ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 8, pp. 18946-18950, August, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

AN OPTICAL IMAGE ENCRYPTION USING LOXODROMIC CAT MAP WITH DOUBLE RANDOM PHASE ENCODING (LCMDRPE)

Jayaseelan. L[1]* and Sureshkumar. C[2]

[1]Research Scholar, Department of Computer Science, Periyar University, Periyar Palkalai Nagar, Salem, Tamilnadu, India
[2]Principal, Dr. Nagarathinam's College of Engineering, Rasipuram, Namakkal, Tamilnadu, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0808.0598

ARTICLE INFO

Article History:

Received 15th May, 2017
Received in revised form 25th June, 2017
Accepted 23rd July, 2017
Published online 28th August, 2017

Key Words:

Optical Image Encryption, Loxodromic Cat Map (LCM), Double Random Phase Encryption (DRPE)

ABSTRACT

The double random phase encryption (DRPE) technique is a known all-optical architecture that has many advantages especially in terms of encryption efficiency. However, the technique presents some vulnerabilities against attacks and needs a large quantity of information to encode the complex output plane. Encrypt the optical image using chaotic Baker map and DRPE. This scheme is implemented in two layers to improve the security level of the classical DRPE. A pre-processing layer is a first layer of this method that is performed along with the chaotic baker map on the original image. In the second layer, the classical DRPE is utilized. However, low speed problem and number representation problems due to the utilization of floating point values over other number representations. Hence, we propose an Optical Image Encryption using Loxodromic Cat Map with Double Random Phase Encoding (LCMDRPE). Theoretical analysis and experimental results show that our proposed method is providing better results in terms of maximum deviation, correlation coefficient, peak signal-to-noise ratio and mean square error.

INTRODUCTION

Now a days, development of communication and network technologies, both the secure communication and the information security have become one of the most challenging problems. Recently, optical information security methods, particularly optical image encryption methods, have attracted significant interest as they possess superior advantages, such as arbitrary parameter selection and high-speed parallel processing of information. The various methods proposed for optical image encryption, the double random phase encoding is the most well-known method. This method uses two random phase masks respectively placed on the input plane and the Fourier plane to encrypt the input image into a stationary white noise. During the past decades, a number of DRPE-based optical encryption methods have been presented, such as the Gyrator transform encryption scheme (Singh and Sinha, 2009), the Fresnel transform encryption scheme (Situ and Zhang, 2004), and the fractional Fourier transform encryption scheme (Unnikrishnan *et al*, 2000). However, due to the inherent linear property, the DRPE-based encryption schemes have been proved to be vulnerable to different types of attacks.

An optical image encryption based on chaotic baker map and double random phase encoding (CBMDRPE) was proposed (Elshamy *et al*, 2013). In this method, implemented in two layers to improve the security level of the classical DRPE. The first layer is a pre-processing layer that is executed with the chaotic Baker map on the original image. The second layer, the classical DRPE is utilized. In chaotic baker map, low speed problem and number representation problems due to the utilization of floating point values over other number representations. Hence, we propose an optical image encryption based on Loxodromic Cat Map with Double Random Phase Encoding (LCMDRPE) which structurally invariant systems are known as Anosov maps, they are ergodic, mixing and have positive entropy. Loxodromic behaviour appears as a new alternative with respect to usual cat maps with one degree of freedom. Loxodromic behaviour has been quantized. The quantum periodicity function has been found to be insensitive to the structural stability.

The rest of the article is organized as follows: In Section 2, description of different optical encryption schemes is given. In Section 3, detailed information of the proposed Loxodromic Cat Map with Double Random Phase Encoding scheme is

Corresponding author:* **Jayaseelan, L
Research Scholar, Department of Computer Science, Periyar University, Periyar Palkalai Nagar, Salem, Tamilnadu, India

described. In Section 4, results of experimental results are presented. In Section 5, conclusion of the research work is given.

