applied sciences

MDPI

Article

Cryptanalysis of a New Color Image Encryption Using Combination of the 1D Chaotic Map

Yuqiang Dou * and Ming Li

College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, Henan, China; liming@htu.edu.cn

* Correspondence: douyuqiang@htu.edu.cn

Received: 17 February 2020; Accepted: 16 March 2020; Published: 23 March 2020

Abstract Security of image communication is more and more important in many applications such as the transmission of military and medical images. To meet the requirement, a new color image encryption algorithm using a new one-dimension (1D) chaotic map was proposed recently, which can resist various attacks because the range of the new chaotic map is larger than that of the previous ones. In our study, the security of the new original method is analyzed and a novel attack method is proposed. It is demonstrated that the scheme is not secure under chosen-plaintext attack, by which the encrypted image can be successfully converted into the corresponding plaintext image without any error.

Keywords: cryptanalysis; color image encryption; 1D chaotic maps; chosen-plaintext attack

1. Introduction

Encryption of color image is a critical issue for confidentiality and security. Lots of encryption methods [1–8] using chaotic maps have been proposed for the excellent properties such as ergodicity and sensitivity to initial condition and control parameters. However, some cryptanalysis articles in [9–14] have verified the vulnerability of common chaotic encryption methods based on the permutation-diffusion structure. Hence, chaotic image encryption algorithms [15,16], combined with other special technologies, such as DNA, information entropy etc., have been nearly introduced. For example, the sensitivity mechanism is built up utilizing the information entropy of the plain-image in [16]. Cryptanalysis works have been correspondingly proposed in [17,18] to evaluate the security of image cryptosystems, which can improve the security of the existing cryptosystems. For example, Li et al. attacked the chaotic image encryption algorithm based on information entropy in [18].

Recently, some more chaotic image encryption algorithms based on Latin square have been designed [19–21] due to the cryptography property of Latin square. But Hu et al., found out an algebraic weakness in [22] and the chaotic image cipher is broken by chosen-plaintext attack with chosen ciphertext attack. In addition, Ge et al. in [23] found out the defect of the feedback image encryption algorithm with compound chaotic stream cipher based on perturbation and attacked the algorithm.

In [24], the image block encryption algorithm achieves high security level where three different chaotic maps are utilized respectively for controlling pixel shuffling, blocking size, and value encryption. However, Ma found out that there are some critical security defects in [25] and derive the secret key with a chosen plaintext attack.

Most cryptanalysis works have mainly focused on single round of permutation–diffusion image ciphers. However, most encryption schemes are based on multiple rounds of permutation-diffusion [26–32]. In [29], two rounds of permutation and pixel adaptive diffusion was proposed. In [32], an improved chaotic image encryption method using Latin square based on two rounds of permutation–

diffusion was proposed, which has weak security defects. However, Ming Li et al. find out the equivalent key streams and attacked the scheme in [33] and attacked the scheme.

However, most chaotic maps, used in generating the security key in encryption process, are multi-dimensional, which cause high level computation complexity. Recently, some 1D chaotic map encryption algorithms have been proposed in [34–36] which have lower computation complexity for software/hardware implementations. In [37] a new 1D chaotic map model is proposed where a new 1D chaotic map is made by using the classic chaotic map such as logistic, sine and Chebyshev maps. A bifurcation property of the chaotic map and the Lyapunov exponent, in addition to information entropy evaluation are much better than the classic chaotic system.

Aiming at [37], Hui Wang et al., found out an algebraic weakness of the cryptosystem in [38] and attacked its equivalent cryptographic scheme by chosen plaintext attack. The authors acquire the rotation factor by constructing two special functions and attack permutation with the methods in [39,40] which have high computation complexity. In this paper, a novel attack method to directly crack the original encryption scheme in [37] is proposed. The proposed method attacks the factor and diffusion using the properties of bit-level Xor and attacks permutation with a new scheme which has lower computation.

This paper organizes as follows. Section 2 overviews the new encryption method. Security of the scheme is analyzed and the attack scheme by chosen plaintext images is presented in Section 3. The simulation experiments to verify the proposed method are presented in Section 4. Conclusions are provided in Section 5.

2. Review of the Original Scheme

Before encryption divides the color image with size $M \times N$, this needs to be encrypted, into three grayscale images according to trichromatic theory. Then, link the grayscale images into another grayscale image with size $M \times 3N$. The sequence $S = \{s_1, s_2, \ldots s_{M\times 3N}\}$ is produced by reshaping the last gray image, and the length of which is $M \times 3N$.

