Cryptanalysis Of An Authenticated Image Encryption Scheme Based On Chaotic Maps And Memory Cellular Automata.

Saeideh Kabirirad[1], Hamideh Hajiabadi[2]
[1,2] Department of Computer Engineering, Birjand University of Technology, Birjand, Iran
[1]kabiri@birjandut.ac.ir, [2]hajiabadi@birjandut.ac.ir

1 Abstract

In this paper, the security of an authenticated image encryption scheme based on chaotic maps and memory cellular automata is evaluated. It is demonstrated that the scheme can be broken by chosen plain-text attack. Furthermore, the authentication algorithm of the scheme is faulty and reveals information about the plain-image and it also results in a brute search attack with efficient time complexity. Also the scheme suffers from differential attacks because of low sensitivity to the plain-image. We provide experimental results to support the proposed attacks. Finally, we suggest some remedial methods to fix the weaknesses and enhance sensitivity to the plain-image modifications.

Keywords

Image encryption, Security, Chosen plain-text attack, Brute search attack, Differential attack.

2 Introduction

Recent advances in computing technology have turned secure storing and transmission of confidential digital data an important issue. Images have extensive application in various fields and are widely used in Internet communications. So, the secure transmission of images has become more significant and image encryption schemes have attracted scholars. Due to some intrinsic features of images such as bulky size and high correlation among pixels, traditional encryption methods like DES and RSA are not suitable for images. Properties of chaotic systems such as strong sensitivity to the initial conditions and control parameters, random-like behavior and ergodicity are quite advantageous in image encryption schemes [1] and consequently chaos-based image encryption schemes obtain high complexity and security. These algorithms are mainly composed of two aspects: (1) confusion that the pixels of plain-image are permutated; and (2) diffusion that the pixels' values are changed such that the effect of slight change in a pixel of plain-image is reflected on large number of pixels in cipher-image.

In recent years, image encryption schemes based on various chaotic maps have been extensively studied [2-11]. Some of these image encryption schemes [4,8-10] have authentication property, i.e. integrity of decrypted image can be checked. However, researchers have analyzed some of them and showed they are not secure enough to resist against some common attacks [12-16]. Some 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 statistical attack, low sensitivity to the keys and so on and proposed rules to guarantee a reasonable degree of security [17].

Specifically key-stream must be thoroughly correlated with plain-image's pixels otherwise the attacker can obtain information about the key-stream. This point is not considered in some image encryption schemes. For example in [13] the security of proposed algorithm in [7] was evaluated, and it was discovered that the scheme can be broken by chosen plain-text attack. Also, it was showed that the scheme hasn't enough sensitivity to the slight change of plain-image. Paper [18] evaluated an image encryption algorithm using Chebyshev generator, proposed in [19] and showed that the scheme is vulnerable to chosen plain-text attack, isn't sensitive enough to the alteration of plain-image and there exist weak keys for the encryption scheme. Wang et al [20] analyzed the image encryption proposed in [21] and Cokal and Solak [12] analyzed proposed scheme in [11]. They figured that the key-stream was revealed by chosen plain-text attack.

In [10] an authenticated image encryption scheme based on chaotic maps and memory cellular automata (MCA) has been proposed. In this paper and another papers [4, 5] application of cellular automata results in high security, low computational complexity and large key space. This paper focuses on security analysis of the scheme [10] and reports the following results: (1) the scheme can be broken by chosen-plaintext attack with one or more pair(s) of plain-image/cipher-image; (2) its authentication mechanism results in an efficient brute search attack that is concluded permuted image; (3) the scheme is not sufficiently sensitive to plain-image; (4) experimental results of the proposed attacks are represented and (5) some remedial methods are proposed and implemented.

The rest of this paper is organized as follows. In the next section, the analyzed image encryption scheme is reviewed. In section 3, the cryptanalysis of the algorithm is fully described. Section 4 includes several proposed improvements in order to fulfill the drawbacks. In Section 5 authentication algorithm is analyzed. The last section concludes the paper.

