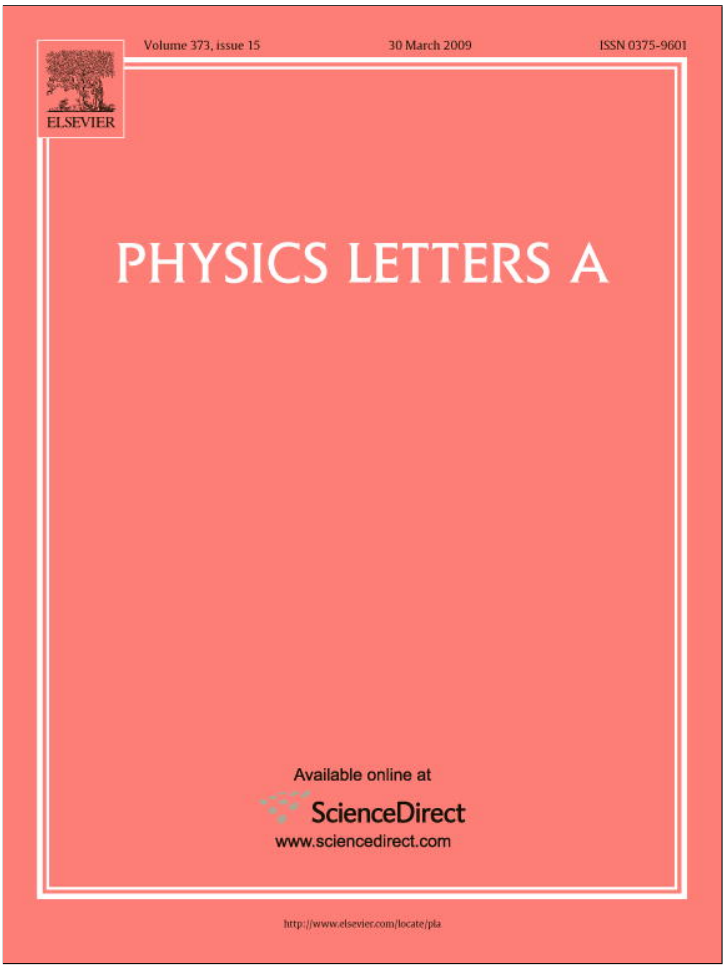

Physics Letters A 373 (2009) 1357–1360

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Cryptanalysis of a chaos-based image encryption algorithm

Cahit Çokal, Ercan Solak *

Department of Computer Engineering, Isik University, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 25 November 2008
Accepted 18 February 2009
Available online 20 February 2009
Communicated by A.R. Bishop

PACS:
05.45.Vx

Keywords:
Communication using chaos
Cryptanalysis

ABSTRACT

A chaos-based image encryption algorithm was proposed in [Z.-H. Guan, F. Huang, W. Guan, Phys. Lett. A 346 (2005) 153]. In this Letter, we analyze the security weaknesses of the proposal. By applying chosen-plaintext and known-plaintext attacks, we show that all the secret parameters can be revealed.

1. Introduction

In this Letter, we give a complete break of the chaos-based image encryption algorithm proposed in [1]. The algorithm uses Arnold's cat map [2] to shuffle the image pixels and Chen's chaotic system [3] to change the gray levels of the shuffled image pixels.

The outline of the Letter is as follows. In the next section we describe the encryption algorithm in detail. In Section 3, we demonstrate a chosen-plaintext attack that reveals all the secret parameters. In Section 4, we do the same with a known-plaintext attack. In Section 5, we illustrate the success of our break with simulation examples. Finally, we give concluding remarks.

2. Description of the encryption algorithm

The encryption process consists of two parts. In the first part, the algorithm takes an image P and shuffles its pixels using Arnold cat map. The second part of the algorithm changes the gray levels of the pixels using Chen's chaotic system.

2.1. Arnold cat map

Assume that we have an $N \times N$ image P with the pixel coordinates $I = \{(x, y) \mid x, y = 0, 1, 2, \ldots, N-1\}$. Arnold cat map is given as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N, \tag{1}$$

where p, q are positive integers and x', y' are the coordinate values of the shuffled pixel. After iterating this map n times, we have

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A^n \begin{bmatrix} x \\ y \end{bmatrix} \mod N = M \begin{bmatrix} x \\ y \end{bmatrix} \mod N, \tag{2}$$

where

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} = A^n \mod N.$$

The shuffled image S is related to the original image P as

$$S(x', y') = P(x, y), \quad 0 \leqslant x, y \leqslant N-1.$$

2.2. Chen's chaotic system

Chen's chaotic system is a set of differential equations given as

$$\begin{aligned} \dot{x} &= a(y-x), \\ \dot{y} &= (c-a)x - xz + cy, \\ \dot{z} &= xy - bz, \end{aligned} \tag{3}$$

where a, b and c are parameters of the system. Chen's system is chaotic when the parameters have the values; $a = 35$, $b = 3$ and $c \in [20, 28.4]$ [1].

