

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2021.DOI

Cryptanalysis and Improvement of the Image Encryption Scheme Based on Feistel Network and Dynamic DNA Encoding

WEI FENG¹, (Member, IEEE), ZHENTAO QIN¹, JING ZHANG¹, AND MUSHEER AHMAD²

¹School of Mathematics and Computer Science, Panzhihua University, Panzhihua 617000, China

²Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

Corresponding authors: Zhentao Qin (qinzhentaovip@126.com) and Musheer Ahmad (musheer.cse@gmail.com)

This work was supported in part by the Program of Science and Technology Center of Ministry of Education of China under Grant 2018A0105, in part by the Natural Science Key Project of the Education Department of Sichuan Province under Grant 18ZA0288, in part by the Guiding Science and Technology Plan Project of Panzhihua City under Grant 2019ZD-G-18 and 2020ZD-S-40, and in part by the Doctoral Research Startup Foundation of Panzhihua University under Grant 2020DOC019.

ABSTRACT In order to improve the security and efficiency of image encryption, many researchers have continuously proposed new image encryption schemes in recent years. However, these image encryption schemes have not been fully analyzed and evaluated. In this paper, a newly reported image encryption scheme based on Feistel network and dynamic Deoxyribonucleic Acid (DNA) encoding is deeply and comprehensively investigated. This encryption scheme mainly adopts four encryption steps to encrypt the plain image, which are Generation of chaotic sequences, Hill encryption, Feistel network and Pixel diffusion. Our analyses show that there are some problems in the secret key design and encryption process of this encryption scheme. After pointing out and analyzing these problems, we have made several necessary improvements to this encryption scheme and proposed the corresponding chosen-plaintext attack algorithm. The subsequent simulation tests and analyses have confirmed the effectiveness and feasibility of the proposed attack algorithm. Finally, for the problems in this encryption scheme and some current image encryption schemes, improvement suggestions are presented to provide references for the designers of future image encryption schemes.

INDEX TERMS Chosen-plaintext attack, cryptanalysis, DNA sequence operation, diffusion, image encryption, scrambling, substitution.

I. INTRODUCTION

NOWADAYS, digital images are widely used because they can convey information vividly and intuitively. In order to ensure commercial security, military security, privacy protection and so on, people hope to provide secure and efficient protection for digital images [1], [2]. As we know, among various protection technologies, image encryption is the most convenient and effective one. The encrypted image looks similar to a noisy image. Without the correct secret key, no one can obtain any valuable information from it. However, image data has many salient features that are different from

text data, such as large amount of data, high information redundancy, and strong correlation between adjacent pixels. Consequently, in many application scenarios, traditional encryption schemes such as Data Encryption Standard (DES) cannot well meet the requirements of protecting image data [3], [4]. At present, image encryption is receiving more and more attention from researchers, who are committed to using new technologies and methods to improve the security and efficiency of image encryption [5]–[33]. Among these new technologies and methods, chaotic systems and Deoxyribonucleic Acid (DNA) computing have been favored

by many researchers [5], [6], [8], [9], [12], [13], [16]–[19], [21], [24], [29].

Since Lorenz [34] discovered the first chaotic attractor in 1963, chaotic systems have now been widely used [3], [4], [35]–[38]. As a deterministic pseudo-random and nonlinear phenomenon, chaotic systems have many characteristics that are very suitable for the design requirements of modern cryptographic systems [24], [29], [39]. For example, the trajectory of a chaotic system is very sensitive to its initial state values and control parameters, even if the two change very slightly, the chaotic system presents a completely different trajectory. This characteristic of chaotic systems makes their initial state values or control parameters very suitable for use as the secret key [40]. Therefore, in recent years, more and more researchers have exploited chaotic systems to design new image encryption schemes. In [41], an image encryption scheme based on the Lorenz chaotic system was proposed. This scheme encrypts the plain image through layered pixel diffusion and non-sequential pixel access mechanism, and its improved permutation process can change the pixel values while scrambling the pixels. Exploiting the Logistic-sine-cosine map, Hua *et al.* [42] proposed an image encryption scheme using four round iterative structure. Their scheme first changes the position of the pixels through high efficiency scrambling, and then shuffles all the pixels through image rotation. Lastly, the final cipher image is obtained through random order substitution. In [43], a chaotic image encryption scheme based on Galois fields was presented. This scheme first uses matrix multiplication operations to diffuse the plain image, and then scrambles the pixels through two chaotic maps. Based on a spatiotemporal chaotic system, Wang *et al.* [44] designed an image encryption scheme with the classic permutation-diffusion structure. Their scheme adopts different strategies to encrypt gray and color images, and has demonstrated good encryption effects through a series of tests. In [45], an image encryption scheme based on high level chaotic maps and improved gravity model was presented. This scheme uses a new chaotic map with excellent chaotic characteristics, and introduces an improved gravity model, thus achieving a very ideal encryption effect. Based on two novel chaotic maps, a color image encryption including two encryption steps of pixel shuffling and pixel diffusion was proposed. Compared with other pixel permutation methods, while reducing the computational overhead, the pixel shuffling adopted by this scheme can better reduce the correlation between adjacent pixels [46].

Because of the remarkable advantages of high parallelism, low power consumption and high information density, DNA computing is increasingly being adopted in image encryption schemes. In [47], an image encryption scheme based on DNA sequence operations was proposed. This scheme performs

scrambling operations at the DNA plane level, and generate the cipher image by performing DNA XOR on scrambled matrices. By combining DNA sequence operations and a Mandelbrot set, Jithin *et al.* [48] presented an image encryption scheme based on Arnold map. In their scheme, a map selection algorithm is designed to select the chaotic map according to image attributes, and the DNA sequence operations are used to enhance the encryption effect. In [49], a multi-image encryption scheme using Algebra-chaos amalgamated random sequence and DNA transform was suggested. This scheme utilizes the Algebra-chaos amalgamated random sequence to replace traditional S-box, and combines DNA transformation and substitution-permutation operations to complete the encryption of the plain image.

Like the designers of image encryption schemes, there are also many researchers dedicated to the cryptanalysis of image encryption schemes [50]–[59]. In [55], a chaotic image encryption scheme based on Latin square was cryptanalyzed. And the equivalent key streams of permutation and diffusion are determined in turn by chosen-plaintext attacks. For an image encryption scheme based on a discrete chaotic map and DNA encoding, Chen *et al.* [56] simplified it to a substitution and permutation structure, and then broke it by a chosen-plaintext attack algorithm. In [57], the design and structure of a chaotic image encryption scheme for embedded systems was scrutinized. And this image encryption scheme is proved to be weak against differential attacks. Chen *et al.* [58] analyzed and evaluated an image encryption scheme using high-speed scrambling and pixel adaptive diffusion. They find that the encryption scheme does not have the claimed security, and successfully break it by chosen-plaintext attacks. Undoubtedly, for the security, feasibility and practicality problems pointed out in the cryptanalysis works, the designers of image encryption schemes will pay attention to them, so as to avoid the recurrence of similar problems. It can be said that cryptanalysis is an important guarantee for the sound development of image encryption technology. Therefore, in this paper, an Image Encryption Scheme based on Feistel network and Dynamic DNA encoding (IES-FD) is comprehensively analyzed and evaluated, and the security, feasibility and practicality problems in it are pointed out and discussed. Besides, after necessary improvements to IES-FD, a targeted chosen-plaintext attack algorithm is proposed. Without knowing any information about the secret key, the proposed attack algorithm can completely recover the plain image from the cipher image. The contributions of this paper can be summarized as follows.

(1) A newly reported image encryption scheme is comprehensively analyzed and its problems are pointed out and discussed.

(2) Necessary improvements are made to IES-FD, and a

targeted chosen-plaintext attack algorithm is proposed.

(3) The effectiveness and feasibility of the proposed attack algorithm is confirmed by simulation tests and theoretical analyses.

(4) Some common problems existing in current image encryption schemes are listed and analyzed, and several improvement suggestions are given.

The rest of this paper is organized as follows. Section II presents a brief description of IES-FD. In Section III, IES-FD is comprehensively cryptanalyzed, and the identified problems are pointed out and discussed. Section IV describes the necessary improvements made to IES-FD. And the targeted chosen-plaintext attack algorithm is proposed in Section V. In Section VI, simulation tests and theoretical analyses are carried out to verify the effectiveness and feasibility of the proposed attack algorithm. Section VII lists and analyzes some common problems in current image encryption schemes, and puts forward several improvement suggestions. Finally, the conclusion is given in Section VIII.

II. BRIEF DESCRIPTION OF IES-FD

In this section, IES-FD is briefly described. For more information about IES-FD, please refer to the original paper [1]. IES-FD consists of four parts, *Generation of chaotic sequences*, *Hill encryption*, *Feistel network*, and *Pixel diffusion*. Because the symbols in the original paper are inconsistent and irregular, some equations and symbols are adjusted appropriately. Please note that we describe IES-FD as it is. For the security, feasibility, and practicability problems identified in IES-FD, we point out and analyze them in Section III.

