Indonesian Journal of Electrical Engineering and Computer Science
Vol. 9, No. 1, January 2018, pp. 97~100
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i1.pp97-100

Chaos Based Image Encryption

Suresh G.B[1], V. Mathivanan[2]
[1]Research Scholar, AMET University, Chennai
[2]Professor, SRM University, Chennai

Article Info

Article history:

Received Jun 27, 2017
Revised Nov 23, 2017
Accepted Dec 19, 2017

Keywords:

Chaos Map
Decryption
Encryption
Histogram
Image

ABSTRACT

New method of secure image encryption and decryption scheme based on the chaos is proposed. There are two steps are followed after the preprocessing step in the proposed system namely, Encryption and Decryption. In preprocessing, images are denoised using median filter. Then the original input images will be encrypted by using the chaos mapping algorithm. At last the original images are retrieved back from the encrypted image by using the key that is specified during the encryption process for the decryption of the original images. Then the histogram mapping is done for the encrypted and the decrypted images. The proposed system is tested on well-known images like Lena, Mandrill, Clown and Barbara. The experimental results have demonstrated that the introduced image encryption scheme can achieve high security for practical image encryption.

Corresponding Author:

Suresh G.B,
Research Scholar, AMET University, Chennai

1. INTRODUCTION

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse- grained level.

2. BACKGROUND

Image Encryption using impulsive synchronization of reaction–diffusion neural networks with mixed delays is presented in [1]. This principle is established by given an impulse-time-dependent Lyapunov functional combined with the use of a kind of integral dissimilarity for treating the reaction-diffusion terms. Swapping based confusion approach based chaotic image encryption scheme is discussed in [2]. To enhance the protection and effectiveness of chaos-based image cryptosystems is discussed. Correlation coefficients, key sensitivity analysis, differential analysis, histograms and information entropy are included for analyzing the image encryption.

Lag synchronization of switched neural networks through neural activation function in image encryption is investigated in [3]. Output depending controller in the case of packed circuits is discussed in this system while it is rigid to measure the inner state of the circuits. It is grave to design the controller based on the neuron activation task. Digital image encryption using image scrambling methods is described in [4]. Non-Commutative wavelet transforms and Poker Shuffle transform based image scrambling method is presented. Performance of this method is increased because of Non-commutative Wavelet transform over conventional Wavelet transform and non-linearity and non analytic computation characteristics of Poker Shuffling suitability. Magic squares scheme based image encryption is discussed in [5]. Magic square encryption method referred as Good Lattice Point (GLP) method. Disordering status of pixel points are focused by traditional magic square encryption method according to magic squares. But various encryption periods and better encrypted effect are obtained in GLP method compare to traditional one.

Discrete Wavelet Transform (DWT) and chaos system based image encryption and decryption is presented in [6]. 2D-DWT and chaos system are used to understand the image encryption and decryption during the transmission of digital image for the security problem. 'bior3.7' wavelet is used for decomposition and I-D Logistic chaos sequence is used to reorder the low frequency wavelet coefficient matrix. Decryption process is reverse with encryption. Compression system and efficient image encryption design through prediction error clustering and random permutation is described in [7]. Image encryption-then-compression system, where both lossless and lossy compression is considered in this method. An arithmetic coding-based approach can be demoralized to efficiently compress the encrypted images is demonstrated. Combine technique [8] for classification of IRS P6 LISS-III was proposed to combine the images efficiently. Multi level classification techniques are used here. Image super resolution reconstruction [9] using genetic algorithm as well as iterative adaptive regularization method was proposed for reconstructing the images. High-resolution seismic imagery [10] was proposed to extract the images for palaeo channels. This mechanism is proposed for obtaining high resolution images for the special kind of long distance images. Method for full security of medical imaging and its data dedicated to m-Health and based on an approach which combine a semi reversible build watermarking method robust to JPEG compression, build fragile watermarking, and a stream cipher symmetric encryption algorithm is presented in [11]. Implementation of image encryption algorithm to produce a quick image encryption system is employed in [12]. The algorithm developed was super-encryption algorithm [13] that combines Play fair cipher and the Vigenere cipher. Cipher image histogram has a distribution of diversity and a important difference to the plain image histogram, and frequency of incidence of every intensity value in the histogram of cipher image is also not level, which means cannot give clues to do statistical attack. Cryptosystem for fine-grained sharing of encrypted data that we call key-policy attribute-based encryption is developed in [14].