3 Review of Bakhshandeh and Eslami's scheme

The scheme [10] 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 aiming to detect any interference during the transmission. In the permutation phase, pixels are permuted according to a sequence made by piecewise linear maps as a chaotic map. In the encrypting phase, blocks of pixels are diffused by a reversible cellular automata (L) and then their hashed values are encrypted using logistic chaotic map. The piecewise linear map is explained according to the following formula:

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

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

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

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

3.1 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 $\{x_1, x_2 \ldots, x_{MN}\}$, the piecewise linear map is iterated $M \times N$ times.
2. The set $\{x_1, x_2, \ldots, x_{MN}\}$ is sorted increasingly and a new set $\{x'_1, x'_2, \ldots, x'_{MN}\}$ is obtained.
3. Indexes of the items included in the set $\{x'_1, x'_2, \ldots, x'_{MN}\}$ are retrieved from $\{x_1, x_2, \ldots, x_{MN}\}$ and the index set $S = \{s_1, s_2, \ldots, s_{MN}\}$ 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 $P' = \{P'_1, P'_2, \ldots, P'_{M\times N}\}$, where $P'_i = P_{s_i}$ $(i = 1,2,\ldots,M \times N)$.

3.2 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 $\{C^{(1)}, C^{(2)}, \ldots, C^{(m+2)}\}$ as follows:
   1-1. Set $C^{(1)} = B_i(1)$, $C^{(2)} = B_i(2)$, …, $C^{(m)} = B_i(m)$, where $B_i(k)$ denotes the k th pixel of the i th block.
   1-2. Set $C^{(m+1)} = H_i$, in which:
   $$H_i = f_h(B_i(1), \ldots, B_i(m)) \qquad (3)$$
   where f_h is a collision-resistant hash function.
   1-3. If $i = 1$, assign $C^{(m+2)}$ to a random number between 0 and 255, otherwise set $C^{(m+2)} = D_i$, where:
   $$D_i = B_{i-1}(1) \oplus B_{i-1}(2) \oplus \ldots \oplus B_{i-1}(m) \qquad (4)$$
2. Perform L for w times starting from the initial configuration $\{C^{(1)}, C^{(2)} \ldots, C^{(m+2)}\}$ in order to obtain the new configuration $\{A_i(1), A_i(2), \ldots, A_i(m+1), A_i(m+2)\}$.
3. $A_i(m+1)$ is encrypted as following:
   3-1. Compute:
   $$K_i = 1 + mod(A_i(1),4) \qquad (5)$$
   3-2. Iterate the logistic chaotic map (Equation 2) K_i times in order to obtain the value y and then calculate $d_i = \lfloor mod\ (y \times 10^6, 256) \rfloor$.
   3-3. Compute the encrypted value $A_i(m+1)$ according to the following formula:
   $$A'_i(m+1) = A_i(m+1) \oplus \mathrm{mod}(d_i + A_i(m+2), 256) \qquad (6)$$
4. Set the corresponding cipher block $\psi_i = \{A_i(1), A_i(2), \ldots, A'_i(m+1), A_i(m+2)\}$.

3.3 Image Decryption Phase

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

1. $A_i(m+1) = A'_i(m+1) \oplus mod\ (d_i + A_i(m+2),256)$ is computed ,where the value d_i is obtained like the process done in the encryption phase.
2. The inverse of LMCA with initial configurations $\{A_i(1),\ldots, A_i(m+1), A_i(m+2)\}$ is constructed. It is evolved w times to obtain the values $\{B_i(1), \ldots, B_i(m), H_i, D_i\}$.
3. When all of the blocks are recovered, the reverse operation of the permutation phase should be applied.

3.4 Data Integrity Validation Phase

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

1. $h_i = f_h(B_i(1),\ldots, B_i(m))$ is evaluated.
2. If h_i is equal to the value H_i, which is obtained from decryption phase, the block is authenticated.

