Chaos based Image Security Solution
for Social Networking Sites

More Poonam M. & Khobragade Sanjay V.
Department of Electronics and Telecommunication
Dr. B.A.T. University, Lonere, Raigad, India.
E-mail : poonammore306@gmail.com, svk2305@gmail.com

Abstract – The images which individuals upload on social networking sites are being misused by adversaries due to lack of security at receiver end. In this paper, we have proposed one security solution for images, to avoid the misuse. In this security solution, we will be developing a special function which will cipher all the images uploaded on social networking sites whenever receiver at the other end tries to save them on their desktops.

Keywords – Image security, Chaotic map, modified reverse hidden transform (mRHT), random number generator.

I. INTRODUCTION

Now-a-days the Virtual Life on the social networking sites is becoming an integral part of real life, thanks to the advancements in web technologies, as people across the world are sharing each and every detail about each and every moments of their life through these social networking sites. By using social networking sites we can exchange our ideas, experiences, personal information through the posts which may be either in the form of comments or images with people who are at the other end of the world and the part of our social life.

Though the advancements in web technologies enables each individual to be get connected globally. It creates some serious issue like misusing of the information of individuals (e.g. images, other personal data) with wrong intentions. To stop such misuse we need to provide more security not only during the transmission but also at the receiver end so that the adversaries (which might be in the list of friends circle on the social networking site) will not be able to misuse any information of individual. Normally in cryptography we assume that information should be ciphered while transmitting it from transmitter to intended receiver and should be available in the original form, at the intended receiver. But when dealing with social networking sites this assumption has to be altered a little bit to make sure the security of individual’s information specially images as they mostly represents individual’s identity.

Here we have proposed a system which can be considered as a breakthrough in security of images on social networking sites. In this proposed system we will try to make sure that images which individuals are posting/uploading in their accounts will be only visible to all the intended receivers at the other end but won’t be able to access through downloading or saving them on their desktops. Hence the images of individual’s will be more secure and hence misusing of them can be decreased. In proposed security solution for images, we will be implementing a special inbuilt function, in web browser or social networking sites, which will enable all the images from the social networking sites to be saved in ciphered format by using proposed image encryption technique based on chaos, whenever receiver at other end tries to get the images from social networking sites, hence the providing security solution for images on these sites.

This paper is organized as follows: In section II, chaotic maps, modified RHT and random sequence generator are described followed by the proposed encryption technique’s description which will be used for image security in section III, along with the results of proposed system. In section IV, some security analysis techniques are discussed with respect to proposed scheme and in section V we conclude the paper.

II. PRELIMINARIES

For this proposed image security system for social networking sites, we need to have an encryption method which will cipher the image whenever it is being saved. So for that here we have discussed some basic elements which we will be using to establish the proposed image encryption scheme for image security such as chaotic
equations, modified reverse hidden transform (mRHT), random sequence generator.

This proposed image encryption is based on chaos equations which are assumed to be provide most prominent method for encryption as these equations are very sensitive to initial conditions and control parameters, also we will be using modified reverse hidden transform (mRHT) along with random sequence generator to encrypt image.

A. Chaotic Equations

Chaos is sustained and disorderly-looking long-term evolution that satisfies certain special mathematical criteria and that occurs in a deterministic nonlinear system. Chaotic equations are also known as chaotic maps and these are the principles and mathematical operations underlying chaos. The proposed image encryption is based on chaos equations which are have become interesting research areas because of their attractive features such as aperiodicity, sensitivity to initial conditions and system parameters [1] and hence are assumed to provide prominent encryption method for images.

Mostly, one-dimensional chaotic equations, such as Logistic maps with the advantages of high-level efficiency and sensitivity, are widely used but have some drawbacks, such as weak security and nonuniformity, which are disturbing factors while using them.

In this paper, the another chaotic map having better performance than logistic map [1, 2, 7] is used, namely PWLCM, which is mathematically represented as

\[ x_{i+1} = P_p(x_i) = \begin{cases} 
\frac{x_i}{p} & \text{if } 0 \leq x_i \leq p \\
\frac{(x_i-p)}{(1-x_i)} & \text{if } p \leq x_i \leq 0.5 \\
\frac{1-x_i}{p} & \text{if } x_i \geq 0.5 
\end{cases} \]

(1)

Where \( x_i (\cdot) \in (0,1) \) and the control parameter \( p \in (0, 0.5) \).

