Cryptanalysis of an authenticated image encryption scheme based on chaotic maps and memory cellular automata

S. Kabirirad * H. Hajiabadi

Department of Computer Engineering, Birjand University of Technology, Birjand, Iran

Abstract

Recently an image encryption scheme based on chaotic maps and memory cellular automata has been proposed. In this paper, the security of the scheme is evaluated and it is demonstrated that the scheme can be broken by chosen plain-text attack. Having one or more monochrome plain-images and their corresponding cipher-images, a part of key-stream can be retrieved. Furthermore, it is discovered that the scheme can be broken by brute search attack with efficient time complexity, and it is also vulnerable to differential attack. Meanwhile, we provide experimental results to support the proposed attacks and suggest several improvements to make scheme stronger.

Key words: Image encryption, Cryptanalysis, Chosen plain-text attack, Brute search attack, Differential attack, Improvement

* Corresponding author. Tel.: +985632391299
Email addresses: kabiri@birjandut.ac.ir (S. Kabirirad), hajiabadi@birjandut.ac.ir (H. Hajiabadi).

1 Introduction

In order to store and transmit information in many fields like military, medical, industry or personal usages, digital images are widely used. To protect images against unauthorized accesses, a commonly used way is utilizing cryptography schemes. Because of certain properties of images such as bulky data capacity and strong correlation among pixels, the traditional cryptographic protocols are not suitable. Therefore particular encryption schemes are used to encrypt images. According to Shannon theory [1] for high security of encryption scheme, two principles of confusion and diffusion must be regarded. Confusion means that the relationship between key and cipher-text is complicated. Diffusion refers to dispersing the statistical features of plain-text over cipher-text.

In the image encryption scheme, confusion and diffusion are provided using different methods. One of the prevalent methods is chaotic maps. Some of the essential properties of chaotic maps which make it interested are the important role of initial conditions and control parameters. Therefore image encryption schemes based on chaotic maps obtain high complexity, diffusion and security.

In recent years, image encryption schemes based on chaotic maps have been extensively studied [2–6]. These schemes have applied various chaotic maps and different encryption algorithms. Meanwhile, some researches have focused on cryptanalysis of these schemes [7–11]. Alvarez et.al [12] listed well-known attacks in chaos based cryptosystems including: weak robustness against chosen cipher-text attack or chosen plain-text attack, poor statistical characteristics of chaotic map, vulnerability to differential attack or statical attack, low sensitivity to the keys and so on and proposed rules to guarantee a reasonable degree of security. Specifically key-stream must be thoroughly correlated with plain-image's pixels, otherwise the attacker can obtain information about key-stream.

In this paper, we analyze an image encryption scheme [13] and propose several attacks and

corresponding improvements. In [13] an authenticated image encryption scheme based on chaotic maps and memory cellular automata has been proposed. In permutation phase, pixels are permuted using a chaotic map. Cellular automata and another chaotic map are applied to modify pixels in diffusion phase. In the paper and another papers [5,6], application of cellular automata is resulted to high security, low computation time and large key space.

In this paper, it is fully discussed that the scheme, is vulnerable to chosen plain-text attack. Having one or more monochrome plain-image and corresponding cipher-image, a part of key-stream can be obtained. Furthermore an efficient brute search attack is proposed that can retrieve permuted image. We explain that the scheme is not sufficiently robust against differential attack. Also, we presented experimental results of proposed attacks.

The rest of this paper is organized as follows. In the next section, the image encryption scheme is reviewed. In section 3, the cryptanalysis of the algorithm is fully described. Section 4 is included several proposed improvements in order to fulfill the drawbacks. The last section concludes the paper.

2 Review Of The Protocol

The scheme [13] can be divided into four phases: (1) the permutation phase, (2) the image encrypting phase, (3) the image decryption phase and (4) the data integrity validation phase intended to detect any interference during the transmission. In the scheme, the pseudorandom key-streams are created by piecewise linear maps in permutation phase and logistic chaotic map in image encrypting phase. The piecewise linear map is explained

according to the following formula:

$$f(x) = \begin{cases} x/p & \text{if } x \in [0, p), \\ (x-p)/(0.5-p) & \text{if } x \in [p, 0.5), \\ f(1-x, p) & \text{if } x \in [0.5, 1) \end{cases} \tag{1}$$

where $x \in [0, 1]$ and $p \in [0, 0.5]$. The following equation described the logistic chaotic map:

$$y_{n+1} = 4y_n \times (1 - y_n), \quad y_n \in [0, 1] \tag{2}$$

In the following the image cryptosystem phases are described in details.

