Cryptanalysis of image encryption with compound chaotic sequence

Ercan Solak
Department of Computer Engineering
Isik University, Istanbul, Turkey
Email: ercan@isikun.edu.tr

***Abstract*—Recently, an image encryption algorithm based on compound chaotic sequence was proposed [Tong et al., Image and Vision Computing 26 (2008) 843]. In this paper, we analyze the security weaknesses of the proposal. We give chosen-plaintext and known-plaintext attacks that yield the secret parameters of the algoritm. Our simulation results show that the computational complexity of the attacks is quite low.**

I. Introduction

During the last two decades, there has been a steady increase in the number of proposals for chaotic cryptosystems. Early proposals included the use of synchronized dynamical systems. In synchronization-based systems, a common coupling signal provides synchronized states. These states are, in turn, used to encrypt and decrypt messages [1]. Synchronization based cryptosystems can generate ciphertext with desirable statistical properties. However, these systems are weak against adaptive synchronization and identification attacks [2], [3], [4].

More recently, a number of chaotic image encryption systems have been proposed. Some of them use discretized chaotic systems in order to obtain algebraic transformations which operate directly on the plaintext image pixels [5], [6]. Others quantize discrete-time chaotic signals to obtain running key sequences [7], [8]

Although these approaches provide a framework similar to the general practice in classical cryptography, we still need to rigorously analyze each proposal in order to establish trust in its secure operation. For example, even if the statistical properties of a cryptosystem are at a desirable level, the algebraic structure of the system might contain flaws and weaknesses that can be exploited to compromise its security. Hence, a healthy co-development of chaos cryptography and chaos cryptanalysis provides the necessary framework for designing more secure chaotic cryptosystems.

In this paper, we give a complete break of the image encryption algorithm proposed in [7]. We apply chosen-plaintext and known-plaintext attacks and show that the algorithm can be completely broken using only a couple of known or chosen images. The method we employ is similar in spirit to the one proposed in [9]. However, in our approach, we use the particular structure of the permutation to yield an exact break.

The organization of the paper as follows. In the next section we give the description of the algorithm proposed in [7]. In Section 3, we give the chosen-plaintext attack. In section 4, we give known-plaintext attack. Section 5 illustrates the attacks with simulations. We finish with concluding remarks.

II. Description of the encryption scheme

The plaintext is an image of size $h \times w$, where each pixel is represented as a byte. The encryption involves three operations; mixing, row rotation and column rotation.

The scheme uses three chaotic systems to generate the pseudo-random variables used in the three steps. The key of the overall system is two real parameters $x_0, y_0 \in (-1, 1)$.

The first chaotic system is a 2D discrete-time system given as

$$\begin{aligned} \begin{bmatrix} x_n \\ y_n \end{bmatrix} &= F(\begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix}) \\ &= \begin{cases} \begin{bmatrix} f_0(x_{n-1}) \\ y_n \end{bmatrix} & \text{if } x_{n-1} + y_{n-1} < 0, \\ \begin{bmatrix} x_{n-1} \\ f_1(y_{n-1}) \end{bmatrix} & \text{if } x_{n-1} + y_{n-1} \geq 0, \end{cases} \end{aligned} \tag{1}$$

where $f_0(u) = 8u^4 - 8u^2 + 1$ and $f_1(u) = 4u^3 - 3u$. At each step, one of the state variables $x_n,\ y_n$ is chosen as

$$z_n = \begin{cases} x_n & \text{if } x_{n-1} + y_{n-1} < 0 \\ y_n & \text{if } x_{n-1} + y_{n-1} \geq 0 \end{cases} .$$

Finally, we obtain from z_n an integer k_n in the set $\{0, 1, \ldots, 255\}$ as

$$k_n = \lfloor 128(z_n + 1) \rfloor .$$

The chaotic system (1) is iterated hw times and the sequence $\{k_1, k_2, \ldots, k_{hw}\}$ is reshaped into an image using row scan. Let K denote this noise-like image.

