Journal of Engineering and Applied Sciences 13 (Special Issue 7): 5490-5497, 2018
ISSN: 1816-949X

Chaos-Based Image Encryption Methods: A Survey Study

[1]Sabah Fadhel, [1, 2]Mohd Shafry Mohd Rahim and [1]Omar Farook Mohammad
[1]Faculty of Computing, University Teknologi Malaysia (UTM),
[2]IRDA Digital Media Center, Institute of High Current Electronics (IHCE),
University Teknologi Malaysia (UTM), Skudai, Johor, Malaysia

Abstract: With increasing dependence on communications over internet and networks, secure data transmission is coming under threat. One of the best solutions to ensure secure data transmissions is encryption. Multiple forms of data such as text, audio, image and video can be digitally transmitted. Of these, images are the most popular and old encryption techniques such as AES, DES, RSA, etc., shows low security level when used for image encryption. This problem was resolved by using chaos encryption which is an acceptable form of encryption for image data. The sensitivity to initial conditions and control parameters make chaos encryption suitable for image applications. This study discussed and analyzed several chaotic-based image encryption methods and found that changing both the location and value of the image pixels is very important to resist statistical analysis while the use of multi chaotic map leads to increase the key space size, making brute force attack infeasible.

Key words: Chaos, initial conditions, control parameters, map, permutation, chaotic-based

INTRODUCTION

Multimedia technology, especially image technology is currently undergoing rapid change and growth (Bashardoost *et al*., 2014) due to increased adoption of internet and communications (Sankpal and Vijaya, 2014; Sharifara *et al*., 2013). The demand to transfer these images in a secure manner has also increased and encryption is the preferred method to transfer image data. Current encryption techniques such as AES, DES and RSA are unsuitable for image data encrypting and cannot guarantee data confidentiality and security (Jolfaei and Mirghadri, 2010) because of the size and redundancy of images (Wang *et al*., 2012; Chen *et al*., 2013; Coppersmith, 1994). Over the last couple of decades numerous techniques have been proposed for encrypting image data of which chaos based encryption has been proven to be the most effective (Jain, 2016). Chaos theory was first proposed in the 1970's for use in physics, mathematics, biology and engineering. It would not be until the 1980's that chaos theory was found to have cryptographic applications (Liu *et al*., 2009). Chaos based encryption methods are popular due to their randomness, unpredictability, sensitivity and topological transitivity (Alsafasfeh and Arfoa, 2011). The properties of chaotic systems met most of the cryptographic system properties (Gao *et al*., 2006). After chaotic encryption algorithm was proposed in 1989 (Li *et al*., 2002) the researches of chaotic-based image encryption methods has been increasing dramatically (Gao *et al*., 2006; Zhang, 2014).

This study deals with the chaotic-based image encryption systems and shows the principles and properties of chaotic systems with illustration of the differences and similarities between chaotic systems and cryptography algorithm. This study provides an illustration of the general scheme of chaotic-based image encryption. Several chaotic-based image encryption methods and ten of the most important image encryption analysis methods are also discussed.

Chaos theory: A dynamic, chaotic system is any deterministic system that is both highly random and sensitive to initial conditions (Sankpal and Vijaya, 2014). Chaotic systems are similar to noisy systems because both are highly unpredictable because they are pseudorandom, unpredictable and sensitive to initial condition (starting point) and control parameters (Nesakumari and Maruthuperumal, 2012; Shuangshuang and Min, 2014). Therefore, chaotic systems have uses in cryptography (Sankpal and Vijaya, 2014). Chaotic systems are useful for encryption because they appear to be random data and their sensitivity to initial conditions allows for this randomness to be unpredicted, allowing a basis for decryption (Maadeed *et al*., 2012). The main difference between chaos maps and chaos cryptography

Corresponding Author: Sabah Fadhel, Faculty of Computing, University Teknologi Malaysia (UTM), Skudai, Johor, Malaysia

Table 1: The differences and similarities between chaotic system and cryptography algorithm

Chaotic system	Cryptography algorithm
Sensitive to the initial conditions and control parameters	Diffusion
Iterations	Rounds
Parameters	Key
Set of real numbers	Finite set of integer numbers

