

Cryptanalyzing an image encryption algorithm based on scrambling and Veginère cipher

Li Zeng · Renren Liu · Leo Yu Zhang · Yuansheng Liu · Kwok-Wo Wong

Received: 26 March 2014 / Revised: 8 February 2015 / Accepted: 13 February 2015 /
Published online: 7 March 2015
© Springer Science+Business Media New York 2015

Abstract Recently, an image encryption algorithm based on scrambling and Veginère cipher has been proposed. However, it was soon cryptanalyzed by Zhang et al. using a method composed of both chosen-plaintext attack and differential attacks. This paper briefly reviews the two attack approaches proposed by Zhang et al. and outlines their mathematical interpretations. Based on these approaches, we present an improved chosen-plaintext attack to further reduce the number of chosen-plaintexts required, which is proved to be optimal. Moreover, it is found that an elaborately designed known-plaintext attack can efficiently compromise the image cipher under study. This finding is confirmed by both mathematical analysis and numerical simulations. The cryptanalyzing techniques developed in this paper provide some insights for designing secure and efficient multimedia ciphers.

Keywords Image scrambling · Cryptanalysis · Known-plaintext attack · Chosen-plaintext attack

1 Introduction

The rapid development of computer networks enables us to enjoy multimedia contents such as images and video clips conveniently. However, it also leads to challenges in the security of multimedia data which are transmitted over public channels. Due to bulk data volume and high correlation among neighboring pixels/frames of the raw image/video data, traditional encryption techniques, such as AES, 3DES and IDEA, are not appropriate for image/video encryption. The imperoperness appears in the following scenarios:

L. Zeng (✉) · R. Liu · Y. Liu
College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China
e-mail: lily173864258@gmail.com

L. Y. Zhang · K.-W. Wong
Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong

- The block size of traditional block ciphers is too small when comparing with the amount of multimedia data to be encrypted. For natural gray-scale images at a resolution of 1024×1024 , it requires the execution of 3DES for more than 10^5 times to encrypt one single image. The efficiency problem makes traditional block ciphers inappropriate for real-time applications, such as online TV, video conferencing, etc.
- Generally, the security level of traditional block ciphers is higher than that required in multimedia data encryption. For the protection of commercial movies, it merely requests that breaking the cipher will cost the attacker more than that for buying one genuine copy of the movie. In such scenario, some lightweight encryption algorithms, such as perceptual encryption [13] and selective encryption [9], are competent for this purpose.
- The strong correlation among adjacent pixels/frames of image/video cannot be thoroughly removed by traditional block ciphers in some operation modes. Here, an example is given to illustrate this phenomenon. The cartoon image shown in Fig. 1a is encrypted using DES under the electronic codebook mode, the corresponding cipher-image is depicted in Fig. 1b. It is clear that the shape of the cartoon image can be recognized from the cipher-image directly without decryption.

Chaos, which has been extensively studied since 1960s, appears to be a promising solution to the above mentioned challenges. This is because some intrinsic characteristics of chaotic maps, such as sensitivity and ergodicity, coincide with the confusion and diffusion properties of a good cryptographic algorithm [20]. Consequently, many chaos-based encryption algorithms [3, 6–8, 18, 19] have been proposed in the past decade. At the same time, the cryptanalyses of these ciphers also received considerable research attention [2, 5, 11, 17, 21, 27]. When a chaotic system is implemented using finite precision computation, it suffers seriously from the so-called dynamical degradation, which accounts for the phenomenon that some dynamical properties are substantially different from those found in the continuous setting [12]. A typical cryptanalysis work making use of the dynamical degradation of chaotic functions was presented in [15].

With the aim of bypassing the intractable dynamical degradation problem, Li et al. proposed a novel image encryption algorithm based on a 2D coupled logistic map [16].

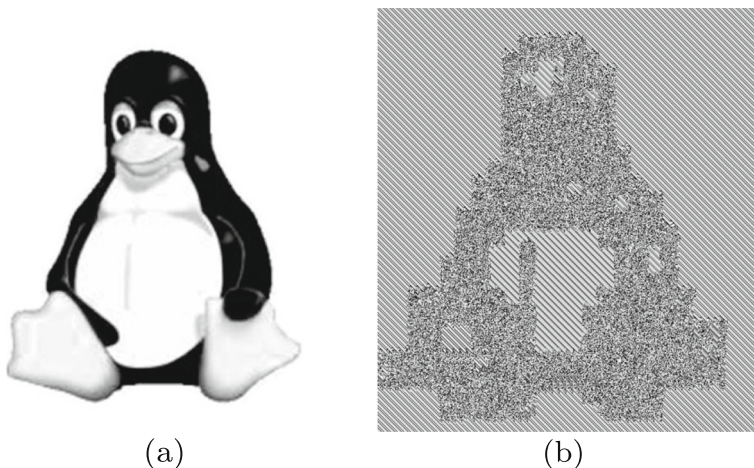


Fig. 1 **a** A cartoon image; **b** cipher-image of **(a)** using DES under the electronic codebook mode

Instead of using quantized output sequences of the underlying chaotic map, which is a common method employed by most chaotic ciphers, two random sequences are generated by means of sorting the chaotic outputs. Then, one of the random sequences is used to mask the plain-image as performed in the Veginère cipher and the remaining one is used to further scramble the previous output. Intuitively, this cipher is not as secure as the authors claimed in [16, Section 3] since it does not possess sufficient avalanche effect [22].

