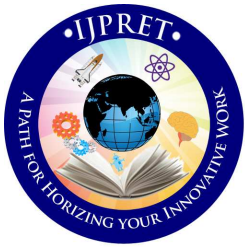
Research Article *ISSN: 2319-507X*
Poonam More, IJPRET, 2013; Volume 1(8): 801- 808 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

IMAGE SECURITY SOLUTION BASED ON CHAOS

MORE POONAM M., PROF. KHOBRAGADE SANJAY V

Electronics and Telecommunication Department, Dr. Babasaheb Ambedkar Technological University, Lonere, Raigad, Maharashtra, India

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Image encryption,
Piecewise Linear Chaotic map,
Modified Reversible Hidden Transform (MRHT),
Random sequence generator

Corresponding Author

Ms. Poonam M. More

Abstract

In this paper new encryption technique for image is described which may be considered as efficient security solution for image. This encryption technique is based on chaotic map with modified Reversible Hidden transform and, random sequences. The basic idea of this technique is to process gray values in the special domain using chaotic map with RHT which is being further processed by random sequences generated by random sequence generator.

• INTRODUCTION

Encryption is used to securely transmit as well as to store the data. Each type of data presents a relative importance, especially images; therefore different techniques should be used to protect confidential image data from unauthorized access or modification. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Many image content encryption algorithms have been proposed [3-6, 8]. Many among these are chaotic based algorithms since chaotic system properties such as aperiodicity, sensitivity to initial conditions and system parameters are preferred.

In this paper, a new encryption technique is proposed based on modified reversible hidden transform (mRHT), piecewise linear chaotic map which may provide a security solution for images. The core idea will be to transform the original image first using chaotic map with modified RHT. Then, the transformed image will be further processed by random sequences generated by chaotic map to get the encrypted image. Exact reverse process will be followed at receiver to decrypt the image.

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 in section III, then 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.

• PRELIMINARIES

In this section, the description of RHT is discussed along with the basic details of chaotic maps.

A. Chaotic Maps

Chaos is sustained and disorderly-looking long-term evolution that satisfies certain special mathematical criteria and that occurs in a deterministic nonlinear system. Chaotic maps are the principles and mathematical operations underlying chaos. Recently chaotic maps have become interesting research areas because of their attractive features such as aperiodicity, sensitivity to initial conditions and system parameters [1].

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

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

$$x_{i+1} = F_p(x_i) = \begin{cases} \frac{x_i}{p} & if\ 0 \le x_i \le p \\ \frac{(x_i - p)}{(0.5 - p)} & if\ p \le x_i \le 0.5 \\ F_p(1 - x_i) & if\ x_i \ge 0.5 \end{cases}$$

(1)

where x_i (·) ϵ (0,1) and the control parameter p ϵ (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= (x₁, x₂)* can be transformed into another pair of pixels, *y= (y₁, y₂)* by using two fixed numbers *α, β* as follows:

Forward Transform:

$$y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \alpha x_1 + \beta x_2 \\ \alpha x_2 + \beta x_1 \end{bmatrix} \qquad (2)$$

such that *α + β=1,* and *0 ≤ α, β ≤* 1.

Inverse Transform:

$$\tilde{x} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} \frac{\alpha y_1 - \beta y_2}{\alpha^2 - \beta^2} \\ \frac{\beta y_1 + \alpha y_2}{\beta^2 - \alpha^2} \end{bmatrix} \qquad (3)$$

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= (x₁, x₂),* 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:

$$y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \alpha x_1 + \beta x_2 \\ \alpha x_2 + \beta x_1 \end{bmatrix} \qquad (4)$$

Modified Inverse Transform:

$$\tilde{x} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} \frac{\alpha y_1 - \beta y_2}{\alpha^2 - \beta^2} \\ \frac{\alpha y_2 - \beta y_1}{\alpha^2 - \beta^2} \end{bmatrix} \qquad (5)$$

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 *α* and *β* are generated randomly, and hence all transformed images corresponding to an image will be different as the values of *α* and *β* will be different.