The second chaotic system is given by

$$x_n = f_0(x_{n-1}). \tag{2}$$

An integer sequence ρ_n in $\{0, 1, \ldots, w-1\}$ is obtained using

$$\rho_n = \left\lfloor 3\frac{w}{2}(x_n + 1) \right\rfloor \bmod w. \tag{3}$$

The chaotic system (2) is iterated h times so, we obtain the sequence $\{\rho_1, \rho_2, \cdots \rho_h\}$.

The third chaotic system is given by

$$y_n = f_1(y_{n-1}). \tag{4}$$

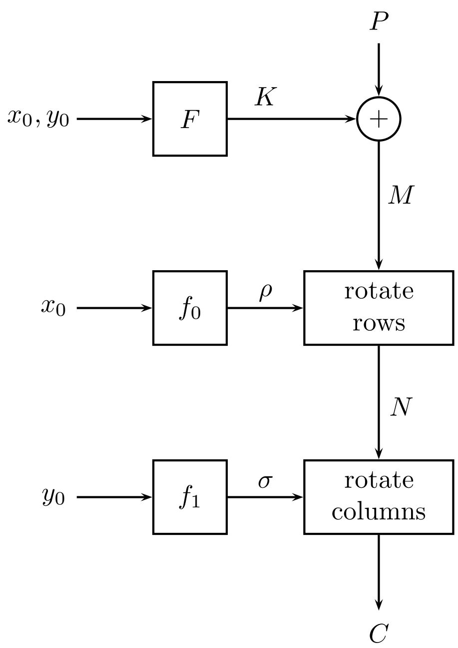


Fig. 1. Encryption algorithm.

Again, an integer sequence σ_n in $\{0, 1, \ldots, h-1\}$ is obtained using

$$\sigma_n = \left\lfloor \frac{h}{2}(y_n + 1) \right\rfloor. \tag{5}$$

The chaotic system (4) is iterated w times so, we obtain the sequence $\{\sigma_1, \sigma_2, \cdots \sigma_w\}$.

The generated parameters $K,\ \rho$ and σ are used in the encryption as follows.

Let P denote the plaintext image. In the mixing step, the plaintext is XORed with K to obtain the intermediate value M as

$$M = P \oplus K. \tag{6}$$

In the row rotation step, each row of M are circularly rotated right with rotation amounts given in the sequence ρ. The row rotation step can be written as

$$N(i, j+(\rho_i \bmod w)) = M(i,j),\ 1 \le i \le h,\ 1 \le j \le w, \tag{7}$$

where N denotes the second intermediate variable. Finally, the columns of N are circularly rotated down with rotation amounts taken from the sequence σ. The column rotation can be written as

$$C(i + (\sigma_i \bmod h), j) = N(i,j),\ 1 \le i \le h,\ 1 \le j \le w. \tag{8}$$

The image C is the ciphertext.

The decryption is straightforward. Using the secret parameters, x_0, y_0, we use (1), (2) and (4) to produce $K,\ \rho$ and σ. We go from C to M using (8) then (7). We recover P with $P = M \oplus K$.

Figure 1 shows the block diagram representation of the encryption algorithm.

III. Chosen plaintext attack

A naive attack on the cryptosystem might try to reveal the secret keys x_0 and y_0. However, we note that the parameters $K,\ \rho$ and σ uniquely specify the encryption and the decryption operations. Hence if an attacker manages to reveal these parameters, he can decrypt ciphertext images as if he is the legal recipient. He does not need to know the original keys x_0 and y_0. In this and the next section, we give attacks that try to recover $K,\ \rho$ and σ.

Assume that the attacker knows a plaintext-ciphertext image pair (P_1, C_1). He choses a plaintext image P_2 such that

$$\begin{aligned} P_2(1,j) &= P_1(1,j) \oplus 1,\ 1 \le j \le w, \\ P_2(i,j) &= P_1(i,j),\ 2 \le i \le h,\ 1 \le j \le w. \end{aligned} \tag{9}$$

Namely, P_2 differs from P_1 only in the first row, and the difference in every pixel is just 1. The attacker observes the ciphertext C_2.

