DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4606

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

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

Jayaseelan. L
Research Scholar, Department of Computer Science
Periyar University
Salem, India

Sureshkumar. C
Principal
Dr. Nagarathinam's College of Engineering
Namakkal, India

Abstract: Recently, a new kind of image encryption approach Loxodromic Cat Map with Double Random Phase Encoding (LCMDRPE) has received much attention due to the advantages such as increased correlation coefficient and reduced deviation value. However, the encryption scheme performance was low. Hence, we propose an optical image encryption using Loxodromic Cat Map with Improved Double Random Phase Encoding (LCMIDRPE). Then we introduce Hilbert Huang Transform (HHT) instead of Fourier transform. This approach improves the double random phase encoding. 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.

Keywords: Optical Image Encryption, Loxodromic Cat Map (LCM), Improved Double Random Phase Encryption

I. INTRODUCTION

With the development of communication and computer technology, digital image encryption and hiding method has come to the research hotspot, which has many applications in information security domain such as the product masks, passport verification, credit card, human facial images and so on. Out of the various techniques for optical image encryption [1, 2], double random phase encoding is the most well known method [3]. If the red (R), green (G) and blue (B) components of the color image to be encrypted was separately encoded using double random phase encoding method, complexity and cost of the optical system will increases. This template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. PLEASE DO NOT RE-ADJUST THESE MARGINS. Some components, such as multi-leveled equations and graphics, are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

An Optical Image Encryption Using Loxodromic Cat Map with Double Random Phase Encoding (LCMDRPE) [4] was proposed. Loxodromic behaviour appears as a new alternative with respect to usual cat maps with one degree of freedom and quantized. The quantum periodicity function has been found to be insensitive to the structural stability. However, the double random phase encoding performance was low and complexity. Hence, we propose Loxodromic Cat Map with Improved Double Random Phase Encoding (LCMIDRPE) for optical image encryption. In IDRPE method, we introduce Hilbert-Huang Transform (HHT) for enhance the encryption performance.

The remainder of the article is organized as follows: In Section 2, some related works are given. In Section 3, the proposed scheme is described. Experimental Results are presented in Section 4. And the last section concludes the research work.

II. RELATED WORK

A single-channel color image encryption technique using double random phase encoding approach and orthogonal composite grating [5] was proposed. A RGB (Red, Green and Blue) image was decomposed into RGB components before they are modulated into an orthogonal composite grating. In this scheme, the modulated composite grating was encrypted though double random phase encoding system. By the side of decryption, the modulated composite grating was decrypted via using the secret keys. The RGB components are recovered through phase demodulating and filtering. However, a small filtering loss of this method was happening. An encryption algorithm via using the random pixel scrambling operation in fractional Fourier transforms domains [6] were proposed to improve the security of secret image, the data of the second random phase P2 in DRPE are employed in the scrambling operation of the amplitude information of the output and input in fractional Fourier transform. However, very difficult to guarantee that the scrambled code stream will not crash a standard decoder.

A new fractional two dimensional triangle function combination discrete chaotic map (2D-TFCDM) [7] was proposed by utilizing the discrete fractional calculus. Then, new chaotic dynamics behaviors were found with the map. In addition, the map was applied in decryption and encryption of image transmission in information security. A novel visually secure image encryption scheme based on compressive sensing (CS) [8] was proposed. The plain image was first transformed to the coefficient matrix using DWT, and then scrambled by a plain image related zigzag path and encrypted into a compressed cipher image by compressive sensing. Next, the cipher image was embedded into a carrier image and finally gets a visually secure cipher image.

An image encryption method [9] was proposed based on fuzzy cellular neural network (FCNN). The shortcomings of FCNN in encrypting image are identified, and the FCNN model was then modified to address these shortcomings. Specifically, a framework was developed to recognize the values of the parameters of FCNN to create chaotic signals that are in turn utilized to encrypt the image. The encryption scheme was

© 2015-19, IJARCS All Rights Reserved

designed where an encrypted pixel was created based on the corresponding plaintext pixel together with the neighbouring encrypted pixels. However, this approach provided the slow computation method. A novel compressive sensing (CS) based image cipher associated with DRPE method [10] was proposed. In this scheme, to ensure the resistance to chosen plaintext attack (CPA), a newly measurement matrix updating approach with low complexity was introduced in the CS sampling process. In addition, the sparsity constraint of the CS reconstruction issue was exploited to improve the security of this technique. However, CS was required to impose constraints such as sparsity and incoherence that are introduced for this signal recovery to be efficient.

