Sindh Univ. Res. Jour. (Sci. Ser.) Vol.49(1) 113-118- (2017)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Chaos Image Encryption Followed By the Steganography Technique

S. BUKHARI, M. R. ANJUM, I. S. BAJWA, S. DILBAR

Department of Electronics Engineering, The Islamia University Bahawalpur, Pakistan

Received 23rd January 2016 and Revised 10th September 2016

Abstract: This paper presents the chaos image encryption technique which is followed by the image steganography. The first layer of this proposed technique is to encrypt the grey scale image by the chaotic map which produce randomizations in the original image and make it secure against any forgery attacks. In this technique the performance of two chaotic maps (bakers map and Arnold cat map) are evaluated and the best evaluated chaotic map (Arnold cat map) is used in the proposed technique. The second layer takes the encrypted image and hides it inside another image (cover image) by the image steganography technique and in the result stego image is formed. Stego image hide the secret information from the eavesdroppers and show only the cover image which is common to all. Matlab simulations and analysis tests like contrast, correlation, homogeneity, histogram analysis and energy that has been performed on the proposed technique to evaluate its strength reveals that the proposed method is resistant against attacks of transmission of images in communication systems.

Keywords: Image encryption, Bakers map, Arnold cat map, Steganography technique

1. INTRODUCTION

As we moves towards the modernization of technology there is more advancement in transferring of data from one place to another. To keep our data safe from attackers while transmitting through communication channels, the need for the security increases. There are many threats faced in communication systems like fabrication: middle person (attacker) makes the false information and sends it to the intended person, interruption: the information is not access to the intentional receiver, modification: the confidential data is eavesdrop by the attacker which send the data to the recipients by changing it and interception: in this the confidential data is not only received by the intentional receiver but invader also receive it. In communication systems the privacy of data becomes a supreme need (Abbas, and Mohsin. 2016). (Gautam, *et al.,* 2011). From the old times the cautious writing is a unique field. The study of this unique field in secretly writing or modify the transmitted data in that way which is not understandable by the forger is called the cryptography. In the beginning many raw cryptography techniques were used which not fully covered or hide contents of message in public channels. The good cryptographic system has two major properties first to keep the data private from eavesdropping and second is to prevent the data from spoofing. Cryptography is consisting of encryption part and the decryption part. Encryption process is done at the transmitter side and the decryption process is carried out at the receiver side. In encryption process the plain data or information is encoded by encryption algorithm and key. The encoded data is called the ciphered or encrypted data. The strength of the encrypted data is depending on the length of the key and only that person gets the original data who knows about the key. The encryption algorithm mainly has two types which is based on key first is symmetric enciphering in which the key is kept secret and same key is used for encryption and decryption processes. Symmetric encryption is used when heavy or large amount of data is needed to send. It is further divided into block ciphers and stream ciphers. The second type of encryption algorithm is asymmetric encryption algorithm in which two keys are used one is public and another is private. In asymmetric algorithm the public key is used to encode the plain text and private key is used for decryption process. To get the plain text back at the receiver side decryption process is required which is opposite to the encryption process. In decryption process the key is required. There are many cryptography algorithms are used such as double random phase encoding, vector quantization, watermarking, digital signatures techniques, substitution methods, AES algorithm, DES algorithm, transformation techniques and chaotic maps. Chaotic maps are used to provide more security in modern cryptography systems. They create chaos in the plain data. In this paper two chaotic maps are compared first is the Bakers map and second is the Arnold cat map which is used to provide security at the beginning of the proposed encryption algorithm (Abd-El-Hafiz, *et al.,* (2014).

++Corresponding author:Email:sadafbukhari02@hotmail.com, imran.bajwa@iub.edu.pk,

*Department of Computer Science & IT, The Islamia University Bahawalpur, Pakistan

Depend on the type of multimedia data there are three types of enciphering algorithms; audio encryption algorithm, video encryption algorithm and image encryption algorithm. The image encryption algorithm is subpart of the image processing. Image processing has much importance in medical, science, military, remote sensing application and research. In image processing many processes like filtration, compression, decompression, removal of blurriness, orientation and coding etc. are performed on the images. Image is actually a matrix with two or three dimensions like grey scale image and RGB image respectively. The entries of matrix are called pixels which gives the intensities of the colors. Another technique which provides high level of security is the Image steganography. In this technique the message image is hiding inside the cover image. The embedded image is called the stego image. During transmission there is no difference found in stego image and the cover image. Large amount of data can be transmitted by the properly implemented steganography technique by making no change in file components (Abuhaiba, *et al.,* 2012). In this paper first we compare the two chaotic maps (bakers map and Arnold cat map) and evaluate its performances by statistical tests then use the best evaluated chaotic map in proposed encryption technique as a pre-processing layer for encryption of image. In second part of the proposed technique image steganography (least significant bit) is performed on the encrypted image.

