Engineering Science and Technology, an International Journal 51 (2024) 101634

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch

Full length article

Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps

Heping Wen *, Yiting Lin, Zhaoyang Feng

University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

ARTICLE INFO

Keywords:
Image encryption
Cryptanalysis
Image privacy
Multimedia security
Chaos

ABSTRACT

Recently, a bit-level image encryption algorithm based on chaotic maps (BCIEA) has been presented. BCIEA consists of diffusion and confusion, and its security performance mainly relies on the dynamic mechanisms introduced during diffusion and confusion, respectively. However, after a careful cryptanalysis, we found that BCIEA has fatal security issues. Although the bit-level diffusion formally employs complex chaining operations, there is a defect that the chaotic sequences can be used as an equivalent key. In addition, by analyzing its confusion, it is found that the dynamic mechanism adopted has obvious statistical characteristics, and it is especially difficult to resist all zero ciphertext attack. In addition, we also found that the BCIEA description is not rigorous, resulting in algorithm details that cannot be decrypted. On the basis of slightly reasonable modification, we propose a chosen-ciphertext attack method for cracking BCIEA. The method first uses the all-zero ciphertext to degrade it into a diffusion-only algorithm, and then chooses a cipher image with the same sum value as that of the target cipher image to break the confusion module possessing a dynamic mechanism. Theoretical analyses and experimental results verify the effectiveness and efficiency of the proposed attack method. This work can provide a reference for improving the security of image encryption schemes based on bit-level techniques.

1. Introduction

Nowadays, with the continuous rapid development of network communication technology, the security of storage and transmission of multimedia information, especially images and video, is becoming more and more interesting [1–3]. The image has the characteristics of strong correlation and high redundancy of adjacent pixels, thus the traditional cryptographic algorithms, such as AES, DES and IDEA, are not suitable [4–6]. To cope with this challenge, many different methodologies have been studied for exploiting various image encryption schemes [7–9]. For example, quantum cryptography [10–12], thumbnail-preserving encryption [13–15], biological coding [16–18], discrete memristive [19–21], frequency domain encryption [22–24], bit-level encryption [25–27], fourier transform [28–30], chaos theory [31–33], and so on [34,35]. In particular, the application of chaos in image encryption algorithms is popular due to its inherent unpredictability, pseudo-randomness, and sensitivity to initial values [36–38]. However, due to the lack of authoritative metrics, the security of these cryptographic algorithms is still worth exploring and researching [39,40].

In recent years, to improve the granularity of spatial image encryption, researchers have paid more and more attention [41–43] to transforming the basic information processing unit from pixel to bit and DNA to obtain better coding encryption effect [44–46]. In 2022, Chen et al. analyzed the medical privacy protection scheme based on chaos and DNA coding [47], and pointed out that the equivalent key can be obtained based on the chosen-plaintext attack. In 2023, Wen et al. performed a cryptanalysis [48] on QCMDC-IEA and found that the equivalent permutation key was first obtained by differential cryptanalysis, and then only four chosen plain images and their corresponding cipher images were enough for breaking its DNA domain encryption. In the same year, Wen et al. reassessed the security of CIEA-IOCM [49] and presented that it can be completely cracked by chosen-plaintext attack. These cryptanalysis works prove that the related target image encryption algorithm has security defects, and there is no theoretically provable security. In fact, compared with image encryption design, the corresponding cryptanalysis work is extremely lacking. Therefore, it is extremely necessary to implement a comprehensive cryptanalysis of various image encryption algorithms [50].

In 2016, Lu et al. [51] proposed a bit-level image encryption algorithm based on chaotic maps named BCIEA, and claimed that it is sufficiently secure owing to the statistically numerical analysis results. BCIEA consists of diffusion and confusion, and its security performance mainly relies on the dynamic mechanisms introduced during diffusion

* Corresponding author at: University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China.
E-mail addresses: wenheping@uestc.edu.cn (H. Wen), Dr.YitingLin@gmail.com (Y. Lin), 202102021045@stu.zsc.edu.cn (Z. Feng).

https://doi.org/10.1016/j.jestch.2024.101634
Received 12 June 2023; Received in revised form 5 January 2024; Accepted 27 January 2024
Available online 12 February 2024

and confusion, respectively. However, after a careful cryptanalysis, we found that BCIEA has fatal security issues. Although the bit-level diffusion formally employs complex chaining operations, there is a defect that the chaotic sequences can be used as an equivalent key. In addition, by analyzing its confusion, it is found that the dynamic mechanism adopted has obvious statistical characteristics, and it is especially difficult to resist all zero ciphertext attack. In addition, we also found that the BCIEA description is not rigorous, resulting in algorithm details that cannot be decrypted. On the basis of slightly reasonable modification, we propose a chosen-ciphertext attack method for cracking BCIEA. The method first uses the all-zero ciphertext to degrade it into a diffusion-only algorithm, and then chooses a cipher image with the same sum value as that of the target cipher image to break the confusion module possessing a dynamic mechanism. Theoretical analyses and experimental results verify the effectiveness and efficiency of the proposed attack method.

The rest of the paper is organized as follows: Section 2 repeats the target image cryptosystem; Section 3 discuss the decryption of BCIEA; Section 4 presents a cryptanalysis; Section 5 gives the experimental results; The last section concludes the paper.

2. The cryptosystem under study

This section firstly presents a bit-level technique and the adopted chaotic map, and then introduces BCIEA briefly.

2.1. A bit-level technique

As [52], binary bitplane decomposition (BBD) is one of three bitplane decomposition technologies. Also, BBD is adopted in BCIEA for decomposing a grayscale image $\boldsymbol{P}$ into 8 binary bitplanes, given as

$$\boldsymbol{P} = \sum_{n=1}^{8} 2^{n-1}\boldsymbol{p}_n = \boldsymbol{p}_1 + 2\boldsymbol{p}_2 + 2^2\boldsymbol{p}_3 + \cdots + 2^7\boldsymbol{p}_8 \tag{1}$$

where $\boldsymbol{P} \in \mathbb{Z}_{256}$, and $\boldsymbol{p}_n \in \mathbb{Z}_2$. Conversely, binary bitplane composition (BBC) combines 8 bit planes into one grayscale image.

2.2. The adopted chaotic map

In BCIEA, a chaotic map is used twice to generate several keystreams for encryption. The piece-wise linear chaotic map (PWLCM) is mathematically modeled by

$$x_i = F(x_{i-1}, \eta) = \begin{cases} x_{i-1}/\eta, & 0 < x_{i-1} < \eta \\ (x_{i-1} - \eta)/(0.5 - \eta), & \eta \le x_{i-1} < 0.5 \\ F(1 - x_{i-1}, \eta), & 0.5 \le x_{i-1} < 1 \end{cases} \tag{2}$$

where x is the state variable, $x_0 \in (0, 1)$ is the initial value and $\eta \in (0, 0.5)$ is the control parameter, respectively.