2.3. Encryption algorithm

In this section, we describe the encryption algorithm in detail. The secret keys of the algorithm are the parameters p, q, n of Arnold cat map and the initial values x_0, y_0, z_0 of Chen's chaotic system. The encryption steps are as follows:

* Corresponding author. Tel.: +90 216 528 7149; fax: +90 216 710 2872.
E-mail addresses: cahit.cokal@isik.edu.tr (C. Çokal), ercan@isikun.edu.tr (E. Solak).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2009.02.030

(1) Shuffle the image P using Arnold cat map and obtain the shuffled image S.
(2) By scanning the image S row-by-row, arrange its pixels as the sequence $S = \{s_1, s_2, \ldots, s_{N\times N}\}$.
(3) Using Runge–Kutta step size 0.001, iterate Chen's chaotic system $N_0 = (N \times N)/3$ times and obtain the real values x_i, y_i, z_i, $1 \leqslant i \leqslant N_0$.
(4) Obtain the key sequence $K = \{k_1, k_2, \ldots, k_{N\times N}\}$ as

$$k_{3(i-1)+1} = \left|x_i - \lfloor x_i \rfloor\right| \times 10^{14} \mod 256,$$
$$k_{3(i-1)+2} = \left|y_i - \lfloor y_i \rfloor\right| \times 10^{14} \mod 256,$$
$$k_{3(i-1)+3} = \left|z_i - \lfloor z_i \rfloor\right| \times 10^{14} \mod 256, \tag{4}$$

where $\lfloor x \rfloor$ denotes the largest integer not larger than x. Here, we assume that the encryption setup represents the real numbers with 14 decimal digits after the point.
(5) Obtain the encrypted sequence $C = \{c_1, c_2, \ldots, c_{N\times N}\}$ as

$$c_i = s_i \oplus k_i, \quad 1 \leqslant i \leqslant N \times N, \tag{5}$$

where $\oplus$ represents bitwise exclusive OR operation.
(6) By reshaping the sequence C into an $N \times N$ image, obtain the ciphertext image.

3. Chosen-plaintext attack

In this section, we describe how the secret parameters of the proposed encryption algorithm can be extracted using a chosen-plaintext attack.

If an attacker knows the parameters M and K, he can reverse the two steps of the encryption and decrypt a ciphertext image. Indeed, if an attacker knows K, by using (5), he can obtain the shuffled image S. If he also knows M, he uses (2) and obtains the original image P. Thus, there are only two secret parameters to extract and these are M and K. The attack consists of two steps. First, K is recovered. Then, the attacker uses K in calculating the key M of Arnold cat map.

3.1. Extracting K

The attacker choses an image P_1 that consists of $N \times N$ zero-valued pixels, and obtains the corresponding ciphertext image, C_1.

The shuffling process does not change the image because P_1 is identically 0. Hence, the shuffled image S_1 is equal to the image P_1. Using this fact and (5), the attacker can easily see that the cipher-image C_1 is exactly equal to the key K as

$$C_1 = S_1 \oplus K = P_1 \oplus K = 0 \oplus K = K.$$

3.2. Extracting M

The attacker choses another image P_2 and gets the corresponding ciphertext image C_2. The image P_2 is chosen such that it contains only two non-zero and distinct pixels $P_2(1,1) = v_1$, $P_2(1,2) = v_2$ so that $v_1 \neq v_2$ and $v_{1,2} \neq 0$. The attacker already knows K. By using (5), the attacker obtains the corresponding shuffled image S_2 from C_2 as

$$S_2 = C_2 \oplus K.$$

Now, the attacker has the image P_2 and the corresponding shuffled image S_2. By searching for pixel values v_1, v_2 in S_2, the attacker determines the shuffled coordinates (x'_1, y'_1) and (x'_2, y'_2).

Using (2), the attacker obtains the following sets of equations:

$$\begin{bmatrix} x'_1 \\ y'_1 \end{bmatrix} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \mod N,$$
$$\begin{bmatrix} x'_2 \\ y'_2 \end{bmatrix} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mod N. \tag{6}$$

Solving these equations, the attacker finds that $m_2 = x'_2 - x'_1 \bmod N$, $m_1 = x'_1 - m_2 \bmod N$, $m_4 = y'_2 - y'_1 \bmod N$, $m_3 = y'_1 - m_4 \bmod N$. Hence, the key M is extracted. Now, the attacker has all the secret parameters of the encryption algorithm.

