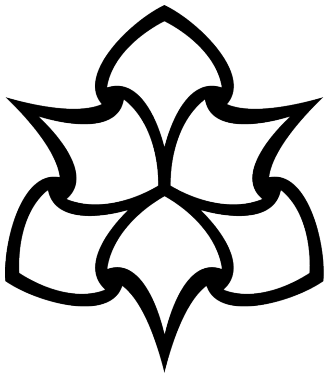


B*l*-IEA: A Bit-level Image Encryption Algorithm for Cognitive Services in Intelligent Transportation Systems

Yi SUN [1,2], Keping YU[3], Ali Kashif Bashir[4,5] and Xin LIAO[6]

[1]*School of Computer Science(National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing, China*
[2]*National Engineering Laboratory for Mobile Network Technologies, Beijing, China*
[3]*Global Information and Telecommunication Institute, Waseda University, Japan*
[4]*Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, United Kingdom*
[5]*School of Electrical Engineering and Computer Science (SEECS), National University of Science and Technology, Islamabad (NUST), Pakistan*
[6]*College of Computer Science and Electronic Engineering, Hunan University, Changsha, China*

***Abstract*—In Intelligent Transportation Systems, images are the main data sources to be analyzed for providing intelligent and precision cognitive services. Therefore, how to protect the privacy of sensitive images in the process of information transmission has become an important research issue, especially in future no non-private data era. In this article, we design the *Rearrangement-Arnold Cat Map* (R-ACM) to disturb the relationship between adjacent pixels and further propose an efficient *Bit-level Image Encryption Algorithm*(B*l*-IEA) based on R-ACM. Experiments show that the correlation coefficients of two adjacent pixels are 0.0022 in the horizontal direction, -0.0105 in the vertical direction, and -0.0035 in the diagonal direction respectively, which are obviously weaker than that of the original image with high correlations of adjacent pixels. What's more, the NPCR is 0.996120172, and the UACI is 0.334613406, which indicate that B*l*-IEA has stronger ability to resist different attacks compared with other solutions. Especially, the lower time complexity and only one round permutation make it particularly suitable to be used in the time-limited intelligent transportation field.**

Keywords: Intelligent Transportation Systems, Cognitive Services, Image Encryption, Re-arrangement, Logistic Chaotic Map

I. Introduction

As the main information carriers and data sources, images are of paramount importance to Intelligent Transportation Systems (ITS) from nearly half a century ago since it presented [1]–[5]. Because of the excellent characteristics such as information-rich, intuitive, and easy to obtain, images accompany the whole life cycle of the vehicle to provide specialized and intelligent services in ITS. When a vehicle is in a factory, images are used for design and inspection. When vehicle is parked, images are still produced by Drive Recorder, Traffic camera, etc. When a vehicle is on the road, images are everywhere at any time. The images from camera located beside or upon the road can be used for vehicle detection, velocity analysis, and parking management, etc. The images from camera located in vehicle can be used for preceding car detection, distance measurement, obstacle detection, and AR navigation, etc. Besides, the images from of the drivers and passengers' portable devices such as smartphones, laptops, tablets, watches, and etc., can be used for communication, accident recording and responsibility determination, vehicle tracking, and etc.

Since images are widely used in the acquisition and transmission of actual information, the amount of information transmitted by image communication is far more than other means of communication. Moreover, the emergence of new image technologies like computer version (CV) and augmented reality (AR) has made the security issues like illegal interception, tampering and destruction of images are increasingly prominent. Therefore, from the perspective of information security [6]–[9], protecting the security and privacy of images has become an urgent problem to be solved to realize both secure and intelligent transportation modernization.

In face of this problem, image encryption technology is vital for protecting the image from such attacks. Image encryption is able to transform a sensitive image into an unrecognizable, noise-like cipher-image [10]. However, conventional encryption algorithms can't work smoothly in encrypting images due to bulky data capacity, high redundancy, and strong correlations between two adjacent pixels [11]. In the previous study of image encryption, it has emerged many solutions based on chaos theory, optical transform [12], DNA coding, compressed sensing [13] and quantum theory.

Among them, due to the excellent intrinsic properties such as high sensitivity, pseudo-randomness and ergodicity, chaotic is widely used in image encryption era [14]. In [15], the authors proposed a chaotic image encryption scheme using DNA sequence operations which employ coupled-map lattices (CML) chaotic system and DNA encoding to achieve DNA-level permutation and confusion. In [16], it presented a noise-resistive image encryption scheme for gray images based on piecewise linear chaotic map (PWLCM), logistics chaotic

Corresponding Authors: Yi SUN, sybupt@bupt.edu.cn; Keping YU, keping.yu@aoni.waseda.jp

maps and DNA complementary rules. But one dimensional chaotic map has security weaknesses such as short period window and small key space, so they are vulnerable to many attacks. To increase the complexity of the map, there are a number of hyper-dimensional chaotic map have been proposed. In [10], they proposed the 2D Logistic Adjusted Sine Map(LASM) and a 2D-LASM based image encryption scheme, which introducing some random values to enhance the security. In [17], Hua et al. introduced two-dimensional(2D) Logistic Sine Coupling Map(LSCM) and designed a 2D-LSCM based image encryption algorithm. Xian et al. [18] proposed an image encryption scheme based on chaotic digit selection diffusion and chaotic sub-block scrambling. This scheme changed all pixel points position in one round, and both the time and space complexities were significantly reduced.

All these image encryption schemes mentioned above are encrypted at pixel-level. There are many bit-level image encryption algorithms due to the advantages of bit-level permutation, which can change both the position and the value of a pixel simultaneously [19]. Xu et al. [20] presented a bit-level image encryption algorithm based on cyclic shift and swapping, and Piecewise Linear Chaotic Map(PWLCM). The proposed algorithm has excellent performance. In [20], the authors introduced a new diffusion strategy to mutually diffuse two binary sequences of the same size which is transformed by the plain-text image. This algorithm was able to permute the bits in one bitplane into another one and achieved outstanding efficiency.

Many encryption schemes adopt *Arnold cat map* in the permutation operation. The disadvantage is that these cat map schemes can't resist the chosen plaintext attacks and have short periodic. They are not secure enough in practical applications. Then, a non-adjacent CML-based encryption algorithm is proposed in [21]. It used the *Arnold cat map* to permute mutually at bit-level requiring no extra storage cost. In [22], the author designed the image encryption scheme based on independent component analysis. In 2015, Zhang [23] utilized cat map and hyperchaotic lorenz to design an image encryption scheme. It introduced a plaintext related keystream generation strategy in diffusion process and employed *Arnold cat map* to confuse the positions of the image pixels directly in permutation process. Then, Joshi et al. [24] proposed the triple color image encryption method by 2D Multiple Parameter Fractional Discrete Fourier Transform (2D MPFrDFT) and 3D Arnold Transform (3D AT). It firstly permutes rows and columns on the bayer image to obtain the Complex Valued Image(CVI), and then applies 2D MPFrDFT and 3D AT on CVI. Wang et al. [25] used the dynamic random growth technique to design a chaotic block image encryption algorithm, which eliminates the drawback in short periodic and can resist chosen plaintext attacks while keeping a fast operating speed. However, this algorithm needs to invoke cat map many times, costing a lot of time. In addition, the relations of the adjacent pixels have no changes after implementing the cat map.