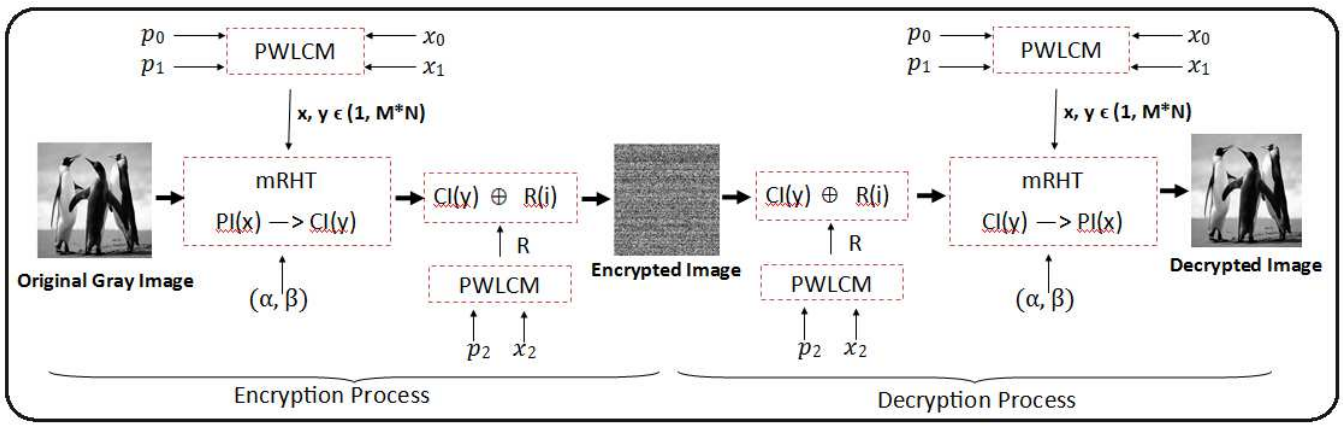


Figure 1: Block diagram of proposed system

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 α and β.

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.

$$R_i = x_i \, mod \, K \qquad (6)$$

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.

- **PROPOSED SECURITY SOLUTION FOR IMAGE**

In this section we are discussing the method of encryption and decryption for making image secure as shown in fig. 2.

A. Encryption Process

1) Create two x and y random integer sequences using piecewise linear chaotic map with p_1, p_2 as control parameters and x_0, y_0 as initial values for x and y respectively, such that *x, y ϵ (1, M*N),* where M, N are dimensions of original image say 'A'.

2) Perform modified RHT on original image A using x, y sequences as pixel indices of the original and transformed image respectively to get transformed image B.

3) Generate another random sequence R_i using Eq. (1) by considering the p_3 as control

parameter and x_1 as initial value and perform EXOR operation as follows on the transformed image using randomly generated sequences to get encrypted image *E*.

$$E_i = B_i \oplus R_i \quad (7)$$

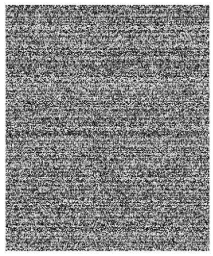
where *i ϵ (1, M*N).*

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.

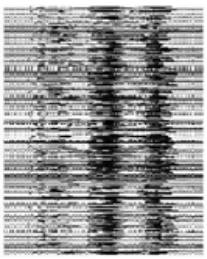
The robustness and validity of the proposed scheme are demonstrated using MATLAB platform. Different images are used as experimental images for experimental purpose. Fig. 2 shows the original fingerprint image, encrypted fingerprint images, and decrypted fingerprint images with correct and wrong keys.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

(a) Original image



(b) Encrypted Image

(c) Decrypted Image with all correct keys



(d) Decrypted Image with wrong keys

Figure 2: key Test analysis

- **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.

a. 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

$$KS = \frac{Dif(C,\tilde{C})}{M \times N} \times 100\ \% \qquad (8)$$

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

$$Dif(C,\tilde{C}) = \sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j) \otimes \tilde{C}(i,j) \qquad (9)$$

where

$$C(i,j) \otimes \tilde{C}(i,j) = \begin{cases} 1, & C(i,j) \neq \tilde{C}(i,j) \\ 0, & C(i,j) = \tilde{C}(i,j) \end{cases} \qquad (10)$$

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).

