Expert Systems With Applications 250 (2024) 123748

Contents lists available at ScienceDirect

Expert Systems With Applications

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

Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos

Heping Wen[a,b,c,*], Yiting Lin[a,b], Lincheng Yang[a], Ruiting Chen[a]

[a] *University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China*
[b] *School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*
[c] *Guangdong Provincial Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou, 510006, China*

ARTICLE INFO

Keywords:
Image encryption
Cryptanalysis
Chosen-plaintext attack
Chosen-ciphertext attack

ABSTRACT

In 2019, a chaotic image encryption scheme based on a variant of the Hill cipher (VHC-CIES) was proposed by the Moroccan scholars. VHC-CIES introduces a Hill cipher variant and three improved one-dimensional chaotic maps to enhance the security. In this paper, we conduct a comprehensive cryptanalysis, and find that VHC-CIES can resist neither chosen-plaintext attack nor chosen-ciphertext attack due to its inherent flaws. When it comes to chosen-plaintext attack, firstly, we select a plaintext with the pixel values are all 0 and its corresponding ciphertext, and then use algebraic analysis to obtain the equivalent key stream for cracking VHC-CIES. Secondly, we select a plaintext which the pixel values are invariably 1 and obtain its corresponding ciphertext to obtain some Hill cipher variant parameters of VHC-CIES. Finally, we use the resulting steps of the first two to recover the original plain image from a given target cipher image. Similarly, a chosen-ciphertext attack method can also break VHC-CIES. Theoretical analysis and experimental results show that both chosen-plaintext attack and chosen-ciphertext attack can effectively crack VHC-CIES with data complexity of only $O(2)$. For color images of size $256 \times 256 \times 3$, when our simulation encryption time is 0.3150 s, the time for complete breaking by chosen-plaintext attack and chosen-ciphertext attack is about 0.6020 s and 0.9643 s, respectively. To improve its security, some suggestions for further improvement are also given. The cryptanalysis work in this paper may provide some reference for the security enhancement of chaos-based image cryptosystem design.

1. Introduction

Nowadays, the rapid progress of network communication technology is driving a revolutionary and disruptive change in people's production and lifestyle (Ding et al., 2023; Gao et al., 2022; Liu, Sun, Wang et al., 2023). While enjoying the convenience brought by technological progress, people also face threats in terms of information theft and privacy leakage (Feng et al., 2021; Lu, Li et al., 2023; Zou et al., 2022). In view of the challenges that these information security issues may cause, information security privacy protection technology has attracted widespread attention (Lai et al., 2023; Teng et al., 2021; Wu et al., 2023). Due to the characteristics of vivid expression and interactivity of digital images, the use of digital images for communication and interaction in the network has become an extremely common way of communication (Jiang & Ding, 2023; Liu, Sun, He et al., 2023). However, due to the highly open nature of network sharing, security problems such as the leakage of sensitive information in digital images have come to the forefront, making the research and development of image information security technology imminent (Hua et al., 2023; Zhou, Qiu et al., 2023; Zhou, Wang et al., 2023). Therefore, image encryption technology (Wen & Lin, 2023a; Wen, Lin et al., 2024) has now become an important research branch in the field of information and communication security.

In recent years, researchers have combined various theoretical methods to report various new image encryption technology solutions, such as chaos theory (Bao et al., 2023; Cao et al., 2022; Zhang et al., 2021), frequency domain encryption (Liang et al., 2023; Luo et al., 2023), bit-level coding (Jiang et al., 2020; Lai et al., 2022; Tang et al., 2023), DNA coding (Chen et al., 2023; Su et al., 2023; Wen et al., 2023c), compressed sensing (Chai et al., 2023; Wang et al., 2022; Ye et al., 2023), thumbnail-preserving encryption (Chai et al., 2022; Zhang, Zhou et al., 2022) and so on Li et al. (2023), Luo et al. (2022). Among them, chaos theory is the most basic and common theoretical method. In 1963, Professor Lorenz, an American meteorologist, accidentally discovered the existence of chaos in the study of atmospheric changes (Lorenz, 1963). The randomness, topological

[*] 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), YitingLin@stu.zsc.edu.cn (Y. Lin), 202101001025@stu.zsc.edu.cn (L. Yang), ruitingchen@stu.zsc.edu.cn (R. Chen).

https://doi.org/10.1016/j.eswa.2024.123748
Received 16 April 2023; Received in revised form 8 March 2024; Accepted 18 March 2024
Available online 3 April 2024

transfer and dense periodic points of chaotic systems coincide with the basic requirements of traditional cryptography. Therefore, image encryption technology based on chaos theory has gradually developed into one of the academic research hotspots in recent years (Hraoui et al., 2019; Yasser et al., 2021; Zheng & Liang, 2020). However, due to the lack of in-depth security analysis of chaotic image encryption, the inherent security vulnerabilities in many algorithms have not been fully explored (Jiang et al., 2023; Liu et al., 2022; Zhang, Chen et al., 2022), which restricts it from theory to application (Chen et al., 2022; Lu, Xie et al., 2023; Ma et al., 2020). In summary, the systematic cryptanalysis of existing chaotic encryption algorithms is extremely necessary, and it is also an important prerequisite for determining whether a chaotic cryptosystem can be put into practical application (Wen, Feng et al., 2024; Wen, Huang et al., 2023; Wen, Lin et al., 2023; Wen, Xie et al., 2024).

Throughout the international research status, in view of the challenges brought by data security, researchers have proposed many related chaotic encryption algorithms (Alawida et al., 2023, 2022; Erkan et al., 2022). However, many of these algorithms have been broken by analysts after they were proposed due to various security flaws. In 2023, Wen and Lin (2023b) performed cryptographic analysis on an improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos (Kalpana & Murali, 2015). This cracking method uses differential analysis to break the DNA base arrangement process, then eliminates the DNA domain encryption, and finally uses the equivalent key to achieve complete cracking. In the same year, Wen, Chen et al. (2023) performed a cryptographic analysis of the color image encryption technique CIEA-IOCM (Pak et al., 2018), which is based on improved one-dimensional chaotic map and bit-level operations. Vulnerabilities in the presence of equivalent keys in the bit-level arrangement and diffusion steps, as well as in the simplifiable linear transformations, make it completely crackable by a choice of plaintext attack methods. In summary, with the development of chaotic cryptography, the existing chaotic cryptographic design level is constantly improving and the difficulty of analyzing and deciphering chaotic cryptographic algorithms is also increasing. However, there are still some chaotic encryption algorithms that are insufficient in security performance and difficult to resist common cryptography attack methods.

In 2019, a chaotic image encryption scheme based on a variant of the Hill cipher (VHC-CIES) was proposed (Essaid et al., 2019). VHC-CIES introduces a Hill cipher variant and three improved one-dimensional chaotic maps to enhance the security. However, from the perspective of cryptographic analysis, it can be found that several security defects in VHC-CIES are as follows:

- The key used for encryption is independent of the plain image: In VHC-CIES, the secret keys required for its encryption are $(x_0, y_0, z_0, \mu, r_1, r_2)$. However, the pseudo-random number sequences (PRNS) generated by these keys have nothing to do with the plain image. In other words, when the key is fixed, the chaotic pseudo-random number sequences used for encryption remain unchanged for different plain images of the same size. Thus, these sequences can be regarded as equivalent keys.
- The parameters of the variant Hill cipher are easy to determine: In Eqs. (6) and (10), h_{11}, h_{11}^{-1} and h_{21} can be considered as static unknowns. Based on the chosen-plaintext attack, the attackers can determine these unknowns by selecting some specific plain images and obtaining their cipher images. And we only need to know the first two encrypted pixel values to solve h_{11}, h_{11}^{-1} and h_{21}.
- The key streams can be determined because of the paradigm of the encryption equations: Based on the chosen-plaintext attack, under the premise of obtaining h_{11}, h_{11}^{-1} and h_{21}, the ciphertext pixels are composed of two separate parts: the plaintext pixels stream and the key stream. Therefore, the attackers can construct some special plain images to cancel the plaintext pixel stream in the ciphertext pixels, and obtain its corresponding cipher image to solve the key stream.

Based on the above, we conduct a comprehensive cryptanalysis, and find that VHC-CIES can resist neither chosen-plaintext attack nor chosen-ciphertext attack due to its inherent flaws. When it comes to chosen-plaintext attack, firstly, we select a plaintext with the pixel values are all 0 and its corresponding ciphertext, and then use algebraic analysis to obtain the equivalent key stream for cracking VHC-CIES. Secondly, we select a plaintext which the pixel values are invariably 1 and obtain its corresponding ciphertext to obtain some Hill cipher variant parameters of VHC-CIES. Finally, we use the resulting steps of the first two to recover the original plain image from a given target cipher image. Similarly, a chosen-ciphertext attack method can also break VHC-CIES. Theoretical analysis and experimental results show that both chosen-plaintext attack and chosen-ciphertext attack can effectively break VHC-CIES.

The rest of the paper is organized as follows: Section 2 briefly introduces the VHC-CIES; Section 3 gives the cryptanalysis of VHC-CIES; Section 4 gives the experimental simulation results; Section 5 presents suggestions for improvement of VHC-CIES; Section 6 concludes the paper.

2. Encryption and decryption method proposed by VHC-CIES

This section presents three chaotic maps and a variant Hill cipher used in VHC-CIES, and then the specific steps of VHC-CIES are introduced.

