International Journal for Modern Trends in Science and Technology, 8(S05):01-05, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IIJMTST08S0501
Available online at: https://www.ijmtst.com/vol8si05.html

A Novel Cryptography System using Double Random Phase Encoding with Circular Harmonic Key

Dr.A.V.Bharadwaja | D.Gangadhar| D.Rama Koteswara Rao| G.Bala Chandrudu|G.Balavardhan

Department of Electronics and Communication Engineering, Godavari Institute of Engineering and Technology(A), JNTUK, Kakinada.

To Cite this Article
Dr.A.V.Bharadwaja, D.Gangadhar, D.Rama Koteswara Rao, G.Bala Chandrudu and G.Balavardhan. A Novel Cryptography System using Double Random Phase Encoding with Circular Harmonic Key. International Journal for Modern Trends in Science and Technology 2022, 8(S05), pp. 01-05. https://doi.org/10.46501/IJMTST08S0501

Article Info
Received: 26 April 2022; Accepted: 24 May 2022; Published: 30 May 2022.

ABSTRACT

We demonstrated a cryptosystem technique based on variation of rotation key using circular harmonic key with the help of double random phase masks in Fourier transform approach. It is observed that the encryption key generated in rectangular coordinates bear a tolerance of 0.2 degrees rotation of key in the decryption process. This leads to low efficiency security of whole system and less effective to brute force attacks and forgeries. A novel cryptosystem based on circular harmonics is introduced in Fourier domain, where the key is generated in polar coordinates, which gives the high tolerance with rotation of angle key. This resolves the security and efficiency of the cryptosystem. The numerical experiments are presented to demonstrate the efficient of the system and to show the proof of the concept.

KEYWORDS:Circular harmonic key, random phase masks, cryptosystem, Fourier transform, encryption and decryption,

1.INTRODUCTION

Through the mid1970's, cryptology was overwhelmed by state run administrations both on the grounds that PCs were extravagant and in light of the requirement for data retention.Several factors pushed encryption towards the standard. The most significant of these was the creation of the World Wide Web in 1989 and the inescapable utilization of PCs. Both modern business and individual correspondence must be secured.Cryptography is the investigation of secure interchanges strategies that permit just the cipher and expected beneficiary of a message to see its items. Data confidentiality, Integrity, Authentication, Non-repudiation are the center standards of advanced cryptography.we executed thiskind of encryption course of action involving the encryption-keys inrectangular Coordinates K(u,v), Thenwe saw that theunscrambling is a variation activity with the rotation of the key.Practically speaking, this difference is an issue that should be settled. We have proposed a solution for the issue utilizing a decay ofthe key in circular harmonics

2. METHODOLOGY

2.1.Encryption using Double random phase encoding

Cryptosystem techniques are widely used in image security applications since this type of techniques can deal with a large amount of data rapidly with image processing algorithms. In the recent literature, theDouble Random Phase Encoding (DRPE) has been widely attracted in many image encryption applications. The DRPE uses the principle of Fourier Transform (FT) that enables the spatial and spectral information to be encrypted.In the present paper, the input 2D image encryption is implemented by using random-phase masks encoding (RPM) for both the input and the Fourier planes. Therefore, the whole image information encryption process transforms the input image into white noise. Similarly, the decryption process is carried out using its inverse process of encryption procedure. The original image is obtained only when the key and its spatial data are perfectly matched. The schematic illustration of proposed encryption and decryption system for image cryptosystem is shown in Fig.1.

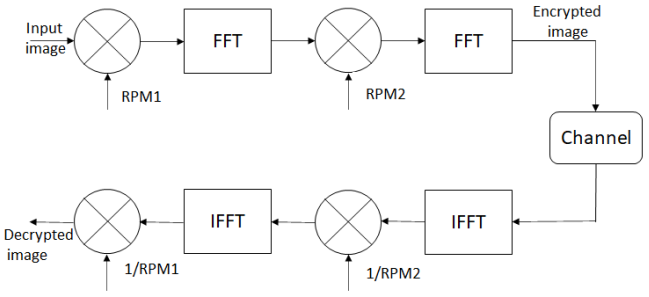


Fig.1: Schematic diagram of proposed cryptosystem using double random phase encoding scheme

