I.J. Image, Graphics and Signal Processing, **2010, 2, 39-45**
Published Online December 2010 in MECS (http://www.mecs-press.org/)

Improved Cryptanalysis of CMC Chaotic Image Encryption Scheme

Jiansheng Guo
Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Email: tsg_31@126.com

Lei Zhang
Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Email: zzll2000@163.com

Abstract—**Recently, chaos has attracted much attention in the field of cryptography. To study the security with a known image of a symmetric image encryption scheme, the attack algorithm of equivalent key is given. We give the known image attacks under different other conditions to obtain the equivalent key. The concrete step and complexity of the attack algorithm is given. So the symmetric image encryption scheme based on 3D chaotic cat maps is not secure.**

Index Terms—**Cryptanalysis; Equivalent key attack algorithm; Image encryption; Chaotic cipher**

I. INTRODUCTION

Because of the chaotic map's random behavior and sensitivity to initial conditions and parameter settings, Some researchers have pointed out that there exists tight relationship between chaos and cryptography [1–7]. Many fundamental characteristics of chaos, such as the ergodicity, mixing and exactness property and the sensitivity to initial conditions, can be connected with the "confusion" and "diffusion" property in cryptography. So it is a natural idea to use chaos to enrich the design of new ciphers.

Chaos-based encryption is not a very new idea. In 1989, Matthews [8] used chaotic dynamical systems in cryptography firstly. He derived a one-dimension chaotic map, which is used to generate a sequence of pseudo-random numbers. Then, Fridrich proposed another encryption algorithm based on two-dimensional chaotic systems is in [9]. After that the map is extended to three dimensions to obtain a more complicated substitution cipher that can be used for the purpose of image encryption. In [1], a new image encryption algorithm based on chaotic map has been proposed. The main ideal of the image encryption algorithm is that Chen et al extending the traditional two-dimensional Cat mapping to three-dimensional generalized Cat mapping. Additionally, based on this the chaotic mapping, they designed a symmetric image encryption algorithm (denoted as CMC). In the algorithm, the domain of the three-dimensional generalized Cat mapping is limited in the remain class ring of the three-dimensional space. However, the strict mathematical chaotic transformation is defined in the real fields. We noticed that the designer ignored this weakness, and based on this, we can attack on the CMC chaotic image encryption algorithm with known image.

In [10], Guo analyzed the security of Chen's image encryption algorithm when the round function iterates only one time, and the case that the algorithm iterates more than one times is not analyzed. Additionally, the proposed solution algorithm did not use the characteristics of gray transformation. To the best of our knowledge there is no security analysis of this image encryption algorithm. Therefore, the aim of this paper is to assess the security of such cryptosystem, and we study the security with known image of CMC chaotic image encryption scheme, give an attack algorithm of equivalent key, and analyze the concrete computation complex of proposed attack algorithm. The result shows CMC algorithm is not secure with known image.

The rest of the paper is organized as follows. Section II describes the cryptosystem introduced in [1]. After that, Section III points out some design problems inherent to that cryptosystem, and Section IV gives some attacks on the cryptosystem under study. Then, section V presents the efficient of the attacking algorithm. Finally, Section VI concludes the paper.

II. DESCRIPTION OF THE ENCRYPTION SCHEME

The traditional two-dimensional Cat map is now generalized to three-dimensional Cat map by introducing Arnold transformation. The extended Cat map is a three-dimensional invertible chaotic map described by

$$f: Z_N \times Z_N \times Z_N \ \text{a} \ Z_N \times Z_N \times Z_N$$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} \text{a} \ A \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \mod N$$

where

$$A = \begin{bmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z a_z + a_x a_y a_z + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \quad (1)$$

and $a_x, b_x, a_y, b_y, a_z, b_z$ are all positive integers.

Copyright © 2010 MECS

Based on the generalized Cat map, the complete image encryption scheme consists of five steps of operations, as shown in Fig. 3.

Step1 Pile up the two-dimensional image into three-dimensional. Suppose that the image to be encrypted is of W -pixel length and H-pixel wide, in totally $W \times H$. First, one needs to pile up all pixels of the image, to form several cubes of size $N_1 \times N_1 \times N_1$, $N_2 \times N_2 \times N_2$, …., $N_i \times N_i \times N_i$, respectively. To convert an image into several cubes, the following condition must be satisfied:

$$W \times H = N_1^3 + N_2^3 + \mathrm{L} + N_i^3 + R$$

where $N_i \in \{2,3,\mathrm{K},N\}$ is the side length of each cube. N is the size of the maximum allowable cube, and $R \in \{0,1,2,\mathrm{K},7\}$ is the remainder.