B. Modified RHT

The RHT, used in [2] states that if \([0, L]\) is the image gray level range then a pair of pixels, \(x = (x_1, x_2)\) can be transformed into another pair of pixels, \(y = (y_1, y_2)\) by using two fixed numbers \(\alpha, \beta\) as follows:

**Forward Transform:**

\[ y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \alpha x_1 + \beta x_2 \\ \alpha x_2 + \beta x_1 \end{bmatrix} \]

(2)

such that \(\alpha + \beta = 1\), and \(0 \leq \alpha, \beta \leq 1\).

**Inverse Transform:**

\[ x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \frac{y_1 - \beta y_2}{\alpha - \beta} \\ \frac{\alpha y_1 - y_2}{\alpha - \beta} \end{bmatrix} \]

(3)

But these forward and inverse transform equations pairs will not be able to reconstruct the original image properly. That means, reconstruction of a pair of pixels, \(x = (x_1, x_2)\), is not possible in reverse way using above mentioned inverse transform. Hence we change these equations and proposed a modified RHT as follows:

**Modified Forward Transform:**

\[ y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \alpha x_1 + \beta x_2 \\ \alpha x_2 + \beta x_1 \end{bmatrix} \]

(4)

**Modified Inverse Transform:**

\[ x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \frac{y_1 - \beta y_2}{\alpha - \beta} \\ \frac{\alpha y_1 - y_2}{\alpha - \beta} \end{bmatrix} \]

(5)

This pair of modified forward and inverse transform equations will give us proper mapping of integer values of pixel pairs in forward and reverse direction. The term hidden is used because of the values of \(\alpha\) and \(\beta\) are generated randomly, and hence all transformed images corresponding to an image will be different as the values of \(\alpha\) and \(\beta\) will be different.

In the proposed encryption technique, we have used modified RHT to transform an integer pair to another integer pair with lower mathematical computation based on some secret parameters that are nothing but \(\alpha\) and \(\beta\).

C. Random Sequence Generator

To process the resultant transformed image from mRHT further a random sequence is required which can be obtained by using the Eq. (1) and using different initial and parameter values. The generated sequence of Eq. (1) is processed as follows to obtained proper random integer sequence which will be used to generate encrypted image.

\[ R_i = x_i \mod K \]

(6)

Where \(R_i\) is generated random sequence, \(x_i\) is sequence generated by Eq. 1, and \(K\) is the maximum pixel value in the transformed image.
III. PROPOSED SECURITY SOLUTION FOR IMAGE

In this section we are discussing the method of encryption and decryption which will be used for image secure as shown in fig. 1.

A) Encryption Process

1) Create two $x$ and $y$ random integer sequences using piecewise linear chaotic map with $p_0, p_1$ as control parameters and $x_0, x_1$ as initial values for $x$ and $y$ respectively, such that $x, y \in (1, M \times N)$, where $M, N$ are dimensions of original image say ‘PI’.

2) Perform modified RHT on original image ‘PI’ using $x, y$ sequences as pixel indices of the original and transformed image respectively to get transformed image ‘CI’.

3) Generate another random sequence $R_i$ using Eq. (1) by considering the $p_2$ as control parameter and $x_2$ as initial value and perform EXOR operation as follows on the transformed image using randomly generated sequences to get encrypted image $E$.

$$ E_i = C_l_i \oplus R_i $$

where $i \in (1, M \times N)$.

B) Decryption Process

Decryption process is exact reverse of the encryption process. It is assumed that all the basic key values used for encryption are available at the receiver end to decrypt the encrypted image.

The robustness and validity of the proposed scheme are demonstrated using MATLAB platform. Different images are used as experimental images for experimental purpose. Fig. 2 shows the original fingerprint image, encrypted fingerprint images, and decrypted fingerprint images with correct and wrong keys. Fig. 2(c) shows the decrypted image with all correct keys.

