Cryptanalysis of an Image Encryption Scheme Based on a Compound Chaotic Sequence

Chengqing Li [a,*], Shujun Li [b,*], Guanrong Chen [a] and Wolfgang A. Halang [b]

[a] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong SAR, China*

[b] *FernUniversität in Hagen, Lehrstuhl für Informationstechnik, 58084 Hagen, Germany*

Abstract

Recently, an image encryption scheme based on a compound chaotic sequence was proposed. In this paper, the security of the scheme is studied and the following problems are found: (1) a differential chosen-plaintext attack can break the scheme with only three chosen plain-images; (2) there is a number of weak keys and some equivalent keys for encryption; (3) the scheme is not sensitive to the changes of plain-images; and (4) the compound chaotic sequence does not work as a good random number resource.

Key words: Cryptanalysis, image encryption, chaos, differential chosen-plaintext attack, randomness test

⋆ This paper has been accepted by *Image and Vision Computing* in September 2008.

* Corresponding authors: Chengqing Li (swiftsheep@hotmail.com), Shujun Li (http://www.hooklee.com).

1 Introduction

Security of multimedia data is receiving more and more attention due to the widespread transmission over various communication networks. It has been noticed that the traditional text encryption schemes fail to safely protect multimedia data due to some special properties of these data and some specific requirements of multimedia processing systems, such as bulky size and strong redundancy of uncompressed data. Therefore, designing good image encryption schemes has become a focal research topic since the early 1990s. Inspired by the subtle similarity between chaos and cryptography, a large number of chaos-based image encryption schemes have been proposed [1–6]. Unfortunately, many of these schemes have been found insecure, especially against known and/or chosen-plaintext attacks [7–10]. For a recent survey of state-of-the-art image encryption schemes, the reader is referred to [11]. Some general rules about evaluating the security of chaos-based cryptosystems can be found in [12].

Recently, an image encryption scheme based on a compound chaotic sequence was proposed in [13]. This scheme includes two procedures: substitutions of pixel values with XOR operations, and circular shift position permutations of rows and columns. The XOR substitutions are controlled by a compound pseudo-random number sequence generated from two correlated chaotic maps. And the row and column circular shift permutations are determined by the two chaotic maps, respectively. This paper studies the security of the image encryption scheme and reports the following findings:

(1) the scheme can be broken by using only three chosen plain-images;
(2) there exist some weak keys and equivalent keys;
(3) the scheme is not sufficiently sensitive to the changes of plain-images; and
(4) the compound chaotic sequence is not random enough to be used for encryption.

This paper is organized as follows. In the next section the image encryption scheme under study is briefly introduced. Then, in Section 3, some security problems of the scheme are discussed. A differential chosen plain-image attack is introduced in Section 4 with some experimental results reported. Finally, some conclusions are given in Section 5.

2 The image encryption scheme under study

Although not explicitly mentioned, the image encryption scheme was specifically tailored to 24-bit RGB true-color images. However, the algorithm itself is actually independent of the plain-image's structure and can be used to encrypt any 2-D byte array. Therefore, in this cryptanalytic paper, it is assumed that the plain-image is an $M \times N$ (width×height) 8-bit gray-scale image. In other words, to encrypt a 24-bit RGB true-color image, one only needs to consider the true-color image as a $3M \times N$ 8-bit gray-scale image, and then perform the encryption procedure.

Denoting the plain-image by $\mathbf{I} = \{I(i,j)\}_{\substack{1\le i\le M\\1\le j\le N}}$ and the corresponding cipher-image by $\mathbf{I}' = \{I'(i,j)\}_{\substack{1\le i\le M\\1\le j\le N}}$, the image encryption scheme proposed in [13] can be described as follows[1].

- The *secret key* includes two floating-point numbers of precision 10^{-14} $x_0, y_0 \in [-1,1]$, which are the initial states of the following two chaotic maps: $f_0(x) = 8x^4 - 8x^2 + 1$ and $f_1(y) = 4y^3 - 3y$.
- The *initialization procedure* includes generation of three pseudo-random integer sequences.