The flow diagram of the 1D chaotic encryption scheme is shown in Figure 1. In permutation phase, X, which is a chaotic sequence, is acquired by iterating the new chaotic system $M \times 3\ N+N_0$ times and discarding the former N_0 elements. The new chaotic map in [37] is defined by the following equation:

$$x_{n+1} = F_{chaos}(u, x_n) \times 2^k - floor\left(F_{chaos}(u, x_n) \times 2^k\right) \quad (1)$$

where $F_{chaos}(u, x_n)$ is one of 1D chaotic maps as logistic, sine and Chebyshev maps. x_n is the output chaotic sequence. $u \in (0, 10]$ and $k \in [8, 20]$ are the initial values. The parameters of u, k and N_0 are utilized as the security key. The permutation position vector $X' = \{x'_1, x'_2, \ldots x'_{M\times 3N}\}$ is acquired by sorting vector S in ascending order. The image pixel vector P, which is permuted, is acquired by the equation of $P(i) = S(X'(i))$.

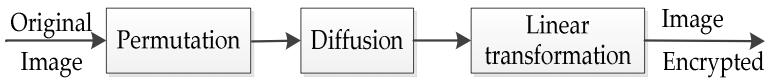


Figure 1. The flow diagram of the 1D chaotic image encryption.

In the diffusion phase, the diffused image pixel sequence C is acquired by the following equation:

$$C(i) = \mathrm{mod}(P(i) + D(i), 256) \oplus C(i-1) \quad (2)$$

where $C(0)$ is $P(M \times 3N)$ and D is the diffusion sequence which is obtained by Equation (3):

$$D(i) = \mathrm{mod}(floor(X(i) \times 10^{14}), 256) \quad (3)$$

The new cipher sequence of C' is acquired after C is rotated to the left by the quantity of lp which is used as the security key, too. The eventual cipher image is obtained by reshaping C' into RGB images.

3. Chosen-Plaintext Attack

The attack scheme is proposed in this part. Compared with other chaotic encryption algorithms, the rotation step is added in [37]. The rotation amount lp is used as the security key. If lp can be acquired, the permutation and diffusion steps can be attacked by imitating the attack method in [17]. Hence, the proposed attack method can be divided into two phases. In the first phase, we find the rotating amount of lp and the diffusion matrix D by shifting the Xor operations. In the second phase, we attack the permutation with some special plaintext images by imitating the attack method in [17]. We denote the original image I and the corresponding encrypted image C_I.

3.1. The First Phase of Attack

The two special properties of the Xor operator are utilized and the properties are given as below.

Property 1 $\alpha \oplus \alpha = 0$

Property 2 If $\alpha \oplus \beta = \lambda$, $\alpha = \lambda \oplus \beta$
where α, β, γ are positive integers.

The process for find out lp and D is conducted as the following steps.

Step 1: Choose a plaintext color image Z of size $M \times N$, the elements of which are all zero-pixel values. Z can be expressed as below.

$$Z = \begin{bmatrix} (0)(0)(0) & (0)(0)(0) & \cdots & (0)(0)(0) \\ (0)(0)(0) & (0)(0)(0) & \cdots & (0)(0)(0) \\ \cdots & \cdots & \cdots & \cdots \\ (0)(0)(0) & (0)(0)(0) & \cdots & (0)(0)(0) \end{bmatrix}_{M \times N} \tag{4}$$

The encrypted image C_Z is obtained from the encryption method above. Divide Z into three images according to RGB theory. The sequence of C' corresponding to C_Z is acquired by linking the three grayscale images and the length of that is $M \times 3N$. Denote the obtained sequence C after the diffusion. The diffusion equation corresponding to Z can be expressed according to Property 1, as below:

$$C(i) = D(i) \oplus C(i-1) \tag{5}$$

Obtain the pixel sequence C according to Equation (5) as below:

$$\begin{aligned} C = \{&D(1) \oplus C(0), D(2) \oplus C(1), D(3) \oplus C(2), \ldots, D(M*3N-1) \oplus C(M*3N-2), \\ &D(M*3N) \oplus C(M*3N-1)\} \end{aligned} \tag{6}$$

where D remains unchanged in the encryption process. C' is obtained by rotating C by the quantity of lp to the left as the follow sequence:

$$\begin{aligned} C' = \{&D(lp+1) \oplus C(lp), D(lp+2) \oplus C(lp+1), \ldots, D(M*3N-1) \oplus C(M*3N-2), \\ &D(M*3N) \oplus C(M*3N-1), D1 \oplus C0, D2 \oplus C1, \ldots, D(lp) \oplus C(lp-1)\} \end{aligned} \tag{7}$$

C'' is obtained by rotating C' once to the left as the following sequence:

$$\begin{aligned} C'' = \{&D(lp+2) \oplus C(lp+1), D(lp+3) \oplus C(lp+2), \ldots, D(M*3N) \oplus C(M*3N-1), \\ &D1 \oplus C0, D2 \oplus C1, D3 \oplus C2, \ldots, D(lp+1) \oplus C(lp)\} \end{aligned} \tag{8}$$

G is acquired according to Property 2 by the equation $G(i) = C'(i) \oplus C''(i)$ and given as below:

$$\begin{aligned} G = \{&D(lp+2),\ D(lp+3), \ldots, D(M*3N),\ D(1) \oplus C(0) \oplus D(M*3N) \oplus C(M*3N-1),\\ &D(2),\ D(3),\ \ldots,\ D(lp+1)\} \end{aligned} \tag{9}$$

$D(i)$ is acquired where $i \in [2, M*3N]$ but $D(1)$ remains unknown.