4 Cryptanalysis

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

4.1 Chosen Plain-text Attack

In this section, we show that the proposed scheme is not robust against chosen plain text attack. The main idea of the attacks is to recover key-stream of the encrypting phase. With the key-stream instead of the secret key itself, the cipher-image can be decrypted.

At first, we specify the key-stream and then express the attack in detail. It is explained that there is weak correlation between the key-stream and the plain-image, hence with knowing one or more plain-images and corresponding cipher-images, the key-stream can be found.

Suppose that the attacker selects an image P of $M \times N$ size includes pixels with the arbitrary same value $0 \leq l \leq 255$ and acquires corresponding cipher-image ψ. In the permutation phase, the shuffled image P' will be equal to P. The attacker can obtain the following information by ith ($1 \leq i \leq n_b$) block of P' $(= P)$ and ψ:

1. The values of pixels in the ith block of P' are denoted as: $B_i = \{B_i(1), B_i(2), \ldots, B_i(m)\}$
2. The values of pixels in the ith block of ψ are denoted as: $\psi_i = \{A_i(1), A_i(2), \ldots, A_i(m), A'_i(m+1), A_i(m+2)\}$
3. The values of D_{i+1}, H_i can be calculated by equations 3 and 4.
4. The value of $A_i(m+1)$ can be obtained by evolving LMCA for w times with initial configuration $C^{(1)} = B_i(1), \ldots, C^{(m)} = B_i(m),\ C^{(m+1)} = H_i, C^{(m+2)} = D_{i-1}$
5. Using Eq. 6 and the previously obtained results, sequences $\{d_i\}_{i=1}^{n_b}$, where d_i means d in ith block, can be extracted from the following equation:

$$\mathrm{mod}(d_i + A_i(m+2), 256) = A'_i(m+1) \oplus A_i(m+1) \qquad (7)$$

Because both value of d_i and $A_i(m+2)$ are in range [0,255], then with having $A_i(m+2)$, we can calculate d_i easily.

Now we explained how the key-stream is evaluated. For this purpose, we show that key-stream is obtained using sequence $\{d_i\}_{i=1}^{n_b}$.

Suppose that sequence of the logistic map values with initial value y_0 is $\{y_j\}_{j=0}$. This sequence can be considered as the key-stream and with knowing it, the decryption phase can be proceed for each encrypted image with the same key. Sequence $\{y_j\}_{j=0}$ is independent from plain-image pixels and only related to initial value y_0. Now, we show how obtain partial values of it by one selected image and corresponding cipher-image. According to step 3-2 in image encrypting phase, the logistic map initialized with previous value of y, must be iterated K_i times to obtain y, i.e. for calculating y in the first block, the logistic map should be iterated K_1 times initialized with y_0, therefore y in first block equals with y_{K_1}. y in the second block is obtained from K_2 times iteration of the logistic map initialized with y_{K_1},that equals with $y_{K_1+K_2}$ and so as y in ith block equals with $y_{\sum_{j=0}^{i} K_j}$. Then correlation between sequences $\{d_i\}_{i=1}^{n_b}$ and $\{y_j\}_{j=0}$ can be formulated as:

$$\begin{aligned} d_1 &= floor\left(mod\left(y_{R_1} \times 10^6\right), 256\right) \stackrel{\text{def}}{=} y'_{R1}, \\ d_2 &= floor\left(mod\left(y_{R_2} \times 10^6\right), 256\right) \stackrel{\text{def}}{=} y'_{R2}, \\ &\ldots, \\ d_{nb} &= floor(mod(y_{R_{nb}} \times 10^6), 256) \stackrel{\text{def}}{=} y'_{R_{nb}} \end{aligned} \qquad (8)$$

where $R_l = \sum_{j=1}^{l} K_j$. For simplicity, we define $y'_i \stackrel{\text{def}}{=} floor(mod(y_i \times 10^6), 256)$ where is computable only using y_i. The sequence $\{y'_j\}_{j=0}$ so considered as the key-stream because this can be directly computed using the key-stream $\{y_j\}_{j=0}$and is applied in encryption/decryption process. Because maximum value of each $K_j, j = 1, .., n_b$ is equal to 4, the sequence $\{y'_j\}_{j=1}$ has at most $4 * n_b$ members. n_b members of the key-stream $\{y'_i\}$ are cleared using sequence $\{d_i\}_{i=1}^{n_b}$ of plain-image

P. Other members of $\{y'_j\}_{j=1}$ can be obtained by other selected monochrome images and their encrypted images with the same key. Flowchart of this attack can be found in Figure 1.

