Review on 3D Chaotic Map Encryption and Data Hiding Technique

Pradeep H Kharat  
M.TECH student (Communication), Department of Electronics & Telecommunication Engineering  
Priyadarshini College Of Engineering, Nagpur  
E-mail: pradeepkharat91@gmail.com

Dr.S.S.Shiriramwar  
Associate Professor, Department of Electronics &  
Telecommunication Engineering  
Priyadarshini College Of Engineering, Nagpur  
E-mail: ssshriramwar@yahoo.com

Abstract—Transmission of important data like text, images, video, etc over the internet is increases now days, hence it’s necessary to use of secure methods for multimedia data. Image encryption is most secure than other multimedia components encryption because some inherent properties, such as huge data capacity and high correlation between pixels. The older encryption techniques such as AES, DES, RTS are not suitable for highly secure data transmission on wireless media. Thus we combine the chaotic theory and cryptography to form an valuable technique for information security. In the first stage, a user encrypts the original uncompressed image using chaotic map theory. Then, data-hider compresses the least significant bits of the encrypted image using a data-hiding key to make space for accommodate some additional data. In now days image encryption is chaos based for some unique characteristics such as correlation between neighboring pixels, sensitivity to initial conditions, non-periodicity, and control parameters. There are no image encryption algorithms based on chaotic maps have been implemented some of them are time consuming, complex and some have very little key space. In this paper we implement three non linear differential chaos based encryption technique where for the first time 3 differential chaos is used for position permutation and value transformation technique. In the data hiding phase, data which is in the the binary forms embedded into encrypted image by using least significant bit algorithm. We tabulate correlation coefficient value both horizontal and vertical position for cipher and original image and compare performance of our Method with some existing methods. We also discuss about different types of attack, key sensitivity, and key space of our proposed approach.

The given approach is very simple, fast, accurate and it have been applied together as a double algorithm in order to serve best results in highly unsecure and complex environment. Each of these algorithms are been discussed one by one below.

Keywords—encryption; correlation; algorithm.

I. INTRODUCTION

The dramatically spreading of the communication networks over the world increased dependency on digitized information in our life. As a result digital information is more valuable. Now days this digital information contain multimedia data consist of image, audio, video, text, etc. Today the web is going towards multimedia data due to the development of digital and multimedia technology. The digital images become one of the most important information carriers which are helpful for authentication, Biological science, military, online banking transactions, online shopping, online personal photograph album, etc. [1]. Image encryption is different from text encryption [7]. Older cipher algorithms such as DES, IDEA, AES, 3DES etc. are not suitable for images, videos and graphics due to data capacity, strong neighboring pixel correlation and high redundancy which minimized the encryption performance [2]-[6].

Chaos theory was firstly used in the encryption system by Edward Lorenz in 1963. During the last few decade chaos based cryptography has receive more attention due to noise like signal for unauthorized person, ergodicity, mixing, making confusion in the pixels of images, sensitivity to initial conditions, can be connected with those of good ciphers, such as confusion and diffusion [7][8]. In the research of information security and a lot of image encryption algorithms based on chaotic systems have been proposed [2]-[33]. There have been many image encryption algorithms based on chaotic maps like the Logistic map [12]-[16]. Higher dimension chaos functions are highly secure from cryptanalytic attacks [19].

Position permutation value transformation are two main processes in image encryption. In position permutation technique, permute image position without changing pixel value of original image and in value transformation technique pixel value replaced by another pixel value without changing position. XOR operation is one of the most important value transformation operation in which user create linear independency between two or more variable. The basic idea for use of XOR Encryption is that it is impossible to reverse the operation without knowing the initial value of one of the two components. Shuffling the positions of pixels in the image and then changing the gray values of the shuffled image pixels is used to improve the security performance of the transmitting image.

In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image the additional data is inserted using LSB algorithm.

The rest of the paper is organized as follows. The proposed hybrid image encryption strategy is described in Section II. Section III includes data hiding technique. Section IV includes image recovery and data extraction. Section V includes the comparison with some existing algorithm and VI concludes the paper.
II. ENCRYPTION STRATEGY

There are five steps to complete the overall encryption process. They are:

A) 3D Chaos generation.
B) Chaos Histogram Equalization.
C) Row Rotation.
D) Column Rotation.
E) XOR operation.

Figure 1 shows the overall encryption process where x, y, z are the key. All stage operation described gradually in bellow.

