Front. Electr. Electron. Eng. China 2009, 4(1): 5–9
DOI 10.1007/s11460-009-0016-z

RESEARCH ARTICLE

Feng HUANG, Yong FENG

Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm

Abstract The article proposes a new algorithm to improve the security of image encryption based on two-dimensional chaotic maps. Chaotic maps are often used in encrypting images. However, the encryption has periodicity, no diffusion, and at the same time, the real keys space of encryption are fewer than the theoretical keys space, which consequently results in potential security problems. Thus, this article puts forward several ways to solve the problems including adding diffusion mechanism, changing the design of keys and developing a composite encryption system. It designs an algorithm for the version B of the discretized baker map, which is one of the most prevalent chaotic maps, based on which a new image encryption is proposed to avoid the above problems. The simulation results show that the new encryption algorithm is valid and the result can be applied to other two-dimensional chaotic maps, such as the cat map.

Keywords chaotic map, baker map, image encryption

1 Introduction

Chaos has been widely used in cryptography in recent years [1–5]. However, some actual digital chaos systems face the problem of degradation dynamics [6,7]. The two-dimensional chaotic maps can 'stretch-and-fold' images by use of the natural features of images. Small changes in keys for a plain image can diffuse to everywhere in an encrypted image. At the same time, the analysis of keys is very difficult because there are too many combinations of encryption. Typical chaotic maps used for image encryption include the cat map, the baker map, the standard map, the tent map [8,9], etc. In Ref. [8], Fridrich proposes a class of invertible encryption systems based on the baker map. It uses a two-dimensional chaotic map to permutate the position of pixels. The permutations induced by the baker map behave as typical random permutations. The encryption has good diffusion properties with respect to the plain image and the keys. However, the baker map does not have a simple formula and the keys are limited by the size of the image. In Refs. [10,11] new image encryption schemes are constructed based on an extended three-dimensional chaotic baker map and the cat map.

There are similar characteristics in two-dimensional chaotic maps. With the two-dimensional baker map, the article analyzed security of image encryption and obtained factors for weakened encryption. Then the article designs a new image encryption based on the discretized baker map to improve security. The simulation results show that the new encryption algorithm is valid.

Translated from *Journal of Harbin Institute of Technology*, 2007, 39(9): 1411–1414 [译自: 哈尔滨工业大学学报]

Feng HUANG (✉)
Department of Electrical and Information Engineering, Hunan Institute of Engineering, Xiangtan 411104, China
E-mail: huangfeng@hit edu.cn

Yong FENG
School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China

2 Two-dimensional chaotic map

Image pixels can be arranged arbitrarily and any pixel can be inserted between adjacent pixels. The process of this arrangement can be regarded as the stretch-and-fold of images. The encryption of the two-dimensional chaotic map uses this feature. The cat map is a geometric transformation process. The line map stretches all the pixels to form a straight line, and then folds them according to laws. After the process the pixels in plain image are randomly distributed in the encrypted image and the adjacent pixels are no longer relevant. The baker map is one of the major chaotic maps. It stretches the image horizontally, and then folds it vertically. Repeating this process, the positions of all the pixels of the plain image are changed.

Assume a square image consisting of $N \times N$ pixels. It can be divided into k rectangle-shaped parts horizontally whose size is $[N_{i-1}, N_i] \times [0, 1]$ (here $i = 1, 2, ..., k$) and

$N_i = P_1 + P_2 + \cdots + P_i$ (here $N_0 = 0$, P_i is the rectangular width and $i \leqslant k$). Thus to any (x, y) in the parts $[N_{i-1}, N_i] \times [0, 1]$, the formula of the baker map is

$$B(x', y') = A\left(\frac{1}{P_i}(x - N_i),\ P_i y + N_i\right),$$

where $i = 1, 2, \ldots, k$.

