Optik 127 (2016) 192–199

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Crypt analysis of an image encryption algorithm and an enhanced scheme

Devaraj Ponnain, Kavitha Chandranbabu*

Department of Mathematics, College of Engineering, Guindy, Anna University Chennai, Chennai 25, India

ARTICLE INFO

Article history:
Received 28 November 2014
Accepted 27 September 2015

Keywords:
Modified logistic map
Diffusion
Chaos
Permutation

ABSTRACT

This paper analyzes the security issues of the recently proposed JPEG image encryption scheme. A new image encryption algorithm using modified logistic map is proposed. The chaotic sequences generated using modified logistic map are used for permutation, bit swapping and random diffusion. These processes impose the confusion and diffusion effect on the image and make the scheme secure. The security parameters such as entropy, correlation, NPCR and UACI are tested and the results show the scheme is secure.

1. Introduction

The drastic development in the network technology has taken communication to new era. People communicate with each other anytime, anywhere using laptops, personal computers, mobile phones, etc. In the present world, starting from sensitive military, business and banking communication to day-to-day messaging among people is taking place through insecure open channel which is either wired or wireless connection. Hence, it becomes essential to address the security issues during communication which gives rise to many encryption techniques. Though, many encryption techniques are available for text message, they do not suit for image encryption, due to the hereditary nature of images. Hence, many image encryption algorithms are being developed. Most of these algorithms use chaotic system due to their nature such as ergodicity, mixing property and sensitivity to initial condition and parameters. As many algorithms arise, cryptanalysis is also being done on many algorithms proving not all algorithms are secure.

In recent days, many chaotic maps are also modified for improving the security. Sam et al. [1], proposed an encryption scheme using intertwining logistic map and non-linear diffusion. The intertwining logistic map and reversible cellular automata was used in an image encryption scheme proposed in [2]. This encryption scheme performs operations at bit level considering higher four bits of each pixel value. In [3], Zhou et al., introduced a new parametric switching chaotic system (PSCS) that integrates the Logistic, Sine and Tent maps into one single system. The logistic map was used as a control sequence which controls the switch to select either the Sine map or the Tent map as a generator to produce the PSCS's output sequence. Zhou et al., also generalized his technique of combining the chaotic maps in [4] and introduced a chaotic system. Zhu's encryption scheme [5], shuffles the plain image using 2D hyper-chaos discrete nonlinear dynamic system whereas compression and diffusion is performed using Chinese remainder theorem. In [6], a novel image encryption algorithm was introduced based on hyper-chaotic system with one round diffusion process. The main idea of this algorithm is to encrypt each pixel, using the sum of pixels which are located after that pixel. Zhang et al. in [7], applied known plaintext and chosen plaintext attacks to reveal the secret key of the encryption scheme in [6]. An image encryption scheme using chaotic function and xor operator was presented in [8]. This scheme was proved to be weak due to the linearity that exist in the scheme and was broken using chosen cipher text attack in [9]. Many encryption scheme also arise to encrypt the color images, which consider the three color components separately and apply the encryption technique [1,10–12]. D. Zhang et al. [12], separated the red, green and blue components into three two dimensional matrices and applied permutation considering each 8 × 8 block of the matrix as unit.

In this paper, the encryption scheme proposed in [12] is analyzed using security measures such as histogram, NPCR and UACI. These results show it is vulnerable against known/chosen plain text attack. Also, a new image encryption scheme is presented using modified logistic map and applying random diffusion technique. The scheme is tested against different security parameter such as entropy, correlation and sensitivity to changes in plain image and

* Corresponding author. Tel.: +91 8098445292.
E-mail address: kavistha@gmail.com (K. Chandranbabu).

http://dx.doi.org/10.1016/j.ijleo.2015.09.207
0030-4026/© 2015 Elsevier GmbH. All rights reserved.

key. The results show that the scheme is faster and secure to be used for real time applications.

2. D. Zhang encryption scheme

The scheme proposed in [12] generates two chaotic sequences and applies them for scrambling the plain image. Encryption involves the following steps:

Step 1. A JPEG image file is represented by means of two-dimensional data matrix. If the image is gray, then it is denoted by a two-dimensional data matrix. If the image is color, then it is denoted by three two-dimensional data matrices, each for a component.
Step 2. Every 8×8 data block of every two-dimensional data matrix is scrambled in row and column positions by chaotic sequences. Scrambling the row and column positions of every 8×8 data block of the two-dimensional data matrix is to move the 8×8 data block to the row and column positions of some 8×8 data block of the two-dimensional data matrix. The original row and column positions occupied by an 8×8 data block and its new occupying positions through scrambling are one to one.
Step 3. The two-dimensional scrambled data matrixes are denoted by JPEG format to give an encrypted JPEG image.

In [12], the author has proposed two schemes based on the above encryption steps. The first scheme generates two chaotic sequences using logistic map. These sequences combine together to scramble the three two dimensional data matrix. The second scheme generates six sequences using logistic map. The first sequence and the second sequence combine, the third sequence and the fourth sequence combine, the fifth sequence and the sixth sequence combine, respectively scramble the row and column positions of all the 8×8 data blocks of three two-dimensional data matrixes of the original image.