2.1 The Permutation Phase

Denoting the size of the original grayscale image P by $M \times N$, the permutation process follows these steps:

(1) To achieve $\{x_1,\ x_2...,\ x_{MN}\}$, the piecewise linear map is iterated $M \times N$ times.

(2) The set $\{x_1,\ x_2,\ ...,\ x_{MN}\}$ are sorted increasingly and a new set $\{x'_1,\ x'_2,\ ...,\ x'_{MN}\}$ is obtained.

(3) Indexes of the items included in the set $\{x'_1,\ x'_2,\ ...,\ x'_{MN}\}$ is retrieved from $\{x_1, x_2, ..., x_{MN}\}$ and the index set $S = \{s_1,\ s_2,\ ...,\ s_{MN}\}$ is formed, where x'_i is the value of x_{s_i}.

(4) Pixels of the plain-image P are permutated using the set S in order to achieve $P' = \{P'_1,\ P'_2,\ ...,\ P'_{M\times N}\}$, where $P'_i = P_{s_i}\ \ (i = 1, 2, ..., M \times N)$.

2.2 Image Encrypting Phase

The permuted image P' is divided into n_b block with size m, where $n_b = \lceil M \times N/m \rceil$. For each block B_i , the following steps are executed:

(1) Reversible linear memory cellular automata (LMCA) of order $m+2$, denoted as L, is constructed and initialized with configuration $\{C^{(1)},\ C^{(2)},\ ...,\ C^{(m+2)}\}$ as follows:

   (a) Set $C^{(1)} = B_i(1),\ C^{(2)} = B_i(2),\ ...,\ C^{(m)} = B_i(m)$, where $B_i(k)$ denotes the kth pixel of the ith block.

   (b) Set $C^{(m+1)} = H_i$, in which $H_i = f_h(B_i(1),\ ...,\ B_i(m))$, where f_h is a collision-resistant hash function.

   (c) If $i = 1,\ C^{(m+2)}$ is assigned to a random number between 0 and 255, otherwise $C^{(m+2)} = D_i$, where $D_i = B_{i-1}(1) \oplus B_{i-1}(2) \oplus ... \oplus B_{i-1}(m)$.

(2) L is performed w times, starting from the initial configuration $\{C^{(1)},\ C^{(2)}... ,C^{(m+2)}\}$ in order to obtain the new configuration $\{A_i(1),\ A_i(2),\ ...,\ A_i(m+2)\}$.

(3) $A_i(m+1)$ encrypted as following:

- $K_i = \ 1 + mod(A_i(1), 4)$ is computed.
- The logistic chaotic map (2) is iterated K_i times in order to obtain the value y.
- The encrypted value $A_i(m+1)$ is computed according to the following formula:

$$A'_i(m+1) = \ A_i(m+1) \oplus mod\Big(d + A_i(m+2), 256\Big) \tag{3}$$

  Where $d = floor(mod(y \times 10^6), 256)$.

(4) The corresponding cipher block is set to $\psi_i = \{A_i(1),\ A_i(2),\ ..., A'_i(m+1),\ A_i(m+2)\}$.

2.3 Image Decryption Phase

The decryption algorithm is somehow similar to the encryption one. For each cipher block, the following steps must be performed.

(1) $A_i(m+1) = A'_i(m+1) \oplus mod\Big(d + A_i(m+2), 256\Big)$ is computed ,where the value d is obtained like the process done in the encryption phase.

(2) The inverse of LMCA with initial configurations $\{A_i(1),\ ...,\ A_i(m+1),\ A_i(m+2)\}$

is constructed. It is evolved w times to obtain the values $\{B_i(1),\ ...,\ B_i(m),\ H_i,\ D_i\}$.

(3) When all of the blocks are recovered, the reverse operation of the permutation phase should be employed.

2.4 Data Integrity Validation Phase

Block P' which is contained m pixels is authenticated as follows.

