CRYPTANALYSIS OF A CHAOTIC IMAGE ENCRYPTION METHOD

Shujun Li [1], *Xuan Zheng* [2]

[1] Institute of Image Processing, School of Electronics and Information Engineering
Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China
E-mail: hooklee@mail.com
[2] Department of Electrical Engineering, Polytechnic University
5 MetroTech Center, Brooklyn, NY 11201
E-mail: zhxfifa@photon.poly.edu

ABSTRACT

The security of digital images attracts much attention recently, and many image encryption methods have been proposed. In ISCAS2000, a new chaotic key-based algorithm (CKBA) for image encryption was proposed. This paper points out CKBA is very weak to the chosen/known-plaintext attack with only one plain-image, and its security to brute-force ciphertext-only attack is overestimated by the authors. That is to say, CKBA is not secure at all from cryptographic viewpoint. Some experiments are made to show the feasibility of the chosen/known-plaintext attack. We also discuss some remedies to the original scheme and their performance, and we find none of them can essentially improve the security of CKBA.

1. INTRODUCTION

In the digital world nowadays, the security of digital images becomes more and more important since the communications of digital products over network occur more and more frequently. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image database/communications and confidential video conferencing, etc. In order to fulfill such a task, many image encryption methods have been proposed [1–9] to protect the content of digital images, but some of them [7–9] have been known to be insecure [2, 10].

In [1], a chaotic key-based algorithm (CKBA) for image encryption was proposed, which is a value substitution cipher. This paper estimates its security and points out that known-plaintext and chosen-plaintext attacks can break it with only one known/chosen plain-image. In addition, its security to brute-force ciphertext-only attack is overestimated by the authors. So CKBA is not secure at all from the strongly cryptographic viewpoint. We also discuss some possible remedies and their performance.

This paper is organized as follows. In section 2, a brief introduction of CKBA is given. Cryptanalytic studies are given in section 3, and the experimental results in section 4. Section 5 discusses some remedies of CKBA and their performance. The last section is the concludes.

2. CKBA IMAGE ENCRYPTION METHOD

The encryption procedure of CKBA can be briefly depicted as follows. Assume the size of the plain-image is $M \times N$. Select two bytes $key1$ and $key2$ (8 bits) and the initial condition $x(0)$ of a one-dimensional chaotic system as the secret keys of the encryption system. Run the chaotic system to make a chaotic sequence $\{x(i)\}_{i=0}^{MN/8-1}$ (Assume $MN|8$). Generate a pseudo-random binary sequence (PRBS) $\{b(i)\}_{i=0}^{2MN-1}$ from the 16-bit binary representation of $x(i) = 0.b(16i+0)b(16i+1)\cdots b(16i+15)$. Once $\{b(i)\}$ is generated, the encryption can start. For the plain-pixel $f(x,y)(0 \le x \le M-1, 0 \le y \le N-1)$, the corresponding cipher-pixel $f'(x,y)$ is determined by the following rule:

$$f'(x,y) = \begin{cases} f(x,y) \text{ XOR } key1, b'(x,y) = 3 \\ f(x,y) \text{ XNOR } key1, b'(x,y) = 2 \\ f(x,y) \text{ XOR } key2, b'(x,y) = 1 \\ f(x,y) \text{ XNOR } key2, b'(x,y) = 0 \end{cases}, \quad (1)$$

where $b'(x,y) = 2 \times b(l) + b(l+1)$ and $l = x \times N + y$. The decryption procedure is just like the encryption since XOR and XNOR are both involutive operations. Because not all secret keys can make well disorderly cipher-images, the basic criterion to select $key1$ and $key2$ should be satisfied: $\sum_{i=0}^{7}(a_i \oplus d_i) = 4$, where $key1 = \sum_{i=0}^{7} a_i \times 2^i$ and $key2 = \sum_{i=0}^{7} d_i \times 2^i$.