A multiple-image encryption (MIE) algorithm based on the permutation and mixed image element [11] was proposed that was encrypt k images at once, where k can be designated by the user. This scheme was performed following procedures, 1) segment the original images into pure image elements; 2) scramble all the pure image elements with the permutation generated through the piecewise linear chaotic map (PWLCM) system; 3) combine mixed image elements into scrambled images; 4) diffuse the content of mixed image elements via performing the exclusive OR (XOR) operation between the chaotic image and scrambled images generated by another PWLCM system. A new secure image encryption algorithm [12] was proposed which employs a new chaos based RNG and S-BOX structures. In this algorithm, S-Box which was one of the most important components of block encryption algorithms was used. Chaotic system was developed for creating S-Box and image encryption algorithm. Chaos based random number generator was designed with the help of the new chaotic system. Then, NIST tests are run on generated random numbers to verify randomness. In addition, S-Box design algorithm was developed to generate the chaos based S-Box to be utilized in encryption algorithm and performance tests are made.

III. PROPOSED METHODOLOGY

A. *Loxodromic Cat Map with Improved Double Random Phase Encoding (LCMIDRPE)*

Generally double random phase encoding was used Fourier transform but in this paper, we introduce Hilbert Huang Transform (HHT). The Hilbert transform $H[x(t)]$ for any signal $x(t)$ is described as

$$H[x(t)] = y(t) = \frac{1}{\pi}\int \frac{x(T)}{t-T}dT \qquad (1)$$

where $H[\bullet]$ indicates the Hilbert transform operation. Theoretically, any analytic signal $z(t)$ through the sum of its real part $x(t)$ and imaginary part $y(t)$, with the latter being the Hilbert transform of the real part. This output in

$$z(t) = x(t) + jy(t) \qquad (2)$$

The above equation can be rewritten in polar coordinate system as

$$z(t) = a(t)e^{j\theta(t)} \qquad (3)$$

where

$$\begin{cases} a(t) = \sqrt{x(t)^2 + y(t)^2} \\ \theta(t) = tan^{-1}\left(\frac{y(t)}{x(t)}\right) \end{cases} \qquad (4)$$

represents the instantaneous amplitude and phase of the analytic signal, respectively. From the instantaneous phase $\theta(t)$, the instantaneous frequency $\omega(t)$ of the signal can be derived as

$$\omega(t) = \frac{d(\theta(t))}{dt} = \frac{\dot{y}(t)x(t) - y(t)\dot{x}(t)}{x^2(t) + y^2(t)} \qquad (5)$$

Accordingly, the real part of the signal $x(t)$ can be rewritten in terms of the amplitude and instantaneous frequency as a time dependent function

$$x(t) = \Re(z(t)) = \Re\left(a(t)e^{j\int \omega(t)dt}\right) \qquad (6)$$

Where the symbol $\Re(\bullet)$ indicates the real part of the analytic signal $z(t)$.

Decomposition of such a signal is based on the following observations.

1) The signal has at least two extrema

- One maximum and
- One minimum.

2) The characteristic time scale is clearly described through the time lapse among successive alternations of local maxima and minima of the signal.

3) If the signal has no extrema but contains inflection points, then it can be differentiated one or more times to reveal the extrema.

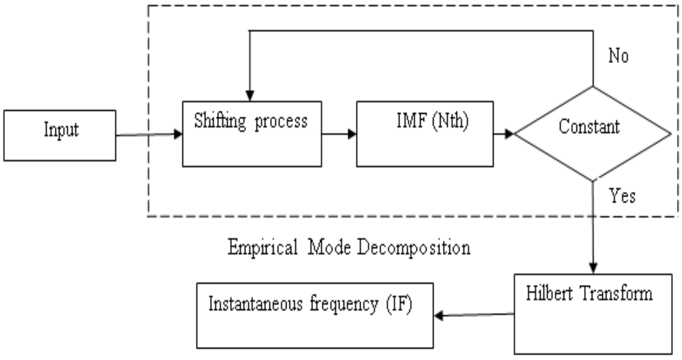

Figure 1. Hilbert Huang Transform process

The Empirical Mode Decomposition (EMD) method decomposes the signal into a number of Intrinsic Mode Functions (IMFs), each of which a monocomponent function. Then, the Hilbert transform is applied to compute the instantaneous frequencies of the original signal.