In [28], Zhang et al. suggested two attacks to compromise the scheme of [16]. They can be considered as a combination of chosen-plaintext attack and differential attack. Though the proposed attacks are feasible in theory, they require a large number of chosen plain-images, so the computation complexity is high. By breaking the equivalent key streams in reverse order as suggested in [28], we propose a chosen-plaintext attack which is optimal in terms of the required number of chosen plain-images. Moreover, we present an elaborately designed known-plaintext attack to break this encryption algorithm efficiently.

The rest of this paper is organized as follows. The next section introduces the original image encryption algorithm briefly. In Section 3, the two attack methods suggested by Zhang et al. are reviewed. Then we present the proposed optimal chosen-plaintext attack and the efficient known-plaintext attack, together with the simulation results. Section 4 is devoted to the extension of our known-plaintext attack to all permutation-only ciphers. Some remedies by slightly modifying the original design are also suggested to achieve higher security. Finally, conclusions are drawn in the last section. All the results presented in this paper is reproducible and the scripts needed to generate the simulation results are openly accessible.¹

2 The image encryption algorithm under study

In this section, we describe the image cipher of [16] in a concise way provided that its security is not changed. Some simulation results are presented after the description. Given the secret key $(x_0, y_0, \mu_1, \mu_2, \gamma_1, \gamma_2)$, the cipher operates as follows:

1. Input an 8-bit gray-scale image of size L and convert it to a one-dimensional sequence $P = \{p(i)\}_{i=1}^L$ in raster scan order.
2. Generate two sequences $\{x_i\}_{i=1}^L$ and $\{y_i\}_{i=1}^L$ using the 2D coupled logistic map given by (1) with initial condition $\{x_0, y_0\}$ and control parameters $\{\mu_1, \mu_2, \gamma_1, \gamma_2\}$,

$$\begin{cases} x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_1 y_i^2, \\ y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2(x_i^2 + x_i y_i). \end{cases} \tag{1}$$

3. Sort the two sequences $\{x_i\}_{i=1}^L$ and $\{y_i\}_{i=1}^L$ to obtain

$$\begin{aligned} [U, \hat{X}] &= \text{sort}(\{x_i\}_{i=1}^L), \\ [V, \hat{Y}] &= \text{sort}(\{y_i\}_{i=1}^L), \end{aligned}$$

where \hat{X} and \hat{Y} are the resultant sequences after sorting $\{x_i\}_{i=1}^L$ and $\{y_i\}_{i=1}^L$ in ascending order, respectively, $U = \{u(i)\}_{i=1}^L$ and $V = \{v(i)\}_{i=1}^L$ are their corresponding index values.

¹<https://sites.google.com/site/leoyuzhang>.

4. Compute the corresponding pixel value of the cipher-image according to the following formula:

$$c(v(i)) = p(i) \dot{+} u(i), \quad (2)$$

where $i \in \{1, 2, \dots, L\}$ and $(a \dot{+} b) = (a + b) \bmod 256$.

5. Rearrange the one-dimensional sequence $\{c(i)\}_{i=1}^L$ to a two-dimensional matrix row by row and the cipher-image is thus obtained.

We are not going to describe the detailed decryption algorithm since it is very similar to the encryption one. Two 512×512 plain-images, “Baboon” and “Lenna” depicted in Fig. 2a and c, respectively, are encrypted using the secret key $(x_0, y_0, \mu_1, \mu_2, \gamma_1, \gamma_2) = (0.02145, 0.3678, 2.93, 3.17, 0.179, 0.139)$, which is identical to the key chosen in [16, Section 4.1]. Their cipher-images are shown in Fig. 2b and d, respectively.

3 Cryptanalysis

In the original paper [16], the authors claimed that the initial condition $\{x_0, y_0\}$ and the control parameters $\{\mu_1, \mu_2, \gamma_1, \gamma_2\}$ of the $2D$ coupled logistic map should serve as the

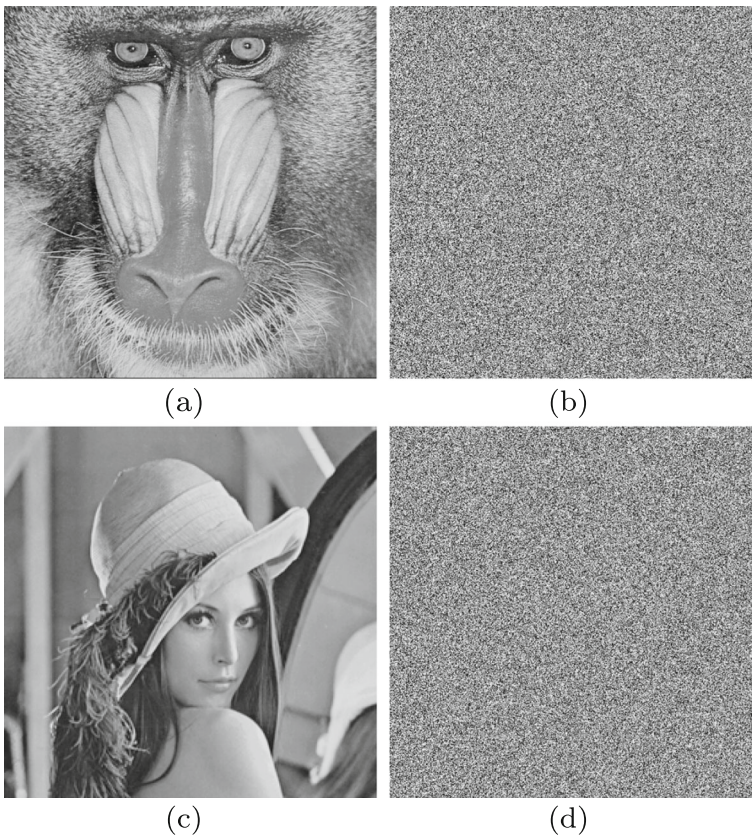


Fig. 2 Two plain-images and their corresponding cipher-images: **a** plain-image “Baboon”; **b** cipher-image of “Baboon”; **c** plain-image “Lenna”; **d** cipher-image of “Lenna”

secret key to guarantee a huge key space for resisting brute-force attacks. From the crypt-analytic point of view, our objective is to reveal the equivalent keystreams $\{u(i)\}_{i=1}^L$ and $\{v(i)\}_{i=1}^L$ used in the encryption process [28, Section 3], rather than finding the exact initial key $(x_0, y_0, \mu_1, \mu_2, \gamma_1, \gamma_2)$. Also, it is commonly believed that iterating a chaotic system reversely from its output is computational intractable.

