

# On the Security of a Class of Image Encryption Schemes

Chengqing Li

Department of Electronic Engineering,  
City University of Hong Kong,  
Hong Kong SAR, China  
Email: swiftsheep@hotmail.com

Guanrong Chen

Department of Electronic Engineering,  
City University of Hong Kong,  
Hong Kong SAR, China

**Abstract**—Recently four chaos-based image encryption schemes were proposed. Essentially, the four schemes can be classified into one class, which is composed of two basic parts: permutation of position and diffusion of pixel value with the same cipher-text feedback function. The operations involved in the two basic parts are determined by a pseudo random number sequence (PRNS) generated from iterating a chaotic dynamic system. According to the security requirement, the two basic parts are performed alternatively for some rounds. Although the designers claimed that the schemes are of high quality, we found the following security problems: 1) the schemes are not sensitive to the changes of plain-images; 2) the schemes are not sensitive to the changes of the key streams generated by any secret key; 3) there exists a serious flaw of the diffusion function; 4) the schemes can be broken with no more than  $\lceil \log_L(MN) \rceil + 3$  chosen-images when the iteration number is equal to one, where  $MN$  is the size of the plain-image and  $L$  is the number of different pixel values; 5) the cryptanalysis on one scheme proposed by another research group is questionable.

## I. INTRODUCTION

With the rapid development of multimedia and network technologies, the transmission of multimedia data takes place more and more frequently. Consequently, the security of multimedia data is becoming more and more important. However, traditional text encryption schemes fail to encrypt the multimedia data efficiently due to special properties of multimedia data, such as the bulky size and strong redundancy of uncompressed data. To satisfy the emerging demand, a large number of multimedia encryption schemes have been proposed in the past decade [1]–[9]. Meanwhile, cryptanalysis work has been developed, and some of the proposed schemes have been found insecure from the viewpoint of cryptography [10]–[14].

In [5], an image encryption scheme based on 3D chaotic cat maps was proposed, which is an enhanced version of the one proposed in [15]. The scheme is composed of two basic components: position permutation and diffusion of pixel value with a cipher-text feedback function. To improve the security of the scheme, the two basic components are performed alternatively for some rounds. However the authors did not discuss how many rounds is enough for a satisfactory degree of security. Afterwards, three other schemes were presented in [6]–[8]. Essentially, the three schemes share the same structure with the one proposed in [5]. In [16], it was pointed out that

the one-round version of the scheme proposed in [5] can be broken with a chosen plain-image attack.

In this paper, we analyze the four schemes altogether, and find the following problems: 1) the schemes are not sensitive to the changes of plain-images; 2) the schemes are not sensitive to the changes of the key streams generated by any secret key; 3) there exists a serious flaw of the diffusion function; 4) the equivalent version of the whole pseudo random number sequence (PRNS) used for diffusion can be recovered when the round number is only one; 5) the cryptanalysis proposed in [16, Sec. 3.1] is questionable.

The rest of this paper is organized as follows. The next section gives a brief introduction to the class of image encryption schemes. Section III focuses on the security analysis of the class of encryption schemes. The last section concludes the paper.

## II. BASIC STRUCTURE OF THE CLASS OF ENCRYPTION SCHEMES

Assuming the plain image  $\mathbf{I}$  is of size  $M \times N$  and every pixel  $\mathbf{I}(i, j)$  is of  $n_0$  bits, the two main basic parts of the class of encryption schemes can be described briefly as follows, where  $0 \leq i < M, 0 \leq j < N$ .

- *Position Permutation*

Although different methods were adopted to realize the position permutation in [5]–[8], they can be presented with the following general equation (See [17]):

$$\mathbf{I}^*(w(i, j)) = \mathbf{I}(i, j) \quad (1)$$

where  $\mathbf{W} = [w(i, j) = (i', j') \in \mathbb{M} \times \mathbb{N}]_{M \times N}$  denotes the permutation matrix,  $\mathbb{M} = \{0, \dots, M-1\}$  and  $\mathbb{N} = \{0, \dots, N-1\}$ .