Using (6), we have

$$\Delta M_{12} = M_1 \oplus M_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2 = \Delta P_{12}.$$

Hence, ΔM_{12} is an image with zeros everywhere except on the first row, where we have 1s. Using this with (7), we have $\Delta N_{12} = N_1 \oplus N_2 = \Delta M_{12}$. Namely, ΔM_{12} remains the same under row rotation. When we apply the column rotation to ΔN_{12}, the row of 1s is distributed according to σ in $\Delta C_{12} = C_1 \oplus C_2$ as

$$\Delta C_{12}(i,j) = \begin{cases} 1 & i = \sigma_j + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, if the attacker observes that $\Delta C_{12}(i,j) = 1$, then he concludes that $\sigma_j = i - 1$. Since each column of ΔC_{12} has only one nonzero pixel, the attacker can thus determine σ_j, $1 \le j \le w$.

Now that the attacker knows σ, he chooses another plaintext P_3 and obtains the ciphertext C_3. This time, P_3 differs from P_1 only in the first column. Difference is again just 1 in every pixel. Since the attacker knows $\Delta C_{13} = C_1 \oplus C_3$, he uses (8) to obtain the value of $\Delta N_{13} = N_1 \oplus N_3$. He also knows $\Delta M_{13} = P_1 \oplus P_3$. Note that, by the particular choice of P_3, the first column of ΔM_{13} is 1s and it is zero everwhere else. Comparing ΔM_{13} with ΔN_{13} and using (7) we have

$$\Delta N_{13}(i,j) = \begin{cases} 1 & j = \rho_i + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, if the attacker sees that $\Delta N_{13}(i,j) = 1$, he concludes that $\rho_i = j - 1$.

Once the attacker has revealed the rotation amounts ρ and σ, finding K is straightforward. He starts with C_1 and uses (8) then (7) to obtain M_1. Then, he reveals K using $K = P_1 \oplus M_1$.

The chosen-plaintext attack requires one known and two chosen plaintext images. The attack requires very little amount of computation.

IV. Known plaintext attack

In some cases, it might be difficult for the attacker to choose a plaintext and apply chosen-plaintext attack. In this section we describe a known-plaintext attack that requires about two known plaintext-ciphertext pairs of images.

Assume the plaintext-ciphertext pairs (P_1, C_1) and (P_2, C_2) are known by the attacker. We know that $\Delta M = M_1 \oplus M_2 = \Delta P = P_1 \oplus P_2$. So the attacker knows ΔM. Also, he calculates $\Delta C = C_1 \oplus C_2$.

Going from ΔM to ΔC we have first the rows and then the columns rotated. There are no modifications to the pixel values of ΔM. Assume that the attacker observes

$$\Delta M(i_1, j_1) = \Delta C(s_1, t_1) = \Delta C(s_2, t_2) = \cdots = \Delta C(s_m, t_m).$$

So, the pixel (i_1, j_1) of ΔM is moved to one of the locations $(s_1, t_1), (s_2, t_2), \ldots, (s_m, t_m)$ in ΔC. Using (7) and (8), we have

$$\rho_{i_1} \in A_1 = \{t_1 - j_1 \bmod w, t_2 - j_1 \bmod w, \ldots, t_m - j_1 \bmod w\}.$$

Repeating the observation for another pixel $\Delta M(i_1, j_2)$ on the same row, the attacker sees that $\Delta M(i_1, j_2)$ is moved to one of the locations $(\bar{s}_1, \bar{t}_1), (\bar{s}_2, \bar{t}_2), \ldots, (\bar{s}_{\bar{m}}, \bar{t}_{\bar{m}})$ in ΔC. Thus,

$$\rho_{i_1} \in A_2 = \{\bar{t}_1 - j_2 \bmod w, \bar{t}_2 - j_2 \bmod w, \ldots, \bar{t}_{\bar{m}} - j_2 \bmod w\}.$$

Hence, the attacker knows that $\rho_{i_1} \in A_1 \cap A_2$. Considering all the pixels on the same row, we obtain

$$\rho_i \in \bigcap_{j=1}^{w} A_j.$$

If the intersection is a single point then the attacker has found ρ_i. If not, he uses another plaintext-ciphertext pair. The attacker repeats the whole procedure for all the rows and reveals ρ_i, $1 \le i \le h$.