To solve the above problems, we proposed B*l*-IEA based on R-ACM at bit level. It combines the permutation and diffusion processes and performs the two stages simultaneously. In short, the main contributions of this paper can be summarized as follows.

1) We construct R-ACM to break the correlations between the adjacent pixels by only one round. The correlation coefficients of two adjacent pixels are 0.0022, -0.0105, and -0.0035 respectively, which are obviously weaker than that of the original image.
2) B*l*-IEA is secure to resist many different attacks. The NPCR is 0.996120172, and the UACI is 0.334613406, which indicate that B*l*-IEA has stronger ability to resist different attacks compared with other solutions.
3) B*l*-IEA has low time complexity. It only needs $\theta\left(2 \times M \times N\right)$ iterations of shuffle pixels.

The rest of this paper is organized as follows. Section 2 introduce the preliminaries such as the chaotic map and the rearrangement technique we proposed. The framework of the application scenario in ITS, the encryption and decryption algorithms are presented in Section 3. Then, we describe the details of the experiments in Section 4. The results and security analysis are presented in Section 5. Last section gives the conclusion.

II. Preliminaries

In this section, we introduce three mathematical tools, *Arnold Cat Map*, *Logistic Chaotic Map*, *2D Logistic-Sine-Coupling Map* and the proposed *Rearrangement-Arnold Cat Map*, respectively.

A. Arnold Cat Map

Arnold cat map is proposed by Arnold and Avez in 1968, which is a dynamic discrete map. It is defined as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\bmod N) = \begin{bmatrix} a & p \\ q & b \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\bmod N) \tag{1}$$

$$det(A) = 1 \tag{2}$$

If we use (x, y) to describe the position of pixel point in an $N * N$ image, (x_n, y_n) and (x_{n+1}, y_{n+1}) are the positions of the sample pixel point in the original image and the transformed position after mapping, respectively. In the permutation process, the general formula of matrix *A* is as follows:

$$A = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \tag{3}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod} N) \tag{4}$$

The control parameter p and q are positive integers [22]. Different values lead to the dynamics of the chaos. Since the matrix determinant equals 1, the map is area preserving [26]. Besides, cat map has two vital features which bring the chaotic behaviour. Firstly, the matrix multiplication operation stretches the original image and then the modular arithmetic folds it in order to ensure that the new position (x_{n+1}, y_{n+1}) falls in (N, N).

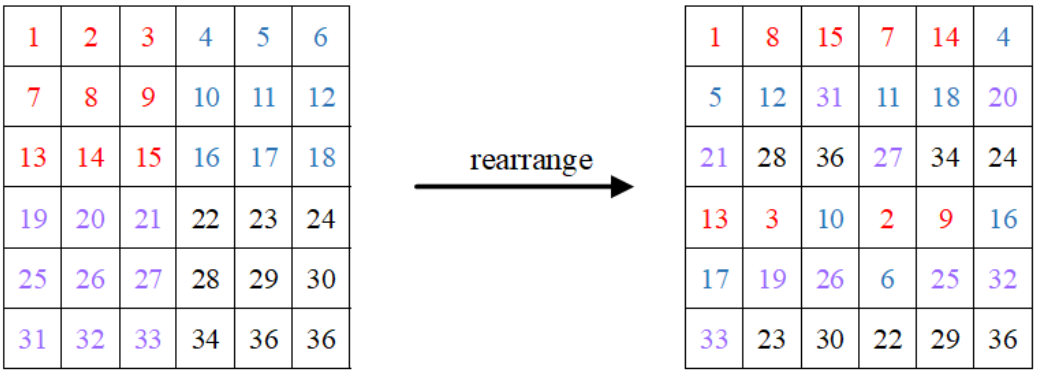


Fig. 1: An example of pixels rearrangement

- *R-ACM*

Although *Arnold cat map* is fast and simple to be used, it can be easily attacked by chosen plaintext attacks since permutation processes every once in a while [25].

In this paper, we construct R-ACM based on rearrangement technology. Specifically, we changed the original pixel positions to break the relationship between two adjacent pixels. The calculation processes can be described as follows:

$$x'_n = \{[x_n + N * (y_n + 1)]\ /4\}\ /(N/2) + ((N/2) * k_1) \quad (5)$$

$$y'_n = \{[x_n + N * (y_n + 1)]\ /4\} \bmod (N/2) + ((N/2) * k_2) \quad (6)$$

$$t = [x_n + N * (y_n + 1)] \bmod 4 \quad (7)$$

$$k_1 = \begin{cases} 0 & , t = 0 \text{ or } 1 \\ 1 & , t = 2 \text{ or } 3 \end{cases} \quad (8)$$

$$k_2 = \begin{cases} 0 & , t = 0 \text{ or } 2 \\ 1 & , t = 1 \text{ or } 3 \end{cases} \quad (9)$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x'_n \\ y'_n \end{bmatrix} (\mathrm{mod} N) \quad (10)$$

Herein, (x_n, y_n) and (x'_n, y'_n) are the original and the new pixel positions after implementing the rearrangement technology. Eq.(10) describes the proposed R-ACM. The example of R-ACM is shown in Fig.1.

B. Logistic Chaotic Map

We use logistic map to generate random sequences. It is defined as follows:

$$x_{n+1} = \mu x_n (1 - x_n), \quad 3.5699456 < \mu \leq 4 \quad (11)$$

Where the parameter μ, $\mu \in [0,\ 4]$, is the control coefficient. The map is chaotic when μ is in the interval of $(3.5699456\ ,\ 4]$ [25]. The specific steps are described in [25].

C. 2D LSCM

2D-LSCM was firstly proposed in [17]. It couples the Logistic map and Sine map together, and mixes the complexity of the Logistic map and Sine map sufficiently to obtain more complex chaotic characteristics [17]. 2D-LSCM can be described as follows:

$$\begin{cases} x_{i+1} = \sin(\pi(4\theta x_i(1 - x_i) + (1 - \theta)\sin(\pi y_i))) \\ y_{i+1} = \sin(\pi(4\theta y_i(1 - y_i) + (1 - \theta)\sin(\pi x_{i+1}))) \end{cases} \quad (12)$$

where θ, $\theta \in [0, 1]$ is the control parameter.