2.3. Description of BCIEA

The block diagram of the encryption process of BCIEA is shown in Fig. 1. As can be seen, the main components of BCIEA are introduced briefly as follows:

- *The Secret Key*:
  In BCIEA, two different groups of initial values and control parameters $(x_0, \eta_1, y_0, \eta_2)$ are served as the secret keys.
- *Initialization*:
  With the initial parameter η_1 and the initial value x_0, get a sequence $\boldsymbol{X}_1$ by iterating Eq. (2) for $N_0 + MN$ times and discard the former N_0 values, given as

  $$X_1(i) = \mathrm{mod}(floor(x(i)) \times 10^{14}, 256)$$

  where $i = 1 \sim MN$, $floor$ is the function that takes an integer, and $X_1(i) \in \mathbb{Z}_{256}$. Then, two sequences $\boldsymbol{b}_1, \boldsymbol{b}_2$ of length L are obtained from $\boldsymbol{X}_1$ by the method of binary bitplane decomposition. Here, $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \mathbb{Z}_2$.
- *Pre-processing*:
  For the sake of generality, the encrypted object is an 8-bit grayscale image of size $\boldsymbol{P}$ of size $M \times N$ (height × width). Convert the plain image $\boldsymbol{P}$ of size $M \times N$ (height × width) into two 1D sequences $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$ of length $4MN$. For convenience, let L be $4MN$.
- *Stage 1. Diffusion*:
  Step 1. Firstly calculate the sum of $\boldsymbol{A}_2$, represented as

  $$sum_1 = \sum_{i=1}^{L} A_2(i) \tag{3}$$

  Then run a cyclic right shift operation on $\boldsymbol{A}_1$ with sum_1 bits to obtain $\boldsymbol{A}_{11}$.
  Step 2. Get $\boldsymbol{B}_1$ by performing the bitwise XOR operations between $\boldsymbol{A}_{11}$, $\boldsymbol{A}_2$ and $\boldsymbol{b}_1$:

  $$\begin{cases} B_1(1) = A_{11}(1) \oplus A_{11}(L) \oplus A_2(1) \oplus b_1(1) \\ B_1(i) = A_{11}(i) \oplus A_{11}(i-1) \oplus A_2(i) \oplus b_1(i) \end{cases} \tag{4}$$

  where $i = 2 \sim L$.
  Step 3. Like Step 1, firstly compute the sum values sum_2 of $\boldsymbol{B}_1$:

  $$sum_2 = \sum_{i=1}^{L} B_1(i) \tag{5}$$

  Then, get $\boldsymbol{A}_{22}$ cyclic right shifting $\boldsymbol{A}_2$ with sum_2 bits.
  Step 4. Similar to Step 2, obtain $\boldsymbol{B}_2$ from $\boldsymbol{A}_{22}$, $\boldsymbol{B}_1$ and $\boldsymbol{b}_2$, modeled by

  $$\begin{cases} B_2(1) = A_{22}(1) \oplus A_{22}(L) \oplus B_1(1) \oplus b_2(1) \\ B_2(i) = A_{22}(i) \oplus A_{22}(i-1) \oplus B_1(i) \oplus b_2(i) \end{cases} \tag{6}$$

  where $i = 2 \sim L$.
- *Stage 2. Confusion*:
  Step 1. Compute the sum values of $\boldsymbol{B}_1$ and $\boldsymbol{B}_1$ by

  $$sum = \sum_{i=1}^{L} (B_1(i) + B_2(i)) \tag{7}$$

  Further update the initial value of the chaotic map by

  $$s_0 = \mathrm{mod}(y_0 + sum/L, 1) \tag{8}$$

  Then, with the initial parameter η_2 and the initial value s_0, using Eq. (2) again, generate a chaotic sequence of length $2L$, and then process it into two integer sequences $\boldsymbol{Y}$ and $\boldsymbol{Z}$ both of length L. Here, $\boldsymbol{Y}, \boldsymbol{Z} \in [1, L]$.
  Step 2. Use $\boldsymbol{Y}$ and $\boldsymbol{Z}$ as coordinate indexes, and then get $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ by confusing the positions of the elements in $\boldsymbol{B}_2$ and $\boldsymbol{B}_1$ respectively. Exactly, given as

  $$\begin{cases} C_1(i) = B_2(Y(i)) \\ C_2(i) = B_1(Z(i)) \end{cases} \tag{9}$$

  where $i = 1 \sim L$.
- *Post-processing*:
  Finally, get the cipher image $\boldsymbol{C}$ from $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ by the method of BBC.

As stated in [51], the decryption process is the inverse of the encryption process. For more details, please refer to [51].

3. On the decryption of BCIEA

3.1. Problems with the decryption

As everyone knows, ensuring the decryption is available is a basic condition for good cryptosystems. In addition, decryption is an integral part of cryptanalysis. For this reason, we discuss the decryption part firstly. The block diagram of the decryption process of BCIEA is shown in Fig. 2.

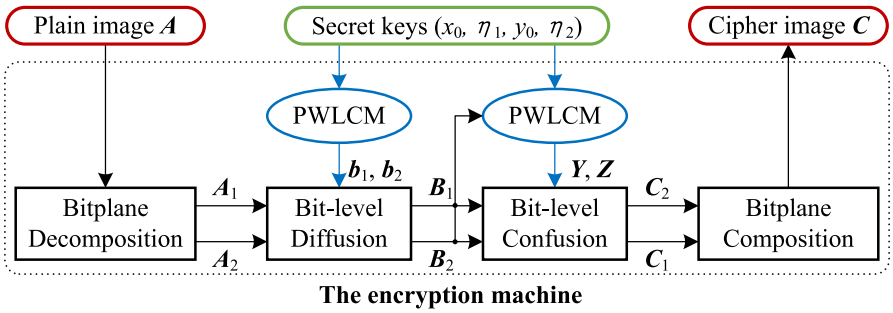


Fig. 1. The block diagram for the encryption process of BCIEA.

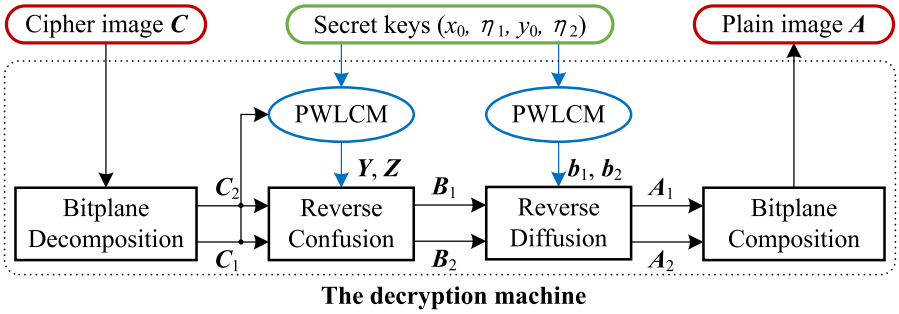


Fig. 2. The block diagram for the decryption process of BCIEA.

- *Initialization*:
  As with encryption, generate the keystreams $\boldsymbol{b}_1, \boldsymbol{b}_2$ by the secret keys (η_1, x_0).
- *Pre-processing*:
  Get $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ from the cipher image $\boldsymbol{C}$ by BBD.
- *Stage 1. Anti-confusion*:
  Step 1. Compute the sum values of $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ by

$$sum = \sum_{i=1}^{L} (C_1(i) + C_2(i)) \tag{10}$$

  Note that the sum of $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ is equal to the sum of $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ because the confusion only changes the positions of the elements. Then, with the same secret keys (η_2, y_0), update the initial value y_0 to s_0 and further obtain the two coordinate indexes sequences $\boldsymbol{Y}$ and $\boldsymbol{Z}$.
  Step 2. Restore $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ from $\boldsymbol{C}_2$ and $\boldsymbol{C}_1$ by the reverse confusion:

$$\begin{cases} B_1(Z(i)) = C_2(i) \\ B_2(Y(i)) = C_1(i) \end{cases} \tag{11}$$

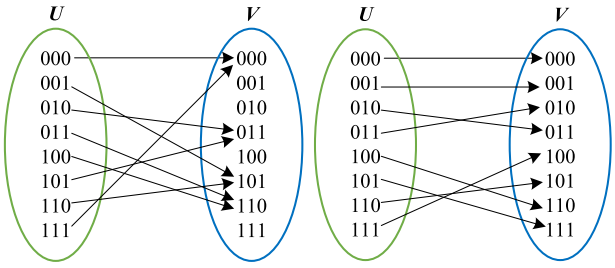
  where $i = 1 \sim L$.
- *Stage 2. Anti-diffusion*:
  Step 1. Corresponding to Step 4 of the confusion, recover $\boldsymbol{A}_{22}$ from $\boldsymbol{B}_2$, $\boldsymbol{B}_1$ and $\boldsymbol{b}_2$, modeled by

$$\begin{cases} A_{22}(1) \oplus A_{22}(L) = B_2(1) \oplus B_1(1) \oplus b_2(1) \\ A_{22}(i) \oplus A_{22}(i-1) = B_2(i) \oplus B_1(i) \oplus b_2(i) \end{cases} \tag{12}$$

  where $i = 2 \sim L$.
  Step 2. Obtain sum_2 from Eq. (5), and then get $\boldsymbol{A}_2$ by doing cyclic left shift operation on $\boldsymbol{A}_{22}$ with sum_2 bits.
  Step 3. Recover $\boldsymbol{A}_{11}$ by performing the bitwise XOR operations between $\boldsymbol{B}_1$, $\boldsymbol{A}_2$ and $\boldsymbol{b}_1$:

$$\begin{cases} A_{11}(1) \oplus A_{11}(L) = B_1(1) \oplus A_2(1) \oplus b_1(1) \\ A_{11}(i) \oplus A_{11}(i-1) = B_1(i) \oplus A_2(i) \oplus b_1(i) \end{cases} \tag{13}$$

  where $i = 2 \sim L$.
  Step 4. Obtain sum_1 from Eq. (3), and then get $\boldsymbol{A}_1$ by doing cyclic left shift operation on $\boldsymbol{A}_{11}$ with sum_1 bits.



(a) Neither injection nor surjection (b) Both injection and surjection

Fig. 3. The illustration diagram of two examples about injection and surjection in BCIEA with $L = 3$.

- *Post-processing*:
  Finally, get the plain image $\boldsymbol{A}$ from $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$ by the method of BBC.

Observing Eq. (12) and (13), the decryption results are the bitwise XOR values of two elements, instead of the values of an element. In fact, this paradigm will lead to solutions that are not unique. To this end, the following proof is given from the perspective of algebraic analysis.

Take Eq. (12) as an example, let $u(i) = A_{22}(1)$, $v(i) = B_2(i) \oplus B_1(i) \oplus b_2(i)$. Thus, Eq. (12) becomes

$$\begin{cases} u(1) \oplus u(L) = v(1) \\ u(i) \oplus u(i-1) = v(i) \end{cases} \tag{14}$$

where $i = 2 \sim L$, $u(i), v(i) \in \mathbb{Z}_2$. Here, $\boldsymbol{u}$ is known, and $\boldsymbol{v}$ is to be determined. One can conclude that $\boldsymbol{u}$ has two solutions regardless of the value of $\boldsymbol{v}$ due to the symmetry of two unknowns in this equation.

For example, given $L = 3$, one has $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{U}$. The mapping process is shown in Fig. 3(a). $\boldsymbol{v}$ = "101" is known. Then, both "110" and "001" are solutions of $\boldsymbol{u}$ in Eq. (14).

Obviously, this violates the condition that the encryption and decryption functions required by the cryptosystem are single shot.

3.2. A slight correction on the decryption

To ensure correct decryption, and refer to other similar algorithm designs [53], a reasonable correction is to remove $A_{11}(L)$, $A_{22}(L)$ to meet both injection and surjection. Thus, similarly given $L = 3$, the mapping process is shown in Fig. 3(b). Then, without changing the idea of the algorithm, the equations of encryption do not need to be modified, except for their first equation of Eqs. (4) and (6). Exactly, revised as

$$B_1(1) = A_{11}(1) \oplus A_2(1) \oplus b_1(1) \tag{15}$$

and

$$B_2(1) = A_{22}(1) \oplus B_1(1) \oplus b_2(1) \tag{16}$$

respectively. Accordingly in the decryption, the first equation of Eqs. (12) and (13) become

$$A_{22}(1) = B_2(1) \oplus B_1(1) \oplus b_2(1) \tag{17}$$

and

$$A_{11}(1) = B_1(1) \oplus A_2(1) \oplus b_1(1) \tag{18}$$

This ensures the correctness of the decryption.

4. Cryptanalysis

For the adversary, the goal is to restore the acquired cipher images to the original plain images. A common way is to get its real or equivalent key. In BCIEA, the secret keys are $(x_0, \eta_1, y_0, \eta_2, A_{11}(0), A_{22}(0))$ based on the correction for the decryption given in Section 3.2. In fact, it is very hard to determine $(x_0, \eta_1, y_0, \eta_2)$, or even impossible, because the preprocess operation as shown in Eq. (1) is used. To deal with the challenge, we turn our goal to get their equivalent keys, exactly $(\boldsymbol{b}_1, \boldsymbol{b}_2, A_{11}(0), A_{22}(0))$ for diffusion and $(\boldsymbol{Y}, \boldsymbol{Z})$ for confusion respectively.

4.1. Analysis on the diffusion part

The generation process of the two diffusion sequences $\boldsymbol{b}_1, \boldsymbol{b}_2$ are independent of the plain images. Also, $A_{11}(0)$ and $A_{22}(0)$ are not related to plain images. Thus, $(\boldsymbol{b}_1, \boldsymbol{b}_2, A_{11}(0), A_{22}(0))$ can be considered as a permanent equivalent key of the diffusion under a given secret key.

Based on chosen-ciphertext attack, one can choose the all-zero cipher image $\boldsymbol{C}^{(0)}$ and get its corresponding plain image $\boldsymbol{A}^{(0)}$. Then, one gets $\boldsymbol{B}_1^{(0)} = 0$ and $\boldsymbol{B}_2^{(0)} = 0$ because the confusion does not change the element value. Also, $\boldsymbol{A}_1^{(0)}$ and $\boldsymbol{A}_2^{(0)}$ are also known according to the basic assumption of the cipher is public. At this point, the original algorithm is actually a diffusion-only process. Thus, Eq. (12) becomes

$$\begin{aligned} A_{22}^{(0)}(1) &= A_{22}(0) \oplus B_2^{(0)}(1) \oplus B_1^{(0)}(1) \oplus b_2(1) \\ &= A_{22}(0) \oplus b_2(1) \end{aligned} \tag{19}$$

$$\begin{aligned} A_{22}^{(0)}(i) &= A_{22}^{(0)}(i-1) \oplus B_2^{(0)}(i) \oplus B_1^{(0)}(i) \oplus b_2(i) \\ &= A_{22}^{(0)}(i-1) \oplus b_2(i) \end{aligned} \tag{20}$$

where $i = 2 \sim L$. Here, one has $sum_2 = 0$ because $\boldsymbol{B}_1^{(0)} = 0$. Thus, $\boldsymbol{A}_2^{(0)} = \boldsymbol{A}_{22}^{(0)}$. Moreover, $A_{22}(0)$ is fixed for a given key. Let $\hat{b}_2(1) = A_{22}(0) \oplus b_2(1)$, Eq. (19) evolves to

$$\hat{b}_2(1) = A_{22}(0) \oplus b_2(1) = A_{22}^{(0)}(1) \tag{21}$$

And Eq. (20) evolves to

$$b_2(i) = A_{22}^{(0)}(i) \oplus A_{22}^{(0)}(i-1) \tag{22}$$

where $i = 2 \sim L$. Thus, one can determine the result of $A_{22}(0) \oplus b_2(1)$, namely $\hat{b}_2(1)$, and $b_2(i)$ for $i = 2 \sim L$. Note that $A_{22}(0)$ and $b_2(1)$ always appear in pairs, so there is no need to ask for specific $A_{22}(0)$ and $b_2(1)$. Here, let $\hat{\boldsymbol{b}}_2$ be a sequence identical to $\boldsymbol{b}_2$ except that only the first element is different, exactly is $\hat{b}_2(1) = A_{22}(0) \oplus b_2(1)$.