$$G = FFT\{RPM_2 . FFT\{I . RPM_1\}\}(1)$$

Now, decryption process can be expressed as given below

$$I = IFFT\{IFFT\{G\} . RPM_2\} . RPM_1(2)$$

Where I denotes the input image, RPM_1 and RPM_2 indicates the random phase mask, G denotes the encrypted image after RPM_2, FFT and IFFT indicates the Fourier transforms and inverse Fourier transforms. In this section, the DRPE is described in rectangular coordinates and this can lead to unauthorised access even with small variation in the decryption keys. To avoid such scenarios, we propose an encryption and decryption system using circular harmonic key in the Fourier domain using transformed polar coordinates with the help of DRPE. Generally, therandom phase masks are considered to be the secret keys in encryption where the key acquires more size .so it will be hard to rebuild the original image using these keys in the process of proposed scheme.

2.2. Proposed Encryption using Circular Harmonic key in DRPE

In the proposed method, the circular harmonic key is utilized in the random phase mask in the (DRPE) algorithm to enhance the security of the cryptosystem. In this phenomenon, an image in rectangular coordinates is converted to polar coordinates for circular harmonic key generation with rotation of angle along with radius [7,8]. The circular harmonic key (CHK) is in the form of polar coordinates. The CHK is distribution in the Fourier domain can mathematical expressed as below,

$$RPM(\rho, \varphi) = exp[i\emptyset(\rho, \varphi)](3)$$

where $\emptyset$ contains the randomness values. The key mentioned in equation (3)is decomposed into circular harmonic with the polar coordinates position (ρ, φ) as the centre and it can be written as

$$\emptyset(\rho\, cos\varphi, \rho\, sin\varphi) = \emptyset(\rho, \varphi) = \sum_{n=-\infty}^{\infty} \emptyset_m(\rho) \exp[in\varphi] \quad (4)$$

where n indicates the order of circular harmonics and $\emptyset_n(\rho)$is obtained as shown in equation (5).

$$\emptyset_n(\rho) = \frac{1}{2\pi} \int_0^{2\pi} \emptyset(\rho, \varphi) \exp[in\varphi]\, d\varphi\, (5)$$

Now the first RPM using a CHK key in the Fourier domain is written as

$$RPM_1 = K(\rho_1, \varphi_1) = exp[i\Re\{\Phi_m(\rho_1, \varphi_1)\}] \quad (6)$$

where $\Re\{i\}$define the real part of CHK, $\emptyset_n$ contains the distribution of random values in polar coordinates. Similarly, the second RPM_2can be written as

$$RPM_2 = V(\rho_2, \varphi_2) = exp[i\Re\{\Phi_m(\rho_2, \varphi_2)\}](7)$$

The proposed encryption and decryption process is illustrated in Figure 2. Let I be input image to be encrypted in proposed system. Firstly, the image is

encrypted by multiplying RPM1 with CHK $K(\rho_1, \varphi_1)$. After that the encrypted information is transformed to Fourier domain using FFT. Later RPM2 with CHK $V(\rho_2, \varphi_2)$ is multiplied with first encrypted information and the transformed into Fourier domain using another FFT. Mathematically model for the DRPE process with CHKs are shown in Equations (8-9)

$$G = FFT\{V(\rho_2, \varphi_2).FFT\{I.K(\rho_1, \varphi_1)\}\} \quad (8)$$

In the decryption process, the original image is retrieved using correct keys by performing the inverse process of the encryption procedure. Now, decryption process can be expressed as given below

$$I = IFFT\{IFFT\{G\}.V^*(\rho_2, \varphi_2)\}.K^*(\rho_1, \varphi_1) \quad (9)$$

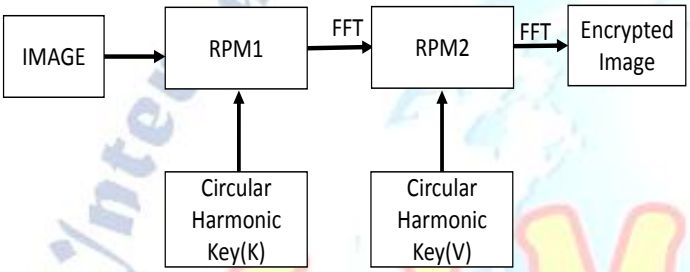


Fig.2(a): Schematic diagram of the proposed encryption system using DRPE with circular harmonic key in Fourier domain

