A NON-LINEAR TWO DIMENSIONAL HENON-SINE CHAOTIC MAP BASED IMAGE CRYPTOSYSTEM

Sujarani.R 1, Manivannan.D 2
1 Department of Computer science, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam 612001, India
rsujarani@src.sastra.edu
2 School Of Computing, SASTRA University, Thanjavur 613401, India

Abstract: An image cryptosystem based on combining two chaotic maps is proposed to ensure secure transmission of sensitive images over insecure network. A new two dimensional Henon-Sine map (2DHS) is proposed by combining Henon and sine map. The proposed 2DHS generate two chaotic series. These chaotic series are used to perform permutation and substitution process of proposed image cryptosystem. Comparison between existing standard two dimensional (2D) Henon map and 2DHS map shows that the proposed map has more random behaviour than the existing one. To evaluate the security strength, the proposed image cryptosystem is subjected to different analysis such as differential and cipher image attack analysis. The analysed result shows that the proposed cipher has good security level and it can be used for securing different image communication applications.

Keywords: Image Cryptosystems, Henon-Sine Chaotic Map

1. Introduction

The significance of images in social media, industrial application and medical process has increased over the past decade. Security becomes an important consideration when these images are transferred over insecure networks. So, there is a great demand for encryption algorithms to securely transfer the images over the communication media. Images have some inherent properties, such as high data redundancy, high relationship among pixel values and are usually large in size. Because of these features, some conventional encryption techniques are challenging to use and they slow down the encryption process[1]. To overwhelm these problems chaos based image cryptosystem has emerged as a new field in cryptography. Chaos owned good cryptosystem properties such as ergodicity, dependent on initial values, high randomness, because of these features chaos began widespread between many cryptographers[2]. Different types of chaos based image cryptosystem have been developed by many researchers[3][4]. Confusion and diffusion are common methods used in these chaos cryptosystems. Chaos cryptosystems are developed by using either one - dimensional (1D) chaotic map or multi- dimensional chaotic maps. Chaotic series generated by 1D chaotic map has been used in many image cryptosystems. But due to its simplicity, these encryption methods are cryptanalyzed by different researchers[5][6]. As a result multi- dimensional chaos based image cryptosystems have emerged. Ruisong et al.[7] developed encryption algorithm for color images using two dimensional (2D) skew tent map, it generate two chaotic series, from this one series is used for permutation and another is used for substitution to achieve good encryption effect. Naeem et al.[8] introduced a new approach of image cryptosystem by utilizing 2D chaotic Baker map for confusion and for diffusion different transform domains are used. Chong Fu et al.[9] proposed medical image cryptosystem by combining 1D and 2D chaotic map, medical images are permuted multiple times by using 2D Arnold cat map and diffused by using chaotic series generated by single dimensional logistic map. In [10] cross chaotic map generate two chaotic series; these series are used for scrambling the pixels of the image, after pixels are diffused by using ciphertext feedback method. A novel image cryptosystem has proposed based on Henon chaotic map; a substitution box is created by using chaotic series produced by Henon map and this s-box is used to diffuse the pixels of images[11]. Some researchers developed new image cryptosystems by using multiple 1D chaotic maps[12][13] or by combining single and multi- dimensional chaotic maps[14][15]. Some authors proposed new chaotic maps by combining some of the existing chaotic maps[16][17] to enhance the random behaviour of the chaotic series.

In this paper, a new chaotic map has proposed by combining Henon and Sine map for efficient image cryptosystem. The proposed scheme is a symmetric key cipher with two major units, chaotic series index based image permutation unit and chaotic series based pixel substitution unit. The proposed Henon-Sine(HS) map is used to generate chaotic series which has more
randomness than the series generated by Henon and sine map.

Remaining of this paper is organized as follows. In section 2, the proposed chaotic map has discussed. The entire procedures of the proposed image cryptosystem are explained in section 3. The experimental result shown in section 4. The security analysis is illustrated in section 5. Finally, conclusion is drawn in section 6.

2. Basic concept of the proposed chaotic map

2.1 Henon Map
The French mathematician and astronomer Michel Henon proposed Henon map in 1976[11] and it is the most widely used two dimensional chaotic map. The mathematical expression of the Henon map is described in Eq. (1).

\[
\begin{pmatrix}
  x_{n+1} \\
  y_{n+1}
\end{pmatrix} = \begin{pmatrix}
  y_n + 1 - ax_n^2 \\
  \beta x_n
\end{pmatrix}
\]  

(1)

Where \(\alpha\) and \(\beta\) are state variables, \(i^{th}\) iteration value of \(x\) and \(y\) are denoted by \(x_n\) and \(y_n\) respectively. To keep the generated series in chaotic state, the control parameters must have the value of \(\alpha = 1.4\) and \(\beta = 0.3\)[18].

