels from input image given to the scheme and encrypted image in horizontal, diagonal and vertical directions. It is noted from the Figure 8 that input image pixels shows high correlation with their adjacent pixels in horizontal, vertical and diagonal directions as shown in Figure 8(a, c, e) but from the plot of encrypted image no detectable correlation is found as shown in Figure 8(b, d, f).

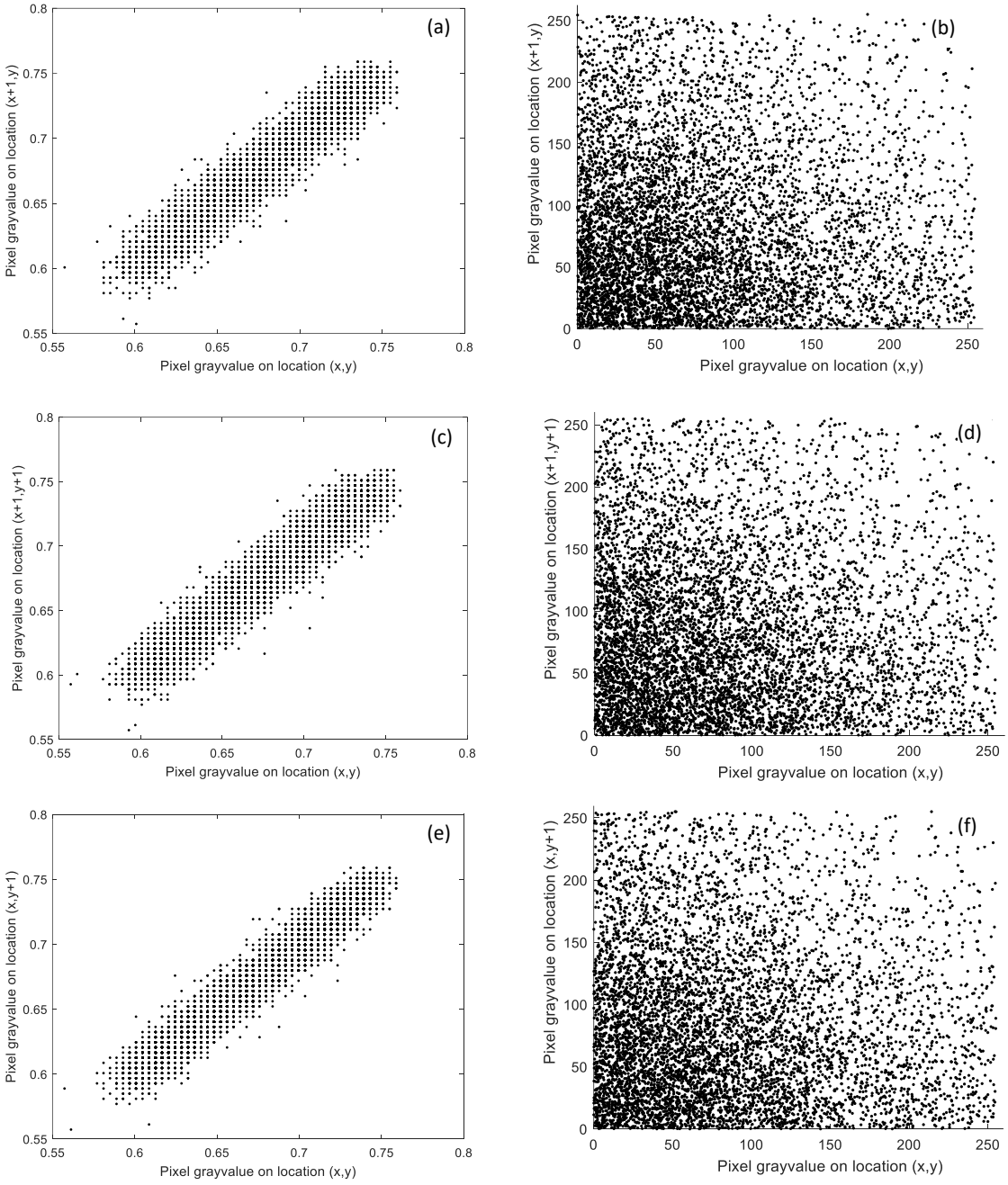

Fig. 8. Correlation distribution analysis of the plaintext image (a, c, e) and its encrypted image (b, d, f) in horizontal, diagonal and vertical direction respectively.