A. GENERATION OF CHAOTIC SEQUENCES

For the plain image \mathbf{P} with the size of $M \times N$, use the Keccak algorithm to generate its hash value H . Divide H into 64 bytes, namely h_1, h_2, \dots, h_{64} . Generate the initial state values x_0, y_0, z_0, w_0 of the hyper-chaotic Chen system by using (1) and (2).

$$t_i = ((h_{j+1} \oplus h_{j+2} \oplus h_{j+3}) + h_{j+4} + h_{j+5} + h_{j+6})/256, \quad (1)$$

$$\begin{cases} x_0 = x'_0 + \text{abs}(\text{round}(t_1) - t_1), \\ y_0 = y'_0 + \text{abs}(\text{round}(t_2) - t_2), \\ z_0 = z'_0 + \text{abs}(\text{round}(t_3) - t_3), \\ w_0 = w'_0 + \text{abs}(\text{round}(t_4) - t_4), \end{cases} \quad (2)$$

where $i = 1, 2, 3, 4, j = 6 \times (i - 1)$, \oplus represents bitwise XOR operation, x'_0, y'_0, z'_0, w'_0 are given values, $\text{abs}(\cdot)$ returns the absolute value of the operand, and $\text{round}(\cdot)$ represents rounding up the operand. Input x'_0, y'_0, z'_0, w'_0 into the hyper-chaotic Chen system to generate four chaotic sequences $A^{(1)} = \{a_1^{(1)}, a_2^{(1)}, \dots, a_L^{(1)}\}$, $A^{(2)} = \{a_1^{(2)}, a_2^{(2)}, \dots, a_L^{(2)}\}$, $A^{(3)} =$

$\{a_1^{(3)}, a_2^{(3)}, \dots, a_L^{(3)}\}$, $A^{(4)} = \{a_1^{(4)}, a_2^{(4)}, \dots, a_L^{(4)}\}$. Finally, use (3) to convert $A^{(1)}, A^{(2)}, A^{(3)}, A^{(4)}$ into the sequences $B^{(1)}, B^{(2)}, B^{(3)}, B^{(4)}$, which are required for encryption.

$$\begin{cases} B^{(1)} = A^{(1)} - \text{fix}(A^{(1)}), \\ B^{(2)} = A^{(2)} - \text{fix}(A^{(2)}), \\ B^{(3)} = A^{(3)} - \text{fix}(A^{(3)}), \\ B^{(4)} = \text{fix}(\text{mod}(10^4 \times (A^{(4)} - \text{fix}(A^{(4)})), 256)), \end{cases} \quad (3)$$

where $\text{fix}(\cdot)$ returns the integer part of the operand, $\text{mod}(\cdot, \cdot)$ represents modular operation.

B. HILL ENCRYPTION

Construct $\text{ceil}(M \times N/4)$ Hill encryption matrices, each matrix is a self-inverse matrix obtained as follows. Here, $\text{ceil}(\cdot)$ returns the smallest integer greater than the operand.

(1) Select four elements from $B^{(4)}$ to form a 2×2 matrix

$$\mathbf{X}_{1,1} = \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}.$$

(2) Let $\mathbf{X}_{1,2} = \mathbf{I} - \mathbf{X}_{1,1}$, $\mathbf{X}_{2,1} = \mathbf{I} + \mathbf{X}_{1,1}$, $\mathbf{X}_{2,2} = -\mathbf{X}_{1,1}$, where \mathbf{I} is the 2×2 identity matrix.

(3) Combine $\mathbf{X}_{1,1}$, $\mathbf{X}_{1,2}$, $\mathbf{X}_{2,1}$, and $\mathbf{X}_{2,2}$ into a Hill encryption matrix

$$\mathbf{X} = \begin{bmatrix} \mathbf{X}_{1,1} & \mathbf{X}_{1,2} \\ \mathbf{X}_{2,1} & \mathbf{X}_{2,2} \end{bmatrix}.$$

Divide \mathbf{P} into 4×1 blocks, that is, every four pixels form a block. Then, use the Hill encryption matrices to encrypt these blocks. The encryption method is as follows.

$$\tilde{\mathbf{C}} = \text{mod}(\mathbf{X} * \tilde{\mathbf{P}}, 256), \quad (4)$$

where $\tilde{\mathbf{C}}$ is a 4×1 block obtained after Hill encryption, $*$ denotes matrix multiplication, and $\tilde{\mathbf{P}}$ is a 4×1 plain image block. After performing Hill encryption on all plain image blocks, the intermediate cipher image $\mathbf{C}^{(1)}$ is obtained.

C. FEISTEL NETWORK

As shown in Figure 2 of the original paper, the so-called Feistel network of IES-FD actually iterates the two encryption steps of pixel scrambling and DNA XOR for three rounds. The encryption process of the first round is as follows.

(1) Pixel scrambling: Sort $B^{(1)}$ in ascending order to obtain the index sequence I . Then, pixel scrambling is performed on $\mathbf{C}^{(1)}$ according to I to obtain the scrambled image $\mathbf{C}^{(2)}$.

(2) DNA XOR based on dynamic DNA encoding: Download the specified DNA sequence from the GenBank database and extract $6 \times M \times N$ bases from it. Then, $\mathbf{C}^{(2)}$ is divided into blocks, and every 8 pixels constitute a block. The dynamic DNA encoding is performed on each block. The encoding rule used for each pixel depends on where each pixel is

located. Specifically, the encoding rule $r^{(i,j)}$ of $C_{i,j}^{(2)}$ is defined as follows.

$$r^{(i,j)} = (\text{mod}((i-1) \times N + j, 8)) + 1, \quad (5)$$

where $i = 1, 2, \dots, M$, $j = 1, 2, \dots, N$. The encoded DNA sequences are further divided into two parts, L and R, and DNA XORed with the downloaded bases. Finally, select DNA encoding rule 1 to perform decoding, and restore the decoding result to a matrix form, thereby obtaining the intermediate cipher image $C^{(3)}$.

In the second round of iterations, according to $B^{(2)}$, scramble $C^{(3)}$ to obtain $C^{(4)}$. Then, perform dynamic DNA encoding, DNA XOR and DNA decoding to obtain $C^{(5)}$.

In the third round of iterations, according to $B^{(3)}$, scramble $C^{(5)}$ to obtain $C^{(6)}$, and perform dynamic DNA encoding, DNA XOR and DNA decoding to obtain $C^{(7)}$.

D. PIXEL DIFFUSION

Convert $C^{(7)}$ into the 1D sequence $S = \{s_1, s_2, \dots, s_{M \times N}\}$ in row-major order, and perform pixel diffusion to obtain the intermediate cipher image sequence $\tilde{S} = \{\tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_{M \times N}\}$.

$$\tilde{s}_{i+1} = s_i \oplus \tilde{s}_{i-1}, \quad (6)$$

where $i = 1, 2, \dots, M \times N$ and $\tilde{s}_0 = 127$. Finally, the final cipher image C is obtained through \tilde{S} .

The decryption process of IES-FD is the inverse process of its encryption process, and it is no longer elaborated.

III. CRYPTANALYSIS AND IDENTIFIED PROBLEMS

According to the description of the original paper, IES-FD have no substantial difference in processing different types of images. Therefore, we only discuss its encryption processing for gray images. After careful study of the original paper, we have identified the following security, feasibility, and practicability problems.

A. PROBLEMS RELATED TO SECRET KEY

In terms of the secret key of IES-FD, the problems identified in the original paper and IES-FD are as follows.

(1) *For the secret key of IES-FD, the description in the original paper is vague and inconsistent.* Firstly, in Section 4.1 of the original paper, the hash value of the plain image generated by the Keccak algorithm is described as the secret key. And it is claimed that using the hash value as the secret key can ensure the key space of $2^{512} \approx 10^{154}$. Secondly, in step 7) of the encryption process described in the original paper, the DNA sequence downloaded from the GenBank database is described as the secret key. And this secret key is as long as $6 \times M \times N$. Lastly, in Section 5 and Section 5.1 of the original paper, $\{x'_0, y'_0, z'_0, w'_0\}$ is described as the

secret key, and it is claimed that the key space of 10^{100} can be ensured.

(2) *For the DNA sequence whose data volume exceeds the plain image and needs to be downloaded from a third party, it is not practical and feasible to be used as the secret key.* Obviously, the DNA sequence as long as $6 \times M \times N$ can never be used as the secret key. To encrypt the plain image with the size of $M \times N$, a DNA sequence of length $6 \times M \times N$ should be securely transmitted, which would make the encryption meaningless.