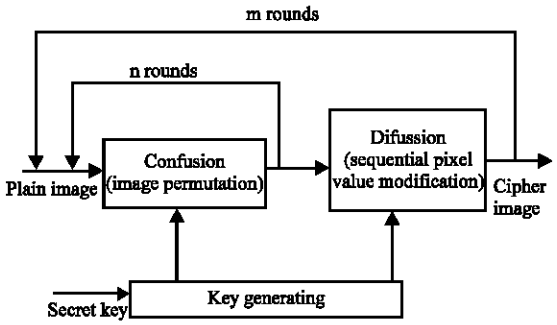

Fig. 1: A chaos-based image encryption general scheme

is that chaos cryptography is defined by finite sets while chaos maps are defined by real numbers as shown in Table 1 (Sankpal and Vijaya, 2014). Each chaos map has its own parameters and encryption key. Chaos maps can be applied using chaotic systems to generate a pseudorandom key or the generation from a key or plain text. Generation from a pseudorandom key produces a stream cipher and generation from plain text produces a block cipher (Soleymani *et al*., 2012).

Chaos-based general image encryption scheme: Many data encryption methods use chaotic maps (Habutsu *et al*., 1991; Pichler and Scharinger, 1995; Masuda and Aihar, 2002; Yen and Guo, 2000a; Yen and Guo, 2000b; Chen *et al*., 2004; Lian *et al*., 2005) because it is widely applicable and easy to understand. Chaotic based image encryption occurs in two stages, confusion and diffusion. Figure 1 shows the general chaos-based image encryption scheme (Sankpal and Vijaya, 2014).

In the confusion stage, an image's pixels are scrambled using a secret key based upon control parameters while in the diffusion stage, pixel values are changed using chaotically generated sequences. Both of these methods make chaotic encryption highly secure (Sankaran and karishna, 2011). Figure 1 shows the chaotic encryption process.

MATERIALS AND MATHODS

Different chaos-based encryption methods: Dong *et al*. (2010) proposed an image-scrambling algorithm that made use of chaotic mapping by engaging each pair of pixels in an image with counterparts in the same image. Pixels are exchanged using a scrambling matrix that is generated from logistic map principles. The proposed algorithm uses the chaotic principle to change the pixels position to reduce the correlation between adjacent pixels and this goal is achieved by exploiting the characteristics of logistic chaotic system in terms of the sensitivity to initial condition and control parameters in addition to the pseudo-randomness features. In this study, a random key series is generated based on logistic map. The key series is converted into a two dimensional random matrix and then this matrix is used to control the process of the swapping of the plain image's pixels. The proposed method is not considered the diffusion process, so, the evaluation results are expected to show good correlation results between adjacent pixels while the histogram is still the same for plain image. The key space of proposed algorithm does not satisfy the security requirement because it is smaller than the acceptable one. Therefore, the transmission of ciphered image will be threatened by brute force attack. Table 2 shows the expected results of the proposed method.

In the algorithm proposed by Alsafasfeh and Arfoa (2011) both a Rossler chaotic system and a Lorenz chaotic system are used for encryption. The use of two or more chaotic systems in an algorithm is highly unusual. Long-term chaotic behavior is periodic and dependent on initial variables (Wang *et al*., 2008). Both Rossler and Lorenz schemes depend on three variables thus, increasing the security of proposed chaotic system. This is because the total number of parameters depends on six variables, making it highly secure. This algorithm changes the image grayscale values for a set number of iterations before storing the randomized image data in a chaotic matrix the same size as the original image. XOR operations are used for both encryption and decryption. The key space of the proposed algorithm is good in terms of increasing the total number of initial values to six instead of three for each one of the used chaotic systems. In addition because the proposed method uses XOR operation between plain image and the random one without make any permutations to the image's pixels, the expected correlation value between the adjacent pixels of the encrypted image will be moderate as shown in Table 2.