Secondly, one gets $\boldsymbol{A}_{11}^{(0)}$ from $\boldsymbol{A}_1^{(0)}$ by doing cyclic right shift with sum_1 bits. Here, sum_1 associated with $\boldsymbol{A}_2^{(0)}$ and $\boldsymbol{A}_1^{(0)}$ are both known, thus $\boldsymbol{A}_{11}^{(0)}$ is determined. Further, similarly following Eq. (18).

Let $\hat{b}_1(1) = A_{11}(0) \oplus b_1(1)$, one has

$$\hat{b}_1(1) = A_{11}^{(0)}(1) \oplus A_2^{(0)}(1) \tag{23}$$

When $i = 2 \sim L$, one has

$$b_1(i) = A_{11}^{(0)}(i) \oplus A_{11}^{(0)}(i-1) \tag{24}$$

Similarly, let $\hat{\boldsymbol{b}}_1$ be a sequence identical to $\boldsymbol{b}_1$ except that only the first element is different, exactly is $\hat{b}_1(1) = A_{11}(0) \oplus b_1(1)$.

Consequently, another equivalent key $\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2$ are determined. They can be used to eliminate the diffusion part for any given images. This also laid the foundation for the entire cryptanalysis. As a result, these two sequences are different for different plaintext or ciphertext.

4.2. Analysis on the confusion part

Once the diffusion can be eliminated, BCIEA degenerates into a permutation-only algorithm. Referring to existing research, many permutation-only encryption algorithms are unable to defend against known-plaintext attacks and chosen-plaintext attacks. However, the objects deciphered in these studies are static replacement processes that are unrelated to plaintext. These analytical methods may not be directly applicable.

Unlike the diffusion part, the confusion keystreams $\boldsymbol{Y}, \boldsymbol{Z}$ are dynamic for the different plain or cipher images because of Eqs. (8) and (10). Thus, there is no permanent equivalent key for the confusion. Nevertheless, by observing Eqs. (8) and (10), one can see that this dynamic attribute also has certain rules. More, according to the given ciphertext, the sum value can be obtained, thereby providing a basis for selecting the ciphertext. This is also an important reason for adopting chosen-ciphertext attack.

The purpose of the attacker is to restore the original information of the target ciphertext. By Eq. (10), the value of *sum* for the target cipher image $\boldsymbol{C}$ can be calculated. Thus, the diffusion sequences $\boldsymbol{Y}$ and $\boldsymbol{Z}$ are identical under the premise of selecting ciphertexts having the same sum value.

For a simple example, given $L = 8$ and $\boldsymbol{Y} = (8, 4, 5, 7, 2, 1, 6, 3)$. One can choose the cipher images as

$$\begin{cases} \boldsymbol{C}_1^{(1)} = (0, 1, 0, 1, 0, 1, 0, 1) \\ \boldsymbol{C}_1^{(2)} = (0, 0, 1, 1, 0, 0, 1, 1) \\ \boldsymbol{C}_1^{(3)} = (0, 0, 0, 0, 1, 1, 1, 1) \end{cases} \tag{25}$$

Simultaneously, construct the other part $\boldsymbol{C}_2^{(1)}, \boldsymbol{C}_2^{(2)}, \boldsymbol{C}_2^{(3)}$ so that the sum of the chosen cipher images are all *sum*. Thus, one of the forms is

$$\begin{cases} \boldsymbol{C}_2^{(1)} = (1, 1, 1, 1, 1, 0, 0, 0) \\ \boldsymbol{C}_2^{(2)} = (1, 1, 1, 1, 1, 0, 0, 0) \\ \boldsymbol{C}_2^{(3)} = (1, 1, 1, 1, 1, 0, 0, 0) \end{cases} \tag{26}$$

Correspondingly, one gets $\boldsymbol{B}_2$ by performing anti-confusion on $\boldsymbol{C}_1$, given by

$$\begin{cases} \boldsymbol{B}_2^{(1)} = (1, 1, 0, 0, 1, 0, 1, 0) \\ \boldsymbol{B}_2^{(2)} = (1, 1, 0, 1, 0, 0, 0, 1) \\ \boldsymbol{B}_2^{(3)} = (1, 0, 1, 1, 0, 0, 1, 0) \end{cases} \tag{27}$$

In the confusion, the elements of $\boldsymbol{B}_1$ are only replaced by $\boldsymbol{C}_2$, and the elements of $\boldsymbol{B}_2$ are only replaced by $\boldsymbol{C}_1$. Thus, one can get the confusion sequence $\boldsymbol{Y}$ by comparing all the elements in Eqs. (25) and (27).

Similarly, the cipher images are constructed by exchanging $\boldsymbol{C}_1$ in Eq. (25) and $\boldsymbol{C}_2$ in Eq. (26), thus the above method can be used to find the confusion sequence $\boldsymbol{Z}$.

Algorithm 1: The method of constructing some chosen cipher images for breaking the confusion.

Input: The value *sum* of a target encrypted image $\hat{\boldsymbol{C}}$
Output: Two groups of chosen cipher images $\{\boldsymbol{C}_n\}_{n=1}^{N}$ and $\{\boldsymbol{C}'_n\}_{n=1}^{N}$
Step 1. Let $\boldsymbol{C}_1^V$ be a sequence $(0, 1, 2, ..., L-1)$ with the length of L;
Step 2. Construct N sequences $\boldsymbol{C}_1^n$ for $n = 1 \sim N$ by a decomposition: $\boldsymbol{C}_1^V \rightarrow \sum_{n=1}^{N} 2^{n-1}\boldsymbol{C}_1^n$, where $N = \lceil \log_2(L) \rceil$;
Step 3. Construct the other N sequences $\boldsymbol{C}_2^n$ for $n = 1 \sim N$ in which just $\sum_{i=1}^{L}(C_1^n(i) + C_2^n(i)) \equiv sum$ holds;
Step 4. Obtain N chosen cipher images $\boldsymbol{C}^n$ by BBC with $\boldsymbol{C}_1^n$ and $\boldsymbol{C}_2^n$ for $n = 1 \sim N$ respectively;
Step 5. Get the other N chosen cipher images $\boldsymbol{C}'^n$ by swapping $\boldsymbol{C}_1^n$ and $\boldsymbol{C}_2^n$ as Step 4;
return $\boldsymbol{C}^n$ and $\boldsymbol{C}'^{(n)}$ for $n = 1 \sim N$;

4.3. The proposed attack method

Based on the above, the diffusion and the confusion of BCIEA cannot resist a chosen-ciphertext attack method. Thus, for a given cipher image $\hat{\boldsymbol{C}}$, the specific steps for breaking BCIEA by chosen-ciphertext attack is given as follows:

- Step 1. Based on the condition of chosen-ciphertext attack, choose the all-zero cipher image and the $2\lceil \log_2(L) \rceil$ special cipher images with the same *sum* value as $\hat{\boldsymbol{C}}$ by the method constructed in Algorithm 1, and then use the decryption machine of BCIEA to get their corresponding cipher images respectively.
- Step 2. As Section 4.1, get the two diffusion keystreams $\boldsymbol{b}_1, \boldsymbol{b}_2$ with the all-zero chosen cipher image and the corresponding plain image.
- Step 3. Obtain the two confusion sequences $\boldsymbol{Y}$ and $\boldsymbol{Z}$ by the method given in Section 4.2.
- Step 4. Recover the original image $\hat{\boldsymbol{A}}$ of a given cipher image $\hat{\boldsymbol{C}}$ with the equivalent keys $\boldsymbol{b}_1, \boldsymbol{b}_2$ and $\boldsymbol{Y}$ and $\boldsymbol{Z}$.

