ISSN 2320 -2610
Volume 4, No.1, January – February 2015
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://warse.org/pdfs/2015/ijmcis02412015.pdf

Image Encryption Scheme Using Chaotic Map

Pragati Thapliyal[1], Madhu Sharma[2]
[1]MTech Student DIT University, India, capricornpragati3@gmail.com
[2]Asst. Professor DIT University, India, madhuashishsharma@gmail.com

ABSTRACT

Swift development in contingencies of information transmission and communication, cryptographic techniques are in great demand. A variety of effective chaos-based image encryption schemes have been proposed. The intent of this paper is to propose an image encryption scheme using chaotic map. Arnold cat map is used for diffusion as well as for substitution. This paper applies an alternate structure of the classic block cipher applied with Arnold Cat map. The paper that is being followed uses Arnold cat map and OCML for encryption which leads to large computational time, whereas our schemes computational time is less as compared to the previous.

Key words: Arnold Cat map, Cryptography, Chaotic Maps, Image Encryption.

1. INTRODUCTION

In current scenario of information age, communication has a crucial role and has a great impact on the growth of technology. The computer security has continuously involved in making communication more rife and robust. Security mainly consists of three parts namely data confidentiality, data integrity and data authenticity. The data confidentiality is the protection of data from unauthorized disclosure. The data integrity is defined as the assurance that the data received are exactly as sent by an authorized entity. The authentication is the assurance that the communication entity is the one that it claims to be [10]. A mechanism is a need for security and privacy of data that is transferred over the electronic media. Either the communication media is wired or wireless, protection is needed from the unauthorized access of information. The method of transforming the original information into an unreadable format is called Encryption and the reverse process is called Decryption of information. The study of encryption and decryption is known as Cryptography.

A process in which data is protected from destroying or from unauthorized access is called data protection. Data protection could be provided on different ways. One of them is cryptology, it consists of both cryptography and cryptanalysis. Cryptography involves the study and the applications of the principles and techniques by which the information is rendered unintelligible to all but the intend to receive. It is an effective way for protecting sensitive information as it is stored on the media and transmitted through non trusted network communication paths. Cryptography is used to create and use methods for transformation of data, information or messages in order to make that transformed message visible only for precise, desired person. Breaking and exploiting the characteristics of cryptographic method in order to get information is known as cryptanalysis.

Chaos word has been derived from the Greek, which refers to unpredictability and it is defined as a study of nonlinear dynamic system. Chaos theory is a mathematical physics which was developed by Edward Lopez. Chaotic maps are simple unstable dynamical systems with high sensitivity to initial conditions. Due to butterfly effect small deviations in the initial conditions (due to approximations or numerical calculations) lead to large deviations of the corresponding orbits, rendering the long-term forecast for the chaotic systems intractable. Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Traditional image encryption [2] algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large. The chaos-based encryption [5] has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. Images are used in distinct areas such as medical, military, science, engineering, art, entertainment, advertising, education as well as training.

Digital information and data are transmitted more often over the Internet now a days. The availability and efficiency of global computer networks for the communication of digital information and data have accelerated the popularity of digital media. Digital images, video and audio have been revolutionized in the way they can be captured, stored, transmitted and manipulated, and this gives rise to a wide range of applications in education, entertainment, media and military, as well as other fields.

Traditional image encryption algorithm such as data encryption standard (DES), AES etc. has the weakness of low-level efficiency when the image is large [6]-[7]. The chaos-based encryption [2]-[3] has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behavior, repeated processing and very high

diffusion and confusion properties that are desirable for cryptography.

The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behavior, repeated processing and very high diffusion and confusion properties that are desirable for cryptography. Chaos is the apparently chaotic state generated by the nonlinear equations of motion. With the fast evolution of digital data exchange, security of information becomes much important in data storage and transmission. Due to the increasing use of images in industrial processes, it is essential to protect confidential images from unauthorized access.

Due to the rapid growth of internet, the security of digital images has become more important and gained attention. The prevalence of multimedia technology in the above aspect has promoted digital images to play a more significant role than the traditional texts, which require serious protection for users and privacy for all applications. In present age chaos based cryptosystem has gained attention in research of information security and number of chaos based image encryption algorithms has been proposed. In general, many digital image services require reliable security in storage and transmission, due to which the individual appreciation and privacy differ from a person to person. The reason for the image encryption is to transmit the image securely over the network so as to protect it from unauthorized user.