Step2 Perform the three-dimensional Cat map. Use $a_x, b_x, a_y, b_y, a_z, b_z$ as control parameters to perform the three-dimensional discrete Cat map on each image cubes, generating shuffled images.

Step3. Diffusion process. Set $C(0) = S$, then perform the diffusion process once according to the algorithm described as follow.

$$C(k) = \phi(k) \oplus \{[I(k) + \phi(k)] \bmod M\} \oplus C(K-1)$$

where $I(k)$ is the currently operated pixel and $C(k-1)$ is the previously output cipher pixel. M is the color level (for a 256 grey-scale image, M=256). Set the initial value $x(0) = L_i$. Computer the chaotic Logistic map:

$$x(k+1) = 4x(k)[1 - x(k)]$$

If the next value obtained is within the subinterval (0.2, 0.8), then digitize it by amplifying it with a proper scaling and sampling, and obtained the valued $\phi(k)$; otherwise, the iteration goes on until a desired number in (0.2, 0.8) is obtained.

Step4. Transform the three-dimensional cubes back to a two-dimensional image. The three-dimensional cubes are appropriately arranged, laying back to a two-dimensional image for display or for storage.

Step5. Key generation. The image encryption scheme uses the chaotic system as follow:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \qquad (2)$$

where *a*, *b*, *c* are parameters. When $a = 35, b = 3, c \in [20,28.4]$, the system is chaotic. The key used in the proposed encryption scheme is a binary sequence of 128 bits. The binary sequence is divided into eight segments, denoted as $k_{a_x}, k_{b_x}, k_{a_y}, k_{b_y}, k_{a_z}, k_{b_z}, k_l, k_s$, respectively, each with 16-bit long. Parameters $k_{a_x}, k_{b_x}, k_{a_y}, k_{b_y}, k_{a_z}, k_{b_z}$ are used to generate the six control parameters of the extended three- dimensional Cat map (1), while k_l and k_s are used to generate the initial two values L_i , S of Step 4.

In detail, to generate a_x and b_x, the following formulas are first used to compute the control parameter *c* of Chen's system:

$$c = K_{a_x} \times 8.4 + 20$$

where $K_{a_x} = \sum_{i=0}^{15} K_{a_x}(i) \times 2^i$, $K_{a_x}(i)$ is the *i*-th bit in sequence K_{a_x} . Initial values x_0, y_0, z_0 are also derived from K_{a_x} and K_{b_x} , by using the following formulas:

$$x_0 = K_{b_x} \times 80 - 40,$$
$$y_0 = K_{a_x} \times 80 - 40,$$
$$z_0 = K_{b_x} \times 60.$$

Then, in the next step, parameters are set as $a = 35, b = 3$, and the other parameters obtained above of (2) are used to iterate (2) for 100 and 200 times, respectively, yielding two values: $(x_{100}, y_{100}, z_{100})$ and $(x_{200}, y_{200}, z_{200})$. Next, then, the following formulas are used instead, to generate the final parameter values of a_x and b_x.

$$a_x = round(z_{100}/60 \times N),$$
$$b_x = round(z_{200}/60 \times N).$$

where *N* is the side length of cube to be scrambled by the 3D cat map.

A similar process is performed to obtain the control parameters a_y, b_z, a_z, b_y , and the initial values of the Logistic map L_i, and the initial value of the mod operation, *S*. The following two formulas are used instead, to generate L_i and *S*:

$$L_i = z_{100}/60$$
$$S = round(z_{200}/60 \times 255)$$

The complete image encryption scheme shows in Figure. 1.