To encrypt the image the baker map must be discretized. For different keys, the discretized baker map is divided into two versions: version A and version B. When the map is of version A, every part of the keys is the divisor of the image size. The formula of version A is

$$B(x', y') = A\left(\frac{N}{n_i}(x - N_i) + y \bmod \frac{N}{n_i},\ \frac{n_i}{N}\left(y - y \bmod \frac{N}{n_i}\right) + N_i\right),$$

where $N = n_1 + n_2 + \cdots + n_k$, $N_i = n_1 + n_2 + \cdots + n_i$, $N_i \leqslant x < N_i + n_i$.

Take an image with 8×8 for example. If the Key = (2, 2, 4), the process of encryption can be seen in Fig. 1.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

baker

13	5	14	6	15	7	16	8
29	21	30	22	31	23	32	24
45	37	46	38	47	39	48	40
61	53	62	54	63	55	64	56
27	19	11	3	28	20	12	4
59	51	43	35	60	52	44	36
25	17	9	1	26	18	10	2
57	49	41	33	58	50	42	34

Fig. 1 Process of encryption by version A of baker map

When part of the keys is not the divisor of the image size, the encryption uses version B of the discretized baker map. In Ref. [8], version B has no common formula. Taking an image with 8×8 for example. If the Key = (3, 5), encryption can be seen in Fig. 2.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

baker

4	5	14	6	15	7	16	8
20	12	21	13	22	23	32	24
28	37	29	38	30	39	31	40
44	36	45	46	55	47	56	48
60	52	61	53	62	54	63	64
9	1	18	10	2	19	11	3
33	25	17	34	26	43	35	27
57	49	41	58	50	42	59	51

Fig. 2 Process of encryption by version B of baker map

The article first gives an algorithm for version B of the baker map. If the image consists of $N \times N$ pixels, the pixel (x, y) in the image is mapped to (x', y') by the baker map.

Here, Key = $(n_1, n_2, \ldots, n_k)$ $(N = n_1 + n_2 + \cdots + n_k,\ i = 1, 2, \ldots, k)$, n_i is not the divisor of N.

If $N_i \leqslant x < N_i + n_i$, $0 \leqslant S < N$, we suppose

$$m = \text{floor}\left(\frac{(x - N_i) + (N - y) \times n_i - 1}{N}\right),$$

$$d_n = \text{floor}\left(\frac{N - S_n}{n_k}\right) + 1,$$

$$S_{n+1} = d_n \times n_i + S_n - N \qquad (S_1 = 0,\ 1 \leqslant n \leqslant n_i).$$

First, we have $y' = N - N_i - m_i - 1$. Then

1) if $x - N_i \leqslant n_i - S_{m+1}$, when $x - N_i \leqslant n_i - S_{m+2}$, we have

$$x' = (x - N_i - 1) \times d_{m+1} + N - y - \sum_{i=1}^{m} d_m;$$

when $x - N_i > n_i - S_{m+2}$, we have

$$x' = (n_i - S_{m+2}) \times d_{m+1} + [x - (n_i - S_{m+2}) - 1] \times (d_{m+1} - 1) + N - y - \sum_{i=1}^{m} d_m.$$

2) if $x - N_i > n_i - S_{m+1}$, when $x - N_i \leqslant n_i - S_{m+2}$, we have

$$x' = (n_i - S_{m+1}) \times d_{m+1} + [x - (n_i - S_{m+1}) - 1] \times (d_{m+1} + 1) + N - y - \sum_{i=1}^{m} d_m + 1;$$

when $x - N_i > n_i - S_{m+2}$, $S_{m+2} \geqslant S_{m+1}$, we have

$$x' = (n_i - S_{m+2}) \times d_{m+1} + (S_{m+2} - S_{m+1}) \times (d_{m+1} - 1) + [x - (n_i - S_{m+1}) - 1] \times d_{m+1} + N - y - \sum_{i=1}^{m} d_m + 1;$$

when $x - N_i > n_i - S_{m+2}$, $S_{m+2} < S_{m+1}$, we have

$$x' = (n_i - S_{m+1}) \times d_{m+1} + (S_{m+1} - S_{m+2}) \times (d_{m+1} + 1) + [x - (n_i - S_{m+2}) - 1] \times d_{m+1} + N - y - \sum_{i=1}^{m} d_m + 1.$$