(3) *The claims on the key space proposed in the original paper do not hold.* Firstly, in Section 4.1 of the original paper, it is claimed that using the hash value of the plain image as the secret key can ensure the key space of 2^{512} , thus effectively resisting brute force attacks. But according to (1), it can be judged that the possible values of t_i ($i = 1, 2, 3, 4$) are all $\{0/256, 1/256, 2/256, \dots, 255 \times 4/256\}$. And according to (2), we can further determine that the possible values of $\text{abs}(\text{round}(t_i) - t_i)$ are $\{0/256, 1/256, 2/256, \dots, 128/256\}$. Consequently, using the hash value in the manner of IES-FD can only ensure the key space of $129^4 \approx 2^{28} \approx 10^8$. Obviously, this is not enough to effectively resist brute force attacks. Secondly, in Section 5.1 of the original paper, it is claimed that if the computation precision is 10^{-14} , the key space is 10^{100} . However, the key space using $\{x'_0, y'_0, z'_0, w'_0\}$ as the secret key is much smaller than this value. Even without considering the calculation precision and the value ranges of four chaotic system state values, the number of possible combinations of four 64-bit floating point numbers will not exceed $2^{64 \times 4} \approx 10^{77}$.

(4) *Whether the hash value of the plain image is used as the secret key or not, IES-FD has problems in the use of the hash value.* Firstly, if the hash value is used as the secret key, every time a different image is encrypted, the encryption party must change the secret key and provide it to the decryption party securely. When a large number of images need to be encrypted, such a secret key design is not practical. A well-designed symmetric cryptographic system should not rely on constantly changing secret keys to ensure the security. Secondly, if only the given values $\{x'_0, y'_0, z'_0, w'_0\}$ are used as the secret key, the decryption party cannot complete the decryption just with the secret key.

B. PROBLEMS RELATED TO CHAOTIC SEQUENCES

In terms of the chaotic sequences used by IES-FD, the problems identified in the original paper and IES-FD are as follows.

(1) *The original paper does not give any introduction to the hyper-chaotic Chen system used in IES-FD, and even does not cite the paper that proposed this system.* IES-FD utilizes the chaotic sequences generated by a hyper-chaotic

Chen system to complete image encryption. Actually, since Li *et al.* [60] proposed a hyper-chaotic Chen system in 2005, researchers have successively proposed many different hyper-chaotic Chen systems. In order to analyze and study IES-FD, we adopt the hyper-chaotic Chen system introduced in [61], which is defined as follows.

$$\begin{cases} \dot{x} = r_1(y - x), \\ \dot{y} = r_4x - xz + r_3y - w, \\ \dot{z} = xy - r_2z, \\ \dot{w} = x + r_5, \end{cases} \quad (7)$$

where x, y, z, w are state variables, and r_1, r_2, r_3, r_4, r_5 are system parameters. When $(r_1, r_2, r_3, r_4) = (36, 3, 28, -16)$ and $r_5 \in [-0.7, 0.7]$, this system is hyper-chaotic. Some attractors of the adopted system are shown in Figure 1.

(2) *IES-FD may not be feasible due to insufficient length of $B^{(4)}$.* The lengths of $B^{(1)}, B^{(2)}, B^{(3)}, B^{(4)}$ generated by IES-FD are all L . According to Section 4.5 of the original paper or Section II-C of this paper, IES-FD uses the sort indexes of $B^{(1)}, B^{(2)}, B^{(3)}$ to scramble the intermediate cipher images, so it can be determined that $L = M \times N$. This means that the length of $B^{(4)}$ should also be $M \times N$. However, in step 3) of the encryption process described in the original paper, the number of Hill encryption matrices to be constructed is $\text{ceil}(M \times N/4)$. According to the Hill matrix construction method of IES-FD, the length of $B^{(4)}$ should be $\text{ceil}(M \times N/4) \times 4$. Obviously, when $M \times N$ is not an integer multiple of 4, $M \times N < \text{ceil}(M \times N/4) \times 4$, thus making the Hill encryption of IES-FD infeasible.

C. PROBLEMS RELATED TO HILL ENCRYPTION

In terms of the Hill encryption of IES-FD, the problems identified in the original paper and IES-FD are as follows.

(1) *The plain image may not be divided normally in the way described in IES-FD.* In the process of performing Hill encryption, IES-FD divides the plain image into the blocks with the size of 4×1 . Therefore, when $M \times N$ is not an integer multiple of 4, there is not only the problem of insufficient length of $B^{(4)}$, but also the problem that the plain image cannot be divided normally.

(2) *The encryption effect of Hill encryption performed by IES-FD is poor, and there is the design defect that can be exploited by the attacker.* According to Section 4.3 of the original paper or Section II-B of this paper,

$$\mathbf{X}_{1,2} = \mathbf{I} - \mathbf{X}_{1,1} = \begin{bmatrix} 1 - x_{1,1} & -x_{1,2} \\ -x_{2,1} & 1 - x_{2,2} \end{bmatrix}, \quad (8)$$

$$\mathbf{X}_{2,1} = \mathbf{I} + \mathbf{X}_{1,1} = \begin{bmatrix} 1 + x_{1,1} & x_{1,2} \\ x_{2,1} & 1 + x_{2,2} \end{bmatrix}, \quad (9)$$

$$\mathbf{X}_{2,2} = \mathbf{I} + \mathbf{X}_{1,1} = \begin{bmatrix} -x_{1,1} & -x_{1,2} \\ -x_{2,1} & -x_{2,2} \end{bmatrix}, \quad (10)$$

and

$$\begin{aligned} \mathbf{X} &= \begin{bmatrix} \mathbf{X}_{1,1} & \mathbf{X}_{1,2} \\ \mathbf{X}_{2,1} & \mathbf{X}_{2,2} \end{bmatrix} \\ &= \begin{bmatrix} x_{1,1} & x_{1,2} & 1 - x_{1,1} & -x_{1,2} \\ x_{2,1} & x_{2,2} & -x_{2,1} & 1 - x_{2,2} \\ 1 + x_{1,1} & x_{1,2} & -x_{1,1} & -x_{1,2} \\ x_{2,1} & 1 + x_{2,2} & -x_{2,1} & -x_{2,2} \end{bmatrix}. \end{aligned} \quad (11)$$

So,

$$\begin{aligned} \tilde{\mathbf{C}} &= \text{mod}(\mathbf{X} * \tilde{\mathbf{P}}, 256) \\ &= \text{mod} \left(\begin{bmatrix} x_{1,1} \times (p_1 - p_3) + x_{1,2} \times (p_2 - p_4) + p_3 \\ x_{2,1} \times (p_1 - p_3) + x_{2,2} \times (p_2 - p_4) + p_4 \\ x_{1,1} \times (p_1 - p_3) + x_{1,2} \times (p_2 - p_4) + p_1 \\ x_{2,1} \times (p_1 - p_3) + x_{2,2} \times (p_2 - p_4) + p_2 \end{bmatrix}, 256 \right), \end{aligned} \quad (12)$$

where $\tilde{\mathbf{P}} = [p_1 \ p_2 \ p_3 \ p_4]^T$. As one can see, letting $p_1 = p_3$ and $p_2 = p_4$ can completely invalidate Hill encryption. In other words, for the plain image with single pixel value, Hill encryption has no encryption effect. It is well known that such plain images are often used by the attacker to launch chosen-plaintext attacks [3], [50], [51].

D. PROBLEMS RELATED TO FEISTEL NETWORK

In terms of the Feistel network of IES-FD, the problems identified in the original paper and IES-FD are as follows.

(1) *For the Feistel network of IES-FD, the description in the original paper is vague and inconsistent.* Firstly, the iterative structure of DES is introduced in Section 3.1 of the original paper, but the specific iterative structure of IES-FD is not clearly described. As we know, various cryptographic systems that follow the Feistel structure/network have their own unique iterative structure. For example, the encryption process of each round of RC5 mentioned in the original paper is significantly different from DES. Secondly, there are obvious errors in the iterative structure given in Figure 2 of the original paper. For a Feistel structure/network, the round function F should be part of the iterative structure rather than its input. Besides, according to the description of the original paper, the DNA XOR operation should not be the input of the round function but the round function itself. Combining the descriptions in Section 4.5 and Section 6 of the original paper, the iterative structure of IES-FD should be as shown in Figure 2.