2D-LSCM is chaotic if $\theta \in (0,\ 1)$, and hyperchaotic if $\theta \in (0,\ 0.34) \cup (0.67,\ 1)$.

III. B*l*-IEA

In this section, we firstly introduce the framework of the Secure Advanced Transportation Assistant Systems (ADAS) and then demonstrate B*l*-IEA.

A. Secure Advanced Transportation Assistant Systems

Traditional Advanced Driver Assistant Systems (ADAS) use a variety of data collected from vehicle and its environments to evaluate safety risks and threats without considering the security of the sensitive data [27]. Herein, we present the Secure Advanced Transportation Assistant Systems (SATAS) as an upgrade to the traditional ADAS in two ways.

1) Firstly, in terms of the data collection scope, we consider all image-form data from the vehicle, its environments, the driver and all passengers.

2) Secondly, in terms of the data security, the B*l*-IEA will be implemented before processing images after being captured by various environment sensors such as camera, radar, infrared, or obtained from users' portal devices.

The framework of SATAS is presented in Fig.2. Like traditional ADAS, there are three stages, Image Capture, Pre-processing, and Post-processing. The difference is that B*l*-IEA is deployed before the pre-processing stage besides various functions like stabilization, classification, noise reduction, color conversion and motion analysis. And the images can be captured by various sensors and smart devices of the vehicle, its environments, the driver and all passengers. During the

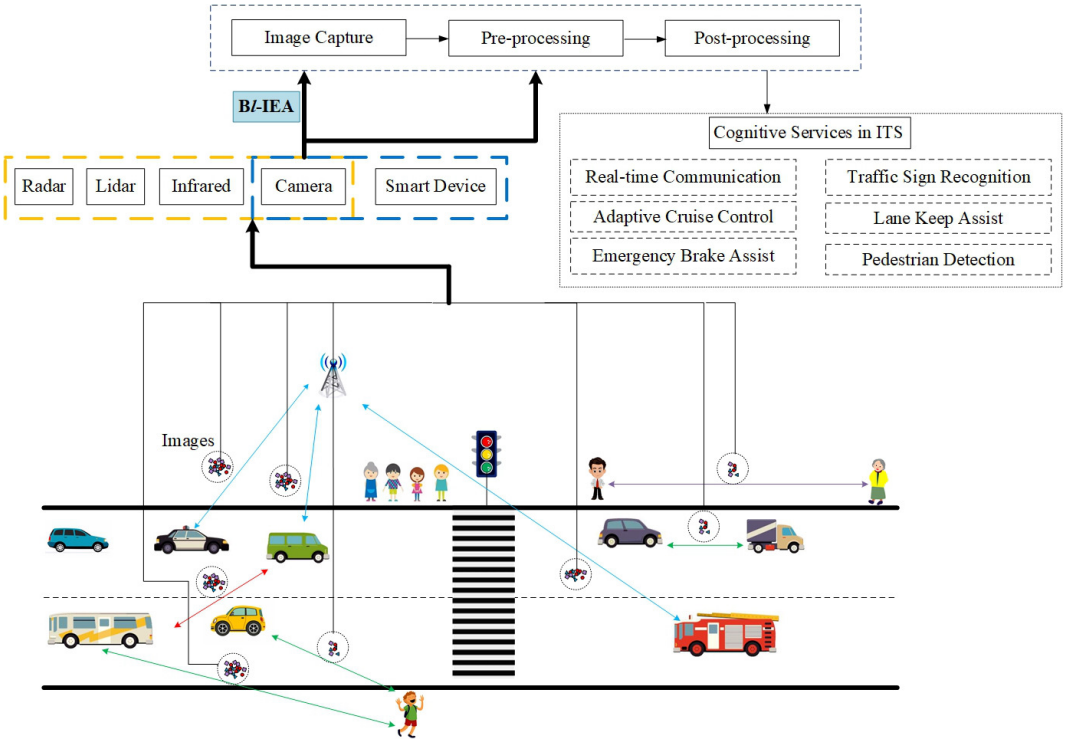


Fig. 2: The Framework of SATAS

post-processing stage, SATAS can provide intelligent cognitive services in ITS [28], [29], such as Real-time Communication, Adaptive Cruise Control, Emergency Brake Assist, Traffic Sign Recognition, Lane Keep Assist, Pedestrian Detection.

B. Bit-level Image Encryption Algorithm

In our proposed Bl-IEA, we execute permutation and diffusion simultaneously at bit-level. The encryption and decryption processes are displayed in Fig.3 and Fig.4, respectively. The details of encryption are described below.

1) Set the control parameter μ, the initial value x_0 and iterate Eq.(11) 200 times.
2) Continue to iterate Eq.(11) to produce a sequence which is used to add surroundings of the plain image:

$$X_1 = \{x_{200+1}, x_{200+2}, \ldots, x_{200+n}\} \tag{13}$$

$$n = 2(M+1) + 2(N+1) \tag{14}$$

For each element from X_1, apply the following formula to convert x_k $(k \in [200,\ 200+n])$ to the nonnegative integer x'_k less than 256.

$$x'_k = \mathrm{mod}\left(\lfloor x_k \times 10^{16} \rfloor, 256\right) \tag{15}$$

Where mod $(x,\ y)$ returns the remainder of x divided by y, $\lfloor x \rfloor$ is the nearest integer less than or equal to x. Adding surrounding pixels can affect all the pixels after permutation and diffusion operations. Because these values are randomly generated and different in each encryption round, the obtained cipher-images are different from each other after encrypting a plain-image several times with the same secret key [10]. This important nature shows better performance on the chosen-plaintext and brute-force attacks. The sequence of size n after Eq.(15) has the same representation format as the pixels of P. Fig.3(a-c) shows a numerical example of the process to add surrounding pixels.

3) Set θ, $(y_0,\ z_0)$ and iterate Eq.(12) 200 times.
4) Continue to iterate Eq.(12) over t times to generate two chaotic sequences (Y, Z), and employ Eq.(15) to transform elements of this sequence format. Then, expand the plain image with the generated two sequences according to the number of odd or even rows.

$$Y = \{y_{200+1}, y_{200+2}, \ldots, y_{200+t}\} \tag{16}$$

$$Z = \{z_{200+1}, z_{200+2}, \ldots, z_{200+t}\} \tag{17}$$

$$t = \begin{cases} [2(N+2) - (M+2)](N+2) & ,2N > M \\ \left[\frac{(M+2+i)}{2} - (N+2)\right](M+2+i) & ,2N \leq M \end{cases} \tag{18}$$

$$i = \begin{cases} 0 & ,M \bmod 2 = 0 \\ 1 & ,M \bmod 2 = 1 \end{cases} \tag{19}$$