The algorithm by C programming language is as follows:

```
for(j = 1; j < n_k; j ++)
{
        if(n_k − 1 < S_{n+1})
            m = 1;
        else
            m = 0;
        if(n_k − 1 < S_{n+2})
            n = 1;
```

```
        else
            n = 0;
        for(i = 1 − m; i ⩽ d_{n+1} − n; i ++)
        {
            x = N − (i − 1) − Σ_{i=1}^{n} d_n;
            y = N − N_i − m_i − 1;
        }
}
```

In Ref. [11], there is a formula of version *B* of the baker map. However, the direction of the map is different from the map in Ref. [8].

The keys space in version *A* of the baker map can be seen in Table 1.

Table 1 Keys space of version *A*

N	*K*(*N*)	*N*	*K*(*N*)	*N*	*K*(*N*)
4	5	10	128	16	5271
6	24	12	1627	18	45315
8	55	14	741	20	83343
9	19	15	449	21	3320

The keys space of version *B* is $K(N)= 2^{N-1}$. Obviously, it is much bigger than that of version *A*.

3 Security analysis of encryption of two-dimensional chaotic map

Because there are too many possible combinations of substitution algorithms and replacement algorithms of the two-dimensional chaotic map, analysis of the keys is very difficult. Currently, the ways of attacking keys are very few. However, the encryptions by the two-dimensional chaotic map inherently have potential security problems.

1) Encrypting an image by the two-dimensional chaotic map is only a process of permutation. Because the size of the image is limited, the process is cyclical. Acting as the baker map, pixels will first be divided by the keys. Then it stretches the image horizontally and folds it vertically. The cat map is a geometric transformation process. The line map stretches all the pixels to form a straight line, and then folds them according to laws. When the number of the transformation by these two-dimensional maps is small, the pixels of the image can be very confusing. However, because the image is a group of pixels, the combinations of pixels are limited. According to the feature of the system, the encrypted image can be restored to the plain image by mapping. Thus, if the encryption algorithm is known, an encrypted image can be chosen arbitrarily. By mapping the encrypted image and repeating the process, the plain image may be restored.

2) The encryption of the two-dimensional chaotic map is a technique without information loss. It only changes the position of pixels instead of the value of the pixels. Therefore, the encryption cannot resist cipher-text-only attack. Before encryption, it can choose a pixel (x, y) and then change its value to (x', y'), which is a special act as (0, 0). After encryption it can find pixels whose value is (x', y'). Repeating the process, it can validate a group of relationships between the pixels in the plain image and the ones in the encrypted image. Storing those relationships and creating a table. Using the table, the encrypted image may be restored to the plain image without keys.

3) The actual keys space is far less than the theoretic one. It can be seen in Fig. 3 that most of the plain image can be restored even with error keys. This is because images have visibility, and their part also has visibility and can be identified. Taking the baker map for example, in encryption, the image will be a division. If the difference between the parts of the plain image is little, the parts in the encrypted image are also similar, and thus it can attack the encrypted image by different keys.