A. 3D Chaos Generation:
The logistic map is the simplest process of chaos generation given by an equation

$$x_{n+1} = \mu x_n (1 - x_n)$$  \hspace{1cm} (1)

For 0 < Xn<1 and \( \mu = 4 \) is the condition to make this equation chaotic. Hongjuan Liu et al proposed the 2D map by using quadratic coupling for enhanced security [20] and its extended 3D version are proposed in [16] given by the formula as follows.

$$x_{n+1} = \beta x_n y_n + \alpha x_n^3$$  \hspace{1cm} (2)

$$y_{n+1} = \beta y_n (1 - y_n) + \alpha x_n^3$$  \hspace{1cm} (3)

$$z_{n+1} = \beta z_n (1 - z_n) + \alpha x_n^3$$  \hspace{1cm} (4)

Here the above equations shows the confusion behavior for 3.53 < \( \gamma < 3.81 \), 0 < \( \beta < 0.022 \), 0 < \( \alpha < 0.015 \) and the initial value of x, y, z any value in-between 0 and 1. Presence of cubic, quadratic coupling and 3 constant terms make the 3D logistic map even more complex and secure.

B. Chaos Histogram Equalization:

Histogram of x, y and z is not uniformly distributed. For more security we need to equalize histogram. If image with MxN dimension where M is the number of row and N is the number of column then equalizes histogram by following formulae as follows:

$$x = \text{integer}(x \times N2) \mod N$$  \hspace{1cm} (5)

$$y = \text{integer}(y \times N4) \mod M$$  \hspace{1cm} (6)

$$z = \text{integer}(z \times N6) \mod 256$$  \hspace{1cm} (7)

Where N2,N4,N6 are large random numbers its value more than 10000, to equalize histogram of image we choose the number equal in magnitude.

C. Row Rotation:

For image pixel permutation we invent new approach for rotation of row column. For the rotation of row of a image having a dimension of MxN we need to select M number of chaos sequence. At first we generate a large random number N1 then select M number of chaos starting from index N1 and rotate row according to the value of chaos ‘x’ from Eq. 5. If chaos is even then we rotate row left and when the chaos value is odd then rotate row at right if the chaos value is odd.

D. Column Rotation:

Column rotation operation is equivalent as row rotation. For the rotation of column of a gray image have a dimension of MxN we need to select M number of chaos sequence. At first we generate a large random number N3 then select M number of chaos starting from index N3 and rotate column based on value of chaos ‘y’ from Eq. 6. For enhance security we rotate up when the chaos is even and rotate down if the chaos value is odd. After the rotation of row column the image becomes encrypted but the problem is non equalized histogram which can cause histogram attack. To protect from this problem we need to changes the image pixel value.

E. XOR operation:

The last step of this encryption process is XOR operation. XOR operation change the pixel value into new value and can’t reverse without knowing chaos key. At first we generate large random number N5 and convert MxN image
into 1xMN image. After that we XOR the chaos (starting from index N5) and row-column shifted image and finally we get encrypted image.

III. Data Embedding:

In encrypted image data is embedded within each pixels by using LSB algorithm. The other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. The detailed procedure is given below.

A. LSB: (Least Significant Bit) Algorithm:-

When using a 24-bit image, each of 8 bit red, 8 bit green and 8 bit blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. For example 800 × 600 pixel image a grid for 3 pixels of a 24-bit image can be as follows count of 1,440,000 bits.

\[
\begin{align*}
(00101101 & \quad 00011100 \quad 11011100) \\
(10100110 & \quad 11000100 \quad 00001100) \\
(11010010 & \quad 10101101 \quad 01100011)
\end{align*}
\]

When the number 200, which binary representation is11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

\[
\begin{align*}
(00101101 & \quad 00011101 \quad 11011100) \\
(10100111 & \quad 11000101 \quad 00001100) \\
(11010010 & \quad 10101100 \quad 01100011)
\end{align*}
\]

IV. IMAGE RECOVERY AND DATA EXTRACTION:

A. Image Decryption:

When obtain an encrypted image which consist hideded data. This encrypted image is now decrypted by using same keys that used for encryption. Suppose that the user at receiver has the encryption key but not knows the data-hiding key. That’s why he cannot obtain the values of parameters and cannot extract the embedded data.

b) Data extraction:

In encrypted image there is additional data, if the user at receiver side has knows only the data-hiding key, he can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. He can able extract both image and data only if he knows both the encryption key and data-hiding key resp.

V. Comparison With Some Existing Algorithm:

There is number of chaos based image encryption methods already implemented with their simulation result. In this project we compare the some properties of our method to others based on some parameter analysis. For test the performance of on paper image of 256x256. We compare NPCR, UACI and Entropy of our method to other algorithm [24, 25, 18] and comparatively same with respect to [23]. In [18] which use 3D chaos for image encryption have poor performance.

VI. CONCLUSION

In this paper we proposed a 3 differential chaos based simple encryption and data hiding technique in which first time chaos is used for position permutation and value transformation. With the help of this algorithm we can achieve high security purpose. Complexity of algorithm is reduced by eliminating any step from algorithm for low medium. However, With the help of out result we can show that this algorithm is best for any attack. Finally, we can calculate some tests like entropy analysis, statistical analysis and plain-text sensitivity, we also show that our algorithm has a high secure against different types of attacks. Our algorithm is ready to be applied in fast real time encryption applications and suitable for practical use in the secure transmission of multimedia information over the internet. It is not just limited to this area and can be widely applied in other information security fields.

REFERENCES