Related Work

Simple and reliable criteria to give feedback in the brute-force attack on DRPE (Nalegaev and Petrov, 2015) was proposed that allowing to perform more accurate investigations of the particularities of such numerical task. In this technique, criteria were applied, if the gray scale, binary or color images are used as a source. A criterion based on the statistical analysis of the reconstructed images was considered. Then it was used for the recovery, if the statistical distribution of the original data follows the known law. Another criterion is based on the enlarged sampling frequency of the histogram. However, the computational complexity of this method was increased. A novel optical interference-based encryption algorithm (Wang *et al*, 2015) was proposed in which the primitive image was encoded into two encoded complex field functions whose amplitude parts have rotational symmetric configuration via using circular harmonic component (CHC) expansion technique and iterative retrieval gyrator transform (GT) algorithm. However, in this scheme not used scale invariant recognition.

An innovative hybrid method to improve the performance of DRPE method in terms of compression and encryption (Neji *et al*, 2016) was proposed. In this method consists in using an innovative randomized arithmetic coder (RAC) that was well compress the DRPE output planes and simultaneously improve the encryption. Moreover, arithmetic coding was used to reduce the quantity of information of the DRPE output plane and RAC was employed to enhance the security level of the DRPE method. An Optical Image Encryption using Chaotic Kicked Rotator Map with Double Random Phase Encoding (Sivamalar and Sharma, 2016) was proposed. This method decreases the complexity in computations and increases the speed of mapping through employing bit-wise representation thus improving the encryption process. This approach was not affected via the known-plaintext attack.

A practical scheme for optically encrypting and decrypting a gray-scale image based on QR codes (Jiao *et al*, 2017) was proposed that compatible with common QR code generators and readers. In this method, optically encrypting and decrypting a gray-scale image employing QR codes. A gray-scale image was transformed to a decimal number sequence and the decimal number sequence was converted to multiple QR codes. However, many users that have mobile phones that have cameras are unable to get QR reading software for their phones. Optical image encryption using Kronecker product and hybrid phase masks (Kumar and Bhaduri, 2017) was proposed. The Kronecker product of two random matrices together with the double random phase encoding (DRPE) method in the Fresnel domain for optical image encryption. This method provides multiple levels of security for image encryption. Other security keys in this method were Fresnel propagation distances, two random matrices used for known plaintext attack (KP) and the randomization operator.

Secret shared multiple-image encryption based on row scanning compressive ghost imaging and phase retrieval in the Fresnel domain (Li *et al*, 2017) was proposed. By applying the wavelet transformation, Arnold transformation, and row scanning compressive ghost imaging for the target image, the ciphertext matrix can be detected via a bucket detector (BD). The measurement key used in row scanning compressive ghost imaging can be decomposed and shared into two pairs of sub-keys through a (t, n) threshold secret sharing algorithm; they are then reconstructed into two phase-only mask (POM) keys with fixed pixel values, which are used for the phase-retrieval scheme in the Fresnel domain, and the other POM key was generated and updated by the iterative encoding of each plaintext image. Optical encryption scheme for multiple color images using complete trinary tree structure (Su *et al*, 2017) was proposed. In this scheme, the encryption modules (EMs) are taken as branch nodes, and the color components of plain images are input as leaf nodes. In every EM that consists of phase truncated Fresnel transforms and random amplitude-phase masks, three input images are subsequently encoded into a complex function and finally encrypted to a real-value image. In this scheme was encrypt multiple color images into a real-value grayscale cipher image, and make different color images have different encryption and decryption paths.

MATERIALS AND METHODS

In this section, the proposed Enhanced Loxodromic Cat Map and Double Random Phase Encoding (LCMDRPE) are explained. A unitary evolution operator or propagator characterizes the quantum dynamics. The chord and centre demonstration of an operator on the torus from its counterpart on the plane. The quantum propagator indicating cat maps in the centre or chord representation obtains simple expressions. Torus quantization implies that the Hilbert space $[H_N^{\chi}]^L$ associated with the 2L-torus has finite dimension N^L and is characterized by a vector Floquet parameter $\chi = (\chi_p, \chi_q)$ whose components are real numbers belonging to [0, 1]. The fact that $[H_N^{\chi}]^L$ has finite dimension implies that position and momentum eigenstates can only take on a set of discrete values that form a discrete lattice called quantum phase space (QPS). Any point x in this QPS has coordinates

$$x = \begin{pmatrix} p_m \\ q_n \end{pmatrix} = \frac{1}{N} \begin{pmatrix} m+\chi_p \\ n+\chi_q \end{pmatrix} \quad (1)$$