(1) $h_i = f_h(B_i(1), ..., B_i(m))$ is evaluated.

(2) If h_i, is equal to the value H_i, which is obtained from decryption phase, the block is authenticated.

3 Cryptanalysis

In the permutation phase x and p are considered as key and in the image encrypting phase y_0 is regarded as key. It is assumed that local rules and the number of iteration of LMCA (w) can not be included in the key. According to this assumption, the cryptanalysis and attacks is proposed and are described below in detail.

3.1 Chosen Plain-text Attack

The proposed algorithm is not robust against chosen plain-text attack and in the encrypting phase the key-stream can be revealed by selecting one or more monochrome images and the corresponding cipher-images. In this section, initially the key-stream are specified and then the attack is expressed in detail. It is explained that there is no correlation between key-stream and plain-image; hence the scheme is not strong against chosen plain-text at-

tack.

Suppose that the selected image is included pixels with the arbitrary same value and $M \times N$ size, hence in the permutation phase, the permutated image P' will be equal to the plain-image P. The information obtained by ith block of $P' = P$ and ψ is illustrated as the following:

(1) The values of pixels in the ith block of the plain-image is denoted as: $B_i = \{B_i(1),\ B_i(2),\ ...,\ B_i(m)\}$

(2) The values can be calculated from $B_i : D_{i+1},\ H_i$

(3) The values of pixels in the ith block of the cipher-image are denoted as: $\psi_i = \{A_i(1),\ A_i(2),\ ...\ , A_i(m),\ A'_i(m+1),\ A_i(m+2)\}$

(4) The value of $A_i(m+1)$ will be obtained by iterating LMCA for w times with initial configuration $C^{(1)} = B_i(1),\ ...,\ C^{(m)} = B_i(m),\ C^{(m+1)} = H_i,\ C^{(m+2)} = D_i$

(5) Using equation (3) and the results which are earlier obtained, d_i (d in ith block) can be achieved as:

$$d_i \equiv \Big(A'_i(m+1) \oplus A_i(m+1)\Big) - A_i(m+2)(mod256) \tag{4}$$

Now we explained how the key-stream is evaluated. The values obtained from logistic map $y_0,\ y_1,\ ...$ only depends on the initial condition y_0. We denote values of d in blocks of the image with sequences $\{d_i\}_{i=1}^{n_b}$. Since to calculate d_i, the logistic map should be iterated for K_i times initialized with previous value of y, then correlation between sequences $\{d_i\}_{i=1}^{n_b}$ and $\{y_j\}_{j=0}$ can be formulated as:

$$\begin{aligned} d_1 &= \ floor(mod(y_{R_1} \times 10^6), 256), \\ d_2 &= \ floor(mod(y_{R_2} \times 10^6), 256), \\ &..., \\ d_{nb} &= \ floor(mod(y_{R_{nb}} \times 10^6), 256) \end{aligned} \tag{5}$$

Where $R_l = \sum_{\{j=1\}}^{l} K_j$.

We consider $y'_i = floor(mod(y_i \times 10^6), 256)$. With knowing $\{y'_j\}_{j=1}^{4n_b}$, sequence $\{d_i\}_{i=1}^{n_b}$ can be computed and the encryption phase and decryption phase can be done for each plain/cipher image with the same key. therefore it can be considered as the key-stream. Although $\{d_i\}_{i=1}^{n_b}$ is influenced by the image's pixels, but the key-stream $\{y'_j\}_{j=1}^{4n_b}$ is independent.

Using this plain-image and some more images and the corresponding cipher-images, all of the key-stream $\{y'_j\}_{j=1}^{4n_b}$ can be achieved from their sequences $\{d_i\}_{i=1}^{n_b}$. Figure 1 shows the block diagram of this attack.

Since the key-stream is finite and K holds in 1 up to 4, a few number of images (much less than 255) are required. Consequently the algorithm can be done in $O(k.t)$ time complexity, where $k \leq 255$ and t is the running time for one image.

Every image which is encrypted by the same key, can be decrypted by key-stream $\{y'_j\}_{j=1}^{4n_b}$. For this reason to obtain K_i for ith block, $A_i(1)$ is utilized. Then sequence $\{d_i\}_{i=1}^{n_b}$ is computed using the sequence $\{y'_j\}_{j=1}^{4n_b}$ and finally steps 1 and 2 of the decryption phase is followed.