Note that the chosen cipher images constructed in Step 1 may change for a given different cipher image. Nevertheless, the attack method is still available and effective for each target encrypted image. Therefore, BCIEA cannot resist chosen-ciphertext attack.

For the data complexity of the attack method, the number of cipher images required is $1 + 2\lceil \log_2(L) \rceil$. Moreover, in the terms of computational complexity, using the decryption machine is $\boldsymbol{O}(1 + 2\lceil \log_2(L) \rceil)$, determining the two equivalent keys $(\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2)$ and $(\boldsymbol{Y}, \boldsymbol{Z})$ are both $\boldsymbol{O}(2L)$, and restoring the original image is $\boldsymbol{O}(8L)$.

5. Experimental results and discussion

In order to verify the validity of our security analyses and the feasibility of the proposed attack method, we conducted experimental verification without changing the idea of the target algorithm [51]. For the experimental platform, we use a PC mainframe with MATLAB R2022a experimental software installed, the processor of the PC is an AMD Ryzen™ 9 5950X CPU with 3.88 GHz, the RAM size is 64 GB, the hard disk size is 8 TB, and the operating system is Windows 10. For the sake of generality, we first chose the same standard image "Lena" of size 256 × 256 as in [51], and then performed the experiments on other images of different types from the MISC image database [54]. Considering that the secret keys of the cryptosystem are not fixed and unknown to the attackers, different keys were chosen for experimental simulation.

5.1. Attacking BCIEA for standard image

We choose a standard image as the experimental object, i.e., a 256 × 256 8-bit grayscale image "Lena", the image and its histogram are shown in Figs. 4(a)–(d). At this point, the encryption key parameter is $(x_0 = 0.3, \eta_1 = 1.58, y_0 = 0.2, \eta_2 = 1.58)$. Under this encryption key, the encrypted image and its histogram are shown in Figs. 4(c)–(d).

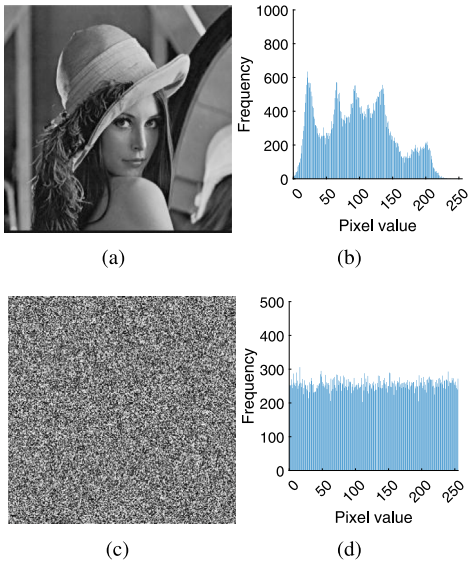


Fig. 4. The standard image "Lena", cipher image and the corresponding histograms: (a)Plain image; (b)Histogram of (a); (c)Cipher image; (d)Histogram of (c).

According to Section 4, it can be seen that our attack idea is to first crack the diffusion part, then decipher the confusion part, and finally, according to the equivalent key, decipher and recover the original plain image according to the conditions of the chosen-ciphertext attack.

First, it is known from Section 4.1 that the chosen all-zero cipher image can invalidate the confusion part of BCIEA, which degenerates into a diffusion-only process. Therefore, using the all-zero cipher image $\boldsymbol{C}^0$ and its corresponding recovery image $\boldsymbol{A}^0$ as shown in Figs. 5(a)–(b), the equivalent diffusion keys $\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2$ can be obtained.

Next, the confusion part of BCIEA is analyzed. According to Section 4.2, it is known that for an image of size 256 × 256, implementing an effective attack requires special $N = 2\lceil \log_2(L) \rceil = 36$ chosen cipher images. It is worth mentioning that the pixel sum value of any of the chosen cipher images should be equal to the target cipher image as shown in Figs. 4(c). According to Step 3 of Section 4.3, using the 18 chosen cipher images as shown in Figs. 6(a)–(r) and the corresponding plain images as shown in Figs. 8(a)–(r), the confusion sequence $\boldsymbol{Y}$ can be solved. Similarly, the confusion sequence $\boldsymbol{Z}$ can be solved by Figs. 7(a)–(r) and 9(a)–(r).

Finally, according to Step 4 in Section 4.3, using the confusion sequences $\boldsymbol{Y}$ and $\boldsymbol{Z}$ and the equivalent diffusion keys $\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2$, the plain image of "Lena" can be recovered, and the restored image and its histogram are shown in Figs. 10(a)–(b) respectively. We found that the two images in Figs. 4(c) and 10(a) are identical after comparison, which verifies the feasibility of our attack method.

Based on the above effective attack experiments, the attack complexity of standard images is briefly analyzed. The attack complexity

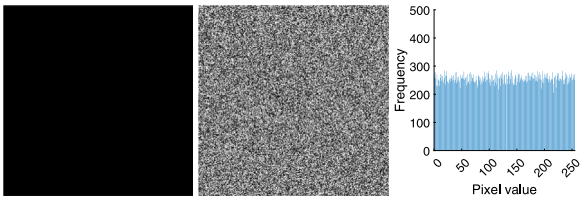


Fig. 5. The all-zero chosen cipher image and the corresponding plain image for attacking BCIEA: (a)All-zero image $\boldsymbol{C}^0$; (b)Recovery image $\boldsymbol{A}^0$; (c)Histogram of (b).

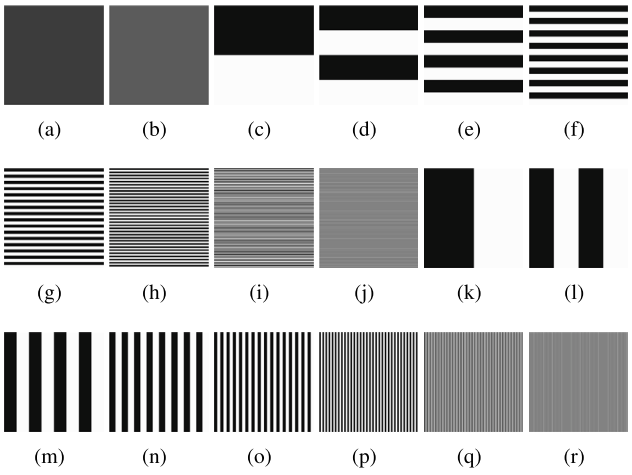


Fig. 6. The 18 chosen cipher images to solve $\boldsymbol{Y}$: (a)$\boldsymbol{C}_Y^{18}$; (b)$\boldsymbol{C}_Y^{17}$; (c)$\boldsymbol{C}_Y^{16}$; (d)$\boldsymbol{C}_Y^{15}$; (e)$\boldsymbol{C}_Y^{14}$; (f)$\boldsymbol{C}_Y^{13}$; (g)$\boldsymbol{C}_Y^{12}$; (h)$\boldsymbol{C}_Y^{11}$; (i)$\boldsymbol{C}_Y^{10}$; (j)$\boldsymbol{C}_Y^{9}$; (k)$\boldsymbol{C}_Y^{8}$; (l)$\boldsymbol{C}_Y^{7}$; (m)$\boldsymbol{C}_Y^{6}$; (n)$\boldsymbol{C}_Y^{5}$; (o)$\boldsymbol{C}_Y^{4}$; (p)$\boldsymbol{C}_Y^{3}$; (q)$\boldsymbol{C}_Y^{2}$; (r)$\boldsymbol{C}_Y^{1}$.