4.4 Special Attack analysis

The proposed scheme's performance is analyzed for a special attack proposed by Wang et.al. [48] which can be applied on the equal modulus-based cryptosystems. The results in Figure 9(a) shows that the retrieved image can be recognized which is obtained by applying the Wang attack on a scheme which is based on diffractive imaging and EMD [31]. Because in EMD based scheme the modulus of private key and ciphertext are same so if any attacker knows about the scheme and ciphertext, then he/she can retrieve the private key and then finally can obtain the information about the

plaintext. Here, we have tested the performance of the proposed scheme against this attack and the results shows that the retrieved image does not reveal any leakage about the input image even after 1500 iterations as shown in Figure 9(b).

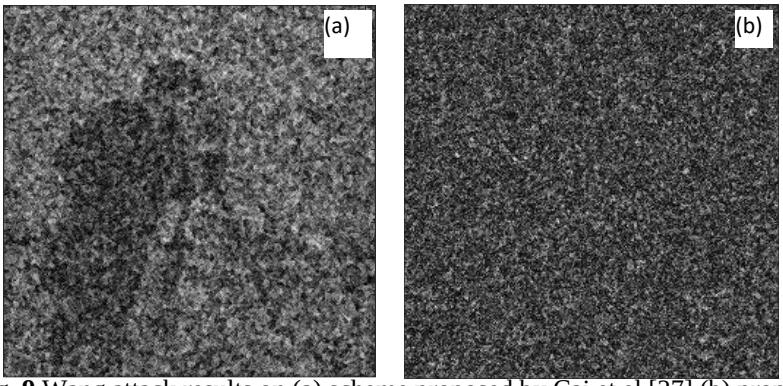

Fig. 9 Wang attack results on (a) scheme proposed by Cai et.el.[27] (b) proposed scheme

5. Conclusion and Future research Suggestion

A new secure optical asymmetric cryptosystem using unequal decomposition and diffractive imaging in Fresnel domain is proposed. The security is enhanced by enlarging the key space using Fresnel parameters. The feasibility and security of the proposed scheme are signified by numerical simulations in MATLAB environment performed on grayscale images using histogram, 3D plot analysis, entropy analysis and correlation distribution analysis. High resistance to various types of attack is achieved using the proposed scheme, while keeping the asymmetric characteristics of the cryptosystem. Further the extension of the proposed scheme can be checked for color images and for the encryption of multiple images.

6. References:

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

[2] B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.*, vol. 25, no. 1, p. 28, Jan. 2000, doi: 10.1364/OL.25.000028.

[3] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Appl. Opt.*, vol. 41, no. 26, p. 5462, Sep. 2002, doi: 10.1364/AO.41.005462.

[4] Y. Wang, C. Quan, and C. J. Tay, "Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask," *Opt. Commun.*, vol. 344, pp. 147–155, Jun. 2015, doi: 10.1016/j.optcom.2015.01.045.

[5] H. Xu, W. Xu, S. Wang, and S. Wu, "Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain," *Opt. Commun.*, vol. 402, pp. 302–310, Nov. 2017, doi: 10.1016/j.optcom.2017.05.035.

[6] H. Chen, C. Tanougast, Z. Liu, and L. Sieler, "Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains," *Opt. Lasers Eng.*, vol. 93, pp. 1–8, Jun. 2017, doi: 10.1016/j.optlaseng.2017.01.005.

[7] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Fully phase image encryption using double random-structured phase masks in gyrator domain," *Appl. Opt.*, vol. 53, no. 28, p. 6472, Oct. 2014, doi: 10.1364/AO.53.006472.

[8] R. Kumar, B. Bhaduri, and B. Hennelly, "QR code-based non-linear image encryption using Shearlet transform and spiral phase transform," *J. Mod. Opt.*, vol. 65, no. 3, pp. 321–330, Feb. 2018, doi: 10.1080/09500340.2017.1395486.

[9] M. Chen, G. Ma, C. Tang, and Z. Lei, "Generalized optical encryption framework based on Shearlets for medical image," *Opt. Lasers Eng.*, vol. 128, p. 106026, May 2020, doi: 10.1016/j.optlaseng.2020.106026.

[10] H. Chen, L. Zhu, Z. Liu, C. Tanougast, F. Liu, and W. Blondel, "Optical single-channel color image asymmetric cryptosystem based on hyperchaotic system and random modulus decomposition in Gyrator domains," *Opt. Lasers Eng.*, vol. 124, p. 105809, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105809.

[11] E. Kumari, P. Singh, S. Mukherjee, and G. Purohit, "Optical Chaotic Cryptosystem for Phase Images Using Random Amplitude and Phase Masks with Lorenz Map in Fresnel Domain," 2020, pp. 1–13. doi: 10.1007/978-981-15-5414-8_1.

