Hindawi Publishing Corporation
International Journal of Optics
Volume 2015, Article ID 926135, 13 pages
http://dx.doi.org/10.1155/2015/926135

Research Article

Optical Image Encryption Using Devil's Vortex Toroidal Lens in the Fresnel Transform Domain

Hukum Singh, A. K. Yadav, Sunanda Vashisth, and Kehar Singh

Department of Applied Sciences, The Northcap University, Sector 23-A, Gurgaon 122 017, India

Correspondence should be addressed to Hukum Singh; hukumsingh@ncuindia.edu

Received 4 September 2015; Accepted 10 December 2015

Academic Editor: Augusto Beléndez

We have carried out a study of optical image encryption in the Fresnel transform (FrT) domain, using a random phase mask (RPM) in the input plane and a phase mask based on devil's vortex toroidal lens (DVTL) in the frequency plane. The original images are recovered from their corresponding encrypted images by using the correct parameters of the FrT and the parameters of DVTL. The use of a DVTL-based structured mask enhances security by increasing the key space for encryption and also aids in overcoming the problem of axis alignment associated with an optical setup. The proposed encryption scheme is a lensless optical system and its digital implementation has been performed using MATLAB 7.6.0 (R2008a). The scheme has been validated for a grayscale and a binary image. The efficacy of the proposed scheme is verified by computing mean-squared-error (MSE) between the recovered and the original images. We have also investigated the scheme's sensitivity to the encryption parameters and examined its robustness against occlusion and noise attacks.

1. Introduction

In today's interconnected world, the security of information exchanged over a network is a critical issue. The safe storage and transmission of data continues to be a challenge because of increasing threats to the confidentiality, integrity, and availability of information. In the recent decades, optical processing techniques have provided effective solutions to some of these problems and therefore have become an active research field [1–8]. Optical security systems based on optoelectronics can perform highly accurate encryption and decryption in almost real time. The most widely known technique, first proposed by Refregier and Javidi [1], for optical image encryption is based on double random phase encoding (DRPE). The DRPE is an optically symmetric-key technique that encrypts a given image using two RPMs: one in the spatial plane and the other in the frequency plane. It may be implemented digitally or optically and has potential applications in many areas such as security verification systems, watermarking, information hiding, and multiple-image encryption.

In an attempt to strengthen security, the DRPE was further extended to several other transform domains such as the fractional Fourier [9, 10], Fresnel [11–23], gyrator [24, 25], and fractional Mellin [26, 27]. However, majority of these techniques use random phase keys making them vulnerable to a variety of plaintext and ciphertext attacks. It is also known that the conventional DRPE technique suffers from the problem of optical axis alignment. Several studies have attempted to overcome these problems by using structured phase mask (SPM), instead of RPM. The use of SPM offers additional advantage of having more encryption keys for enhanced security [28–31]. The SPM is generally made from a Fresnel zone plate (FZP) and a spiral phase plate (SPP). Barrera et al. [28, 29] introduced an SPM called toroidal zone plate (TZP). The TZPs are easier to position in the decoding and provide their own centering mask. They are diffractive optical element (DOE) and are very difficult to replicate. They have the properties of multiple keys in a single mask which provide extra security parameters. Rajput and Nishchal [30] used wavelength-dependent SPM instead of RPM in fractional Fourier transform domain to study a single-channel asymmetric color image encryption scheme. Their scheme alleviates the alignment problem of interference and does not need to iterate encoding and offers multiple levels of security. Abuturab [31] introduced a new method for encoding color information based on Arnold transformation and double structured phase mask in gyrator transform domain.

In the present work, we propose for the first time a new scheme for image encryption using a DVTL-based phase mask in the FrT domain. The use of FrT possesses an advantage over Fourier domain by providing additional parameters such as propagation distances (z_1, z_2) and propagation wavelength (λ_p) which constitutes the keys to the encryption process. The paper is organized as follows: in Section 2, we present a brief mathematical description of FrT, formation of DVTL, and the encryption-decryption scheme. Section 3 contains the results based on computer simulations for validation and evaluation of the scheme's performance. Finally, the conclusions of the study are summarized in Section 4.

2. Principle

2.1. The Fresnel Transform. The Fresnel transform (FrT) of an input image $f(x, y)$ at a propagation distance z, when it is illuminated by a plane wave of wavelength λ can be written [32, 33] as

$$F_z(u, v) = \mathrm{FrT}_{\lambda,z}\{f(x, y)\} = \iint_{-\infty}^{+\infty} f(x, y)\, h_{\lambda,z}(u, v, x, y)\, dx\, dy, \tag{1}$$

where the operator $\mathrm{FrT}_{\lambda,z}$ denotes the Fresnel transform with parameters λ and z and $h_{\lambda,z}$ is the kernel of the transform given by

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

A useful property of the FrT is

$$\mathrm{FrT}_{\lambda,z_1}\left\{\mathrm{FrT}_{\lambda,z_2} f(x)\right\} = \mathrm{FrT}_{\lambda,z_1+z_2}\{f(x)\}. \tag{3}$$

The distance parameters z_1 and z_2 are selected according to the size of the aperture to satisfy the Fresnel approximation. The distributions of complex amplitude in the adjacent planes are determined by a Fresnel transform with respect to z_1, z_2, and λ.

2.2. DVTL-Based Phase Mask. A phase mask based on devil's lens can be described by one-dimensional Cantor function [34], a particular case of devil's staircase. A triadic Cantor set in the interval [0, 1] can be defined as [34, 35]

$$F_S(x) = \begin{cases} \dfrac{l}{2^S} & \text{if } p_{S,l} \le x \le q_{S,l} \\ \dfrac{1}{2^S}\dfrac{x - q_{S,l}}{p_{S,l+1} - q_{S,l}} + \dfrac{l}{2^S} & \text{if } q_{S,l} \le x \le p_{S,l+1}, \end{cases} \tag{4}$$

where $F_S(0) = 0$, $F_S(1) = 1$, S is the order of Cantor function, and l defines the number of horizontal sections of the function, having a value from 0 to $2^S - 1$. Here, q and p are the start and end points of each segment of the Cantor set. For some basic values of S, the values of $q_{S,l}$ and $p_{S,l+1}$ are provided in [34, 36–40]. A DVTL can be constructed by combining a devil's lens, a Fresnel toroidal lens, and a vortex lens. A devil's lens is a circularly symmetric pure phase diffractive optical element and is defined as

$$D_S(\zeta) = e^{(-i2^{S+1}\pi F_S)}, \tag{5}$$

where $\zeta = (r/a)^2$ is the normalised quadratic radial coordinate and a is the lens radius. Thus, the phase variation along the radial coordinate is quadratic in each zone of the lens. The phase shift at the gap regions defined by the Cantor set is $-l2\pi$, with $l = 1 \cdots 2^S - 1$.

The radial Hilbert transform mask (RHM) is another SPM which can serve to make an image edge-enhanced relative to the input image in addition to increasing the key space. The radial Hilbert transform [41, 42] is expressed in terms of a vortex function as

$$V_m(\emptyset) = e^{(im\emptyset)}, \tag{6}$$

where $\emptyset$ is the azimuth angle and m is an integer denoting the order of transformation, also called topological charge. It is apparent that the opposite halves of any radial line of the mask have a relative phase difference of $m\pi$ radian. Therefore, for each radial line, we have the equivalent of a one-dimensional Hilbert transform of order m. The radial Hilbert transform can be helpful in aligning the axis of the optical setup.