Note that the intersection might shrink to a single point even with the first few A_j's.

Once the attacker has the sequence ρ, he uses a similar set intersection method to reveal σ. First, using (7) and ΔM, the attacker finds ΔN. Going from ΔN to ΔC, only the columns are rotated. Now, he compares the pixel value of $\Delta N(i, j)$ to the pixel values on the j^{th} column of ΔC. Assume that he observes,

$$\Delta N(i, j) = \Delta C(s_1, j) = \Delta C(s_2, j) = \cdots = \Delta C(s_n, j).$$

Then, he knows that

$$\sigma_j \in B_i = \{s_1 - i \bmod h, s_2 - i \bmod h, \ldots, s_n - i \bmod h\}. \tag{10}$$

Repeating the observation for all pixels on the j^{th} column, the attacker obtains

$$\sigma_j \in \bigcap_{i=1}^{h} B_i. \tag{11}$$

Again, the attacker repeats the set intersection, with additional known plaintexts if necessary, until the intersection is a single point. Then, he knows the value of σ_j. He repeats the whole procedure for all the columns.

Once the attacker has ρ and σ, he uses (8) then (7) on a ciphertext image C_1 to obtain M_1. He then recovers the key as $K = M_1 \oplus P_1$.

The attack requires only a few known plaintext-ciphertext pairs for moderate image sizes.

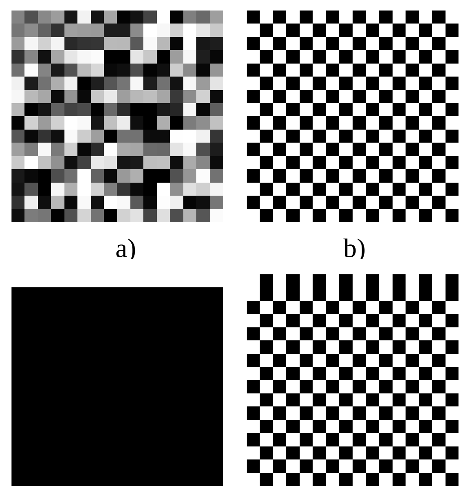
V. Simulation results

A. Chosen plaintext attack

In order to better illustrate the steps of the attack, we work with 16×16 images. We choose the secret keys as $x_0 = 0.41$ and $y_0 = 0.87$. Using (2), (3), (4) and (5), we obtain the rotation sequences ρ and σ as

$$\begin{aligned} \rho &= \{5, 13, 0, 13, 6, 4, 3, 9, 2, 15, 10, 14, 9, 15, 7, 1\}, \\ \sigma &= \{8, 7, 9, 3, 15, 11, 0, 1, 11, 0, 0, 5, 14, 7, 8, 6\}. \end{aligned}$$

The key image K is shown in Figure 2a .



a) b) c) d)

Fig. 2. a) The key K b) Plaintext P_1 c) ΔP_{12} d) P_2

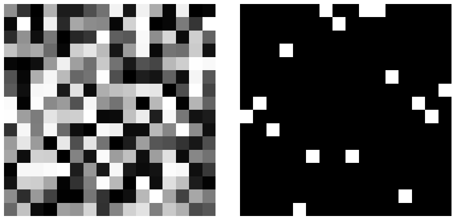
Assume that the attacker knows that the known plaintext P_1 is the two-level checkerboard image shown in Figure 2b. He chooses the plaintext P_2 by flippping the values on the first row of P_1. P_2 and $\Delta P_{12} = P_1 \oplus P_2$ are shown in Figure 2d and 2c. Note that ΔP_{12} is all zeros except in the first row where it is all ones.

In Figure 2a, the pixel values span the full grayscale range $0 - 255$. In Figures 2b, 2c and 2d, we used scaling so that a white square represents a pixel value of 1 rather than 255.