3. CRYPTANALYSIS

3.1. Ciphertext-Only Attack

The authors of [1] claimed that the attack complexity of CKBA is 2^{2MN} since $\{b(i)\}_{i=0}^{2MN-1}$ has $2MN$ bits. Actually, such a statement is not true because of the following fact: total $2MN$ bits are uniquely determined by the equation of the chaotic system and its initial condition $x(0)$, which has only 16 secret bits. Actually, the secret keys of CKBA are $key1$, $key2$ and $x(0)$, we can find the right secret keys with brute-force ciphertext-only attack. Since the keys totally contain $2 \times 8 + 16 = 32$ bits, the key entropy should be about 32. But not all keys can be used in CKBA because of the basic criterion $\sum_{i=0}^{7}(a_i \oplus d_i) = 4$, only $2^{16} \times 2^8 \times C_8^4 = 2^{24} \times 70 \approx 2^{30}$ keys are available in total $2^{16} \times 2^8 \times 2^8 = 2^{16}$ ones. Thus the key entropy is about $14 + 16 = 30$.

The exact attack complexity can be estimated as follows. Averagely, $2^{15} \times MN/8$ chaotic iterations are needed for the generation of $\{b(i)\}$, and $(2^8 \times 70/2) \times MN = 8960 \times MN \approx$

$2^{13} \times MN$ XOR/XNOR operations are needed to decrypt the cipher-image, then the total attack complexity is about $2^{15+13-3} \times (MN)^2 = 2^{25} \times (MN)^2$, which is much smaller than 2^{2MN} when M, N are not too small ($M > 4, N > 4$). That is to say, the security of CKBA is overestimated by the authors, even under brute-force attack. Because of the rapid progress of digital computer and distributed arithmetic, the complexity not lower than 2^{128} is required for a strict cipher, but CKBA can not provide enough security. Without loss of generality, assume $M = N = 512 = 2^9$, which is the typical size of a "large" digital image, the attack complexity will be only $2^{25} \times (MN)^2 = 2^{63}$.

3.2. Known-Plaintext and Chosen-Plaintext Attacks

Under known-plaintext or chosen-plaintext attack, CKBA can be broken with only one plain-image and its cipher-image. Assume one knows a plain-image f and the corresponding cipher-image f' (both $M \times N$). For the plain-pixel $f(x, y)$, the cipher-pixel $f'(x, y)$ must be one of the four values: $f(x, y)$ XOR $key1$, $f(x, y)$ XNOR $key1$, $f(x, y)$ XOR $key2$, $f(x, y)$ XNOR $key2$. Since a XNOR $b = a$ XOR $\overline{b}$, $f(x, y)$ XOR $f'(x, y)$ must be one of the four values: $key1$, $\overline{key1}$, $key2$, $\overline{key2}$. Therefore, if we XOR f and f', we can get a mask image f_m, which can be used to decrypt other cipher-images encrypted with the same key K if their sizes are not larger than $M \times N$. For a plain-image whose size is larger than MN, the left MN pixels can be also decrypted directly. The computation complexity obtaining f_m is only $O(MN)$, and is independent of $key1$, $key2$ and $x(0)$.

If we want to entirely decrypt a plain-images with larger size, the right secret key $K = \{key1, key2, x(0)\}$ must be known. Based on f_m, it is rather easy to deduce K. Because f_m only contains four possible gray values: $\{key1, \overline{key1}, key2, \overline{key2}\} = \{k_1, k_2, k_3, k_4\}$, we can find the right $key1$ and $key2$ by brute-force search. The search procedure can be described as the following steps.

Step 1: Assume $key1 = k_m$ (for $m = 1 \sim 4$), and $key2 = k'_{m'}$ (for $m' = 1 \sim 2$), where k'_1 and k'_2 are the two possible values of $key2$ when $key1$ is determined (the other two are $key1$ and $\overline{key1}$);
Step 2: Calculate $b'(x, y)$ for all pixels using the following rule:

$$b'(x,y) = \begin{cases} 3, f_m(x,y) = key1 \\ 2, f_m(x,y) = \overline{key1} \\ 1, f_m(x,y) = key2 \\ 0, f_m(x,y) = \overline{key2} \end{cases}. \quad (2)$$

Step 3: Generate the chaotic orbits $\{x(i)\}_{i=0}^{MN/8-1}$ from $b'(x, y)$.
Step 4: Verify whether or not $\{x(i)\}_{i=0}^{MN/8-1}$ satisfies the chaotic equation. If the answer is yes, the search procedure stops and output the current $key1$, $key2$ and $x(0)$, which are the right secret keys K. Here please note that we need not calculate the whole chaotic orbit $\{x(i)\}_{i=0}^{MN/8-1}$, just two chaotic values $x(0)$ and $x(1)$ are enough to make correct judgement.