Step 2: Choose a plaintext color image Q with all k pixel values and the size of which is $M \times N$. Q can be expressed as below.

$$Q = \begin{bmatrix} (k)(k)(k) & (k)(k)(k) & \cdots & (k)(k)(k) \\ (k)(k)(k) & (k)(k)(k) & \cdots & (k)(k)(k) \\ \cdots & \cdots & \cdots & \cdots \\ (k)(k)(k) & (k)(k)(k) & \cdots & (k)(k)(k) \end{bmatrix}_{M \times N} \tag{10}$$

The encrypted image C_Q is obtained from the encryption system above. Divide Q into three images according to RGB theory. The sequence of C_q' corresponding to C_Q is acquired by linking the three gray scale images and the length of that is $M \times 3N$. Then we denote the obtained sequence C_q after the diffusion. The diffusion equation corresponding to Q can be expressed as follows:

$$C_q(i) = \mathrm{mod}(k + D(i), 256) \oplus C_q(i-1) \tag{11}$$

Following this, we can obtain the pixel sequence of C_q according to Equation (5), as below:

$$\begin{aligned} C_q = \{&\mathrm{mod}(k + D(1), 256) \oplus C_q(0), \mathrm{mod}(k + D(2), 256) \oplus C_q(1), \ldots,\\ &\mathrm{mod}(k + D(M*3N), 256) \oplus C_q(M*3N-1)\} \end{aligned} \tag{12}$$

where D remains unchanged in the encryption process. C' is obtained by rotating C by the quantity of lp to the left as the following sequence:

$$\begin{aligned} C_q' = \{&\mathrm{mod}(k + D(lp+1), 256) \oplus C_q(lp),\ \mathrm{mod}(k + D(lp+2), 256) \oplus C_q(lp+1),\ \ldots,\\ &\mathrm{mod}(k + D(M*3N-1), 256) \oplus C_q(M*3N-2),\ \mathrm{mod}(k + D(M*3N), 256) \oplus\\ &C_q(M*3N-1),\ \mathrm{mod}(k + D(1), 256) \oplus C(0),\ \mathrm{mod}(k + D2(lp+1), 256) \oplus C_q(1),\\ &\ldots,\ \mathrm{mod}(k + D(lp), 256) \oplus C_q(lp-1)\} \end{aligned} \tag{13}$$

C_q'' is obtained by rotating C' once to the left as the following sequence:

$$\begin{aligned} C_q'' = \{&\mathrm{mod}(k + D(lp+2), 256) \oplus C_q(lp+1),\ \mathrm{mod}(k + D(lp+3), 256) \oplus C_q(lp+2),\ \ldots,\\ &\mathrm{mod}(k + D(M*3N), 256) \oplus C_q(M*3N-1),\ \mathrm{mod}(k + D(1), 256) \oplus C_q(0),\\ &\mathrm{mod}(k + D(2), 256) \oplus C1, \mathrm{mod}(k + D(3), 256) \oplus C(2), \ldots,\\ &\mathrm{mod}(k + D(lp+1), 256) \oplus C_q(lp)\} \end{aligned} \tag{14}$$

G_q is acquired according to the Equation $G_q(i) = C_q'(i) \oplus C_q''(i)$ and is given below:

$$\begin{aligned} G_q = \{&\mathrm{mod}(k + D(lp+2), 256),\ \mathrm{mod}(k + D(lp+3), 256), \ldots, \mathrm{mod}(k + D(M*3N), 256),\\ &\mathrm{mod}(k + D(1) \oplus C_q(0), 256) \oplus \mathrm{mod}(k + D(M*3N), 256) \oplus C_q(M*3N-1), 256),\\ &\mathrm{mod}(k + D(2),\ 256), \mathrm{mod}(k + D(3), 256),\ \ldots,\ \mathrm{mod}(k + D(lp+1), 256\} \end{aligned} \tag{15}$$

Compared with Equation (9), we can't directly get $D(i)$ from Equation (15), but $D(i)$ can be acquired except $D(1)$ by $D = \mathrm{mod}(G_q - k, 256)$.