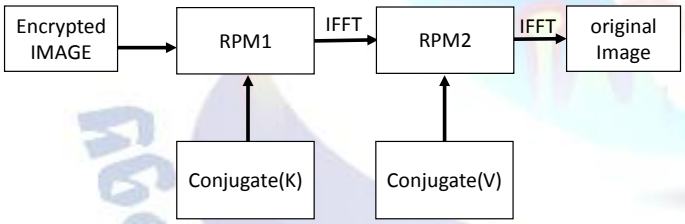


Fig.2(b): Schematic diagram of the proposed decryption system using DRPE with circular harmonic key in Fourier domain

In the proposed method, the circular harmonic key is utilized in the random phase mask in the DRPE algorithm to enhance the security of the cryptosystem. The system has three keys i.e. angle of circular harmonic key (m1,m2), radius of CHK (r1,r2), transform key (d1,d2) along with FFT. To verify and test the cryptosystem, we have carried out the numerical simulations to show the proof of the concept of the proposed encryption and decryption system.

3. COMPUTATIONAL EXPERIMENTS, RESULTS AND DISCUSSION

To validate the proposed encryption and decryption scheme, numerical experiments are performed. Let's us consider a 2-D image called as phantom of size 256×256is used in the simulation process. The parameters used in the simulations are,CHK key $n = 2$, the rotation angle of the two CHKkeys are $\varphi_1 = 3°$, $\varphi_2 = 6°$ and the radius $\rho_1 = 40mm$, $\rho_2 = 40mm$. Figure 3 show the input image considered for the simulation experiments.

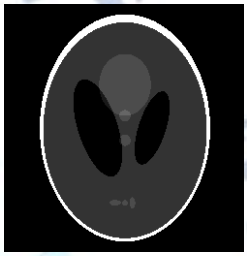


Fig.3 input phantom image used for the encryption

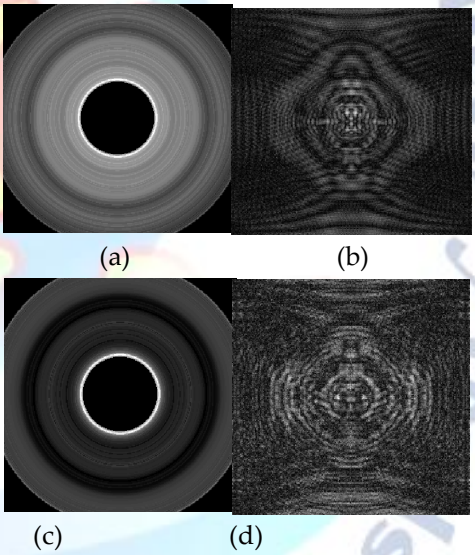
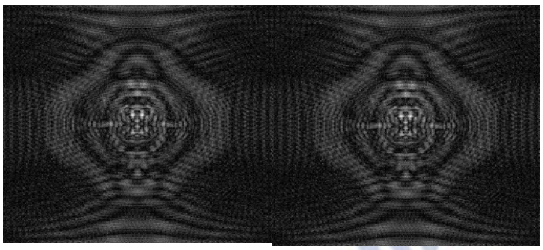


Fig.4 Encryption process

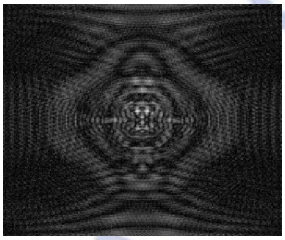
From fig.4, (a) image when RPM1= $K(\rho_1, \varphi_1)$, (b) encrypted information after RPM1 and FFT,(c)image when RPM2=$V(\rho_2, \varphi_2)$ (d) encrypted information after RPM2 and second FFT.