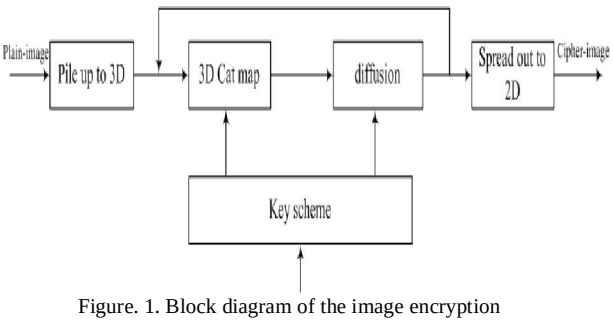

Figure. 1. Block diagram of the image encryption

III. THE ANALYSIS OF CHAOTIC IMAGE ENCRYPTION ALGORITHM

Chen et al extended the traditional two-dimension Cat mapping to three-dimensional generalized Cat mapping in [1], and using the extended mapping, designed an image encryption algorithm. The algorithm consists of five parts, limited to the article length, specific processes and symbolic description see [1] and [10].

Firstly, we analyze the three-dimensional generalized Cat mapping used in the image encryption scheme. In the image encryption scheme, the three-dimensional

Copyright © 2010 MECS

generalized Cat mapping A is 3-order degree matrix which defined in $Z/(N)$, where N is the allowed maximum length side of cube in the step 2. Set

$$B = A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \mod N$$

Obviously, if we compute the value of B, that is to say we get the $a_{ij}(1 \le i, j \le 3)$ in the domain $Z/(N)$, we can easily obtain the image pixel transformation's equivalent key.

Theorem 1[10] Suppose $w(i,j,k) + w'(l,m,n)$ is the linear combination of the pixel positions (i,j,k) and (l,m,n), and after the step 2 transformation, set the coordinate pixel positions are (x',y',z') and (x'',y'',z''), then

$$(x'',y'',z'') = w(x,y,z) + w'(x',y',z') \mod N$$

In particular, if one of w and w' is 0, let $w' = 0$, then

$$(x'',y'',z'') = w(x,y,z) \mod N$$

Theorem 2[11] If $N \ge 1$, set

$$\Delta = imq + lpk + jno - omk - pnk - ljq,\ (\Delta, N) = 1,$$

then the pair of congruent polynomial equation

$$\begin{cases} ir + js + kt = e \pmod N \\ lr + ms + nt = g \pmod N \\ or + ps + qt = f \pmod N \end{cases}$$

has a unique solution in $Z/(N)$

$$\begin{cases} r = \Delta^{-1}(emq + gpk + jnf - fmk - pne - gjq) \pmod N \\ s = \Delta^{-1}(igq + lfk + eno - ogk - fni - leq) \pmod N \\ t = \Delta^{-1}(imf + lpe + jgo - ome - pgi - ljf) \pmod N \end{cases}$$

where $\Delta^{-1}\Delta = 1 \pmod N$.

The three-dimensional generalized Cat mapping A as a part of the algorithm is reversible transformation. According to theorem 2, as long as we know three pixels' positions (i,j,k), (l,m,n), (o,p,q) which content the equation

$$(imq + lpk + jno - omk - pnk - ljq, N) = 1$$

The corresponding pixels' positions after the pixel transformation are (x,y,z), (x',y',z'), (x'',y'',z''), then we can obtain the unique equivalent key of the pixel transformation.

IV. THE EQUIVALENT KEY ATTACK ALGORITHM OF CMC

Define 1 If the adversary except knew the image encryption algorithm, but also obtained a pair of image information (plain-image and the corresponding cipher-image using the identical key), we called this condition is attack with image known.

We attack the image encryption algorithm under the condition that we know the plain-image and the corresponding cipher-image. Firstly, we attack the kind of algorithm that step2 and step 3 only iterate only one time. According to the key schedule of the cipher, the key parameters L_i, S are related with k_l, k_s. Therefore, we can first transform the known two-dimension image into three-dimensional image, then exhaust the values k_l, k_s and use the key generation algorithm to generate L_i, S, using inverse transformation of step 3

$$I(k) = \{\phi(k) \oplus C(k) \oplus C(k-1) + M - \phi(k)\} \bmod M$$

Then, decrypt the three-dimensional cipher-image, denoted the decryption image as three-dimensional chaotic cipher-image. By the encryption algorithm, the three-dimensional chaotic cipher-image is the three-dimensional plain-image after the three-dimensional generalized Cat transformation.