Alfy and Al-Utaibi (2011) proposed an encryption method for colored images using a genetic operator and a chaotic map to minimize the correlation coefficient of adjacent pixels. The proposed algorithm has four steps. First, a logistical map is used to generate four different chaotic sequences by using four control parameters and four initial values to act as shared keys for the encryption

Table 2: The expected results of the discussed methods

Methods	Histogram analysis	Correlation results	Key space size
Gao *et al.* (2006)	Low	Good	Low
Dong *et al.* (2010)	Good	Moderate	Good
wang *et al.* (2008)	Good	Good	Good
Alfy and Utaibi (2011)	Good	Good	Good
Sharifara *et al.* (2013)	Good	Good	Good
Gao *et al.* (2006)	Low	Good	Moderate
Liu and Tian (2012)	Good	Good	Good
Abdulgader *et al.* (2015)	Low	Good	Low
Abdulgader *et al.* (2015)	Good	Good	Good

process. Second, quantification which is used to map the four sequences into key streams for use in the remaining phases. Third, a crossover is used to confuse the image row-by-row and column-by-column. Fourth, a mutation phase is used to implement XOR operator between the intermediate images (resulted from crossover stage) and random image. The implementation of the proposed method is done by the following process.

Four, logistic maps are used to generate four chaotic sequences and then these four generated sequences will be divided into two groups. The first of these two groups consists of first and second chaotic sequences (S1 and S2) while the second group consists of third and fourth sequences (S3 and S4). The first group sequences are used in pixel permutation process (confusion stage) and the second group sequences are used in the altering of image pixel values (diffusion stage).

The quantification unit that has been proposed in this study is responsible for generating digital random values based on real-valued sequences that have been generated by the four chaotic maps. In crossover unit, a process of pixel permutation or image confusion is done. As mentioned earlier, the first group of chaotic sequences has been used to achieve this goal and the process of image pixels permutation is performed row-by-row and column by column. The last unit of the proposed method is the mutation unit and in this unit, the second group of the generated chaotic sequences is used. XOR operation is implemented between the intermediate (confused) image and the generated pseudo-random matrix. The expected performance of this method is a good result in key space (because of the use of four initial values and four control parameters of the four used logistic maps). The correlation between adjacent pixels is expected to be at minimum value as shown in Table 2.

New image encryption scheme based on one of three chaotic systems was proposed by (Sankaran and Krishna, 2011) to shuffle the positions of image's pixels by selecting a chaotic system based on a 16- byte key length. Another chaotic system is used to create a chaotic map to disturb the relationship between the encrypted image and the plain image. The main goal of this study is to increase the security by increasing of the key space size. The expected results for this study is good in terms of key space as seen in Table 2.

A new image encryption scheme was proposed by Jolfaei and Mirghadri (2010) using a combination of W7 and pixel shuffling. A chaotic Henon map is used to generate a permutation matrix using W7 as a secret key and for initial conditions. Pixel shuffling was achieved using horizontal and vertical permutations. As a synchronous symmetric (W7) stream cipher was used, the proposed system is very suitable for use in hardware implementations at very high data rates such as GSM security. W7 supports 128-bit key length and consists of the function unit that is responsible for the generating of key stream. The proposed method used the key stream that is resulted from the implementation of chaotic map in the pixel permutation (confusion) stage while the key stream generated by W7 is used in the process of diffusion stage. Because of the use of W7 that supports 128-bit key space length in addition to the use of chaotic map, the proposed method is expected to achieve good security level as seen in Table 2.

Liu and Tian (2012) proposed a colored image encryption algorithm based on chaotic map and Spatial Bit-Level Permutations (SBLP). Image pixel positions were shuffled using a sequence generated from using two chaotic logistical maps before the shuffled image is transformed into binary matrix. A permutation of the binary matrix is created by scrambling the map generated from the (SBLP) process. A second sequence was generated from a chaotic logistical map to rearrange the pixel positions of the new images. The proposed scheme deals with the bit-level of image pixels and the random sequences generated by the implementation of two logistic maps that are used in both confusion diffusion processes. First, step in the proposed method is the generation of the two random sequences using two initial conditions and two control parameters. The first of these generated sequences is used to permute the image pixels. The permutation is done by converting the image from two-dimensional matrix into one dimension array and rearranging this array according to the randomness order of the random sequence. The resulted array will be analyzed into bit-level matrix (each element in this array will be analyzed into its bits component). The second chaotic sequence resulted from using the second initial condition and second control parameter will be used in the permutation process of bit-level matrix element. As shows in Table 2 because the analysis achieved by this survey study (SBLP) method is weak in image encryption security criteria, the expected histogram will not be close to uniform one.