Table I: Test Results

Images	Key Sensitivity Test Results in %	NPCR Test Results in %
	99.6002	99.9984
	99.5941	99.9969
	99.6337	99.9968
	99.5910	99.9969
	99.6017	99.9866
	99.6337	99.9969

b. 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 C1 and C2 are ciphered images before and after one pixel change in a plaintext image respectively, and D is a bipolar array defined as

$$D = \begin{cases} 1 & if\ C1(i,j) = C2(i,j) \\ 0 & otherwise \end{cases} \quad (11)$$

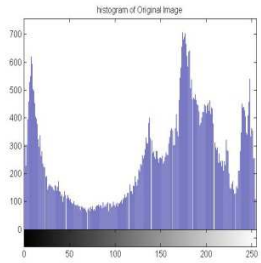
Then the NPCR is defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (12)$$

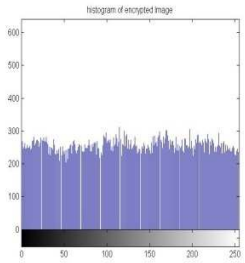
Ideally encrypted image always have 100% NPCR value. And with our encryption method we have got approximately 99.9969% of NPCR values in most of the cases as shown in Table I.

B. Perceptual Security

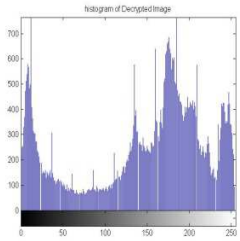
The perceptual security ensures that the encrypted image cannot reveal the overview of the original image. Histogram analysis is the popularly used analysis to check perceptual security of system. The histograms of the original and encrypted image are compared. If the histogram of the encrypted image 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.



(a) Histogram of fig. 2(a)



(b) Histogram of fig. 2(b)



(c) Histogram of fig. 2(c)

Figure 3: Histogram Analysis

The corresponding histograms of the original, encrypted and decrypted images are depicted in Fig. 3. Fig. 3 shows that, after encryption, the histogram becomes uniform, and the decryption process makes it similar to the original image histogram, which is the major requirement of the image encryption.

• 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 can be used in the web applications to secure images from the adversaries.

REFERENCES

1. G. P. Williams, Chaos Teory Tamed. NW Washington DC: Joseph Henry Press, 1999, ch. 2.

2. G. Bhatnagar, Q. M. Jonathan Wu, "Chaos-Based Security Solution for Fingerprint Data during Communication and Transmission", IEEE Trans. Instrum. Meas., Vol. 61, No. 4, pp. 876–887, April 2012.

3. K. D. Patel, Sonal Belani, "Image Encryption Using Different Techniques: A Review", IJETAE International Journal of Emerging Technology and Advanced Engineering, Vol.1, No. 1, November 2011.

4. Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, "Digital image encryption algorithm based on chaos and improved DES", IEEE International Conference on Systems, Man and Cybernetics, 2009.

5. Ismail Amr Ismail, Mohammed Amin, Hossam Diab, "A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, pp.1 -10, July 2010.

6. Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

7. H. Gao, Y. Zhang, S. Liang, D. Li, "A New Chaotic Algorithm For Image Encryption," Chaos Solitons Fractals, vol. 29, pp. 393–399, 2006.

8. N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image Vis. Comput., vol. 24, no. 9, pp. 926–934, 2006.