To demonstrate the attack is applicable and effective, we selected 12 monochrome images of size 256×256 and their corresponding ciphers that encrypted with the same key, and performed the algorithm. We discovered whole of the key-stream of the image encrypting phase and then employed it to recovered Figure 2b that is diffused of Figure 2a (using the image encrypting phase). Recovered image is illustrated in Figure 3a which is identical with the original image.

Also, according to equation 1 there is no correlation between key-stream used in permutation phase and the plain-image; so the key-stream of this phase can be discovered using chosen plain-text attack.

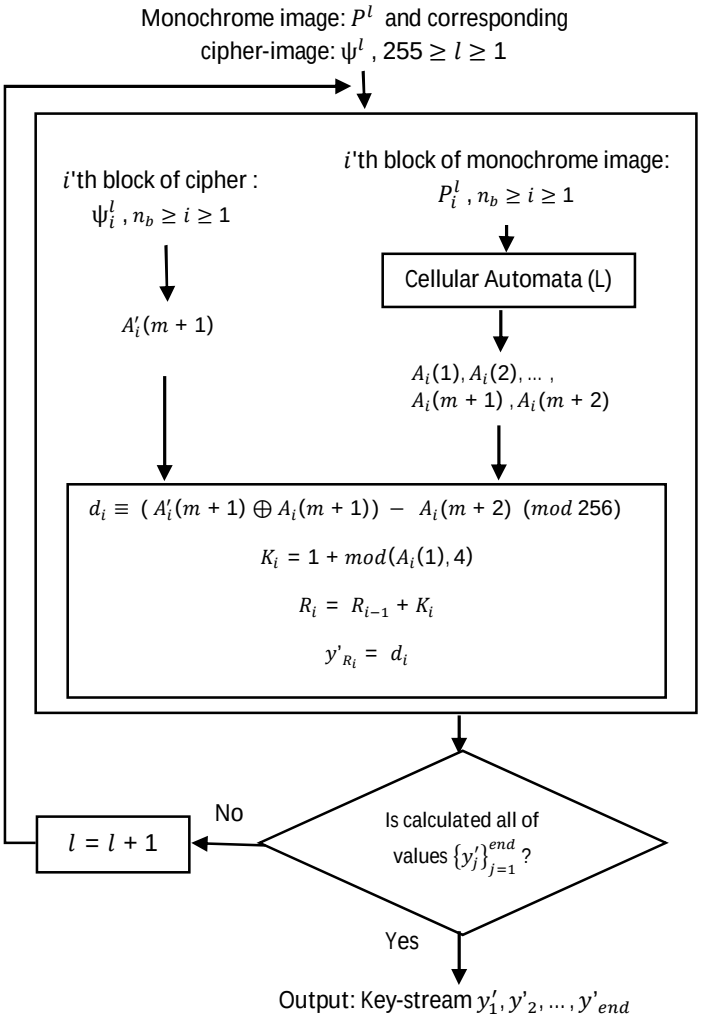
3.2 Brute Search Attack

In decryption phase, for initializing of reverse of LMCA ($\widetilde{L}$), all of the cells are clarified except $A_i(m+1)$ which is included 8 bits. The number of all possible states is 2^8. Because of the few candidate state and the speed of cellular automata, the brute search attack (BSA) will be succeed. In the following, the attack is explained.
For each block $1 \leq i \leq n_b$, the attacker executes the following steps.

(1) The attacker selects an integer number $b \in \{0, 1, ..., 255\}$,
(2) The attacker considers $A'_i(m+1) = b$,
(3) Sets initial configuration of $\widetilde{L}$ with $A_i(1),\ A_i(2),\ ...,\ A_i(m),\ b,\ A_i(m+2)$,
(4) After executing $\widetilde{L}$, the attacker achieves the values $\{B'_i(1)\ , ...,\ B'_i(m+2)\}$,
(5) Calculates $H'_i = f_h(B'_i(1),\ ...,\ B'_i(m))$.
(6) If $H'_i \neq B'_i(m+1)$, the steps are iterated for next b, else the block's value is recovered.