Abdulgader *et al*. (2015) proposed an enhancement of Advanced Encryption Standard (AES). The proposed method is an attempt to make AES method useful in image encryption field. It is well known that AES has many drawbacks when implemented in image encryption field such as high computational costs, predictable patterns and fixed S-box weak points. To overcome the problem of high computation process of MixColumn transforms, the proposed method reduces the high computations by replacing the stage of MixColumn in AES algorithm with chaotic map and XOR operation. The proposed method succeeds in reducing the computational process and makes the amended AES adaptive for the encryption of large image data. The expected results of this method will show good criteria as seen in Table 2.

To reduce the complexity of image encryption (Jain *et al*., 2016) proposed a simple image encryption method based on Dual-Tree Complex Wavelet Transformations (DT-CWT). First stage in this scheme is to transform plain image using wavelet transformation, then a pixel chaotic scrambling is used for approximation and an arnold transformation is used for the details. The suggested image encryption method is simple method and it expects to achieve good results in adjacent pixels correlation as seen in Table 2.

An algorithm for generating random bit sequences based on chaotic maps was proposed by Khanzadi *et al*. (2014). This algorithm uses random bit sequence generated from tent and chaotic logistic maps. The permutation of plain image pixels was done by these chaotic functions, after which the image was divided into 8-bit map planes. Bits were replaced by other bit values according to a chaotic ergodic matrix. The proposed algorithm consists of stages which are pixel permutation, pixel decomposition, bitmap permutation, bitmap substitution and bitmap composition. The expected correlation results for the proposed method is good as shown in Table 2.

In Table 2, the expected results for the discussed encryption methods are stated according to the technique used in each of these methods. High indicates the desired result while low indicates the drawbacks of the encryption method. Table 2 is representing the expectation of the author of this study and not all the results that are stated in the reference studys are considered.

Performance analysis of chaotic cryptography systems: After Pecora and Carroll (1990) discovered synchronization in chaotic systems in chaotic dynamics has received significant attention due to its use in securing communications (Alvarez and Li, 2006; Guzman *et al*., 2008, 2009). Chaotic signal encoding was first used in 1990 (Hernandez *et al*., 2005). Researchers in the field of cryptography give special attention on how to analyze the security of image encryption methods. Several methods are used to evaluate image encryption systems and the following is an explanation of these methods.

RESULTS AND DISCUSSION

Random number generation analysis: To analyze the randomness for the generated number 15 different tests were developed and these tests were included in a package called NIST test suite. This tool has the ability to test random keys produced either from physical or logical generator and it can test random keys of arbitrary length. These tests are based on several different types of non-randomness that can occur in the generated key sequences. These tests are listed as follows:

- The frequency (monobit) test
- Frequency test within a block
- The runs test
- Tests for the longest-run-of-ones in a block
- The binary matrix rank test
- The discrete fourier transform (spectral) test
- The non-overlapping template matching test
- The overlapping template matching test
- Maurer's "Universal statistical" test
- The linear complexity test
- The serial test
- The approximate entropy test
- The cumulative sums (cusums) test
- The random excursions test
- The random excursions variant test

Key space analysis: Key space is the number of attempts necessary to guess a correct decryption key. Strong encryption should have an encryption key No. $<2^{100}$ (Pareek, 2012) with the exponent indicating the number of bits in a key. Large encryption keys provide greater security against brute force attacks (Sankpal and Vijaya, 2014).

Key sensitivity analysis: The use of a secret key for encryption produces strong encryption as any change in the secret key produces another encrypted image. Secure image cryptosystems makes use of secret keys to evaluate the robustness of an encryption scheme. In a cryptosystem an image cannot be decrypted if there is any difference between the encryption and decryption keys (Aissa *et al*., 2013). In a strong encryption algorithm, key sensitivity should be >50% (Mahmood *et al*., 2016).