Obviously, the function of two sequences $\{u(i)\}_{i=1}^L$ and $\{v(i)\}_{i=1}^L$ is identical to the secret key when the algorithm is used to encrypt plain-images of the same size. According to **Fact 1** and the encryption formula (2), we know that the sequence $\{u(i)\}_{i=1}^L$ is equivalent to $\{k(i)\}_{i=1}^L$ in the encryption process if $k(i) = u(i) \bmod 256$. Now, we can rewrite the encryption equation (2) as

$$c(v(i)) = p(i) \dot{+} k(i). \tag{3}$$

Fact 1 $(a \dot{+} b) = (a \dot{+} (b \bmod 256))$.

Taking these factors into consideration, we are now able to compromise the cipher under study. Section 3.1 presents some cryptanalysis work performed by Zhang et al. [28]. We briefly review their attacks and provide the mathematical interpretations of *Method II* in [28, Section 3.2] based on a simple fact.² Section 3.2 presents an optimal chosen plaintext attack using the minimum number of chosen plain-images. This is a direct application of the result reported in [10, 14] after carrying out a change of variables. In Section 3.3, we focus on the cryptanalysis of this cipher under the known plain-image attack scenario. Theoretical analyses and experimental results are provided to demonstrate the effectiveness of our attacks.

3.1 Attacks proposed by Zhang et al.

Chosen-plaintext attack is a fundamental attack scenario which plays a significant role in evaluating the security of a cipher. In this attack scenario, the attackers have the freedom to choose any plaintexts to be encrypted and obtain the corresponding ciphertexts. Differential attack, which was firstly proposed by Biham and Shamir for cracking DES [4], is an effective tool to evaluate a cipher with Feistel structure. It is also found useful for analyzing other encryption algorithms [11, 25].

In [28], Zhang et al. suggested two methods to break the cipher under study. Both methods are composed of chosen plain-image attack and differential attack. The basic ideas behind these methods are the same but the second method requires fewer chosen plain-images.

The first method operates as follows. Choose a black image $P = \{p(i)\}_{i=1}^L$ whose pixel values are all zero. Then select another plain-image $P' = \{p'(i)\}_{i=1}^L$ with only one pixel different from P , e.g., $p'(1) = 1$ and $p'(i) \equiv 0$ for all $i > 1$. Encrypt these two images and denote the corresponding cipher-images as $C = \{c(i)\}_{i=1}^L$ and $C' = \{c'(i)\}_{i=1}^L$, respectively. According to the encryption formula given by (3), it can be concluded that, only one pair of pixel elements are different in the two corresponding cipher-images. Making use of the differential relationship of the cipher-image pixels, we can formulate this phenomenon as

$$\begin{aligned} c(v(1)) \dot{-} c'(v(1)) &= (0 \dot{+} k(1)) \dot{-} (1 \dot{+} k(1)) \neq 0, \\ c(v(i)) \dot{-} c'(v(i)) &= (0 \dot{+} k(i)) \dot{-} (0 \dot{+} k(i)) = 0, \end{aligned}$$

²Instead of proving the effectiveness of *Method II* mathematically, the authors of [28] solved the problem by trying all possible combinations.

where $i > 1$ and $(a \dot{-} b) = (a - b + 256) \bmod 256$. Thus, it is easy to identify $v(1)$ by finding the nonzero element of the difference image between C and C' . Moreover, one can determine $k(1)$ from the relationship $k(1) = c(v(1)) \dot{-} p(1)$. Repeat the process for $(L - 1)$ more times using different chosen plain-images who have only one pixel different from the black image, one can finally reveal all the equivalent key streams $\{k_i\}_{i=1}^L$ and $\{v_i\}_{i=1}^L$ at the cost of $(1 + L)$ chosen-plain images.

The second method improves the first one in terms of the required number of chosen plain-images by utilizing the fact that a gray-scale image has 256 different pixel values. Randomly set 255 pixels different from P having gray values $\{1, 2, \dots, 255\}$, and denote this chosen-image as P' . Referring to **Fact 2**, it is easy to conclude that the difference between P and P' is exactly the same as the difference of their corresponding cipher-images, but the locations are shuffled by the key stream $\{v(i)\}_{i=1}^L$. According to the bijection relationship of the 255 different gray values between difference of plain-images and difference of cipher-images, one can obtain 255 distinct position relationships and thus the corresponding values of $k(i)$ are revealed. In conclusion, the image scrambling algorithm can be broken with $(1 + \lceil L/255 \rceil)$ chosen plain-images.

Fact 2 $f(x) = (x \dot{+} k) \dot{-} k = x$, where k and x are integers in the interval $[0, 255]$.