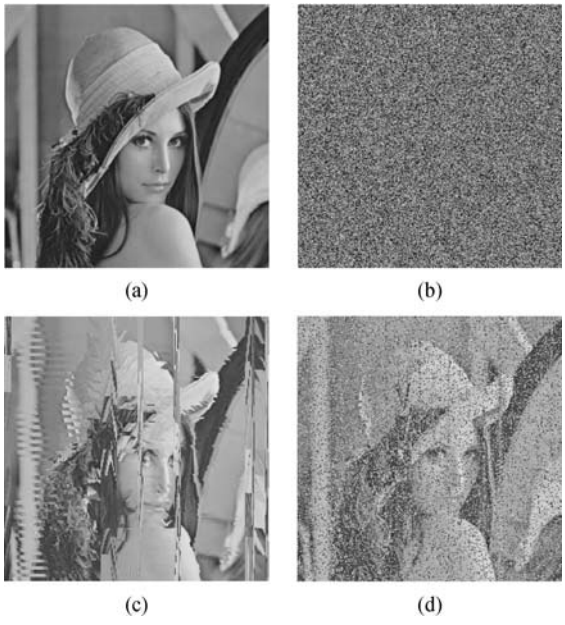

Fig. 3 Decryption with error keys. (a) Plain image; (b) encrypted image; (c) decryption with error keys; (d) decryption with error keys

To improve the security of encryption of the two-dimensional chaotic map, several improvements should be made.

1) Because the combinations of encryption are limited, the keys space can be enlarged and the number of iterations reduced to ensure the security of encryption.

The methods of adding keys space uses the general formula, increases the length of keys and takes a part of the keys to encrypt the image, and designs a composite encryption system, uses random sequence to modify the keys before encryption.

2) Confuse the value of pixels and change the demographic characteristics of the encrypted image. One simple method is using a little XOR function: $(x', y') = (x, y) \oplus (i \times j) \bmod N$. By the function, the histogram of the encrypted image is uniformly distributed. Another method is using XOR with a random sequence.

3) Designing a composite image encryption system can improve the security of encryption with several chaotic maps. Two classes of methods are presented. One is changing the value of pixels. Use the baker map and cat map to encrypt the image in order. The keys space of encryption can be enlarged. The other method is changing the pixels with some chaotic maps. The encryption might resist the ciphered-text attack and avoid regional analysis.

4) Develop the two-dimensional map to be a higher-dimensional map. After that, the speed of encryption is higher and encryption is more difficult to attack. In Ref. [10], the two-dimensional cat map is developed to a three-dimensional map. In Ref. [11], the baker map is also developed to be a three-dimensional one. These three-dimensional maps are proved to have an encryption that is faster with larger keys space.

4 Improved algorithm of encryption with two-dimensional chaotic map

Some chaotic maps are used, including PWLCM, logistic map and baker map, to design a composite image encryption system. Using the logistic map,

$$X_{n+1} = a \times X_n \times (1 - X_n), \tag{1}$$

here, $a \in (0, 4]$, $X_n \in (0, 1)$, $n = 1, 2, 3$.

First, design an encryption algorithm. Suppose the image size is $m \times n$, with 256 levels of gray, where the Key $= (n_1, n_2, ..., n_k, ..., n_{uk})$. Key_1 and Key_2 are parts of the Key respectively. The initial values of the logistic map are a, N. The whole algorithm includes two steps.

The first step: according to $\text{Key}_1 = (n_1, n_2, ..., n_k)$,

1) Calculate $X_{0i} = n_i/m\,(i = 1, 2, ..., k)$ (two significant digits);

2) By Eq.(1), it can get a chaotic sequence with X_{0i}, a. Then take a subsequence $S_i = (a_1, a_2, ..., a_{i\times n})$ from the sequence from the beginning of the N whose length is $n_i \times n$;

3) Calculation:

$$S_i \Rightarrow S_i'.$$

Here, S_i' is a sequence that chooses three digits after the decimal point from the sequence S_i and mods with 256. Thus $0 \leqslant S_i' \leqslant 256$;

4) Set n_i as the keys in encryption with the baker map. Then take the value of pixels XOR with S_i' one by one.

The second step: encrypt the image with k keys in $\text{Key}_2 = (n_{k+1}, n_{k+2}, ..., n_{2k}, ..., n_{uk})$.

The above algorithm is applicable to other chaotic maps.