- *Value Diffusion*

The intermediate image  $\mathbf{I}^*$  is scanned in raster order and the  $k$ -th pixel  $\mathbf{I}^*(k)$  is diffused by the following equation:

$$\mathbf{I}'(k) = \phi(k) \oplus [\mathbf{I}^*(k) \dot{+} \phi(k)] \oplus \mathbf{I}'(k-1) \quad (2)$$

where  $k = i \times N + j + 1$ ,  $a \dot{+} b = (a+b) \bmod 2^{n_0}$ ,  $\{\phi(k)\}$  is a PRNS generated by iterating a chaotic system, and  $\mathbf{I}'(0)$  is a pre-defined value.

According to the security requirement, the above two parts are performed alternatively for some rounds. Finally,  $I'$  is the obtained cipher image.

In [5]–[7], three color channels of plain-image are encrypted separately,  $n_0 = 8$ . In [8], the three bytes corresponding to the three color channel are combined together,  $n_0 = 24$ . In this paper, we will only focus on cryptanalysis of the case  $n_0 = 8$ , which can be easily generalized to the case  $n_0 = 24$ . Note that the cryptanalysis presented in this paper is independent of how position permutation is derived, which is the main difference between the four schemes proposed in [5]–[8].

### III. CRYPTANALYSIS

#### A. Low Sensitivity with Respect to Plain-image

From above section, we can see that the class of encryption schemes under study only includes the module addition operation and bitwise exclusive OR operation no matter what the number of round is. Given two plain-images  $I_1, I_2$  and corresponding cipher-images  $I'_1, I'_2$ , we have  $I'_1 \oplus I'_2 \in \{0, 128\}$  if  $I_1 \oplus I_2 \in \{0, 128\}$  from Proposition 1. The value of  $I'_1(k) \oplus I'_2(k)$  depends on the parity of the measure of index set  $\mathbb{S}$ , where  $I(s)$  is used an odd number of times for the computation of  $I'(k)$  and  $I_1(s) \oplus I_2(s) = 128 \forall s \in \mathbb{S}$ . Obviously,  $I_1(k) \oplus I_2(k) = 0$  if the parity is even,  $I_1(k) \oplus I_2(k) = 128$  if the parity is odd.

*Proposition 1:*  $\forall a, b \in \mathbb{Z}$ , the following equality is true:  $(a \oplus 128) \dot{+} b = (a \dot{+} b) \oplus 128$ .

*Proof:* First,  $a \oplus 128 = a \dot{+} 128$  can be proved under the following two conditions: 1) when  $a \in \{0, \dots, 127\}$ , we have  $a \oplus 128 = a + 128$  and  $a \dot{+} 128 = a + 128$ , so  $a \oplus 128 = a \dot{+} 128$ ; 2) when  $a \in \{128, \dots, 255\}$ , we have  $a \oplus 128 = a - 128$  and  $a \dot{+} 128 = (a + 128) - 256 = a - 128$ , so  $a \oplus 128 = a \dot{+} 128$ . Then, we have  $(a \oplus 128) \dot{+} b = (a \dot{+} 128) \dot{+} b = (a \dot{+} b) \dot{+} 128 = (a \dot{+} b) \oplus 128$ . ■

To validate this problem, we carried out some experiments with the scheme proposed in [6], where  $K = "49505152535455565748495051525354"$  and round number is 8. One experiment result is shown in Fig. 1. The bitwise exclusive OR differential image between Fig. 1b) and Fig. 1d) is shown in Fig. 2, where the numbers of 0's and 128's are 131371 (50.11%) and 130773 (49.89%) respectively.

Now we can see that the encryption result of the class of image encryption schemes under study is not sensitive to the change of MSB of any pixel of plain-image. Actually, this problem hold for other bits of any pixel. The change of the  $p$ -th significant bit only may influent the  $q$ -th bit of pixels of cipher-image, where  $1 \leq p < 8, p \leq q \leq 8$ .