2.1. Three chaotic maps

In VHC-CIES, three one-dimensional chaotic maps are adopted. The details are as follows:

- The Enhanced Logistics Map (ELM) is mathematically modeled by:

$$x_{n+1} = \mathrm{mod}(\mu x_n(1 - x_n) \times G(k), 1) \tag{1}$$

  where x is the state variable, $\mu \in (0, 4)$ is the control parameter, mod represents modulo operation, $G(k)$ is an adjustment function and $k = 6$.
- The Enhanced Chebyshev Map (ECM) is defined as:

$$y_{n+1} = \mathrm{mod}(cos(r_1 arcos(y_n)) \times G(k), 1) \tag{2}$$

  where y is the state variable and $r_1 \in N$ is the control parameter.
- The Enhanced Sine Map (ESM) is defined as:

$$z_{n+1} = \mathrm{mod}(r_2 sin(\pi z_n) \times G(k), 1) \tag{3}$$

  where z is the state variable and $r_2 \in (0, 1)$ is the control parameter.

2.2. A variant Hill cipher

Hill cipher is a polyalphabetic cryptosystem coined in 1929 by Lester S. Hill, and its basic idea is to take linear combinations on matrices (Ghazanfaripour & Broumandnia, 2020). For example, given a Hill encryption matrix H of size 2 × 2, the encryption process is described herein as:

$$\begin{pmatrix} y_1, y_3, \dots, y_{n-1} \\ y_2, y_4, \dots, y_n \end{pmatrix} = \left(\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} x_1, x_3, \dots, x_{n-1} \\ x_2, x_4, \dots, x_n \end{pmatrix} \right) \mathrm{mod}\ 26 \tag{4}$$

where $x = (x_1, x_2, \dots, x_n)$ is a plaintext sequence, $y = (y_1, y_2, \dots, y_n)$ is the corresponding ciphertext sequence and $x, y, H \in \mathbb{Z}_{26}$. Using matrix notation: $y = Hx$. Correspondingly, its decryption form is expressed as $x = H^{-1}y$, where H^{-1} is a Hill decryption matrix. Here, $HH^{-1} = I$ holds, where I is the identity matrix of size 2×2.

A variant Hill cipher is used in Essaid et al. (2019). Unlike the classical one, the variant form has two differences: Firstly, the transform domain is $\mathbb{Z}_{256}$ instead of $\mathbb{Z}_{26}$; Secondly, only the first element of the construction of the Hill cipher matrix needs to be reversible, rather than the entire matrix's elements are reversible.

2.3. Description of VHC-CIES

The main contents of the encryption and decryption process of VHC-CIES are briefly introduced as follows. For more details, please refer to Essaid et al. (2019).

- The Secret Key:
  The secret keys of VHC-CIES consist of $(x_0, y_0, z_0, \mu, r_1, r_2)$, in which (x_0, y_0, z_0) are the initial values and (μ, r_1, r_2) are the parameters of three chaotic maps, given in Eqs. (1)–(3), respectively. The keys are used to generate the pseudo-random number sequences (PRNS) for encryption.
- Encryption of VHC-CIES:
  - Initialization:
    For a gray image of size $H \times W$ (height × width), the total number of pixels is $L = H \times W$. Accordingly, three PRNS are generated by iterating Eqs. (1)–(3)L times respectively, given as:

    $$\begin{cases} K_1(i) = \mathrm{mod}(floor(x(i) \times 10^6), 256) \\ K_2(i) = \mathrm{mod}(floor(y(i) \times 10^6), 256) \\ K_3(i) = \mathrm{mod}(floor(z(i) \times 10^6), 256) \end{cases} \tag{5}$$

    where $i = 1 \sim L$, $floor$ is the function that takes an integer. In addition, a secret Hill matrix of size 2×2 is obtained from ELM. Exactly, the four parameters of the matrix are $h_{11}, h_{12}, h_{21}, h_{22}$. Note that the parameter h_{11} is invertible in the ring $\mathbb{Z}/256\mathbb{Z}$.
  - Stage 1. Encrypt the first pixel:
    The first pixel value of cipher image $C(1)$ is obtained as:

    $$\begin{pmatrix} C(1) \\ T(1) \end{pmatrix} = \left(\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} P(1) \\ K_1(1) \end{pmatrix} + \begin{pmatrix} K_2(1) \\ K_3(1) \end{pmatrix} \right) \bmod 256 \tag{6}$$

    where $P(1)$ is the first pixel value of the plain image, and $T(1)$ is a temporary value for randomizing the adjacent pixel. Then, the second randomized pixel $S(2)$ is achieved, defined as:

    $$S(2) = (T(1) + P(2)) \bmod 256 \tag{7}$$

    where $P(2)$ is the second pixel value of the plain image.
  - Stage 2. The generation of the other cipher pixels:
    The other pixel values of cipher image $C(i)$ are obtained as:

    $$\begin{pmatrix} C(i) \\ T(i) \end{pmatrix} = \left(\begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} S(i) \\ K_1(i) \end{pmatrix} + \begin{pmatrix} K_2(i) \\ K_3(i) \end{pmatrix} \right) \bmod 256 \tag{8}$$

    and

    $$S(i) = (T(i-1) + P(i)) \bmod 256 \tag{9}$$

    where $i = 2 \sim L$ and $T(i)$ is a temporary value for randomizing the $(i+1)$-th pixel.
- Decryption of VHC-CIES:
  Decryption is the inverse process of encryption. It can be introduced briefly below:
  - *Initialization*:
    Like encryption, generate $K_1(i), K_2(i), K_3(i)$ for $i = 1 \sim L$ and $h_{11}, h_{12}, h_{21}, h_{22}$ in the same way. Then, get the reverse of h_{11} in the ring $\mathbb{Z}/256\mathbb{Z}$, namely h_{11}^{-1}.
  - Stage 1. Decryption of the first pixel:
    The first pixel value of cipher image $C(1)$ is decrypted as:

    $$P(1) = \left(h_{11}^{-1}\left(C(1) - h_{12}K_1(1) - K_2(1)\right)\right) \bmod 256 \tag{10}$$

    where $P(1)$ is the first pixel value of the decrypted plain image. Then it can be defined as:

    $$tmp(1) = \left(h_{21}h_{11}^{-1}\left(C(1) - h_{12}K_1(1) - K_2(1)\right) + h_{22}K_1(1) + K_3(1)\right) \bmod 256 \tag{11}$$

    where, $tmp(1)$ is a temporary variable, it will be calculated at each iteration, and then use it to decrypt the next pixel.
  - Stage 2. Decryption of the other pixels:
    The other pixels of the plain image $P(i)$ are recovered by:

    $$\begin{cases} P(i) = \left(h_{11}^{-1}\left(C(i) - h_{12}K_1(i) - K_2(i)\right) - tmp(i-1)\right) \bmod 256 \\ tmp(i) = \left(h_{21}h_{11}^{-1}\left(C(i) - h_{12}K_1(i) - K_2(i)\right) + h_{22}K_1(i) + K_3(i)\right) \bmod 256 \end{cases} \tag{12}$$

    where $i = 2 \sim L$.

3. Cryptanalysis

This section first introduces the algebraic analysis of the VHC-CIES encryption process, and then proposes a method of chosen-plaintext attack to decipher the VHC-CIES encryption process. Then, the algebraic analysis of the decryption process of VHC-CIES is introduced. Finally, a method of chosen-ciphertext attack is proposed to decipher the process of VHC-CIES.

Modern cryptology is divided into cryptography and cryptanalysis. The purpose of cryptography is to propose algorithms that can resist attacks by third parties or unauthorized eavesdroppers, so that the information hidden in the process of transmission and reception will not be leaked. Even if it is leaked, the complexity of its encoding algorithm makes it difficult for many attackers to analyze. The idea of cryptanalysis is the opposite, mainly used to analyze and decipher encrypted information.

In cryptography, Kerckhoffs's principle is widely accepted, which emphasizes that the security of a cryptosystem depends on the key rather than the encryption scheme. Therefore, in cryptanalysis, an attacker can be considered to have temporary access to the encryption/decryption machine with the ultimate aim of obtaining the equivalent key. Under the Kerckhoffs's principle, four common attack methods are briefly described below:

- Ciphertext-only attack: The attacker only intercepts one or several ciphertexts encrypted with the same key, analyzing them to find the plaintext or the key;
- Known-plaintext attack: The attacker has partial plaintext and its corresponding ciphertext, analyzing them to find the key or encryption algorithm;
- Chosen-plaintext attack: The attacker can arbitrarily select the plaintext and obtain its corresponding ciphertext, analyzing them to find the key;
- Chosen-ciphertext attack: Based on chosen-plaintext attack, the attacker can arbitrarily select the ciphertext and obtain its corresponding plaintext, analyzing them to find the key.

A well-performing cryptosystem is required to be able to resist at least these four attack methods, and if this criterion is not achieved, this system is considered insecure.