(2) *The input image may not be divided normally in the way described in IES-FD.* In each iteration of Feistel network, the input image is divided into the blocks with the length of 8. Therefore, when $M \times N$ is not an integer multiple of 8, there is the problem that the input image cannot be

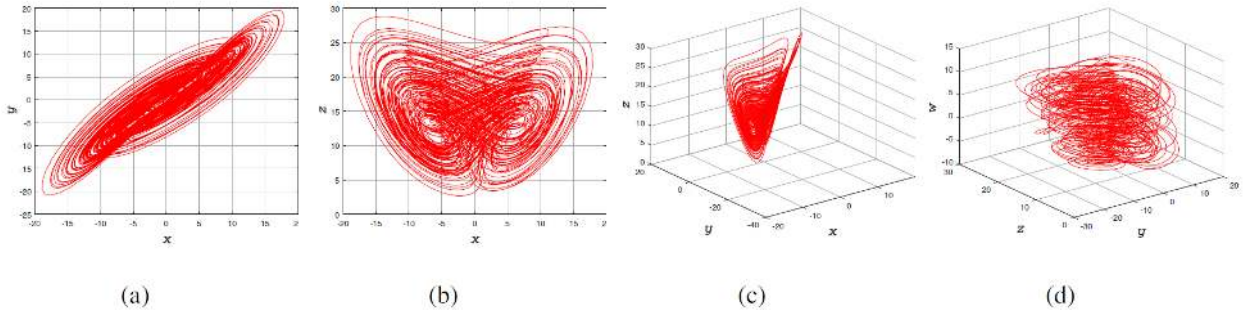


FIGURE 1. Some attractors of adopted hyper-chaotic Chen system: (a) x-y plane; (b) x-z plane; (c) x-y-z plane; (d) y-z-w plane.

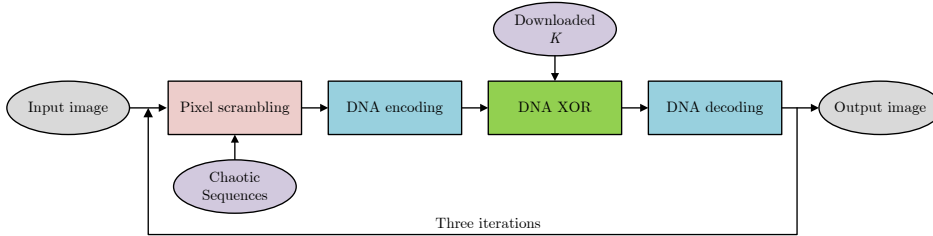


FIGURE 2. Iterative structure of IES-FD.

divided normally.

(3) When processing the input image, the Feistel network of IES-FD needs to rely on a long DNA sequence downloaded from a third party. Such a design not only has the problem pointed out in Section III-A, but also has the problem of feasibility. If the GenBank database becomes unavailable, or the genetic data in it changes, IES-FD will not work properly.

E. PROBLEMS RELATED TO PIXEL DIFFUSION

In terms of the Pixel diffusion of IES-FD, the problems identified in the original paper and IES-FD are as follows.

(1) The Pixel diffusion of IES-FD is not feasible. According to Section 4.4 of the original paper or Section II-D of this paper, obviously, $\tilde{s}_{M \times N+1}$ in (6) does not exist.

(2) Since its encryption effect can be eliminated under the condition of the ciphertext-only attack, the Pixel diffusion of IES-FD has no meaning. For the attacker, \tilde{S} is known, so the attacker can utilize the following simple processing to obtain S .

$$s_i = \tilde{s}_{i+1} \oplus \tilde{s}_{i-1}. \quad (13)$$

IV. IMPROVEMENTS TO IES-FD

Undoubtedly, an image encryption scheme is meaningless if it is not practical and feasible. Therefore, before launching the chosen-plaintext attack, we first make necessary improvements to IES-FD. It is worth noting that our improvements have not weakened the original security of IES-FD. Besides,

to avoid major changes to IES-FD, we do not consider the problems that the plain image and input image cannot be divided normally. In fact, unless the encryption structure of IES-FD is changed, simple pixel filling may cause other feasibility and practicality problems.

(1) In order to solve the problems related to the secret key, a 256-bit binary sequence $K = S_1^{(K)} S_2^{(K)} S_3^{(K)} S_4^{(K)} S_5^{(K)}$ is designed as the secret key. Here,

$$S_1^{(K)} = b_1^{(1)} b_2^{(1)} \dots b_{51}^{(1)},$$

$$S_2^{(K)} = b_1^{(2)} b_2^{(2)} \dots b_{51}^{(2)},$$

$$S_3^{(K)} = b_1^{(3)} b_2^{(3)} \dots b_{51}^{(3)},$$

$$S_4^{(K)} = b_1^{(4)} b_2^{(4)} \dots b_{51}^{(4)},$$

$$S_5^{(K)} = b_1^{(5)} b_2^{(5)} \dots b_{52}^{(5)}.$$

According to the floating-point number representation defined in IEEE 754 [62], K is converted into the initial state value x_0, y_0, z_0, w_0 and system parameter r_5 of the adopted hyper-chaotic Chen system as follows.

$$x_0 = \sum_{i=1}^{51} b_i^{(1)} \times 2^{3-i}, \quad (14)$$

$$y_0 = \sum_{i=1}^{51} b_i^{(2)} \times 2^{3-i}, \quad (15)$$

$$z_0 = \sum_{i=1}^{51} b_i^{(3)} \times 2^{4-i}, \quad (16)$$

$$w_0 = \sum_{i=1}^{51} b_i^{(4)} \times 2^{3-i}, \quad (17)$$

$$r_5 = -0.5 + \sum_{i=1}^{52} b_i^{(5)} \times 2^{-i}. \quad (18)$$

(2) The hyper-chaotic Chen system introduced in [61] is adopted to generate the sequences $B^{(1)}, B^{(2)}, B^{(3)}, B^{(4)}$.

(3) Since it is neither feasible nor practical to adopt the downloaded DNA sequence with the length of $6 \times M \times N$, the DNA sequence required for encryption is generated through $B^{(1)}, B^{(2)}, B^{(3)}$. Specifically,

$$\begin{cases} D^{(1)} = \text{mod}(B^{(1)}, 16), \\ D^{(2)} = \text{mod}(B^{(2)}, 16), \\ D^{(3)} = \text{mod}(B^{(3)}, 16). \end{cases} \quad (19)$$

Using the same encoding rules as the input image, $D^{(i)} (i = 1, 2, 3)$ can be encoded into the DNA sequence required for each iteration.

(4) In fact, the Pixel diffusion of IES-FD is just the single-pixel forward diffusion. Obviously, its correct form is as follows.

$$\tilde{s}_i = s_i \oplus \tilde{s}_{i-1}, \quad (20)$$

where s_i is the element of the input pixel sequence S , \tilde{s}_i is the element of the output pixel sequence \tilde{S} , $i = 1, 2, \dots, M \times N$ and $\tilde{s}_0 = 127$.

V. PROPOSED ATTACK ALGORITHM

Based on the cryptanalysis done in Section III, the specific chosen-plaintext attack algorithm against IES-FD is proposed in this section. For the cipher image \mathbf{C} with the size of $M \times N$, it is known that \mathbf{C} is generated by IES-FD with the unknown secret key K , and the corresponding plain image is \mathbf{P} . As one can see, under the condition of the chosen-plaintext attack, the attacker can arbitrarily choose special plain images and obtain the corresponding cipher images generated by IES-FD with K .

As shown in Figure 3, the step-by-step breaking strategy is adopted to break IES-FD. Specifically, the pixel diffusion effect is first eliminated by Algorithm 1. Then, Algorithm 2 is exploited to obtain the equivalent substitution matrix, so as to eliminate the pixel substitution effect. Finally, the Hill encryption matrices and equivalent scrambling matrix are determined by Algorithm 3, so as to eliminate the pixel scrambling effect and Hill encryption effect. In this way, the plain image can be recovered without knowing the secret key.

According to the original paper or Section II of this paper, one can use the following mathematical model to describe IES-FD.

$$\mathbf{C} = d(f(h(\mathbf{P}, K), K), K), \quad (21)$$

Where $h(\cdot, K)$ represents the Hill encryption performed on the input image under the control of K , $f(\cdot, K)$ represents the Feistel iterations performed on the input image under the control of K , and $d(\cdot, K)$ represents the Pixel diffusion performed on the input image under the control of K . As mentioned in Section III-E, using Algorithm 1, one can simplify IES-FD into the following mathematical model.

$$\mathbf{C}^{(7)} = f(h(\mathbf{P}, K), K), \quad (22)$$

where $\mathbf{C}^{(7)}$ is the intermediate cipher image whose pixel diffusion effect has been eliminated.

Algorithm 1 Eliminate the pixel diffusion effect.

Input: The cipher image \mathbf{C} with the size of $M \times N$, $\tilde{s}_0 = 127$.

- 1: Convert \mathbf{C} into $\tilde{S} = \{\tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_{M \times N}\}$ in row-major order;
- 2: **for** $i = M \times N$ to 1 **do**
- 3: $s_i = \tilde{s}_i \oplus \tilde{s}_{i-1}$;
- 4: **end for**
- 5: Reshape $S = \{s_1, s_2, \dots, s_{M \times N}\}$ into $\mathbf{C}^{(7)}$;

Output: The intermediate cipher image $\mathbf{C}^{(7)}$, whose pixel diffusion effect has been eliminated.