#### B. Low Sensitivity with Respect to the Key Stream

Still from Proposition 1, we have

$$\begin{aligned} & \phi(k) \oplus [I^*(k) \dot{+} \phi(k)] \oplus I'(k-1) \\ = & (\phi(k) \oplus 128) \oplus [I^*(k) \dot{+} (\phi(k) \oplus 128)] \oplus I'(k-1). \end{aligned}$$

Given two secret keys  $K_1, K_2$ , we assume that the corresponding PRBS used for diffusion are  $\{\phi_1(k)\}$  and  $\{\phi_2(k)\}$  respectively. If  $\phi_1(k_0) = \phi_2(k_0) \oplus 128$  and  $\phi_1(k) = \phi_2(k)$

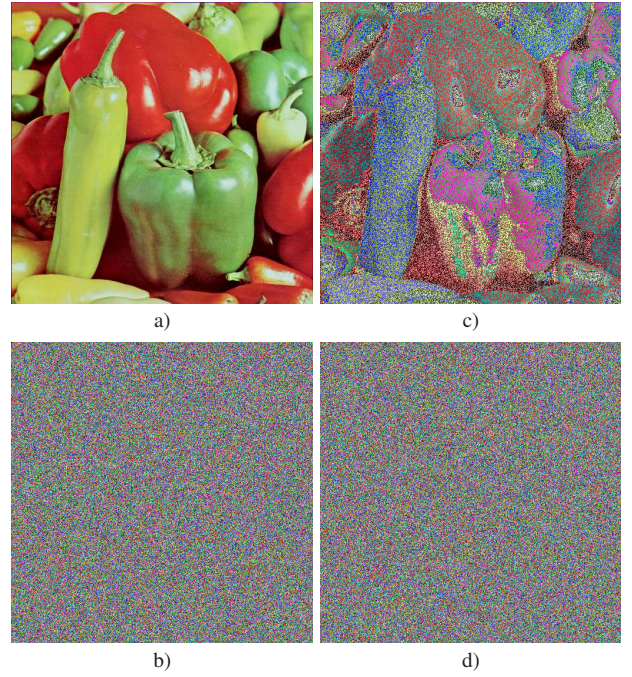


Fig. 1. Low sensitivity with respect to plain-image: a) plain-image “Peppers”, b) the encryption result of Fig. 1a), c) the masked version of Fig. 1a) with a random  $\{0, 128\}$  binary image, d) the encryption result of Fig. 1c).

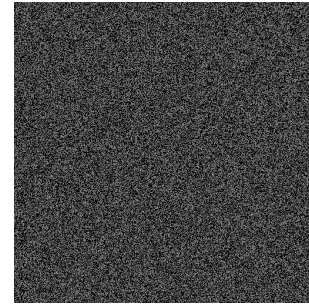


Fig. 2. The bitwise exclusive OR differential image between Fig. 1b) and Fig. 1d).

$\forall k \neq k_0$ , we can assure that the two encryption results with the two secret keys are the same.

Considering all possible cases, we have that for any secret key there may exist  $2^{MN \cdot n}$  equivalent key stream that can generate the same encryption results, where  $n$  is the round number.

#### C. A Defect of the Diffusion Function when the Round Number is One

In [16] it is pointed out that  $I'(k) = I'(k-1)$  when  $I(k) = 0$ . Beside this, there still exists another problem: the number of possible values of  $I'(k) \oplus I'(k-1)$  is too small when the round number is equal to one.