By employing the chaotic sequences to expand the original image, there are mainly two reasons. On the one hand, this can increase the randomness after permutation and diffusion operations. On the other hand, the *Arnold cat map* only can be used on the square image, therefore,

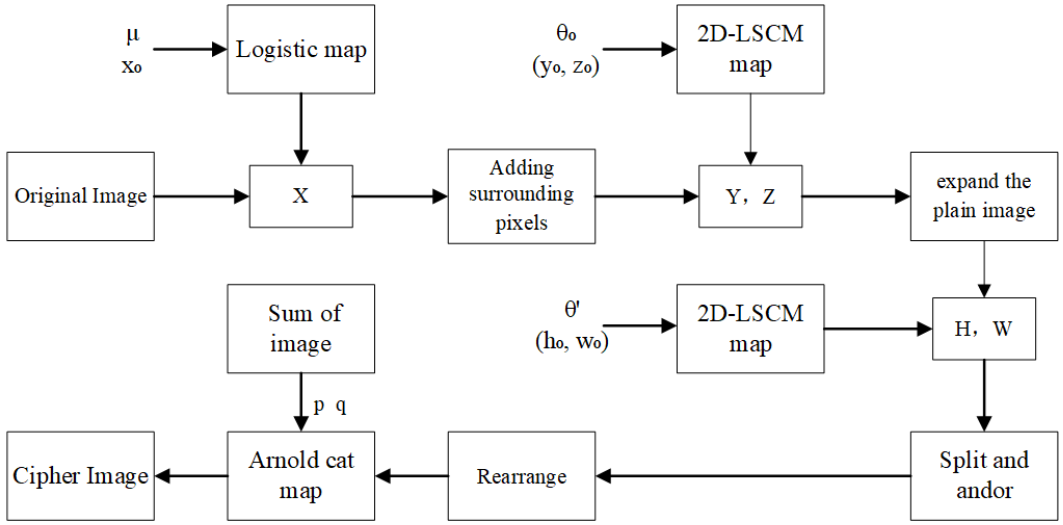


Fig. 3: B*l*-Image Encryption Algorithm

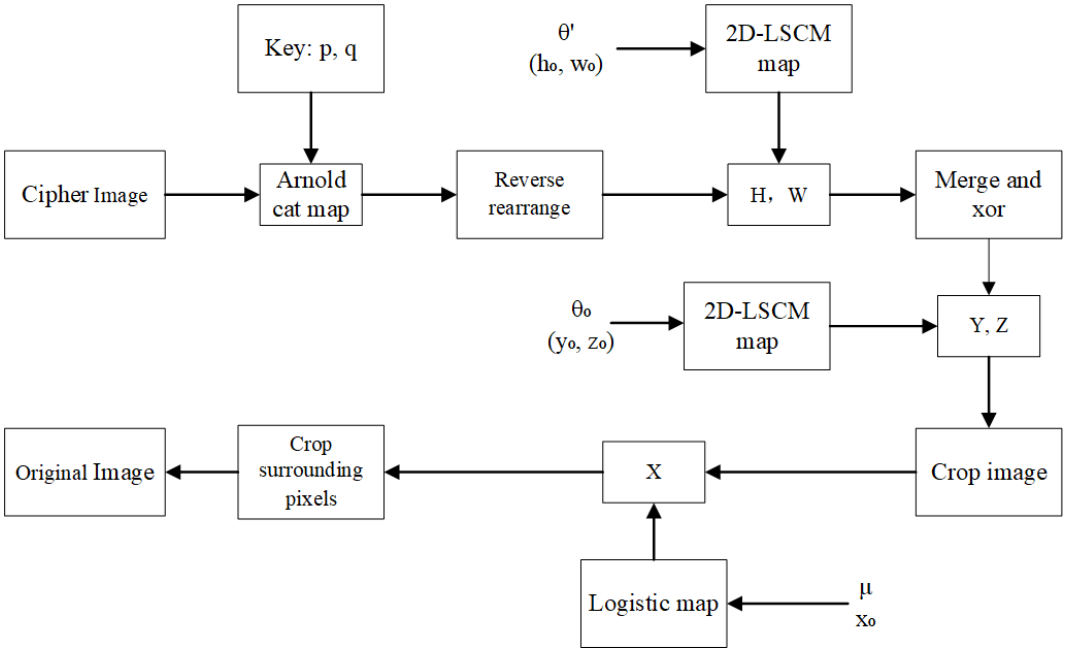


Fig. 4: B*l*-Image Decryption Algorithm

it's necessary to fill in the image to meet the condition of map.

5) Convert the 10 to 2. Because the permutation and diffusion at bit level can simultaneously change the value and position of pixel in image. For a pixel p' in image, it presents as follow:

$$p' = d_7 d_6 d_5 d_4 d_3 d_2 d_1 d_0 \tag{20}$$

6) Split the pixel value of the above image. In our proposed scheme, we split the 8-bit pixel value into two 4-bit groups. For the higher 4-bits $d_7 d_6 d_5 d_4$ of the each pixel value as the lower 4-bits of the new pixels, and lower 4 bits $d_3 d_2 d_1 d_0$ form the higher 4-bits [20]. The details of this step showed in Fig.4.

7) Set θ', $(w_0,\ h_0)$, and use the Eq.(12) again to obtain another two random sequences $(W,\ H)$ and employing Eq.(23), Eq.(24) at each elements from the sequences to form the sequences (W', H'). By this way, a pixel p' generate two adjacent pixels p'_l and p'_r. This can make the distribution of pixel values more uniform. There is a numerical example to express this process at Fig.5.

$$W = \{w_{200+1}, w_{200+2}, \ldots, w_{200+k}\} \tag{21}$$

$$H = \{h_{200+1}, h_{200+2}, \ldots, h_{200+k}\} \tag{22}$$

$$w'_k = \mathrm{mod}\left(\lfloor w_k \times 10^{16} \rfloor, 16\right) \tag{23}$$

Fig. 5: A numerical example of B*l*-IEA operation

$$h'_k = \mathrm{mod}\left(\left\lfloor h_k \times 10^{16} \right\rfloor, 16\right) \tag{24}$$

$$p'_l = d_7 d_6 d_5 d_4 \oplus h'_k + w'_k \times 16 \tag{25}$$

$$p'_r = d_3 d_2 d_1 d_0 \oplus w'_k \times 16 + h'_k \tag{26}$$

8) The parameters p and q of *Arnold cat map* are generated by calculating the sum of the pixel values. For p, we calculate the sum of all the pixel, and then modular m or n. The image is divided into several blocks, and a pixel is randomly selected from each block, and then the sum and residual operation is performed to obtain q.
9) For the obtained image, using the *Arnold cat map* in Eq.(10). As described before, the *Arnold cat map* we proposed can efficiently solve the periodic drawback of cat map than that of [25] and break the correlation of two adjacent pixels by only one time mapping.
10) Executing the encryption process until meeting the security requirements.