Just as a Fresnel lens, the toroidal lens is based on quadratic phase change and is given by

$$L_{\lambda,f_0}(\zeta) = e^{\{-i\pi(r-r_0)^2/\lambda f_0\}}, \tag{7}$$

where f_0 is the focal length and λ is the wavelength of incident light. Now, a DVTL-based phase mask is obtained by taking the product of the three functions $D_S(\zeta)$, $V_m(\emptyset)$, and $L_{\lambda,f_0}(\zeta)$ as follows:

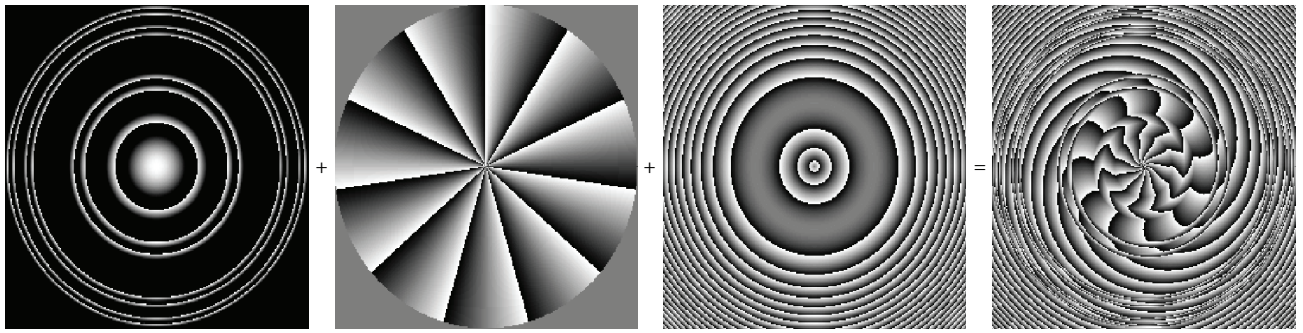
$$(\mathrm{DVTL})_{S,l,\lambda,f_0} = e^{i\{-2^{S+1}\pi F_S + m\emptyset - \pi(r-r_0)^2/\lambda f_0\}}. \tag{8}$$

A plot of DVTL, which is a combination of Devil's lens (DL), a vortex lens (VL), and Fresnel toroidal lens (TL), is shown in Figure 1.

2.3. The Encryption and Decryption Scheme. A flowchart of encryption and decryption process of the proposed scheme is presented in Figure 2. In this scheme, the input image $I(x, y)$ to be encrypted is first bonded with an RPM defined as $e^{2i\pi n(x,y)}$ in the input plane where $n(x, y)$ is uniformly distributed in [0, 1]. The resulting complex image is subjected to a Fresnel transform $\mathrm{FrT}_{\lambda,z_1}$. Then, in the frequency domain, it is bonded with an SPM based on $(\mathrm{DVTL})_{S=3}$ defined as $e^{i\{-2^{S+1}\pi F_S + m\emptyset - \pi(r-r_0)^2/\lambda f_0\}}$. Thereafter, it is subjected to another Fresnel transform $\mathrm{FrT}_{\lambda,z_2}$. Mathematically, the encryption process can be written as (see Figure 2(a))

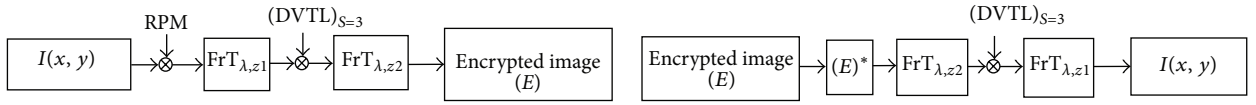
$$E(x, y) = \mathrm{FrT}_{\lambda,z_2}\left\{\left[\mathrm{FrT}_{\lambda,z_1}\{I(x, y) \times \mathrm{RPM}\}\right] \times (\mathrm{DVTL})_{S=3}\right\}. \tag{9}$$

The decryption process (Figure 2(b)) is the reverse of encryption with the following steps: the conjugated encrypted image E^* is first subjected to the Fresnel transform $\mathrm{FrT}_{\lambda,z_2}$. The resulting complex image is multiplied by



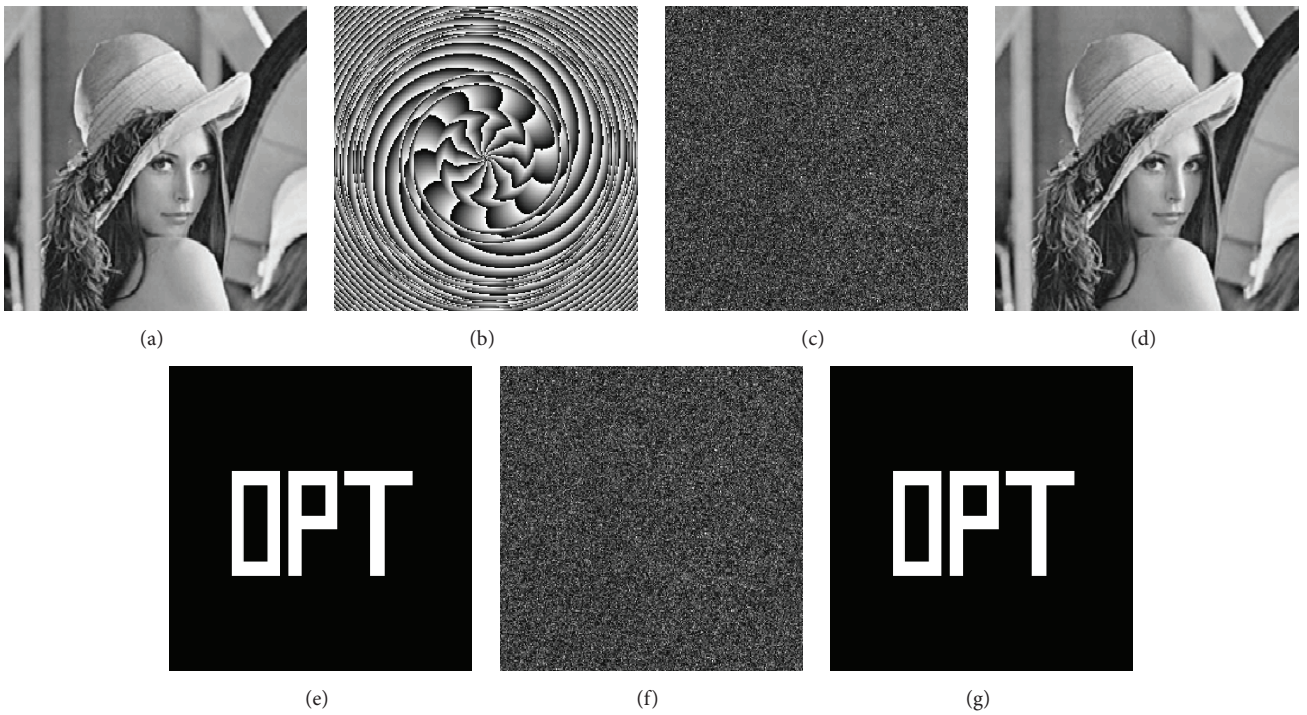
(a) (b) (c) (d)

Figure 1: Phase plots of each component which when combined result in Devil's vortex toroidal lens (DVTL); (a) DL for $S = 3$; (b) VL for $m = 11$; (c) TL; (d) DVTL.



(a) (b)

Figure 2: Flow chart of the proposed scheme: (a) encryption process and (b) decryption process.



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

(e) (f) (g)

Figure 3: Results of validation of the proposed scheme for grayscale and binary images: (a) input image Lena of size 256 × 256 pixels; (b) $\text{DVTL}_{S=3}$ phase key at pixel spacing = 0.023, $\lambda = 632.8$ nm, $f = 350$ mm, $m = 11$, and $S = 3$; (c) encrypted image; (d) decrypted image; (e) input binary image; (f) encrypted binary image; (g) decrypted binary image.

