Optik 127 (2016) 5695–5701

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

Breaking an image encryption algorithm based on the new substitution stage with chaotic functions

Benyamin Norouzi*, Sattar Mirzakuchaki

Electronic Research Center, School of Electrical Engineering, Iran University of Science and Technology, P.O. Box 16846-13114, Tehran, Iran

ARTICLE INFO

Article history:
Received 19 June 2015
Received in revised form 27 October 2015
Accepted 29 March 2016

Keywords:
Image encryption algorithm
Cryptanalysis
Substitution
Keystream

ABSTRACT

This paper is a cryptanalysis of a recent proposed image encryption algorithm based on chaotic functions. The cryptosystem is composed of two-stage permutation and one-stage substitution for encryption of the gray scale plain-image. However, by applying chosen plaintext attack which is described in this paper, we show that all the secret parameters can be revealed. In addition, some other security defects of the cryptosystem are also highlighted. Both mathematical analysis and experimental results confirm the feasibility of this attack. As a result, the cryptosystem in this structure cannot be recommended when we need a higher level of security.

1. Introduction

A chaotic system is a good candidate for cryptography due to its characteristics such as deterministic dynamic, random-like behavior, ergodicity, and sensitivity to initial conditions and control parameters [1–3]. These features characterize excellent properties of diffusion and confusion, which are of great importance in cryptography and image encryption algorithms. As a result, many proposals dealing with both cryptography and chaos have been published in the last decades [1–7]. These algorithms are mainly composed of two aspects: confusion and diffusion. In the confusion process, the pixels of the image are permutated by some chaotic maps while in the diffusion phase, the pixels are modified such that a minute change in one pixel of the plain image causes the corresponding cipher image to be considerably different [6]. Meanwhile, some cryptanalysis work demonstrated that some image cryptosystems are insecure against various conventional attacks, especially on chosen-plaintext attack. The common feature of these algorithms is that the keystream used to encrypt different plain-images are the same. In other words, the keys are independent of the plain-images. For example, Huang proposed an image encryption algorithm based on a Chebyshev function [7]. But Wang et al. broken it with cryptanalytic methods and pointed out some other weaknesses of this cryptosystem [8]. Zhang and Wang [9] analyzed the potential flaws in Zhu's cryptosystem [10] in detail and developed a chosen-plaintext attack and chosen-ciphertext attack on this algorithm. Zhu et al. in [11] demonstrated that Zhang and Liu's cryptosystem [12] is not suitable for cryptography. Also, some image encryption algorithms such as Refs. [13–15] are cracked by Refs. [16–18], respectively.

Moreover, Parvin et al. proposed a new image encryption scheme based on chaotic sequences [19]. This algorithm includes permutation of rows and columns and substitution of pixels values with XOR operation. In the permutation procedure, the row and column transform vectors are derived from chaotic functions. And in the substitution procedure, the authors use

* Corresponding author.
E-mail addresses: Benyamin_Norouzi@elec.iust.ac.ir (B. Norouzi), M_Kuchaki@iust.ac.ir (S. Mirzakuchaki).

http://dx.doi.org/10.1016/j.ijleo.2016.03.076
0030-4026/

simple operations to achieve diffusion. One idea of this algorithm is using all pixels of the plain-image except the first pixel to produce the first pixel of cipher matrix. Although there are a lot of advantages (such as large key space, less encryption time and high key sensitivity which are described in [19]), we find that the encryption algorithm is not robust to resist chosen-plaintext attack. In this paper, we make some analysis on Parvin's algorithm, and break it using chosen-plaintext attack.

The rest of the paper is organized as follows. In the next section the cryptosystem under study is described. In Section 3, a chosen plaintext attack that reveals the equivalent keys is analyzed. After that, the experimental results are given in Section 4. Finally, the last section summarizes the results of the previous sections and concludes the paper.

2. Description of the cryptosystem under study

In The cryptosystem proposed in [19], two-stage permutation and one-stage substitution are used for encryption of the gray scale plain-image of size $M \times N$. Three pseudorandom number matrices (K_1–K_3) are generated to be used in permutation and substitution stages. The detailed descriptions of each stage are presented next.

2.1. Key generation

The cryptosystem is based on two one-dimensional chaotic functions and the combination of them. These chaotic functions are given by Eqs. ((1)–(3)).

$$f_1(x_i) = x_{i+1} = 8{x_i}^4 - 8{x_i}^2 + 1; i = 1, 2, \ldots, M \tag{1}$$

The produced sequences are mapped to the interval [0,255] and are used as matrix K_1. The size of this matrix is $M \times 1$ (M is the number of rows of plain-image).

$$f_2(x_i) = x_{i+1} = 4{x_i}^3 - 3x_i; i = 1, 2, \ldots, N \tag{2}$$

Also, the outputs of above equation are mapped into [0,255] to obtain the chaotic matrix K_2. The size of this matrix is $1 \times N$ (N is the number of rows of plain-image). The combination of the two functions is then used.

$$a = \frac{x_1 + x_2}{2}$$
$$\begin{cases} \text{if } a < 0, \ f_1 = 8{x_1}^4 - 8{x_1}^2 + 1 \\ f_1 = x_1 \\ \text{if } a > 0, f_2 = 4{x_2}^3 - 3x_2 \\ f_2 = x_2 \end{cases} \tag{3}$$

The number of iterations of Eq. (3) is $M \times N$. The outputs are mapped to the scale of 0–255. These numbers are used in matrix K_3. So, the size of matrix K_3 is $M \times N$.

2.2. Circular shift by row

The rows of plain-image are shifted using the corresponding number in matrix K_1. So, the first row of plain-image is shifted circularly using first number of matrix K_1 and the same action as first row is done in each row.

2.3. Circular shift by column

After horizontal rotation of all rows of plain-image, the resulted matrix is then shifted circularly in the vertical direction with respect to the matrix K_2.

2.4. Substitution

The resulted image of previous stage is converted into one-dimensional 8-bit integer vector $P = \{p_1, p_2, \ldots, p_{M \times N}\}$. The substitution operation is as follows:

$$c_1 = \text{bitxor}\left(p_1, \text{bitxor}\left(\text{mod}\left(\sum_{i=2}^{M \times N} p_i, 256\right), k_1\right)\right) \tag{4}$$

$$c_i = \text{bitxor}\left(p_i, \text{bitxor}\left(\text{mod}\left(c_{i-1} + k_i, 256\right), k_i\right)\right); i = 1, 2, \ldots, M \times N \tag{5}$$

where $K_3 = \{k_1, k_2, \ldots, k_{M \times N}\}$ is the key stream and cipher-image is denoted by one-dimensional vector $C = \{c_1, c_2, \ldots, c_{M \times N}\}$. By reshaping the sequence C into an $M \times N$ image, the cipher-image is obtained.