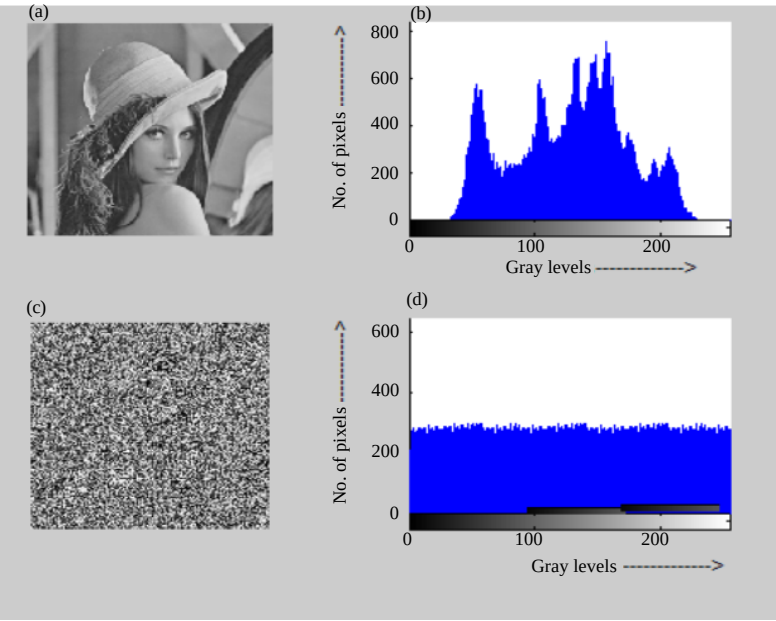

Fig. 2: Images and their corresponding histograms; a) Pain image; b) Encrypted image; c) Decrypted image; e) Histogram of plain image and f) Histogram of decrypted image

Image histogram analysis: Image histogram is the description of occurrence frequency for each pixel value in an image. The histogram of the encrypted image must be fully statistically different from the histogram of plain image and it should be uniform to avoid statistical histogram attack (Jain *et al*., 2016). In image histogram plot each bar represents specific number of occurrence for the corresponding pixel value where in 8-bit grayscale images, the pixels value are arranged from 0 (which represents black pixel) and 255 (which represents white pixel) (Kamali *et al*., 2010) as explained in Fig. 2.

Image entropy analysis: Entropy is used to measure uncertain associations between random variables (Salameh and Karak, 2016). A grayscale image has a theoretical entropy value of 8 Sh or bits. Image encryption algorithms should produce an encrypted image with an entropy value similar to grayscale values (Sivakumar and Venkatesan, 2016). The information entropy can be calculated based on Eq. 1:

$$H(m)=\sum_{i=0}^{M-1}P(m_i)\log_2\frac{1}{P(m_i)} \quad (1)$$

Where:

M = The total number of pixels

m_i = The symbolizes the possibility of occurrence of symbol m_i

log = Denotes the base 2 logarithm so that the entropy is expressed in binary mode

The amount of information entropy in a perfect random image is 8. Cipher image entropy close to 8 indicates that the cipher images are close to random and the used algorithm is secure against the entropy-based attack.

Correlation between adjacent pixels: It is well known that the most successful attacks of an encrypted image are the statistical-based attacks. Thus, to encrypt images securely, the encrypted image must resist statistical attacks. To ensure that the used encryption method delivers strong performance against statistical attacks, a correlation between horizontal, vertical and diagonal must be calculated for adjacent pixels in both of plain and encrypted images (Su *et al*., 2017). To verify the robustness against statistical correlation attack for the proposed image encryption framework, Eq. 2-5 are used in the calculation of image correlation:

$$Cor=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (2)$$

Where:

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-x')^2 \quad (3)$$

$$D(y)=\frac{1}{N}\sum_{i=1}^{N}(y_i-y')^2 \quad (4)$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-x')(y_i-y') \quad (5)$$

Correlation coefficient between original and encrypted images: The evaluation of the Correlation Coefficient (CC) between both plain and its corresponding ciphered image, the similarity between plain image and its related ciphered one must be measured (Norouzi *et al*., 2014). The calculation of CC is done by using Eq. 6-8:

$$\bar{A}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}A_{ij} \quad (6)$$

$$\bar{B}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}B_{ij} \quad (7)$$

$$CC=\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\bar{A})(B_{ij}-\bar{B})\Big/\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\bar{A})\right)^2\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{ij}-\bar{B})\right)^2} \quad (8)$$

Where:

A and B = The plain and ciphered image

M and N = The dimensions of both plain and ciphered images

A CC = Close to zero means there is a significant difference between plain and ciphered image which indicates the strength of encryption method