From Eq. (2), one has

$$I'(k) \oplus I'(k-1) = \phi(k) \oplus [I^*(k) \dot{+} \phi(k)]. \quad (3)$$

To facilitate the following discussion, we rewrite Eq. (3) as

$$b = x \oplus (a \dot{+} x). \quad (4)$$

Since  $(b \oplus 128) = x \oplus (a \dot{+} 128 \dot{+} x)$ , we only need to consider the case when  $0 \leq a \leq 127$ . Then, one can easily verify Eq. (4) has following equivalent forms.

$$\begin{aligned} b &= (a \dot{+} x) \oplus ((256 - a) \dot{+} (a \dot{+} x)), \\ b &= (x \dot{+} 128) \oplus (a \dot{+} (x \dot{+} 128)), \\ b \oplus 128 &= (a \dot{+} x) \oplus ((128 - a) \dot{+} (a \dot{+} x)). \end{aligned}$$

The existence of the above equalities make the number of possible values of  $b$  for a given value of  $a$  becomes very small (see Fig. 3).

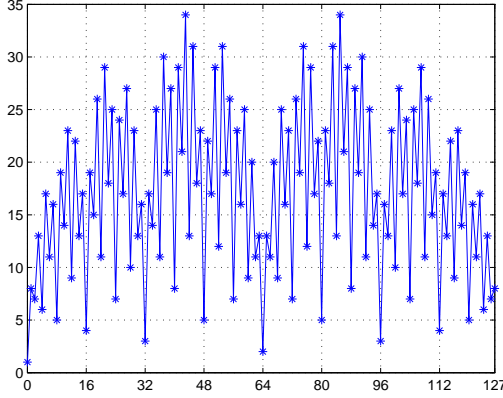


Fig. 3. The value of  $a$  vs. the number of possible values of  $b$ .

Proposition 1 only discuss the problem of MSB. In fact, the problem also exist in any other bit. In the following, we present some examples. When  $0 \leq a + x \leq 63$ ,  $x \oplus (a \dot{+} x) = (x + 64) \oplus (a \dot{+} (x + 64))$ ; when  $64 \leq a + x \leq 127$  and  $0 \leq x \leq 63$ ,  $x \oplus (a \dot{+} x) \oplus 128 = (x + 64) \oplus (a \dot{+} (x + 64))$ ; when  $128 \leq a + x \leq 191$  and  $0 \leq x \leq 63$ ,  $x \oplus (a \dot{+} x) = (x + 64) \oplus (a \dot{+} (x + 64))$ ; when  $0 \leq x \leq \lfloor \frac{63-a}{2} \rfloor$ ,  $x \oplus (a \dot{+} x) = (63 - (a + x)) \oplus (a \dot{+} 63 - (a + x)) = (a + x) \oplus 64 \oplus x \oplus 64$ . The direct result of above relations is the distribution of  $b$  for a given  $a$  is not uniform (See Fig. 4).

#### D. Chosen-Plaintext Attack when the Round Number is One

Under the scenario of chosen-plaintext attack, the attacker can deliberately choose some plaintext and observe corresponding ciphertext. When the round number is one, the two basic parts of the class of scheme under study can be broken with a strategy of ‘‘Divide and Conquer’’. Obviously, the position permutation part is failed for chosen plain-image of the fixed value and only value diffusion part is left.

In [16, Sec. 3.1], Wang et al. claimed that the secret key used for generating key stream  $\{\phi(k)\}$  in [5] can be recovered with the following two steps.

- *Step 1:* Brute-forcelly search the value of  $\phi(k)$  satisfying Eq. (3) for one chosen plain-image of fixed value 11;
- *Step 2:* Estimate secret key (initial condition of PRBS) from the obtained sequence  $\{\phi(k)\}$  with symbolic dynamics theory.

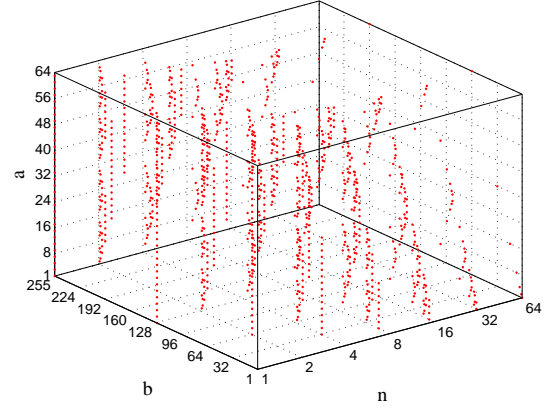


Fig. 4. The value of  $a$  vs. distribution of  $b$ , where the axis of  $n$  presents the number of  $b$  for a given  $a$ .