3. THE PROBLEM

One drawback of encrypting data is that it can be selectively shared only at a coarse- grained level i.e., giving another party your private key. Many healthcare leaders believe that encrypting data increases the time to retrieve and review information, which ultimately decreases efficiency.

4. PROPOSED SOLUTION

A new method of secure image encryption and decryption scheme based on the chaos mapping is proposed. In our method there are two steps namely, Encryption and Decryption. First, the input original images will be encrypted by using the chaos mapping algorithm. Secondly, the original images are retrieved back from the encrypted image by using the key that is specified during the encryption process for the decryption of the original images.

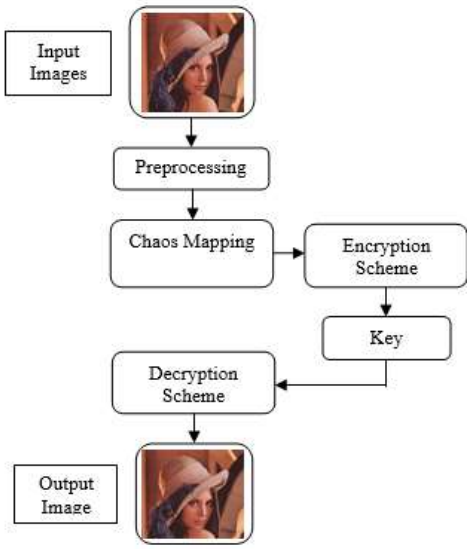

Figure 1. Proposed Encryption & Decryption Block Diagram

Then the histogram mapping is done for the encrypted and the decrypted images. The proposed system is tested on well-known images like Lena, Mandrill, Clown and Barbara. The block diagram for our proposed system is been shown in the Figure 1.

5. MODULES

5.1. Pre-Processing

In the image encryption and the decryption process, first the input images are taken as an account that the input should be encrypted by allotting a key to it as the decryption scheme. For this the pre-processing step is done to denoise the input image and also the RGB images will be change into grey scale image for the easy implementation without any loss of the image data.

5.2. Encryption Process

The encryption process is done as said above in the proposed scheme by using the chaos mapping scheme. The process of developing a chaos-based encryption can be summarized as follows. First, a chaos map is generalized by introducing parameters into the map. Then, the map is modified so that its domain and range are both the same square lattices of points (pixels, or some other general data items). Then a certain key values will be generated for the encryption process to be completed. Only this is very important for the decryption of the original image from the encrypted image.

5.3. Decryption Process

The decryption process is nothing but a reverse process of the encryption process. Only the difference is that the encrypted images will be taken as the input to the decryption process and the key will be given along with that encrypted output image for the decryption of the original image without any data loss of that image. By this way the image encryption and decryption can be done by using the chaos mapping scheme.

6. RESULTS AND DISCUSSION

The performance of the proposed method using chaos mapping for encryption and decryption was done. Secret key was generated for encrypt and decrypt an image. The experimental results have demonstrated that the introduced image encryption scheme can achieve high security for practical image encryption. Figure 2 shows the secret key and encrypted image using chaos mapping with bit-xor method using the generation of secret key.