The two chosen plain-images shown in Fig. 3a and b are encrypted using the key selected in [16, Section 4.1]. The difference of the two cipher-images,³ which is shown in Fig. 3c, are used to recover 255 unknowns of the key stream $\{v(i)\}_{i=1}^L$. Repeat this process for $(\lceil L/255 \rceil - 1)$ more times using other chosen plain-images as we described above, the equivalent key streams used for encryption can be revealed completely. The recovered key streams are further used to attack the cipher-image depicted in Fig. 2b. The retrieved image is exactly the same as the original image “Baboon”, as shown in Fig. 3.

3.2 Optimal chosen-plaintext attack

As observed in Section 3.1, the attacks suggested in [28] retrieve the equivalent secret key $v(i)$ and $k(i)$ sequentially, i.e., recover $v(i)$ first and then $k(i)$. Here, we suggest recovering $v(i)$ and $k(i)$ in a reversed order. It is shown that the optimality of the chosen plain-image attack can be achieved by employing a simple change of variables technique.

Without loss of generality, suppose that there exists a random sequence $\{r(j)\}_{j=1}^L$ such that

$$r(v(i)) = k(i),$$

where $\{v(i)\}_{i=1}^L$ is the undetermined equivalent key stream. Substitute $r(j)$ into (3), we have

$$c(v(i)) = p(i) \dot{+} r(v(i)). \tag{4}$$

First, choose a plain-image P with constant pixel values, i.e., $P = \{p(i) \equiv d\}_{i=1}^L$ and $d \in [0, 255]$. Then obtain the corresponding cipher image $C = \{c(i)\}_{i=1}^L$. Referring to (4), we can reveal the equivalent key stream $\{r(j)\}_{j=1}^L$ by solving

$$r(i) = d \dot{-} c(i),$$

where $i = 1, 2, \dots, L$.

³Perceptually, Fig. 3c is identical to Fig. 3a. However, there are 255 nonzero pixels uniformly distributed in Fig. 3c but not in Fig. 3a.

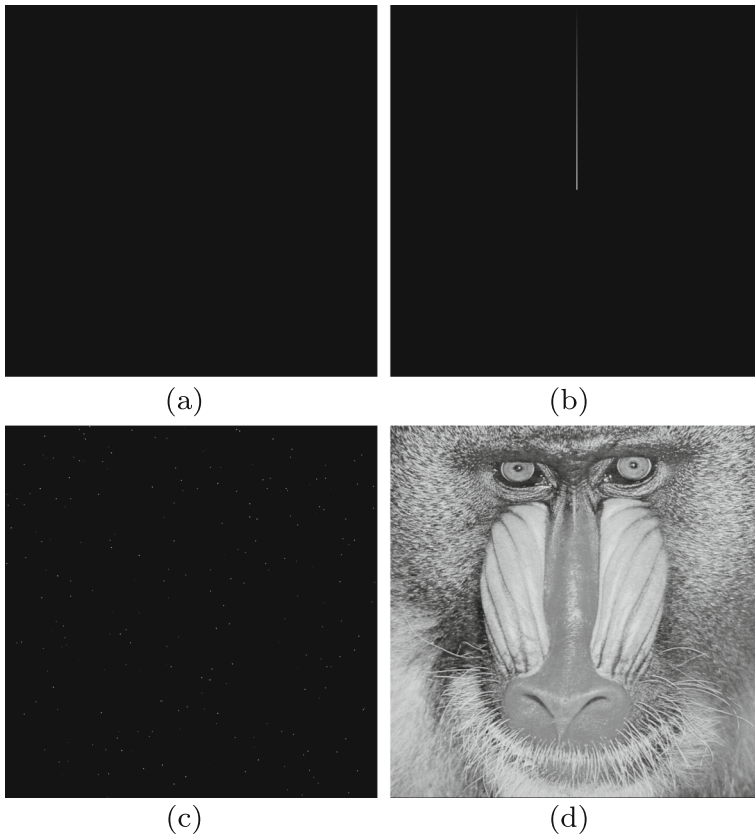


Fig. 3 Test of *Method II* in [28]: **a** the black chosen plain-image; **b** a modified chosen plain-image; **c** the difference between cipher-images of **(a)** and **(b)**; **d** the image recovered from the cipher-image shown in Fig. 2b

Once the sequence $\{r(i)\}_{i=1}^L$ has been recovered, the image encryption algorithm under study is reduced to a permutation-only encryption algorithm. Referring to the cryptanalysis of permutation-only encryption algorithms [10, 14], $\lceil (\log_2 L)/8 \rceil$ pairs of chosen plain-images are sufficient to recover the unknown equivalent key sequence $\{v(i)\}_{i=1}^L$. The optimality of the proposed chosen plain-image attack is trivial since we only require a chosen image to recover $\{r(i)\}_{i=1}^L$ and its optimality on permutation-only cipher has already been proven in [10].

3.3 The proposed known-plaintext attack

In a known-plaintext attack scenario, the attacker possesses some samples of both the plaintext and the corresponding ciphertext. Different from the chosen-plaintext attack, the attacker is not allowed to choose the plaintext to be encrypted. In other words, if the attacker inputs a message with elaborately designated structures for encryption, a trusted third party or the encryption machine will reject this request. Generally speaking, cryptanalysis based on known-plaintext attack is more difficult than that using chosen-plaintext attack.