The scheme of the remaining paper is presented as section II presents the bakers map, section III presents the Arnold cat map, section IV presents the image steganography, section V explains the proposed technique methodology, section VI discuss the experimental results and outcomes and section VII present the conclusion.

2. BAKER'S MAP

In image processing; encryption process, study of dynamic systems and in the communication theory the chaotic baker's map plays an important role. It works in real space domain. In image encryption process it creates randomization in image pixels position by permutation. It separately works on x component and y component of the image pixels positions by changing the position of one pixel by another pixel position. It means that baker's map does not transform the pixel values but provide mapping in square matrix with the help of secret key. The discretized baker map is formulated as;

$$D(m_1,\ldots\ldots m_n)(k,r) = \left[\frac{B}{u_i}\left(k - B_i + rmod\,\frac{B}{u_i}\,,\ \frac{u_i}{B}\left(r - rmod\,\frac{B}{u_i}\right) + \ B_i\right)\right] \qquad (1)$$

Where B is the number of elements in square matrix B×B , $u_1,u_2,\ldots..u_n$ is sequence of n integers, u_i divides the B, (k,r) is the pixel indices and $B_i= u_1+\ldots\ldots u_i$. The stages of the above baker's map formula is describe as in the first stage the square matrix B×B is divided in to blocks according to the key and each block contains equal number of elements. In second stage the permutation process is carried out from right upper block to the left. In this stage the elements in the block are rearranged in rows which form the permuted matrix. The strength of the Baker's map depend on the key length if there is creativity in key arrangement then the Baker's map will easily be suspect able. In this paper we use [100 100 100] key for the message image.

3. ARNOLD CAT MAP

Russian mathematician Vladimir I discovered the Arnold cat map chaotic algorithm. The algorithm named is cat map because he used the cat image for encryption. In cat map, the position of the pixels of image is rearranged according to the transformation matrix whose determinant is unity and due to the use of the matrix with determinant 1 it is reversible at receiver side for decryption process. Cat map which is 2D transformation map creates ergodicity in the encrypted image. It formulates as

$$\begin{bmatrix} x_{i+1} \\ y_{j+1} \end{bmatrix} = \begin{bmatrix} 1 & C \\ D & DC+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_j \end{bmatrix} \qquad (2)$$

Where C and D are constant positive integer, (x_i,y_i) are real image pixel position and (x_{i+1},y_{j+1}) is the new mapped positions of pixels. The two parameters C, D and iteration number are needed to be kept secret for the secure encryption. The rearranged pixels are comes back to their original positions after some iterations so that's why Arnold cat map algorithm is not used alone for encryption processes. In this paper we use C=10 and D=8 and 7 iterations for Arnold cat map.

4. IMAGE STEGANOGRAPHY

Steganography is a word derived from Greek language means secret writing. Steganography techniques depend upon the type of multimedia data like audio steganography, video steganography and image steganography. The data use in this technique must be in serial format so that each bit certainly hides inside the cover image. Image steganography is a hiding technique in which the two images are used. The first is the message image and other is the cover image. The message image is a confidential image which needs to be hiding in the cover image that is common to all. The choice of cover image has much importance in steganography technique. The cover image may be any image but the more variety of color images is more secure than the single color images. The size of the cover image and the message image must be same. The embedding in single color image can certainly noticeable. After hiding the message image in cover image a resultant image is formed that is called stego image. Stego image is seen like a cover image on the public channel and no one can find the difference between stego image and the cover image. To break the stego image through information is difficult. In this paper we use the least significant bit (LSB) steganography method to embed secret information in the cover image. LSB is very simple spatial domain technique of steganography. It is most commonly used technique because of its effectiveness and simplicity. It uses the least significant bit(s). LSB embedding method is different from the other embedding method which causes variations in colors of image while the LSB reduce this effect. In LSB method the message image is embeds in the least significant bits of the cover.