The above figure represents Encryption decryption results of the applied input image, figure4(a) represents output image derived from random phase mask-1 multiplied with Circular harmonic key-1 the figure-4(b) represents that the input image is given to Random phase mask-1 which is multiplied with circular Harmonic Key-1 of order=1 and the figure 4(c) represents the output of previous image is given to Random Phase Mask-2

which is Multiplied with the Circular Harmonic Key-2 which results in a highly Encrypted image as shown figure-4(d) so when the receiver enters the accurate key the original image will be restored



(a) (b)



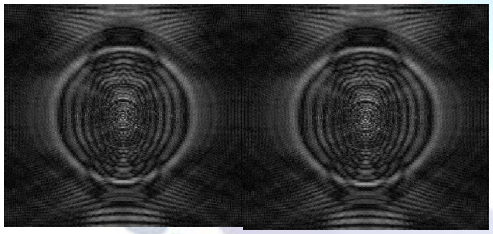
(c)

Fig.5 Decryption process

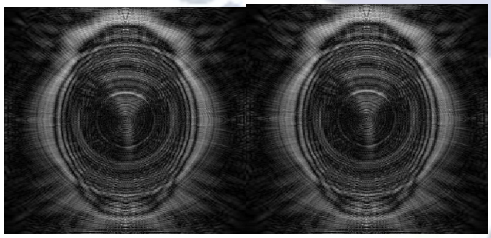
From fig.5 (a) Decrypted information after IFFT and $V^*(\rho_2, \varphi_2)$

(b) Decrypted informationafter IFFT and $K^*(\rho_1, \varphi_1)$

(c)Decrypted original phantom image using correct keys.



(a) (b)



(c) (d)

Fig.6 Decryption process using incorrect keys

From fig.6, (a) Decrypted image using incorrect RPM_2 and $V^*(\rho_2, \varphi_2)$ (b) Decrypted image using incorrect RPM_1 and $K^*(\rho_1, \varphi_1)$ (c) Decrypted image using incorrect K_2 key (d)Decrypted using incorrect K_1 key.

When any one of the encrypted keys is wrongly given then the decrypted image looks like noisy image as shown in Fig.6. Fig.(a) shows the decrypted and reconstructed image when wrong RPM2 and V* key is used for the decryption process. It is clear that the original image is obtained only when the encryption key and decrypted key are exactly matched with each other and in case of mismatch leads to noisy output as shown in fig.6(d).

4. CONCLUSION

The variance rotation of key is achieved through this encryption technique using circular harmonics and Double Random phase encoder so in this way the proposed method provides high resistance to the encrypted information from Third party access and cipher attacks in the channel as the image is highly encrypted by the duality of Random phase encoder as it will convert rectangular co-ordinates into polar co-ordinates so any third party access try to access the information using wrong the keys the information will not be as like of original image and also allow recipient to decrypt the information without any difficulty

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Fan, H., and Li, M. (2019). Cryptanalysis and Improvement of ChaosBased Image Encryption Scheme with Circular Inter-Intra-Pixels BitLevel Permutation. Mathematical Problems in Engineering, 201

[2] [2] Zhu, B., Liu, S., and Ran, Q. (2017). image encryption based on multifractional Fourier transforms. Digital letters, 25(16), 1159–1161.

[3] [3] Kong, D., Shen, X., Xu, Q., Xin, W., and Guo, H. (2013). Multiple image encryption scheme based on cascaded fractional Fourier transform. Applied Digital, 52(12), 2619–2625

[4] [4] Wu, J., Zhang, L., and Zhou, N. (2012). Image encryption based on the multiple-order discrete fractional cosine transform. Image processing, 283(9), 1720–1725.

[5] [5] Liu, Z., Guo, Q., and Liu, S. (2016). The discrete fractional random cosine and sine transforms. Digital communications, 265(1), 100–105. [27] Liu, Y., Lin, J., Fan, J., and Zhou, N. (2012). Image encryption based on cat map and fractional fourier transform. Journal of Computational Information Systems, 8(18), 7485–7492.

[6] [6] Rao, K. R., and Yip, P. (2014). Discrete cosine transformalgorithms, advantages, applications. Academic press.

[7] [7] Image Encryption Based on Double Random Phase Encoding Zhe Liu, Mee Loong Yang and Wei Qi Yan Department of Computer Science School of Engineering, Computer and Mathematical Science, Auckland university of engineering(2013)

[8] [8] Song, Z. Z. (2013) Image Encryption Algorithm Based on Chaotic Mapping and Double Random Phase Encoding Technology, Master's thesis, Harbin Institute of Technology