This image encryption algorithm also applies to RGB color images. Specifically, the color images are firstly divided into three channels R, G and B, and then applying the above algorithm in each channel.

C. Bit-level Image Decryption Algorithm

The decryption procedure is the reverse process of the above encryption. Fig.4 presents the decryption algorithm.

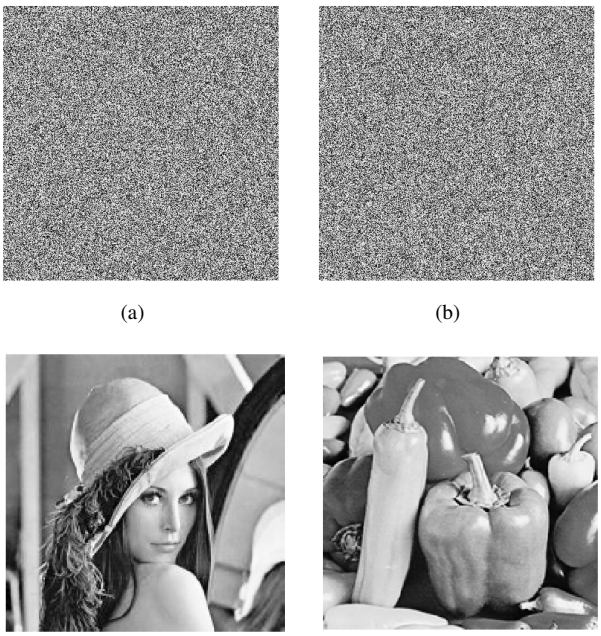
IV. Experiment Results

The proposed B*l*-IEA is applied to the gray images of Lena, Peppers in size 200×200 shown in Fig.6(a) and Fig.6(b). The initial values and control parameters of the Logistic map are $\mu = 3.987654321011137$ and $x_0 = 0.123456789101112$. For 2D-LSCM, the initial seeds and control parameters are $\theta = 0.918765124367853$, $y_0 = 0.788891365924760$, $z_0 = 0.511765894267890$, $\theta' = 0.966854816273549$, $w_0 = 0.748892123456789$ and $h_0 = 0.675438987654321$, respectively. The iteration and encryption parameters of *Arnold cat*

map are 1.The encryption and decryption images are shown in Fig.7(a-d).

(a) (b)

Fig. 6: Original images of Lena (a) and Peppers (b)



(a) (b)

(c) (d)

Fig. 7: The encrypted images (a) and (b); The decryption results (c) and (d)

V. Security and time complexity analysis

A. Key space analysis

K(secret key)									
μ	x_0	θ	y_0	z_0	θ'	w_0	h_0	p	q

Fig. 8: Secret key

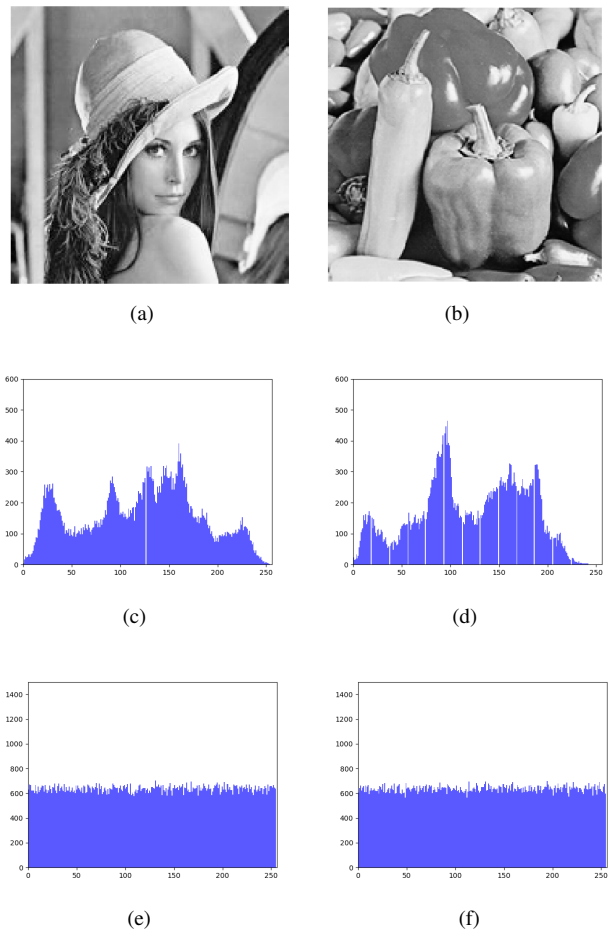
The key space is the total number of different keys that can be used in the encryption process [20]. A secure encryption algorithm should have enough key space to resist brute-force attack. In our proposed scheme, the keys consist of $(\mu,\ x_0,\ \theta',\ w_0,\ h_0,\ \theta,\ y_0,\ z_0,\ p,\ q)$ as the initial values and control parameters of logistic chaotic map and 2D-LSCM chaotic map, respectively. As for p, q, they are the *Arnold cat map* parameters. Fig.8 shows the secret key. Suppose the size of plaintext image is $N * N$. By the four-tuple $[1,\ (p+k_1N),\ (q+k_2N),\ (p+k_1N)\,(q+k_2N)+1]$or $[1,\ p,\ q,\ (pq+1)]$, we can obtain the same cipher for any $k_1, k_2\ \in Z$. Therefore, the total number of ciphering keys which the *Arnold cat map* can provide is N^{2*m}, where m is the iteration times [23]. Besides, if the precision is 10^{-15}, the key space is calculated as follows:

$$10^{15\times 8} \times N^{2\times m} > 10^{15\times 8} \tag{27}$$

where m equals one in the paper. According to Eq.(27), the key space is greater than 2^{250}, which is large enough to resist brute-force attacks [24]. Thus, the brute force attacks on such encryption algorithm becomes infeasible.

B. Statistical analysis

In this section, we have made a statistic analysis of the proposed algorithm from the view of the histogram of the ciphered image, correlations of adjacent pixels in the ciphered image and information entropy of the ciphered image.