Chords are of the form

$$\xi_{r,s} = \frac{1}{N} \begin{pmatrix} r \\ s \end{pmatrix} = \frac{1}{N} \bar{\xi} \quad (2)$$

With r and s integer numbers and $\bar{\xi} = \begin{pmatrix} r \\ s \end{pmatrix}$, while the centre points $x_{a,b}$ are labelled by half-integer numbers a and b,

$$x_{a,b} = \frac{1}{N} \begin{pmatrix} a+\chi_p \\ b+\chi_q \end{pmatrix} \quad (3)$$

The Floquet parameters $\chi = (0,0)$. The matrix M must satisfy

$\sum_{j=1}^{L} M_{i,j} M_{i,j+L}$ = even integer for all i. (4)

N is coprime numbers and τ_{ξ} is invariant with respect to general similarity transformations, a complete representation of the propagator is obtained having the symbol on a lattice of chords Ξ such that

$$\Xi = \xi + n = \frac{2\tau_{\xi}^{'}}{N} \bar{\Xi} \quad (5)$$

where the components of $\bar{\Xi}$ are integer numbers up to N. So for any chord ξ there is an equivalent chord Ξ. For the allowed

values of N, the propagator for cat maps in the chord representation takes the form

$$U_M(\Xi) = (\tau_\xi)^{-1/2} e^{-i2\pi N\left[\frac{1}{4}\Xi\beta\Xi\right]} \sum_{m\in\Diamond_\xi} e^{-i2\pi N\frac{1}{4}m(\beta-\tilde{\Im})m} \quad (6)$$

Where τ_ξ is the number of fixed points of the classical map. For β matrices that fulfil the feline conditions, the symbol $U_M(\Xi)$ must represent a unitary operator.

$$U_M(\Xi) = \frac{e^{i\varphi_N(M)}}{\sqrt{N}^L} e^{-i2\pi N\left[\frac{1}{4}\Xi\beta\Xi\right]} \quad (7)$$

that restricts

$$\frac{e^{i\varphi_N(M)}}{\sqrt{N}^L} = (\tau_\xi)^{-1/2} \sum_{m\in\Diamond_\xi} e^{-i2\pi N\frac{1}{4}m(\beta-\tilde{\Im})m} \quad (8)$$

The phase $\varphi_N(M)$ is only an unimportant global phase factor, but the interference of the different $\varphi_N(M^l)$ for the different powers l of the map will have a crucial importance for the density of states.

ξ and Ξ are equivalent chords, the symbols $U_M(\xi)$ and $U_M(\Xi)$ are related through symmetry relations. So that

$$U_M(\xi) = \frac{e^{i\varphi_N(M)}}{\sqrt{N}^L} e^{-i2\pi N[S(\xi,n)]} \quad (9)$$

where $S(\xi,n)$ is the action of the classical orbit whose chord is ξ and that executes n loops around the torus.

The symplectically invariant form $g(m) = \frac{1}{4}m\beta m$ for the ξ-independent part of the chord generating function, instead of $f(m) = \frac{1}{4}m(B+\tilde{\Im})m$ and $g(m) = \frac{1}{4}m(\beta-\tilde{\Im})m$. We would have in (9) a supplementary phase factor $e^{i2\pi N\frac{1}{4}n\tilde{\Im}n} = e^{i\gamma_n}$ with γ_n a 'Maslov index' for the orbit. This observation is true for all of the following quantum theory.