Step 3: W of size $M \times 3N$ is obtained by $W(i) = \mathrm{mod}(G_q(i) - G(i), 256)$ as below:

$$W = \{k,\ k,\ \ldots,\ k,\ p,\ k,\ k,\ \ldots,\ k\} \tag{16}$$

where

$$p = \mathrm{mod}(k + D(1) \oplus C_q(0), 256) \oplus \mathrm{mod}(k + D(M*3N), 256) \oplus C_q(M*3N-1) - D(1) \oplus C(0) \oplus D(M*3N) \oplus C(M*3N-1)$$

lp can be obtained according to the position of p in W by the following equation:

$$lp = M \times 3N - Pos_p \tag{17}$$

where Pos_p is the position of p.

Step 4: C can be obtained by rotating C' to the right lp times. $D(1)$ can be obtained by:

$$C(1) = D(1) \oplus C(0) \tag{18}$$

The permuted matrix P corresponding to the original can be obtained by:

$$P(i) = \mathrm{mod}(C_1(i) \oplus C_1(i-1) - D(i), 256) \tag{19}$$

Now we discuss if we can get lp by the two special plains where one is with all k_1 pixel values and the other is with all k_2 pixel values according to Equations (12) and (13).

$$W' = \{\mathrm{mod}(k_2 - k_1, 256),\ \mathrm{mod}(k_2 - k_1, 256), \ldots, \mathrm{mod}(k_2 - k_1, 256),\ p',\ \mathrm{mod}(k_2 - k_1,\ 256),\ \ldots,\ \mathrm{mod}(k_2 - k_1, 256\} \tag{20}$$

where

$$p' = \mathrm{mod}(k_2 - k_1 + D(1), 256) \oplus C_q(0) \oplus \mathrm{mod}(k_2 - k_1 + D(M*3N), 256) \oplus C_q(M*3N-1) - D(1) \oplus C(0) \oplus D(M*3N) \oplus C(M*3N-1)$$

We can get lp from Equation (20) since all the pixel values of W' except p' are the same. The above steps can be expressed as in Algorithm 1. Since the rotation amount lp and the diffusion matrix D have been obtained, the permuted image P_1 can be acquired by Algorithm 1.

Algorithm 1 Obtain the Rotation Amount lp and the Diffusion Matrix D

1: Set the plain image Z
2: Obtain the encrypted image pixel sequence C' after the reshape Cz
3: Obtain the sequence C''
4: $G(i) \leftarrow C'(i) \oplus C''(i)$
5: $D \leftarrow G$ *except* $D(1)$
6: Set the plain image Z
7: Obtain the encrypted image pixel sequence C_q' after the reshape Cz
8: Obtain the sequence C_q''
9: $G_q(i) \leftarrow C_q'(i) \oplus C_q''(i)$
10: $lp \leftarrow W(i) = \mathrm{mod}(G_q(i) - G(i), 256)$
11: $C \leftarrow lp, C'$
12: $D(1) \leftarrow C(1) = D(1) \oplus C(0)$

3.2. The Second Phase of Attack

In the following description *m*, *n* and μ are all positive integers. The plaintext sequences need to be divided into block. *S*, *R* and *U* represent the plaintext sequence in one division. The process of attacking permutation is as follows.

Step 1: Consider a plain sequence *S* and set it:

$$S = \left[S\{0\}, S\{1\}, \ldots, S\{i\} \ldots S\{\Omega - 1\} \right] \quad 2 \le \Omega \le 256 \tag{21}$$

where $S\{i\} = \left[i, i, \ldots i \right]_{l_1}$, $l_1 = M \times 3N / \Omega$ and call $S\{i\}$ first order sub-block. Convert *S* into the R, G and B color image with the size of $M \times N$ and the permutation sequence P_S corresponding to *S* can be obtained after the first phase.

Step 2: Choose pixel $P_S(j)$. If $P_S(j) = m$, the pixel in *S* corresponding to $P_S(j)$ would be one pixel which is in $S\{m\}$. Register the position of *j* in Set $INDEX\{m\}$. All the pixels of P_S would be registered in one set.

Step3: Consider a plain sequence *R* of size $M \times 3N$ and divide it into Ω first order blocks $R(i), i = 0,1,...,\Omega$. Divide each block into Ω second order blocks $R\{i\}\{j\}$ $j = 0,1,...,\Omega$ and set:

$$R\{i\}\{j\} = \left[j, j, \ldots j \right]_{l_2}, \quad l_2 = M \times 3N / \Omega \wedge 2 \tag{22}$$

The permutation sequence P_R corresponding to *R* can be obtained after the first phase.

Step 4: Choose pixel $P_R(t)$ $t \in Index\{m\}$. If $P_S(t) = n$, the pixel in *R* corresponding to $P_R(t)$ would be one pixel which is in $R\{m\}\{n\}$. Register the position of *t* in set $Index\{m\}\{n\}$. All the pixels of $P_R(t)$ would be registered in one second order set. If l_2=1, each $Index\{m\}\{n\}$ would include only one element and we can get all the corresponding permuted positions corresponding the elements in R. If l_2>1, repeat Step 3, 4 until the element quantity of *l*=1 and get the position matrix X′. The number of times of divisions is *f* and $f = ceil\left(\log_{\Omega} \left(M \times 3N \right) \right)$. The permutation attack process can be expressed as in Algorithm 2.