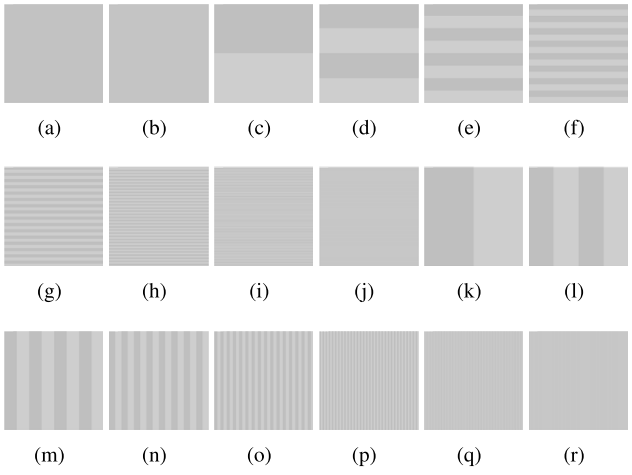


Fig. 7. The 18 chosen cipher images to solve $\boldsymbol{Z}$: (a)$\boldsymbol{C}_Z^{18}$; (b)$\boldsymbol{C}_Z^{17}$; (c)$\boldsymbol{C}_Z^{16}$; (d)$\boldsymbol{C}_Z^{15}$; (e)$\boldsymbol{C}_Z^{14}$; (f)$\boldsymbol{C}_Z^{13}$; (g)$\boldsymbol{C}_Z^{12}$; (h)$\boldsymbol{C}_Z^{11}$; (i)$\boldsymbol{C}_Z^{10}$; (j)$\boldsymbol{C}_Z^{9}$; (k)$\boldsymbol{C}_Z^{8}$; (l)$\boldsymbol{C}_Z^{7}$; (m)$\boldsymbol{C}_Z^{6}$; (n)$\boldsymbol{C}_Z^{5}$; (o)$\boldsymbol{C}_Z^{4}$; (p)$\boldsymbol{C}_Z^{3}$; (q)$\boldsymbol{C}_Z^{2}$; (r)$\boldsymbol{C}_Z^{1}$.

mainly includes time complexity and data complexity. In terms of time complexity, for an 8-bit "Lena" image of size 256 × 256, the total deciphering time of the proposed attack method is about 1.423227 s. In terms of data complexity, for an 8-bit "Lena" image of size 256 × 256, the data complexity required to decipher the proposed attack method is $O(1+2\lceil\log_2(L)\rceil) = O(37)$. These results show that the proposed method can effectively and efficiently decipher BCIEA.

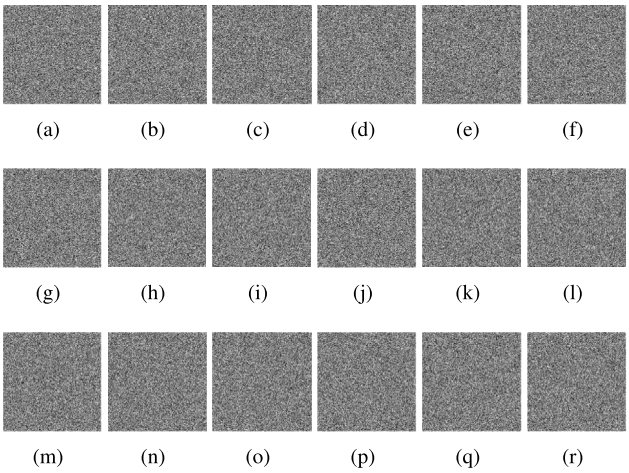


Fig. 8. The 18 recovered plain images corresponding to Fig. 6 for determining $\boldsymbol{Y}$: (a)$\boldsymbol{P}_Y^{18}$; (b)$\boldsymbol{P}_Y^{17}$; (c)$\boldsymbol{P}_Y^{16}$; (d)$\boldsymbol{P}_Y^{15}$; (e)$\boldsymbol{P}_Y^{14}$; (f)$\boldsymbol{P}_Y^{13}$; (g)$\boldsymbol{P}_Y^{12}$; (h)$\boldsymbol{P}_Y^{11}$; (i)$\boldsymbol{P}_Y^{10}$; (j)$\boldsymbol{P}_Y^{9}$; (k)$\boldsymbol{P}_Y^{8}$; (l)$\boldsymbol{P}_Y^{7}$; (m)$\boldsymbol{P}_Y^{6}$; (n)$\boldsymbol{P}_Y^{5}$; (o)$\boldsymbol{P}_Y^{4}$; (p)$\boldsymbol{P}_Y^{3}$; (q)$\boldsymbol{P}_Y^{2}$; (r)$\boldsymbol{P}_Y^{1}$.

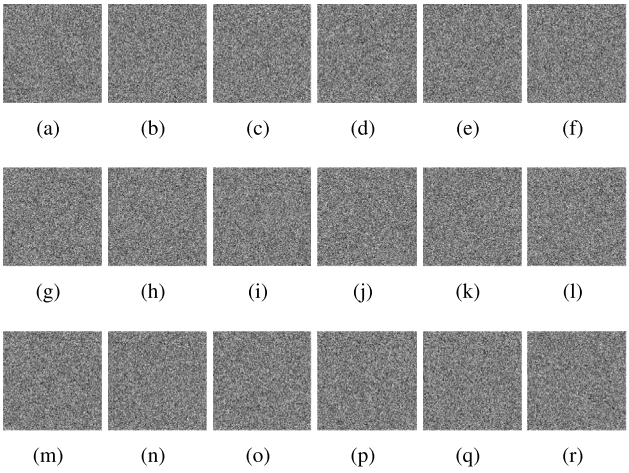


Fig. 9. The 18 recovered plain images corresponding to Fig. 7 for determining $\boldsymbol{Z}$: (a)$\boldsymbol{P}_Z^{18}$; (b)$\boldsymbol{P}_Z^{17}$; (c)$\boldsymbol{P}_Z^{16}$; (d)$\boldsymbol{P}_Z^{15}$; (e)$\boldsymbol{P}_Z^{14}$; (f)$\boldsymbol{P}_Z^{13}$; (g)$\boldsymbol{P}_Z^{12}$; (h)$\boldsymbol{P}_Z^{11}$; (i)$\boldsymbol{P}_Z^{10}$; (j)$\boldsymbol{P}_Z^{9}$; (k)$\boldsymbol{P}_Z^{8}$; (l)$\boldsymbol{P}_Z^{7}$; (m)$\boldsymbol{P}_Z^{6}$; (n)$\boldsymbol{P}_Z^{5}$; (o)$\boldsymbol{P}_Z^{4}$; (p)$\boldsymbol{P}_Z^{3}$; (q)$\boldsymbol{P}_Z^{2}$; (r)$\boldsymbol{P}_Z^{1}$.

5.2. Attacking BCIEA for other images

In order to further verify the universal validity of the attack method, we selected some other images from the MISC database for experiments. Figs. 11(a)–(h) show the four cipher images and their cryptanalysis results. It can be seen that the corresponding plain images can be recovered completely according to the attack method in this paper. Table 1 gives the statistical results of the time and the number of attack images required to attack BCIEA under these images. It can be seen that the attack method proposed in this paper is equally effective for other different images and the time and data complexity required are very low.