The centre representation, for $2\tau_\xi$ described in $B = \frac{\bar{B}}{det(M+1)} = \pm\frac{\bar{B}}{\tau_x} = \pm\frac{\bar{B}}{\tau_x'}$ and $\beta = \frac{\bar{\beta}}{det(M-1)} = \pm\frac{\bar{\beta}}{\tau_\xi} = \pm\frac{\bar{\beta}}{\tau_\xi'}$, and N coprime numbers, a complete representation of the propagator is obtained by performing a transformation to centre points X that are integer multiples of τ_x'/N ,

$$X = x + \frac{1}{2}j = \frac{\tau_x'}{N}\bar{X} \quad (10)$$

where the components of $\bar{X}$ are integer numbers up to N. On these points the centre representation of the propagator takes the form

$$U_M(X) = (\tau_x)^{-1/2} e^{-i2\pi N[X\,B\,X]} \sum_{m\in\Diamond_x} e^{i2\pi N\frac{1}{4}m(B+\tilde{\Im})m} \quad (11)$$

$$= e^{i\varphi_N'(M)} e^{i2\pi N[X\,B\,X]} \quad (12)$$

where the last equality is obtained by imposing the unitarity of $\widehat{U}_M$ and using $\left(\frac{1}{N}\right)^2 \sum_{x_1,x_2} U(x_1)U^*(x_2)e^{i4\pi N(x-x_1)\wedge(x-x_1)} = 1(x) = f_N(x)$. Hence, we describe the angle $\varphi_N'(M)$ so that

$$e^{i\varphi_N'(M)} = (\tau_x)^{-1/2} \sum_{m\in\Diamond_x} e^{i2\pi N\frac{1}{4}m(B+\tilde{\Im})m} \quad (13)$$

From the symmetry relations $A\left(x+\frac{1}{2}m\right) = e^{i2\pi N\left[(x-\chi/N)\wedge m+\frac{1}{4}m\tilde{\Im}m\right]}A(x)$, we find that the symbols on the original points x are

$$U_M(x) = e^{i\varphi_N'(M)} e^{i2\pi N[S(x,j)]} \quad (14)$$

where here $S(x,j)$ is the centre generating function, described in

$S(x,m) = xBx + x(B-\Im)m + \frac{1}{4}m(B+\tilde{\Im})m$ *and* $S(\xi,m) = \frac{1}{4}\xi\beta\xi + \frac{1}{2}\xi(\beta+\Im)m + \frac{1}{4}m(\beta-\tilde{\Im})m$, on a centre point x for an orbit performing j loops. The cases above are then special cases where the propagator on the torus has the same form as its equivalent on the plane; thus, they are ideally suited for the comparison of classical and quantum motion.

The more the more familiar position representation of the propagator from its chord representation, we use $A(q_m,q_n) = \frac{1}{N}\sum_{x_p=0}^{\frac{1}{2}(N-1)} A(x_p, x_{\frac{1}{2}(m+n)} e^{i2\pi N x_p(q_m,q_n)})$,

$$U_M(q_m,q_n) = \frac{e^{i\varphi_N(M)}}{(N)^{3L/2}} \sum_{\xi_p=0}^{N-1} exp\left\{-i2\pi N\left[S(\xi_{p,m-n},n) + \frac{1}{2}(q_m+q_n)\xi_p\right]\right\} \quad (15)$$

and $A(q_m,q_n)$ equation allows us to obtain the position representation from the centre one:

$$U_M(q_m,q_n) = \frac{e^{i\varphi_N'(M)}}{(N)^L} \sum_{x_p=0}^{\frac{1}{2}(N-1)} exp\left\{-i2\pi N\left[S\left(x_{p,\frac{1}{2}(m+n)},j\right) + (q_m-q_n)x_p\right]\right\} \quad (16)$$

Hence, the above equation explains the position representation from the centre one. In LCM, structurally invariant system are called as Anosov maps, they are ergodic, mixing and have positive entropy. Loxodromic behaviour appears as a new alternative with respect to usual cat maps with one degree of freedom.