2.2 Sine Map
The Sine map is one of the familiar one dimension chaotic map which is similar to Logistic map[19]. The mathematical function of sine map can be described by using the following Eq.(2).

\[X_{n+1} = \alpha \sin (\pi X_n) / 4\]  

(2)

where the system parameter \(\alpha \in (0,4)\)

2.3 Proposed Henon-Sine Map
Here, the Sine map is combined with Henon map. The function used for generating first chaotic series (X) is the same as in the Henon map. The sine map is included in the function used for generating second chaotic series (Y). The mathematical function of the proposed Henon-Sine Map is described in Eq.(3).

\[
\begin{pmatrix}
  x_{n+1} \\
  y_{n+1}
\end{pmatrix} = \begin{pmatrix}
  y_n + 1 - ax_n^2 \\
  \beta \sin (\pi x_n)
\end{pmatrix}
\]  

(3)

The state variable \(\alpha\) and \(\beta\) must have the value 1.4 and 0.3 for maintaining the chaotic behaviour of the series generated by this map. \(x_n\) and \(y_n\) represents the \(n^{th}\) iteration value of \(x\) and \(y\).

Non-periodicity comparison

To compare the randomness of the chaotic series generated by Henon map and Henon-Sine map, both functions are iteratively executed for 250 times with initial values and state variables as \(x_0 = 0.56\), \(y_0 = 0.45\) and \(\alpha = 1.4\), \(\beta = 0.3\). The random behaviour of the chaotic series generated by general Henon map and the proposed HS map is illustrated in Fig.1. From the comparison between Fig.1. (a) and (b), it is clear that the proposed map is more non-linear than the existing one. In the proposed image cryptosystem both \(x\) and \(y\) chaotic series index are used for shuffling the pixels of the image. Both \(x\) and \(y\) chaotic series are in the form of decimal, so it is not possible to apply these values directly to the pixel values for diffusion process. Each chaotic series are converted into integer form and then used for diffusion process. The detailed procedure of confusion and diffusion is discussed in section 3.
3. Proposed image cryptosystem based on 2DHS Map

The entire architecture of the proposed image cryptosystem is given in Fig 2. The proposed scheme is the combination of two major steps, image confusion and diffusion. In confusion the position of the pixel values are scattered by utilizing the two chaotic series generated by the proposed HS map and in the diffusion process, each pixel of the scattered image is converted into another value by using the same set of chaotic series. The entire procedure of the proposed algorithm is discussed below.

Step 1: Input 8 bit gray image as I (row x col), where row and col denotes number of rows and columns of original image.

Step 2: Generate two chaotic sequences \( X=\{x_1,x_2,x_3,\ldots,x_{\text{row}}\} \) , \( Y=\{y_1,y_2,y_3,\ldots,y_{\text{col}}\} \) using the proposed HS Map with the condition that the primary and the initial values are taken as secret keys.

Step 3: Confusion process is done by using the index values of the sorted chaotic sequence \( X, Y \). Chaotic Sequences are sorted as given in the following Eq (4)

\[
[\text{sx}, \text{tx}] = \text{sort}(x) \quad [\text{sy}, \text{ty}] = \text{sort}(y) 
\]  

(4)

Where \( \text{sx} \) and \( \text{sy} \) are the new sorted series of \( x \) and \( y \). \( \text{tx} \) and \( \text{ty} \) are the index values of \( x \) and \( y \).

Step 4: By using the index value (\( \text{tx}, \text{ty} \)) the image I is diffused based on the following Eq (5):

\[
I_{ij} \leftrightarrow I_{\text{tx}(i), \text{ty}(j)} \quad \text{Where } i = j = 1,2,3,\ldots, \text{row/col}
\]

At the end of this step we get the shuffled image \( I'(\text{row}, \text{col}) \).

Step 5: For diffusion process the chaotic series are converted into integer form by using mod operator and then the result is XORed with the pixels of confused image. In this diffusion process odd rows of the image is XORed using \( Y \) series and even rows are XORed with \( X \) series which is depicted in Eq (6)

\[
I_i' = I_i \oplus \left( \left[ \left[ I_i \times X^\beta \right] \mod 256 \right] \oplus \left[ \left[ I_i \times Y^\alpha \right] \mod 256 \right] \right) \quad \text{Where } \alpha = 1.4, \beta = 0.3, x1= 0.48, y1=0.56
\]

(5)

(6)

I’ is the final encrypted image and this image is communicated to the concerned receiver. The keys and initial values are communicated in secure manner. For getting the original image, the receiver generate the chaotic series and do the reverse process of the encryption procedure.

4. Experimental result

Matlab 2013a has been used to implement the proposed scheme. Different images have been taken for experimental purpose of size (256 x 256). Two state variables and two initial values should be given as input. These values are taken as keys and transferred between sender and receiver in secure manner. For the experiment, the chosen state variable values and initial values are \( \alpha = 1.4, \beta = 0.3, x1= 0.48, y1=0.56 \). By applying these values, two chaotic series are generated by the proposed Henon-Sine Map. First, the given original image is confused by using the index values of the chaotic series, then the confused image is diffused by XORing the pixel values of the image with the integer format chaotic series. The experimental outcome is illustrated in Fig. 3.