Apparently, the computation complexity from f_m to K is chiefly determined by step 2 and 3. Generally speaking, the complexity is $O(MN)$, which approximately equals to the one obtaining f_m.

There is another possible method to decrypt any plain-image whose size is larger than the size of the known/chosen plain-image. When chaotic systems are realized under finite computing precision L, the cycle length of the chaotic orbits will be much smaller than 2^L [11,12]. For CKBA, the finite precision $L = 16$, the cycle length of each chaotic orbit will be much smaller than 2^{16}, which is not large enough in comparison with the size of many plain-images. For a 256×256 image, the total length of the chaotic orbit $\{x(i)\}$ is $MN/8 = 2^{13}$, for almost every initial condition $x(0)$, the cycle length of $\{x(i)\}$ is even much smaller than 2^{13}. Consequently, it is possible to derive any mask image with larger size from the known mask image f_m whose size is about $256 \times 256 = 2^{16}$. That is to say, without extracting the right secret key K, a 256×256 mask image f_m is enough to decrypt all plain-images. Such a result is supported by our experiments (see the next section and Fig. 4). Assume the size of the larger plain-image is $M' \times N'$, the complexity from f_m to f'_m will be $O(M'N' + MN)$, which is a little larger than the one obtaining f_m.

As we know, the known-plaintext and chosen-plaintext attacks will be very meaningful if a same key is used to encrypt more than one plaintexts, especially in the case that a larger number of plaintexts are all encrypted with a same key [13]. For a "good" cipher, the capability to resist known-plaintext attack is very important and generally needed. It is because of the following fact: the key management will be very complex, inconvenient and inefficient in many applications, if any key must not be used to encrypt more than one plaintexts. Apparently, it is not advisable to apply CKBA to encrypt MPEG video as claimed in [1]. Once one plain-frame in the encrypted MPEG video stream is known for an illegal user, he can easily get all other plain-frames, i.e., the whole video stream.

4. EXPERIMENTS

To verify the feasibility of the above known-plaintext and chosen-plaintext attacks, we give some experimental results in this section. The logistic map is selected as the chaotic system with the control parameter $r = 4$:

$$x_{n+1} = 4x_n(1 - x_n). \quad (3)$$

The logistic map is realized with 16-bit computing precision.

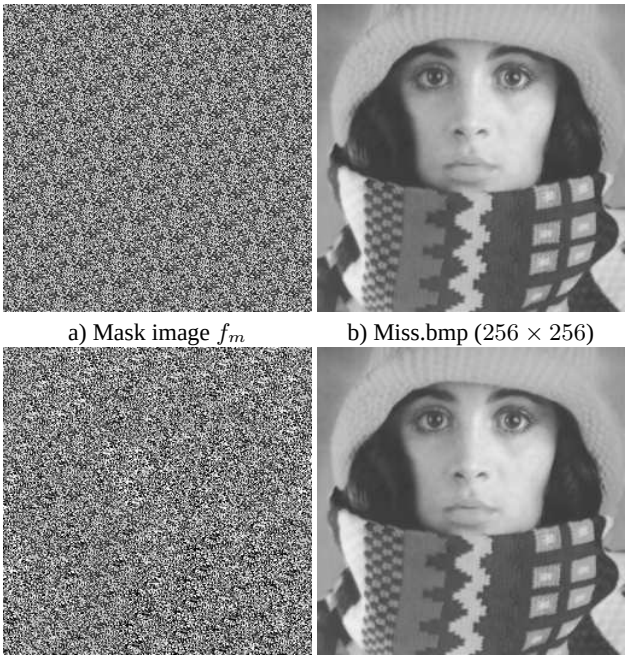
a) Lenna.bmp (256×256) b) Encrypted Lenna.bmp

Fig. 1. One known/chosen plain-image and its cipher-image

For a pseudo-randomly selected key $K = \{key1, key2, x(0)\}$, one 256×256 plain-image f (Lenna.bmp) and its cipher-image f' are given in Fig. 1. We can easily get the mask image $f_m = f$ XOR f' (Fig. 2a).