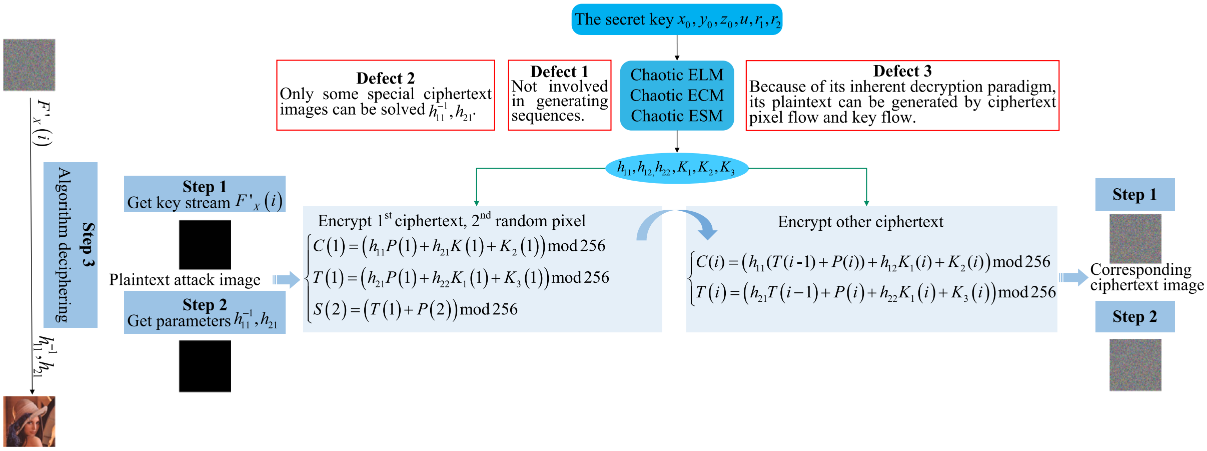
The secret key $x_0, y_0, z_0, u, r_1, r_2$
Defect 2
Only some special ciphertext images can be solved h_{11}^{-1}, h_{21}.
Defect 1
Not involved in generating sequences.
Chaotic ELM
Chaotic ECM
Chaotic ESM
Defect 3
Because of its inherent decryption paradigm, its plaintext can be generated by ciphertext pixel flow and key flow.
$h_{11}, h_{12}, h_{22}, K_1, K_2, K_3$
$F'_X(i)$
Step 3
Algorithm deciphering
h_{11}^{-1}, h_{21}
Step 1
Get key stream $F'_X(i)$
Plaintext attack image
Step 2
Get parameters h_{11}^{-1}, h_{21}
Encrypt 1st ciphertext, 2nd random pixel
$C(1) = (h_{11}P(1) + h_{21}K(1) + K_2(1)) \bmod 256$
$T(1) = (h_{21}P(1) + h_{22}K_1(1) + K_3(1)) \bmod 256$
$S(2) = (T(1) + P(2)) \bmod 256$
Encrypt other ciphertext
$C(i) = (h_{11}(T(i-1) + P(i)) + h_{12}K_1(i) + K_2(i)) \bmod 256$
$T(i) = (h_{21}T(i-1) + P(i) + h_{22}K_1(i) + K_3(i)) \bmod 256$
Step 1
Corresponding ciphertext image
Step 2

Fig. 1. Overall flowchart of cryptanalysis on VHC-CIES under chosen-plaintext attack.

3.1. Algebraic analysis of VHC-CIES based on chosen-plaintext attack method

Observing Eqs. (6) and (8), it can be seen that the operation of its diffusion part is a modular addition, which involves neither linear transformation nor complex diffusion mechanism. Therefore, the algorithm is insensitive to plain images and has security flaws. A basic property of the modular addition operation is described below.

Property 1. *For any positive integer a, b and m, it can be defined as $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$.*

In order to better analyze the encryption process, we first use deductive method to expand the encryption equation. Firstly, following Eq. (6), it can be defined as:

$$\begin{cases} C(1) = (h_{11}P(1) + h_{12}K_1(1) + K_2(1)) \bmod 256 \\ T(1) = (h_{21}P(1) + h_{22}K_1(1) + K_3(1)) \bmod 256 \end{cases} \tag{13}$$

Then, Eq. (8) becomes:

$$\begin{cases} C(i) = (h_{11}S(i) + h_{12}K_1(i) + K_2(i)) \bmod 256 \\ T(i) = (h_{21}S(i) + h_{22}K_1(i) + K_3(i)) \bmod 256 \end{cases} \tag{14}$$

where $i = 2 \sim L$, and $S(i) = (T(i-1) + P(i)) \bmod 256$.

To simplify the equations, the method of substitution is adopted. Let $X_1(i)$ and $X_2(i)$ be $h_{12}K_1(i) + K_2(i)$ and $h_{22}K_1(i) + K_3(i)$ respectively, where $i = 1 \sim L$. Thus, Eqs. (13) and (14) become:

$$\begin{cases} C(1) = (h_{11}P(1) + X_1(1)) \bmod 256 \\ T(1) = (h_{21}P(1) + X_2(1)) \bmod 256 \end{cases} \tag{15}$$

$$\begin{cases} C(i) = \left(h_{11}\,(T(i-1) + P(i)) + X_1(i)\right) \bmod 256 \\ T(i) = \left(h_{21}\,(T(i-1) + P(i)) + X_2(i)\right) \bmod 256 \end{cases} \tag{16}$$

where $i = 2 \sim L$.

When $i = 2$, substituting $T(1)$ in Eq. (15) into Eq. (16), one further gets:

$$\begin{aligned} C(2) &= (h_{11}S(2) + X_1(2)) \bmod 256 \\ &= \left(h_{11}\,(T(1) + P(2)) + X_1(2)\right) \bmod 256 \\ &= \left(h_{11}\,\left(h_{21}P(1) + X_2(1) + P(2)\right) + X_1(2)\right) \bmod 256 \\ &= (h_{11}(h_{21}P(1) + P(2)) + h_{11}X_2(1) + X_1(2)) \bmod 256 \end{aligned}$$

and

$$\begin{aligned} T(2) &= (h_{21}S(2) + X_2(2)) \bmod 256 \\ &= (h_{21}(T(1) + P(2)) + X_2(2)) \bmod 256 \\ &= (h_{21}(h_{21}(P(1) + X_2(1)) + P(2)) + X_2(2)) \bmod 256 \\ &= (h_{21}(h_{21}P(1) + P(2)) + h_{21}X_2(1) + X_2(2)) \bmod 256 \end{aligned}$$

Similarly, when $i = 3$, one gets:

$$\begin{aligned} C(3) &= (h_{11}S(3) + X_1(3)) \bmod 256 \\ &= (h_{11}(T(2) + P(3)) + X_1(3)) \bmod 256 \\ &= (h_{11}(h_{21}(h_{21}P(1) + P(2)) \\ &+ P(3)) + h_{11}(h_{21}X_2(1) + X_2(2)) + X_1(3)) \bmod 256 \end{aligned}$$

$$\begin{aligned} T(3) &= (h_{21}S(3) + X_2(3)) \bmod 256 \\ &= \left(h_{21}\,(T(2) + P(3)) + X_2(3)\right) \bmod 256 \\ &= \left(h_{21}\,\left(h_{21}\,\left(h_{21}P(1) + P(2)\right) + P(3)\right)\right. \\ &\left. + h_{21}\,\left(h_{21}X_2(1) + X_2(2)\right) + X_1(3)\right) \bmod 256 \end{aligned}$$

Observing these above equations, one can see that each ciphertext pixel value is an algebraic result for some plaintext pixel streams and key streams. More importantly, the two parts, plaintext pixel stream and key stream, can be separated independently. Thus, the encryption process can be defined as:

$$C(i) = (F_P(i) + F_X(i)) \bmod 256 \tag{17}$$

where $i = 1 \sim L$, $F_P(i)$ and $F_X(i)$ represent the algebraic results of the plaintext pixel stream and the key stream, respectively. Here, $F_P(i), F_X(i) \in \mathbb{Z}_{256}$. Therefore, the basic assumptions based on cryptanalysis and the algorithm are exposed, the functions $F_P(\cdot)$ and $F_X(\cdot)$ are known as the adversary because the algorithm is public under Kerckhoffs's principle. This also provides an important prerequisite for our cryptanalysis.

3.2. Breaking VHC-CIES by chosen-plaintext attack

In this section, we will introduce the process of breaking VHC-CIES with chosen-plaintext attack. By selecting some special plain images and obtaining their corresponding cipher images, we can evaluate the equivalent key of VHC-CIES.

In the case of chosen-plaintext attack, when $i = 1 \sim L$, only h_{11}, h_{21} and $F_X(i)$ are unknown in Eq. (17). Supposing that the unknowns can be determined, we can recover the original plain images from their corresponding cipher images. Therefore, the goal is to find the unknowns h_{11}, h_{21}, and $F_X(i)$ for $i = 1 \sim L$, which are also equivalent keys. The block diagram of its cryptanalysis is shown in Fig. 1. It is mainly divided into three steps. The steps to decipher VHC-CIES in detail are as follows:

- Step 1. Get $F_X(i)$ for $i = 1 \sim L$ with the all-zero plain image and its corresponding cipher image:
  Under the condition of choosing the all-zero plain image I^0 and its corresponding cipher image C^0, since all the pixel values of plain image are 0, the Eq. (17) becomes:

$$C^0(i) = (F_X(i)) \bmod 256 \tag{18}$$

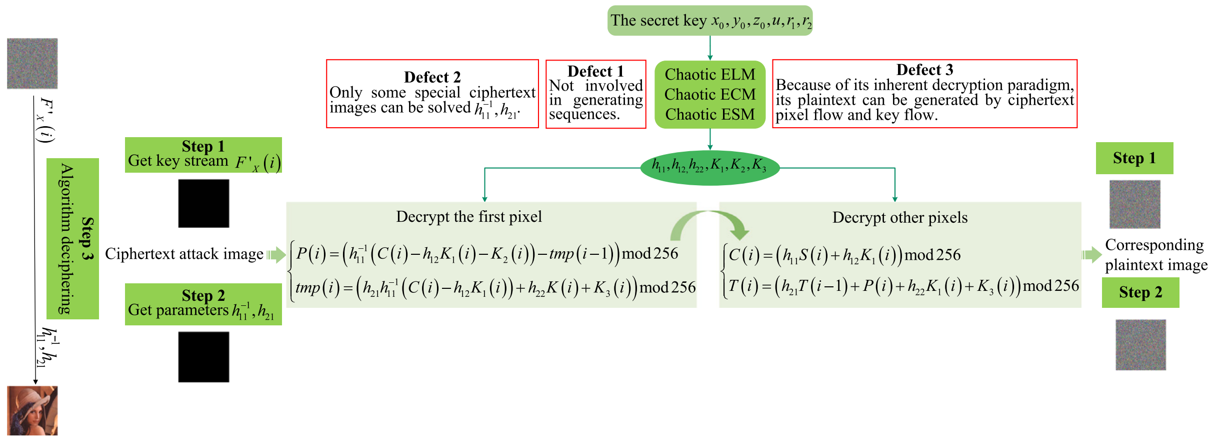
The secret key $x_0, y_0, z_0, u, r_1, r_2$
Defect 2
Only some special ciphertext images can be solved h_{11}^{-1}, h_{21}.
Defect 1
Not involved in generating sequences.
Chaotic ELM
Chaotic ECM
Chaotic ESM
Defect 3
Because of its inherent decryption paradigm, its plaintext can be generated by ciphertext pixel flow and key flow.
$h_{11}, h_{12}, h_{22}, K_1, K_2, K_3$
$F'_X(i)$
Step 3
Algorithm deciphering
h_{11}^{-1}, h_{21}
Step 1
Get key stream $F'_X(i)$
Ciphertext attack image
Step 2
Get parameters h_{11}^{-1}, h_{21}
Decrypt the first pixel
$P(i)=(h_{11}^{-1}(C(i)-h_{12}K_1(i)-K_2(i))-tmp(i-1))\bmod 256$
$tmp(i)=(h_{21}h_{11}^{-1}(C(i)-h_{12}K_1(i))+h_{22}K(i)+K_3(i))\bmod 256$
Decrypt other pixels
$C(i)=(h_{11}S(i)+h_{12}K_1(i))\bmod 256$
$T(i)=(h_{21}T(i-1)+P(i)+h_{22}K_1(i)+K_3(i))\bmod 256$
Step 1
Corresponding plaintext image
Step 2

Fig. 2. Overall flowchart of cryptanalysis on VHC-CIES under chosen-ciphertext attack.

Here, although the cipher image C^0 seems to be very complicated, it is actually the composite operation result of $K_1(i), K_2(i), K_3(i)$ for $i = 1 \sim L$ and $h_{11}, h_{12}, h_{21}, h_{22}$. For the subsequent solution, two equations are defined as:

$$C^0(1) = X_1(1) \bmod 256$$

and

$$C^0(2) = (h_{11}X_2(1) + X_1(2)) \bmod 256$$

- Step 2. Obtain the parameters h_{11} and h_{21} with another chosen plain image and cipher image:
  To determine h_{11} and h_{21}, another plain image in which the pixel values are all 1 is required. Firstly, by the plain image P^1 and the corresponding cipher image C^1, owing to $P^1(1) = 1$, it can be defined as:

  $$C^1(1) = (h_{11}P^1(1) + C^0(1)) \bmod 256$$

  Hence, h_{11} can be solved by:

  $$h_{11} = (C^1(1) - C^0(1)) \bmod 256$$

  Secondly, since $P^1(2) = 1$ and $T^1(1) = (h_{21} + X_2(1)) \bmod 256$, it can be defined as:

  $$\begin{aligned} C^1(2) &= (h_{11}(T^1(1) + P^1(2)) + X_1(2)) \bmod 256 \\ &= (h_{11}(h_{21} + X_2(1) + 1) + X_1(2)) \bmod 256 \\ &= (h_{11}h_{21} + h_{11} + h_{11}X_2(1) + X_1(2)) \bmod 256 \\ &= (h_{11}h_{21} + h_{11} + C^0(2)) \bmod 256 \end{aligned}$$

  Thus, h_{21} can be determined because h_{11} is known.
- Step 3. Recover plain images by using the equivalent keys:
  With Algorithm 1, the attackers can only use the equivalent keys ($F_X(i)$, h_{11}, h_{21}) obtained in Step 1 and Step 2 of the cryptanalysis to restore any given cipher image C to the corresponding original plain image P without knowing the key parameters.

To sum up, according to the chosen-plaintext attack method, only two special plain images and their corresponding cipher images are needed to decipher the original algorithm. It is worth pointing out that the above analysis is a gray image of size $H \times W$. For RGB color images of the same size, the method of analyzing and deciphering is similar, and the number of chosen plain images required is also 2. Therefore, the total data complexity for the attack method is $O(2)$.

3.3. Algebraic analysis of VHC-CIES based on chosen-ciphertext attack method

Based on the above alternative method of chosen-plaintext attack, to simplify the equations, let $X_1(i)$ and $X_2(i)$ be $h_{12}K_1(i) + K_2(i)$ and $h_{22}K_1(i) + K_3(i)$, respectively, where $i = 1 \sim L$. Therefore, Eqs. (10) and (11) become:

Algorithm 1: Recovering plain images by using the equivalent keys under CPA.

```
Input: A given cipher image $C$, and the equivalent keys:
       $h_{11}, h_{21}$ and $C^0(i) = F_X(i)$ for $i = 1 \sim L$
Output: Recovered plain image $P$
$P(1) \leftarrow (h_{11}^{-1}(C(1) - C^0(1))) \bmod 256$;
$M(1) \leftarrow P(1)$;
for $i \leftarrow 2$ to $L$ do
    $M(i) \leftarrow (h_{11}^{-1}(C(i) - C^0(i))) \bmod 256$;
    $P(i) \leftarrow (M(i) - h_{21}M(i-1)) \bmod 256$;
end
return $P(i)$ for $i = 1 \sim L$
```

$$\begin{cases} P(1) = \left(h_{11}^{-1}\left(C(1) - X_1(1)\right)\right) \bmod 256 \\ tmp(1) = \left(h_{21}h_{11}^{-1}\left(C(1) - X_1(1)\right) + X_2(1)\right) \bmod 256 \end{cases} \tag{19}$$

Then, Eq. (12) becomes:

$$\begin{cases} P(i) = \left(h_{11}^{-1}\left(C(i) - X_1(i)\right) - tmp(i-1)\right) \bmod 256 \\ tmp(i) = \left(h_{21}h_{11}^{-1}\left(C(i) - X_1(i)\right) + X_2(i)\right) \bmod 256 \end{cases} \tag{20}$$

where $i = 1 \sim L$.

When $i = 2$, Eq. (12) becomes:

$$\begin{aligned} P(2) &= \left(h_{11}^{-1}\left(C(2) - X_1(2)\right) - tmp(1)\right) \bmod 256 \\ &= \left(h_{11}^{-1}\left(C(2) - X_1(2)\right) - (h_{21}h_{11}^{-1}\left(C(1) - X_1(1)\right) + X_2(1))\right) \bmod 256 \\ &= (h_{11}^{-1}(C(2) - h_{21}C(1)) - h_{11}^{-1}X_1(2) + h_{21}h_{11}^{-1}X_1(1) - X_2(1)) \bmod 256 \end{aligned}$$

and

$$\begin{aligned} tmp(2) &= \left(h_{21}h_{11}^{-1}\left(C(2) - X_1(2)\right) + X_2(2)\right) \bmod 256 \\ &= \left(h_{21}h_{11}^{-1}C(2) - h_{21}h_{11}^{-1}X_1(2) + X_2(2)\right) \bmod 256 \end{aligned}$$

Similarly, when $i = 3$, we can get:

$$\begin{aligned} P(3) &= \left(h_{11}^{-1}\left(C(3) - X_1(3)\right) - tmp(2)\right) \bmod 256 \\ &= \left(h_{11}^{-1}\left(C(3) - X_1(3)\right) - (h_{21}h_{11}^{-1}C(2) - h_{21}h_{11}^{-1}X_1(2) + X_2(2))\right) \bmod 256 \\ &= ((h_{11}^{-1}C(3) - h_{21}h_{11}^{-1}C(2)) - h_{11}^{-1}X_1(3) + h_{21}h_{11}^{-1}X_1(2) - X_2(2)) \bmod 256 \end{aligned}$$

$$\begin{aligned} tmp(3) &= \left(h_{21}h_{11}^{-1}\left(C(3) - X_1(3)\right) + X_2(3)\right) \bmod 256 \\ &= (h_{21}h_{11}^{-1}C(3) - h_{21}h_{11}^{-1}X_1(3) + X_2(3)) \bmod 256 \end{aligned}$$

Looking at the above equations, it can be seen that each plaintext pixel value is the algebraic result of some ciphertext pixel streams and key streams. More importantly, the two parts of the ciphertext pixel stream and the key stream can be separated independently. Therefore, we can express the decryption process as:

$$P(i) = (F_C(i) + F'_X(i)) \bmod 256 \tag{21}$$

where $i = 1 \sim L$, $F_C(i)$ and $F'_X(i)$ represent the algebraic results of the cipher image stream and the key stream, respectively. Here, $F_C(i), F'_X(i) \in \mathbb{Z}_{256}$. Therefore, the attacker's function operation on $F_C(\cdot)$ and $F'_X(\cdot)$ is known, which provides an important prerequisite for our cryptography.

3.4. Breaking VHC-CIES by chosen-ciphertext attack

In this section, the method of breaking VHC-CIES based on chosen-ciphertext attack will be described.