$(\text{DVTL})_{S=3}$ and then the FrT_{λ,z_1} is performed. Mathematical expression for decryption is given by

$$I(x, y) = \text{FrT}_{\lambda,z_1}\left[\text{FrT}_{\lambda,z_2}\{E^*(x, y)\} \times (\text{DVTL})_{S=3}\right], \quad (10)$$

where * denotes the complex conjugate.

3. Simulation Results and Discussion

The proposed scheme has been verified by performing numerical simulation on a MATLAB 7.6.0 (R2008a) platform. We have considered two test images of size 256 × 256 pixels as input, one grayscale image of Lena (Figure 3(a)) and the other binary image of OPT (Figure 3(e)). The structured

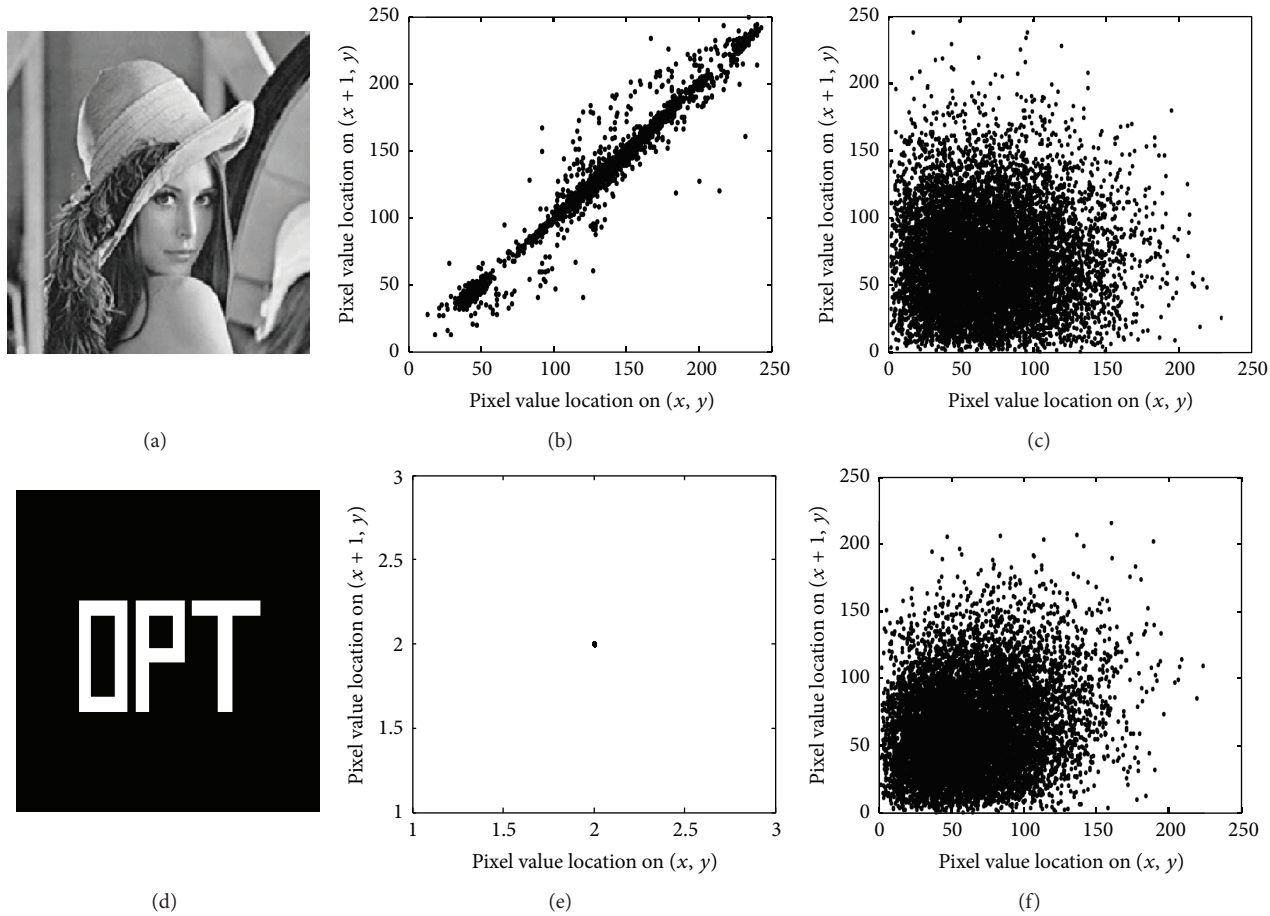


Figure 4: Plots of correlation distribution for randomly chosen 10,000 pixel pairs: (a) input image Lena; (b, c) correlation distribution respectively of input and encrypted image of Lena; (d) input image OPT; (e, f) correlation distribution, respectively, of input and encrypted image of OPT.

phase mask (DVTL) used in the frequency plane during encryption is shown in Figure 3(b). It is generated with parameter values as wavelength (λ) = 632.8 nm, focal length (f) = 350 mm, $m = 11$, $r_0 = 1.15$ mm, and $S = 3$. Figures 3(c) and 3(f) show the encrypted images of the grayscale and binary inputs, respectively, and are pure stationary white noise. The corresponding decrypted images are presented in Figures 3(d) and 3(g). The FrT parameters used in the present simulations are $z_1 = 25$ mm, $z_2 = 35$ mm, and propagation wavelength $\lambda_p = 632.8$ nm. These values have been taken arbitrarily and considered for the sake of simplicity. It can be seen from Figures 3(d) and 3(g) that the input images are faithfully recovered using all the correct parameters.

3.1. Correlation Coefficient (CC) Analysis. Correlation coefficient is a criterion used in the literature [26, 43, 44] to measure the similarity of two images quantitatively. It is obvious that arbitrarily chosen pixels of original images are generally highly correlated in horizontal, vertical, and diagonal directions. We know that CC of the encrypted images is much weaker than that of original images. However, a secure image encryption algorithm must produce an encrypted image having low CC between adjacent pixels. We have randomly selected 10,000 pairs of adjacent pixels (horizontal, vertical, or diagonal) for computation of CC from the input and the encrypted images separately. Then, the CC of each pair is calculated by the following relation [25]:

$$\mathrm{CC} = \frac{\sum_{i=1}^{N} (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\left(\sum_{i=1}^{N} (x_i - \overline{x})^2\right)\left(\sum_{i=1}^{N} (y_i - \overline{y})^2\right)}}, \tag{11}$$

where $\overline{x} = \sum_{i=1}^{N} x_i$ and $\overline{y} = \sum_{i=1}^{N} y_i$ are, respectively, the mean values of x_i and y_i.

The CC values of adjacent pixels in the horizontal, vertical, and diagonal directions of original images and their encrypted versions are given in Table 1. It is clear that, for the original images, the CC values are very high as compared to those of encrypted images. This clearly indicates that the adjacent pixels in the original images are strongly correlated. However, for the encrypted images, CC values are nearly zero, which means that the adjacent pixels in the horizontal, vertical, or diagonal directions are weakly correlated. Figure 4(a) shows the original image of Lena, whereas Figures 4(b) and 4(c) show the scatter plots of correlation distribution of horizontally adjacent pixels, respectively, in the original-, and the encrypted image. Similar information about the binary image OPT is shown in Figures 4(d)–4(f).