(a) (b)

(c) (d)

(e) (f)

Fig. 9: Histogram analysis:(a)(b) are the original images; (c)(d) are the histogram of original images; (e)(f) are the histogram of encrypted images

TABLE I: Chi-square test result of the encryption images

Image	Group 1	Group 2	Group 3
χ^2-value	269.9830	266.5354	286.4665
Decision	Accept	Accept	Accept

1) Histogram: An image histogram is a graph which reflects the relationship of the intensity of the pixels and the number of pixels for each intensity value. Fig.9(c), Fig.9(d) are the histogram of the original images, and Fig.9(e), Fig.9(f) show the histogram of the encrypted images. Comparing the histogram of the original image with the encrypted images', we can see the distribution of the latter is fairly uniform and completely different with the former. The chi-square test can be used to further assess the uniformity of histogram [30].

$$\chi^2 = \sum_{L=0}^{255} \frac{(o_L - e_L)^2}{e_L} \tag{28}$$

where L means the intensity level, O_L and e_L describe the observed datum and the expected one of the L^{th} gray level in the encryption image, respectively. The chi-square test results of the corresponding encryption images of three different groups(contains twelve images) are shown in Tab.I

Apparently, the values of χ^2 are smaller than the critical conditions 293.248 for 255 degrees of freedom with probabilities 5%.Thus, when this method opposes the histogram analysis attack, there is no leakage of any intelligence about the original image.

C. Correlation of two adjacent pixels

Another statistical analysis attack is that the attacker can obtain meaningful information from the high correlation between pixels in the image [21] [31]. Therefore, it is vital to weaken the correlation of adjacent pixels in the encryption. To test the correlation of the adjacent pixels, we randomly selected 1000 adjacent pixel pairs . The calculation of the correlation coefficient of each pair is by Eq.(29).

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{29}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{30}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{31}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)^2 \tag{32}$$

Here x and y are gray values of two adjacent pixels in an image. Eq.(30) is the covariance of the x and y. Besides, $D(x)$ and $E(x)$ describe the variance and expectation of x. Fig.10 shows the specific results of the test. Tab.II indicates the comparation with the algorithm by [32], [33] and [34]. Obviously, the correlation in the encrypted image is significantly weaker than that of the original image.

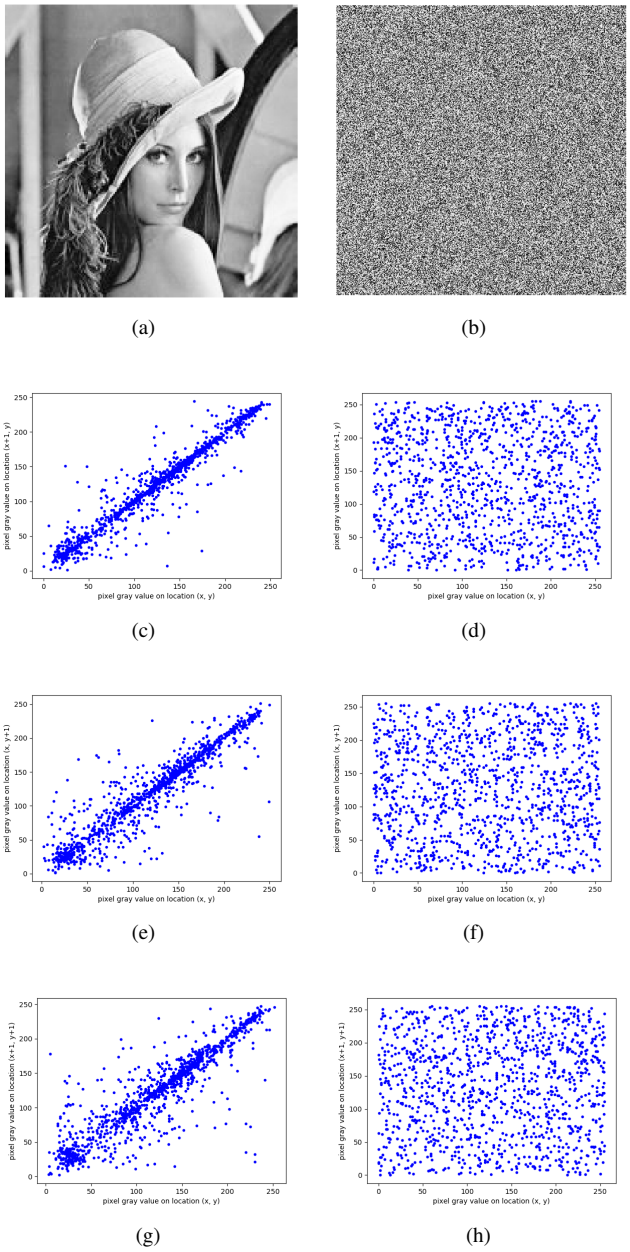


Fig. 10: Auto correlation analysis of plain and encrypted Lena in horizontal, vertical and diagonal directions

TABLE II: Correlation coefficient of two adjacent pixels with different schemes

Algorithm	Image	Horizontal	Vertical	Diagonal
/	Lena	0.9633	0.9341	0.9147
/	Peppers	0.9505	0.9423	0.8928
/	Cameraman	0.9557	0.9174	0.8723
Proposed scheme	Encrypted image	0.0022	-0.0105	-0.0035
[32]		-0.0237	0.0129	0.0283
[33]		0.0385	0.0423	0.0337
[34]		-0.0764	0.0469	-0.0061

D. Information entropy

Information entropy describe the randomness of the information. In image, Shannon entropy is commonly selected to evaluated the randomness of the encryption image [35]. It can describe as following:

$$H(x) = -\sum_{i=1}^{N} p(x_i) \log_2 p(x_i) \tag{33}$$

where $p(x_i)$ is the probability of symbol x_i.The higher entropy means the image is more random. For a true random source generating 2^n symbols, the entropy should be n. Take 256 gray-scale image for example, the entropy is closer to 8 means that the image is more random.From Tab.III, we can find the global value is close to 8. Therefore, the proposed algorithm has the ability to resist information entropy analysis attack .

TABLE III: Global Shannon entropies

Image entropy	Original image	Global Shannon
Lena	7.7691	7.9988
Peppers	7.6223	7.9989
Cameraman	6.8649	7.9987

E. Sensitivity analysis

Sensitivity to key and plaintext image is significant for a security cryptosystem. In this section, we test key sensitivity using original key with tiny change, then estimate the sensitivity to plaintext based on *Number of Pixels Change Rate*(NPCR) and *Unified Averaged Changed Intensity*(UACI).

1) Key sensitivity: An excellent cryptosystem should be sensitive to the secret keys. To test key sensitivity, we performed the experiment with tiny change at one key while kept the others unchanged. The decryption images obtained with the adjusts keys: $\theta' = 0.966854816273548$, $w_0 = 0.748892123456788$, $y_0 = 0.788891365924761$, $a = a+1$, $b = b+1$, respectively. Fig.11 shows all the decryption images with the incorrect keys. The differences between the correct decryption image with the decryption image by the adjusted key are shown in Fig.12. Form the graphes, there are remarkable changes even under a tiny disturbance in the correct fractional order. Obviously, one cannot obtain any meaningful information using the key with tiny change. Therefore, the proposed encryption methods is enough sensitivity to the key.

2) Plaintext sensitivity: In image encryption, the number of pixels change rate(NPCR) and the unified averaged changed intensity(UACI) are two genaral performance indices to analyze plaintext sensitivity [36].