Assume that two plain-images $P_1 = \{p_1(i)\}_{i=1}^L$, $P_2 = \{p_2(i)\}_{i=1}^L$ and the corresponding cipher-images $C_1 = \{c_1(i)\}_{i=1}^L$, $C_2 = \{c_2(i)\}_{i=1}^L$ encrypted with the same secret key are available. Obviously, for any $i, j \in [1, L]$, if $\Delta_p \doteq (p_1(i) \dot{-} p_2(i)) = \Delta_c \doteq (c_1(j) \dot{-} c_2(j))$, one can realize that j is a possible solution of $v(i)$. As $\Delta_c \in [0, 255] \ll L$ and the pixel values of the cipher-images are uniformly distributed in $[0, 255]$, there are roughly $\lceil L/256 \rceil$ locations of the cipher-image pixels whose difference $(c_1(j) \dot{-} c_2(j))$ equals Δ_p , i.e., each $v(i)$ has roughly $\lceil L/256 \rceil$ candidates.

Intuitively, more pairs of known plain-image and the corresponding cipher-image help eliminating the ambiguity of these candidates. To study this effect in a systematic way, we introduce the Self-Difference Matrix (SDM).

Definition 1 (Self-Difference Matrix) Given a sequence $\mathbf{P}_i = \{p_k(i)\}_{k=1}^n$, the Self-Difference Matrix (SDM) of \mathbf{P}_i is defined as follows:

$$\text{SDM}(\mathbf{P}_i) = \begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,n} \\ m_{2,1} & m_{2,2} & \dots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \dots & m_{n,n} \end{pmatrix}, \tag{5}$$

where

$$m_{r,c} = \begin{cases} (p_r(i) \dot{-} p_c(i)), & \text{if } r < c; \\ 0, & \text{if } r = c; \\ (p_c(i) \dot{-} p_r(i)), & \text{if } r > c. \end{cases}$$

Suppose that there are n pairs of known plain-images and the corresponding cipher-images, which are denoted as $\mathbf{P} = \{P_k\}_{k=1}^n$ and $\mathbf{C} = \{C_k\}_{k=1}^n$, respectively. According to the previous analyses and Definition 1, we know that if $\text{SDM}(\{p_k(i)\}_{k=1}^n) = \text{SDM}(\{c_k(j)\}_{k=1}^n)$, j is a possible solution of $v(i)$.

Initialize i with $i = 1$ and set $\mathbb{L} = [1, L]$, the procedures of the proposed known-plaintext attack using n pairs of known plain-images and the corresponding cipher-images can be described as follows:

- Step 1: Find $A_i = \text{SDM}(\{p_k(i)\}_{k=1}^n)$ using Definition 1.
- Step 2: Find $\text{SDM}(\{c_k(j)\}_{k=1}^n)$ for all $j \in \mathbb{L}$. Determine the candidate set of $v(i)$ as $\mathbb{S} = \{j \in [1, L] \mid \text{SDM}(\{c_k(j)\}_{k=1}^n) = A_i\}$, then randomly choose a candidate $j' \in \mathbb{S}$ and set $v(i) = j'$. Delete j' from \mathbb{L} to avoid conflict in the next round.
- Step 3: If $i < L$, go to Step 1 and repeat the above operations.
- Step 4: If $i = L$, compute $k(i)$ for all pixels by

$$k(i) = c(v(i)) \dot{-} p(i).$$

Once $\{k(i)\}_{i=1}^L$ and $\{v(i)\}_{i=1}^L$ are available, we can use them as the equivalent secret key to decipher any intercepted cipher-images encrypted with the same initial key.

The success of the above attack completely relies on Step 2, where we randomly choose a candidate from set \mathbb{S} . We begin the theoretical analysis of the success rate with the following two trivial facts:

- The success rate rises as the number of known plain-images n increases, i.e., the degree of freedom of SDM, $\tau = \frac{n \cdot (n-1)}{2}$, becomes larger.
- If the cardinality of \mathbb{S} satisfies $\#\{\mathbb{S}\} = 1$, it is confirmed that the obtained $v(i)$ is correct.

When $n = 1$, the degree of freedom of SDM is $\frac{2 \cdot (2-1)}{2} = 1$. As explained before, there exists $\lceil L/256 \rceil$ candidates on the condition that pixels of the difference image between two cipher-images are uniformly distributed in $[0, 255]$. For the special case $L = 256$, i.e., the number of pixels is exactly equal to 256, the uniformity of pixels of difference between the two cipher-images forces every integer in $[0, 255]$ appears once and only once.⁴ Then in Step 2, we can find one and only one j such that $\text{SDM}(\{c_k(j)\}_{k=1}^n) = A_i$ for certain A_i . In other words, all $\{v(i)\}_{i=1}^L$ are derived accurately under this circumstance.

Let us consider the practical scenario that the degree of freedom of SDM satisfies $\tau > 1$ and the number of image pixels obeys $L \gg 256$. As analyzed before, every valid entry of SDM has roughly $\lceil L/256 \rceil$ candidates. It is also noted that entries of SDM which have the same gray value contribute nothing to further reduce $\#\{\mathbb{S}\}$ in Step 2. Finally, based on the assumption that pixels of difference image between cipher-images are uniformly distributed, we conclude that the attack will succeed with overwhelming probability if

$$256^\tau \cdot \frac{(256)}{256} \cdot \frac{(256 - 1)}{256} \cdot \dots \cdot \frac{(256 - (\tau - 1))}{256} > L. \tag{6}$$

For illustration purpose, we calculate the required number of known plain-images to crypt-analyze an intercepted cipher-image of size 512×512 . In this case, $L = 512 \times 512$. By (6), one can easily find that $n \geq 3$ should be adopted.