Image encryption can be achieved through two different methods:

1. Share-Based Encryption Schemes

2. Chaos Based Image Encryption

In the former scheme plane image is divided into n secret images share and is transferred to different person through network, on combination of any k secret share, out of all n secret shares. Whereas in the later one plain image goes through diffusion and substitution to form an encrypted image [5].

1.1 ARNOLD'S CAT MAP

Arnold's Cat Map is named after the Russian mathematician Vladimir Arnold, who discovered it in 1960s using an image of a cat. Arnold's Cat Map is a transformation that can be applied to an image. The pixels of the image appear to be randomly rearranged, but when the transformation is repeated enough times, the original image will reappear.

Equivalently, in matrix notation, this is

$$\Gamma\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 \quad (1)$$

The original image of the cat is sheared and then wrapped around in the first iteration of the transformation. After some iterations, the resulting image appears rather random or disordered, yet after further iterations the image appears to have further order ghost-like images of the cat, multiple smaller copies arranged in a repeating structure and even upside-down copies of the original image and ultimately returns to the original image.

Arnold's cat map is a simple discrete system that stretches and folds the trajectories in phase space, which is another typical feature of chaotic processes. The phase space for this simple system can be represented by a square, and the stretching and folding process scrambling effect is relatively best in Arnold's Cat Map. The Arnold Cat Map takes concepts from linear algebra and uses them to change the positions of the pixel values of the original image. The result after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image.

1.2 THE PROPOSED SCHEME:

The proposed scheme is an alteration of the one suggested by Zhang Yi, WANG. In their system, two a general cat-map is used for permutation and diffusion, as well as the OCML (one-way coupled map lattice), which is applied for substitution. These two methods are operated alternately in every round of encryption process [1]. In our altered method the original images should be partitioned or merged into N× 2N pixel blocks at first. In doing so, the proposed algorithm encrypts an N × 2N plaintext block into an N × 2N ciphertext block.

The details are:

1. Take the image pixels as an input.

2. Partition the N× 2N plaintext block into two N × N left and right parts.

3. Shuffle the pixels of image using cat map.

4. Now the output generated from step 2 is xored with the remaining pixels from the image.

5. The output from step 4 will serve as an input for the next round.

6. Reiterate steps 2 — 5 to execute n rounds of encryption.

1.3 ALGORITHM

The image encryption algorithm is based on the Arnold cat map. It uses chaotic sequence generated by Arnold cat map to encrypt image data.

Step1. Initialize required variables(I, Ii, imgX, imgX2, c, nY, newxX)

Step2. I reads an image(.jpg,.gif)

Step3. Ii convert RGB image into gray scale

Step4. imgX creates a zero matrix of the size of original matrix

Step5. imgX2 create another zero matrix of the size of original matrix

Step6. [NoPixelnY, c] store row, column and dimension of image

Step7. for l do 1 to 4

Step8. for i do 1 to NoPixel loop through all the pixels to generate cat map

Step9. for j do 1 to nY

Step10. Imgi it get new row coordinate[(m+n) mod NoPixel]

Step11. Imgj it get new column coordinate[(m+2n) mod NoPixel]

Step12. imgX(Imgi,Imgj) it store image pixel value in new Coordinates from original coordinate

Step13. End for

Step14. End f or

Step15. for i do 1 to NoPixel

Step16. for j do 1tonY

Step17. imgXx(i,j) it adds 245 to pixel value;

Step18. End for

Step19. End for

Step20. newXx is bitxor image

Step21. I newXx replace original image with generated image

Step22. End for

Step23. Reverse steps 8 through 22 to get decrypted image

2. RESULT

The proposed encryption algorithm is implemented in MATLAB for computer simulations. The algorithm will accept and image as input data.

The below figures (1), (2), (3) and (4) represents the original image, its histogram and the encryptrd image and its histogram respecitively.