Mean square error and peak signal to noise ratio analysis: Mean Square Error (MSE) between plain and ciphered image isused to evaluate the reliability of the proposed framework. This evaluation can be achieved by implementing Eq. 9:

$$MSE=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(a(i,j)-b(i,j))^2 \quad (9)$$

where M and N = The dimensions of both plain and ciphered images and are pixel values in ith row and jth column for plain and ciphered images. In image security, the larger the MSE, the better (Norouzi *et al*., 2014). Furthermore, peak signal to noise ratio or PSNR is used to evaluate the quality of proposed image encryption framework which is done by implementing Eq. 10:

$$PSNR=10\log_{10}\frac{(I_{max}^2)}{MSE} \quad (10)$$

where, I_{max} is the maximum possible pixel value of image. Minimum PSNR value between plain and ciphered images indicates a large difference between them, indicating that the proposed encryption method is good.

Measurement of encryption quality: Image encryption quality test process can be described as following: choose one pixel E (I, j) from the encrypted image and another pixel P (I, j) from plain image (the location of both pixels are the same but each in its image) when M and N are image dimensions while G is the gray level values so both E (I, j) and P (I, j) are included in {0, 1, 2, ..., G-1}, HG (P) and HG (E) can be defined as the number of occurrences for each G in both plain and encrypted images, respectively. Encryption quality EQ is responsible to evaluate the average number of the change of pixels values G according to the following Eq. 11. The largest EQ is the better in security (Norouzi *et al*., 2014). Equation 11 is used to calculate encryption quality:

$$EQ=\sum_{G=0}^{255}(H_G(E)-H_G(P))^2/256 \quad (11)$$

Differential analysis: If one minor change in plain image causes an essential change in the ciphered image, the differential analysis will be useless (Pareek, 2012):

$$D(i,j)=\begin{cases}0, \text{if } c1(i,j)=c2(i,j)\\ 1, \text{if } c1(i,j)\neq c2(i,j)\end{cases} \quad (12)$$

$$NPCR=\frac{1}{M\times N}\sum_{i,j}^{M,N}D(i,j)\times 100\% \quad (13)$$

$$UACI=\frac{1}{M\times N}\sum_{i,j}^{M,N}\frac{|c1(i,j)-c2(i,j)|}{255}\times 100\% \quad (14)$$

To verify high security for the encryption method the difference between the encrypted forms should be as large as possible. If small changes in the plain image cause small change in the ciphered image this can be exploited by differential analysis by collecting useful information successfully (Pareek, 2012). The most useful security analysis for differential attack in image encryption field is Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR focuses on the total absolute number of changed pixels during differential attack while UACI is concerned with the average changes in a pair of ciphered pixels.

Suppose c1 and c2 are respectively both ciphered images before and after small changes have been made on plain image. The pixel value at grid (i, j) in

c1 and c2 are denoted as c1 (i, j) and c2 (i, j) and a bipolar array D is defined by Eq. 12. Then the NPCR and UACI can be mathematically defined by Eq. 13 and 14, respectively. Where M and N are the width and height of c^1 and c^2.

CONCLUSION

The expansion of the internet and digital communications has increased the need for data protection. The high usage of images for communication means that secure image encryption is necessary. Chaotic based image encryption is one of the best ways to encrypt an image file due its properties. In this study, multiple chaotic image encryption methods are discussed and evaluated.

RECOMMENDATIONS

This study found that the use of image confusion principles is necessary to reduce the correlation between adjacent pixels while the image diffusion is used to obliterate the image information. Key size which represents the necessary attempt to guess a correct decryption key could be increased by using multi chaotic map. Therefore, the successful chaotic-based image encryption system could increase the security through the implementation of both confusion and diffusion stages together and using multiple chaotic maps.

REFERENCES

Abdulgader, A., M. Ismail, N. Zainal, T. Idbeaa and K.S. Yoyon *et al*., 2015. Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption. J. Theor. Appl. Inf. Technol., 71: 1-12.

Aissa, B., D. Nadir and R. Mohamed, 2013. Image encryption using stream cipher based on nonlinear combination generator with enhanced security. New Trends Math. Sci., 1: 10-19.

Alfy, E.E.S. and A.K. Utaibi, 2011. An encryption scheme for color images based on chaotic maps and genetic operators. Proceedings of the 7th International Conference on Networking and Services, May 22-27, 2011, ICNS, Venice, Italy, ISBN:978-1-61208-133-5, pp: 92-97.