In the case of chosen-ciphertext attack, when $i = 1 \sim L$, only h_{11}^{-1}, h_{21} and $F'_X(i)$ are unknown in Eq. (21). We can recover the original plain image from the corresponding cipher image, if the unknowns can be determined. Therefore, the goal is to find the unknowns h_{11}^{-1}, h_{21} and $F'_X(i)$ when $i = 1 \sim L$, which are also equivalent keys. The block diagram of its cryptanalysis is shown in Fig. 2, which is mainly divided into three steps. The steps to decipher VHC-CIES in detail are as follows:

- Step 1. Select the cipher image whose pixel values are all-zero and obtain the corresponding plain image to obtain $F'_X(i)$ for $i = 1 \sim L$:

  $$P^0_{CCA}(i) = (F'_X(i)) \bmod 256 \tag{22}$$

  Here, although the plain image P^0_{CCA} looks very complicated, it is actually known that $i = 1 \sim L$ and $h_{11}, h_{12}, h_{21}, h_{22}$ for $K_1(i), K_2(i), K_3(i)$ composite operation result. For the subsequent solution, two equations are given as follows:

  $$P^0_{CCA}(1) = (-h_{11}^{-1} X_1(1)) \bmod 256$$

  and

  $$P^0_{CCA}(2) = (-h_{11}^{-1} X_1(2) + h_{21} h_{11}^{-1} X_1(1) - X_2(1)) \bmod 256$$

- Step 2. Select the cipher image whose pixel values are all-one and obtain the corresponding plain image to obtain parameters h_{11}^{-1} and h_{21}:
  To determine h_{11}^{-1} and h_{21}, another cipher image with pixel values of 1 is needed. Firstly, choose the image C^1_{CCA} and the corresponding plain image P^1_{CCA}, since $C^1_{CCA} = 1$, we get:

  $$P^1_{CCA}(1) = (h_{11}^{-1} - h_{11}^{-1} X_1(1)) \bmod 256$$

  Therefore, h_{11} can pass through:

  $$h_{11}^{-1} = (P^1_{CCA}(1) - P^0_{CCA}(1)) \bmod 256$$

  Secondly, since $C^1_{CCA}(1) = 1, C^1_{CCA}(2) = 1$, we get:

  $$\begin{aligned} P^1_{CCA}(2) = {} & (h_{11}^{-1}(C^1_{CCA}(2) - h_{21} C^1_{CCA}(1)) - h_{11}^{-1} X_1(2) \\ & + h_{21} h_{11}^{-1} X_1(1) - X_2(1)) \bmod 256 \\ & = (h_{11}^{-1} - h_{11}^{-1} h_{21} - h_{11}^{-1} X_1(2) + h_{21} h_{11}^{-1} X_1(1) - X_2(1)) \bmod 256 \\ & = (h_{11}^{-1} - h_{11}^{-1} h_{21} + P^0_{CCA}(2)) \bmod 256 \end{aligned}$$

  Therefore, h_{21} can be determined, which can be given by the following formula:

  $$h_{21} = (-h_{11}(P^1_{CAA}(2) - P^0_{CAA}(2) - h_{11}^{-1})) \bmod 256$$

- Step 3. Recover plain images by using the equivalent keys $F'_X(i)$, ${h_{11}}^{-1}$ and h_{21}:
  With Algorithm 2, the attackers can only use the equivalent keys $(F'_X(i), {h_{11}}^{-1}, h_{21})$ obtained in Step 1 and Step 2 of the cryptanalysis to restore any given cipher image to the corresponding original plain image without knowing the key parameters.

Algorithm 2: Recovering plain images by using the equivalent keys under CCA.

```
Input: A given cipher image $C$, and the equivalent keys:
       $h_{11}^{-1}, h_{21}$ and $P^0_{CCA}(i) = F'_X(i)$ for $i = 1 \sim L$
Output: Recovered plain image $P$
$P(1) \leftarrow (h_{11}^{-1} C(1) + P^0_{CCA}(1)) \bmod 256$;
$M'(1) \leftarrow h_{11}^{-1} h_{21} C(1)$;
for $i \leftarrow 2$ to $L$ do
    $M'(i) \leftarrow (h_{11}^{-1} h_{21} C(i)) \bmod 256$;
    $P(i) \leftarrow (h_{11}^{-1} C(i) - M'(i-1) + P^0_{CCA}(i)) \bmod 256$;
end
return $P(i)$ for $i = 1 \sim L$
```

To sum up, according to the chosen-ciphertext attack method, only two special cipher images and their corresponding plain images are needed to decipher the original algorithm. It is worth pointing out that the above analysis is a gray image of size $H \times W$. For RGB color images with the same size, the method of analyzing and deciphering is similar, and the number of chosen cipher images required is also 2. Therefore, the total data complexity for the attack method is $O(2)$.

4. Experimental simulation and verification

4.1. Experimental simulation of chosen-plaintext attack method

To verify the effectiveness of the attack method, some experiments are carried out. The key parameters selected in the experiment are exactly the same as the Essaid et al. (2019). Specifically, the six secret keys are: $x_0 = 0.75147854321781$, $y_0 = 0.92791237172793$, $z_0 = 0.61247892775319$, $\mu = 3.98745632101279$, $r_1 = 0.14785214785423$ and $r_2 = 0.61247892775319$. The experimental results are shown in Table 1 and Fig. 9. It can be seen that this attack method can effectively decipher VHC-CIES.

- Case 1 Break VHC-CIES using images of size 2 × 2 × 3:
  Firstly, according to Step 1 in Section 3.2, select the plain image I^0 shown in Fig. 3(a) whose pixel value is zero and obtain the corresponding cipher image C_0 as shown in Fig. 3(c). Their corresponding histograms are shown in Fig. 3(b) and Fig. 3(d) respectively. At the same time, their corresponding RGB numerical matrix are:

  $$\boldsymbol{IR}^0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}; \boldsymbol{IG}^0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}; \boldsymbol{IB}^0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

  $$\boldsymbol{CR}^0 = \begin{bmatrix} 206 & 76 \\ 35 & 133 \end{bmatrix}; \boldsymbol{CG}^0 = \begin{bmatrix} 22 & 156 \\ 26 & 77 \end{bmatrix}; \boldsymbol{CB}^0 = \begin{bmatrix} 113 & 178 \\ 19 & 54 \end{bmatrix}$$

  Secondly, according to Step 2 in Section 3.2, select the plain image I^1 shown in Fig. 4(a) whose pixel value is all one, and obtain the corresponding cipher image C^1 shown in Fig. 4(c). Their matrix values are:

  $$\boldsymbol{IR}^1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}; \boldsymbol{IG}^1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}; \boldsymbol{IB}^1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

  $$\boldsymbol{CR}^1 = \begin{bmatrix} 69 & 13 \\ 216 & 186 \end{bmatrix}; \boldsymbol{CG}^1 = \begin{bmatrix} 147 & 129 \\ 79 & 130 \end{bmatrix}; \boldsymbol{CB}^1 = \begin{bmatrix} 198 & 167 \\ 72 & 107 \end{bmatrix}$$

  Then, we got $h_{11} = 119$ and $h_{21} = 134$.
  Finally, based on Algorithm 1, use the equivalent keys to recover the plain image I shown in Fig. 5(c) from the cipher image C shown in Fig. 5(a).
- Case 2 Break VHC-CIES with "Lenna" of size 256 × 256 × 3:
  Firstly, according to Step 1 of Section 3.2, select the all zero plain image I^0 shown in Fig. 6(a) and temporarily use the encryption machine of VHC-CIES, and then obtain the corresponding cipher

Table 1
The time required to break VHC-CIES with the chosen-plaintext attack method (unit: seconds).

Image	Type	Size	Encryption time	Breaking time	Data complexity
Fig. 5(c)	RGB Image	$2 \times 2 \times 3$	0.0094	0.0122	$O(2)$
Fig. 8(c)	RGB Image	$256 \times 256 \times 3$	0.3150	0.6020	$O(2)$
Fig. 9(b)	RGB Image	$374 \times 500 \times 3$	1.3917	1.6804	$O(2)$
Fig. 9(d)	RGB Image	$424 \times 640 \times 3$	1.1435	2.2627	$O(2)$
Fig. 9(f)	RGB Image	$1192 \times 690 \times 3$	3.3734	7.1176	$O(2)$

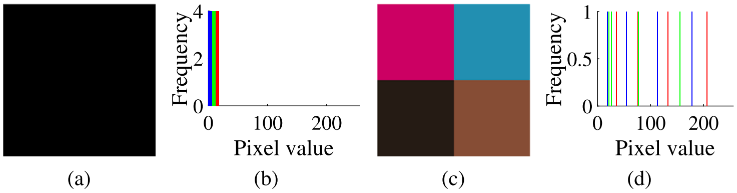

Fig. 3. The all-zero chosen image I^0 and its corresponding cipher image C^0 of size 2 × 2 × 3: (a) I^0; (b) Histogram of I^0; (c) C^0; (d) Histogram of C^0.

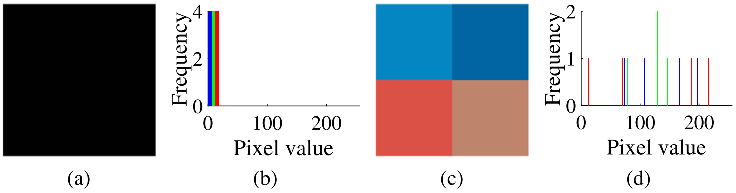

Fig. 4. The all-one chosen image and its corresponding cipher image C^1 of size 2 × 2 × 3: (a) I^1; (b) Histogram of I^1; (c) C^1; (d) Histogram of C^1.