Algorithm 2 Permutation Attack

1: the plain sequence *S* from the first division and encrypt *S*
2: $P_S \leftarrow$ the first phase
3: $INDEX\{m\} \leftarrow check\ P_S$
4: set the plain sequence *R* from the second division and encrypt *R*
5: P_R from the first phase
6: $INDEX\{m\}\{n\} \leftarrow check\ P_R$
7: repeat further division until the element quantity *l*=1
8: $INDEX\{m\}\{n\}\cdots\{\mu\} \leftarrow$ check the last permuted matrix

For clarity of the relationship of *f*, Ω and image size, some values of *f* are shown as Table 1. *f* ascends when Ω descends and image size ascends according to Table 1.

Table 1. Values of *f* according to image size and Ω.

Image Size	Ω=256	Ω=128	Ω=64	Ω=32	Ω=16	Ω=8
256 × 256	3	3	3	4	5	6

512×512	3	3	3	4	5	6
1024×1024	3	3	4	4	5	7

If the size of I is 256×256 and $\Omega=256$, $f=3$. At the first time of division the plaintext sequence *S* can be set as:

$$S=\left[\left(0\,0\cdots0\right)_{256\times3}\left(1\,1\cdots1\right)_{256\times3}\left(2\,2\cdots2\right)_{256\times3}\cdots\left(255\,255\cdots255\right)_{256\times3}\right]_{256\times256\times3} \tag{23}$$

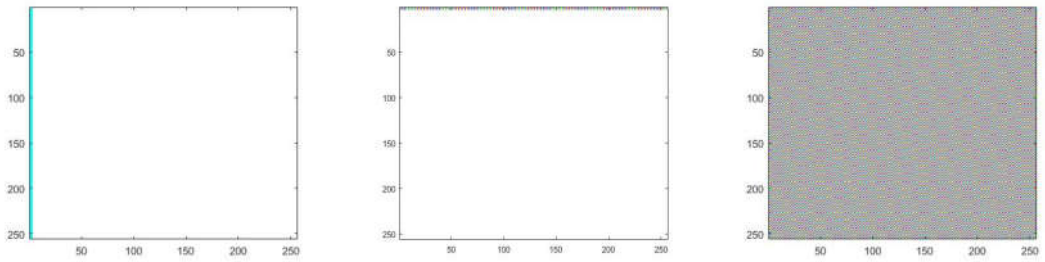
At the second time of division the plaintext sequence *R* can be set as:

$$R=\left[\left(0\,0\,0\right)\ \left(1\,1\,1\right)\cdots\left(255\right)\ \left(0\,0\,0\right)\ \left(1\,1\,1\right)\cdots\left(255\right)\cdots\left(0\,0\,0\right)\ \left(1\,1\,1\right)\cdots\left(255\right)\right]_{256\times256\times3} \tag{24}$$

At the third time of division the plaintext sequence *R* can be set as:

$$U=\left[\left(0\,1\,2\right)\ \left(0\,1\,2\right)\cdots\left(0\,1\,2\right)\right]_{256\times256\times3} \tag{25}$$

In the above sequences the right subscripts represent the length of the vectors.
Convert S, *R* and *U* into a color image, respectively, as shown in Figure 2a–c where most of the images of Figure 2a,b is white.



(a) (b) (c)

Figure 2. Images corresponding to the three division plaintext sequences: (a) Image corresponding to *S*, (b) Image corresponding to *R*, (c) Image corresponding to *U*.

Obviously, we can recover the corresponding original image *I* according to the above two phases.

4. Experiments and Analysis

A series of simulation experiments have been carried out to verify our attacking scheme with an Intel(R) Core(TM) i5-5300 CPU 2.39 GHz and 8 GB memory capacity. MALTAB R2016b is used for the experiments. Five standard images with the size of 256×256 are chosen in the experiments including 'Baboon', 'Soccer', 'Pepper', 'Lena', and 'Monarch as shown in Figure 3a1–e1. The corresponding encrypted images are shown in Figure 3(a2,b2,c2,d2,e2). We attack the *lp* and diffusion using the steps in the first phase in Section 3. The retrieved permutation-diffusion images and retrieved permutation-only images are obtained as in Figure 3(a3,b3,c3,d3,e3) and Figure 3(a4,b4,c4,d4,e4), respectively. After attacking permutation in the second phase in Section 3, the restored images are obtained which have been shown in Figure 3(a5,b5,c5,d5,e5). Figure 3(a5,b5,c5,d5,e5) coincides with the original images, compared with Figure 2(a1,b1,c1,d1,e1). The recovery performance evaluation can also be made by root mean square error (RMSE). Denoting the original image I and the recovered image I', RMSE defined as below.

$$RMSE=\sqrt{\sum_{j=1}^{n}\sum_{i=1}^{m}\left(I(i,j)-I'(i,j)\right)^2} \tag{26}$$

In all the experiments, the values of RMSE are all zeros which mean the recovered images are all the same as the corresponding original images. In other words, the original images are accurately recovered. Therefore, the attack results demonstrate the effectiveness of the cryptanalysis.