Alsafasfeh, Q.H. and A.A. Arfoa, 2011. Image encryption based on the general approach for multiple chaotic systems. J. Signal Inf. Process., 2: 238-244.

Alvarez, G. and S. Li, 2006. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos, 16: 2129-2151.

Bashardoost, M., M.S.M. Rahim, A. Altameem and A. Rehman, 2014. A novel approach to enhance the security of the LSB image steganography. Res. J. Appl. Sci. Eng. Technol., 7: 3957-3963.

Chen, C., T. Wang, Y. Kou, X. Chen and X. Li, 2013. Improvement of trace-driven I-Cache timing attack on the RSA algorithm. J. Syst. Software, 86: 100-107.

Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals, 21: 749-761.

Coppersmith, D., 1994. The data encryption standard (DES) and its strength against attacks. IBM. J. Res. Dev., 38: 243-250.

Dong, Y., J. Liu, C. Zhu and Y. Wang, 2010. Image encryption algorithm based on chaotic mapping. Proceedings of the 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT) Vol. 1, July 9-11, 2010, IEEE, Chengdu, China, ISBN:978-1-4244-5537-9, pp: 289-291.

Gao, H., Y. Zhang, S. Liang and D. Li, 2006. A new chaotic algorithm for image encryption. Chaos Solitons Fractals, 29: 393-399.

Guzman, G.L., C.C. Hernandez, G.R.M. Lopez and G.E.E. Garcia, 2008. Synchronization of multi-scroll chaos generators: Application to private communication. Rev. Mex. Phys., 54: 299-305.

Guzman, G.L., C.C. Hernandez, G.R.M. Lopez and G.E.E. Garcia, 2009. Synchronization of chua's circuits with multi-scroll attractors: Application to communication. Commun. Nonlinear Sci. Numer. Simul., 14: 2765-2775.

Habutsu, T., Y. Nishio, I. Sasase and S. Mori, 1991. A secret key cryptosystem by iterating a chaotic map. Proceedings of the Workshop on Advances in Cryptology Eurocrypt Theory and Application of Cryptographic Techniques Eurocrypt Vol. 91, April 8-11, 1991, Springer, Brighton, England, pp: 127-136.

Hernandez, C.C., M.D. Lopez, G.V. Garcia, G.H. Serrano and P.R. Nunez, 2005. Experimental realization of binary signals transmission using chaos. J. Circuits Syst. Comput., 14: 453-468.

Jain, A., 2016. Pixel chaotic shuffling and Arnold map based image security using complex wavelet transform. J. Network Commun. Emerging Technol. JNCET., 6: 8-11.

Jain, Y., R. Bansal, G. Sharma, B. Kumar and S. Gupta, 2016. Image encryption schemes: A complete survey. Intl. J. Signal Process. Image Process. Pattern Recognit., 9: 157-192.

Jolfaei, A. and A. Mirghadri, 2010. An image encryption approach using chaos and stream cipher. J. Theor. Applied Inform. Technol., 19: 117-125.

Kamali, S.H., R. Shakerian, M. Hedayati and M. Rahmani, 2010. A new modified version of advanced encryption standard based algorithm for image encryption. Proceedings of the 2010 International Conference On Electronics and Information Engineering (ICEIE), August 1-3, 2010, IEEE, Kyoto, Japan, ISBN:978-1-4244-7679-4, pp: V1-141-V1-141.

Khanzadi, H., M. Eshghi and S. Borujeni, 2014. Image encryption using random bit sequence based on chaotic maps. Arabian J. Sci. Eng. Springer Sci. Bus. Media BV., 39: 1039-1047.

Li, S.J., X. Zheng, X.Q. Mou and Y.L. Cai, 2002. Chaotic encryption scheme for real-time digital video. Real Time Imaging, 6: 149-160.

Lian, S., J. Sun and Z. Wang, 2005. Security analysis of a chaos-based image encryption algorithm. Phys. A. Stat. Mech. Appl., 351: 645-661.

Liu, R. and X. Tian, 2012. New algorithm for color image encryption using chaotic map and spatial bit-level permutation. J. Theor. Appl. Inf. Technol., 43: 89-93.