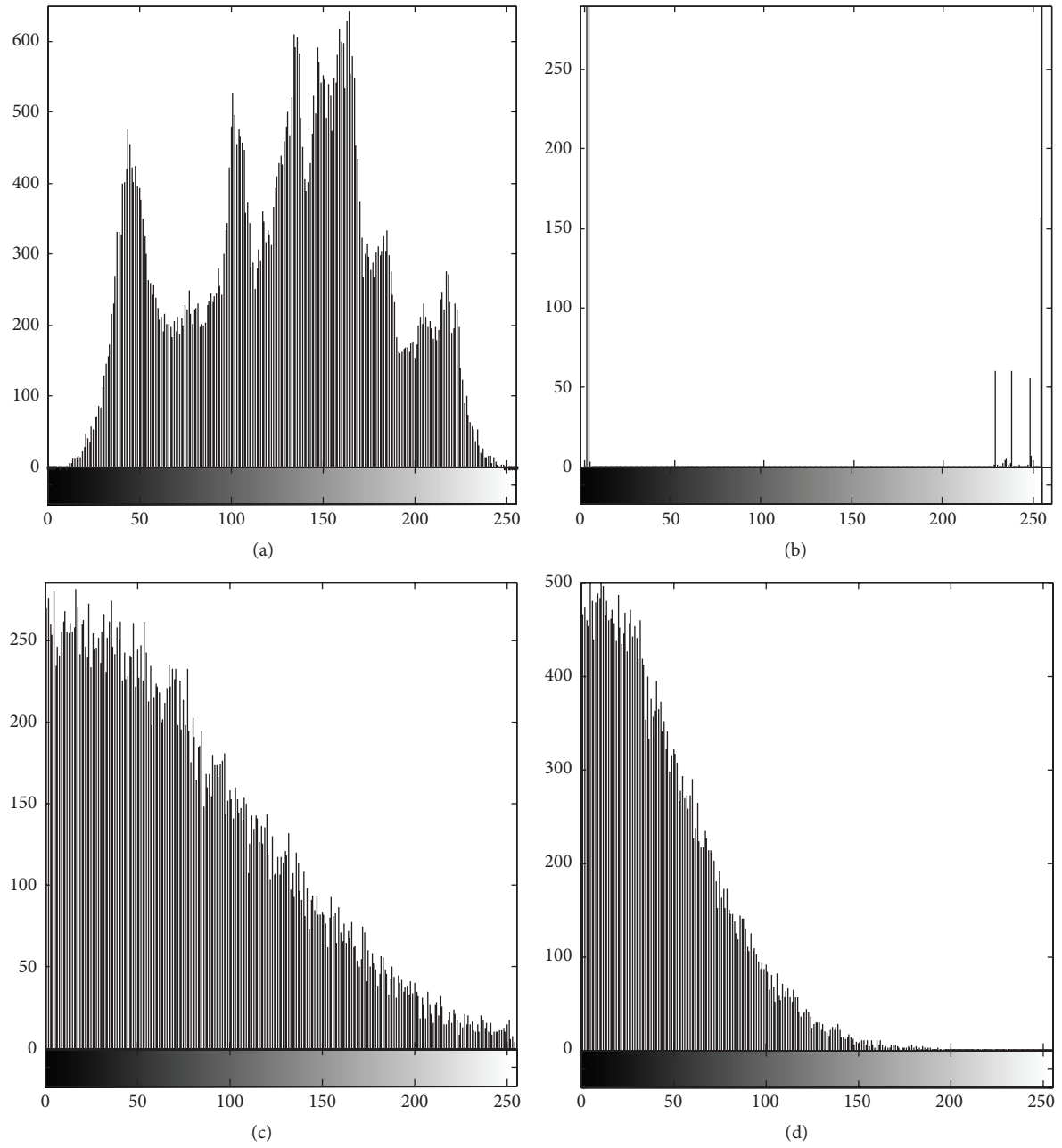


Figure 5: Histogram of (a) input image Lena, (b) input image OPT, (c) encrypted image Lena, and (d) encrypted image OPT.

Table 1

Image	Original image			Cipher image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Lena	0.9562	0.9509	0.9817	0.0093	0.0121	0.0086
OPT	0.9497	0.9354	0.9695	0.0106	0.0020	0.0092

3.2. Statistical Analysis

3.2.1. Histogram Analysis. Statistical analysis has been performed on the proposed image encryption algorithm. Image histogram is another very important feature in image analysis. Figures 5(a) and 5(b) show the histograms of Lena and OPT which are obviously quite different from each other. On the other hand, we observe that the histograms (Figures 5(c) and 5(d)) of their encrypted images are quite similar. After a number of simulations, we can conclude that the ciphertext of different original images have similar histograms. So,

Figure 6: Results with incorrect parameters of FrT: (a–c) decrypted images with incorrect values of z_1 = 25.3, 26, and 27 mm, (d–f) decrypted images with incorrect values of z_2 = 35.3, 36, and 37 mm, and (g–i) decrypted images with variation in λ_p by 10, 20, and 40 nm.

attackers cannot obtain useful information according to the statistical properties.

3.2.2. Image Entropy Analysis. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. A secure encryption should provide a situation in which the encrypted image does not provide any information about the original image. Image information entropy measures the distribution of image gray values. The more uniform the gray value distribution is, the bigger the information entropy is.

The entropy $H(s)$ of message source s can be calculated [26, 43, 44] as

$$H(s) = -\sum_{i=0}^{255} p(s_i) \log_2 p(s_i), \tag{12}$$

where $p(s_i)$ represents the probability of symbol s_i. The ideal value for the cipher information entropy is 8. The information entropy of the cipher-image of Lena and OPT generated by the proposed algorithm is 7.7484 and 7.1122.

3.3. Sensitivity Analysis. We have also examined the scheme's sensitivity to the individual encryption parameters by considering wrong parameter values. The recovered grayscale images for wrong parameters are shown, respectively, in Figures 6 and 7 for various parameters of FrT and DVTL. Figures 6(a)–6(c) correspond to minor-to-small deviation from the correct value of the propagation distance z_1 (=25.3 mm, 26 mm, and 27 mm, resp.). Similarly, Figures 6(d)–6(f) correspond to the second propagation distance z_2 (=35.3 mm, 36 mm, and 37 mm, resp.) and Figures 6(g)–6(i) correspond to the propagation wavelength λ_p (=642.8 nm, 652.8 nm, and 672.8 nm, resp.). In each case, even the minor change in parameter value results in significant drop in the quality of the recovered images (Figures 6(a), 6(d), and 6(g)), whereas it is barely recognizable in the third column (Figures 6(c), 6(f), and 6(i)) which corresponds to slightly higher departure from the correct value. It clearly shows that the proposed scheme is highly sensitive to FrT parameters. Likewise, the sensitivity to DVTL parameters is observed in Figure 7 for wrong values of the focal length (Figures 7(a)–7(c)), the wavelength

Figure 7: Results with incorrect parameters of DVTL: (a–c) decrypted images with incorrect focal lengths with deviation from correct value as 5, 10, and 50 mm, respectively, (d–f) decrypted images with incorrect λ with deviation from correct value as 10, 40, and 100 nm respectively, (g, h) decrypted images with incorrect topological charge with deviation from the correct value as 1 and 9, respectively, and (i) decrypted image with $S = 2$.

(Figures 7(d)–7(f)), the topological charge (Figures 7(g)-7(h)), and the devil's parameter S (Figure 7(i)).

In order to assess the efficacy of the proposed scheme, mean-squared-error (MSE) between the original input image and the decrypted image has been computed. If $I_0(x, y)$ and $I_d(x, y)$ denote, respectively, the pixel values of the original input image and the decrypted image, a mathematical expression for MSE can be written as

$$\text{MSE} = \sum_{x=0}^{255} \sum_{y=0}^{255} \frac{\left|I_0(x, y) - I_d(x, y)\right|^2}{256 \times 256}. \tag{13}$$

The computed values of MSE between the input and the recovered images for the grayscale and the binary images using the proposed scheme are 1.7087×10^{-20} and 2.3995×10^{-21}, respectively.