The ciphertext C_1 and the difference $\Delta C_{12} = C_1 \oplus C_2$ are shown in Figure 3. Obviously, σ appears as the distances of the nonzero pixels from the first row in ΔC_{12}.

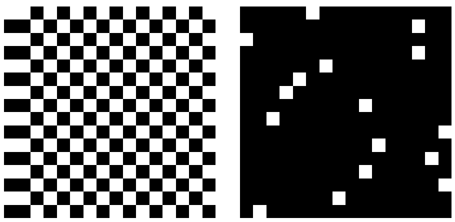
Next, the attacker chooses the plaintext P_3 shown in Figure 4a. Note that P_3 is obtained by flipping the pixels of P_1 on the first column. Now that the attacker knows σ, he applies (8) to ΔC_{13} and obtains $\Delta N_{13} = N_1 \oplus N_3$. The difference ΔN_{13} is shown in Figure 4b. This time, ρ appears as the distances of nonzero pixels from the first column in ΔN_{13}.

Finally, the attacker uses (8) and (7) to get M_1 from C_1. He calculates K as $K = M_1 \oplus P_1$.



a) b)

Fig. 3. a) C_1 b) ΔC_{12}

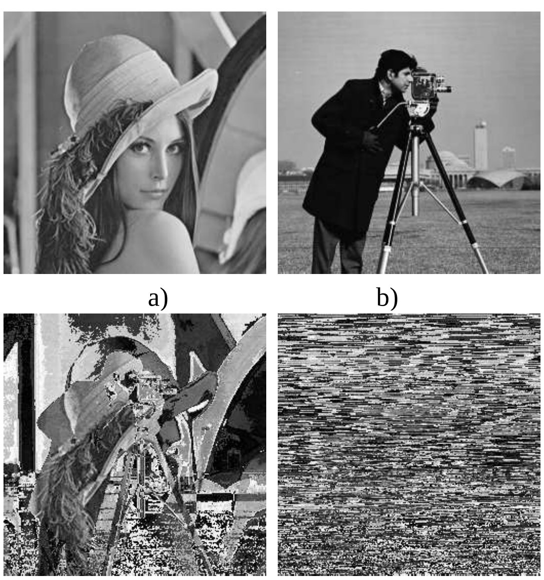


a) b)

Fig. 4. a) P_3 b) $\Delta N_{13} = N_1 \oplus N_3$

B. Known plaintext attack

Assume that the attacker knows the two plaintext-cipher text pairs shown in Figures 5a and 5b. The image sizes are 256×256. Assume the secret parameters x_0, y_0 are as before. The difference of images, $\Delta P = \Delta M = P_1 \oplus P_2$, is shown in Figure 5c.



a) b)

c) d)

Fig. 5. a) P_1 b) P_2 c) $\Delta P = P_1 \oplus P_2$ d) ΔN

Starting with the pixel $\Delta M(1,1)$, we see that $\bigcap_{j=1}^{38} A_j$ contains just one element. So, we do not need to further intersect the sets A_j, $38 < j \leq 256$, to find ρ_1. In general, we need far fewer number of sets than the number of columns. Figure 6 shows the number of sets we intersected to pin down ρ_i, $1 \leq i \leq 256$. We see that we need to intersect at most 40 sets.

Once the attacker knows ρ, he uses (7) to calculate ΔN from ΔM. ΔN is shown in Figure 5d. Note that ΔN does not look like a random image because it is only the row-rotated version of $\Delta M = \Delta P$.

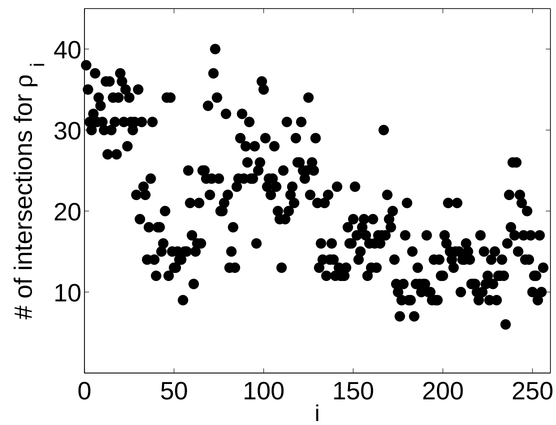


Fig. 6. The number of set intersections until ρ_i is uniquely found.