[12] E. Kumari, S. Mukherjee, P. Singh, and R. Kumar, "Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain," *Results Opt.*, vol. 1, p. 100005, Nov. 2020, doi: 10.1016/j.rio.2020.100005.

[13] E. Kumari, P. Singh, S. Mukherjee, and G. N. Purohit, "Analysis of triple random phase encoding cryptosystem in Fresnel domain," *Results Opt.*, vol. 1, p. 100009, Nov. 2020, doi: 10.1016/j.rio.2020.100009.

[14] G. Sun, W. Song, M. Tian, C. Tanougast, Z. Liu, and H. Chen, "A novel optical video cryptosystem based on improved 3D arnold transform in gyrator domains," *Opt. Laser Technol.*, vol. 168, p. 109891, Jan. 2024, doi: 10.1016/j.optlastec.2023.109891.

[15] "Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain - Singh - 2018 - IET Image Processing - Wiley Online Library." Available: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ipr.2018.5399
[16] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.*, vol. 31, no. 8, p. 1044, Apr. 2006, doi: 10.1364/OL.31.001044.
[17] H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, "Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack," *Opt. Express*, vol. 18, no. 13, p. 13772, Jun. 2010, doi: 10.1364/OE.18.013772.
[18] "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding." Available: https://opg.optica.org/oe/fulltext.cfm?uri=oe-23-15-18955&id=322640
[19] W. Qin, "Vulnerability to chosen-plaintext attack of optoelectronic information encryption with phase-shifting interferometry," *Opt. Eng.*, vol. 50, no. 6, p. 065601, Jun. 2011, doi: 10.1117/1.3590725.
[20] K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext–ciphertext pairs," *Appl. Opt.*, vol. 53, no. 28, p. 6435, Oct. 2014, doi: 10.1364/AO.53.006435.
[21] Z. Liu, H. Chen, W. Blondel, Z. Shen, and S. Liu, "Image security based on iterative random phase encoding in expanded fractional Fourier transform domains," *Opt. Lasers Eng.*, vol. 105, pp. 1–5, Jun. 2018, doi: 10.1016/j.optlaseng.2017.12.007.
[22] Y. Xiong, R. Kumar, and C. Quan, "Security Analysis on an Optical Encryption and Authentication Scheme Based on Phase-Truncation and Phase-Retrieval Algorithm," *IEEE Photonics J.*, vol. 11, no. 5, pp. 1–14, Oct. 2019, doi: 10.1109/JPHOT.2019.2936236.
[23] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Security analysis of optical encryption," presented at the European Symposium on Optics and Photonics for Defence and Security, E. M. Carapezza, Ed., Bruges, Belgium, Oct. 2005, p. 598603. doi: 10.1117/12.633677.
[24] X. Wang, Y. Chen, C. Dai, and D. Zhao, "Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform," *Appl. Opt.*, vol. 53, no. 2, p. 208, Jan. 2014, doi: 10.1364/AO.53.000208.
[25] Y. Wang, C. Quan, and C. J. Tay, "Improved method of attack on an asymmetric cryptosystem based on phase-truncated Fourier transform," *Appl. Opt.*, vol. 54, no. 22, p. 6874, Aug. 2015, doi: 10.1364/AO.54.006874.
[26] X. Wang and D. Zhao, "A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Commun.*, vol. 285, no. 6, pp. 1078–1081, Mar. 2012, doi: 10.1016/j.optcom.2011.12.017.
[27] "Cyphertext-only attack on the double random-phase encryption: Experimental demonstration." Available: https://opg.optica.org/oe/fulltext.cfm?uri=oe-25-8-8690&id=362781
[28] Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.*, vol. 33, no. 21, p. 2443, Nov. 2008, doi: 10.1364/OL.33.002443.
[29] Q. Wang, "Optical image encryption with silhouette removal based on interference and phase blend processing," *Opt. Commun.*, vol. 285, no. 21–22, pp. 4294–4301, Oct. 2012, doi: 10.1016/j.optcom.2012.06.071.
[30] X. Wang and D. Zhao, "Optical image hiding with silhouette removal based on the optical interference principle," *Appl. Opt.*, vol. 51, no. 6, p. 686, Feb. 2012, doi: 10.1364/AO.51.000686.
[31] J. Cai, X. Shen, M. Lei, C. Lin, and S. Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Lett.*, vol. 40, no. 4, p. 475, Feb. 2015, doi: 10.1364/OL.40.000475.
[32] A. Fatima, I. Mehra, and N. K. Nishchal, "Optical image encryption using equal modulus decomposition and multiple diffractive imaging," *J. Opt.*, vol. 18, no. 8, p. 085701, Aug. 2016, doi: 10.1088/2040-8978/18/8/085701.
[33] J. Wu, W. Liu, Z. Liu, and S. Liu, "Cryptanalysis of an 'asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition,'" *Appl. Opt.*, vol. 54, no. 30, p. 8921, Oct. 2015, doi: 10.1364/AO.54.008921.
[34] J. Cai and X. Shen, "Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Laser Technol.*, vol. 95, pp. 105–112, Oct. 2017, doi: 10.1016/j.optlastec.2017.04.018.
[35] P. Rakheja, R. Vig, and P. Singh, "Optical asymmetric watermarking using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain," *Optik*, vol. 176, pp. 425–437, Jan. 2019, doi: 10.1016/j.ijleo.2018.09.088.
[36] P. Rakheja, R. Vig, and P. Singh, "Asymmetric hybrid encryption scheme based on modified equal modulus decomposition in hybrid multi-resolution wavelet domain," *J. Mod. Opt.*, vol. 66, no. 7, pp. 799–811, Apr. 2019, doi: 10.1080/09500340.2019.1574037.
[37] P. Rakheja, R. Vig, P. Singh, and R. Kumar, "An iris biometric protection scheme using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain," *Opt. Quantum Electron.*, vol. 51, no. 6, p. 204, Jun. 2019, doi: 10.1007/s11082-019-1921-x.
[38] J. Wang, X. Chen, J. Zeng, Q.-H. Wang, and Y. Hu, "Asymmetric Cryptosystem Using Improved Equal Modulus Decomposition in Cylindrical Diffraction Domain," *IEEE Access*, vol. 7, pp. 66234–66241, 2019, doi: 10.1109/ACCESS.2019.2917994.