We have shown MSE plots for a wider range of values of FrT parameters in Figures 8(a)–8(c) and for DVTL parameters in Figures 8(d)–8(f). Each plot shows the MSE curves relative to the deviation from the correct parameter value for the grayscale and the binary inputs. It is clearly visible from the plots that the proposed algorithm is highly sensitive to the propagation parameters of FrT. Though the scheme is sensitive to DVTL parameters also, the variation in MSE is less steep. In all these subfigures, a comparison of the two curves indicates that the algorithm shows greater sensitivity for the grayscale as compared to the binary for each of the encryption parameters.

3.4. Occlusion Attack Analysis. We examine the robustness of the proposed algorithm against occlusion attacks on the encrypted image. The occluded images are shown in Figures 9(a)–9(d) for 10%, 25%, 50%, and 75% occlusion of the encrypted image of Lena. Figures 9(e)–9(h) show the corresponding decrypted images which are recovered fairly well even for occlusion up to 75%. Similar results are obtained when we tested the scheme's robustness for occlusion of the binary image (Figures 9(i)–9(l)). Additionally, we have

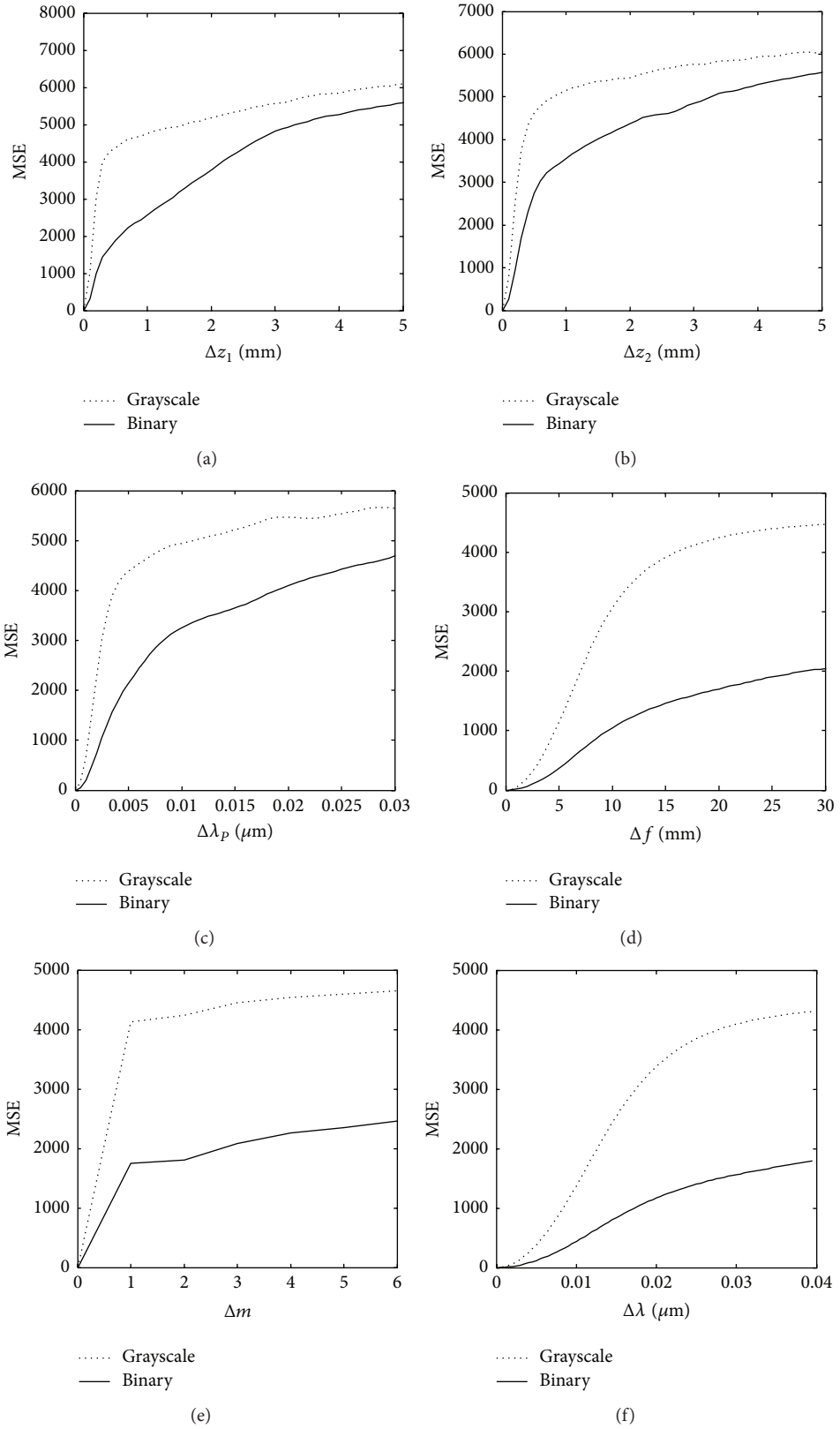


FIGURE 8: Sensitivity plots of MSE as a function of deviation from the correct values of various parameters of FrT and DVTL: (a) Δz_1 (mm), (b) Δz_2 (mm), (c) $\Delta\lambda_p$ (μm), (d) focal length f (mm), (e) topological charge m, and (f) wavelength λ (μm).