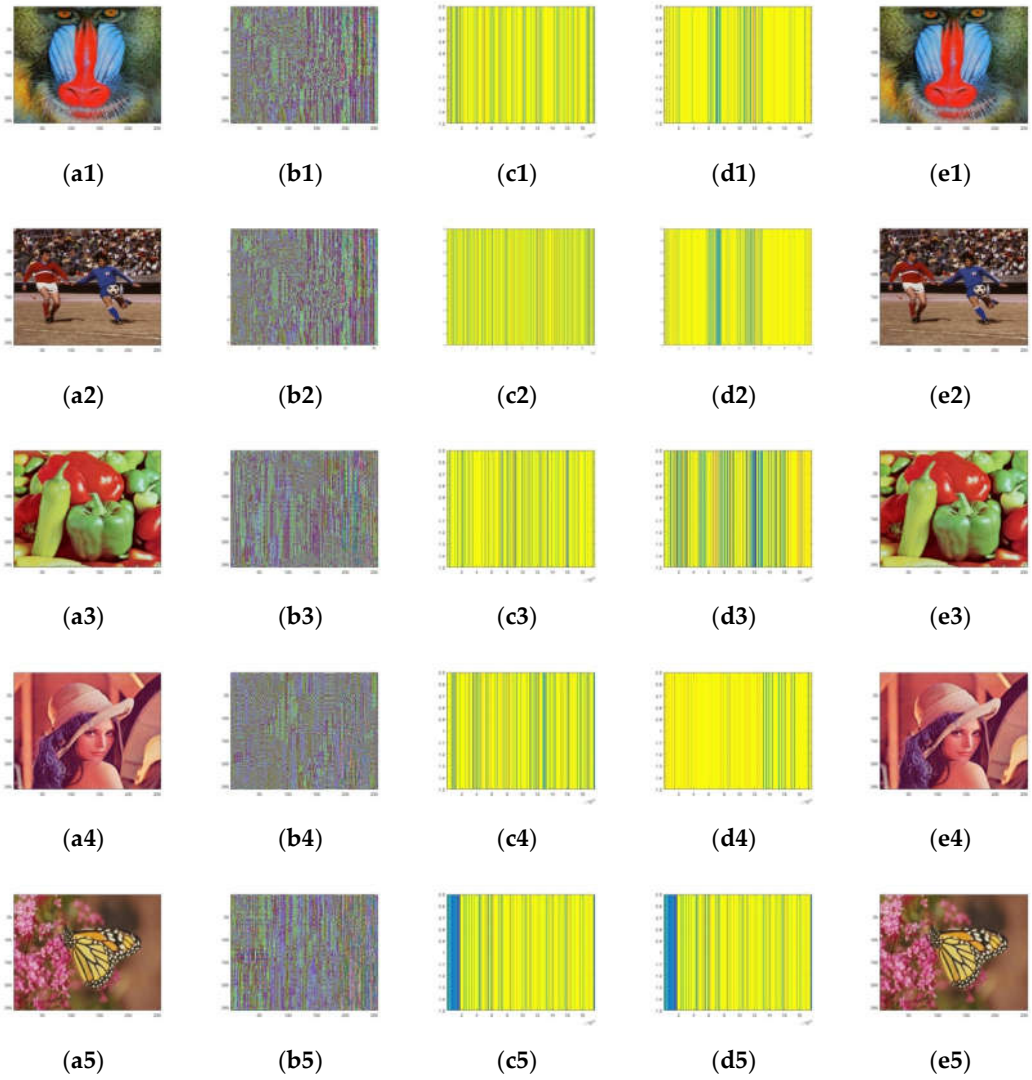


Figure 3. Images from Column 1 to Column 5 are original images, cipher images, retrieved permutation-diffusion images, retrieved permutation-only images, restored images.

The running times of the proposed scheme and Chen's scheme in terms of attacking *lp* and diffusion and attacking permutation are shown in Table 2. The images are chosen in different sizes including 256×256, 512×512 and 1024×1024. From Table 2, the average running time of attacking the amount of *lp* and diffusion in two schemes is almost the same. But the average running time of attacking permutation in the proposed method is less than that in Chen's scheme. The total average running time of the proposed method attacking the encrypted images of size 256×256 is 3.9151 s which is 1.33 s less than that of Chen's scheme. The difference values of attacking the encrypted the images with size 512×512 and 1024×1024 are about 2.80 s and 18.2 s, respectively. Therefore, the cryptanalysis speed of the proposed method is better than the existing scheme.