5.3. Suggestions for improvement

(1) Avoiding the existence of equivalent keys in the cryptosystem. The existence of an equivalent key will allow an attacker to decipher the original algorithm simply by obtaining its equivalent key without knowing information about the key parameters. Therefore, the designed encryption system should be carefully examined to avoid the existence of equivalent keys.

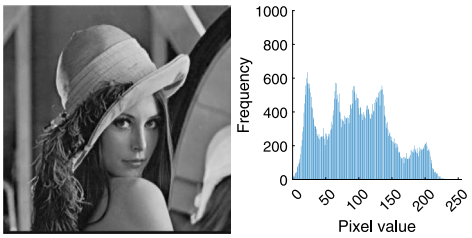


Fig. 10. Attacking results under the standard image: (a)Recovery image; (b)Histogram of (a).

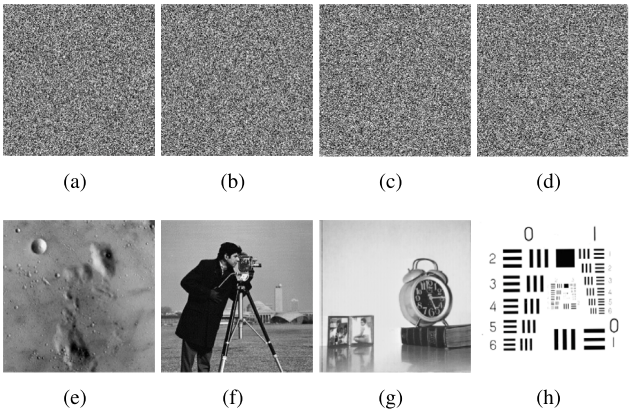


Fig. 11. Supplementary experiment: (a)Ciphertext of grayscale image "5.1.09"; (b)Ciphertext of grayscale image "Cameramen"; (c)Ciphertext of grayscale image "5.1.12"; (d)Ciphertext of grayscale image "5.1.13"; (e)Grayscale image "5.1.09"; (f)Grayscale image "Cameramen"; (g)Grayscale image "5.1.12"; (h)Grayscale image "5.1.13".

(2) Enhancing the complexity and relevance of confusion and diffusion. The purpose of diffusion and confusion is to make the relationship between plaintext, ciphertext and key more complex, but BCIEA does not achieve this. In BCIEA, both the confusion and diffusion modules are relatively simple, making them easy to decipher. In addition, the correlation between the two is weak. Therefore, more complex and better correlated cryptographic operations should be considered to improve security.

6. Conclusions

This paper performed a comprehensive cryptanalysis on a bit-level image encryption cryptosystem named BCIEA based on chaotic maps. From the perspective of cryptography, BCIEA has fatal security problems. First, BCIEA has equivalent diffusion key because the chaotic sequences are fixed for different plain image. Second, there is a certain regularity in the part of confusion, so it can be simplified under some special chosen cipher images. Third, based on the equivalent simplification, BCIEA can be broken by chosen-ciphertext attack with the divide-and-conquer strategy. Thus, BCIEA deviates from the basic principles of symmetric cryptosystem design. On the basis of reasonable and tiny corrections to BCIEA, we propose a chosen-ciphertext attack method to break BCIEA. Theoretical analyses and experimental results support that BCIEA can be broken by our attack method with low computational and data complexity. This research can provide a reference for improving the security of image encryption schemes based on bit-level techniques. Of course, due to the limitations of the case of cryptanalysis in this paper, in the future work, it is planned to discuss a class of related image cryptosystems, and reveal the working process and mechanism more systematically and deeply.

Table 1
Statistical results of the time and data complexity for attacking BCIEA.

Images	Encryption/Breaking times	Complexity
Moon surface	1.4260862 s/ 1.471862 s	37
Cameramen	1.4243640 s/ 1.481161 s	37
Clock	1.4070490 s/ 1.478388 s	37
Resoiution chart	1.4345460 s/ 1.491824 s	37

CRediT authorship contribution statement

Heping Wen: Supervision, Project Administration, Investigation, Funding acquisition, Validation, Formal analysis, Writing – original draft, Writing – review & editing. **Yiting Lin:** Software, Formal Analysis, Conceptualization, Methodology, Resources, Writing – original draft, Writing – review & editing. **Zhaoyang Feng:** Validation, Formal analysis, Data Curation , Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part by Guangdong Basic and Applied Basic Research Foundation, China under Grant 2023A1515011717, and in part by Project for Zhongshan Science and Technology, China under Grant 2021B2062, and in part by Special Projects for Key Fields of the Education Department of Guangdong Province, China under Grant 2023ZDZX1041.

References

[1] Y. Luo, C. Zhang, X. Wang, X. Liang, K. Qiu, Robust key update with controllable accuracy using support vector machine for secure OFDMA-PON, J. Lightwave Technol. 41 (14) (2023) 4663–4671.
[2] X. Liang, C. Zhang, Y. Luo, X. Wang, K. Qiu, Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion, J. Lightwave Technol. 41 (6) (2023) 1619–1625.
[3] T. Wu, W. Zeng, Y. Liu, S. Song, L. Zhao, C. Chen, C. Zhang, L. Guo, Secure turbulence-resistant coherent free-space optical communications via chaotic region-optimized probabilistic constellation shaping, Opt. Lett. 48 (3) (2023) 684–687.
[4] W. Liu, K. Sun, S. He, H. Wang, The parallel chaotification map and its application, IEEE Trans. Circuits Syst. I. Regul. Pap. (2023) 1–10.
[5] O. Kocak, U. Erkan, A. Toktas, S. Gao, PSO-based image encryption scheme using modular integrated logistic exponential map, Expert Syst. Appl. 237 (2024) 121452.
[6] U. Erkan, A. Toktas, S. Memiş, Q. Lai, G. Hu, An image encryption method based on multi-space confusion using hyperchaotic 2D vincent map derived from optimization benchmark function, Nonlinear Dynam. 111 (21) (2023) 20377–20405.
[7] Z. Man, J. Li, X. Di, R. Zhang, X. Li, X. Sun, Research on cloud data encryption algorithm based on bidirectional activation neural network, Inform. Sci. 622 (2023) 629–651.
[8] L. Chen, C. Li, C. Li, Security measurement of a medical communication scheme based on chaos and DNA coding, J. Vis. Commun. Image Represent. 83 (2022) 103424.
[9] A. Toktas, U. Erkan, S. Gao, C. Pak, A robust bit-level image encryption based on Bessel map, Appl. Math. Comput. 462 (2024) 128340.
[10] H. Wen, Y. Lin, S. Kang, X. Zhang, K. Zou, Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion, iScience 27 (1) (2024) 108610.
[11] M. Hu, J. Li, X. Di, Quantum image encryption scheme based on 2D $Sine^2$ - logistic chaotic map, Nonlinear Dynam. 111 (3) (2022) 2815–2839.
[12] Z.-Y. Yang, X. Cao, R.-Z. Xu, W.-C. Hong, S.-L. Sun, Applications of chaotic quantum adaptive satin bower bird optimizer algorithm in berth-tugboat-quay crane allocation optimization, Expert Syst. Appl. 237 (2024) 121471.