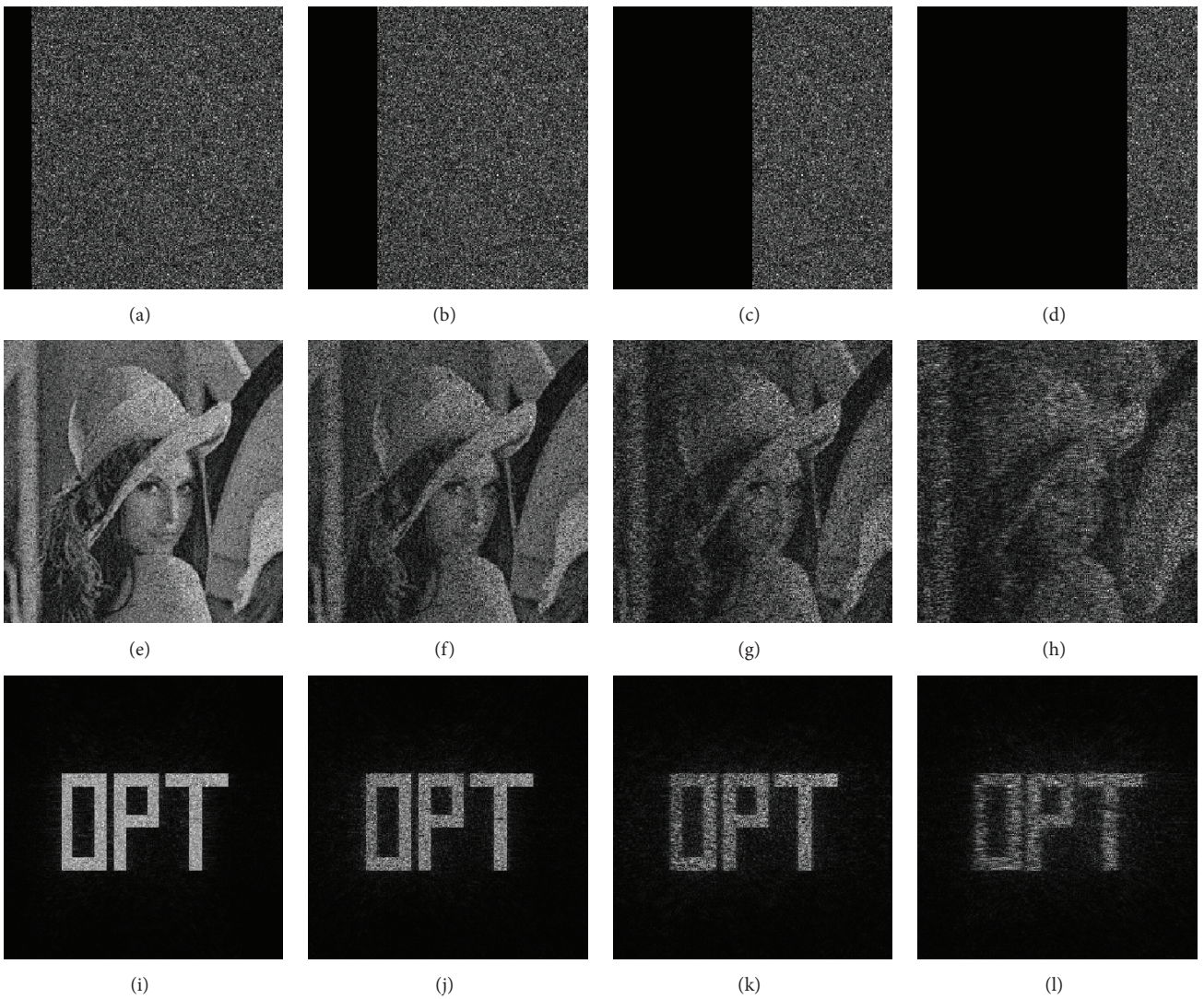


Figure 9: Occlusion results for the grayscale and the binary image for varying degrees of occlusion: encrypted image with (a) 10% occlusion, (b) 25% occlusion, (c) 50% occlusion, (d) 75% occlusion, (e–h) corresponding recovered grayscale images, and (i–l) corresponding recovered binary images.

plotted MSE and correlation coefficient (CC) against varying degrees of occlusion of the encrypted images (Figures 10(a)-10(b)). The variation of MSE and CC curves clearly indicates the scheme's robustness to occlusion attack. As expected, the binary image shows higher robustness as compared to the grayscale image.

3.5. Noise Attack Analysis. It is inevitable that the noise impacts directly the quality of the decrypted image. We have also tested the strength of the proposed scheme against noise attack [45–48] by considering additive noise (Gaussian, salt and pepper) and multiplicative noise (speckle) in the encrypted images. The multiplicative noise interferes with the encrypted images according to the following relation [48]:

$$e' = e\,(1 + kG)\,, \tag{14}$$

where e and e' are, respectively, the encrypted and the noise-affected encrypted amplitude images, k is a coefficient which represents the noise strength, and G is a Gaussian random noise with zero-mean and unit standard deviation.

The input image of Lena (Figure 11(a)) is compared with the recovered images (Figures 11(b)–11(d)) when the encrypted image is affected by noise of the type salt and pepper (density = 0.05), additive Gaussian (variance = 0.05), and speckle (variance = 0.05), respectively. The corresponding images for the binary input are shown in Figures 11(e)–11(h). From the recovered images, we observe that the scheme is robust to noise attack, with maximum resistance to speckle noise. The drop in quality of the recovered images is comparable in the cases of additive noise. Figures 12(a)-12(b) show the plots of MSE curves against density/variance for grayscale and binary images, respectively. We see that there is a monotonic increase in MSE curves of both grayscale and

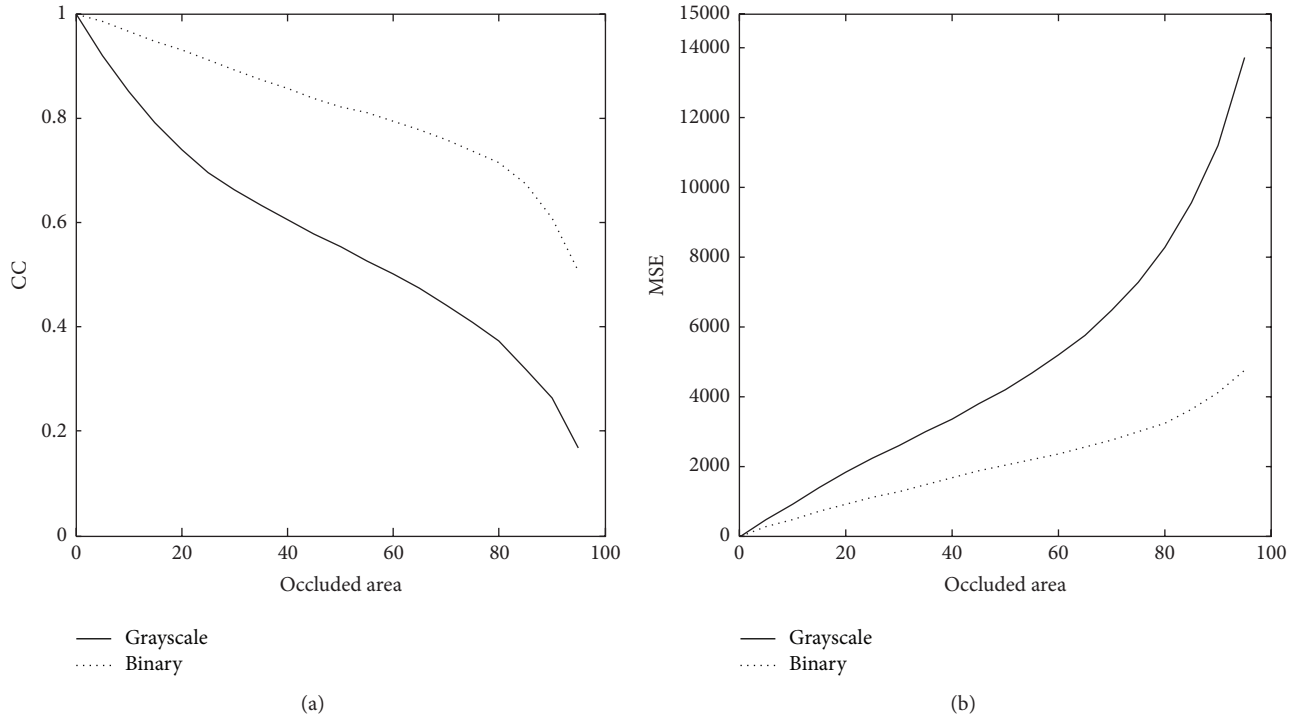


Figure 10: Plots of (a) correlation coefficient and (b) MSE for grayscale and binary images with varying occluded area.