Figure 1. Original Image

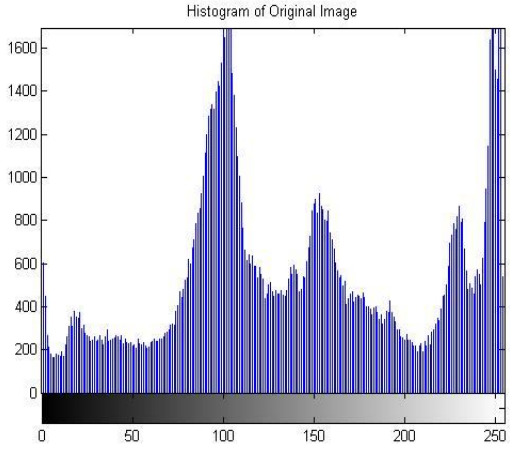

Figure 2. Histogram of original image

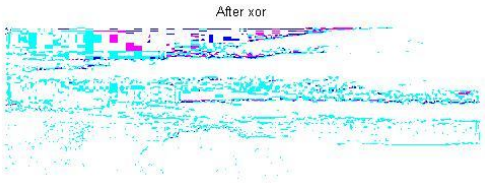

Figure 3. Encrypted Image

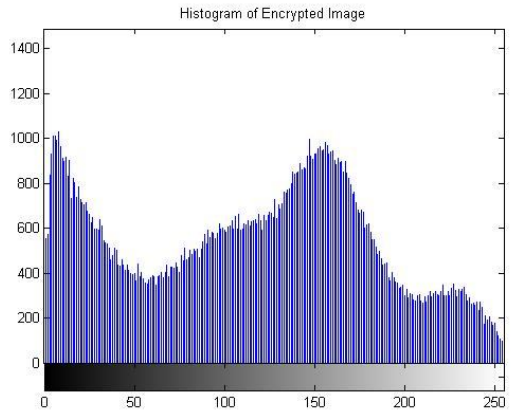

Figure 4. Histogram of encrypted image

Correlation coefficient 'r' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related. The coefficient r can be calculated by the following formula:

$$r = cov(x, y)/(D(x)\, D(y)) \qquad (2)$$

The table 1 below shows the results of correlation coefficient between two adjacent pixels.

Table 1: Correlation coefficient

Direction	Before Encryption	After encryption
Horizontal	0.9937	-0.01931
Vertical	0.9589	0.01047
Diagonal	0.9117	-0.01769

Table 1 represents the Correlation coefficient of before and after the encryption.

3. CONCLUSION

An Image encryption algorithm using Arnold Cat map is discussed in this paper. The proposed system will work efficiently for image encryption. The algorithm is based on the concept of shuffling the pixels positions and diffusion through Arnold Cat map. The scheme is more time efficient and hence effective in current scenario as compared to the previously proposed schemes. Use of multiple diffusions in the encryption scheme of the image make the cryptosystem more secure, rife and robust.

REFERENCES

1. Zhang YiWei, WANG YuMin2 & SHEN XuBang. **A Chaos-Based Image Encryption Algorithm Using Alternate Structure**, Sci China Ser F-Inf Sci, vol 50(3), pp 34-341, June 2007,
2. Huang Yuanshi, Xu Rongcong, Lin Weiqiang. **An Algorithm for JPEG Compressing with Chaotic Encrypting**, in Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation ,CGIV'06, 2006
3. Peng Fei, Shui-Sheng Qui, Long Min. **An Image Encryption Algorithm Based on Mixed Chaotic Dynamic Systems and External Keys**, in Proceedings of 2005 International Conference on Communications, Circuits and Systems,,Vol. 2, pp.11-39, 27-30 May 2005.
4. Changjiang Zhang. **Digital Image watermarking with Double Encryption by Arnold Transform and Logistic** , Fourth International conference on Networked Computing & advanced information Management, pp. 329-334, 2008
5. Nikhil Debbarma, Lalita Kumari, and Jagdish Lal Raheja. **2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation**, IJETTCS volume 2, Issue 4, August 2013.
6. Chen GR, Mao YB**. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps**. Chaos, Solitons & Fractals 2004, vol 21, pp 749–61, 2004.
7. Chiaraluce F, Ciccarelli L. **A New Chaotic Algorithm for Video Encryption**. IEEE Trans Consum Electron 2002, vol 48, pp 838–43, 2007.
8. Ogorzatek M J, Dedieu H. **Some Tools for Attacking Secure Communication Systems Employing Chaotic Carriers.** in proceedings of the 1998 IEEE Symposium on Circuits and Systems, Monterey, 1998, pp 522－525
9. Hu G J, Feng Z J, Meng R L. **Chosen Ciphertext Attack on Ohaos Communication Based on Chaotic Synchronization**. IEEE Trans Circ Syst, vol 50(20), pp 275-279, 2003.
10. William Stallings, **Cryptography and Network Security,** 4th ed. Pearson, 2006, ch. 1, pp. 18-19.