Observing Fig. 5 or Fig. 6, one can see that there exist 32 possible values of  $\phi(k)$  for a chosen plain-image of fixed value 11. Fortunately, choosing more plain-images will reduce the number of possible values of  $\phi(k)$ . With the help of computer, we have verified that the value of  $(\phi(k) \bmod 128)$  can be determined with three chosen plain-images of fixed value 43, 53 and 85. However, we can not distinguish  $\phi(k)$  and  $\phi(k) \oplus 128$ . Considering the estimation method based on symbolic dynamics theory is very sensitive to the value of every element of the obtained sequence, we can assure that the cryptanalysis proposed in [16, Sec. 3.1] is problematic.

From Sec. III-B, we can see that PRBS  $\{\phi(k) \bmod 128\}$  can be used to decrypt any other cipher-image encrypted with the same secret key correctly. Some experiment results are shown in Fig. 7. Since the position permutation part can be broken with  $\lceil \log_L(MN) \rceil$  chosen plain-images [17], we discarded this part in the experiment of Fig. 7. The correct percentages of the images shown in Figs. 7a), b) and c) are 53.88%, 82.81% and 100% respectively.

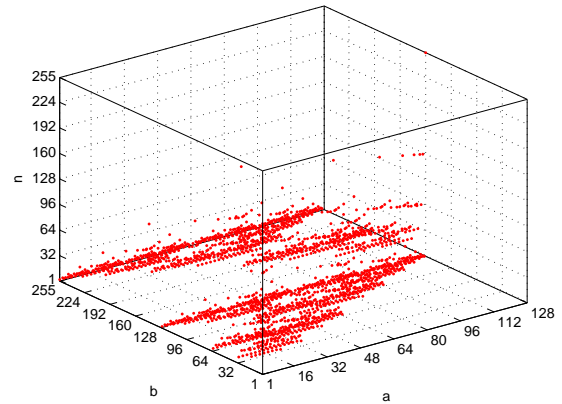


Fig. 5. The pair of  $(a, b)$  and the number of  $x$  satisfying  $b = x \oplus (a \dot{+} x)$ .

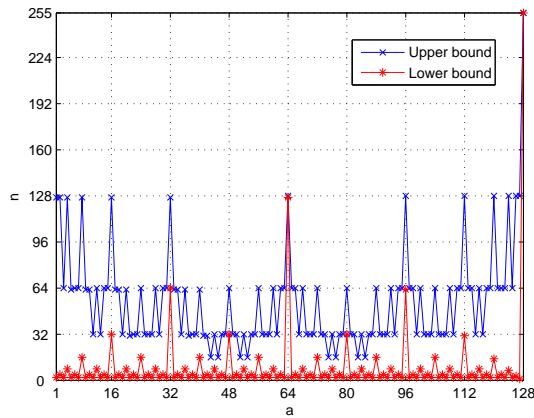


Fig. 6. The value of  $a$  vs. the number of  $x$  satisfying  $b = x \oplus (a \dagger x)$ .