(1) *Pseudo-random sequence* $\{S_1(k)\}_{k=1}^{MN}$ *for XOR substitution of pixel values*

Starting from $k_0 = k_1 = 0$, iterate the following compound chaotic map for MN times to construct a compound chaotic sequence $\{z_k\}_{k=1}^{MN}$:

$$z_{k_0+k_1+1} = \begin{cases} x_{k_0+1} = f_0(x_{k_0}), & \text{if } (x_{k_0} + y_{k_1}) < 0, \\ y_{k_1+1} = f_1(y_{k_1}), & \text{if } (x_{k_0} + y_{k_1}) \ge 0. \end{cases} \tag{1}$$

For each iteration of Eq. (1), update k_0 with $k_0 + 1$ if the first condition is satisfied, and update k_1 with $k_1 + 1$ otherwise.

Then, an integer sequence $\{S_1(k)\}_{k=1}^{MN}$ is obtained from $\{z_k\}_{k=1}^{MN}$ as

$$S_1(k) = \begin{cases} \left\lfloor \frac{1+z_k}{2} \cdot 256 \right\rfloor, & \text{if } z_k \in [-1,1), \\ 255, & \text{if } z_k = 1, \end{cases} \tag{2}$$

where $\lfloor a \rfloor$ denotes the greatest integer that is not greater than a.

(2) *Pseudo-random sequence* $\{S_2(j)\}_{j=1}^{N}$ *for circular shift operations of rows*

Iterate f_0 from x_{k_0} for N more times to obtain a chaotic sequence $\{x_{k_0+j}\}_{j=1}^{N}$, and then transform it into $\{S_2(j)\}_{j=1}^{N}$ by

$$S_2(j) = \begin{cases} \left\lfloor \frac{1+x_{k_0+j}}{2} \cdot M \right\rfloor, & \text{if } x_{k_0+j} \in [-1,1), \\ M-1, & \text{if } x_{k_0+j} = 1. \end{cases}$$

(3) *Pseudo-random sequence* $\{S_3(i)\}_{i=1}^{M}$ *for circular shift operations of columns*

[1] To make the presentation more concise and complete, some notations in the original paper are modified, and some missed details about the encryption procedure are supplied here.

Iterate f_1 from y_{k_1} for M more times to obtain a chaotic sequence $\{y_{k_1+i}\}_{i=1}^{M}$, and then transform it into $\{S_3(i)\}_{i=1}^{M}$ by

$$S_3(i) = \begin{cases} \left\lfloor \frac{1+y_{k_1+i}}{2} \cdot N \right\rfloor, & \text{if } y_{k_1+i} \in [-1, 1), \\ N-1, & \text{if } y_{k_1+i} = 1. \end{cases}$$

- The *encryption procedure* includes an XOR substitution part and two permutation parts.

(1) *XOR substitution part*

Taking $\mathbf{I}$ as input, an intermediate image $\mathbf{I}^* = \{I^*(i,j)\}_{\substack{1\le i\le M \\ 1\le j\le N}}$ is obtained as

$$I^*(i,j) = I(i,j) \oplus S_1((j-1)\cdot M + i), \tag{3}$$

where $\oplus$ denotes the bitwise XOR operation.

(2) *Permutation part – horizontal circular shift operations*

Taking $\mathbf{I}^*$ as input, a new intermediate image $\mathbf{I}^{**} = \{I^{**}(i,j)\}_{\substack{1\le i\le M \\ 1\le j\le N}}$ is obtained by performing the following horizontal circular shift operations[2]:

$$I^{**}(i,j) = I^*((i - S_2(j)) \bmod M, j). \tag{4}$$

(3) *Permutation part – vertical circular shift operations*

Taking $\mathbf{I}^{**}$ as input, the cipher-image $\mathbf{I}'$ is obtained by performing the following vertical circular shift operations:

$$I'(i,j) = I^{**}(i, (j - S_3(i)) \bmod N). \tag{5}$$

Combining the above three operations, the encryption procedure can be represented in the following compact form:

$$I'(i,j) = I(i^*, j^*) \oplus S_1((j^*-1)\cdot M + i^*), \tag{6}$$

where $j^* = (j - S_3(i)) \bmod N$ and $i^* = (i - S_2(j^*)) \bmod M$.

