Chaos Image Encryption Methods: A Survey Study

Sabah Fadhel\textsuperscript{1,\,*}, Mohd Shafry\textsuperscript{2}, Omar Farook\textsuperscript{3}

\textsuperscript{1,\,3}Faculty of Computing-Universiti Teknologi Malaysia (UTM), Skudai, Johor, Malaysia
\textsuperscript{2}IRDA Digital Media Center, IHCE-Universiti Teknologi Malaysia (UTM)
\textsuperscript{*}Corresponding author, email: sabahuqaidy@yahoo.com

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, nowadays images being the most popular and old encryption techniques such as: AES, DES, RSA etc., show low security level when used for image encryption. This problem was resolved by using of 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 discusses various chaos encryption techniques.

Keywords: chaos, initial conditions, control parameters, map, permutation

1. Introduction

Multimedia technology, especially image technology is currently undergoing rapid change and growth [6] due to increased adoption of internet communications [1]. Current encryption techniques, such as AES, DES, and RSA are unsuitable for image data encrypting and cannot guarantee data confidentiality and security [2] because of the size and redundancy of images [3-5]. 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 [7]. 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 [8]. Chaos based encryption methods are popular due to their randomness, unpredictability, sensitivity and topological transitivity [9-10].

Literature review that has been done author used in the chapter "Introduction" to explain the difference of the manuscript with other papers, that it is innovative, it are used in the chapter "Research Method" to describe the step of research and used in the chapter "Results and Discussion" to support the analysis of the results [2]. If the manuscript was written really have high originality, which proposed a new method or algorithm, the additional chapter after the "Introduction" chapter and before the "Research Method" chapter can be added to explain briefly the theory and/or the proposed method/algorithm [4].

2. Chaos Theory

A chaotic dynamical system is any deterministic system that is both highly random and sensitive to initial conditions [11]. Chaotic systems are similar to noisy systems because both are highly unpredictable. Chaotic systems have uses in cryptography because they are pseudorandom, unpredictable and sensitive to initial condition (starting point) and control parameters [1]. 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 [12]. The main difference between chaos maps and chaos cryptography is that chaos cryptography is defined by finite sets, while chaos maps are defined by real numbers, as is shown in Table 1 [11]. Each chaos map has its own parameters and encryption key.
Table 1. Illustrate the Differences and Similarities Between Chaotic System and Cryptography Algorithm

<table>
<thead>
<tr>
<th>Chaotic System</th>
<th>Cryptography Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive to the initial conditions and control parameters</td>
<td>Diffusion</td>
</tr>
<tr>
<td>Iterations</td>
<td>Rounds</td>
</tr>
<tr>
<td>Parameters</td>
<td>Key</td>
</tr>
<tr>
<td>Set of real numbers</td>
<td>Finite set of integer numbers</td>
</tr>
</tbody>
</table>

Chaos maps can be applied by the use of 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 [13].

3. Chaos-Based General Image Encryption Scheme

Many data encryption methods use chaotic maps [14-20] because it is widely applicable and easy to understand. Chaotic based image encryption occurs in two stages, confusion and diffusion.

![Figure 1. Illustrates a Chaos-Based Image Encryption General Scheme](image-url)

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 these methods make chaotic encryption highly secure [21]. Figure 1 illustrates the chaotic encryption process.

4. Different Chaos-Based Encryption Techniques

[22] Proposed an image-scrambling algorithm that made use of chaotic mapping by encaging 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 is both simple and efficient. The proposed algorithm was evaluated using a correlation algorithm that indicated the relationship between the degree of scrambling and the scrambling numbers. From our viewpoint the key space of proposed algorithm is 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.

In the algorithm proposed by [23], both a Rössler 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 [24]. Both of Rössler and Lorenz schemes are each dependent on three variables, making increasing in the security of proposed chaotic system, because of the total parameters number dependent on six variables, making it highly secure. This algorithm shuffles an image’s pixels and changes its 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. From our viewpoint the key space of the proposed algorithm is good in terms of
increasing the total number of initial parameters to six instead of three for each chaotic system; also the correlation of resulted ciphered image is better.