Table 2. Execution time (seconds).

Image Size	Image	The Proposed Scheme	Chen's Scheme

		Attack *lp* and Diffusion	Attack Permutation	Total Time	Attack *lp* and Diffusion	Attack Permutation	Total time
256 × 256	Lena	1.2386	2.7358	3.9744	1.2173	3.8253	5.0426
	Baboon	1.0537	2.8356	3.8893	1.1562	3.9376	5.0938
	Pepper	0.9697	2.9121	3.8818	1.0127	4.5862	5.5989
Average time		1.0873	2.8278	3.9151	1.1287	4.1164	5.2451
512 × 512	Lena	1.5413	10.0327	11.574	1.7135	13.7236	15.4371
	Baboon	1.6331	11.7731	13.4062	1.5233	13.1027	14.626
	Pepper	1.6975	10.9173	12.6148	1.5872	14.3379	15.9251
Average time		1.6240	10.9077	12.5317	1.6080	13.7214	15.3294
1024 × 1024	Lena	2.5136	32.4377	34.9513	2.4759	47.7536	50.2295
	Baboon	2.7572	35.7728	38.53	2.8364	58.5927	61.4291
	Pepper	2.6673	39.8154	42.4827	2.6581	56.3619	59.02
Average time		2.6460	36.0086	38.6546	2.6568	54.2361	56.8929

5. Conclusions

This paper attacks a new color image encryption algorithm combining a few the 1D chaotic maps which has been recently proposed in [37]. The encryption process depends on the linear-nonlinear-linear structure of the encryption algorithm. The vulnerability of this algorithm is revealed, and the attacking scheme is developed by the chosen plaintext attack in Section 3, based on the security weakness. Experimental results demonstrate the attack scheme of this paper can completely collapse the encryption algorithm and has low computation complexity.

Author Contributions: Conceptualization, M.L.; Methodology, M.L. and Y.D.; Software, Y.D.; Validation, Y.D.; Formal Analysis, Y.D.; Investigation, M.L. and Y.D.; Writing—Original Draft Preparation, Y.D.; Writing—Review and Editing, M.L. and Y.D.; Visualization, Y.D.; Supervision, M.L.; Funding Acquisition, M.L. and Y.D.

Funding:

Acknowledgments: This research was funded by the National Natural Science Foundation of China by the Ph.D Scientific Research Foundation of Henan Normal University (Grant no. qd18027) and the National Natural Science Foundation of China (Grant no. 61602158).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang, Y.S.; Xiao, D.; Shu, Y.L.; Li, J. A novel image encryption scheme based on a linearhyperbolic chaotic sys-tem of partial differential equations. *Signal Process. Image Commun.* **2013**, *28*, 292–300.
2. Zhang, Y.S.; Xiao, D. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Opt. Lasers Eng.* **2013**, *51*, 472–480.
3. Ye, G.D.; Wong, K.W. An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear Dyn.* **2012**, *69*, 2079–2087.
4. Mirzaei, O.; Yaghoobi, M.; Irani, H. A new image encryption method: Parallel sub-image encryption with hyperchaos. *Nonlinear Dyn.* **2011**, *67*, 557–566.
5. Liu, Y.B.; Tian, S.M.; Hu, W.P.; Xing, C.C. Design and statistical analysis of a new chaotic block cipher for wireless sensor networks. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 3267–3278.
6. Wong, K.W.; Kwok, B.; Law, W. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **2008**, *372*, 2645–2652.
7. Norouzi, B.; Mirzakuchaki, S.; Seyedzadeh, S.M.; Mosavi, M.R. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimed. Tools Appl.* **2014**, *71*, 1469–1497.
8. Kassem, A.; Hassan, H.A.H.; Harkouss, Y.; Assaf, R. Efficient neural chaotic generator for image encryption. *Digit. Signal Process.* **2014**, *25*, 266–274.
9. Arroyo, D.; Diaz, J.; Rodriguez, F.B. Cryptanalysis of a one round chaos-based substitution permutation

