International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Chaos Based Image Encryption Technique

Jalpa Shah, J S Dhobi
Department of Computer Engineering, Government Engineering College,
Gandhinagar, Gujarat, India

ABSTRACT

Due to internet explosion there has been considerable rise in transmission of data such as tex, images, text, videos, etc over internet. Here security is required for transmission of data over internet so that data is secure from sender to receiver. Image Encryption plays an important role for image transmission over the Internet and using chaos system prove more secure than existing traditional cryptographic algorithms like AES, RC5, etc. With Image Encryption it becomes difficult to analyze the image that is communicated over untrusted network.. The paper provides an introduction to Chaos system and encryption as well decryption of images using confusion and diffusion methods achieved by arnold cat map and chen respectively. Comparison with existing algorithms is also done.

Keyword: *Internet; Image Encryption; Arnold Cat Map; Chen System; Confusion; Diffusion*

1. INTRODUCTION

Digital image processing is the use of computer algorithms to perform image processing on digital images. The input of that system is a digital image and the system process that image using efficient algorithms, and gives an image as an output.

Image Encryption is the conversion of image to unknown format using some cryptography algorithm and a key. Similarly Image Decryption is the conversion of unknown format of image to original image using the decryption algorithm. The model of Image Encryption & Image Decryption is shown in Fig 1 and Fig 2 respectively.

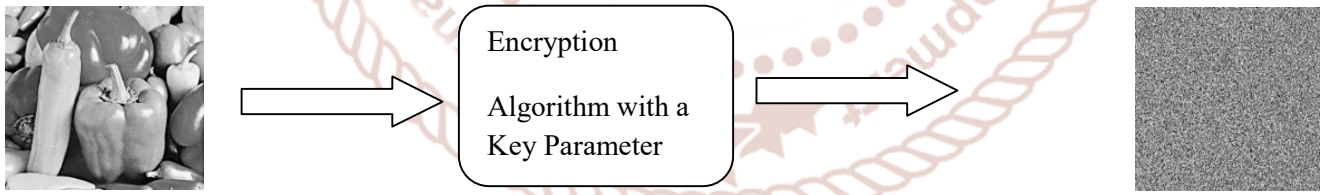

Fig 1: Model of Image Encryption (Grayscale Image)

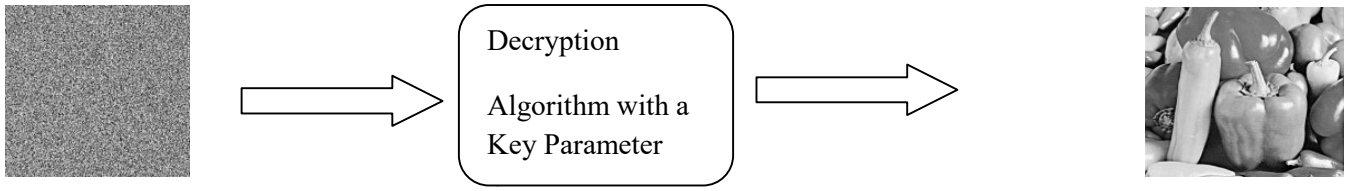

Fig 2: Model of Image Decryption (Grayscale Image)

Based on the number of keys there are 2 types of Cryptography algorithms: Secret Key Algorithm in which only 1 key parameter is used to encrypt and decrypt the data(text, video, images, etc) and Private Key Algorithm in which 2 keys are used for encryption and decryption purpose. The former is known as Symmetric Key Algorithm and latter is known as Asymmetric algorithm.

The digital images have high correlation between adjacent pixels; hence traditional cryptography algorithms cannot be used.

2. CHAOS SYSTEM

The implementation of chaotic maps in the development of cryptography systems lies in the fact that a chaotic map is characterized by: (a) the initial conditions and control parameters with high sensitivity, (b) unpredictability of the orbital evolution, (c) the simplicity of the hardware and software implementation leads to a high encryption rate. These characteristics can be connected with some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties [1].

3. LITERATURE REVIEW

Shadow number method uses 2 keys -1 as image another is derived using the equation. the method is 2D Cat Map and Shadow method for RGB image[3]. A New Fast Color Image Encryption Scheme using Chen Chaotic System is proposed in which Less no of cipher rounds. Good security & Speed performance[4]. A Chaotic Cryptosystem for Images based on Henon and Arnold Cat Map in which confusion is done by ACM and diffusion is achieved by Henon maps but other better maps could also be employed[5]. Image encryption based on Independent Component Analysis & Arnold's Cat Map in which a new method ICA is employed but 2 images are used for encryption[6]. ACM with Henon & Logistic Map for Grayscale images is done but lacks several sensitivity tests[7]. Image encryption using Camellia and Chaotic maps is done with a large key space[8]. Arnold's Cat Map algorithm in Digital Image Encryption is done but ACM has limitation that after fixed no of iterations original image is retrieved[10].