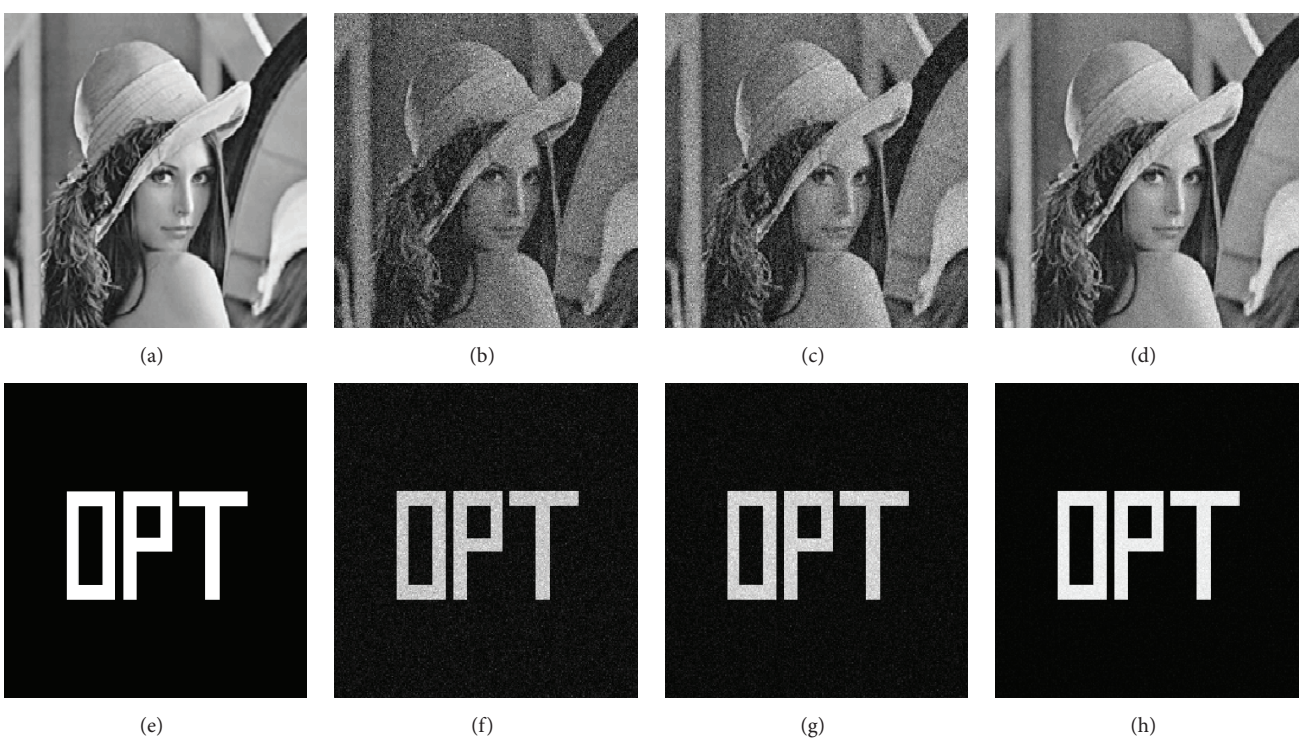


Figure 11: (a) Input image Lena; (b–d) recovered grayscale images corresponding to salt and pepper noise (density = 0.05), Gaussian noise (variance = 0.05), and speckle noise (variance = 0.05), respectively; (e) input binary image OPT; (f–h) recovered binary images corresponding to salt and pepper noise, Gaussian noise, and speckle noise, respectively.

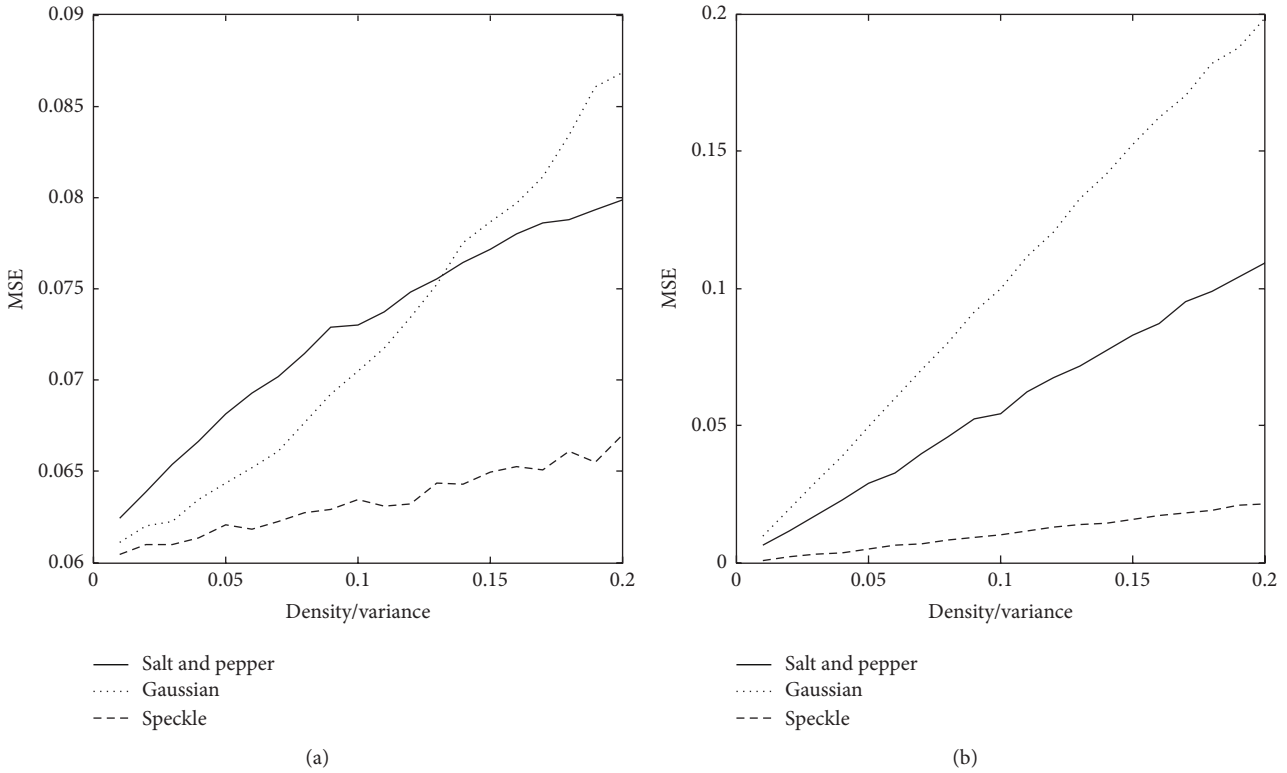


Figure 12: MSE plots for three types of noise against density/variance for (a) grayscale image Lena and (b) binary image OPT.

binary images, with the increase in density/variance. Unlike grayscale (Figure 12(a)), there is a distinct trend of MSE curves of binary image (Figure 12(b)) for the three types of noise. This establishes robustness of the proposed algorithm against commonly reported noise attacks.

4. Conclusions

A scheme for binary and grayscale images has been proposed, using RPM in the input plane and a DVTL phase mask in the frequency plane. The DVTL phase mask is preferred to introduce additional encryption parameters that enlarge the key space. This approach not only overcomes the problem of axis alignment of optical setup but also makes the proposed scheme more secure. The proposed scheme has been validated in the FrT domain. The entropy values and histograms show the validity of proposed scheme. Numerical results are presented to demonstrate the feasibility and security of the proposed system. The efficacy of the proposed scheme is seen from the computed values of MSE. The sensitivity of the scheme has also been studied for various parameters of FrT and DVTL. In addition, the results also demonstrate excellent robustness against noise and occlusion attacks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors wish to thank the management of THE NORTHCAP UNIVERSITY for their encouragement.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[2] B. Javidi, *Optical and Digital Techniques for Information Security*, Springer, New York, NY, USA, 2005.

[3] K. Singh, G. Unnikrishnan, and N. K. Nishchal, "Photorefractive optical processing for data security," in *Photorefractive Fiber and Crystal Devices: Materials, Optical Properties, and Applications VIII*, vol. 4803 of *Proceedings of SPIE*, pp. 205–219, Seattle, Wash, USA, July 2002.

[4] O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," *Proceedings of the IEEE*, vol. 97, no. 6, pp. 1128–1148, 2009.

[5] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Advances in Optics and Photonics*, vol. 1, no. 3, pp. 589–636, 2009.

[6] A. Kumar, M. Singh, and K. Singh, "Speckle coding for optical and digital data security applications," in *Advances in Speckle Metrology and Related Technique*, G. H. Kaufmann, Ed., chapter 6, pp. 239–299, Wiley-VCH, 2011.