According to Section III-E, one can know that the Hill encryption of IES-FD has no encryption effect on the plain image with single pixel value, which means

$$\hat{\mathbf{P}}^{(i)} = h(\hat{\mathbf{P}}^{(i)}, K), \quad (23)$$

where $\hat{\mathbf{P}}^{(i)}$ is the plain image with single pixel value, $i = 0, 1, 2, \dots, 255$. Then, IES-FD can be further simplified.

$$\hat{\mathbf{C}}^{(i)} = f(h(\hat{\mathbf{P}}^{(i)}, K), K) = f(\hat{\mathbf{P}}^{(i)}, K) \quad (24)$$

where $\hat{\mathbf{C}}^{(i)}$ is the corresponding cipher image of $\hat{\mathbf{P}}^{(i)}$ obtained after encryption processing. In this way, one can use $\hat{\mathbf{P}}^{(i)}$ and its corresponding cipher image $\hat{\mathbf{C}}^{(i)}$ to construct an equivalent substitution matrix, so as to eliminate the substitution effect of $f(\cdot, K)$. Specifically, for $\hat{\mathbf{P}}^{(0)}$ whose pixel values are all 0, convert its corresponding cipher image $\hat{\mathbf{C}}^{(0)}$ into the 1D vector

$$\left[\hat{c}_1^{(0)} \quad \hat{c}_2^{(0)} \quad \dots \quad \hat{c}_{M \times N}^{(0)} \right]$$

in row-first order. Then, add the vector to the equivalent substitution matrix $\bar{\mathbf{M}}^{(f)}$, and make it the first row of $\bar{\mathbf{M}}^{(f)}$. Similarly, for $\hat{\mathbf{P}}^{(i)}$ whose pixel values are all i , convert its corresponding cipher image $\hat{\mathbf{C}}^{(i)}$ into the 1D vector

$$\left[\hat{c}_1^{(i)} \quad \hat{c}_2^{(i)} \quad \dots \quad \hat{c}_{M \times N}^{(i)} \right]$$

in row-first order. Then, add the vector to $\bar{\mathbf{M}}^{(f)}$, and make

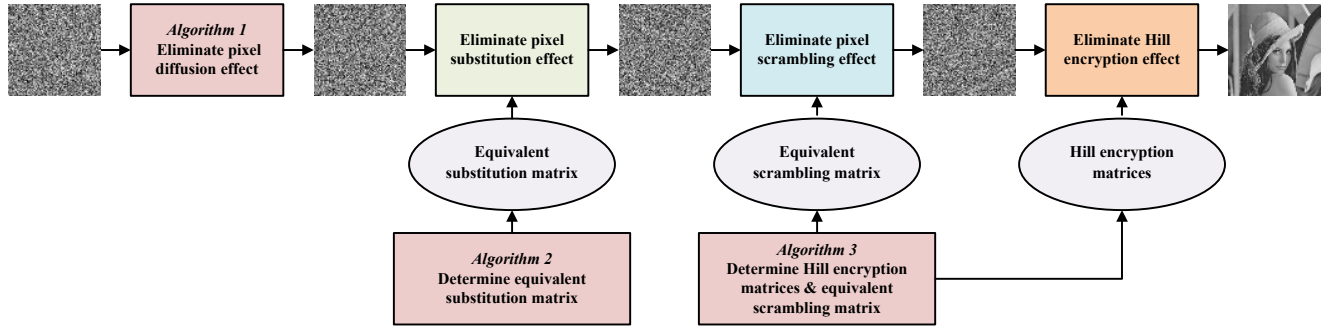


FIGURE 3. The flowchart of proposed attack algorithm.

it the i -th row of $\bar{\mathbf{M}}^{(f)}$. After the above processing, one can obtain the equivalent substitution matrix

$$\bar{\mathbf{M}}^{(f)} = \begin{bmatrix} \hat{c}_1^{(0)} & \hat{c}_2^{(0)} & \dots & \hat{c}_{M \times N}^{(0)} \\ \hat{c}_1^{(1)} & \hat{c}_2^{(1)} & \dots & \hat{c}_{M \times N}^{(1)} \\ \dots & \dots & \dots & \dots \\ \hat{c}_1^{(255)} & \hat{c}_2^{(255)} & \dots & \hat{c}_{M \times N}^{(255)} \end{bmatrix}$$

required to eliminate the substitution effect of $f(\cdot, K)$. For any cipher image $\mathbf{C}^{(a)}$ generated by (22), one can determine the original value of the pixel $c_i^{(a)} \in C^{(a)} (i = 1, 2, \dots, M \times N)$ before being processed by $f(\cdot, K)$. Specifically, one only need to find $c_i^{(a)}$ in the i -th column of $\bar{\mathbf{M}}^{(f)}$, and subtract 1 from the row index where $c_i^{(a)}$ is found. For example, to determine the original value of $c_2^{(a)}$ before being substituted, one can first find $c_2^{(a)}$ in the second column of $\bar{\mathbf{M}}^{(f)}$. Assuming that the row index where $c_2^{(a)}$ is found is 5, then the original value of $c_2^{(a)}$ is 4. Consequently, with $\bar{\mathbf{M}}^{(f)}$, one can once again simplify IES-FD into the following mathematical model.

$$\bar{\mathbf{C}}^{(7)} = f'(h(\mathbf{P}, K), K), \quad (25)$$

where $\bar{\mathbf{C}}^{(7)}$ is the intermediate cipher image whose diffusion effect and substitution effect have been eliminated, $f'(\cdot, K)$ represents the Feistel iterations with only scrambling effect. Algorithm 2 shows the main steps to determine $\bar{\mathbf{M}}^{(f)}$.

Algorithm 2 Determine the equivalent substitution matrix.

Input: The size $M \times N$ of the cipher image \mathbf{C} .

- 1: Initialize the equivalent substitution matrix $\bar{\mathbf{M}}^{(f)}$;
- 2: **for** $i = 1$ to 256 **do**
- 3: Construct the special plain image $\hat{\mathbf{P}}^{(i-1)}$ with single pixel value $i - 1$, and encrypt it to obtain its corresponding cipher image $\hat{\mathbf{C}}^{(i-1)}$;
- 4: Call Algorithm 1 to eliminate the pixel diffusion effect of $\hat{\mathbf{C}}^{(i-1)}$, and stretch $\hat{\mathbf{C}}^{(i-1)}$ into a 1D row vector, let $\bar{\mathbf{M}}^{(f)}(i, :) = \hat{\mathbf{C}}^{(i-1)}$;
- 5: **end for**

Output: The equivalent substitution matrix $\bar{\mathbf{M}}^{(f)}$.

According to the cryptanalysis done in Section III-E, combined with the chosen-plaintext attack, one can utilize (12) to determine $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}$ and the scrambled positions of four pixels. Let us take the encryption processing of the first block under the Hill encryption of IES-FD as an example. Construct the special plain image $\hat{\mathbf{P}}^{(1)}$, in which all pixels except two pixels are 0. The two non-zero pixels are the first pixel $\hat{p}_1^{(1)} = 2$ and the third pixel $\hat{p}_3^{(1)} = 1$. Then, according to (12), after the encryption process of the Hill encryption of IES-FD, the values of the first four pixels are

$$\begin{bmatrix} \bar{c}_1^{(1)} \\ \bar{c}_2^{(1)} \\ \bar{c}_3^{(1)} \\ \bar{c}_4^{(1)} \end{bmatrix} = \text{mod} \left(\begin{bmatrix} x_{1,1} + 1 \\ x_{2,1} \\ x_{1,1} + 2 \\ x_{2,1} \end{bmatrix}, 256 \right).$$

Similarly, another special plain image $\hat{\mathbf{P}}^{(2)}$ can be constructed, in which all pixels except two pixels are 0. The two non-zero pixels are the second pixel $\hat{p}_2^{(2)} = 2$ and the fourth pixel $\hat{p}_4^{(2)} = 1$. Then, after the encryption process of the Hill encryption of IES-FD, the values of the first four pixels are

$$\begin{bmatrix} \bar{c}_1^{(2)} \\ \bar{c}_2^{(2)} \\ \bar{c}_3^{(2)} \\ \bar{c}_4^{(2)} \end{bmatrix} = \text{mod} \left(\begin{bmatrix} x_{1,2} \\ x_{2,2} + 1 \\ x_{1,2} \\ x_{2,2} + 2 \end{bmatrix}, 256 \right).$$

Therefore, one can first eliminate the diffusion effect and substitution effect of the corresponding cipher images of $\hat{\mathbf{P}}^{(1)}$ and $\hat{\mathbf{P}}^{(2)}$, and then find $(\bar{c}_1^{(1)}, \bar{c}_2^{(1)}, \bar{c}_3^{(1)}, \bar{c}_4^{(1)})$ and $(\bar{c}_1^{(2)}, \bar{c}_2^{(2)}, \bar{c}_3^{(2)}, \bar{c}_4^{(2)})$ in them respectively. In this way, $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}$ and the scrambled positions of the first four pixels can be determined. Similarly, other Hill encryption matrices and the scrambled positions of the remaining pixels can also be determined. For a very small number of blocks, some pixels in $(\bar{c}_1^{(1)}, \bar{c}_2^{(1)}, \bar{c}_3^{(1)}, \bar{c}_4^{(1)})$ and $(\bar{c}_1^{(2)}, \bar{c}_2^{(2)}, \bar{c}_3^{(2)}, \bar{c}_4^{(2)})$ may not be found because they are exactly 0. At this time, one can solve it by taking the union of the found positions

and constructing more special plain images. In other words, $M \times N/4$ Hill encryption matrices and the equivalent scrambling matrix can be obtained through approximately $M \times N/2$ special plain images. Algorithm 3 presents the main steps to determine the Hill encryption matrices and equivalent scrambling matrix.