[39] J. Cai, X. Shen, and C. Lin, “Security-enhanced asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition,” *Opt. Commun.*, vol. 359, pp. 26–30, Jan. 2016, doi: 10.1016/j.optcom.2015.09.058.
[40] L. Chen, X. Gao, X. Chen, B. He, J. Liu, and D. Li, “A new optical image cryptosystem based on two-beam coherent superposition and unequal modulus decomposition,” *Opt. Laser Technol.*, vol. 78, pp. 167–174, Apr. 2016, doi: 10.1016/j.optlastec.2015.11.009.
[41] M. Abdelfattah, S. F. Hegazy, N. F. F. Areed, and S. S. A. Obayya, “Compact optical asymmetric cryptosystem based on unequal modulus decomposition of multiple color images,” *Opt. Lasers Eng.*, vol. 129, p. 106063, Jun. 2020, doi: 10.1016/j.optlaseng.2020.106063.
[42] W. Chen, X. Chen, and C. J. R. Sheppard, “Optical image encryption based on diffractive imaging,” *Opt. Lett.*, vol. 35, no. 22, p. 3817, Nov. 2010, doi: 10.1364/OL.35.003817.
[43] Y. Qin, Q. Gong, and Z. Wang, “Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme,” *Opt. Express*, vol. 22, no. 18, p. 21790, Sep. 2014, doi: 10.1364/OE.22.021790.
[44] Y. Qin, Z. Wang, and Q. Gong, “Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern,” *Appl. Opt.*, vol. 53, no. 19, p. 4094, Jul. 2014, doi: 10.1364/AO.53.004094.
[45] T. Li and Y. Shi, “Security risk of diffractive-imaging-based optical cryptosystem,” *Opt. Express*, vol. 23, no. 16, p. 21384, Aug. 2015, doi: 10.1364/OE.23.021384.
[46] Q. Gong, H. Wang, Y. Qin, and Z. Wang, “Modified diffractive-imaging-based image encryption,” *Opt. Lasers Eng.*, vol. 121, pp. 66–73, Oct. 2019, doi: 10.1016/j.optlaseng.2019.03.013.
[47] R. Lyda and J. Hamrock, “Using Entropy Analysis to Find Encrypted and Packed Malware,” *IEEE Secur. Priv. Mag.*, vol. 5, no. 2, pp. 40–45, Mar. 2007, doi: 10.1109/MSP.2007.48.
[48] Y. Wang, C. Quan, and C. J. Tay, “New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition,” *Appl. Opt.*, vol. 55, no. 4, p. 679, Feb. 2016, doi: 10.1364/AO.55.000679.