network. *Signal Process.* **2013**, *67*, 1358–1364.
10. Zhang, Y.; Xiao, D. Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack. *Nonlinear Dyn.* **2013**, *72*, 751–756.
11. Zhang, Y.; Li, C.; Li, Q.; Zhang, D.; Shu, S. Breaking a chaotic image encryption algorithm based on perceptron model. *Nonlinear Dyn.* **2012**, *69*, 1091–1096.
12. Zhang, Y.; Xiao, D.; Wen, W.; Li, M. Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Nonlinear Dyn.* **2014**, *76*, 1645–1650.
13. Su, M.; Wen, W.; Zhang, Y. Security evaluation of bilateral-diffusion based image encryption algorithm. *Nonlinear Dyn.* **2014**, *77*, 243–246.
14. Zhang, Y.; Xiao, D.; Wen, W.; Li, M. Cryptanalyzing a novel image cipher based on mixed transformed logistic maps. *Multimed. Tools Appl.* **2014**, *73*, 1885–1896.
15. Jain, A.; Rajpal, N. A robust image encrytion algorithm resistant to attacks using DNA and chaotic logistic maps. *Mutitimed. Tools Appl.* **2016**, *75*, 5455–5472.
16. Ye, G.; Pan, C.; Huang, X.; Zhao, Z.; He, J. A chaotic image encryption algorithm based on information entropy. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850010.
17. Dou, Y.; Liu, X.; Fan, H.; Li, M. Cryptanalysis of a DNA and chaotic logistic maps based image encryption algorithm. *OPTIK* **2017**, *145*, 456–464.
18. Li C , Lin D , Feng B , et al. Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy[J]. IEEE Access, **2018**:75834-75842..
19. Panduranga, H.T.; Kumar, S.N. Image encryption based on permutation-substitution using chaotic map and latin square image cipher. *Eur. Phys. J. Spec. Top.* **2014**, *223*, 1663–1677.
20. Machkour, M.; Saaidi, A.; Benmaati, M. A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher. *3D Res.* **2015**, *6*, 1–18.
21. Chapaneri, S., Chapaneri, R.: Chaos based image encryption using latin rectangle scrambling. In: 2014 annual IEEE India conference (INDICON), pp. 1–6. IEEE (**2014**)
22. Hu, G.; Xiao, D.; Wang, Y.; Li, X. Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion. *Nonlinear Dyn.* **2017**, *88*, 1305–1316.
23. Ge, X.; Lu, B.; Liu, F.; Luo, X. Cryptanalyzing an image encryption algorithm with compound chaotic stream cipher based on perturbation. *Nonlinear Dyn.* **2017**, *90*, 1141–1150.
24. Lin, J.; Wang, Z. Image block encryption algorithm based on chaotic maps. *IET Signal Process.* **2017**, *12*, 22–30.
25. Ma, Y.; Li, C. Cryptanalysis of an Image Block Encryption Algorithm Based on Chaotic Maps. *J. Inf. Secur. Appl.* arXiv, **2019**, arXiv:1912.12915.
26. Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process*. **2019**, *155*, 44–62.
27. Zhu, C.X.; Wang, G.J.; Sun, K.H. Improved cryptanalysis and enhancements of an image encryption scheme us in combined 1D chaotic maps. *Entropy* **2018**, *20*, 843.
28. Wang, M.X.; Wang, X.Y.; Zhang, Y.Q.; Gao, Z.G. A novel chaotic encryption scheme based on image segmentation an multiple diffusion models. *Opt. Laser Tecnnol.* **2018**, *108*, 558–573.
29. Hua, Z.; Yi, S.; Zhou, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **2018**, *144*, 134–144.
30. Belazi, A., Abd Ellatif, A.A., Belghith, S.: A novel image encryption scheme based on substitution–permutation network and chaos. Signal Process. **2016**, 128, 155–170
31. Chen, J.X.; Zhu, Z.L.; Fu, C.; Zhang, L.B.; Zhang, Y.S. An efficient image encryption scheme using lookup table-base confusion and diffusion. *Nonlinear Dyn.* **2015**, *81*, 1151–1166.
32. Belazi, A.; Abd Ellatif, A.A.; Belghith, S. A novel image encryption scheme based on substitution–permutation network and chaos. *Signal Process.* **2016**, *128*, 155–170.
33. Li, M.; Lu, D.; Xiang, Y.; Zhang, Y.; Ren, H. Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion. *Nonlinear Dyn.* **2019**, *96*, 31–47.
34. Zhou, Y.; Bao, L.; Chen, C.L.P. A new 1d chaotic system for image encryption. *Signal Process.* **2014**, *97*, 172–182.
35. Wen, W.; Zhang, Y.; Fang, Z.; Chen, J.X. Infrared target-based selective encryption by chaotic maps. *Opt. Commun.* **2015**, *341*, 131–139.
36. Lv-Chen, C.; Yu-Ling, L.; Sen-Hui, Q.; Jun-Xiu, L. A perturbation method to the tent map based on

Lyapunov exponent and its application. *Chin. Phys. B* **2015**, *24*, 78–85.
37. Pak, C.; Huang, L. A new color image encryption using combination of the 1D chaotic map. *Signal Process.* **2017**, *138*, 129–137.
38. Wang, H.; Xiao, D.; Chen, X.; Huang, H. cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. *Signal Process.* **2018**, *144*, 444–452.
39. Li, C.; Lo, K.T. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process.* **2011**, *91*, 949–954.
40. Zhang, L.Y.; Liu, Y.; Wang, C.; Zhou, J.; Zhang, Y.; Chen, G. Improved known-plaintext attack to permutation-only multimedia ciphers. *Inf. Sci.* **2018**, *430*, 228–239.