Algorithm 3 Determine the Hill encryption matrices and equivalent scrambling matrix.

Input: The size $M \times N$ of the cipher image \mathbf{C} .

- 1: Initialize the equivalent scrambling matrix $\bar{\mathbf{M}}^{(f')}$;
- 2: **for** $i = 1$ to $M \times N/4$ **do**
- 3: Construct the special plain image $\bar{\mathbf{P}}^{(2 \times (i-1)+1)}$, in which all pixels except two pixels are 0. The two non-zero pixels are the $(4 \times (i-1)+1)$ -th pixel $\bar{p}_{4 \times (i-1)+1}^{(1)} = 2$ and the $(4 \times (i-1)+3)$ -th pixel $\bar{p}_{4 \times (i-1)+3}^{(1)} = 1$. Encrypt $\bar{\mathbf{P}}^{(2 \times (i-1)+1)}$ to obtain its corresponding cipher image $\bar{\mathbf{C}}^{(2 \times (i-1)+1)}$;
- 4: Construct the special plain image $\bar{\mathbf{P}}^{(2 \times (i-1)+2)}$, in which all pixels except two pixels are 0. The two non-zero pixels are the $(4 \times (i-1)+2)$ -th pixel $\bar{p}_{4 \times (i-1)+2}^{(1)} = 2$ and the $(4 \times (i-1)+4)$ -th pixel $\bar{p}_{4 \times (i-1)+4}^{(1)} = 1$. Encrypt $\bar{\mathbf{P}}^{(2 \times (i-1)+2)}$ to obtain its corresponding cipher image $\bar{\mathbf{C}}^{(2 \times (i-1)+2)}$;
- 5: Call Algorithm 1 to eliminate the pixel diffusion effects of $\bar{\mathbf{C}}^{(2 \times (i-1)+1)}$ and $\bar{\mathbf{C}}^{(2 \times (i-1)+2)}$. Then, utilize $\bar{\mathbf{M}}^{(f')}$ to eliminate the pixel substitution effects of $\bar{\mathbf{C}}^{(2 \times (i-1)+1)}$ and $\bar{\mathbf{C}}^{(2 \times (i-1)+2)}$;
- 6: Find non-zero values in $\bar{\mathbf{C}}^{(2 \times (i-1)+1)}$ and $\bar{\mathbf{C}}^{(2 \times (i-1)+2)}$, and take the union of the indexes of found non-zero values. If the number of indexes obtained is less than 4, repeat the steps from line 3 to line 5 to construct two different special plain images until the number of indexes obtained is 4;
- 7: In the cipher images from which four indexes are obtained, find the corresponding pixel values and use them to determine the Hill encryption matrix $\mathbf{X}^{(i)}$ and scrambled positions of the four pixels in the i -th block;
- 8: Save the four scrambled positions to $\bar{\mathbf{M}}^{(f')}$;
- 9: **end for**

Output: The Hill encryption matrices $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}, \dots, \mathbf{X}^{(M \times N/4)}$ and equivalent scrambling matrix $\bar{\mathbf{M}}^{(f')}$.

So far, IES-FD has been completely cracked. Based on Algorithm 1, Algorithm 2, and Algorithm 3, the chosen-plaintext attack algorithm for IES-FD is proposed, as shown in Algorithm 4.

VI. SIMULATION TESTS AND ANALYSES

In order to confirm the effectiveness and feasibility of the proposed attack algorithm, four commonly used test images are adopted to conduct simulation tests. The four test images are Lena, Cameraman, 5.1.09, and 5.1.10, the latter two

Algorithm 4 Proposed chosen-plaintext attack algorithm for IES-FD.

Input: The cipher image \mathbf{C} with the size of $M \times N$, whose plain image needs to be recovered.

- 1: Call Algorithm 1 to eliminate the pixel diffusion effect of \mathbf{C} , thereby obtaining $\mathbf{C}^{(7)}$;
- 2: If the equivalent substitution matrix $\bar{\mathbf{M}}^{(f')}$ does not exist, call Algorithm 2 to determine $\bar{\mathbf{M}}^{(f')}$.
- 3: Utilize $\bar{\mathbf{M}}^{(f')}$ to eliminate the pixel substitution effect of $\mathbf{C}^{(7)}$, thereby obtaining $\mathbf{C}'^{(7)}$;
- 4: If the Hill encryption matrices $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}, \dots, \mathbf{X}^{(M \times N/4)}$ and equivalent scrambling matrix $\bar{\mathbf{M}}^{(f')}$ do not exist, call Algorithm 3 to determine them;
- 5: Utilize $\bar{\mathbf{M}}^{(f')}$ to eliminate the pixel scrambling effect of $\mathbf{C}'^{(7)}$, thereby obtaining $\mathbf{C}'^{(1)}$;
- 6: Utilize $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}, \dots, \mathbf{X}^{(M \times N/4)}$ to eliminate the Hill encryption effect of IES-FD, thereby obtaining \mathbf{P} ;


























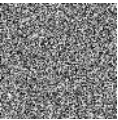
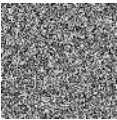

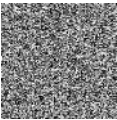








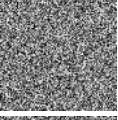
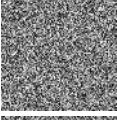
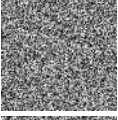
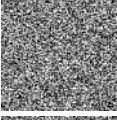







Output: The recovered plain image \mathbf{P} .

are selected from the USC-SIPI image database. The main hardware configurations used in the simulation tests are Intel (R) Xeon (R) CPU E3-1231 v3 @ 3.40 GHz and 8 GB RAM, and the main software configurations are 64-bit Windows 7 Ultimate and MATLAB R2017a (9.2.0.538062).

Without loss of generality, 5 randomly generated secret keys are adopted for simulation tests. For each secret key, Algorithm 2 is used to obtain the equivalent substitution matrix, and Algorithm 3 is used to obtain the Hill encryption matrices and the equivalent scrambling matrix. Then, use IES-FD to encrypt the plain images to obtain corresponding cipher images. Finally, through the cipher images, Algorithm 4 is used to recover the plain images without knowing the secret key. In five rounds of 200 attack tests, the attack algorithm proposed in this paper have completely recovered the plain images without exception. Table 1 shows the result images of each attack stage saved in the last round of attack tests. The test images with the size of 128×128 are reduced versions of the test images with the size of 256×256 . It can be seen that the attack algorithm proposed in this paper is effective.

The proposed attack algorithm is mainly composed of four parts, which are the elimination of pixel diffusion effect, the elimination of pixel substitution effect, the elimination of pixel scrambling effect and the elimination of Hill encryption effect. Since the encryption of the special plain images required for the attack can be prepared in advance and can be completed in parallel by multiple computing units, the encryption of the special plain images is not considered in the following time complexity analysis and test time statistics. According to Algorithm 4, the elimination of pixel diffusion effect requires $M \times N$ XOR operations on the pixels, so its time complexity is $O(M \times N)$. The elimination of pixel sub-

TABLE 1. Test results of proposed attack algorithm in terms of effectiveness.

Plain image	Size	Cipher image	Diffusion effect eliminated	Substitution effect eliminated	Scrambling effect eliminated	Hill encryption effect eliminated
	128 × 128					
	128 × 128					
	128 × 128					
	128 × 128					
	256 × 256					
	256 × 256					
	256 × 256					
	256 × 256					

stitution effect requires determining the equivalent substitution matrix, and then finding each intermediate cipher image pixel in the matrix. So, its time complexity is $O(M \times N)$. The elimination of pixel scrambling effect requires determining the equivalent scrambling matrix, and then rearranging each intermediate cipher image pixel. Thus, its time complexity is $O((M \times N)^2)$. Similarly, it can be determined that the time complexity of the elimination of Hill encryption effect is $O(M \times N)$. Table 2 presents the average times required for each attack stage under different input scales. As can be seen from Table 2, the test results are basically consistent with the time complexity analysis done above. Therefore, the proposed attack algorithm is also computationally feasible.