EXPERIMENTAL RESULTS

In this section, the performance of the proposed approach is analyzed with the other techniques. The comparison is made between CBMDRPE and LCMDRPE in terms of Maximum Deviation (MD) value, Correlation Coefficient (CC), Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

Maximum Deviation (MD) Value

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation among the original and the encrypted images. The steps of calculating this metric are:

1. Count the number of pixels for each gray-scale value in the range of 0 to 255 and present the results graphically for both the original and encrypted images (i.e. get their histogram distributions).
2. Calculate the absolute difference or deviation among the two curves and represent it, graphically.
3. Estimate the area under the absolute difference curve that is the sum of deviations.

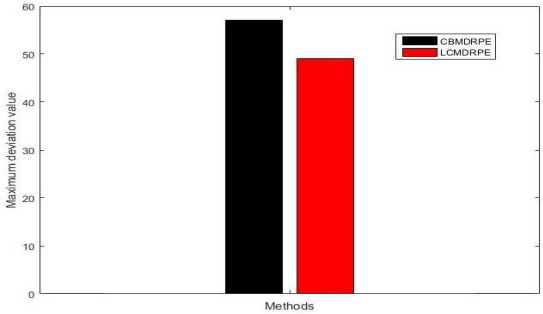

Figure 1 Maximum Deviation Value

Figure 1 shows the comparison of LCMDRPE and CBMDRPE in terms of maximum deviation. CBMDRPE has 57 while LCMDRPE 49 which means the LCMDRPE provides better result with decreased deviation value.

Correlation Coefficient (CC)

The correlation coefficient among the original and the encrypted images has been used as a tool for encryption quality evaluation. The correlation coefficient is estimated as:

$$r = \frac{cov(f,\psi)}{\sqrt{D(f)}\sqrt{D(\psi)}}$$
$$D(f) = 1/L\sum_{l=1}^{L}(f_l - E(f))^2$$
$$cov(f,\psi) = 1/L\sum_{l=1}^{L}(f_l - E(f)(\psi_t - E(\psi))$$
$$E(f) = 1/L\sum_{l=1}^{L} f_l$$

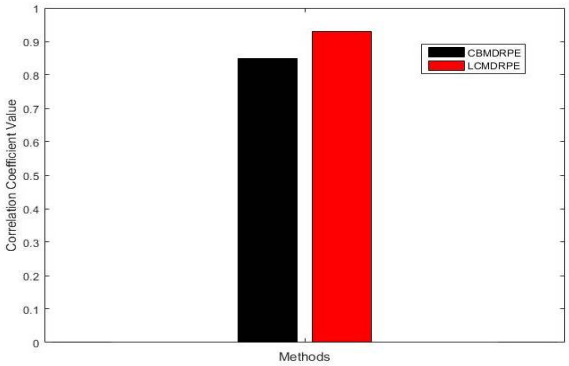

Figure 2 Correlation Coefficient

Figure 2 shows the comparison of LCMDRPE and CBMDRPE in terms of correlation coefficient. CBMDRPE has 0.85 while LCMDRPE 0.93 which means the LCMDRPE provides better result with increased value of correlation coefficient.

Mean Square Error (MSE)

Mean Square Error (MSE) among the decrypted and original images is computed. It is described as:

$$MSE = \frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}|f(x,y) - \hat{f}(x,y)|^2$$

where X and Y are the image dimensions.$f(x,y)$ and $\tilde{f}(x,y)$ indicate the original and the decrypted images, respectively.

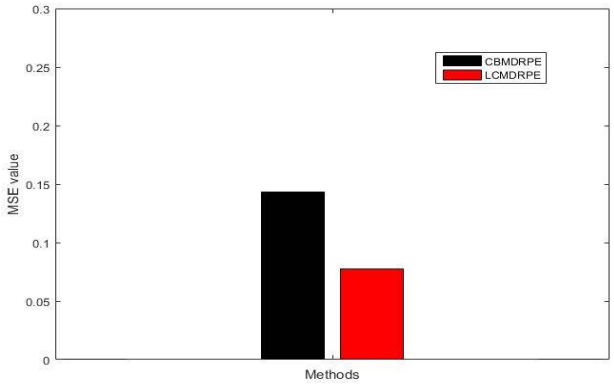

Figure 3 Mean Square Error comparison

Figure 3 shows the comparison of LCMDRPE and CBMDRPE in terms of MSE values. CBMDRPE has 0.1433 while LCMDRPE 0.0778 which means the LCMDRPE provides better result with decreased MSE values.

Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio is estimated from the MSE

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

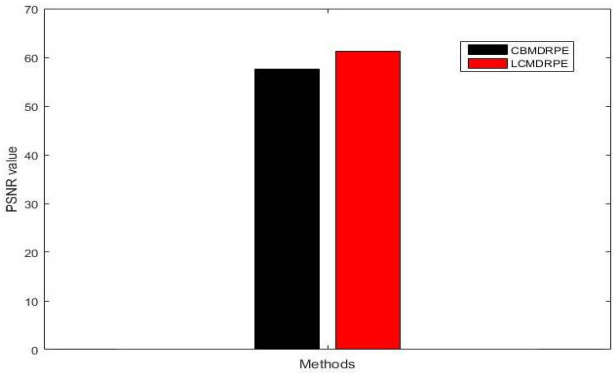

Figure 4 Peak Signal-to-Noise Ratio comparison

Figure 4 shows the comparison of LCMDRPE and CBMDRPE in terms of PSNR values. CBMDRPE has 57.65 while LCMDRPE 61.23 which means the LCMDRPE provides better result with increased PSNR.

CONCLUSION

In this paper, Loxodromic Cat Map with DRPE method was proposed. This scheme behaviour appears as a new alternative with respect to usual cat maps with one degree of freedom. This approach is providing better results in terms of maximum deviation, correlation coefficient, mean square error and peak signal-to-noise ratio.

References

Singh, N., & Sinha, A. (2009). Gyrator transform-based optical image encryption, using chaos. *Optics and Lasers in Engineering*, 47(5), 539-546.

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

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

Elshamy, A. M., Rashed, A. N., Mohamed, A. E. N. A., Faragalla, O. S., Mu, Y., Alshebeili, S. A., & El-Samie, F. A. (2013). Optical image encryption based on chaotic baker map and double random phase encoding. *Journal of Lightwave Technology*, 31(15), 2533-2539.

Nalegaev, S. S., & Petrov, N. V. (2015). Simple Criteria to Determine the Set of Key Parameters of the DRPE Method by a Brute-force Attack. *Physics Procedia*, 73, 281-286.

Wang, Q., Guo, Q., Lei, L., & Zhou, J. (2015). Optical interference-based image encryption using circular harmonic expansion and spherical illumination in gyrator transform domain. *Optics Communications*, 346, 124-132.

Neji, N., Jridi, M., Alfalou, A., & Masmoudi, N. (2016). Enhancement of DRPE performance with a novel scheme based on new RAC: Principle, security analysis and FPGA implementation. *Optics Communications*, 360, 73-82.

Sivamalar, R., & Sharma, S. (2016). An optical image encryption using chaotic kicked rotator map with double random phase encoding.

Jiao, S., Zou, W., & Li, X. (2017). QR code based noise-free optical encryption and decryption of a gray scale image. *Optics Communications*, 387, 235-240.

Kumar, R., & Bhaduri, B. (2017). Optical image encryption using Kronecker product and hybrid phase masks. *Optics & Laser Technology*, 95, 51-55.

Li, X., Meng, X., Wang, Y., Yang, X., Yin, Y., Peng, X., & Chen, H. (2017). Secret shared multiple-image encryption based on row scanning compressive ghost imaging and phase retrieval in the Fresnel domain. *Optics and Lasers in Engineering*, 96, 7-16.

Su, Y., Tang, C., Gao, G., Gu, F., Lei, Z., & Tang, S. (2017). Optical encryption scheme for multiple color images using complete trinary tree structure. *Optics and Lasers in Engineering*, 98, 46-55.

How to cite this article:

Jayaseelan, L and Sureshkumar, C.2017, An Optical Image Encryption Using Loxodromic Cat Map With Double Random Phase Encoding (Lcmdrpe). *Int J Recent Sci Res.* 8(8), pp. 18946-18950. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0808.0598

****