Separating $c_1(t)$ from the original signal $x(t)$, the residue is derived as

$$r_1(t) = x(t) - c_1(t) \qquad (7)$$

The residue $r_1(t)$ can be treated as the new signal and the iteration procedure is repeated to extract the rest of the IMFs inherent to the signal $x(t)$ as

$$\begin{cases} r_1(t) - c_2(t) = r_2(t) \\ \quad\vdots \\ r_{n-1}(t) - c_n(t) = r_n(t) \end{cases} \qquad (8)$$

The signal decomposition procedure is terminated when $r_n(t)$ becomes a monotonic function, from which no further IMFs can be extracted. By substituting (8) into (7), the signal $x(t)$ is decomposed into a IMFs that are the constituent components of the signal. As a outcome, the signal $x(t)$ can be expressed as

$$x(t) = \sum_{i=1}^{n} c_i(t) + r_n(t) \tag{9}$$

where $c_i(t)$ indicates the i th intrinsic mode function and $r_n(t)$ is the residue of the signal decomposition. Equation (9) provides a complete description of the empirical mode decomposition process that can be evaluated through checking the amplitude error among the reconstructed and the original signal.

Equation (1)-(5) and (9), (6) can be modified as

$$x(t) = \Re\left(\sum_{i=1}^{n} a_i(t) e^{j\int \omega_i(t)dt}\right) \tag{10}$$

The HHT of the signal is mathematically described as

$$HHT(t,\omega) = \sum_{i=1}^{n} HHT_i(t,\omega) \equiv \sum_{i=1}^{n} a_i(t,\omega_i) \tag{11}$$

where $HHT_i(t,\omega)$ indicates the time frequency distribution obtained from the i th IMF of the signal. The symbol ≡ indicates ‘by definition’ and $a_i(t,\omega_i)$ combines the amplitude $a_i(t)$ and instantaneous frequency $\omega_i(t)$ of the signal together.

IV. EXPERIMENTAL RESULTS

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

A. *Maximum Deviation Analysis*

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.

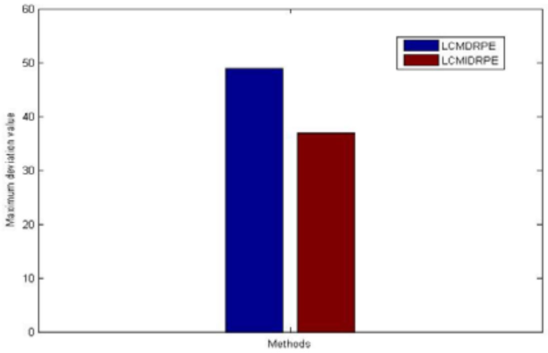

Figure 2. Maximum Deviation Value

Figure 2 shows that the comparison of LCMIDRPE and LCMDRPE methods in terms of Maximum Deviation. The X-axis indicates the methods. Y-axis indicates the Maximum deviation value. The Maximum deviation value decreased for proposed LCMIDRPE method compare to existing LCMDRPE method.

B. *Correlation Coefficient Analysis*

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:

$$r = \frac{cov(f,\psi)}{\sqrt{D(f)}\sqrt{D(\psi)}}$$

and $D(f) = 1/L\sum_{l=1}^{L}(f_l - E(f))^2$

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

$$E(f) = 1/L\sum_{l=1}^{L} f_l$$

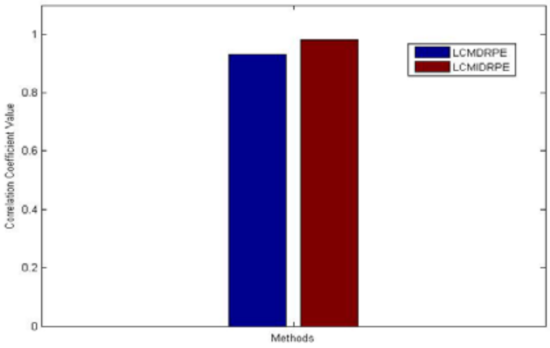

Figure 3. Correlation coefficient

Figure 3 shows that the comparison of LCMIDRPE and LCMDRPE methods in terms of Correlation Coefficient. The X-axis indicates the methods. Y-axis indicates the Correlation Coefficient value. The Correlation Coefficient value increased for proposed LCMIDRPE method compare to existing LCMDRPE method.