4. Known-plaintext attack

In this section, we describe how the secret parameters of the proposed encryption algorithm can be extracted using a known plaintext attack. In this case, the attacker does not choose plaintexts. Instead, we assume that he has obtained some plaintext–ciphertext pairs. The attack consists of two steps; the first step is to calculate the key of Arnold cat map, M, and the second step is to extract the key K of Chen's chaotic system.

4.1. Extracting M

Assume that the attacker knows two plaintext–ciphertext image pairs (P_1, C_1) and (P_2, C_2). Let us define the differences as $\Delta P = P_1 \oplus P_2$ and $\Delta C = C_1 \oplus C_2$. Using (5), the attacker calculates

$$\Delta C = S_1 \oplus K \oplus S_2 \oplus K = S_1 \oplus S_2 = \Delta S$$

Hence, the attacker can calculate ΔS. Going from ΔP to ΔS, there is only shuffling by the Arnold cat map. Next, we give a method to reveal the parameters of this map.

Let $\Delta P(x_1, y_1) = v_1$, $\Delta P(x_2, y_2) = v_2$ be two pixels of ΔP with different values, i.e. $v_1 \neq v_2$. Let (x'_1, y'_1) and (x'_2, y'_2) denote their respective coordinates in ΔS. Using (2), we have

$$\begin{bmatrix} x'_1 & x'_2 \\ y'_1 & y'_2 \end{bmatrix} = MU = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} U \mod N, \tag{7}$$

where $U = \left[\begin{smallmatrix} x_1 & x_2 \\ y_1 & y_2 \end{smallmatrix}\right]$.

Let V_1 denote the set of coordinates at which ΔS has value v_1. Namely,

$$V_1 = \{(i,j) \mid \Delta S(i,j) = v_1\}. \tag{8}$$

Similarly, define the set V_2 as

$$V_2 = \{(k,l) \mid \Delta S(k,l) = v_2\}. \tag{9}$$

Assuming that U is invertible, let us define the set V of matrices as

$$V = \left\{ \begin{bmatrix} i & k \\ j & l \end{bmatrix} U^{-1} \;\middle|\; (i,j) \in V_1,\ (k,l) \in V_2 \right\}. \tag{10}$$

By the definitions of the sets V_1 and V_2, we have $(x'_1, y'_1) \in V_1$ and $(x'_2, y'_2) \in V_2$. So, using (7), we conclude that $M \in V$.

Thus, once the attacker constructs the set V, he has $|V| = |V_1||V_2|$ candidates for M. Repeating the procedure with another pair of pixels $\Delta P(\bar{x}_1, \bar{y}_1) = \bar{v}_1$, $\Delta P(\bar{x}_2, \bar{y}_2) = \bar{v}_2$, $\bar{v}_1 \neq \bar{v}_2$, he finds another set $\bar{V}$ that contains M. Obviously,

$$M \in V \cap \bar{V}. \tag{11}$$

Continuing in this fashion, he intersect more and more sets until the intersection contains only one element. This element is necessarily M.

In order to make the set V of candidates smaller, the attacker chooses rare pixel pairs in ΔP.

4.2. Extracting K

The attacker knows the image P_1 and the corresponding cipher image C_1. Using (2) and the Arnold cat map parameter M revealed in the previous step, the attacker calculates S_1.

Using S_1 in (5), the attacker obtains Chen's chaotic system parameter K as

$$K = C_1 \oplus S_1.$$

Thus, the attacker knows all the secret parameters of the encryption algorithm.

5. Simulation results

In order to illustrate each type of attacks, we give simulation results for two cases. Simulations are performed under MATLAB running on Mac OS X 10.5.4 with Intel Core 2 Duo 2.16 GHz processor and 2 GB RAM. The secret parameters are chosen from the example in [1]. Arnold cat map parameters are: $p = 1$, $q = 1$, $n = 5$, Chen's chaotic system parameters are: $a = 35$, $b = 3$, $c = 28$, The initial conditions for the Chen system are: $x_0 = -10.058$, $y_0 = 0.368$, $z_0 = 37.368$.