Compute the greatest common factor d of N, and exhaust the position values of three-dimensional image pixel transformation. In particular, the position value $(0,0,d)$ after the step 2 transformation would have the least results. Let the transformation result is (e,f,g). Because of the three-dimensional generalized Cat transformation only changes the position of the image pixels and not changes the value of the image pixels. So, the position pixel (e,f,g) can only select the cipher-image pixel that has the same gray value with $(0,0,d)$ in the plain-image.

According to theorem 1, after transformation, the corresponding image positions of $(0,0,wd)(w = 2,3,\mathrm{L})$ are (e,f,g) and $(we \pmod N, wf \pmod N, wg \pmod N)$. Thus the two pixel positions $(0,0,d)$ and $(0,0,wd)$ would be changed to be (e,f,g), $(we \pmod N, wf \pmod N, wg \pmod N)$. Meanwhile, we can compute the gray values of the four pixel positions in the three-dimensional plain-image and cipher-image, denoted as $g(0,0,d)$, $g(0,0,wd)$, $g'(e,f,g)$ and $g'(we \pmod N, wf \pmod N, wg \pmod N)$. As the three-dimensional generalized Cat mapping transformation only change the pixel gray position and does not change the gray value, then to verify the equation

$$g(0,0,wd) = g'(we \pmod N, wf \pmod N, wg \pmod N)$$

This condition can be used to verify the exhaustive values of k_l and k_s, further more it also test whether the supposition (e,f,g) is correct or not. Set the count of the position $(0,0,d)$ that in the three-dimensional chaotic cipher-image and plain-image has the same gray value is M_s'. A wrong supposition through the above test's probability approximate is $1/M'_s$, so take the number of w is T, and by T times the corresponding probability is $(1/M_s')^T$. After the transformation, the number of the supposition position is M_s', so take $T > 1$, and make the expectation that false assumption tested by T times $M_s' \times (1/M_s')^T < 1$.

At this time, the guessed values k_l, k_s that go through the test and the position (e,f,g) can be thought to be correct values.

In the same way, we can exhaust all the possible results when the three-dimensional plain-image pixel position $(0,d,0)$ after the pixel transformation, and set the transformed position is (h,i,j). Due to the same reason that the three-dimensional generalized Cat mapping only

Copyright © 2010 MECS

changes the gray position and not changes the gray value. So, (h,i,j) can choose the particular position that the pixel position $(0,d,0)$ has the same gray value in the plain-image and cipher-image, set the number of these pixels are M_s''. For any w, the transformed position of $(0,d,wd)$ is $(h,i,j)+w(e,f,g)$, search the gray values of pixel positions $(0,d,0)$, $(0,d,wd)$, (h,i,j), $(h,i,j)+w(e,f,g)$ in plain-image and cipher-image, then

$$g(0,d,wd)=g'((h,i,j)+w(e,f,g))$$

Using this condition can check whether the assumed position (h,i,j) is right or not. Then test all the values of $(0,d,wd)$, $0\le w\le T'(T'>1)$, the expectation that a wrong guessed value go through the all tests is $M_s''\times(1/M_s'')^T<1$, so if (h,i,j) can go through all the tests, it would be thought to be correct position.

Now, we can exhaust all the possible transformed results of the three-dimensional plain-image pixel position $(d,0,0)$, and set the transformed position is (k,l,m). Because of the three-dimensional generalized Cat mapping only changes the gray position and not changes the gray value. So, (k,l,m) can choose the particular position that the pixel position $(d,0,0)$ has the same gray value in the plain-image and cipher-image, set the number of these pixels is M_s'''. For any w, the transformed position of $(d,0,wd)$ is $(k,l,m)+w(e,f,g)$, search the gray values of pixel positions $(d,0,0)$, $(d,0,wd)$, (k,l,m), $(k,l,m)+w(e,f,g)$ in plain-image and cipher-image, then

$$g(d,0,w)=g'((k,l,m)+w(e,f,g))$$

Using this condition can check whether the assumed position (k,l,m) is right or not. Then test all the values of $(d,0,wd)$, $0\le w\le T'(T'>1)$, the expectation that a wrong guessed value go through the all tests is $M_s'''\times(1/M_s''')^T<1$, so if (k,l,m) can go through all the tests, it would be thought to be correct position.