- The *decryption procedure* is the reversion of the above (after finishing the same initialization process) and can be described as

$$I(i,j) = I'(i^*, j^*) \oplus S_1((j-1)\cdot M + i), \tag{7}$$

where $i^* = (i + S_2(j)) \bmod M$ and $j^* = (j + S_3(i^*)) \bmod N$.

[2] In [13], the authors did not explain in which direction the circular shift operations are performed. Since the direction is independent of the scheme's security, here it is assumed that the operations are carried out towards larger indices. The same assumption is made for vertical circular shift operations.

3 Some security problems

3.1 Insufficient randomness of the compound chaotic sequence

In [13, Sec. 4.3], the authors claim that the randomness of the generated chaotic sequences has been verified by employing the four random tests defined in FIPS PUB 140-2 [14]. Here, it is noticed that what they actually refer to is an intermediate edition of FIPS PUB 140-2 (updated in October 2001), which has been superseded in December 2002, and as a result all the four random tests have been removed from the publication (see Change Notices 1 and 2, pp. 54–58 in [15]).[3]

Even for the four random tests defined in the intermediate edition of FIPS PUB 140-2, the randomness of the chaotic sequences is still questionable due to the following two facts:

(1) Only the experimental result about one random sequence generated from the key $(x_0, y_0) = (0.32145645647836, 0.48124356788345)$ is shown in [13]. However, to study the randomness of a random number resource, a sufficiently large number of samples should be tested.

(2) The results of repeating the same test are shown in Table 1, which does not agree with the data shown in Table 2 of [13].

To investigate the level of randomness of the chaotic compound sequence $\{z_k\}_{k=1}^{MN}$ generated by iterating Eq. (1), 100 binary sequences have been tested for the encryption of 256 × 256 images with the test suite proposed in [17]. The secret keys to generate the 100 binary sequences were chosen randomly. For each test, the default significance level 0.01 was adopted. The results are shown in Table 2, from which one can see that the compound chaotic function Eq. (1) cannot be used as a good random number generator.

3.2 Weak keys

For the image encryption scheme under study, it is found that some keys will cause some or even all encryption parts to fail, due to the existence of some fixed points of the chaotic maps involved: $f_0(1) = 1$, $f_1(1) = 1$, $f_1(0) = 0$,

[3] In [13], the authors cite [15] as the source of FIPS PUB 140-2. However, [15] only contains an introduction to FIPS PUB 140-1 (the first edition of FIPS PUB 140) [16]. By comparing the required intervals shown in Table 2 of [13] with those published in different editions of FIPS PUB 140, we finally concluded that FIPS PUB 140-2 (Change 1) was the one used by the authors of [13].

Table 1
Randomness test results of the chaotic compound sequence generated from the key $(x_0, y_0) = (0.32145645647836, 0.48124356788345)$. For runs tests, the two output values are the numbers of 0-bit and 1-bit runs, respectively.

Test item		Required interval	Output value(s)	Result
Monobit test		9725 – 10275	9968	Pass
Runs test	$r = 1$	2315 – 2685	2124, 2142	Fail
	$r = 2$	1114 – 1386	962, 966	Fail
	$r = 3$	527 – 723	537, 498	Fail
	$r = 4$	240 – 384	266, 273	Pass
	$r = 5$	103 – 209	153, 167	Pass
	$r \geq 6$	103 – 209	301, 297	Fail
	$r \geq 26$	0 – 0	3, 3	Fail
Poker test		2.16 – 46.17	799.37	Fail

Table 2
The performed tests with respect to a significance level 0.01 and the number of sequences passing each test in 100 randomly generated sequences.