IV. SECURITY ANALYSIS

Security is the main thrust of the encryption techniques. Some security analysis has been performed on the proposed biometrics encryption technique that includes cryptographic security along with the perceptual security. Both the security analyses for the proposed technique are discussed as follows.
A. Cryptographic security

The cryptographic security can be viewed as the ability of the technique to resist the cryptanalysis process. Cryptanalysis is the science of analyzing and breaking the secure channel; this report includes the key and original image sensitivity analysis.

1) Key Sensitivity:

Key sensitivity is defined as the change in the encrypted fingerprint due to change in the key. For a good security solution, the slight difference in the keys should cause great changes in the encrypted media. The key sensitivity (KS) can be computed by

\[ KS = \frac{\text{Diff}(C, \hat{C})}{M \times N} \times 100\% \]  

(8)

where \( C \) and \( \hat{C} \) are the encrypted fingerprint images using correct and wrong keys with \( M \times N \) as the dimension of encrypted images. Mathematically, \( \text{Diff}(C, \hat{C}) \) is defined as

\[ \text{Diff}(C, \hat{C}) = \sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) \otimes \hat{C}(i,j)) \]  

(9)

where

\[ C(i,j) \otimes \hat{C}(i,j) = \begin{cases} 1, & C(i,j) \neq \hat{C}(i,j) \\ 0, & C(i,j) = \hat{C}(i,j) \end{cases} \]  

(10)

Generally, for a good encryption scheme, the value of KS is about 75%. And with our encryption method it is achieved around 100% (Refer fig. 2).

2) NPCR:

Similar to key sensitivity, Number of Changing Pixel Rate (NPCR) is defined as the changes in the encrypted image caused by the changes in the original fingerprint image. For better security, the slight difference in the original media should cause great changes in the encrypted media. It is the most common test used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks. A high NPCR score is usually interpreted as a high resistance to differential attacks. If \( C_1 \) and \( C_2 \) are ciphered images before and after one pixel change in a plaintext image respectively, and \( D \) is a bipolar array defined as

\[ D = \begin{cases} 1, & \text{if } C_1(i,j) = C_2(i,j) \\ 0, & \text{otherwise} \end{cases} \]  

Then the NPCR is defined as

\[ \text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \]  

(12)

Ideally encrypted image always have 100% NPCR value. And with our encryption method we have got approximately 99.9969% of NPCR values in most of the cases as shown in Table I.

B. Perceptual Security

The perceptual security ensures that the encrypted image cannot reveal the overview of the original image. Histogram analysis is the popularly used analysis to check perceptual security of system. The histograms of the original and encrypted image are compared. If the histogram of the encrypted image is fairly uniform and is significantly different from the histogram of the original one, then the encryption is said to be perfect. Moreover, the histogram of the decrypted fingerprint must be similar to the original one.

![Histogram of fig. 2(a)](a) Histogram of fig. 2(a)

![Histogram of fig. 2(b)](b) Histogram of fig. 2(b)

**TABLE I: TEST RESULTS**

<table>
<thead>
<tr>
<th>Images</th>
<th>Key Sensitivity Test Results in %</th>
<th>NPCR Test Results in %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>99.0002</td>
<td>99.9984</td>
</tr>
<tr>
<td></td>
<td>99.9941</td>
<td>99.9969</td>
</tr>
<tr>
<td></td>
<td>99.9337</td>
<td>99.9958</td>
</tr>
<tr>
<td></td>
<td>99.9510</td>
<td>99.9959</td>
</tr>
<tr>
<td></td>
<td>99.6017</td>
<td>99.9866</td>
</tr>
<tr>
<td></td>
<td>99.9337</td>
<td>99.9969</td>
</tr>
</tbody>
</table>
V. CONCLUSION

In this paper, a new simple security solution for images is proposed. In the proposed scheme we used PWLCM along with the modified RHT to create randomness in the original image, to make image more secure we have further processed transformed image with random sequences. Then further security analysis like key test analysis, histogram analysis are carried out to ensure the effectiveness of the proposed scheme. This kind of security solution will be used in the social networking sites to secure images from the adversaries.

VI. REFERENCES