As it was explained, although $\{d_i\}_{i=1}^{n_b}$ is influenced by the image's pixels, but the sequence $\{y'_j\}_{j=1}^{4n_b}$ is independent from plain-image. Thus every plain-image PI which is encrypted with the same key, can be decrypted by the key-stream $\{y'_j\}_{j=1}^{4n_b}$. For this purpose, first $K_i, i = 1, \dots, n_b$ corresponding to ith block must be obtained by Equation 5 and then sequence $\{d_i\}_{i=1}^{n_b}$ must be computed using the sequence $\{y'_j\}_{j=1}^{4n_b}$. Finally steps 1 and 2 of the decryption phase can be followed.

Since the key-stream is finite and K holds in 1 up to 4, a few number of selected 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 selected image.

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

To demonstrate that the attack is applicable and effective, we performed the algorithm and can discover whole of the key-stream in the image encrypting phase using 12 selected images and corresponding cipher-images. After, we applied resulting key stream to decrypt secret image of Figure 3.b that is diffused of Figure 3.a. Recovered image is illustrated in Figure 4.a, which is same as the original one.

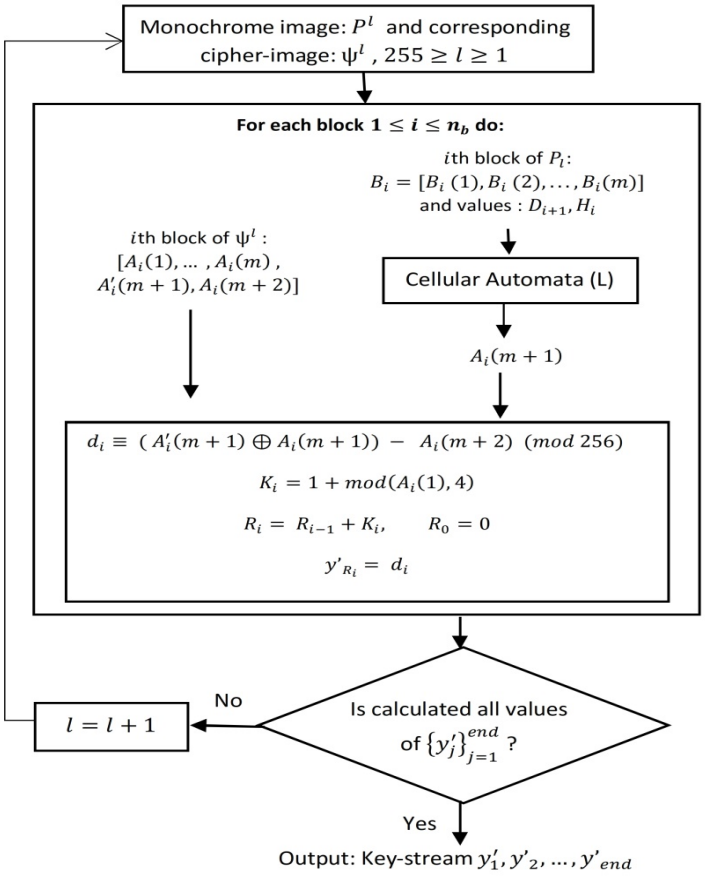

Figure 1. Flowchart of the chosen plain-text attack

4.2 Brute Search Attack

In the decryption phase, local rules and the number of iteration (w) of reverse of LMCA ($\tilde{L}$) are public, also for initializing of $\tilde{L}$, all of the cells are clarified except $A_i(m+1)$ which is included 8 bits. Therefore the number of all possible states is 2^8 . Because of the few candidate state and the high 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 $b \in \{0,1,\ldots,255\}$,
2. The attacker considers $A_i(m+1) = b$,
3. Sets initial configuration of $\tilde{L}$ as $A_i(1), A_i(2), \ldots, A_i(m), b, A_i(m+2)$,