In the end, using the obtained image transformed pixel positions (e,f,g) of $(0,0,d)$, (h,i,j) of $(0,d,0)$, (k,l,m) of $(d,0,0)$, we can get the equivalent transformation of the three-dimensional generalized Cat mapping. In a word, the complete attack algorithm can break the image encryption scheme. The following gives an equivalent key attack algorithm when the step 2 and step 3 only iterate only one time in the image encryption algorithm.

Algorithm 1:

1) compute the greatest common factor d of N;

2) for ($k_l=0$; $k_l<2^{16}$; k_l++)

{

for ($k_s=0$; $k_s<2^{16}$; k_s++)

{

1 use the key generation algorithm to generate key parameters L_i and S ;

2 use the reversible transformation of the step 3

$$I(k)=\{\phi(k)\oplus C(k)\oplus C(k-1)+M-\phi(k)\}\bmod M$$

to decrypt the cipher-image.

3 $(i,j,k)\leftarrow$the plain-image pixel coordinate of $(0,0,d)$

$g(0,0,d)\leftarrow$the plain-image pixel gray value of $(0,0,d)$

4 $i1=1$;

5 if $i1>M_s'$, continue;

else $(e,f,g)\leftarrow$the pixel coordinate that the $i1$th gray value of the chaotic cipher-image is $g(0,0,d)$;

6 $w=2$;

7 $g(0,0,wd)\leftarrow$the gray value of the plain-image pixel $(0,0,wd)$;

8 verification. To verify that

$g(0,0,wd)=g'(we(\bmod N),wf(\bmod N),wg(\bmod N))$;

if not, $i1$++ return 5

else to verify $w\le 7$

If yes, w ++ return 7;

else continue

3) Output the transformed image position (e,f,g) of $(0,0,d)$, and the values of k_l, k_s;

4) $(i,j,k)\leftarrow$the plain-image pixel coordinate of $(0,d,0)$;

$g(0,d,0)\leftarrow$ the plain-image pixel gray value of $(0,d,0)$;

5) $j1=1$;

6) $(h,i,j)\leftarrow$the pixel coordinate that the $j1$th gray value of the chaotic cipher-image is $g(0,d,0)$;

if $(h,i,j)==(e,f,g)$, $j1$++, return 5);

7) $w=1$;

8) $g(0,d,wd)\leftarrow$the plain-image pixel gray value of $(0,d,wd)$;

$g'((h,i,j)+w(e,f,g))\leftarrow$ the chaotic cipher-image pixel gray value of $(h,i,j)+w(e,f,g)$;

to verify $g(0,d,wd)=g'((h,i,j)+w(e,f,g))$

if not, $j1$++ return 5);

else to verify $w\le 7$

if yes, w ++ return 7;

else continue;

9) Output the transformed image position (h,i,j) of $(0,d,0)$;

Copyright © 2010 MECS

10) $(k,l,m) \leftarrow$ the plain-image pixel coordinate of $(d,0,0)$;

$g(d,0,0) \leftarrow$ the plain-image pixel gray value of $(d,0,0)$;

11) $k1=1$;

12) $(k,l,m) \leftarrow$the pixel coordinate that the $k1$th gray value of the chaotic cipher-image is $g(d,0,0)$;

if $(k,l,m)==(h,i,j)$ or $(k,l,m)==(e,f,g)$

$k1$++, return 11);

13) $w=1$;

14) $g(d,0,wd) \leftarrow$the plain-image pixel gray value of $(d,0,wd)$;

$g'((k,l,m)+w(e,f,g)) \leftarrow$ the chaotic cipher-image pixel gray value of $(k,l,m)+w(e,f,g)$;

to verify $g(d,0,wd)=g'((k,l,m)+w(e,f,g))$

if not, $k1$++ return 11);

else to verify $w \le 7$

if yes, w ++ return 13);

else continue;

15) Output the transformed image position (k,l,m) of $(d,0,0)$;

16) By theorem 2, compute A using the results of (e,f,g), (h,i,j), (k,l,m);

17) To verify the obtained key using the plain-image and cipher-image

if yes, output the key; flag=1;

else flag=0; continue;

}

if(flag==1) break;