Obviously, the computation complexity of the proposed attack is mainly caused by the iterations through Step 1 to Step 3. To work out A_i in Step 1, one needs to compute a symmetric SDM at the cost of $O(n^2)$. In Step 2, one needs to find j' which satisfies $\text{SDM}(\{c_k(j')\}_{k=1}^n) = A_i$. Then the rough computation complexity of Step 2 is $O(L)$. Step 3 needs the iteration of Step 1 and Step 2 for L times. Thus the overall complexity of this chosen-plaintext attack is $O(L^2 \cdot n^2)$. As will be shown in the following simulations, $n = 4$ is an empirical setting for practical implementation. For images having a normal size, e.g., 1024×1024 , L reaches $O(10^6)$. Thus the overall complexity of this algorithm could be as large as $O(10^{13})$, which is inefficient for practical implementation. In the following discussion, we will employ a simple strategy to trade space for time. Instead of searching possible solutions for $v(i)$ one by one as described in Step 1 and Step 2, we pre-calculate all $\{A_i\}_{i=1}^L$ by $A_i = \text{SDM}(\{p_k(i)\}_{k=1}^n)$ and store the results as a sequence in a high-dimensional space. For each element of $\{A_i\}_{i=1}^L$, i.e., a SDM, we further map it to an integer between 1 and L . For any SDM's of the cipher-images, i.e., $\text{SDM}(\{c_k(j)\}_{k=1}^n)$, we perform the same mapping for this matrix to obtain an integer fall into the range $[1, L]$ and immediately turn to the corresponding SDM of the plain-images who has the same mapping output. In this way, the computation complexity of the proposed attack is reduced from $O(L^2 \cdot n^2)$ to $O(L \cdot n^2)$ at the cost of extra memory of size $O(L \cdot n^2)$.

To verify the feasibility of the proposed known-plaintext attack, a lot of experiments have been carried out under the same key settings as employed in [16, Section 4.1]. The recovery results of Fig. 2 using 3 and 4 pairs of known plain-images are shown in Fig. 4a and b, respectively. Define the *recovery rate* as

$$\text{recovery rate} = \frac{\text{number of correctly recovered pixels}}{\text{total number of pixels}} \times 100 \%,$$

⁴It should be noticed that pixels of the difference image between two cipher-images are not uniformly distributed in the encryption algorithm under study. It is equal to the difference of the two corresponding plain-images, as pointed out in **Fact 2**.

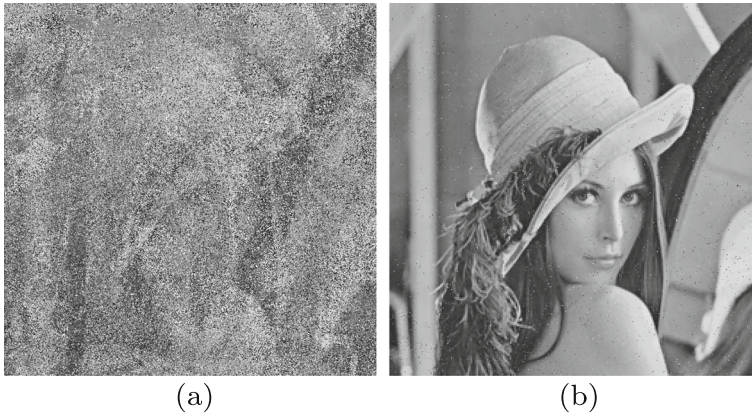


Fig. 4 The “Lenna” image recovered from the cipher-image shown in Fig. 2d using the proposed known-plaintext attack with (a) 3 known plain-images; (b) 4 known plain-images

we found that the *recovery rates* of Fig. 4a and b are 23.63 % and 98.45 %, respectively. It is clear that Fig. 4a only contains a small amount of visual information of the original image, and we can barely figure out the contour of the original image. However, the *recovery rate* reaches 98.45 % in Fig. 4b and almost all subtle details can be observed. The incorrectly

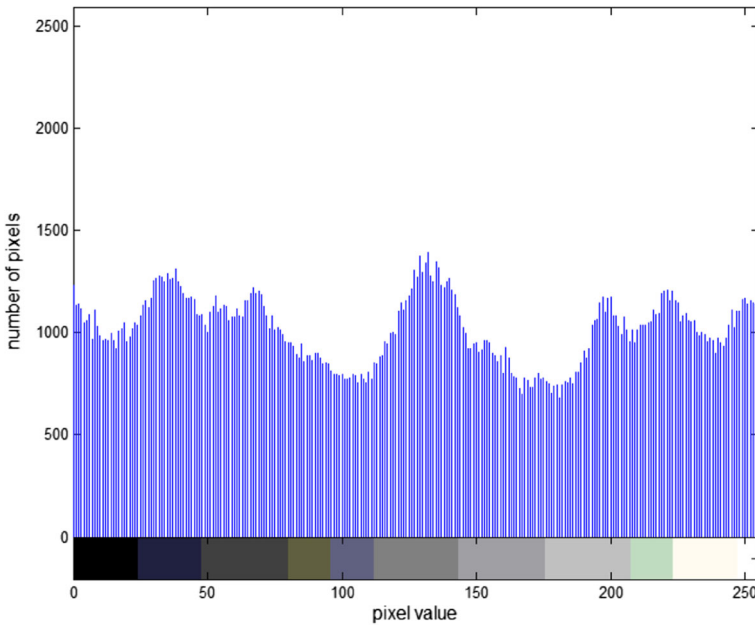


Fig. 5 Histogram of difference of two cipher-images corresponding to known plain-images “Lenna” and “Peppers”. The key used is $(x_0, y_0, \mu_1, \mu_2, \gamma_1, \gamma_2) = (0.02145, 0.3678, 2.93, 3.17, 0.179, 0.139)$

recovered pixels can be treated as noise which can be eliminated by simple spatial filters. There are two reasons accounting for this mismatch between theoretical analyses and experimental results: (1) Pixel distribution of the difference image between cipher-images corresponding to two known plain-images is not uniform, while our theoretical bound are derived under the uniform distribution assumption. A typical example is shown in Fig. 5. (2) From Step 2 of the proposed attack, it can be found that a single incorrectly recovered $v(i)$ will double the error rate.