[13] X. Chai, Y. Wang, X. Chen, Z. Gan, Y. Zhang, TPE-GAN: Thumbnail preserving encryption based on GAN with key, IEEE Signal Process. Lett. 29 (2022) 972–976.
[14] Y. Zhang, W. Zhou, R. Zhao, X. Zhang, X. Cao, F-TPE: Flexible thumbnail-preserving encryption based on multi-pixel sum-preserving encryption, IEEE Trans. Multimed. (2022) 1–15.
[15] D. Xie, Y. Zhang, Z. Hu, F. Chen, T. Wang, ESTPE: An efficient and stable thumbnail-preserving encryption scheme, J. King Saud Univ. Comput. Inform. Sci. 35 (10) (2023) 101815.
[16] H. Wen, Z. Xie, Z. Wu, Y. Lin, W. Feng, Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography, J. King Saud Univ. Comput. Inform. Sci. 36 (1) (2024) 101871.
[17] W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, Y. He, Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform, Mathematics 10 (15) (2022) 2751.
[18] H. Liu, L. Teng, Y. Zhang, R. Si, P. Liu, Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security, Expert Syst. Appl. 235 (2024) 121090.
[19] Y. Ding, W. Liu, H. Wang, K. Sun, A new class of discrete modular memristors and application in chaotic systems, Eur. Phys. J. Plus 138 (7) (2023).
[20] Q. Lai, L. Yang, Y. Liu, Design and realization of discrete memristive hyperchaotic map with application in image encryption, Chaos Solitons Fractals 165 (2022) 112781.
[21] E. Gul, A.N. Toprak, Contourlet and discrete cosine transform based quality guaranteed robust image watermarking method using artificial bee colony algorithm, Expert Syst. Appl. 212 (2023) 118730.
[22] H. Wen, Y. Huang, Y. Lin, High-quality color image compression-encryption using chaos and block permutation, J. King Saud Univ. Comput. Inform. Sci. 35 (8) (2023) 101660.
[23] M.U. Rehman, A. Shafique, K.H. Khan, M.M. Hazzazi, Efficient and secure image encryption using key substitution process with discrete wavelet transform, J. King Saud Univ. Comput. Inform. Sci. 35 (7) (2023) 101613.
[24] F. Cao, D. Guo, T. Wang, H. Yao, J. Li, C. Qin, Universal screen-shooting robust image watermarking with channel-attention in DCT domain, Expert Syst. Appl. 238 (2024) 122062.
[25] Y. Lu, M. Gong, L. Cao, Z. Gan, X. Chai, A. Li, Exploiting 3D fractal cube and chaos for effective multi-image compression and encryption, J. King Saud Univ. Comput. Inform. Sci. 35 (3) (2023) 37–58.
[26] S.M. Basha, P. Mathivanan, A.B. Ganesh, Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map, Optik 259 (2022) 168956.
[27] X. Zhou, W. Hong, G. Yang, T.-S. Chen, J. Chen, An unsolvable pixel reduced authentication method for color images with grayscale invariance, J. King Saud Univ. Comput. Inform. Sci. 35 (9) (2023) 101726.
[28] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, X. Chen, An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map, J. King Saud Univ. Comput. Inform. Sci. 34 (4) (2022) 1535–1551.
[29] M.R. Abuturab, A. Alfalou, Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional Fourier transform, Opt. Laser Technol. 151 (2022) 108071.
[30] D. Zhan, H. Wang, J. Lin, K. Yi, R. Huang, X. Yang, R. Lin, N. Cai, Image denoising and deringing for fourier single-pixel imaging based on upgraded weighted nuclear norm minimization, Opt. Commun. 550 (2024) 130011.
[31] X. Chai, J. Fu, Z. Gan, Y. Lu, Y. Zhang, D. Han, Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission, IEEE Internet Things J. 10 (8) (2023) 7380–7392.
[32] Z. Man, J. Li, X. Di, Y. Sheng, Z. Liu, Double image encryption algorithm based on neural network and chaos, Chaos Solitons Fractals 152 (2021) 111318.
[33] D. An, D. Hao, R. Zhao, J. Lu, Y. Li, Y. Zhang, A novel color image privacy-preserving method: Combining breadth and depth visual encryption with chaotic system, J. King Saud Univ. Comput. Inform. Sci. 35 (2) (2023) 576–589.
[34] S. Zhou, Y. Qiu, G. Qi, Y. Zhang, A new conservative chaotic system and its application in image encryption, Chaos Solitons Fractals 175 (2023) 113909.
[35] S. Zhou, X. Wang, Y. Zhang, Novel image encryption scheme based on chaotic signals with finite-precision error, Inform. Sci. 621 (2023) 782–798.
[36] X. Wang, M. Zhao, An image encryption algorithm based on hyperchaotic system and DNA coding, Opt. Laser Technol. 143 (2021) 107316.
[37] H. Wen, S. Kang, Z. Wu, Y. Lin, Y. Huang, Dynamic RNA coding color image cipher based on chain feedback structure, Mathematics 11 (14) (2023) 3133.
[38] Q. Lai, H. Hua, X.-W. Zhao, U. Erkan, A. Toktas, Image encryption using fission diffusion process and a new hyperchaotic map, Chaos Solitons Fractals 175 (2023) 114022.
[39] H. Wen, Y. Lin, Cryptanalyzing an image cipher using multiple chaos and DNA operations, J. King Saud Univ. Comput. Inform. Sci. 35 (7) (2023) 101612.
[40] R. Lin, S. Liu, J. Jiang, S. Li, C. Li, C.-C.J. Kuo, Recovering sign bits of DCT coefficients in digital images as an optimization problem, J. Vis. Commun. Image Represent. 99 (2024) 104045.
[41] Y. Ma, X. Chai, Z. Gan, Y. Zhang, Privacy-preserving TPE-based JPEG image retrieval in cloud-assisted Internet of Things, IEEE Internet Things J. (2023).
[42] M.B. Farah, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation, Opt. Laser Technol. 121 (2020) 105777.
[43] X. Lu, E.Y. Xie, C. Li, Periodicity analysis of logistic map over ring $\mathbb{Z}_{3^n}$, Int. J. Bifurcation Chaos 33 (5) (2023) 2350063.
[44] H. Wen, Y. Lin, Z. Xie, T. Liu, Chaos-based block permutation and dynamic sequence multiplexing for video encryption, Sci. Rep. 13 (1) (2023).
[45] X. Liu, K. Sun, H. Wang, S. He, A class of novel discrete memristive chaotic map, Chaos Solitons Fractals 174 (2023) 113791.
[46] Y. Ma, C. Li, B. Ou, Cryptanalysis of an image block encryption algorithm based on chaotic maps, J. Inform. Secur. Appl. 54 (2020) 102566.
[47] L. Chen, C. Li, C. Li, Security measurement of a medical communication scheme based on chaos and DNA coding, J. Vis. Commun. Image Represent. 83 (2022) 103424.
[48] H. Wen, Y. Lin, Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding, Expert Syst. Appl. 237 (2024) 121514.
[49] H. Wen, R. Chen, Security analysis of a color image encryption based on bit-level and chaotic map, Multimedia Tools Appl. (2023) 121514.
[50] Y. Ma, C. Li, B. Ou, Cryptanalysis of an image block encryption algorithm based on chaotic maps, J. Inform. Secur. Appl. 54 (2020) 102566.
[51] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Opt. Lasers Eng. 78 (2016) 17–25.
[52] Y. Zhou, W. Cao, C.P. Chen, Image encryption using binary bitplane, Signal Process. 100 (2014) 197–207.
[53] F. Özkaynak, Brief review on application of nonlinear dynamics in image encryption, Nonlinear Dynam. 92 (2) (2018) 305–313.
[54] The USC-SIPI Image Database, Volume 3: Miscellaneous, 2023, https://sipi.usc.edu/database/database.php.