4. After executing $\tilde{L}$, the attacker achieves the values $\{B_i'(1), \ldots, B_i'(m+2)\}$,
5. Calculates $H_i' = f_h(B_i'(1), \ldots, B_i'(m))$.
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 permutated image. Flowchart of the attack can be found in Figure 2.

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 is in $O(256.n_b.t)$ in the worst case, where t is the running time of LMCA for one block.

We executed the attack on Figure 3.b (which is only affected by image encrypting phase). The output is illustrated in Figure 4.b. 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 this attack, we can compute additional parameters (for example D) to optimize implementations.

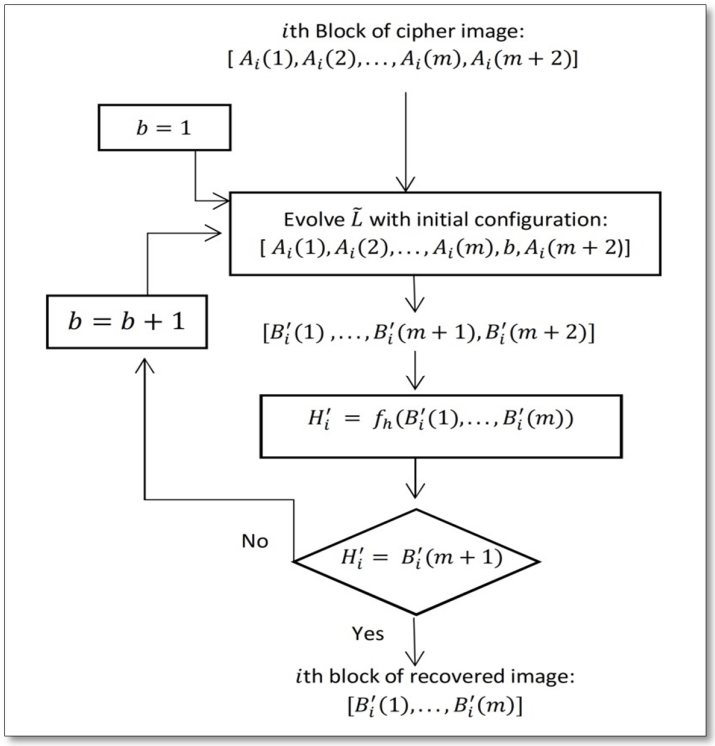

Figure 2. Flowchart of brut search attack

4.3 Robustness against Differential Attack

To make a scheme robust against differential attack, we need a change in plain-image (for example a change in one pixel), which results in alteration of every bit of the corresponding cipher-image with a probability of a half. We show that the algorithm hasn't sufficient sensitivity to plain-image. A change in ith block of permutated image influences on ith block of cipher-image directly. However the change has no effect in the previous encrypted blocks and its effect is low and gradually disappears in the subsequent blocks. Because ith block only influences on one pixel of $(i+1)$th block, i.e. D_{i+1}, and has not direct influence in the next blocks.

In order to measure effect of a slight 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 nearly equal to 100% and UACI nearly equal to 33.5% indicate high sensitivity to alteration of plain-image.

For example, we computed NPCR and UACI for image "Lena" with size 256×256 and obtained NPCR = 0.13% and UACI = 0.09%. Therefore the scheme hasn't sufficient robustness against differential attacks.