Name of Test	Number of Passed Sequences
Frequency	91
Block Frequency ($m = 100$)	0
Cumulative Sums-Forward	88
Runs	0
Rank	67
Non-overlapping Template ($m = 9$, $B = 101001100$)	48
Serial ($m = 16$)	0
Approximate Entropy ($m = 10$)	0
FFT	0

$f_1(-1) = -1$. Four typical classes of weak keys and the negative influences on the randomness of the chaotic sequences are listed below:

(1) $x_0 = 1$: $f(x_0) = 1 \Rightarrow S_2(j) \equiv M - 1$;
(2) $y_0 = 1$: $f_1(y_0) = 1$, only $f_1(y)$ is iterated in Eq. (1) $\Rightarrow S_1(k) \equiv 255$, $S_3(i) \equiv N - 1$;
(3) $y_0 = -1$: $f_1(y_0) = -1 \Rightarrow S_3(i) \equiv 0$;
(4) $x_0 \geq 0$, $y_0 = 0$: $f_1(y_0) = 0$, only $f_1(y)$ is iterated in Eq. (1) $\Rightarrow S_1(k) \equiv 128$, $S_3(i) \equiv N/2$.

By combining the above conditions, three extremely weak keys can be found from the above general ones:

- $x_0 = 1$, $y_0 = 1$: $S_1(k) \equiv 255$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv N - 1$;
- $x_0 = 1$, $y_0 = -1$: $S_1(k) \equiv 0$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv 0$;
- $x_0 = 1$, $y_0 = 0$: $S_1(k) \equiv 128$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv N/2$.

Furthermore, whenever (x_{k_0}, y_{k_1}) satisfies one of the above-listed conditions in the process of iterating Eq. (1), the corresponding secret key (x_0, y_0) is also found to be weak. For instance, from $f_0(-1) = f_0(0) = 1$, $f_1(-0.5) = 1$ and $f_1(0.5) = -1$, the following examples can be derived easily: (1) $x_0 \in \{0, -1\}$; (2) $y_0 = -0.5$; (3) $y_0 = 0.5$. From these examples, one can further discover some extremely weak keys as follows:

- $x_0 \in \{0, -1\}$, $y_0 \in \{-0.5, 1\}$: $S_1(k) \equiv 255$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv N - 1$;
- $x_0 = 0$, $y_0 = 0.5$: $S_1(2) = 255$, $S_1(k) \equiv 0$ for $k \neq 2$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv 0$;
- $x_0 = 0$, $y_0 = -1$ *or* $x_0 = -1$, $y_0 \in \{-1, 0.5\}$: $S_1(1) = 255$, $S_1(k) \equiv 0$ for $k \geq 2$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv 0$;
- $x_0 = 0$, $y_0 = 0$: $S_1(k) \equiv 128$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv N/2$;
- $x_0 = -1$, $y_0 = 0$: $S_1(1) = 255$, $S_1(k) \equiv 128$ for $k \geq 2$, $S_2(j) \equiv M - 1$, $S_3(i) \equiv N/2$.

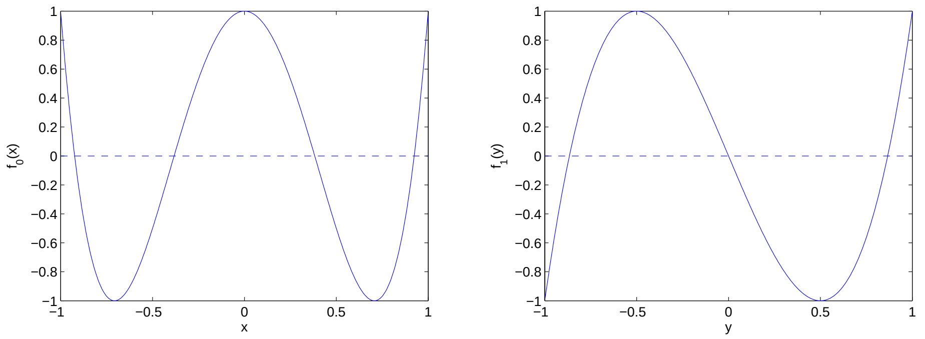
3.3 Equivalent keys

Equivalent keys mean some different keys that generate the same cipher-image for any given plain-image, i.e., they are completely equivalent to each other. From Fig. 1a) one can see that function f_0 may have four points whose functional values are the same: $\pm x$, $\pm\sqrt{1 - x^2}$. From Fig. 1b) one can see that function f_1 may have three points whose functional values are the same: y, $\frac{-y \pm \sqrt{3 - 3y^2}}{2}$.