5. PROPOSED METHODOLOGY

The technique is proposed for the encryption of the image that makes the transferring of image secure in insecure channel. To create confusion and diffusion chaotic maps is used in the proposed method. Before proposing the technique two chaotic maps (Baker's map and Arnold cat map) are evaluated by the statistical tests. Statistical tests have shown that the Arnold cat map creates more chaos in the encryption image than the bakers map. Then the proposed method's first layer use chaotic Arnold cat map to encrypt the message image with the help of its secret parameters C and D. As it is not appropriate to use unaccompanied for the encryption process because after some iteration it gives backs the image. So in the second layer the encrypted image is embedding by the LSB steganography technique. LSB embedding method generates the stego image by hiding the message encoded image in the least significant bits of the cover image. The figure: 2 show the plane image which is used as the message image and the camera man image which used as the cover image in proposed technique

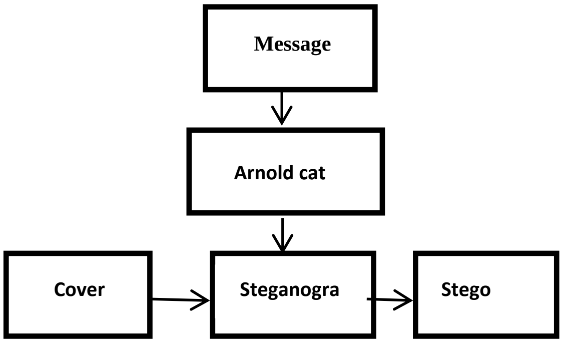


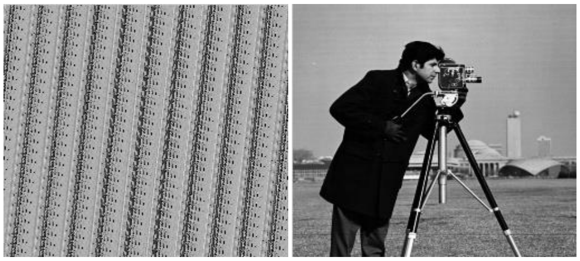
Fig-1: Proposed Image Encryption Technique

(a) (b)

Fig-2: a) Message image, b) Cover image

6. OUTCOMES AND RESULTS

Matlab implementation of proposed technique has shown the visual results and also the tabulated values of statistical analysis tests. Figure:3 depicts the outcomes of proposed image encryption technique first is the encrypted image by the Arnold cat map and second is the stego image that hide the encrypted image. Statistical analysis tests are used to check the performance or strength of the proposed technique. In this paper following tests like contrast, correlation, energy, and homogeneity and histogram analysis are performed on the baker's map image, Arnold map image and on the stego image. With the help of these statistical tests, proposed technique use the Arnold cat map chaotic algorithm for image encryption. The above mentioned statistical tests results are tabulated in below following tables.



(a) (b)

Fig-3: a) Arnold cat map image, b) Stego image

A. *Contrast*

In image processing brightness and contrast of the image is properly adjusted for easily viewing. Contrast is defined as the difference in the objects brightness. In encryption process the contrast value is directly proportion to the randomness of the image. The more the value of the contrast the more confusion and randomness is present it he encrypted image. In contrast analysis intensity is measured between the pixels and its adjacent pixel of the whole encoded image. Constant image has zero contrast value and its range is between zero and square of grey level co-occurrence matrix. It is formulated as

$$\boldsymbol{C} = \sum_{\boldsymbol{k},\boldsymbol{r}}^{\boldsymbol{n-1},\boldsymbol{m-1}} |\boldsymbol{k}-\boldsymbol{r}|^{2}\boldsymbol{P}(\boldsymbol{k},\boldsymbol{r})$$

Where P (k,r) represents number of grey level co-occurrence matrices. **(Table-1)** shows the contrast analysis of message image, baker's map and Arnold cat map image. From the table it is clear that the contrast value of Arnold cat map is higher than the baker's map contrast value.