When the key K is used to encrypt another plain-image with identical size (see Fig. 2b–c), the plain-image can be directly decrypted by f_m (see Fig. 2d).

When the key K is used to encrypt a larger plain-image (384×384, see Fig. 3a–b), f_m can only decrypt MN pixels from the left

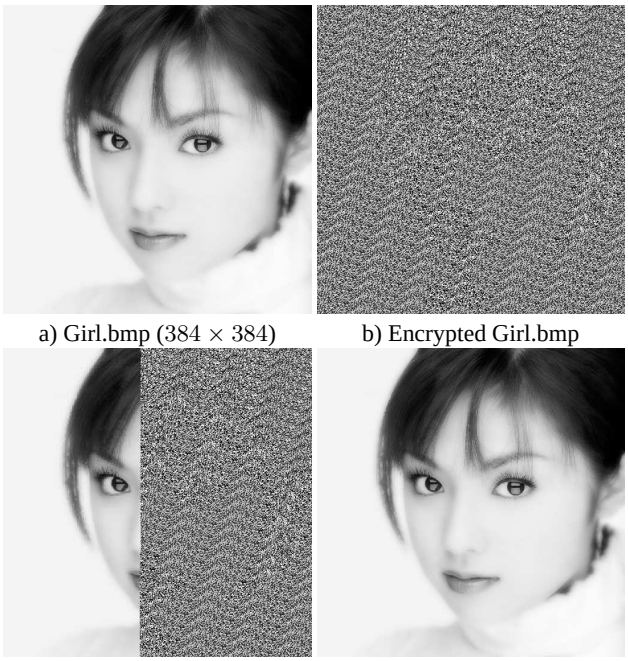


a) Mask image f_m b) Miss.bmp (256×256)

c) Encrypted Miss.bmp d) Decrypted Miss.bmp by f_m

Fig. 2. Cryptanalyze Miss.bmp using f_m

side (see Fig. 3c). To decrypt the whole plain-image, we can derive the right key K from f_m. Using the method described in the last section, we can get $key1 = 92, key2 = 36, x(0) = 12830/2^{16}$, and then the whole plain-image can be decrypted (see Fig. 3d).

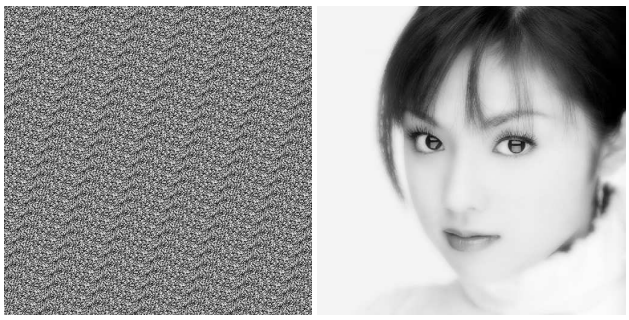


a) Girl.bmp (384×384) b) Encrypted Girl.bmp

c) Decrypted Girl.bmp by f_m d) Decrypted Girl.bmp by K obtained from f_m

Fig. 3. Cryptanalyze Girl.bmp using extracted K from f_m

In the last section, we have mentioned another method to decrypt larger plain-images. Observe f_m (Fig. 2c) obtained from the known/chosen plain-image Lenna.bmp (256×256), we can see some obvious pattern occurs repeatedly for 9 times. It means that the cycle length of $\{x(i)\}_{i=0}^{MN/8-1}$is about $2^{16}/(8 \times 9) = 2^{16}/72$. As a result, we can easily generate the mask image f'_m for 384×384 plain-images from f_m, which is shown in Fig. 4a. The decrypted plain-image Girl.bmp using f'_m is shown in Fig. 4b.