4. PROPOSED METHOD

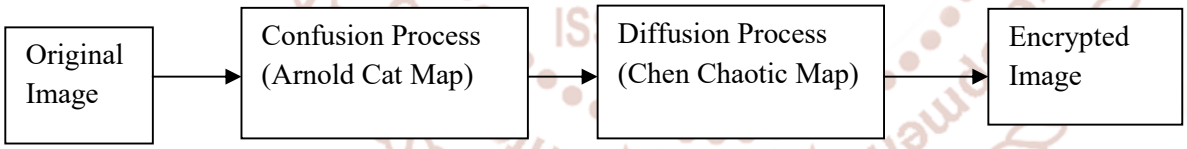

Fig 3 Proposed Image Encryption Method

Here the algorithm steps are explained as:

FOR ENCRYPTION:

(1) Original square image in jpeg format probably is grayscale
(2) The image is confused with fixed number of iterations using ACM
(3) The ACM image is diffused with key parameters of CHEN chaotic system
(3) The resultant image is the encrypted image.

FOR DECRYPTION:

(1) The encrypted image is diffused with CHEN chaotic system and same key parameters as in encryption stage.
(2) The image is confused with fixed number of iterations using ACM as encryption stage.
(3) The image is original image in grayscale.

ARNOLD CAT MAP:

This method is employed for confusion process in which pixels values are re-arranged as per the formula:

$X' = (X + Y) \bmod n$ (1)

$Y' = (X + 2*Y) \bmod n$ (2)

CHEN CHAOTIC SYSTEM:

This method is employed for diffusion process in which pixels values are changed by the chen system of equations as:

$x = a(y_0 - x_0)$
$y = (c - a)x_0 - x_0z_0 + cy_0$
$z = x_0y_0 - bz_0$

These chen system of equations are solved using the numerical method of Runge-Kutta method of order 4 which provide more security than order 3.

5. RESULT ANALYSIS

The comparison result for Cipher image with respect to Correlation coefficient is given in Fig4

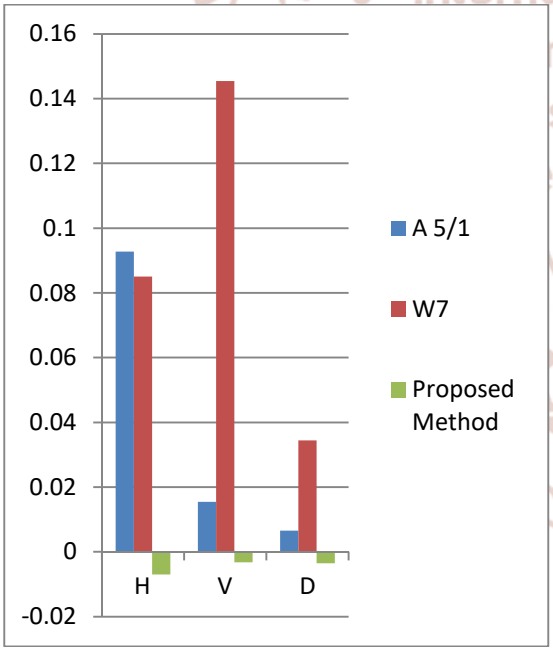

Fig 4: Comparison result for correlation coefficient

6. CONCLUSIONS & FUTURE WORK

Thus the image encryption and decryption with the help of chaos system is better than the existing traditional algorithms as the histogram depict that no difference can be found in pixel value changes. The proposed method has nearly zero coefficient in H, V and D directions than existing methods. The algorithm can be extended for color images as future work.

7. *REFERENCES*

1) Shannon, C. E. (1948). The mathematical theory of communication.The Bell System Technical Journal, 27,379–423.

2) Shannon, C. E. (1949). Communication theory of secrecy systems. The Bell System Technical Journal, 28, 656–715.

3) Nidhai K. El Abbadi, Enas Yahiya, Ahmeda Aladilee. Digital RGB Image Encryption Based on 2D Cat Map and Shadow Numbers, IEEE, 2017.

4) Chong Fu, Zhou-feng Chen, Wei Zhao, Hui-yan Jiang. A New Fast Color Image Encryption Scheme using Chen Chaotic System, IEEE, 2017.

5) Ali Soleymani, Md Jan Nordin, and Elankovan Sundararajan. A Chaotic Cryptosystem for Images based on Henon and Arnold Cat Map, The Scientific World Journal, Hindawi, 2014.

6) Nidaa Abdul Mohsin Abbas. Image encryption based on Independent Component Analysis & Arnold's Cat Map, Egyptioan Informatics Journal, ScienceDirect, 2016, Vol 17, Issue 1, pp. 139-146.

7) Hikmat N. Abdullah, Hamsa A. Abdullah. Image Encryption using Hybrid Chaotic map, IEEE, 2017, pp. 121-125.

8) Marwa S. Elpeltagy, Moataz M. Abdelwahab, Mohammed S. Sayed. Image encryption using Camellia and Chaotic maps, IEEE, 2015, pp. 209-214.

9) Minal Govind Avasare, Vishakha Vivek Kelkar. Image Encryption using chaos theory, IEEE, 2015.

10) Eko Hariyanto, Robbi Rahim. Arnold's Cat Map Algorithm in digital Image Encryption, IJSR, 2013, pp. 1363-1365.

11) Yogita Verma, Neerja Dharmale. A Survey paper based on image encryption and decryption using modified advanced encryption standard, IJSR, 2013, pp. 352-355.