VII. IMPROVEMENT SUGGESTIONS FOR COMMON PROBLEMS

As we know, more and more researchers have been working on designing new image encryption schemes, hoping to continuously improve the efficiency of image encryption while achieving higher security. However, according to this paper and previous cryptanalysis works, some of the current image encryption schemes still have following problems that need to be solved.

(1) The hash value of the plain image is directly used as the secret key. Since the hash value of each image is different, directly using the hash value as the secret key means that every time a different image is encrypted, a different secret key must be replaced. In applications where a large number of images need to be encrypted, such one-time pad secret key is not practical. In addition, if such one-time pad secret key can be established, then there is no need to design any encryption scheme at all. Because the secret key will be constantly changed, only a simple XOR encryption is required.

(2) Some image encryption schemes use random values or secret parameters in the encryption process. Obviously, such design does not conform to the design principles of modern cryptographic systems.

(3) In the process of generating equivalent key streams, some image encryption schemes have a large number of equivalent secret keys in the key space. This undoubtedly reduce the ability of these encryption schemes to resist brute force attacks.

(4) In the encryption process, dependence on external data sources may reduce the practicality of an image encryption scheme. For example, if the GenBank database becomes inaccessible, or the DNA data in it changes, the cipher image

TABLE 2. Average times required for each attack stage under different input scales.

Input scale	Eliminate diffusion effect	Determine equivalent substitution matrix	Eliminate substitution effect	Determine equivalent scrambling matrix	Eliminate scrambling effect	Eliminate Hill encryption effect
64×64	0.0052 s	1.5480 s	0.0041 s	21.4791 s	3.8100×10^{-5} s	1.2900×10^{-4} s
128×128	0.0206 s	5.6372 s	0.0163 s	320.3079 s	1.5250×10^{-4} s	5.1500×10^{-4} s
256×256	0.0817 s	23.0446 s	0.0647 s	5033.6517 s	6.7500×10^{-4} s	0.0029 s

generated by IES-FD cannot be decrypted normally.

(5) There are redundant encryption steps, or encryption steps with the same encryption effect are continuously adopted. For example, in terms of encryption effect, there is no difference between two consecutive pixel substitution operations and one pixel substitution operation.

(6) Under certain conditions, the encryption structures of some image encryption schemes can be easily simplified by an attacker.

(7) In fact, some designers only rely on statistical tests or randomness tests to verify the security of the proposed image encryption schemes, but fail to fully analyze and evaluate their security.

In view of above problems, we put forward some suggestions for improvement. Of course, we also hope that future researchers can provide more specific and reasonable solutions to these problems.

(1) In fact, the purpose of using the hash value of the plain image as the secret key is to generate different equivalent key streams when encrypting different images. Therefore, a more reasonable way should be to apply the statistical information or hash value of the plain image to the encryption process. In other words, the security of an image encryption scheme should be based on a reasonably designed encryption process and the unknownness of the secret key, rather than an impractical or unreasonable secret key design.

(2) In modern cryptographic systems, everything except the secret key should be known, and the security of an image encryption scheme should not rely on other unknowns or uncertainties. Therefore, the designers should avoid using random values or secret parameters in the encryption process.

(3) The designers of new image encryption schemes should carefully analyze and verify the generation process of the equivalent key streams, so as to avoid the situation where different secret keys generate the same equivalent key streams. Additionally, the composition of the secret key should be clear and standardized, defined in the form of a binary bit sequence.

(4) When designing the encryption process, it is necessary to clarify the design purpose and actual encryption effect of each encryption step. That is, carefully analyze the necessity, feasibility and practicality of each introduced encryption step, and avoid redundant or meaningless encryption steps.

The encryption structure of a properly designed image encryption scheme should be a complete and self-contained iterative structure with necessary cryptographic primitives.

(5) For each encryption step in the encryption process, the designers should analyze the relationship between input and output, and consider whether this relationship will degrade or be simplified under specific attack conditions.

(6) When verifying the security of an image encryption scheme, in addition to common security tests, the entire encryption scheme must be analyzed and evaluated from the perspective of an attacker. In other words, for each encryption step, an in-depth and comprehensive analysis must be carried out.

VIII. CONCLUSION

In this paper, a newly proposed image encryption scheme based on Feistel network and dynamic DNA encoding, namely IES-FD, is briefly introduced. Then, some security, feasibility and practicability problems in IES-FD are pointed out. After analyzing and discussing these problems, we made necessary improvements to IES-FD and proposed a targeted chosen-plaintext attack algorithm. The proposed attack algorithm first eliminates the pixel diffusion effect of IES-FD through simple processing, and then determines its equivalent substitution matrix, equivalent scrambling matrix and Hill encryption matrices through about $256 + (M \times N/2)$ special plain images and their corresponding cipher images. Related simulation tests and analyses have confirmed the effectiveness and feasibility of the proposed attack algorithm. Finally, in view of common problems in some current image encryption schemes, we give some improvement suggestions, so as provide useful references for future image encryption scheme designers.

ACKNOWLEDGEMENT

All authors not only express their deep gratitude to the editors and anonymous reviewers for their prompt handling of the paper, but also sincere gratitude to them for their efforts to improve the quality of the paper.

REFERENCES

[1] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic dna encoding," *IEEE Photonics Journal*, vol. 10, no. 4, p. Art. no. 3901014, Aug. 2018.

- [2] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163–185, Nov. 2019.
- [3] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *Journal of Information Security and Applications*, vol. 48, p. Art. no. 102361, Oct. 2019.
- [4] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, Apr. 2018.
- [5] Y. Zhang, Q. He, Y. Xiang, L. Y. Zhang, B. Liu, J. Chen, and Y. Xie, "Low-cost and confidentiality-preserving data acquisition for internet of multimedia things," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3442–3451, Oct. 2018.
- [6] J. Wang, K. Han, S. Fan, Y. Zhang, and J. Lin, "A logistic mapping-based encryption scheme for wireless body area networks," *Future Generation Computer Systems*, vol. 110, pp. 57–67, Sept. 2020.
- [7] Y. Zhang, P. Wang, L. Fang, X. He, and B. Chen, "Secure transmission of compressed sampling data using edge clouds," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6641–6651, Oct. 2020.
- [8] Y. Zhang, Q. He, G. Chen, X. Zhang, and Y. Xiang, "A low-overhead, confidentiality-assured, and authenticated data acquisition framework for iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7566–7578, Dec. 2020.
- [9] Y. Zhang, P. Wang, H. Huang, Y. Zhu, D. Xiao, and Y. Xiang, "Privacy-assured fogcs: Chaotic compressive sensing for secure industrial big image data processing in fog computing," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3401–3411, May 2021.
- [10] R. Zhao, Y. Zhang, X. Xiao, X. Ye, and R. Lan, "TPE2: Three-pixel exact thumbnail-preserving image encryption," *Signal Processing*, vol. 183, p. Art. no. 108019, Jun. 2021.
- [11] Y. Zhang, R. Zhao, X. Xiao, R. Lan, Z. Liu, and X. Zhang, "HF-TPE: High-fidelity thumbnail-preserving encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. PP, no. 99, pp. 1–1, Apr. 2021.
- [12] A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, and A. M. Iliyasu, "Efficient chaos-based substitution-box and its application to image encryption," *Electronics*, vol. 10, no. 12, p. Art. no. 1392, Jun. 2021.
- [13] S. Vaidyanathan, A. Sambas, B. Abd-El-Atty, A. A. A. El-Latif, E. Tlelo-Cuautle, O. Guillén-Fernández, M. Mamat, M. A. Mohamed, M. Alçin, M. Tuna, h. Pehlivan, s. Koyuncu, and M. A. H. Ibrahim, "A 5-d multi-stable hyperchaotic two-disk dynamo system with no equilibrium point: Circuit design, fpga realization and applications to trngs and image encryption," *IEEE Access*, vol. 9, pp. 81 352–81 369, Jun. 2021.
- [14] A. Alanezi, B. Abd-El-Atty, H. Kolivand, A. El-Latif, A. Ahmed, A. El-Rahiem, S. Sankar, H. S Khalifa et al., "Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment," *Security and Communication Networks*, vol. 2021, p. Art. no. 6615512, Feb. 2021.
- [15] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5g internet of things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, Jan. 2020.
- [16] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, Jan. 2021.
- [17] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *International Journal of Information Technology*, vol. 10, no. 3, pp. 247–255, Jan. 2018.
- [18] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. M. S. Beg, and A. A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a ban system, and improved scheme using sha-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, p. Art. no. 266, Jul. 2018.
- [19] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, J. K. C., A. Belazi, I. Mehmood, A. K. Bashir, O.-Y. Song, and A. A. A. El-Latif, "A new chaotic map with dynamic analysis and encryption application in internet of health things," *IEEE Access*, vol. 8, pp. 137 731–137 744, Jul. 2020.
- [20] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," *Optics and Laser Technology*, vol. 124, p. Art. no. 105942, Apr. 2020.
- [21] A. A. Abd el Latif, B. Abd-el Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Scientific reports*, vol. 10, no. 1, p. Art. no. 1930, Feb. 2020.
- [22] H. M. Pandey, "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography," *Future Generation Computer Systems*, vol. 111, pp. 213–225, Oct. 2020.
- [23] J. Wang, L. Y. Zhang, J. Chen, G. Hua, Y. Zhang, and Y. Xiang, "Compressed sensing based selective encryption with data hiding capability," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6560–6571, Dec. 2019.
- [24] W. Feng, Y. He, H. Li, and C. Li, "A plain-image-related chaotic image encryption algorithm based on DNA sequence operation and discrete logarithm," *IEEE Access*, vol. 7, pp. 181 589–181 609, Dec. 2019.
- [25] L. Li, L. Liu, H. Peng, Y. Yang, and S. Cheng, "Flexible and secure data transmission system based on semitensor compressive sensing in wireless body area networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3212–3227, Apr. 2019.
- [26] Z. Mishra and B. Acharya, "High throughput and low area architectures of secure iot algorithm for medical image encryption," *Journal of Information Security and Applications*, vol. 53, p. Art. no. 102533, Aug. 2020.
- [27] A. S. Unde and P. P. Deepthi, "Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia iot," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 167–171, Jan. 2020.
- [28] B. Zhang, D. Xiao, and Y. Xiang, "Robust coding of encrypted images via 2d compressed sensing," *IEEE Transactions on Multimedia*, vol. 23, pp. 2656–2671, Aug. 2020.
- [29] H. Li, T. Li, W. Feng, J. Zhang, J. Zhang, L. Gan, and C. Li, "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic dna-level two-way diffusion," *Journal of Information Security and Applications*, vol. 61, p. Art. no. 102844, Sept. 2021.
- [30] S. S. Moafimadani, Y. Chen, and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," *Entropy*, vol. 21, no. 6, p. Art. no. 577, Jun. 2019.
- [31] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic-tent map," *Entropy*, vol. 21, no. 7, p. Art. no. 656, Jul. 2019.
- [32] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic s-boxes," *Entropy*, vol. 21, no. 8, p. Art. no. 790, Aug. 2019.
- [33] S. Zhou, P. He, and N. Kasabov, "A dynamic dna color image encryption method based on sha-512," *Entropy*, vol. 22, no. 10, p. Art. no. 1091, Sept. 2020.
- [34] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of atmospheric sciences*, vol. 20, no. 2, pp. 130–141, Mar. 1963.
- [35] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Physical review letters*, vol. 71, no. 1, pp. 65–68, Jul. 1993.
- [36] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.
- [37] G. Wang, D. Chen, J. Lin, and X. Chen, "The application of chaotic oscillators to weak signal detection," *IEEE Transactions on Industrial Electronics*, vol. 46, no. 2, pp. 440–444, Apr. 1999.
- [38] M. Zhang and Y. Wang, "Review on chaotic lasers and measurement applications," *Journal of Lightwave Technology*, vol. 39, no. 12, pp. 3711–3723, Jun. 2021.
- [39] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2322–2335, Jun. 2019.
- [40] C. Li, K. Tan, B. Feng, and J. Lü, "The graph structure of the generalized discrete arnold cat map," *IEEE Transactions on Computers*, 2021.