The attack is applicable and it outputs information about permutated image. In order to evaluate the running time of the attack algorithm, since the algorithm is iterated almost 2^8 times for each block, the running time in the worst case is in $O(256.n_b.t)$, where t is the running time of LMCA for one block. We executed the attack on Figure 2b (which is only affected by image encrypting phase). The output is illustrated in Figure 3b. The results show that 91% of pixels are recovered correctly. The remaining pixels which are recovered incorrectly are due to collision in the hash function.
Note that, in two preceding attacks, we can compute additional parameters (for example D in Brute-search attack) to optimize implementations.

Fig. 1. Block diagram of chosen plain-text attack

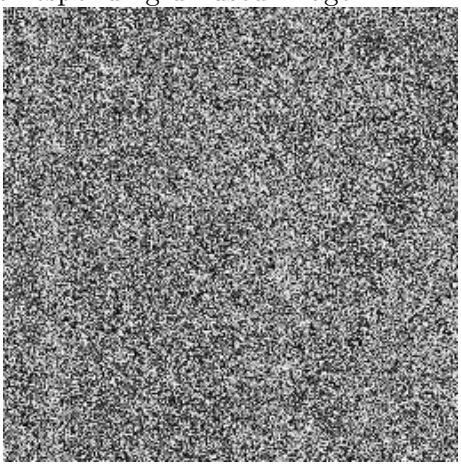


3.3 Robustness Against Differential Attack

To make a scheme robust against differential attack, it needs a little change in plain-image (for example a change in a pixel), results in alteration every bit of the corresponding cipher-image with a probability of a half. This algorithm hasn't sufficient sensitivity with respect to plain-image. If ith block of permutated image is partially changed, there is no effect in the previous encrypted blocks. The change affects on ith cipher block directly, but its effect is low and gradually disappears in the subsequent blocks. Because ith block is

Fig. 2. One Plain-image and corresponding diffused image

(a) Plain-image "Lena"



(b) Diffused image of (a)

Fig. 3. Recovered images by chosen plain-text attack and brute search attack

(a) The recovered image of 2b by CPA

(b) The recovered image of 2b by BSA

only affected in one pixel, D_{i+1}, of $i+1$th block and has not direct influence in next blocks. In order to measure effect of a tiny change of plain-image on its cipher-image, the number of pixel change rate (NPCR) and the unified averaged changing intensity (UACI) are computed. NPCR close to 100% and UACI close to 33.5% indicate high sensitivity of cipher-image with respect to plain-image. For example, we computed NPCR and UACI for image "Lena" of size 256×256 and obtained NPCR = 0.13% and UACI = 0.09%.

Therefore the scheme hasn't sufficient robustness against differential attacks.

4 Remedial Methods

In chaos-based image encryption schemes, key-stream must be thoroughly correlated with plain-image's pixels, otherwise the attacker can obtain information about key-stream. In the following, we propose some improvements to overcome presented drawbacks.

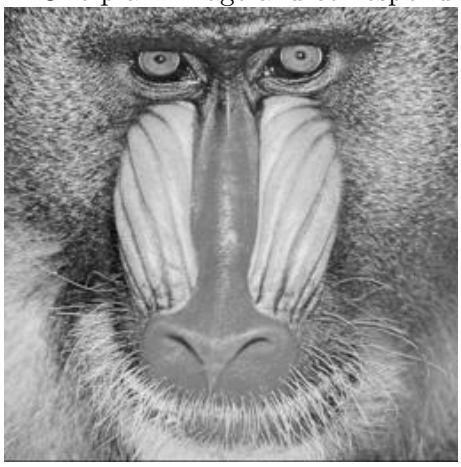
(1) To achieve robustness against known plain-text attack the key-stream for every image must be different from another. Then key-stream should also depend on the pixels of original image. The initial value of logistic chaotic map for every block can be calculated using combination of last value's chaotic map and the image's pixels. For example, initial value of map for first block can be y_0 and for ith ($i > 1$) block can be followed by the subsequent equation:
$y_i = (H_{i-1} \times 10^{-4} + y_{i-1}) mod\ 1$, where y is previous value of chaotic map and H_{i-1} is hash value of the previous block pixels.
Furthermore local rules for each block can be achieved by the image's pixels and a chaos stream. Also, this increases the robustness against the differential attacks.