a) Mask image f'_m (384×384) generated from f_m (256×256) b) Decrypted Girl.bmp by f'_m

Fig. 4. Cryptanalyze Girl.bmp using f'_m generated from f_m

5. HOW TO IMPROVE CKBA?

In above sections, we have shown CKBA image encryption method is not secure enough to ciphertext-only, known-plaintext and chosen-plaintext attacks, from both theoretical and experimental viewpoints. In this section, we will study some remedies to CKBA and their performance of improving the security of CKBA.

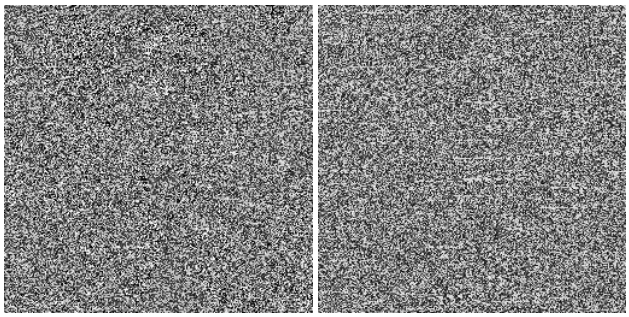
The simplest idea to enhance the original encryption scheme is increasing the bit size (n) of $key1$ and $key2$, and the one (n') of $x(0)$. Accordingly, the basic criterion should be changed to $\sum_{i=0}^{7}(a_i \oplus d_i) = n/2$ [1]. Such a simply enhanced CKBA will be stronger to ciphertext-only attack. Assume $n > 8$ and $n' > 16$, we can calculate the attack complexity is $(2^{n'-1}/(n'/2)) \times (2^n \times C_n^{n/2}/2) \times (MN)^2 = 2^{n+n'-1}/n' \times C_n^{n/2} \times (MN)^2$. When $n = n' = 32$ (consider the fact that 32-bit data is widely used in digital computers) and $M = N = 512 = 2^9$, the complexity will be approximately $2^{123.16}$. In addition, when $n' = 32$, the cycle length of $\{x(i)\}_{i=0}^{MN/8-1}$ will be large enough for almost all plain-images[2], so it will be impossible to generate larger f'_m from a known f_m. However, it can not lower the complexity extracting K from f_m, since the complexity is just determined by M and N.

Another remedy is to add the control parameter(s) of the employed chaotic system as a secret sub-key. It can only enhance the capability against ciphertext-only attack, because different control parameters will make entirely different chaotic orbits even when the initial conditions are same. But it can not enhance the security to known-plaintext and chosen-plaintext attacks, either. Apparently, f_m can still be obtained without knowing the secret control parameter, and then the control parameter and the initial condition can be simultaneously extracted from the chaotic orbits.

[1] The basic criterion can also be replaced with some other ones, such as $\sum_{i=0}^{7}(a_i \oplus d_i) \in [n_1, n_2] \subseteq [1, n-1]$. Such a trivial modification can increase the attack complexity to ciphertext-only attack by some bits.

[2] Even for a "huge" image (4096×4096), MN is only $2^{24} \ll 2^{32}$.

Finally, let us discuss what the condition will be if some other advanced algorithms [14–16] are employed to generate chaotic generate pseudo-random binary sequence $\{b(i)\}_{i=0}^{2MN-1}$. Apparently, they will make the extraction of K from f_m more difficult. But f_m is still available to decrypt the plain-image whose size is not much larger than the size of the known/chosen plain-image, and the complexity of ciphertext-only attack will not be influenced. To avoid the generation of larger f'_m from the known f_m, larger n' or the floating-point arithmetic is suggested being used to generate $\{x(i)\}_{i=0}^{MN/8-1}$. In Fig. 5, we show the cipher-image of Lenna.bmp and the mask image under floating-point arithmetic. It can be seen that the mask image and the cipher-image are more disorderly than the ones given in Fig. 1b and Fig. 2a. However, the advanced algorithms and floating-point arithmetic need more computation complexity, so the enhanced CKBA will run slower than the original one.