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(m,n)}{MN} \times 100 \tag{34}$$

$$\mathrm{UACI} = \frac{1}{MN}\left[\sum m,n \frac{|c_1(m,n) - c_2(m,n)|}{255}\right] \times 100 \tag{35}$$

Here, c_1 and c_2 describe two encryption images with the same size $M \times N$. If $c_1(m,n) \neq c_2(m,n)$, then $D(m,n) = 1$, otherwise, $D(m,n) = 0$.For a secure cipher, the NPCR is closed to 100% and UACI is greater than 33% [20]. We encrypt 8 images of size $(200*200)$ with the plaintext center pixels gray value added with 1. Tab.IV show the UACI and NPCR performance of all the test images from round 1 to round 7. Apparently, the proposed algorithm has good NPCR and UACI performance which means it is sensitivity to the plaintext, which is significant for immune to differential attack. Tab.V give the performance comparison between this algorithm and others. Tab.V indicates the proposed algorithm has a better performance than that when encrypting images 2 rounds [25]. Thus, the method we proposed is plaintext sensitivity to resist different attacks.

TABLE IV: NPCR and UACI of test images

Image	NPCR(%)	UACI(%)
Lena	99.62258602097833	33.46767233508441
Peppers	99.60114204489756	33.50760738566576
Cameraman	99.61645917066954	33.50503410853607
Gorilla	99.61217037545339	33.36504879375532

TABLE V: NPCR and UACI of different algorithms

Algorithm	NPCR	UACI
Proposed algorithm	0.996120172	0.334613406
[19]	0.995864868	0.332533000
[37]	0.995998382	0.310221067
[38]	0.811958313	0.273860931

F. Analysis of resisting different attacks

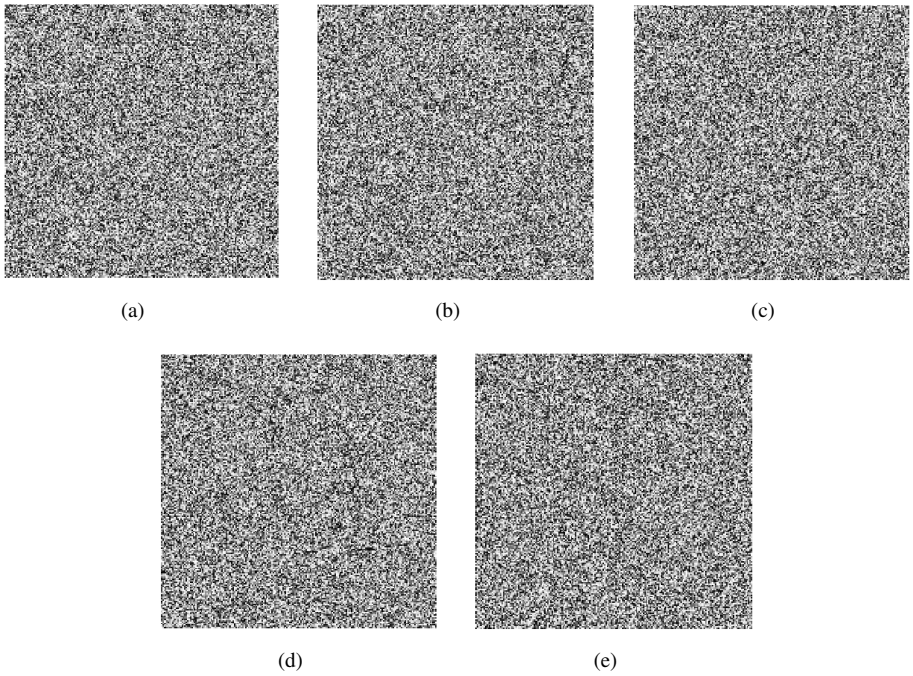
1) differential attacks analysis: The differential attack is that the attacker try to get some meaningful information by the analyzing the different encryption results after adding slight perturbation in the original image [39]. A plaintext sensitivity performance represents the ability of resisting differential attack of the encryption algorithm. In section E(2), we test the UACI and NPCR performance and get a better results in comparative experiments. This indicate the algorithm achieve a higher capacity to against differential attack than other algorithms.

G. Noise attack analysis

An anti-noise image encryption algorithm can obtain the decryption image after add the noise to the encryption image. Suppose that encryption image are attacked by the white noise. It can be described as follow:

$$E' = E + kG \tag{36}$$

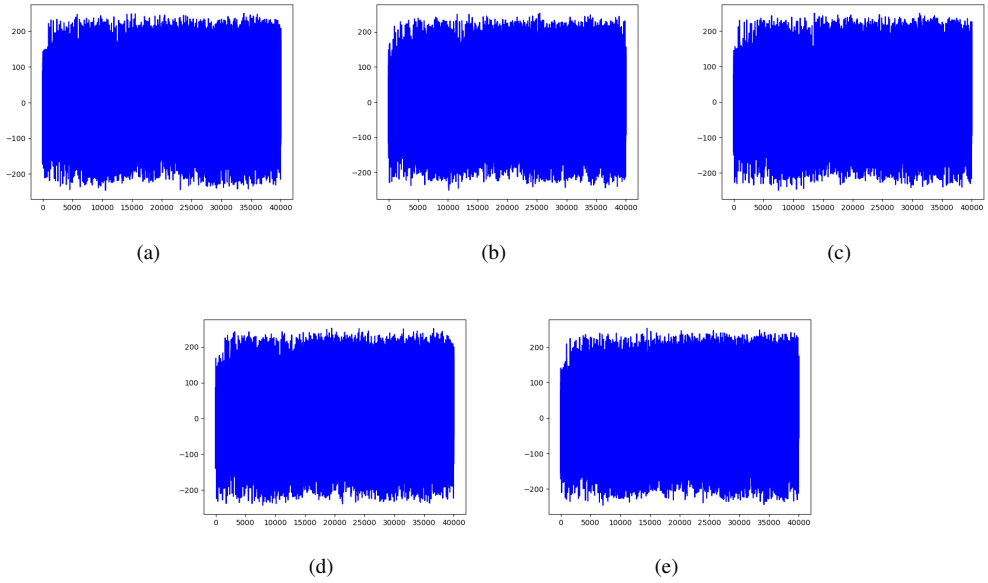
where E and E' represent the noise-free encryption image and the noise-affected encryption image, respectively. G is the white Gaussian noise with zero mean and unit variance, and k denotes the coefficient of noise intensity. To test the ability to noise attack, we decrypt encryption images "Lena" with 4 different noise intensities 0.25, 0.5, 0.75, 1. The results are shown in Fig.13. Although the quality of the decryption decreases with increasing the noise intensity, the proposed algorithm still resist noise attack within a certain range.