Using (10) and (11), the attacker determines σ_j, $1 \leq j \leq 256$. Since the images contain enough variation in their pixel values, only a few B_i sets need to be intersected. Figure 7 shows the number of sets we intersected to pin down σ_j, $1 \leq j \leq 256$. We see that at most 2 sets need to be intersected for every σ_j.

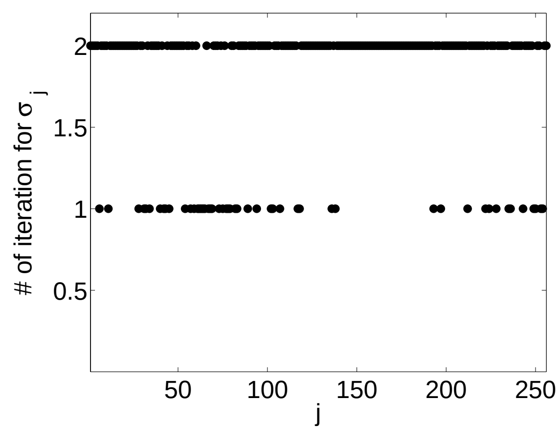


Fig. 7. The number of set intersections until σ_j is uniquely found.

Once the attacker has ρ and σ, he uses (8) and (7) to get M_1 from C_1. He calculates K as $K = M_1 \oplus P_1$.

The attack takes less than a minute on MATLAB running on Mac OS X 10.5.4 with Intel Core 2 Duo 2.16 GHz processor and 2 GB RAM.

VI. Conclusion

In this paper, we gave a complete break of a recently proposed image encryption algorithm. We have demonstrated that the secret parameters can easily be found using chosen-plaintext and known-plaintext attacks. Using simulation examples on real images, we have shown that our proposed attacks require very little amount of computation.

ACKNOWLEDGMENT

This work was supported by the The Scientific and Technological Research Council of Turkey (TÜBİTAK) under Project No. 106E143.

The author thanks an anonymous reviewer for pointing out the similar work in [9]

REFERENCES

[1] Z.-P. Jiang, A note on chaotic secure communication systems, IEEE Tran. Circuits and Systems–I: Fundamental Theory and Applications 49 (1) (2002) 92–96.

[2] F. Anstett, G. Millerioux, G. Bloch, Chaotic cryptosystems: Cryptanalysis and identifiability, IEEE Tran. Circuits and Systems I 53 (12) (2006) 2673–2680.

[3] A. T. Parker, K. M. Short, Reconstructing the keystream from a chaotic encryption scheme, IEEE Tran. Circuits and Systems–I: Fundamental Theory and Applications 48 (5) (2001) 624–630.

[4] E. Solak, Partial identification of Lorenz system and its application to key space reduction of chaotic cryptosystems, IEEE Tran. Circuits and Systems–II: Express Briefs 51 (10) (2004) 557–560.

[5] J. Fridrich, Symmetric ciphers based om two-dimensional chaotic maps, Int. J. of Bifurcation and Chaos 8 (6) (1998) 1259–1284.

[6] T. Xiang, K.-W. Wong, X. Liao, A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map, Physics Letters A 364 (2007) 252–258.

[7] X. Tong, M. Cui, Image encryption with compound chaotic sequence cipher shifting dynamically, Image and Vision Computing 26 (2008) 843–850.

[8] T. Xiang, K. wo Wong, X. Liao, Selective image encryption using a spatiotemporal chaotic system, Chaos: An Interdisciplinary Journal of Nonlinear Science 17 (2) (2007) 023115.

[9] S. Li, C. Li, G. Chen, N. G. Bourbakis, K. -T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing: Image Communication, 23 (2008) 212–223.