Since only the field of rational number is considered, one can see that (x_0, y_0) and $(-x_0, y_0)$ are equivalent when $|y_0| \geq |x_0|$.

3.4 Low sensitivity to plaintext changes

In [13, Sec. 4.4] the authors claim that their scheme is sensitive to plaintext changes, which is, however, not true. From Eq. (6) one can easily see that changing one bit of $I(i^*, j^*)$ influences the same bit of $I'(i, j)$, only. Note that this low sensitivity is actually a common problem with all XOR-based encryption systems. But it becomes trivial if the key is not repeatedly used.



a) b)

Fig. 1. The images of functions $f_0(x)$ and $f_1(y)$

In this case, it is rare that two slightly different plaintexts are encrypted by the same keystream.

3.5 A remark on the compound chaotic map

In Section 2.2 of [13], the authors have provided some theoretical results about the compound chaotic map defined as follows:

$$F(x) = \begin{cases} 8x^4 - 8x^2 + 1, & x < 0 \\ 4x^3 - 3x, & x \geq 0, \end{cases} \tag{8}$$

and claimed that "$F(x)$ can be employed as ideal sequence cipher". Unfortunately, as shown in Eq. (1), what they actually employed in the design of the image encryption scheme is a simple combination of two separately (but not independently) iterated chaotic maps f_0 and f_1, which has nothing to do with the above compound chaotic map (8). This makes all the theoretical results given in [13, Section 2.2] completely irrelevant to their image encryption scheme.

4 Differential chosen-plaintext attack

In [13, Sec. 4.6] the authors claim that their scheme can withstand chosen-plaintext attack efficiently. It is found, however, that their scheme can be broken with only three chosen plain-images.

The proposed attack is based on the following fact: given two plain-images $\mathbf{I_1}$, $\mathbf{I}_2$ and the corresponding cipher-images $\mathbf{I}_1'$, $\mathbf{I}_2'$, one can easily verify that $I_1'(i,j) \oplus I_2'(i,j) = I_1(i^*,j^*) \oplus I_2(i^*,j^*)$, where $j^* = (j - S_3(i)) \bmod N$ and $i^* = (i - S_2(j^*)) \bmod M$. This means that the XOR substitution operations disappear and only the permutations remain. According to the quantitative cryptanalysis given in [6], permutation-only ciphers are always insecure against plaintext attacks, and only $\lceil \log_{256}(MN) \rceil$ plain-images are required for a successful chosen-plaintext attack. Once the permutation part is broken, the XOR substitution can be cracked easily. This is a typical *divide-and-conquer* (DAC) attack that breaks different encryption components separately.

Since the permutations in the image encryption scheme are a simple combination of N row-shift and M column-shift operations, the number of required differential plain-images will not be greater than 2, even when $\lceil \log_{256}(MN) \rceil > 2$. This means that only 3 chosen plain-images suffice to implement the attack. In the sequel, the DAC attack is described step by step.

- *Breaking* $\{S_3(i)\}_{i=1}^{M}$ *(i.e., vertical shift operations)*

  If two plain-images $\mathbf{I}_1$ and $\mathbf{I}_2$ are chosen such that each row of $\mathbf{I}_1 \oplus \mathbf{I}_2$ contains identical pixel values, then the horizontal circular shift operations will be canceled and only vertical ones are left. If further $\mathbf{I}_1$ and $\mathbf{I}_2$ are chosen such that each column of $\mathbf{I}_1 \oplus \mathbf{I}_2$ has an unambiguous pattern to recognize the value $S_3(i)$, then the vertical shift operations are broken. For example, one can choose $\mathbf{I}_1$ and $\mathbf{I}_2$ as

  $$I_1(:,j) \oplus I_2(:,j) = \begin{cases} 0, & j = 1, \\ 255, & 2 \leq j \leq N. \end{cases} \tag{9}$$