Liu, S., J. Sun and Z. Xu, 2009. An improved image encryption algorithm based on chaotic system. J. Comput., 4: 1091-1100.

Maadeed, A.S., A.A. Ali and T. Abdalla, 2012. A new chaos-based image-encryption and compression algorithm. J. Electr. Comput. Eng., 2012: 1-11.

Mahmood, A.S., M.S.M. Rahim and N.Z.S. Othman, 2016. Implementation of the binary random number generator using the knight tour problem. Mod. Appl. Sci., 10: 35-46.

Masuda, N. and K. Aihara, 2002. Cryptosystems with discretized chaotic maps. IEEE Trans. Circuits Syst. I: Fundam. Theory Appl., 49: 28-40.

Nesakumari, G.R. and S. Maruthuperumal, 2012. Normalized image watermarking scheme using chaotic system. Intl. J. Inf. Network Secur., Vol. 1,

Norouzi, B., S. Mirzakuchaki, S.M. Seyedzadeh and M.R. Mosavi, 2014. A s imple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimedia Tools Appl., 71: 1469-1497.

Pareek, N.K., 2012. Design and analysis of a novel digital image encryption scheme. Int. J. Netw. Secur. Applic., 4: 95-108.

Pecora, L.M. and T.L. Carroll, 1990. Synchronization in chaotic systems. Phys. Rev. Lett., 64: 821-830.

Salameh, J.N.B. and M.P.O. Karak, 2016. An investigation of the use of MJEA in image encryption. Wseas Trans. Comput., 15: 12-23.

Sankaran, K.S. and B.V.S. Krishna, 2011. A new chaotic algorithm for image encryption and decryption of digital color images. Int. J. Inform. Educ. Technol., 1: 137-141.

Sankpal, P.R. and P.A. Vijaya, 2014. Image encryption using chaotic maps: A survey. Proceedings of the 2014 5th International Conference on Signal and Image Processing (ICSIP), January 8-10, 2014, IEEE, Jeju Island, South Korea, ISBN:978-0-7695-5100-5, pp: 102-107.

Sharifara, A., M.S.M. Rahim and M. Bashardoost, 2013. A novel approach to enhance robustness in digital image watermarking using multiple bit-planes of intermediate significant bits. Proceedings of the 2013 International Conference on Informatics and Creative Multimedia (ICICM), September 4-6, 2013, IEEE, Kuala Lumpur, Malaysia, ISBN:978-0-7695-5133-3, pp: 22-27.

Shuangshuang, H. and L.Q. Min, 2014. A color image encryption scheme based on generalized synchronization theorem. Indonesian J. Electr. Eng. Comput. Sci., 12: 685-692.

Sivakumar, T. and R. Venkatesan, 2016. A new image encryption method based on knight's travel path and true random number. J. Inf. Sci. Eng., 32: 133-152.

Soleymani, A., Z.M. Ali and M.J. Nordin, 2012. A survey on principal aspects of secure image transmission. World Acad. Sci. Eng. Technol., 66: 1-8.

Su, Y., C. Tang, X. Chen, B. Li and W. Xu *et al*., 2017. Cascaded fresnel holographic image encryption scheme based on a constrained optimization algorithm and henon map. Opt. Lasers Eng., 88: 20-27.

Wang, L., Q. Ye, Y. Xiao, Y. Zou and B. Zhang, 2008. An image encryption scheme based on cross chaotic map. Proceedings of the Congress on Image and Signal Processing, Volume 3, May 27-30, 2008, Sanya, China, pp: 22-26.

Wang, X., L. Teng and X. Qin, 2012. A novel colour image encryption algorithm based on chaos. Signal Process., 92: 1101-1108.

Yen, J.C. and J.I. Guo, 2000b. Efficient hierarchical chaotic image encryption algorithm and its VLSI realization. IEE Proc. Vision Image Signal Process., 147: 167-175.

Yen, J.C. and J.I. Guo, 2000a. A new chaotic key-based design for image enc ryption and decryption. Proceedings of the IEEE International Symposium on Circuits and Systems, Volume 4, May 28-31, 2000, Geneva, Switzerland, pp: 49-52.

Zhang, Y., 2014. Plaintext related image encryption scheme using chaotic map. Indonesian J. Electr. Eng. Comput. Sci., 12: 635-643.