To further study this phenomenon, more experiments were carried out on images having different textures using randomly generated secret keys. The *recovery rates* of 3 and 4 chosen plain-images are plotted in Fig. 6. It can be observed that the *recovery rates* reaches 95 % for all the test images when the number of known plain-images is 4, while the *recovery rates* are around 25 % for almost all test images for 3 known plain-images. Thus, the extra known plain-image and its corresponding cipher-image can be considered as a penalty term to bridge the gap between theoretical analysis and practical implementation.

4 Discussion

In this section, we study the possibility of employing SDM for cryptanalyzing any permutation-only cipher and suggest several remedies to enhance the security of the cipher proposed in [16] under the criterion that the structure of the original design keep unchanged.

Without loss of generality, set $k(i)$ in (3) to zero for all $i \in [1, L]$ and formulate a permutation-only cipher as

$$c(v(i)) = p(i).$$

To fit this new encryption model, we define the Self-Difference Matrix of a permutation-only cipher as follows:

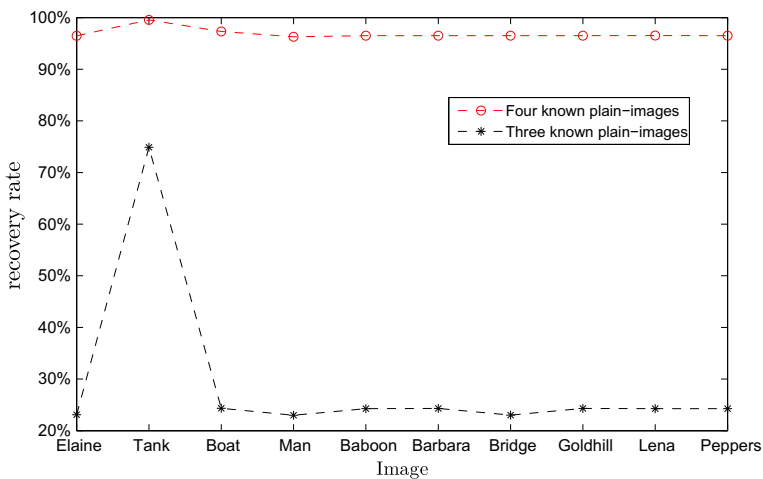


Fig. 6 The *recovery rate* of the proposed known-plaintext attack using 3 or 4 known plain-images and the corresponding cipher-images

Definition 2 (Self-Difference Matrix of a permutation-only cipher) Given a sequence $\mathbf{P}_i = \{p_k(i)\}_{k=1}^n$, the SDM of \mathbf{P}_i is

$$\text{SDM}(\mathbf{P}_i) = \begin{pmatrix} p_1(i) \\ p_2(i) \\ \vdots \\ p_n(i) \end{pmatrix}.$$

Now, it is clear that if one possesses a number of known plain-images and their corresponding cipher-images, he can follow the exact steps described in Section 3.3 to retrieve any intercepted cipher-images.

Both our work and Zhang et al.'s are capable of compromising the cipher in [16] using various methods. This security defect roots in the insensitivity to the changes of plain-image, i.e., insufficient avalanche effect. Nevertheless, there are several techniques to improve the security level of the scheme under study without altering the structure of its original design. The most intuitive one is taking the hash value of plain-image as initial condition or control parameters of the employed chaotic system to guarantee better avalanche effect. However, this approach requires extra transmission load since legitimate users will not be able to decipher the received cipher-image unless he knows the exact hash value of the plain-image. An alternative method employs a dynamical permutation technique by feeding back the plain-image's statistical information to the generation process of the permutation key stream [24]. In this way, the whole cipher operates in an apparent "one time pad" manner and its resistance to known/chosen-plaintext attack is thus improved.

5 Conclusion

This paper re-evaluates the data and computational complexity for breaking an image cipher based on scrambling and Veginère cipher. In the chosen-plaintext attack scenario, we propose the optimal chosen plain-image attack by improving the work of Zhang et al. In the known-plaintext attack scenario, we present an efficient known plain-image attack which makes use of the self-difference matrix. The required number of known-images to guarantee a successful attack has been worked out theoretically. Some practical considerations of this attack are also discussed for the purpose of implementing it on a personal computer.

Our work confirms that it is impossible to avoid the security issues by just incorporating chaotic function as the core of the derived cryptosystem. Rules suggested in [1] should be followed to guarantee a reasonable level of security and fulfill most of the cryptographic requirements. Although our work is focused on the cryptanalysis of a chaotic image cipher, the developed strategy can be applied to ciphers based on other complex and dynamical phenomenon, such as image ciphers based on quantum walk [23], DNA coding [26], etc. Lessons learnt from the cryptanalysis of these ciphers will possibly provide useful insights for designing more secure and efficient image cryptosystem.

