Asymmetric Image Cryptosystem Based on Chaotic Zone Plate Phase Mask and Arnold Transform

Mehak Khurana and Hukum Singh

Abstract An optical asymmetric cryptosystem built on chaotic zone plate phase mask (CZPPM) has been proposed. Here the pixels of an image are shuffled by employing Arnold transform (AT^{ω}) and is then modulated with the CZPPM featuring in the gyrator Transform domain (GT). This increases randomness and adds chaotic parameters that make the system highly secure. The proposed system strengthens the security of the cryptosystem and does not permit the attacker to retrieve the initial image without the expertise of keys. The robustness of the projected cryptosystem has been investigated and validated based on an extra degree of freedom by simulating on MATLAB 9.9.0 (R2020b), and investigational outcomes have been shown to emphasize the efficacy of the algorithm.

Keywords Fresnel zone plate · Chaotic phase mask · Arnold transform · Gyrator transform

1 Introduction

With substantial innovations in transmission and information processing technologies, it has become a challenge to convey the information with security. An optical 4*f* system of DRPE in Fourier domain proposed by Refregier and Javidi was a great accomplishment in this arena in 1995 [1]. This set off the path for many researchers for constructing other cryptosystem centered on DRPE with superior security and elevated noise diminution. These systems were still exposed to many attacks known as known plaintext attack (KPA) [2, 3], chosen plaintext or ciphertext attack (CPA, CCA), etc. [4] An idea has been taken in the direction to

M. Khurana (✉)
Department of Computer Science, The NorthCap University, Gurugram, India
e-mail: mehakkhurana@ncuindia.edu

H. Singh
Department of Applied Sciences, The NorthCap University, Gurugram, India
e-mail: hukumsingh@ncuindia.edu

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_5

model an asymmetric system [5] that deliver solution to insecure transmission concern and make it resilient from numerous attacks by boosting the randomness and improving chaotic mask key parameters.

2 Key Generation: Chaotic Zone Plate Phase Mask

Chaotic random phase masks (CRPM) [6] are used to increase randomness and to add chaotic parameters which makes the system highly secure in terms of private keys. Logistic map is one dimension (1D) non-linear chaotic maps and is used to generate the randomness in the CRPM. It can be expressed [7, 8].

$$x_{n+1} = px_n(1 - x_n) \tag{1}$$

It is iterated n times. Where p is bifurcation parameter and lies between $0 < p < 4$, x_0 is an initial value and $x_n \in [0, 1]$ is an iterative value where n varies from 0 to $M \times N$. M and N are size of a chaotic random mask in pixels. The 1D sequence $X = x_1, x_2, x_3, x_4, \ldots, x_{M \times N}$ that is produced by Eq. (1) is rearranged into 2D matrix as $Y = y_{ij}$, where i varies from $\{1, 2, \ldots, M\}$ and j varies from $\{1, 2, \ldots, N\}$ and $y_{ij} \in (0, 1)$. CRPM a 2D matrix is expressed as

$$\mathrm{CRPM}(x, y) = \exp\big(i2\pi y_{ij}(x, y)\big) \tag{2}$$

The Fresnel lens is built on quadratic phase change and the efficacy of zone plates. It is given [3] by

$$L_{\lambda,f}(r) = \exp(-i\pi r^2/\lambda f) \tag{3}$$

where r is the lens radius, f is the focal length, and λ is the wavelength of incident light. Now, CZPPM(x, y) is obtained by multiplying above two functions $L_{\lambda,f}(r)$ and CRPM(x, y), i.e., Equation (1) and (2) and can be stated as

$$C(x, y) = \exp\left\{ i\pi \left[2y_{ij}(x, y) + \frac{r^2}{\lambda f} \right] \right\} \tag{4}$$

3 Proposed Cryptosystem

Asymmetric encryption technique built on CZPPM and AT$^{\omega}$ [9, 10] is proposed in this paper. The AT$^{\omega}$ scrambles the image $I(x, y)$ of size $M \times M$ by shuffling the pixels arbitrarily as in Eq. (5). Then the obtained result is transformed in gyrator domain [10], and phase is truncated to produce $G(u, v)$ as in Eq. (6). The encrypted image is generated by multiplying $G(u, v)$ with arbitrary phase mask in gyrator domain and further truncating its phase as in Eq. (7). The CZPPM and AT^{ω} applied through encryption operates as supplementary key because it comprises number of parameters as well as expands the randomness which further enhances the security.