Table-1: Contrast analysis of message image, baker's map encrypted image and arnold cat map encrypted image

Message Image	*Baker's map image*	*Arnold cat map image*
0.2688	**0.1746**	**3.6119**

a. Correlation

Correlation analysis measures the closeness of pixel values to its neighbor values. It gives the linear relationship between two pixel values of image. In image processing it is closely related to the convolution. Correlation is measured in vertical, horizontal, diagonal formats. Its range is between -1 and 1. If the value of the correlation is +1 then the image is positively correlated and if it is -1 then the image is negatively correlated. In encryption term it is defined as the less correlated the encrypted image, the more robust the image in insecure channel transmission. The mathematical formula of correlation analysis is as follows

$$\mathbf{K} = \sum_{\mathbf{k,r}} \frac{(\mathbf{k} - \boldsymbol{\mu}\mathbf{k})(\mathbf{r} - \boldsymbol{\mu}\mathbf{r})\mathbf{p}(\mathbf{k},\mathbf{r})}{\boldsymbol{\sigma}_{\mathbf{k}}\boldsymbol{\sigma}_{\mathbf{r}}}$$

Table-2: shows the correlation analysis between the message image, baker's map image and Arnold cat map image. From the table it is clear that Arnold cat map is better chaotic map than the baker's map because it has less value of correlation than the baker's map.

Table-2: Correlation analysis of message image, baker's map encrypted image and Arnold cat map encrypted image

Message Image	*Baker's map image*	*Arnold cat map image*
0.9393	**0.9305**	**0.1826**

b. Homogeneity

In homogeneity analysis, the familiarity of the distribution of components of gray level co-occurrence and diagonal grey level co-occurrence is measured. Its range is between zero and one. In encryption process the homogeneity value is small which reveals the robustness of the encryption algorithm. Homogeneity analysis mathematically defined as

$$\boldsymbol{M} = \sum_{\boldsymbol{k,r}} \frac{\boldsymbol{p(k,r)}}{\boldsymbol{1 + |k - r|}}$$

Table-3 shows the homogeneity analysis between the message image, baker's map image and Arnold cat map image. The below table shows that the Arnold cat map image has lesser value of homogeneity than the original image and the baker's map image which shows the strength of Arnold cat map against the baker's map.

Table-3: Homogeniety analysis of message image, baker's map encrypted image and Arnold cat map encrypted image

Message Image	*Baker's map image*	*Arnold cat map image*
0.9277	**0.9275**	**0.6232**

c. Energy

In energy analysis the sum of the squared elements of grey level co-occurrence is measured. The energy of the encrypted image is small as compared to the original message image. The energy analysis is mathematically define as

$$\boldsymbol{E} = \sum_{\boldsymbol{k,r}} \boldsymbol{p(k,r)^2}$$

Table-4 shows the energy analysis between the message image, baker's map image and Arnold cat map image. It is also clear from the below table that the encrypted image by the cat map has lesser energy value than the baker's map.

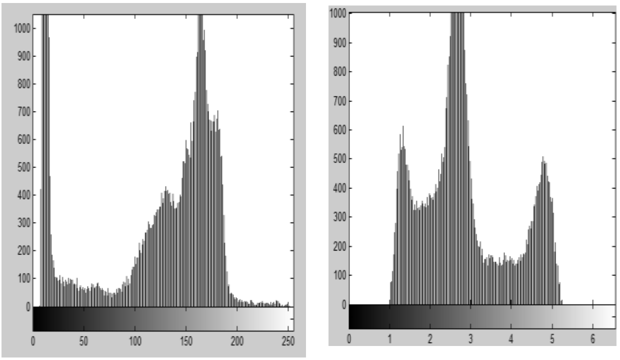
Table-4:Energy analysis of message image, baker's map encrypted image and Arnold cat map encrypted image

Message Image	*Baker's map image*	*Arnold cat map image*
0.2856	**0.2844**	**0.1339**

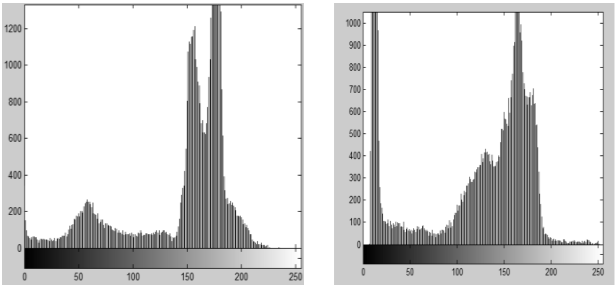
d. Histogram Analysis

In histogram analysis the distribution of intensities of the color values of pixel is illustrated. It is used to find the difference between intensities of colors between enciphered and ciphered image. It is mathematically defined as

$$\boldsymbol{Y^2} = \sum_{\boldsymbol{f=1}}^{\boldsymbol{T}} \frac{\boldsymbol{(Q_i - W_i)^2}}{\boldsymbol{W_i}}$$



a) b)



c) d)