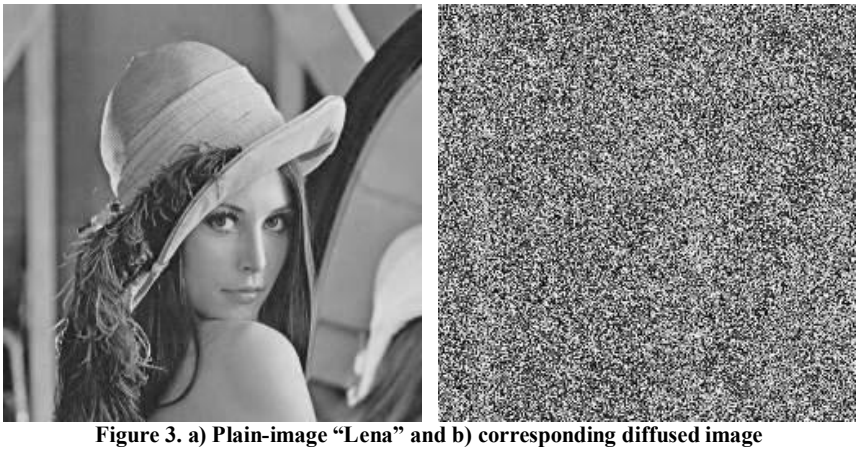

Figure 3. a) Plain-image "Lena" and b) corresponding diffused image

Figure 4. Recovered images by a) chosen plain-text attack and b) brute search attack

5 Remedial Methods

In chaos-based image encryption schemes, key-stream must be thoroughly correlated with the plain-image's pixels, otherwise the attacker can obtain information about the 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 plain-image must be different from another. Then key-stream should also depend on the pixels of plain-image. We offer the initial value of logistic

chaotic map in next block is calculated using combination of its value in previous block and the image's pixels. For example, initial value of map for first block can be y_0 and for i th $(i > 1)$ block can be followed by the subsequent equation: $y_i = (H_{i-1} \times 10^{-4} + y_{i-1}) \, mod \, 1$,

where y_{i-1} is last value of the chaotic map and H_{i-1} is hash value of the previous block's pixels. Furthermore local rules for each block can be achieved by the image's pixels and a chaos stream. Also, this solution 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. Also authentication algorithm must not reveal any information about plain-image.
3. In order to make the proposed algorithm more robust against the differential attack, one way is to applied the cellular automata again from last block to the first block after step 2-c in the image encrypting phase. Consequently a change in a block of image will influence on previous blocks.

Implementations confirm that these correctional methods improve the scheme. Figure 5 shows a plain-image and corresponding cipher-image. Table 1 shows correlation coefficients of several plain-images and corresponding cipher-images. Also Table 2 illustrates NPCR and UACI test results for different plain-images.

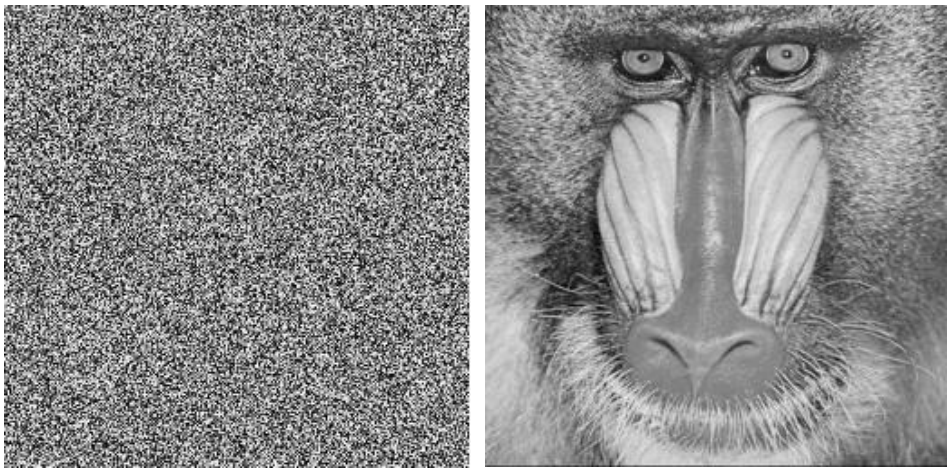

Figure 5. a) plain-image "Baboon" and b) corresponding cipher-image obtained from the improved scheme