In the first simulation, we illustrate the chosen-plaintext attack. The attacker chooses the following two 9×9 images as plaintexts:

$$P_1 = \begin{bmatrix} 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{bmatrix},$$

$$P_2 = \begin{bmatrix} 0&0&0&0&0&0&0&0&0\\ 0&1&2&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{bmatrix}.$$

Note that the first image consists of zero valued pixels and the second image has only two nonzero pixels. By (6), the first secret parameter M is

$$M = \begin{bmatrix} 7 & 1 \\ 1 & 8 \end{bmatrix} \bmod 9.$$

The ciphertext C_1, which is also the Chen key K, is given as

$$C_1 = K = \begin{bmatrix} 255&0&0&210&15&170&32&187&27\\ 225&138&115&22&29&95&140&62&213\\ 152&97&255&222&66&34&164&1&148\\ 225&142&38&133&203&253&201&115&133\\ 70&223&18&151&239&179&137&251&101\\ 64&67&157&22&225&39&70&171&25\\ 83&19&3&209&152&89&121&220&249\\ 87&170&185&30&240&74&47&173&43\\ 155&23&132&113&30&94&4&23&31 \end{bmatrix}.$$

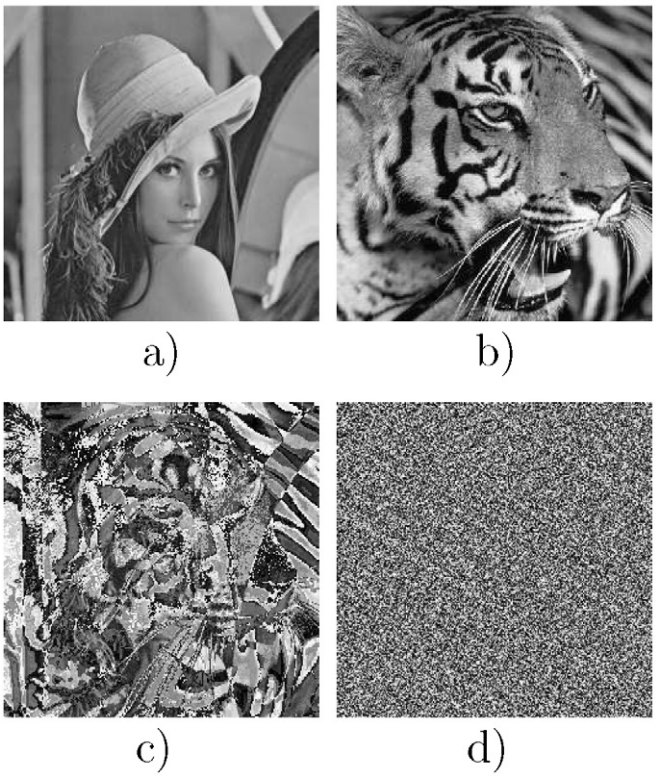

Fig. 1. (a) Plaintext P_1; (b) Plaintext P_2; (c) ΔP; (d) ΔC.

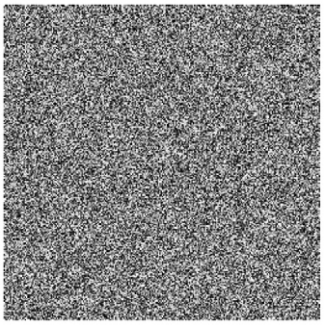

Fig. 2. Chen key K.

Using C_2, the attacker calculates S_2 as $S_2 = C_2 \oplus K$. S_2 is given as

$$S_2 = \begin{bmatrix} 0&0&0&0&0&0&0&0&2\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0 \end{bmatrix}.$$

Inspecting S_2, the attacker finds that $x'_1 = 8$, $y'_1 = 0$, $x'_2 = 0$, $y'_2 = 8$. Substituting these into (6), the attacker finds M.

In the second simulation, we illustrate the known-plaintext attack. Assume that the attacker knows the two 256×256 plaintext images in Fig. 1(a) and 1(b). The difference images $\Delta P = P_1 \oplus P_2$ and $\Delta C = C_1 \oplus C_2$ are also shown in Fig. 1(c) and 1(d). For this case, we have

$$M = \begin{bmatrix} 34 & 55 \\ 55 & 89 \end{bmatrix} \bmod 256.$$

The two rarest pixel values in ΔP are $v_1 = 131$ and $v_2 = 140$. Following are procedure in Section 4.1, we find 25718 candidates for M. Next rarest pair of pixel values are $\bar{v}_1 = 140$ and $\bar{v}_2 = 120$. This time, there are 29058 candidates. Intersecting the two sets of candidates, we find only one candidate. The attack takes less than one minute.

Finally, after calculating S_1 using (2), the attacker reveals K as $K = C_1 \oplus S_1$. K is given in Fig. 2.

6. Conclusion

In this Letter, we gave a complete break of a chaos-based image encryption algorithm. We demonstrated that the secret keys can be revealed using chosen and known plaintext attacks.

Acknowledgement

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

References

[1] Z.-H. Guan, F. Huang, W. Guan, Phys. Lett. A 346 (2005) 153.
[2] http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf.
[3] G. Chen, T. Ueta, Int. J. Bifur. Chaos 9 (7) (1999) 1465.