Use the encryption algorithm to encrypt a Lena image. Suppose the image size is 256×256, the process can be seen in Fig. 4. The keys of the encryption is $\text{Key}_1 = (7, 74, 13, 9, 7, 19, 4, 31, 4, 3, 63, 5, 2, 11, 3, 1)$, $m = 1$, $n = 10$, $a = 4$, $N = 1000$. To test the sensitivity of keys, error keys are used to attack the encrypted image.

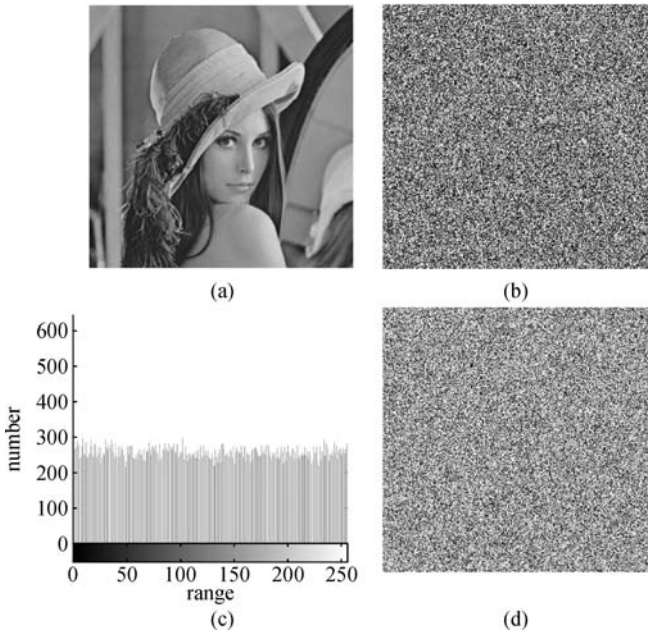

Fig. 4 Simulation of algorithm. (a) Plain image; (b) encrypted image; (c) histogram of encrypted image; (d) decryption with error keys

5 Conclusions

The article first analyzed the security of encryption with a two-dimensional map. Then it proposes some methods to improve it to avoid features that weaken security.

A new encryption algorithm is designed for a composite encryption system. In the encryption, the values of pixels are changed and the keys spaces are enlarged. With the baker map, the algorithm solves the problem of adopting two keys of little difference in encryption. The improved algorithm is applicable to all chaotic maps.

The encryption with chaotic maps is simple and effective and it is easy for hardware implementation.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant No. 60474016), the Scientific Research Foundation of Hunan Provincial Education Department (No. 08B015).

References

1. Schneier B. Applied Cryptography – Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons, Inc., 1996
2. Shannon C E. Communication theory of secrecy systems. The Bell

System Technical Journal, 1949, 28(4): 656–715
3. Matthews R. On the derivation of a “chaotic” encryption algorithm. Cryptologia, 1989, 13(1): 29–42
4. Dachselt F, Schwarz W. Chaos and cryptography. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(12): 1498–1509
5. Lian S G, Sun J S, Wang J W, Wang Z Q. A chaotic stream cipher and the usage in video protection. Chaos, Solitons & Fractals, 2007, 34(3): 851–859
6. Wheeler D D. Problems with chaotic cryptosystems. Cryptologia, 1989, 13 (3): 243–250
7. Li S J, Mou X Q, Cai Y L, Ji Z, Zhang J H. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Computer Physics Communications, 2003, 153(1): 52–58
8. Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259–1284
9. Feng Y, Li L J, Huang F. A symmetric image encryption approach based on line maps. In: Proceedings of the 1st International Symposium on Systems and Control in Aerospace and Astronautics (ISSCAA 2006). 2006, 1362–1367
10. Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 2004, 21(3): 749–761
11. Mao Y B, Chen G R, Lian S G. A novel fast image encryption scheme based on 3D chaotic baker maps. International Journal of Bifurcation and Chaos, 2004, 14(10): 3613–3624