}

Depending on the characteristic of the encryption algorithm transformation, the attack algorithm always can find the equivalent key. The maximal exhaustion complex of k_l and k_s is 2^{32}, and computation complex of three pairs pixel positions ($(0,0,d)$, (e,f,g)), ($(0,d,0)$, (h,i,j)), ($(d,0,0)$, (e,f,g)) is $M_s'+M_s''+M_s'''$ times. So, the whole attack algorithm computation complex is

$$O(2^{32}(M_s'+M_s''+M_s''')).$$

Next, we will give an attack algorithm when the step 2 and step 3 iterate more than one times. Because of the structure of the encryption is S-P type, the algorithm 1 can not attack it. Considering the three-dimensional generalized Cat mapping only infect six independent parameters. If the initialized image size is $N_1 \times N_2$, and the every parameter's exhaustion complex is $N = \left\lfloor \sqrt[3]{N_1 \times N_2} \right\rfloor$, so the whole six parameters maximum exhaustion complex is $N^6 \approx (N_1 \times N_2)^2$, then the maximum equivalent key exhaustion complex is $N^6 \approx (N_1 \times N_2)^2$ when the algorithm iterates one times in this step. In step3, the key parameters is generated by the initialized key k_l and k_s, and the maximum exhaustion complex is 2^{32} in one iteration. When it iterates more than one times, [4][5] proposed a exhaustive attack on the algorithm. If every time the key parameters are generalized by the different 128-bit initialized key, set the iteration number is r, then the attack algorithm maximum computation complex is $2^{32r}(N_1 \times N_2)^{2r}$. We give two different kinds of attack algorithm: algorithm 2 suitable for the encryption scheme that iterates many times and every round uses the same key; algorithm 3 suitable for the encryption scheme that iterates many times and every round uses different key.

Algorithm 2:

Exhaust the values of $a_x, b_x, a_y, b_y, a_z, b_z$, where $a_x, b_x, a_y, b_y, a_z, b_z \in [0, N-1]$;

```
{
 --- {
     for ( k_l = 0 ; k_l < 2^16 ; k_l ++ )
     {
       for( k_s = 0 ; k_s < 2^16 ; k_s ++ )
       {
        generate L_i , S ;
        use the obtained key to decrypt the cipher-image;
        verify the decrypted image and plain-image
        if yes, output the key, flag=1, break;
         else flag=0, continue;
       }
      if (flag==1) break;
     }
     if (flag==1) break;
    }
---}
```

Algorithm 3:

Exhaust all the values of every round key;

```
{
--{
   generate L_i , S ;
  use the obtained key to decrypt the cipher-image;
  verify the decrypted image and plain-image
   if yes, output the key, flag=1, break;
```

```
else flag=0, continue;
    }
    if (flag==1) break;
 ---}
```

V. THE ANALYSIS OF THE ATTACK VALIDITY

The maximum computation complex of the algorithm 1, 2, 3 are $O(2^{32}M)$, $2^{32}(N_1 \times N_2)^2$ and $2^{32r}(N_1 \times N_2)^{2r}$. Take an 512×512 image encryption for example. Under the processing of the image encryption scheme, the value of N is $N = \sqrt[3]{512 \times 512} = 64$, even we assume that $M_s = 64^3$ (as we know, this is impossible, we can not obtain this cube). Under this condition, the maximum computation complex of algorithm 1 is

$$3 \times 2^{32} M_s = 3 \times 2^{32} \times 2^{18} < 2^{52}$$

And the computer complex is less than the number of key space of encryption key scheme, which is 2^{128}. Compared with the popular data encryption standard (DES), which efficient key is 2^{56}, but it is not safe with the enumerate attacking. So, we can realized the attack under the current compute ability

When the image encryption scheme iterate more than one times of Step2 and Step 3, we can attack the scheme using the algorithm 2. By analyzing the algorithm 2, the key parameters are obtained by same 128-bit initial key. When the image encryption size is $N_1 \times N_2$, The maximum computation complex of algorithm 2 is

$$2^{32} \times (N_1 \times N_2)^2,$$

When every key scheme iterates use different key parameters, and the number round of the image encryption scheme is *r*, then the maximum computation complex of algorithm 3 is

$$2^{32r}(N_1 \times N_2)^{2r}$$

In the same way, take an 512×512 image encryption for example. If the key parameters are produced by the same 128-bit initial key, the maximum computation complex of the whole algorithm is

$$2^{32}(N_1 \times N_2)^2 = 2^{32} \times 2^{36} = 2^{68}$$

This result is less than the key space 2^{128}.