$$I(x', \ y') = \mathrm{AT}^{\omega}(I(x, y)) \times C_1(x, y) \tag{5}$$

$$G(u, v) = \mathrm{PT}[\mathrm{GT}^{\alpha}(I(x', \ y'))] \tag{6}$$

$$E(x, y) = \mathrm{PT}\left[\mathrm{GT}^{-\beta}[G(u, v) \times C_2(x, y)]\right] \tag{7}$$

Two decryption keys DK_1 and DK_2 were generated in the process where amplitude truncation is performed as shown in Eqs. (8) and (9)

$$\mathrm{DK}_1 = \mathrm{AT}[\mathrm{GT}^{\alpha}(I(x', \ y'))] \tag{8}$$

$$\mathrm{DK}_2 = \mathrm{AT}\left[\mathrm{GT}^{-\beta}[G(u, v) \times C_2(x, y)]\right] \tag{9}$$

The current graph of the planned encryption stated is displayed in Fig. 1.

The decipherment procedure is the reversal process of the encryption which retrieves the original image $I(x, y)$. Following are the equations to decipher the encoded image $E(x, y)$.

$$G(u, v) = \left[\mathrm{IGT}^{-\beta}[E(x, y) \times \mathrm{DK}_2\ ] \times C_2^*(x, y)\right] \tag{10}$$

$$I(x', \ y') = \mathrm{IGT}^{\alpha}[G(u, v) \times \mathrm{DK}_1] \times C_1^*(x, y) \tag{11}$$

$$I(x.y) = \ \mathrm{AT}^{\omega}(\ I(x', \ y')) \tag{12}$$

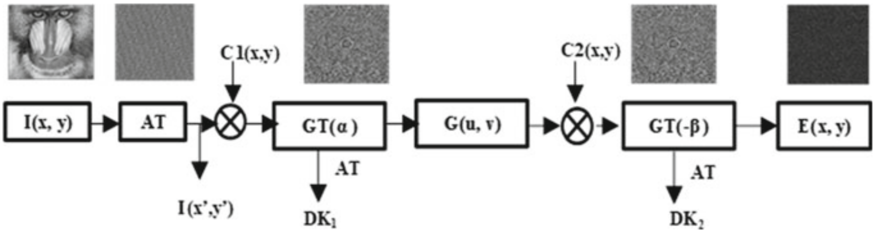

Fig. 1 Flow graph for proposed encryption scheme

4 Simulations Results

This paper demonstrates the statistical analysis and simulation results verifies the sensitivity of the indicated procedure and reveals that it accomplishes superior performance of recuperating a good superiority image. Findings also confirms the protection assessment based on correlation coefficient, noise attack, and key sensitivity. Contemplate initial image of baboon with size 256 × 256.

For simulation values use are $p = 3.96$, $x_0 = 0.35$, $\lambda = 6328$ Å, $f = 200$ mm, $\omega = 5$ and orders of GT are $\alpha = 0.4\pi$ and $\beta = 0.7\pi$. Figure 2 shows the CZPPM key generated from CRPM and Fresnel zone plate (FZP).

4.1 *Statistical Analysis*

For statistical analysis, entropy [11] of the image has been analyzed, and the obtained value for baboon image is 6.319 which is close to standard value that guarantees failure of information is nearby zero. The information is homogenously scattered, and it does not deliver any valuable information to the attacker. It can be confirmed from the value obtained above that the projected system is extremely efficient.

Peak signal to noise ratio (PSNR) [12] achieved 23 dB after first level of phase retrieval and 28 dB attained after the second level of phase retrieval.

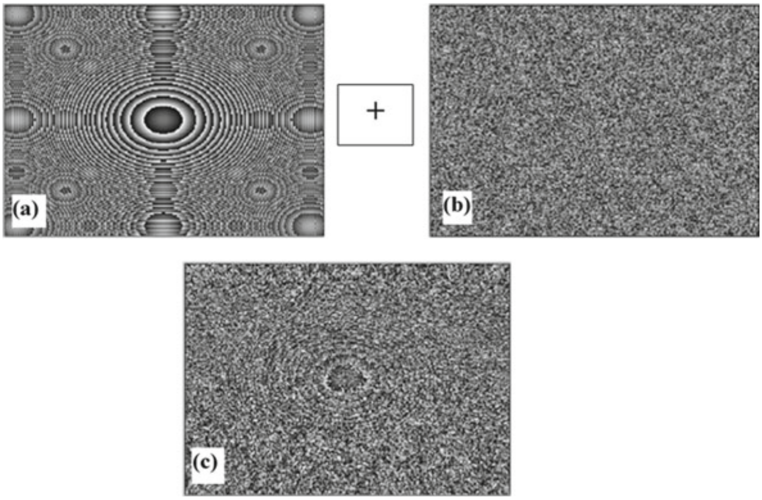

Fig. 2 **a** Fresnel zone plate, **b** chaotic random phase masks, **c** chaotic zone plate phase mask