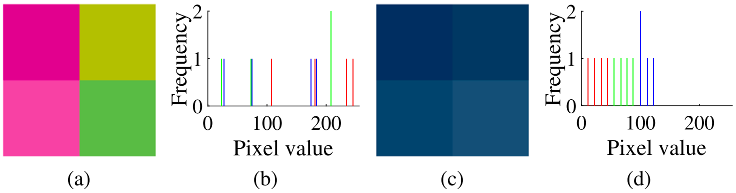

Fig. 5. A target cipher image, original plain image and their histograms of size 2 × 2 × 3: (a) A target cipher image C; (b) Histogram of C; (c) Its plain image I; (d) Histogram of I.

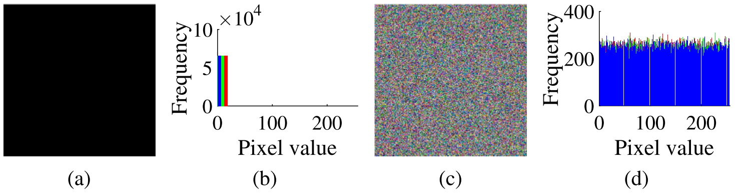

Fig. 6. The all-zero chosen plain image I^0 and its corresponding cipher image of size 256 × 256 × 3: (a) I^0; (b) Histogram of I^0; (c) C^0; (d) Histogram of C^0.

image C^0 shown in Fig. 6(c). Their corresponding histograms are shown in Figs. 6(b) and 6(d).

Secondly, according to Step 2 in Section 3.3, select the plain image I^1 shown in Fig. 7(a) whose pixel value is all one, and obtain the corresponding cipher image C^1 shown in Fig. 7(c). Then, we can get $h_1 = 31$, $h_{21} = 204$.

Finally, based on Algorithm 1, recover the plain image I shown in Fig. 8(c) from the image C shown in Fig. 8(a) with the equivalent keys.

To demonstrate the effectiveness and practicality of chosen-plaintext attack, we also chose other images for testing. The experimental results are shown in Table 1 and Fig. 9. It can be seen that in the experimental environment where we conducted the tests, for breaking a 256 × 256 × 3 sized color image, the breaking time is 0.6020 s, which is only less than twice the encryption time 0.3150 s of the original algorithm, and the proposed attack method can effectively break the VHC-CIES. Last but not least, we verified the data complexity required for the attack, as described in Section 3.2, the total data complexity required to crack VHC-CIES is $O(2)$.

4.2. Experimental simulation of chosen-ciphertext attack method

Similarly, VHC-CIES is deciphered by the chosen-ciphertext attack method proposed in Section 3.4. The size of the given cipher image

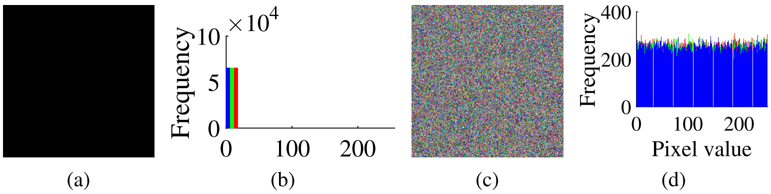

Fig. 7. The all-one chosen plain image I^1 and its corresponding cipher image C^1 of size 256 × 256 × 3: (a) I^1; (b) Histogram of I^1; (c) C; (d) Histogram of C^1.

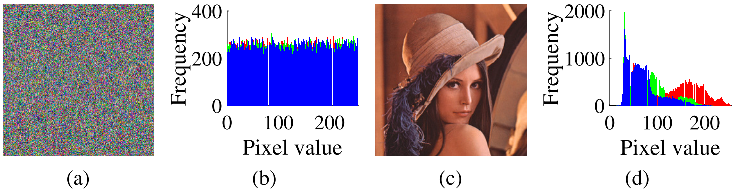

Fig. 8. The cipher image, the original plain image of "Lenna" and their histograms of size 256 × 256 × 3: (a) The cipher image C; (b) Histogram of C; (c) Its plain image I; (d) Histogram of I.

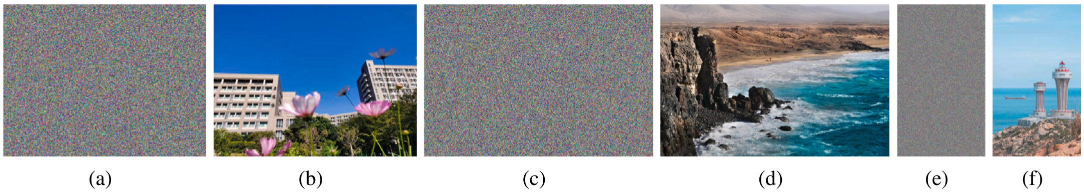

Fig. 9. The experimental results using the chosen-plaintext attack method: (a) 1# cipher image; (b) 1# plain image; (c) 2# cipher image; (d) 2# plain image; (e) 3# cipher image; (f) 3# plain image.

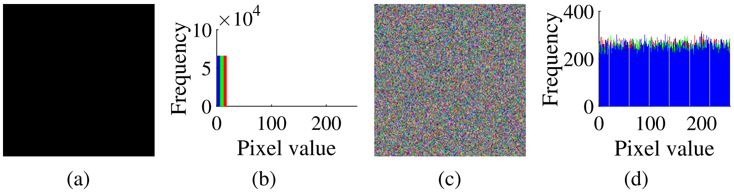

Fig. 10. The all-zero chosen cipher image C^0_{CCA} and its corresponding plain image I^0_{CCA} of size 256 × 256 × 3: (a) Chosen cipher image C^0_{CCA}; (b) Histogram of C^0_{CCA}; (c) Plain image I^0_{CCA}; (d) Histogram of I^0_{CCA}.

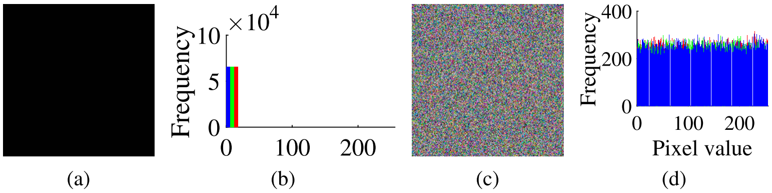

Fig. 11. The all-one chosen cipher image C^1_{CCA} and its corresponding plain image I^1_{CCA} of size 256 × 256 × 3: (a) Chosen cipher image C^1_{CCA}; (b) Histogram of C^1_{CCA}; (c) Plain image I^1_{CCA}; (d) Histogram of I^1_{CCA}.

is 256 × 256 × 3. First of all, based on Step 1 in Section 3.4, we select the all-zero cipher image C^0_{CCA}, which is shown in Fig. 10(a) and temporarily use the VHC-CIES decryption machine, then get the corresponding plain image P^0_{CCA}, as shown in Fig. 10(c). Their corresponding histograms are shown in Fig. 10(b) and 10(d), respectively.

Secondly, according to Step 2 in Section 3.4, the cipher image C^1_{CCA} with pixel values of one shown in Fig. 11(a) is selected to obtain the corresponding plain image C^1_{CCA} shown in Fig. 11(c). Then, we can get $h^{-1}_{11} = 71, h_{21} = 134$.

Finally, based on Algorithm 2, the equivalent keys are used to restore the plain image I shown in Fig. 12(c) from image C shown in Fig. 12(a).

In order to demonstrate the effectiveness and practicality of the chosen-ciphertext attack, we also employed additional images for testing purposes. The experimental results are presented in Table 2 and

Table 2
The time required to chosen-plaintext attack to break VHC-CIES (unit: seconds).

Image name	Type	Size	Decryption time	Breaking time	Data complexity
Fig. 12(c)	RGB Image	$256 \times 256 \times 3$	0.2621	0.9643	$O(2)$
Fig. 13(b)	RGB Image	$1416 \times 690 \times 3$	3.6788	8.0757	$O(2)$
Fig. 13(d)	RGB Image	$350 \times 680 \times 3$	0.8965	1.9566	$O(2)$
Fig. 13(f)	RGB Image	$267 \times 512 \times 3$	0.5398	1.1355	$O(2)$

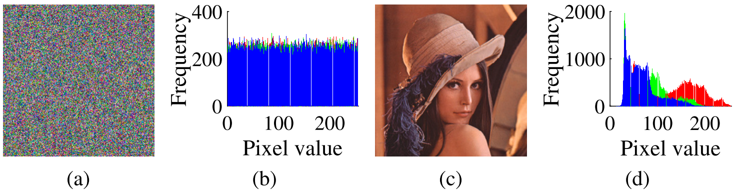

Fig. 12. The cipher image, the original image of “Lenna” and their histograms of size 256 × 256 × 3: (a) Cipher image C; (b) Histogram of C; (c) Plain image I; (d) Histogram of I.

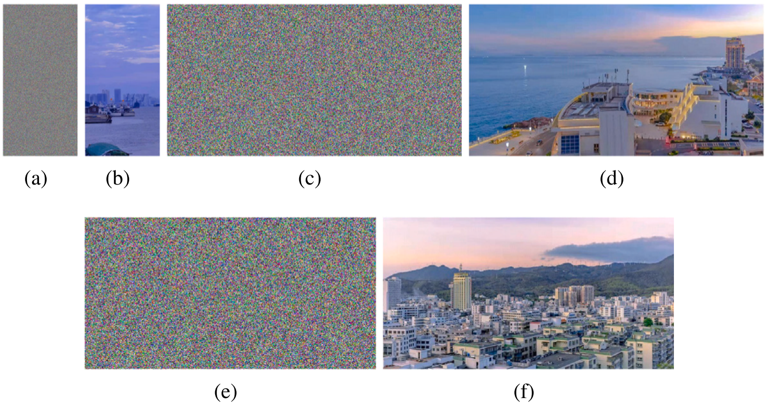

Fig. 13. The experimental results using the chosen-Ciphertext attack method: (a) Cipher image of “Ship”; (b) Plain image “Ship”; (c) Cipher image “City1”; (d) Plain image of “City1”; (e) Cipher image of “City2”; (f) Plain image of “City2”.