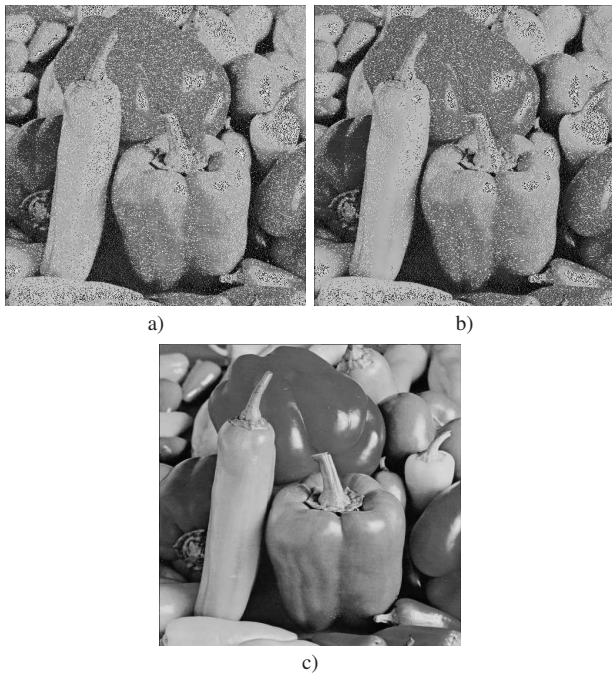


Fig. 7. The results on red channel of three chosen plain-image attacks: a) one chosen plain-image of fixed value 43; b) two chosen plain-images of fixed value 43, 53; c) three chosen plain-images of fixed value 43, 53, 85.

#### IV. CONCLUSION

In this paper, the security of a class of image encryption schemes has been studied in detail. It has been found that the schemes are not sensitive to the changes of plaintexts or key streams generated by any secret key. There exists a defect in the diffusion function. In addition, the schemes can be broken with a chosen plain-image attack when the number of encryption rounds is one. The cryptanalysis work on one scheme given by another research group has been found to be problematic. Nevertheless, the security of the class of encryption schemes with multiple rounds has not been found to have major problem so far, which still needs further study.

#### REFERENCES

- [1] T.-J. Chuang and J.-C. Lin, "New approach to image encryption," *J. Electronic Imaging*, vol. 7, no. 2, pp. 350–356, 1998.
- [2] K.-L. Chung and L.-C. Chang, "Large encryption binary images with higher security," *Pattern Recognition Letters*, vol. 19, no. 5–6, pp. 461–468, 1998.
- [3] J.-I. Guo, J.-C. Yen, and H.-F. Pai, "New voice over Internet protocol technique with hierarchical data security protection," *IEE Proc. – Vis. Image Signal Process.*, vol. 149, no. 4, pp. 237–243, 2002.
- [4] N. Pareek, V. Patidar, and K. Sud, "Discrete chaotic cryptography using external key," *Physics Letters A*, vol. 309, no. 1–2, pp. 75–82, 2003.
- [5] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
- [6] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3d chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.
- [7] J. Shen, X. Jin, and C. Zhou, "A color image encryption algorithm based on magic cube transformation and modular arithmetic operation," *Lecture Notes in Computer Science*, vol. 3768, pp. 270–280, 2005.
- [8] X. He, Q. Zhu, and P. Gu, "A new chaos-based encryption method for color image," *Lecture Notes in Artificial Intelligence*, vol. 4062, pp. 671–678, 2006.
- [9] N. Pareek, V. Patidar, and K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.
- [10] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalysis of an image encryption scheme," *J. Electronic Imaging*, vol. 15, no. 4, p. art. no. 043012, 2006.
- [11] J.-K. Jan and Y.-M. Tseng, "On the security of image encryption method," *Information Processing Letters*, vol. 60, no. 5, pp. 261–265, 1996.
- [12] C. Li, S. Li, D. Zhang, and G. Chen, "Cryptanalysis of a data security protection scheme for VoIP," *IEE Proc. – Vis. Image Signal Process.*, vol. 153, no. 1, pp. 1–10, 2006.
- [13] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key," *Physics Letters A*, vol. 319, no. 3–4, pp. 334–339, 2003.
- [14] C. Li, S. Li, J. Nunez, G. Alvarez, and G. Chen, "On the security of an image encryption scheme," IACR's Cryptology ePrint Archive: Report 2007/108, available online at <http://eprint.iacr.org/2007/108>, 2007.
- [15] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.
- [16] K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3d cat map based symmetric image encryption scheme," *Physics Letters A*, vol. 343, pp. 432–439, 2005.
- [17] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general cryptanalysis of permutation-only multimedia encryption algorithms," IACR's Cryptology ePrint Archive: Report 2004/374, available at <http://eprint.iacr.org/2004/374>, 2007.