Fig-4: a Histogram of Message image, b) Histogram of cover image, c) Histogram of Arnold cat map image, d)histogram of Stego image

Above figure depicts the histogram analysis of proposed technique. It depicts the histogram of message image, cover image, Arnold cat map encrypted image and the stego image. The histogram of message image is different from the encrypted image histogram while the similarity is found in the cover image histogram and stego image histogram. No one can find the difference between stego image and the cover image. In that way steganography gives high level of security to image in transmission medium.

7. CONCLUSION

It is concluded that the image encryption technique proposed in this paper have immunity against the security threats in public channel. The proposed technique is consisting of chaotic map and the steganography technique. The chaotic map used for the encryption of image is Arnold cat map which is evaluated as highly secure map than the bakers map by statistical analysis tests. The chaotic map is used to create confusion in the image in the beginning of the technique then the encrypted image is hiding inside the cover image by the steganography technique. The steganography technique makes the proposed technique more strong than the other security techniques. From the proposed technique the main difference between the image steganography and cryptography is also cleared that the encryption method can hide the contents of message image while steganography technique hides the presence of message image.

REFERENCES:

Abbas, N., A. Mohsin. (2016). "Image encryption based on Independent Component Analysis and Arnold's Cat Map." Egyptian Informatics Journal 17, no. 1: 139-146.

Abuhaiba, I., S. I. Amina Y. AlSallut, H. Hejazi, H. A. AbuGhali, (2012). "Cryptography Using Multiple Two-Dimensional Chaotic Maps." International Journal of Computer Network and Information Security 4, no. 8: 1.

Abd-El-Hafiz, S. Kamal, A. G. Radwan, H. Sherif . A. Haleem, and M. L. Barakat, (2014). "A fractal-based image encryption system." IET Image Processing 8, no. 12: 742-752.

Al-Shakarchy, N., D. Kadhm, H. J. Al-Eqabie, H. F. Al-Shahad. (2014). "Classical Image Encryption and Decryption."

Celik, M. U., G. Sharma, A. M. Tekalp, and E. Saber. (2005): "Lossless generalized-LSB data embedding." IEEE transactions on image processing 14, no. 2 253-266.

Fridrich, J., (1998) "Image watermarking for tamper detection." In Image Processing, 1998. ICIP 98. Proceedings. International Conference on, vol. 2, 404-408. IEEE,.

Gautam, A., M. Panwar, and P. R. Gupta (2011). "A new image encryption approach using block based transformation algorithm." IJAEST) International Journal of Advanced Engineering Sciences And Technologies 8: 090-096.

Ker, A. D. (2005): "Steganalysis of LSB matching in grayscale images." IEEE signal processing letters 12, no. 6 441-444.

Lian, S., (2008). Multimedia content encryption: techniques and applications. CRC press.

Li, Y., K. Kreske, and J. Rosen, (2000) "Security and Encryption Optical Systems Based on a Correlator with Significant Output Images," Appl. Opt., vol. 39, 5295-5301.

Soleymani, A., M. J. Nordin, and E. Sundararajan, (2014). "A chaotic cryptosystem for images based on Henon and Arnold cat map." The Scientific World Journal.

Sturman, R., J. M. Ottino, S. Wiggins, (2006). The mathematical foundations of mixing: the linked twist map as a paradigm in applications: micro to macro, fluids to solids. Vol. 22. Cambridge University Press.

Wang, B., Y. Xie, C. Zhou, S. Zhou, and X. Zheng. (2016): "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps." Optik-International Journal for Light and Electron Optics 127, no. 7 3541-3545.

Wang, P. K., L. A. Watson, and C. Chatwin, (1996) "Random phase encoding for optical security," Opt. Eng., vol. 35, 2464-2469.

Zhang, T., A. El-Fatyany, M. Amin, and A. Ahmed Abd El-Latif. (2015): "Secret Sharing-Based Chaotic Image Encryption." International Journal of Security and Its Applications 9, no. 7 217-224.