  In this case, by looking for the new position of the sole black pixel in each column, one can immediately derive all values of $\{S_3(i)\}_{i=1}^{M}$.
- *Breaking* $\{S_2(j)\}_{j=1}^{N}$ *(i.e., horizontal shift operations)*

  Once all vertical shift operations have been broken, one can use the same strategy to break the horizontal shift operations. For this purpose, one needs to choose $\mathbf{I}_1$ and a new plain-image $\mathbf{I}_3$ such that each column of $\mathbf{I}_1 \oplus \mathbf{I}_3$ contains identical pixel values and each row has an unambiguous pattern so as to recognize the value of $S_2(j)$. For example, one can choose $\mathbf{I}_1$ and $\mathbf{I}_3$ as

  $$I_1(i,:) \oplus I_3(i,:) = \begin{cases} 0, & i = 1, \\ 255, & 2 \leq i \leq M. \end{cases}$$

  In this case, by looking for the new position of the sole black pixel in each row, one can immediately derive all values of $\{S_2(j)\}_{j=1}^{N}$.
- *Breaking* $\{S_1(i)\}_{i=1}^{MN}$ *(i.e., XOR substitutions)*

  After the values of $\{S_2(j)\}_{j=1}^{N}$ and $\{S_3(i)\}_{i=1}^{M}$ are obtained, the encryption scheme becomes a simple XOR-based stream cipher, and $\{S_1(k)\}_{k=1}^{MN}$ can immediately be recovered via

  $$S_1((j-1) \cdot M + i) = I_1(i,j) \oplus I_1'(i^*, j^*),$$

  where $i^* = (i + S_2(j)) \bmod M$ and $j^* = (j - S_3(i^*)) \bmod N$.

To validate the performance of the above attack, some experiments have been carried out for some chosen plain-images of size 256 × 256. Here, the experimental results with the random secret key used in Section 3.1 are reported. One plain-image "Peppers" is chosen as $\mathbf{I}_1$, and the second plain-image is chosen such that the differential image $\mathbf{I}_1 \oplus \mathbf{I}_2$ is as shown in Eq. (9). The third plain-image is chosen such that $\mathbf{I_1} \oplus \mathbf{I_3} = (\mathbf{I}_1 \oplus \mathbf{I}_2)^T$. These three chosen plain-images and the corresponding cipher-images are shown in Fig. 2. The recovered pseudo-random sequences are used to decrypt a new cipher-image $\mathbf{I}'_4$, which is shown in Fig. 2d), and the result is given in Fig. 2h).