Figure 3. Experimental result (a) Origin image (b) Confused image

5. Performance and security analysis

An efficient image cipher should resist various attacks such as linear attack and differential attack. The security level of the proposed cipher has been proved by different analysis such as histogram, correlation,
information entropy analysis and cipher image attack analysis.

5.1. Histogram analysis

Random distribution of pixel values in cipher image can be evaluated by using histogram analysis[20]. It demonstrates the graphical representation of pixel distribution in cipher image. Fig. 4 shows the histogram of the original and the cipher image. Based on the results, it is clear that the pixels of the cipher image are evenly distributed, so it is difficult for the attacker to apply statistical analysis for getting the original image.

5.2. Correlation coefficient analysis

Original image pixels are highly correlated with each other in all directions. A good image cipher should generate the cipher image with less correlation between the pixels values. The best way of finding the efficiency of the proposed image cryptosystem is to find the correlation among the pixel values of the cipher by using correlation coefficient analysis[19]. For checking the correlation, 1000 pairs of pixels are selected from each direction of the original image and cipher image. The computation of correlation coefficient is described in the following Eq. (7). A good cryptosystem achieve less correlation among pixels values of cipher image. Table 1 shows the result of correlation analysis of the proposed cryptosystem and the result is compared with different existing chaos based cryptosystem.

\[
C_{XY} = \frac{E[(x - E(x))(y - E(y))]}{\sigma_x \sigma_y}
\]  

(7)

Where E(x) represents the expected value of x and \( \sigma_x \) and \( \sigma_y \) is the standard deviation of x and y. The correlation coefficient of the original image and the cipher image of each direction is given in Fig. 5. Fig. 5(a) shows the correlation between the pixels of three direction of the origin Lena image and Fig. 5(b) shows the correlation between the pixels of ciphered Lena image.

![Figure 5](image)

(a) Correlation of pixels in original Lena image

(b) Correlation of pixels in ciphered Lena image

<table>
<thead>
<tr>
<th>Table 1. Comparison of Correlation coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Original 1 Image Fig. 5(a)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

5.3 Information entropy

Uncertainties of pixel values in cipher image can be calculated by using entropy analysis[25]. Random image entropy value is exactly 8. For the proposed system, if the entropy value of the cipher image is nearer to 8 then it can be decided that the pixels in the cipher image are uniformly distributed and also have capacity to fight against statistical attack. Entropy value of the image is calculated by using the following Eq. (8).

\[
E(I) = \sum_{i=0}^{n} P(I_i) \log_{2} \frac{1}{P(I_i)}
\]

(8)

\( I_i \) is the \( i^{th} \) pixel value of the n size gray image. \( P(I_i) \) is the probability of \( I_i \). The calculated entropy value of the Lena cipher image is 7.9952 which is nearer to 8, so the proposed image cryptosystem can withstand against statistical attack.

5.4 Cipher image attack analysis

During the time of transmission of cipher image between the sender and receiver, attackers can damage the cipher image by cropping and applying noise attacks. Even though the concerned receiver received
the cipher image, it is not possible for them to decrypt the cipher image by using the correct key, because a single change in the cipher image can entirely collapse the decryption result. Thus, a good image cryptosystem must resist cipher image attacks. The proposed system has been tested by cropping and applying noise attacks.

5.4.1. Cropped attack analysis

Proposed image cryptosystem robustness can be analyzed by applying cropping attack to cipher image[26]. It can be possible to apply cropping attacks in two different ways. In first way, the cipher image is cropped randomly in different regions with small size and the second way the image is cropped only asingle large region. Fig 6. Illustrates that the proposed image cryptosystem has efficiency to fight against cropping attack.

Figure 6. Cropped attack analysis

5.4.2. Noise attack analysis

Different noises degrade the cipher image at the time of transmission. Tiny change in cipher image may cause high distortion in deciphered image, so an authenticated receiver will not be able to visualize the original image even if he decrypts in right way. A good cipher must resist noisy attacks [27]. Proposed scheme’s robustness against noise attack has been checked by applying salt and pepper noise to the cipher image in different densities and visual quality of the deciphered image is checked and illustrated in Fig 7.

Figure 7. Noise attack analysis

6. Conclusion

A new two dimensional Henon-Sine map has been proposed by combining the Henon and sine map which produces chaotic series with high randomness than the existing 2D Henon map. An image cryptosystem has designed by using the proposed 2DHS map. The designed image cryptosystem combines the confusion and diffusion processes. In confusion, the pixel values of the image are shuffled by using the index values of the chaotic series generated by 2DHS map. In diffusion process, the pixels values of the confused image is XORed with the integer format chaotic series. Finally the cipher image is obtained. Result show that the proposed image cipher can withstand different attacks and has sufficient level of security. The proposed algorithm is suitable for providing security for different formats of images such as jpeg, Tiff, bmp, medical images and it is also suitable for colour image cipher.

Acknowledgments

The authors wish to express their sincere thanks to the Department of Science & Technology, New Delhi, India (Project-ID:SR/FST/ETI-371/2014) and SASTRA University, Thanjavur, India for extending the infrastructural support to carry out this work.

References