Fig. 13. It can be observed that, within our testing environment, breaking a $256 \times 256 \times 3$ color image only takes 0.9634 s. Furthermore, the proposed attack method remains effective in breaking VHC-CIES for rectangular images of varying dimensions. This highlights the practical feasibility of the attack approach outlined in this paper.

Last but not least, we validate the data complexity required for the attack. As mentioned in Section 3.4, all the total data complexity required to break VHC-CIES is $O(2)$.

5. Suggestions for improvement

According to Sections 3 and 4, the target VHC-CIES is insecure against both chosen-plaintext attack and chosen-ciphertext attack, and the computational and data complexity required for the attack is low. In order to improve its security, the flowchart of security enhancement strategy based on VHC-CIES is given in Fig. 14. The main recommendations for security enhancements are as follows:

(1) Ensuring the legitimacy and effectiveness of the secret key. In VHC-CIES, due to design flaws, there is an equivalent key. In order to avoid this situation, one of the feasible measures is to associate the generation of chaotic sequences with the encryption process to enhance dynamics and randomness. In addition, attention should be paid to avoid defects such as invalid keys and weak keys (Wen & Yu, 2019).

(2) Adopting a more scientific and reasonable algorithm structure. From the perspective of algorithm structure, VHC-CIES belongs to pure diffusion model. The mainstream structure for image encryption is permutation-diffusion, which is designed to enhance the confusion and diffusion effects. Due to the lack of permutation in VHC-CIES, the confusion effect of the algorithm is weak and vulnerable to attack (Wen et al., 2021). Moreover, mechanisms such as plaintext association and ciphertext feedback can effectively resist attacks (Wen, Lin et al., 2023).

(3) Increasing the number of encryption rounds under the premise of efficiency. In the case of ensuring the efficiency of the algorithm, the number of encryption rounds of the image chaotic encryption algorithm can be considered to increase moderately to improve security (Wen, Chen et al., 2023). In general, increasing the number of encryption rounds can significantly improve the confusion and diffusion of encryption algorithms and the avalanche effect, thereby improving the ability to resist cryptographic attacks.

(4) Introducing more cryptanalysis methods to evaluate its security. At present, image chaotic cryptography mainly uses statistical analysis results to prove its security, and lacks security assessment at the level of cryptanalysis (Wen & Lin, 2023b). In fact, in addition to the common cryptanalysis methods introduced in Section 3, there are many cryptographic attack methods that are worth analyzing to evaluate the security of the algorithm (Lin et al., 2018).

6. Conclusion

In this paper, we analyze a chaotic image encryption scheme named VHC-CIES based on a variant of the Hill cipher. After careful cryptanalysis, it is found that although VHC-CIES is based on the Hill cipher and its iterative module is more complicated, which makes it more difficult for attackers, it can still be attacked due to the inherent security defects.

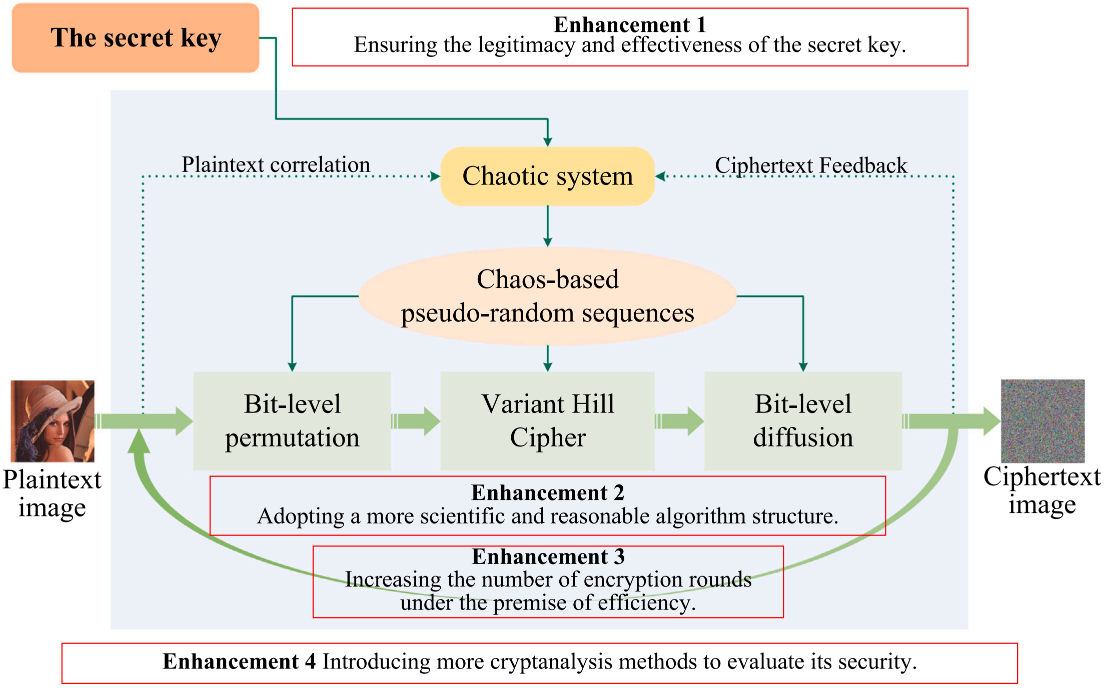
The secret key
Enhancement 1
Ensuring the legitimacy and effectiveness of the secret key.
Plaintext correlation
Chaotic system
Ciphertext Feedback
Chaos-based pseudo-random sequences
Plaintext image
Bit-level permutation
Variant Hill Cipher
Bit-level diffusion
Ciphertext image
Enhancement 2
Adopting a more scientific and reasonable algorithm structure.
Enhancement 3
Increasing the number of encryption rounds under the premise of efficiency.
Enhancement 4 Introducing more cryptanalysis methods to evaluate its security.

Fig. 14. The flowchart of security enhancement strategy based on VHC-CIES.

Specifically, due to the existence of an equivalent key in VHC-CIES, the parameters of the Hill cipher and the encrypted sequences can be accurately determined. This means that the attacker can use these defects to attack the cryptosystem. Based on this, we respectively propose a chosen-plaintext attack and a chosen-ciphertext attack to break VHC-CIES. Both theoretical analysis and experimental results support that VHC-CIES can be deciphered by our attack methods with low computational and data complexity. In fact, the idea of cryptanalysis in this paper may only be applicable to several similar algorithms. Moreover, the study of cryptanalysis is far less than the study of cipher design at present. Therefore, in the future work, we will try to perform cryptanalysis on more complex chaos-based cryptosystems, and strive to condense the universal security criteria that chaotic image encryption algorithms should follow from the cryptanalysis results of each single target algorithm, so as to lay a theoretical foundation for proposing security algorithms with practical security significance.

CRediT authorship contribution statement

Heping Wen: Supervision, Project administration, Funding acquisition, Resources, Writing – original draft, Writing – review & editing. **Yiting Lin:** Conceptualization, Methodology, Software, Formal analysis, Writing – original draft, Writing – review & editing. **Lincheng Yang:** Writing – review & editing. **Ruiting Chen:** Data curation, Investigation, Visualization, 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.

Data availability

Data will be made available on request.

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

Alawida, M., Teh, J. S., & Alshoura, W. H. (2023). A new image encryption algorithm based on DNA state machine for UAV data encryption. *Drones*, *7*(1), 38.

Alawida, M., Teh, J. S., Mehmood, A., Shoufan, A., & Alshoura, W. H. (2022). A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8136–8151.

Bao, B., Wang, Z., Hua, Z., Chen, M., & Bao, H. (2023). Regime transition and multi-scroll hyperchaos in a discrete neuron model. *Nonlinear Dynamics*, *111*(14), 13499–13512.

Cao, C., Cen, Z., Feng, X., Wang, Z., & Zhu, Y. (2022). Straightforward guess and determine analysis based on genetic algorithm. *Journal of Systems Science and Complexity*, *35*(5), 1988–2003.

Chai, X., Fu, J., Gan, Z., Lu, Y., Zhang, Y., & Han, D. (2023). Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission. *IEEE Internet of Things Journal*, *10*(8), 7380–7392.

Chai, X., Wang, Y., Chen, X., Gan, Z., & Zhang, Y. (2022). TPE-GAN: Thumbnail preserving encryption based on GAN with key. *IEEE Signal Processing Letters*, *29*, 972–976.

Chen, L., Li, C., & Li, C. (2022). Security measurement of a medical communication scheme based on chaos and DNA coding. *Journal of Visual Communication and Image Representation*, *83*, Article 103424.

Chen, X., Mou, J., Cao, Y., Yan, H., & Jahanshahi, H. (2023). A chaotic color image encryption scheme based on improved Arnold scrambling and dynamic DNA encoding. *Multimedia Tools and Applications*.

Ding, Y., Liu, W., Wang, H., & Sun, K. (2023). A new class of discrete modular memristors and application in chaotic systems. *The European Physical Journal Plus*, *138*(7).

Erkan, U., Toktas, A., Toktas, F., & Alenezi, F. (2022). 2D eπ -map for image encryption. *Information Sciences*, *589*, 770–789.

Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, A. (2019). Image encryption scheme based on a new secure variant of Hill Cipher and 1D chaotic maps. *Journal of Information Security and Applications*, *47*, 173–187.