We notice that all the computation results are less than the key number in the key space, meanwhile, both algorithm 1 and algorithm 2 can break the image encryption in the actual computation.

In the actual environment, in different round generally would not choose different independent key duo to the reasons such as key association. The use of the DES and AES can explain this point. Even if uses like this, Chen designed image encryption algorithm's effective key also cannot achieve the anticipated goal

VI. CONCLUSION

In this paper, some problems of a new image encryption scheme based on 3D Cat chaotic map are reported and three attacks on this cryptosystem have been presented. The main reason that Chen et al designed image encryption algorithm is not secure is the used chaotic transformation has a strong linear characteristic (proposed in [12][13][14]). And, the algorithm has equivalent key reducing the encryption secure strength.

In order to overcome this can introduce some non-linear transformations and change the key union method. These results also show that before introducing a new transformation into cryptography field, we must study the properties of the transformation (proposed in [15][16]). Introduce the corresponding transformations to overcome the weakness of used transformation's inherent weakness. Only in this way, the designed encryption algorithm can withstand the adversary's cryptanalysis.

REFERENCES

[1] Chen G,Mao Y, Chui C.K. "A symmetric image encryption scheme based on 3D chaotic Cat maps". Chaos, Solitons and Fractals .2004;21(7):749-761.

[2] C. P. Wu, C.C.J.Kuo. "Design of integrated multimedia compression and encryption systems", IEEE Transactions on Mulimedia. 2006, 7(5): 828-839.

[3] N. Pareek, V. Patidar, K. Sud. "Image encryption using chaotic logistic map", Image and Vision Computing. 2006, 24(9): 926-934.

[4] K. L. Chung, L. C. Chang. "Large encryption binary images with higher security", Pattern Recognition Letter, 1998, 19(5-6), 461-468.

[5] J. Fridrich. "Sysmetric cipher based on two-dimensional chaotic maps", Chaos, Solitions & Fractals, 2004, 21(3): 749-761.

[6] A. Pisarchik, N. Flores-Carmona, M. Carpio-Valadez. "Encryption and decryption of images with chaotic map lattices ", Chaos16, 2006.

[7] N. Bourbakis, C. Alexopoulos. "Picture data encryption using scan patterns," Pattern Recognition, 1992, 25(6):567-583.

[8] R. A. J. Matthews. "On the derivation of a chaotic encryption algorithm", Cryptologia, 1989, 13(1): 29-42.

[9] Fridrich J. "Image encryption based on chaotic maps", IEEE International Conference on Systems, Man, and Cybernetics, 1997, 1105-1110.

[10] Guo Jiansheng et al. Attack with known image to a symmetric image encryption scheme (in chinese). CCFTC 2006, 2006,16:361-369.

[11] Pan chengdong, Pan chengbiao. "Elementaty number theoty" (in chinese). Beijing: Beijing university press. 2001, 151-176.

[12] Shujun Li, Xuanqin Mou, Zhen Ji, Jihong Zhang. "Cryptanalysis of a class of chaotic stream ciphers" (in chinese). Journal of Electronics & Information Technology. 2003,25(4):473-479.

[13] Frey D R. Chaotic Digital Encoding: An approach to secure communication. IEEE Trans on CAS q,1993, 40(10): 660- 666.

[14] Hong Zhou, Jun Yu, and Xieting Ling. "Theoretical design of chaotic feed forward stream cipher". Acta Electronic Sinica, 1998,26(1):98-101.

Copyright © 2010 MECS

[15] Ding Wenxia, Lu Huanzhang, Wang Hao el at. “Fast gray code sequence subsection scrambling video encryption algorithm based on chaos system” (in chinese). Journal on Communications. 2007, 28(9): 34-39.

[16] Xu Shujiang, Wang Jizhi. “An improved block cryptosystem based on iterating chaotic map” (in chinese). Chinese Journal of Physics. 2008,57(1):37-41.

Jian-sheng Guo received the Bachelor Degree from the Henan University in Henan province, Master and PhD Degree from the Zhengzhou Information and Technology Institute. His main research interests include Image encryption, Chaots theory, and Information security.

Lei Zhang received the Bachelor Degree from the zhengzhou Information and Technology Institute. His research interests include Image encryption and block cipher cryptanalysis.

Copyright © 2010 MECS