(2) In order to strengthen the proposed algorithm against brute search attack, the local rules and w must be contained in the key.

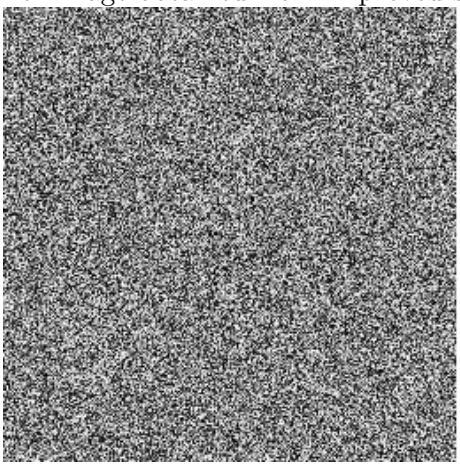
(3) In order to make the proposed algorithm more robust against the differential attack, the cellular automata could be performed again from last block to the first block after step 2-c in image encrypting phase. Consequently a change in a block of image will affect on previous blocks.

Implementations confirm that these remedial methods improve the scheme. Figure 4 shows a plain-image and corresponding cipher-image. Table 1 shows correlation coefficients of the plain-image and its cipher-image. Also Table 2 illustrates NPCR and UACI test results.

Fig. 4. One plain-image and corresponding cipher-image obtained from improved scheme.



(a) plain image "Baboon"



(b) cipher image

Table 1

Correlation coefficients of plain-image ("Baboon") and cipher-image

correlation	Vertical	Horizontal	Diagonal
Plain-image	0.850	0.887	0.803
Cipher-image	-0.018	0.010	0.024

Table 2

The average NPCR and UACI of improved scheme

image name	Lena	Baboon	CameraMan
Average NPCR(%)	99.32	99.43	99.39
Average UACI(%)	33.16	32.81	32.96

5 Conclusion

In this paper, we propose a chosen plain-text attack on an image encryption method based on chaotic maps and cellular automata. It is revealed that a part of key-stream

can be achieved by several images and their corresponding ciphers. Furthermore a brute search attack is fully demonstrated and it is shown that the attack is applicable. We show that the scheme has low sensitivity with respect to the changes of plain-image and also present experimental results of attacks. Finally, we propose some remedial methods and experimental results of improved scheme.

References

[1] C.-E. Shannon, Communication theory of secrecy systems, Bell System Technical Journa 28 (1949) 656–715.

[2] M. François, T. Grosges, D. Barchiesi, R. Erra, A new image encryption scheme based on a chaotic function, Signal Processing: Image Communication 27 (2012) 249–259.

[3] Z. Eslami, A. Bakhshandeh, An improvement over an image encryption method based on total shuffling, Optics Communications 286 (2013) 51–55.

[4] X. Tong, Design of an image encryption scheme based on a multiple chaotic map, Commun Nonlinear Sci Numer Simulat 18 (2013) 1725–1733.

[5] K. Mohamed-Faraoun, Design of fast one-pass authenticated and randomized encryption schema using reversible cellular automata, Commun Nonlinear Sci Numer Simulat 19(9) (2014) 3136–3148.

[6] P. Ping, F. Xu, Z.-J. Wang, Image encryption based on non-affine and balanced cellular automata, Signal Processing 115 (2014) 419–429.

[7] B. Wang, X. Wei, Q. Zhang, Cryptanalysis of an image cryptosystem based on logistic map, Optik 124 (2013) 1773–1776.

[8] C. Çokal, E. Solak, Cryptanalysis of a chaos-based image encryption algorithm, Physics Letters A 373 (2009) 1357–1360.

[9] H. Liu, Y. Liu, Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Optics and Laser Technology 56 (2014) 15–19.

[10] G. Tu, X. Liao, T. Xiang, Cryptanalysis of a color image encryption algorithm based on chaos, Optik 124(22) (2013) 5411–5415.

[11] Y. Zhang, Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system, Optik 126(2) (2015) 223–229.

[12] G. Alvarez, S.-J. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Internat. J. Bifur. Chaos 16 (2006) 2129–2151.

[13] A. Bakhshandeh, Z. Eslam, An authenticated image encryption scheme based on chaotic maps and memory cellular automata, Optics and Lasers in Engineering 51 (2013) 665–673.