[25] 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 of four control parameters and four initial values to act as shared keys for the encryption process. Second, quantification, which used to mapped the four sequences into key streams for use in the remaining phases. Third, a crossover used to confuse the image row-by-row and column-by-column. Fourth, a mutation phase used to implement XOR operator between the intermediate image (resulted from crossover stage) and random image. From our view point the proposed image is good in both of correlation coefficient and key space size. Therefore, it highly resist against the brute force attack.

New image encryption scheme based on one of three chaotic systems (Lorenz, Chen or Lu) was proposed by [26] to shuffle the positions of images’ 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 original image. From our view point, the proposed scheme produces large key space and good results in terms of the resulted correlation coefficient.

A new image encryption scheme was proposed by [2] 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. Pixels shuffling was achieved using horizontal and vertical permutations. Pixel correlations were scattered using a shuffling process. From our view point the proposed scheme has long key space; therefore it is good in brute force resistance. Also it shows good resistance against statistical attack.

A colored image encryption algorithm based on chaotic map and spatial bit-level permutations (SBLP) was proposed by [27]. Image pixel positions were shuffled using a sequence generated from a chaotic logistical map 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 new images pixel positions. From our view point, the proposed algorithm is robust against brute force attack because of suitable size of key space also it deal with bit level permutation. Also because of low complexity ant fast implementation time the proposed algorithm can be used in surveillance video systems.

An Enhancement of Advanced Encryption Standard (AES) was proposed by [28]. AES has many drawbacks such as high computational costs, predictable patterns and fixed S-box weak points. The proposed algorithm mitigates these drawbacks using a chaotic map and a XOR operator. The proposed method was tested by using several images and the results show very small correlation coefficients, improved encryption speed and high security. From our view point the proposed algorithm show good adaption for AES algorithm to be implemented in image encryption field.

To reduce the complexity of image encryption, [29] proposed a scheme 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. From our view point the proposed scheme is suitable, in terms of the key space and correlation coefficient.

An algorithm for generating random bit sequences based on chaotic maps was proposed by [30]. 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 eight-bit map planes. Bits were replaced by another bits value according to a chaotic ergodic matrix. From our view point the performance of this algorithm is good in terms of both key sensitivity and key space. Therefore this algorithm is highly resist against brute force attack and statistical attack.

5. Performance Analysis Of Chaotic Cryptography Systems

After Pecora and Carroll discovered synchronization in chaotic systems in 1990 [31], chaotic dynamics has received significant attention due to its use in securing communications.
Chaotic signal encoding was first used in 1990 [36]. Some of the most important ways that the strength of chaotic encryption methods has been evaluated are [13], [32]:

5.1. 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 [37]. In a strong encryption algorithm, key sensitivity should be greater than 50% [38].

5.2. 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 smaller than $2^{100}$ [39], with the exponent indicating the number of bits in a key. Large encryption keys provide greater security against brute force attacks [1].

5.3. Correlation Coefficient Analysis
The correlation coefficient measures similarities between a plain or an encrypted images pixels in the horizontal, vertical and diagonal directions. In a plain image, the correlation coefficient should be high. In an encrypted image, a smaller correlation coefficient indicates higher security [40]. Smaller correlation coefficients are produced from the confusion and diffusion methods.

5.4. Statistical Analysis
Statistical analysis is the most common cryptanalysis technique, and it is used to measure the relationship between a plain image and a ciphered image. Strong cryptographic techniques, when statistically analyzed, show large differences between the plain and ciphered image.

5.5. Image Entropy Analysis
Entropy is used to measure uncertain associations between random variables [41]. 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 [42]. The closer an encrypted images' entropy value is to 8 Sh, the more robust it is against entropy-based attacks.

6. 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. In this study, multiple chaotic image encryption methods are discussed and evaluated. Image security can be increased through the application of multiple chaotic image encryption methods.

Acknowledgements
Sabah Fadhel is grateful to the ministry of Sciences and Technology (Baghdad-Iraq), for providing study leave to continue his (Ph. D.).

References


*Chaos Image Encryption Methods: A Survey Study (Sabah Fadhel)*


**BIOGRAPHIES OF AUTHORS**

**Sabah Fadhel Hamood**

**Omar Fawrook Mohammado**