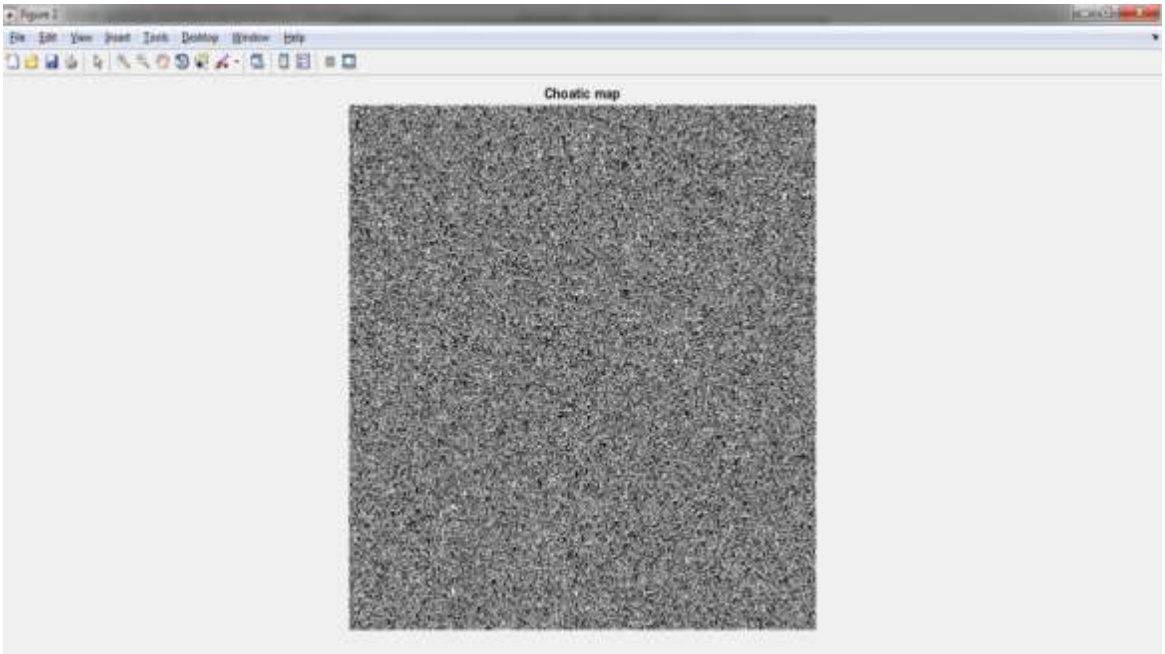

Figure 2. Encrypted Image

7. CONCLUSION

In this paper, we propose a novel image encryption scheme based on chaos mapping method. Secret key was generated to encrypt and decrypt an image. The security and performance of the proposed image encryption scheme have been analyzed thoroughly to show that the proposed image encryption scheme is highly secure and can be applied for secure image and video communication applications.

REFERENCES

[1] Chen W H, Luo S, Zheng W X. Impulsive synchronization of reaction–diffusion neural networks with mixed delays and its application to image encryption. *IEEE transactions on neural networks and learning systems*. 2016; 27(12): 2696-2710.
[2] Ye R, Xi Y, Ma Y. *A chaotic image encryption scheme using swapping based confusion approach*. IEEE International Conference on Computer Communication and the Internet. 2016; 374-377.
[3] Wen S, Zeng Z, Huang T, Meng Q, Yao W. Lag synchronization of switched neural networks via neural activation function and applications in image encryption. *IEEE transactions on neural networks and learning systems*. 2015; 26(7): 1493-1502.
[4] Shelke R, Metkar S. *Image scrambling methods for digital image encryption*. IEEE International Conference on Signal and Information Processing. 2016; 1-6.
[5] Zhong W, Deng Y H, Fang K T. *Image encryption by using magic squares.* In Image and Signal Processing. IEEE International Congress on BioMedical Engineering and Informatics. 2016; 771-775.
[6] Li X, Zhang Y. *Digital image encryption and decryption algorithm based on wavelet transform and chaos system*. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference. 2016; 253-257.
[7] Zhou J, Liu X, Au O C, Tang Y Y. Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *IEEE transactions on information forensics and security*. 2014; 9(1): 39-50.
[8] Upadhyay A, Singh S K, Kambli S. Combine technique for classification of IRS P6 LISS-III satellite images. *International Journal of Control Theory and Applications.* 2016; 9(10): 4293-4299.
[9] Panda S S, Jena G, Sahu S.K. *Image super resolution reconstruction using iterative adaptive regularization method and genetic algorithm.* In Computational Intelligence in Data Mining. 2015; 2: 675-681.
[10] Leslie C, Jones L, Papp É, Wake-Dyster K, Deen T J, Gohl K. *High-resolution seismic imagery of palaeochannels near West Wyalong New South Wales*. 2000; 31(1/2): 383-388.
[11] Boussif M. New Watermarking/Encryption Method for Medical Imaging FULL Protection in m-Health. *International Journal of Electrical and Computer Engineering (IJECE)*, 2017; 7(6).
[12] Prasetio B H, Setiawan E, Muttaqin A. Image Encryption using Simple Algorithm on FPGA. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 2015; 13(4): 1153-1161.
[13] Setyaningsih E, Iswahyudi C, Widyastuti N. Image encryption on mobile phone using super encryption algorithm. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 2012; 10(4): 815-824.
[14] Nandhini M J S, Kumar A, Abishek N, Meerah G, Ashika G. *An Efficient Key Policy Attribute Based Encryption Scheme In Cloud Computing*, 2017; 9(2): 1-14.