- [41] J. Chen, L. Chen, L. Y. Zhang, and Z. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 301–322, Apr. 2019.
- [42] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, Apr. 2019.
- [43] A. Broumandnia, "Image encryption algorithm based on the finite fields in chaotic maps," *Journal of Information Security and Applications*, vol. 54, p. Art. no. 102553, Oct. 2020.
- [44] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dynamics*, vol. 95, no. 4, pp. 2797–2824, Mar. 2019.
- [45] M. Majid, S. Amir, H. Moein, and N. Mahboubeh, "An improved method for image encryption based on high level chaotic maps and improved gravity model," in *2015 International Congress on Technology, Communication and Knowledge (ICTCK)*, 2015, pp. 253–259.
- [46] M. Mollaeefar, A. Sharif, and M. Nazari, "A novel encryption scheme for colored image based on high level chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 607–629, Nov. 2017.
- [47] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, Feb. 2019.
- [48] K. Jithin and S. Sankar, "Colour image encryption algorithm combining arnold map, dna sequence operation, and a mandelbrot set," *Journal of Information Security and Applications*, vol. 50, p. Art. no. 102428, Feb. 2020.
- [49] T. ul Haq and T. Shah, "Algebra-chaos amalgam and dna transform based multiple digital image encryption," *Journal of Information Security and Applications*, vol. 54, p. 102592, Oct. 2020.
- [50] W. Feng, Y. He, H. Li, and C. Li, "Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map," *IEEE Access*, vol. 7, pp. 12584–12597, Jan. 2019.
- [51] W. Feng and Y. He, "Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling," *IEEE Photonics Journal*, vol. 10, no. 6, p. Art. no. 7909215, Dec. 2018.
- [52] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137–2150, Mar. 2018.
- [53] M. Ahmad, M. Z. Alam, S. Ansari, D. Lambić, and H. D. AlSharari, "Cryptanalysis of an image encryption algorithm based on pwlc and inertial delayed neural network," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1323–1332, Mar. 2018.
- [54] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications*, vol. 54, p. Art. No. 102566, 2020.
- [55] M. Li, D. Lu, Y. Xiang, Y. Zhang, and H. Ren, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 31–47, Jan. 2019.
- [56] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a dna-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, May 2020.
- [57] I. El Hanouti, H. El Fadili, and K. Zenkour, "Cryptanalysis of an embedded systems' image encryption," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13801–13820, Jan. 2021.
- [58] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 167, p. Art. no. 107286, Feb. 2020.
- [59] N. Munir, M. Khan, M. M. Hazzazi, A. Aijaedi, A. R. Alharbi, I. Hussain et al., "Cryptanalysis of internet of health things encryption scheme based on chaotic maps," *IEEE Access*, vol. 9, pp. 105678–105685, Jul. 2021.
- [60] Y. Li, W. K. Tang, and G. Chen, "Generating hyperchaos via state feedback control," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3367–3375, 2005.
- [61] T. Gao, Z. Chen, Z. Yuan, and D. Yu, "Adaptive synchronization of a new hyperchaotic system with uncertain parameters," *Chaos, Solitons & Fractals*, vol. 33, no. 3, pp. 922–928, Aug. 2007.
- [62] "IEEE Standard for Floating-Point Arithmetic," *IEEE Standard 754-2008*, pp. 1–70, Aug. 2008.



WEI FENG (M'18) received the M.Sc. degree in computer applied technology from the College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China, in 2007 and the Ph.D. degree in electrical engineering from the School of Electrical Engineering and Automation, Hefei University of Technology, Hefei, China, in 2019. He is currently an Associate Professor with the School of Mathematics and Computer Science, Panzhihua University, Panzhihua, China. His research interests include multimedia security, cloud computing security, big data security, Internet of Things security, and blockchain.



ZHENTAO QIN received the M.Sc. degree in software engineering from the College of Computer Science, University of Electronic Science and Technology of China, Chengdu, China, in 2008 and the Ph.D. degree in applied geophysics from the College of Geophysics, Chengdu University of Technology, Chengdu, China, in 2015. He is currently a Professor with the School of Mathematics and Computer Science, Panzhihua University, Panzhihua, China. His research interests include multimedia security, artificial intelligence, and big data security.



JING ZHANG received the M.Sc. degree in computer software from the College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2005 and the Ph.D. degree in computer architecture from the College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2009. He is currently a Professor and the Head with the School of Mathematics and Computer Science, Panzhihua University, Panzhihua, China. His research interests include multimedia security, cloud computing security, big data security, Internet of Things security, and blockchain.



MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he has worked in the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor in the Department of Computer Engineering, Jamia Millia Islamia. He has published over 85 research papers in international reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 1500 citations of his research works with an H-index of 22. His research interests include Multimedia Security, Chaos-based Cryptography, Cryptanalysis, Machine Learning for Security, Image Processing, and Optimization Techniques. He has served as reviewer and technical program committee member of many international conferences. He has also served as referee of some renowned journals, such as Information Sciences, Signal Processing, Journal of Information Security and Applications, IEEE Journal of Selected Areas in Communications, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Industrial Informatics, IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on NanoBioscience, IEEE Multimedia, IEEE Access, Wireless Personal Communications, Neural Computing and Applications, International Journal of Bifurcation and Chaos, Chaos Solitons & Fractals, Physica A, Signal Processing: Image Communication, Neurocomputing, IET Information Security, IET Image Processing, Security and Communication Networks, Optik, Optics and Laser Technology, Complexity, Computers in Biology and Medicine, Computational and Applied Mathematics, Concurrency and Computation, etc.

• • •