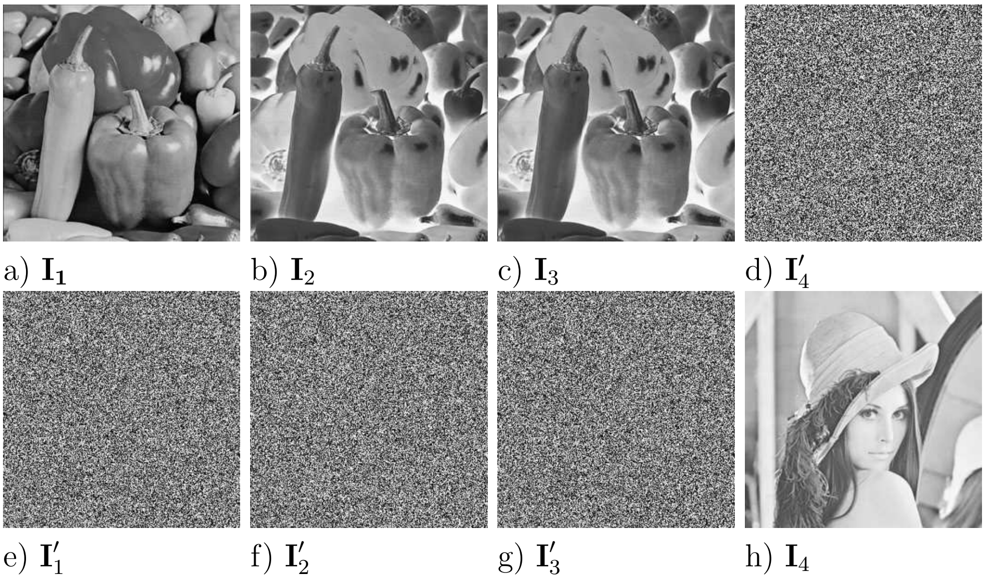

a) $\mathbf{I_1}$ b) $\mathbf{I}_2$ c) $\mathbf{I}_3$ d) $\mathbf{I}'_4$
e) $\mathbf{I}'_1$ f) $\mathbf{I}'_2$ g) $\mathbf{I}'_3$ h) $\mathbf{I}_4$

Fig. 2. The proposed differential chosen-plaintext attack: a demonstration

5 Conclusion

The security of a recently published image encryption scheme based on a compound chaotic sequence has been studied. It is found that the scheme can be broken with only three chosen plain-images. In addition, it is found that the scheme has some weak keys and equivalent keys, and that the scheme is not sufficiently sensitive to the changes of plain-images. Furthermore, the pseudo-random number sequence generated by iterating the compound chaotic function is found not to be sufficiently random for secure encryption. In summary, the scheme under study is not secure enough. Therefore, it is not be recommended for applications requiring a high level of security.

Acknowledgements

This research was supported by the City University of Hong Kong under the SRG grant 7002134. In particular, Shujun Li was supported by a research fellowship of the Alexander von Humboldt Foundation of Germany.

References

[1] J.-C. Yen, J.-I. Guo, A new chaotic key-based design for image encryption and decryption, in: Proc. IEEE Int. Conf. Circuits and Systems, Vol. 4, 2000, pp. 49–52.

[2] H.-C. Chen, J.-C. Yen, A new cryptography system and its VLSI realization, J. Systems Architecture 49 (2003) 355–367.

[3] H.-C. Chen, J.-I. Guo, L.-C. Huang, J.-C. Yen, Design and realization of a new signal security system for multimedia data transmission, EURASIP Journal on Applied Signal Processing 2003 (13) (2003) 1291–1305.

[4] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.

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

[6] 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 (3) (2008) 212–223.

[7] C. Li, S. Li, G. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission, EURASIP Journal on Applied Signal Processing 2005 (8) (2005) 1277–1288.

[8] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, in: Proc. IEEE Int. Symposium on Circuits and Systems, Vol. II, 2002, pp. 708–711.

[9] S. Li, C. Li, G. Chen, K.-T. Lo, Cryptanalysis of RCES/RSES image encryption scheme, Journal of Systems and Software 81 (7) (2008) 1130–1143.

[10] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, IACR's Cryptology ePrint Archive: Report 2007/397, available online at `http://eprint.iacr.org/2007/397` (2007).

[11] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital images and videos, in: B. Furht, D. Kirovski (Eds.), Multimedia Security Handbook, CRC Press, LLC, 2004, Ch. 4, pp. 133–167, the preprint is available at `http://www.hooklee.com/pub.html`.

[12] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurcation and Chaos 16 (8) (2006) 2129–2151.

[13] X. Tong, M. Cui, Image encryption with compound chaotic sequence cipher shifting dynamically, Image and Vision Computing 26 (6) (2008) 843–850.

[14] NIST, Security requirements for cryptographic modules, Federal Information Processing Standards Publication (FIPS PUB) 140-2, available online at `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf` (2002).

[15] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[16] NIST, Security requirements for cryptographic modules, Federal Information Processing Standards Publication (FIPS PUB) 140-1, available online at `http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf` (1994).

[17] A. Rukhin, et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22, available online at `http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html` (2001).