Feng, W., Qin, Z., Zhang, J., & Ahmad, M. (2021). Cryptanalysis and improvement of the image encryption scheme based on feistel network and dynamic DNA encoding. *IEEE Access*, *9*, 145459–145470.

Gao, Z., Wu, Q., Liao, L., Su, B., Gao, X., Fu, S., Li, Z., Wang, Y., & Qin, Y. (2022). Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high speed secure optical communication. *Optics Express*, *30*(17), 31209.

Ghazanfaripour, H., & Broumandnia, A. (2020). Designing a digital image encryption scheme using chaotic maps with prime modular. *Optics and Laser Technology*, *131*, Article 106339.

Hraoui, S., Gmira, F., Abbou, M., Oulidi, A., & Jarjar, A. (2019). A new cryptosystem of color image using a dynamic-chaos Hill Cipher algorithm. *Procedia Computer Science*, *148*, 399–408.

Hua, Z., Liu, X., Zheng, Y., Yi, S., & Zhang, Y. (2023). Reversible data hiding over encrypted images via preprocessing-free matrix secret sharing. *IEEE Transactions on Circuits and Systems for Video Technology*, 1.

Jiang, Z., & Ding, Q. (2023). Second-order side-channel analysis based on orthogonal transform nonlinear regression. *Entropy*, *25*(3), 505.

Jiang, Q., Yu, S., & Wang, Q. (2023). Cryptanalysis of an image encryption algorithm based on two-dimensional hyperchaotic map. *Entropy*, *25*(3), 395.

Jiang, N., Zhao, A., Liu, S., Zhang, Y., Peng, J., & Qiu, K. (2020). Injection-locking chaos synchronization and communication in closed-loop semiconductor lasers subject to phase-conjugate feedback. *Optics Express*, *28*(7), 9477.

Kalpana, J., & Murali, P. (2015). An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos. *Optik*, *126*(24), 5703–5709.

Lai, Q., Hu, G., Erkan, U., & Toktas, A. (2023). A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Systems with Applications*, *213*, Article 118845.

Lai, Q., Zhang, H., Kuate, P. D. K., Xu, G., & Zhao, X.-W. (2022). Analysis and implementation of no-equilibrium chaotic system with application in image encryption. *Applied Intelligence*, *52*(10), 11448–11471.

Li, H., Yu, S., Feng, W., Chen, Y., Zhang, J., Qin, Z., Zhu, Z., & Wozniak, M. (2023). Exploiting dynamic vector-level operations and a 2D-enhanced logistic modular map for efficient chaotic image encryption. *Entropy*, *25*(8), 1147.

Liang, X., Zhang, C., Luo, Y., Wang, X., & Qiu, K. (2023). Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion. *Journal of Lightwave Technology*, *41*(6), 1619–1625.

Lin, Z., Yu, S., Feng, X., & Lü, J. (2018). Cryptanalysis of a chaotic stream cipher and its improved scheme. *International Journal of Bifurcation and Chaos*, *28*(07), Article 1850086.

Liu, S., Li, C., & Hu, Q. (2022). Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE MultiMedia*, *29*(1), 74–84.

Liu, W., Sun, K., He, S., & Wang, H. (2023). The parallel chaotification map and its application. *IEEE Transactions on Circuits and Systems. I. Regular Papers*, 1–10.

Liu, X., Sun, K., Wang, H., & He, S. (2023). A class of novel discrete memristive chaotic map. *Chaos, Solitons & Fractals*, *174*, Article 113791.

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, *20*(2), 130–141.

Lu, D., Li, M., Liao, Y., Tao, G., & Cai, H. (2023). Verifiable privacy-preserving queries on multi-source dynamic DNA datasets. *IEEE Transactions on Cloud Computing*, *11*(2), 1927–1939.

Lu, X., Xie, E. Y., & Li, C. (2023). Periodicity analysis of logistic map over ring $\mathbb{Z}_{3^n}$. *International Journal of Bifurcation and Chaos*, *33*(5), Article 2350063.

Luo, Y., Wang, F., Xu, S., Zhang, S., Li, L., Su, M., & Liu, J. (2022). CONCEAL: A robust dual-color image watermarking scheme. *Expert Systems with Applications*, *208*, Article 118133.

Luo, Y., Zhang, C., Wang, X., Liang, X., & Qiu, K. (2023). Robust key update with controllable accuracy using support vector machine for secure OFDMA-PON. *Journal of Lightwave Technology*, *41*(14), 4663–4671.

Ma, Y., Li, C., & Ou, B. (2020). Cryptanalysis of an image block encryption algorithm based on chaotic maps. *Journal of Information Security and Applications*, *54*, Article 102566.

Pak, C., An, K., Jang, P., Kim, J., & Kim, S. (2018). A novel bit-level color image encryption using improved 1D chaotic map. *Multimedia Tools and Applications*, *78*(9), 12027–12042.

Su, Y., Wang, X., Xu, M., Zou, C., & Liu, H. (2023). A three-dimensional (3D) space permutation and diffusion technique for chaotic image encryption using merkel tree and DNA code. *Sensing and Imaging*, *24*(1).

Tang, Z., Chai, X., Lu, Y., Wang, B., & Tan, Y. (2023). An end-to-end screen shooting resilient blind watermarking scheme for medical images. *Journal of Information Security and Applications*, *76*, Article 103547.

Teng, L., Wang, X., Yang, F., & Xian, Y. (2021). Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. *Nonlinear Dynamics*, *105*(2), 1859–1876.

Wang, X., Liu, C., & Jiang, D. (2022). A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. *Expert Systems with Applications*, *209*, Article 118426.

Wen, H., Chen, R., Yang, J., Zheng, T., Wu, J., Lin, W., Jian, H., Lin, Y., Ma, L., Liu, Z., & Zhang, C. (2023). Security analysis of a color image encryption based on bit-level and chaotic map. *Multimedia Tools and Applications*.

Wen, H., Feng, Z., Bai, C., Lin, Y., Zhang, X., & Feng, W. (2024). Frequency-domain image encryption based on IWT and 3D S-box. *Physica Scripta*.

Wen, H., Huang, Y., & Lin, Y. (2023). High-quality color image compression-encryption using chaos and block permutation. *Journal of King Saud University - Computer and Information Sciences*, *35*(8), Article 101660.

Wen, H., Kang, S., Wu, Z., Lin, Y., & Huang, Y. (2023). Dynamic RNA coding color image Cipher based on chain feedback structure. *Mathematics*, *11*(14), 3133.

Wen, H., & Lin, Y. (2023a). Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. *Expert Systems with Applications*, *237*, Article 121514.

Wen, H., & Lin, Y. (2023b). Cryptanalyzing an image Cipher using multiple chaos and DNA operations. *Journal of King Saud University - Computer and Information Sciences*, *35*(7), Article 101612.

Wen, H., Lin, Y., & Feng, Z. (2024). Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps. *Engineering Science and Technology, an International Journal*, *51*, Article 101634.

Wen, H., Lin, Y., Kang, S., Zhang, X., & Zou, K. (2023). Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion. *iScience*, *27*(1), Article 108610.

Wen, H., Xie, Z., Wu, Z., Lin, Y., & Feng, W. (2024). Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography. *Journal of King Saud University - Computer and Information Sciences*, *36*(1), Article 101871.

Wen, H., & Yu, S. (2019). Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. *The European Physical Journal Plus*, *134*(7).

Wen, H., Zhang, C., Huang, L., Ke, J., & Xiong, D. (2021). Security analysis of a color image encryption algorithm using a fractional-order chaos. *Entropy*, *23*(2), 258.

Wu, T., Zeng, W., Liu, Y., Song, S., Zhao, L., Chen, C., Zhang, C., & Guo, L. (2023). Secure turbulence-resistant coherent free-space optical communications via chaotic region-optimized probabilistic constellation shaping. *Optics Letters*, *48*(3), 684–687.

Yasser, I., Khalil, A. T., Mohamed, M. A., & Khalifa, F. (2021). A new chaos-based approach for robust image encryption. *Journal of Cybersecurity and Information Management*, 51–64.

Ye, G., Liu, M., Yap, W.-S., & Goi, B.-M. (2023). Reversible image hiding algorithm based on compressive sensing and deep learning. *Nonlinear Dynamics*, *111*(14), 13535–13560.

Zhang, C., Chen, J., & Chen, D. (2022). Cryptanalysis of an image encryption algorithm based on a 2D hyperchaotic map. *Entropy*, *24*(11), 1551.

Zhang, Y.-Q., Huang, H.-F., Wang, X.-Y., & Huang, X.-H. (2021). A secure image encryption scheme based on genetic mutation and MLNCML chaotic system. *Multimedia Tools and Applications*, *80*(13), 19291–19305.

Zhang, Y., Zhou, W., Zhao, R., Zhang, X., & Cao, X. (2022). F-TPE: Flexible thumbnail-preserving encryption based on multi-pixel sum-preserving encryption. *IEEE Transactions on Multimedia*, 1–15.

Zheng, D., & Liang, K. (2020). Chaotic butterfly optimization with optimal multi-key image encryption technique for wireless sensor networks. *Journal of Intelligent Systems and Internet of Things*, 80–92.

Zhou, S., Qiu, Y., Wang, X., & Zhang, Y. (2023). Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. *Nonlinear Dynamics*, *111*(10), 9571–9589.

Zhou, S., Wang, X., & Zhang, Y. (2023). Novel image encryption scheme based on chaotic signals with finite-precision error. *Information Sciences*, *621*, 782–798.

Zou, C., Wang, X., Zhou, C., Xu, S., & Huang, C. (2022). A novel image encryption algorithm based on DNA strand exchange and diffusion. *Applied Mathematics and Computation*, *430*, Article 127291.