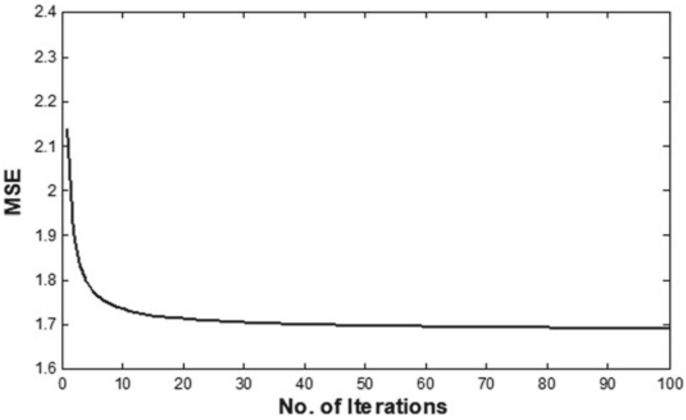

Fig. 3 MSE versus number of iteration graph

4.2 Performance Analysis

The mean square error (MSE) [13] determined for baboon image is 5.6346×10^{-22}. Figure 3 presents the number of iterations versus MSE. Here, MSE drops with the increase in number of iterations and after 50 iterations, MSE becomes constant therefore image randomization stabilizes.

4.3 Robustness Analysis

The proposed algorithm is verified against occlusion attack [14, 15] where the encrypted image has been occluded for different sizes, but the images are still visible from human eye till 75% which proves the system is robust. 45% and 70% occluded encrypted images and its retrieved images are presented in Fig. 4.

4.4 Robustness Analysis

This system has been investigated against KPA, CPA, and special attack to verify its strength. Sets of initial and cipher images have been picked to uncover the authentic key, the erroneous value of parameter headed to incorrect generation of key. To verify the conjunction of the iteration procedure, MSE versus iterations are employed to recover the decryption keys. It can be viewed from MSE plot that decipherment key cannot be recovered even with large iteration number as shown in Fig. 5.

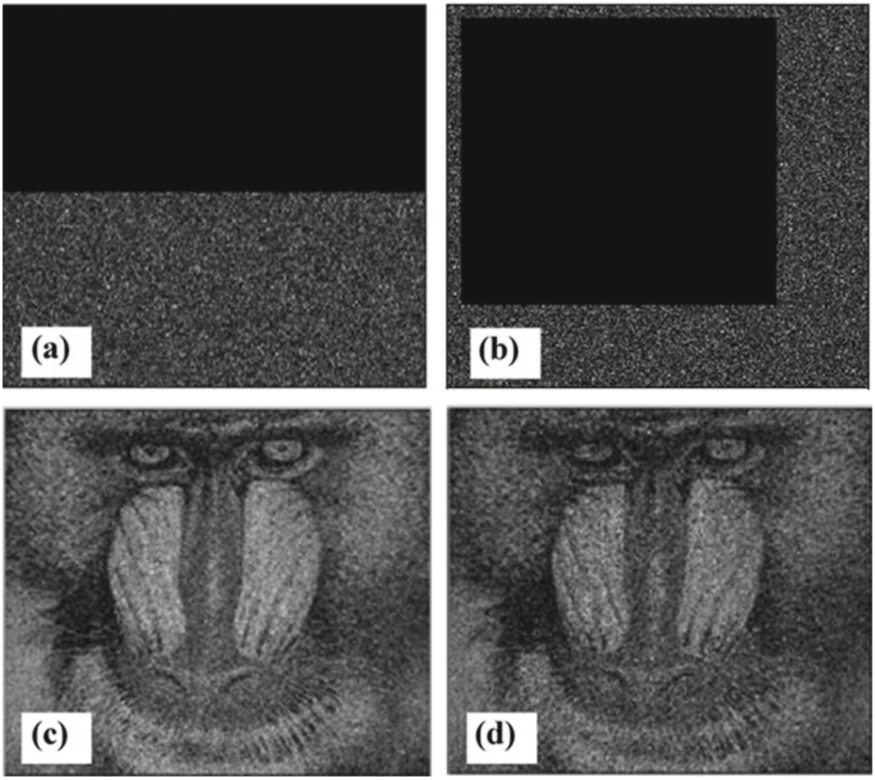

Fig. 4 **a** 45% occluded encoded image, **b** 70% occluded encoded image, **c** recovered image after 45% of occlusion, **d** recovered image after 70% of occlusion