[7] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Optics & Laser Technology*, vol. 57, pp. 327–342, 2014.

[8] W. Chen, B. Javidi, and X.-D. Chen, "Advances in optical security systems," *Advances in Optics and Photonics*, vol. 6, no. 2, pp. 120–155, 2014.

[9] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, pp. 887–889, 2000.

[10] B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," *Optik*, vol. 114, no. 6, pp. 251–265, 2003.

[11] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Optics Letters*, vol. 24, no. 11, pp. 762–764, 1999.

[12] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, vol. 29, no. 14, pp. 1584–1586, 2004.

[13] B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," *Optical Engineering*, vol. 43, no. 10, pp. 2239–2249, 2004.

[14] C.-H. Niu, Y. Zhang, and B.-Y. Gu, "Optical encryption and verification technique for information coding in multiple-wavelengths in Fresnel domain," *Optik*, vol. 117, no. 11, pp. 516–524, 2006.

[15] H. T. Chang, H.-E. Hwang, C.-L. Lee, and M.-T. Lee, "Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain," *Applied Optics*, vol. 50, no. 5, pp. 710–716, 2011.

[16] J.-J. Huang, H.-E. Hwang, C.-Y. Chen, and C.-M. Chen, "Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain," *Optics & Laser Technology*, vol. 44, no. 7, pp. 2238–2244, 2012.

[17] S. Yuan, Y.-H. Xin, M.-T. Liu, S.-X. Yao, and X.-J. Sun, "An improved method to enhance the security of double random-phase encoding in the Fresnel domain," *Optics & Laser Technology*, vol. 44, no. 1, pp. 51–56, 2012.

[18] Q. Wang, Q. Guo, L. Lei, and J. Zhou, "Multiple-image encryption based on interference principle and phase-only mask multiplexing in Fresnel transform domain," *Applied Optics*, vol. 52, no. 28, pp. 6849–6857, 2013.

[19] S. K. Rajput and N. K. Nishchal, "Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain," *Applied Optics*, vol. 52, no. 18, pp. 4343–4352, 2013.

[20] S. K. Rajput and N. K. Nishchal, "Fresnel domain nonlinear optical image encryption scheme based on Gerchberg-Saxton phase-retrieval algorithm," *Applied Optics*, vol. 53, no. 3, pp. 418–425, 2014.

[21] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Nonlinear optical security system based on a joint transform correlator in the Fresnel domain," *Applied Optics*, vol. 53, no. 8, pp. 1674–1682, 2014.

[22] Z. Liu, C. Guo, J. Tan et al., "Securing color image by using phase-only encoding in Fresnel domains," *Optics and Lasers in Engineering*, vol. 68, pp. 87–92, 2015.

[23] 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," *Optics Communications*, vol. 344, pp. 147–155, 2015.

[24] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Gyrator transform: properties and applications," *Optics Express*, vol. 15, no. 5, pp. 2190–2203, 2007.

[25] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Fully phase image encryption using double random-structured phase masks in gyrator domain," *Applied Optics*, vol. 53, no. 28, pp. 6472–6481, 2014.

[26] N.-R. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Optics Communications*, vol. 284, no. 13, pp. 3234–3242, 2011.

[27] S. Vashisth, H. Singh, A. K. Yadav, and K. Singh, "Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform," *International Journal of Optics*, vol. 2014, Article ID 728056, 9 pages, 2014.

[28] J. F. Barrera, R. Henao, and R. Torroba, "Optical encryption method using toroidal zone plates," *Optics Communications*, vol. 248, no. 1–3, pp. 35–40, 2005.

[29] J. F. Barrera, R. Henao, and R. Torroba, "Fault tolerances using toroidal zone plate encryption," *Optics Communications*, vol. 256, no. 4-6, pp. 489–494, 2005.

[30] S. K. Rajput and N. K. Nishchal, "Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask," *Applied Optics*, vol. 51, no. 22, pp. 5377–5386, 2012.

[31] M. R. Abuturab, "Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain," *Optics & Laser Technology*, vol. 45, no. 1, pp. 525–532, 2013.

[32] J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill, New York, NY, USA, 2nd edition, 1996.

[33] D. G. Voelz, *Computational Fourier Optics: A MATLAB Tutorial*, SPIE Press, Bellingham, Wash, USA, 2011.

[34] D. R. Chalice, "A characterization of the Cantor function," *The American Mathematical Monthly*, vol. 98, no. 3, pp. 255–258, 1991.

[35] W. D. Furlan, F. Giménez, A. Calatayud, and J. A. Monsoriu, "Devil's vortex-lenses," *Optics Express*, vol. 17, no. 24, pp. 21891–21896, 2009.

[36] A. Calatayud, J. A. Monsoriu, O. Mendoza-Yero, and W. D. Furlan, "Polyadic devil's lenses," *Journal of the Optical Society of America A*, vol. 26, no. 12, pp. 2532–2537, 2009.

[37] M. Mitry, D. C. Doughty, J. L. Chaloupka, and M. E. Anderson, "Experimental realization of the devil's vortex Fresnel lens with a programmable spatial light modulator," *Applied Optics*, vol. 51, no. 18, pp. 4103–4108, 2012.

[38] A. Calabuig, S. Sánchez-Ruiz, L. Martínez-León et al., "Generation of programmable 3D optical vortex structures through devil's vortex-lens arrays," *Applied Optics*, vol. 52, no. 23, pp. 5822–5829, 2013.

[39] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane," *Optics and Lasers in Engineering*, vol. 67, pp. 145–156, 2015.

[40] A. K. Yadav, S. Vashisth, H. Singh, and K. Singh, "A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask," *Optics Communications*, vol. 344, pp. 172–180, 2015.

[41] J. A. Davis, D. E. McNamara, D. M. Cottrell, and J. Campos, "Image processing with the radial Hilbert transform: theory and experiments," *Optics Letters*, vol. 25, no. 2, pp. 99–101, 2000.

[42] M. Joshi, C. Shakher, and K. Singh, "Image encryption and decryption using fractional Fourier transform and radial Hilbert transform," *Optics and Lasers in Engineering*, vol. 46, no. 7, pp. 522–526, 2008.

[43] X. Tong, Y. Liu, M. Zhang, H. Xu, and Z. Wang, "An image encryption scheme based on hyperchaotic Rabinovich and exponential chaos maps," *Entropy*, vol. 17, no. 1, pp. 181–196, 2015.

[44] Y. Liang, G. Liu, N.-R. Zhou, and J. Wu, "Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion," *Journal of Modern Optics*, vol. 62, no. 4, pp. 251–264, 2014.

[45] X.-F. Meng, L.-Z. Cai, X.-L. Yang et al., "Digital color image watermarking based on phase-shifting interferometry and neighboring pixel value subtraction algorithm in the discrete-cosine-transform domain," *Applied Optics*, vol. 46, no. 21, pp. 4694–4701, 2007.

[46] M. Joshi, C. Shakher, and K. Singh, "Image encryption using radial Hilbert transform filter bank as an additional key in the modified double random fractional Fourier encoding architecture," *Optics and Lasers in Engineering*, vol. 48, no. 5, pp. 605–615, 2010.

[47] M. Joshi, C. Shakher, and K. Singh, "Fractional Fourier plane image encryption technique using radial Hilbert-, and Jigsaw transform," *Optics and Lasers in Engineering*, vol. 48, no. 7-8, pp. 754–759, 2010.

[48] L. Sui, M. Xin, A. Tian, and H. Jin, "Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain," *Optics and Lasers in Engineering*, vol. 51, no. 12, pp. 1297–1309, 2013.