3. Security analysis of [12]

In the above scheme, the encryption process is permuting the data matrix considering 8×8 block as a unit. The permutation procedure is not given explicitly. But the one to one correspondence between the source and the destination location of the 8×8 data block is maintained during permutation. Permutation can only promote confusion in the plain image. Mere confusion cannot hide the statistical properties. Hence, permutation in the scheme is insufficient to provide enough confusion on plain image.

Generating the key sequences using logistic map and encrypting the plain image using the sequence the following analysis is performed.

Since the encryption process involves only permutation, the pixel value are not modified. From the histogram depicted in Fig. 1, it is clear that the distribution of the pixel values of the encrypted image is same as the original image.

Further, for any plain image the correlation of the adjacent pixel values remains unaltered much after the encryption using this scheme. The encryption in [12] scrambles the image by considering 8×8 data block as a single unit. Hence the confusion introduced in the image does not neutralize existing correlation. The Table 1 shows that the encrypted image still remains highly correlated.

The number of pixel change rate (NPCR) and the unified averaged changed intensity (UACI) are used to test the plain image sensitivity. The ideal value for NPCR and UACI are 99.60% and 33.46% respectively. The simulation values of NPCR and UACI in Table 2 shows that change in some pixel values never affect the remaining pixels in the output. However, for an ideal scheme a single pixel change should affect many pixels in the output. Moreover, for this scheme the UACI and NPCR values are very small and this is shown in Table 1.

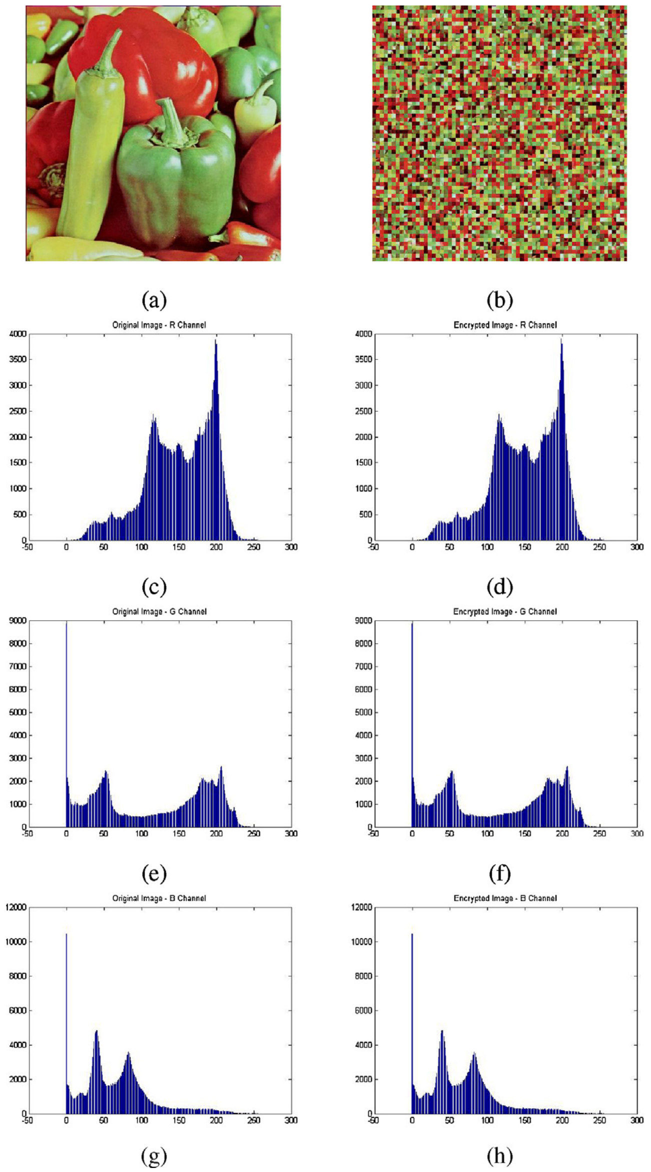
(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)

Fig. 1. (a) Plain image; (b) cipher image. Histogram of plain image: (c) red channel; (e) green channel; (g) blue channel. Histogram of cipher image: (d) red channel; (f) green channel; (h) blue channel.

Hence the encryption algorithm is insecure against attacks such as known/chosen plain text attack and statistical attack.

The encryption scheme is also tested using black image i.e., an image with all pixel value as 0. Fig. 2 shows that when a black image is encrypted the cipher image is again a black image. This shows that no encryption has taken place and hence known plain text attack is possible.

Table 1
Correlation coefficients between adjacent pixels of plain-image and cipher-images.

	Plain image			Cipher image		
	Red	Green	Blue	Red	Blue	Green
Horizontal	0.9757	0.9236	0.9742	0.8286	0.8557	0.8831
Vertical	0.9808	0.9833	0.9656	0.8649	0.8917	0.8262
Diagonal	0.9563	0.9728	0.9421	0.7217	0.7591	0.7180