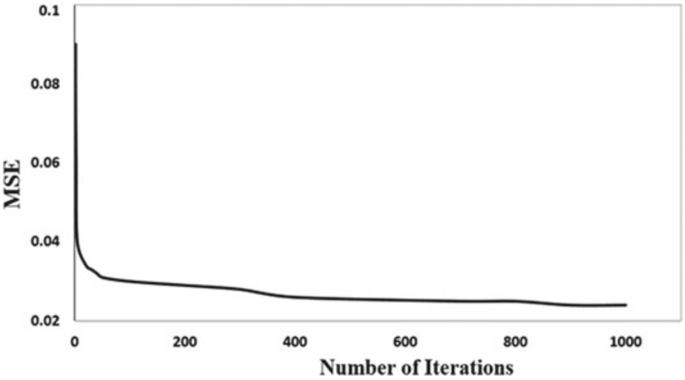

Fig. 5 MSE plot versus number of iterations for decipherment key generation with proposed scheme for 1000 iterations

5 Conclusion

The proposed asymmetric cryptosystem improves the security of the scheme as chaotic mask shifts the phase of the retrieved output and scrambling creates dispersion in the system. The introduced masking accomplishes superior execution of PSNR, MSE, occlusion, and noise as equated to existing systems. The CZPPM is further protected and cannot recapture initial image without the knowledge of all the parameters utilized for producing key. Experimental result reveals the viability and robustness of asymmetric cryptosystem.

References

1. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20**(7), 767–769 (1995)
2. Peng, X., Zhang, P., Wei, H., Yu, B.: Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. **31**(8), 1044–1046 (2006)
3. Gopinathan, U., Monaghan, D.S., Naughton, T.J., Sheridan, J.T.: A known-plaintext heuristic attack on the Fourier plane encryption algorithm. Opt. Express **14**(8), 3181–3186 (2006)
4. Zhang, C., Liao, M., He, W., Peng, X.: Ciphertext-only attack on a joint transform correlator encryption system. Opt. Express **21**(23), 28523–28530 (2013)
5. Qin, W., Peng, X.: Asymmetric cryptosystem based on phase-truncated Fourier transforms. Opt. Lett. **35**(2), 118–120 (2010)
6. Abuturab, M.R.: Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition. Opt. Laser Tech. **98**, 298–308 (2018)
7. Barrera, J.F., Henao, R., Torroba, R.: Optics encryption method using toroidal zone plates. Opt. Commun. **248**, 35–40 (2005)
8. Liansheng, S., Bei, Z., Xiaojuan, N., Ailing, T.: Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. Opt. Express **24**(1), 499–515 (2016)
9. Chen, L., Zhao, D., Ge, F.: Image encryption based on singular value decomposition and Arnold transform in fractional domain. Opt. Commun. **291**, 98–103 (2013)
10. Liu, Z., Chen, H., Liu, T., Li, P., Xu, L., Dai, J., Liu, S.: Image encryption by using gyrator transform and Arnold transform. J. Electron. Imaging. Proc. SPIE. **20**(1), 013020 (2011)
11. Khurana, M., Singh, H.: A spiral-phase rear mounted triple masking for securing optical image encryption based on gyrator transform. Recent Patents Comput. Sci. **12**(2), 80–94 (2019)
12. Khurana, M., Singh, H.: Two-level phase retrieval in fractional Hartley domain for secure image encryption and authentication using digital signatures. Multimedia Tools Appl. **79**, 13967–13986 (2020)
13. Wang, S., Meng, X., Yin, Y., Wang, Y., Yang, X., Zhang, X., Peng, X., He, W., Dong, G., Chen, H.: Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform. Opt. Lasers Eng. **114**, 76–82 (2019)
14. Liansheng, S., Xiao, Z., Chongtian, H., Ailing, T., Krishna Asundi, A.: Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. Opt. Lasers Eng. **113**, 29–37 (2019)
15. Singh, H., Khurana, M.: An asymmetric optical cryptosystem of double image encryption based on optical vortex phase mask using Gyrator transform domain. Recent Patents Comput. Sci. **13**(3), 672–685 (2020)