References

1. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurcation Chaos* 16(08):2129–2151
2. Alvarez G, Montoya F, Romera M, Pastor G (2004) Cryptanalysis of dynamic look-up table based chaotic cryptosystems. *Phys Lett A* 326(3):211–218

3. Behnia S, Akhshani A, Mahmodi H, Akhavan A (2008) A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons Fractals* 35(2):408–419
4. Biham E, Shamir A (1991) Differential cryptanalysis of DES-like cryptosystems. *Adv Cryptol - Crypto* 90 537:2–21
5. Chen Y, Liao X, Wong KW (2006) Chosen plaintext attack on a cryptosystem with discretized skew tent map. *IEEE Trans Circ Syst II: Express Briefs* 53(7):527–529
6. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons Fractals* 21(3):749–761
7. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifurcation Chaos* 8(06):1259–1284
8. Jakimoski G, Kocarev L (2001) Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Trans Circ Syst I: Fundam Theory Appl* 48(2):163–169
9. Kim H, Kim M (2011) A selective protection scheme for scalable video coding. *IEEE Trans Circ Syst Video Technol* 21(11):1733–1746
10. Li C, Lo KT (2011) Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Proc* 91(4):949–954
11. Li C, Zhang LY, Ou R, Wong KW, Shu S (2012) Breaking a novel colour image encryption algorithm based on chaos. *Nonlinear Dyn* 70(4):2383–2388
12. Li S, Chen G, Mou X (2005) On the dynamical degradation of digital piecewise linear chaotic maps. *Int J Bifurcation Chaos* 15(10):3119–3151
13. Li S, Chen G, Cheung A, Bhargava B, Lo KT (2007) On the design of perceptual MPEG-video encryption algorithms. *IEEE Trans Circ Syst Video Technol* 17(2):214–223
14. Li S, Li C, Chen G, Bourbakis NG, Lo KT (2008) A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process Image Commun* 23(3):212–223
15. Li S, Mou X, Cai Y, Ji Z, Zhang J (2003) On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. *Comput Phys Commun* 153(1):52–58
16. Li S, Zhao Y, Qu B, Wang J (2012) Image scrambling based on chaotic sequences and Veginère cipher. *Multimedia Tools Appl* 66(3):1–16
17. Li W, Yuan Y (2009) Improving security of an image encryption algorithm based on chaotic circular shift. In: *Proceedings of IEEE international conference on systems, man and cybernetics (SMC)*, pp. 3694–3698
18. Mao Y, Chen G, Lian S (2004) A novel fast image encryption scheme based on 3D chaotic baker maps. *Int J Bifurcation Chaos* 14(10):3613–3624
19. Riad AM, Hussein AH, El-Azm A (2012) A new selective image encryption approach using hybrid chaos and block cipher. In: *Proceedings of 8th international conference on informatics and systems (INFOS)*, pp. 36–39
20. Shannon CE (1949) Communication theory of secrecy systems. *Bell Syst Tech J* 28(4):656–715
21. Solak E, Çokal C, Yildiz OT, Biyikoğlu T (2010) Cryptanalysis of Fridrich's chaotic image encryption. *Int J Bifurcation Chaos* 20(5):1405–1413
22. Trappe W, Washington LC (2002) *Introduction to cryptography with coding theory*. Prentice Hall, Upper Saddle River
23. Yang YG, Pan QX, Sun SJ, Xu P (2015) Novel image encryption based on quantum walks. *Sci Rep* 5(7784):1–9
24. Zhang LY, Hu X, Liu Y, Wong KW, Gan J (2014) A chaotic image encryption scheme owning temp-value feedback. *Commun Nonlinear Sci Numer Simul* 19(10):3653–3659
25. Zhang LY, Li C, Wong KW, Shu S, Chen G (2012) Cryptanalyzing a chaos-based image encryption algorithm using alternate structure. *J Syst Softw* 85(9):2077–2085
26. Zhang Q, Guo L, Wei X (2010) Image encryption using DNA addition combining with chaotic maps. *Math Comput Model* 52(11):2028–2035
27. Zhang Y, Xiao D, Wen W, Li M (2013) Cryptanalyzing a novel image cipher based on mixed transformed logistic maps. *Multimedia Tools Appl* 73(3):1885–1896
28. Zhang Y, Xiao D, Wen W, Nan H (2014) Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher. *Nonlinear Dyn* 78(1):235–240



Li Zeng received Bachelor's degree in Software Engineering from College of Information Engineering, Xiangtan University, China, in 2013. Currently, she is pursuing his Master degree from College of Information Engineering, Xiangtan University, China. Her research interest includes image processing, image security, etc.



Renren Liu received his Ph.D. degree in Central South University, China. He is currently working as Professor in the Department of College of Information Engineering, Xiangtan University, China. His research interest includes algorithm analysis, multiple-valued logic, etc.



Leo Yu Zhang received both his Bachelor's degree and Master's degree in Computational Mathematics from Xiangtan University in 2009 and 2012, respectively. From 2012 to 2013, he worked at the State Grid Electric Power Research Institute of China as a development engineer. Currently, he is pursuing his Ph.D. degree from the Department of Electronic Engineering, City University of Hong Kong, Hong Kong. His research interests include multimedia security and compressive sensing.



Yuansheng Liu received Bachelor's degree in Software Engineering from College of Information Engineering, Xiangtan University, China, in 2012. Currently, he is pursuing his Master degree from College of Information Engineering, Xiangtan University, China. His research interest includes cryptanalysis, data mining, machine learning, etc.



Kwok-Wo Wong received the B.Sc. degree in electronic engineering from the Chinese University of Hong Kong and the Ph.D. degree from the City University of Hong Kong, where he is currently an associate professor in the Department of Electronic Engineering. His current research interests include chaos, cryptography, and neural networks. He has published more than 100 papers in 25 international mathematics, physics, and engineering journals in the fields of nonlinear dynamics, cryptography, neural networks, and optics. He is a senior member of the IEEE. He is also a chartered engineer and a member of the Institution of Engineering and Technology (IET).