a) Encrypted Lenna.bmp with floating-point arithmetic

b) Mask image with floating-point arithmetic

Fig. 5. Using floating-point arithmetic in CKBA

To sum up, it is easy to enhance the security of CKBA to ciphertext-only attack, but it is rather difficult to essentially enhance the security to known-plaintext and chosen-plaintext attacks. In fact, the essential reason of the above known-plaintext and chosen-plaintext attacks is the encryption procedure of CKBA (see Eq. (1)). But if we change the encryption procedure, CKBA will become an entirely different encryption scheme.

6. CONCLUSION

In this paper, we point out that the CKBA image encryption method proposed in [1] is not secure enough to the ciphertext-only, known-plaintext and chosen-plaintext attack. Detailed cryptanalytic investigations are given and some experiments are made to verify the feasibility of the known/chosen-plaintext attack. We also discuss some remedies to the original scheme and their performance, but none of them can essentially improve the security of CKBA. We suggest not using CKBA in any strict applications, except when it can be ensured that any secret key will never been used repeatedly to encrypt more than one plain-images.

Acknowledgement

The authors would like to thank Miss Yanghui Cao at Xi'an Jiaotong University for her help in the preparation of this paper.

7. REFERENCES

[1] Jui-Cheng Yen and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption," in *Proc. IEEE Int. Conf. Circuits and Systems*, 2000, vol. 4, pp. 49–52.

[2] Howard Cheng and Xiaobo Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[3] Philip P. Dang and Paul M. Chau, "Image encryption for secure internet multimedia applications," *IEEE Trans. Consumer Electronics*, vol. 46, no. 3, pp. 395–403, 2000.

[4] Masaki Miyamoto, Kiyoshi Tanaka, and Tatsuo Sugimura, "Truncated Baker transformation and its extension to image encryption," in *Proc. SPIE*, 1999, vol. 3814, pp. 13–25.

[5] Jiri Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[6] Josef Scharinger, "Fast encryption of image data using chaotic kolmogrov flows," *J. Electronic Imaging*, vol. 7, no. 2, pp. 318–325, 1998.

[7] Henry Ker-Chang Chang and Jiang-Long Liu, "A linear quadtree compression scheme for image encryption," *Signal Processing: Image Communication*, vol. 10, pp. 279–290, 1997.

[8] C. Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou, "Image encrytion method using a class of fractals," *J. Electronic Imaging*, vol. 4, no. 3, pp. 251–259, 1995.

[9] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.

[10] Jinn-Ke Jan and Yuh-Min Tseng, "On the security of image encryption method," *Information Processing Letters*, vol. 60, pp. 261–265, 1996.

[11] Philippe M. Binder and Roderick V. Jensen, "Simulating chaotic behavior with finite-state machines," *Physical Review A*, vol. 34, no. 5, pp. 4460–4463, 1986.

[12] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai, "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding," in *Cryptography and Coding - 8th IMA Int. Conf. Proc.* 2001, Lecture Notes in Computer Science, vol. 2260, pp. 205–221, Springer-Verlag, Berlin.

[13] Bruce Schneier, *Applied Cryptography – Protocols, algorithms, and souce code in C*, John Wiley & Sons, Inc., New York, second edition, 1996.

[14] Tohru Kohda and Akio Tsuneda, "Statistics of chaotic binary sequences," *IEEE Trans. Information Technology*, vol. 43, no. 1, pp. 104–112, 1997.

[15] Zhou Hong and Ling Xieting, "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurcation and Chaos*, vol. 7, no. 1, pp. 205–213, 1997.

[16] Li Shujun, Mou Xuanqin, and Cai Yuanlong, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in *Progress in Cryptology - INDOCRYPT 2001*. 2001, Lecture Notes in Computer Science, vol. 2247, pp. 316–329, Springer-Verlag, Berlin.