C. *Mean Square Error (MSE)*

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

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

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

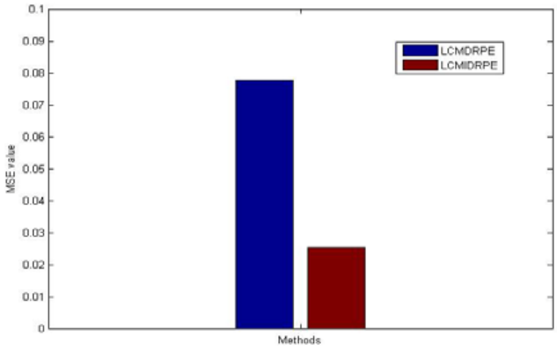

Figure 4. MSE comparison

Figure 4 shows that the comparison of LCMIDRPE and LCMDRPE methods in terms of Mean Square Error. The X-axis indicates the methods. Y-axis indicates the Mean Square Error value. The Mean Square Error value decreased for proposed LCMIDRPE method compare to existing LCMDRPE method.

D. *Peak Signal-to-Noise Ratio (PSNR)*

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

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

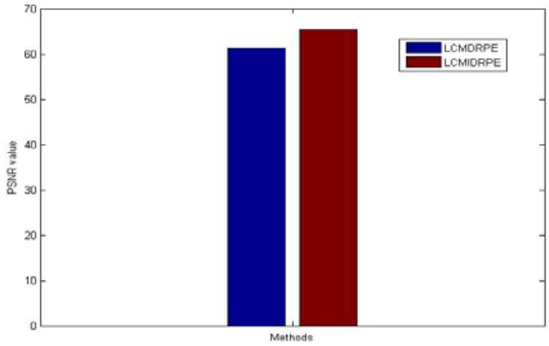

Figure 5. PSNR comparison

Figure 5 shows that the comparison of LCMIDRPE and LCMDRPE methods in terms of PSNR. The X-axis indicates the methods. Y-axis indicates the PSNR value. The PSNR value increased for proposed LCMIDRPE method compare to existing LCMDRPE method.

V. CONCLUSION

In this paper, Improved Double Random Phase Encoding (IDRPE) is proposed to enhance the encryption performance with efficient result. IDRPE was used the Hilbert-Huang Transform. This approach is providing better results in terms of maximum deviation, correlation coefficient, mean square error and peak signal-to-noise ratio.

VI. REFERENCES

[1] Ohtsubo, J., & Fujimoto, A. (2002). Practical image encryption and decryption by phase-coding technique for optical security systems. Applied optics, 41(23), 4848-4855.

[2] Zhang, Y., & Wang, B. (2008). Optical image encryption based on interference. Optics Letters, 33(21), 2443-2445.

[3] Kishk, S., & Javidi, B. (2002). Information hiding technique with double phase encoding. Applied Optics, 41(26), 5462-5470.

[4] 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.

[5] He, Y., Cao, Y., & Lu, X. (2012). Color image encryption based on orthogonal composite grating and double random phase encoding technique. Optik-International Journal for Light and Electron Optics, 123(17), 1592-1596.

[6] Liu, Z., Li, S., Liu, W., Wang, Y., & Liu, S. (2013). Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Optics and Lasers in Engineering, 51(1), 8-14.

[7] Liu, Z., & Xia, T. (2017). Novel Two Dimensional Fractional-order Discrete Chaotic Map and Its Application to Image Encryption. Applied Computing and Informatics.

[8] Chai, X., Gan, Z., Chen, Y., & Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing. Signal Processing, 134, 35-51.

[9] Ratnavelu, K., Kalpana, M., Balasubramaniam, P., Wong, K., & Raveendran, P. (2017). Image encryption method based on chaotic fuzzy cellular neural networks. Signal Processing, 140, 87-96.

[10] Hu, G., Xiao, D., Wang, Y., Xiang, T., & Zhou, Q. (2017). Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes. Optics and Lasers in Engineering, 98, 123-133.

[11] Zhang, X., & Wang, X. (2017). Multiple-image encryption algorithm based on mixed image element and permutation. Optics and Lasers in Engineering, 92, 6-16.

[12] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons & Fractals, 95, 92-101.

© 2015-19, IJARCS All Rights Reserved