Table 1. Correlation coefficients of plain-image ("Baboon") and corresponding 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 the improved scheme

Image name	Lena	Baboon	Cameraman
Average NPCR(%)	99.32	99.43	99.39
Average UACI(%)	33.16	32.81	32.96

6 Analysis of Authentication Algorithm

In the analyzed scheme, authentication was provided using additional pixels (2 pixels per each block) embedded in cipher-image. In the scheme, amount of redundancy is higher than its amount in some authenticated image encryption schemes [8, 9]. In [9] decrypted image is authenticated using a secret 128-bit hash value. In [8] a 132-bit initial key and a 64-bit hash value that are obtained from plain-image are combined and an extended key (148-bit) is resulted, this key is used for decryption and authentication of cipher-image. But, in all of these schemes partial information is revealed about the plain-image. Scheme [4] checks integrity using an extra 256 bits block that is obtained using a supplementary configuration of cellular automata and the secret key. Security of the integrity check algorithm based on sensitivity to small initial configurations variations and it does not reveal any information about image. In [22, 23] authentication and encryption schemes were presented based on optical systems, such that redundancy is low and also cipher-image can be authenticated without direct observation of plain-image information. The optical authentication method implies a sparse data and achieves efficient authentication. Therefore, the cipher designers can apply the idea of authentication in these schemes and utilize their advantages.

7 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 chosen 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 correctional methods and experimental results of improved scheme.

References

[1] Liu, Y., Tang, J., and Xie, T., (2014) Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map, Optics & Laser Technology, 60, 111-115.

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

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

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

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

[6] Zhou, Y., Bao, L. and Chen, P., (2014) A new 1D chaotic system for image encryption, Signal Processing, 97, 172-182.

[7] Abd El-Latif, A.-A., and Niu, X., (2013) A hybrid chaotic system and cyclic elliptic curve for image encryption, International Journal of Electronics and Communications, 67(2), 136-143.

[8] Singh Rajput A. and Sharma, M., (2015) A Novel Image Encryption and Authentication Scheme Using Chaotic Maps,

Advances in Intelligent Systems and Computing, 320, 277-286.

[9] Yang H., Wong, K.-W., Liao X., Zhang, W. and Wei, P., (2010) A fast image encryption and authentication scheme based on chaotic maps," Commun Nonlinear Sci Numer Simulat, 15, 3507-3517.

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

[11] Guan, Z. H., Huang, F., and Guan, W., (2005) Chaos-based image encryption algorithm, Physics Letters A," Physics Letters A, 346(1), 153-157.

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

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

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

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

[16] Jeng, F.-G., Huang, W.-L. and Chen, T.-H., (2015) Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes, Signal Processing: Image Communication, 34, 45-51.

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

[18] Wang, X., Luan, D., and Bao, X., (2014) Cryptanalysis of an image encryption algorithm using chebyshev generator, Digital Signal Processing, 25, 244-247.

[19] Huang, X.-L., (2012) Image encryption algorithm using chaotic chebyshev generator, Nonlinear Dynamics, 67(4), 2411-2417.

[20] Wang, X. and He, G., (2011) Cryptanalysis on a novel image encryption method based on total shuffling scheme, Optics Communications, 284, 5804-5807.

[21] Zhang G. and Liu, Q., (2011) A novel image encryption method based on total shuffling scheme, 2775-2780.," Optics Communications, 284(12), 2775-2780.

[22] Chen, W., Chen, X., Stern, A. and Javidi, B., (2013) Phase-modulated optical system with sparse representation for information encoding and authentication, IEEE Photonics Journal, 5(2), 6900113-6900113.

[23] Pérez-Cabré, E., Cho, M., and Javidi, B., (2011) Information authentication using photon-counting double-random-phase encrypted images, Optics letters, 36- 1, 22-24.