(a) (b) (c)

(d) (e)

Fig. 11: Decryption images with incorrect key: θ'(a), w_0(b), y_0(c), p(d), q(e)



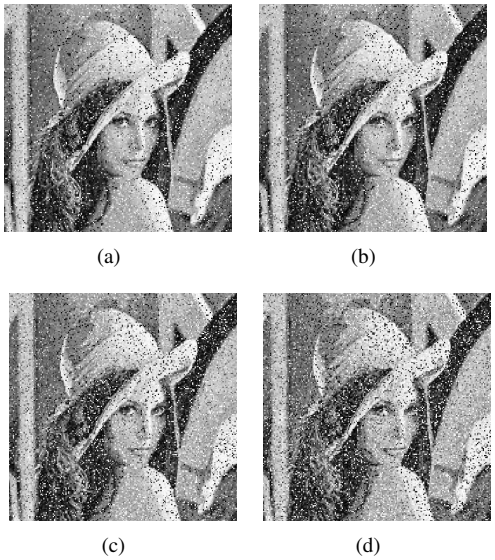
(a) (b) (c)

(d) (e)

Fig. 12: Differences of the decryption between the correct key and the incorrect key: θ'(a), w_0(b), y_0(c), p(d), q(e)

1) Occlusion attack analysis: We perform the encryption image cropped with various format. In our experiment, we fill the cropped part of image with zero to form a new image with the same size. Fig.14 shows the cropped encryption images and the obtained decryption images, respectively. Obviously, the decryption images are still visible and contain most of original visual information within a certain range. Therefore, the proposed algorithm can resist occlusion attack effectively.

2) Analysis of resisting four typical attacks : Among the typical cryptographic attacks, the chosen-plaintext attack is the most difficult to resist.There is no threat to an encryption system if a plaintext attack is chosen, it has the ability against other three typical attacks [40]. There are several image encryption algorithm have been broken by the known-plaintext and chosen-plaintext attacks. Many attackers generally chose all back or white images which has no effect on the shuffling process to attack the algorithm [41]. In this paper, we consider that the encrypted pixel value will be different in the same image as we add the random pixel before the encryption algorithm. Besides, the parameter p of the *Arnold cat map* depend on the plaintext image but q is different from the same plaintext in each encryption process. Therefore, the



(a) (b) (c) (d)

Fig. 13: Decryption of the encrypted images with the noise: $k = 0.25$(a); $k = 0.5$(b); $k = 0.75$(c); $k = 1$(d)

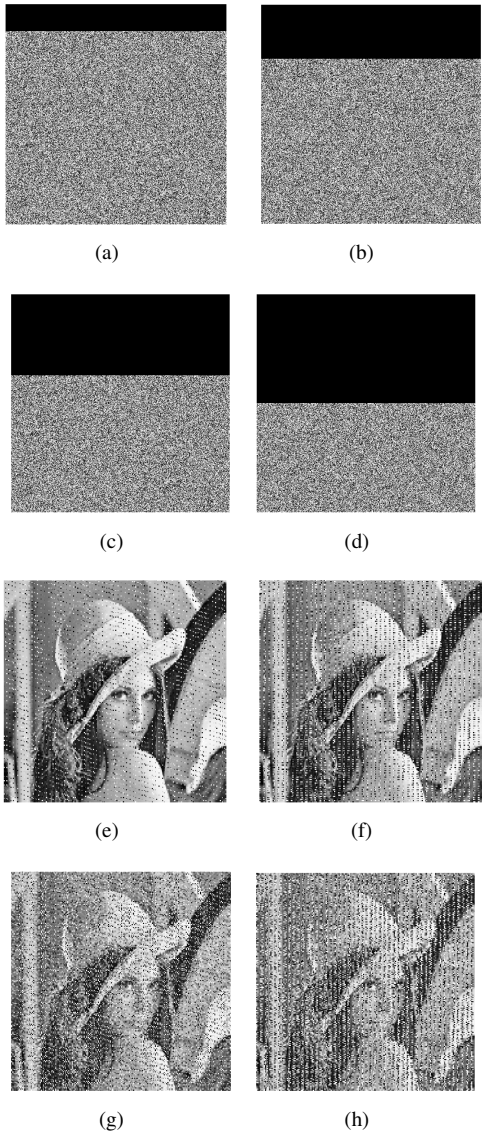
designed algorithm is immune to the known-plaintext and chosen-plaintext attacks and other three typical attack. Fig.15 displays the encrypted results for the all black image and white image and histograms of their encryption images.

H. Time complexity analysis

The efficiency of the encryption algorithm is significant for the real time cryptosystem. The algorithm we proposed executes permutation and diffusion simultaneously to improve the time consumption. In the encryption phase, the algorithm performs well with only one round and employs *Arnold cat map* just one time to break the relationship between adjacent pixels. Comparing with [25], which proposed dynamic random growth technique, the number of times the map is used has been reduced by three times in each round. Without considering the random number generated time-consuming, B*l*-IEA needs $\theta\left(2 \times M \times N\right)$ iterations of shuffle pixels based on *Arnold cat map*, which is less than at least $\theta\left(3 \times M \times N\right)$ iterations. However, since the algorithm in [25] usually performs two rounds to ensure security, so the iterations of shuffle pixels are greater than $\theta\left(6 \times M \times N\right)$. From this perspective, the performance of B*l*-IEA is better.

VI. Conclusion

In this paper, we proposed a novel bit-level image encryption algorithm, B*l*-IEA, based on R-ACM. It breaks the correlations of adjacent pixels well by introducing the rearrangement technology. Moreover, in encryption process, it performs permutation and diffusion simultaneously at bit-level, which improves the encryption efficiency greatly. Experimental results and theoretical analysis also prove that B*l*-IEA is secure enough. Therefore, B*l*-IEA has outstanding performance to be applied in ITS for the collection and transmission of sensitive image information so as to provide more intelligent and precision cognitive services.



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 14: Encryption images with 0.125 (a), 0.25 (c), 0.375 (e), 0.5 (f) occlusion; (b), (d), (f), (h) are the corresponding decryption images

VII. Acknowledgement

This work is supported by the National Key R&D Program of China (No.2020YFB1006002), National Natural Science Foundation of China (No.61972142).

References

[1] G. N. Tytgat, *IEEE Transactions on Intelligent Transportation Systems*. IEEE Transactions on Intelligent Transportation Systems, 2011.

[2] F. Y. Wang, "Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 3, pp. 630–638, 2010.

[3] T. Etsi, "Intelligent transport systems (its); vehicular communications; basic set of applications; definitions," 2009.

[4] Y. Zhang, Y. Li, R. Wang, J. Lu, X. Ma, and M. Qiu, "Psac: Proactive sequence-aware content caching via deep learning at the network edge," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2145–2154, 2020.

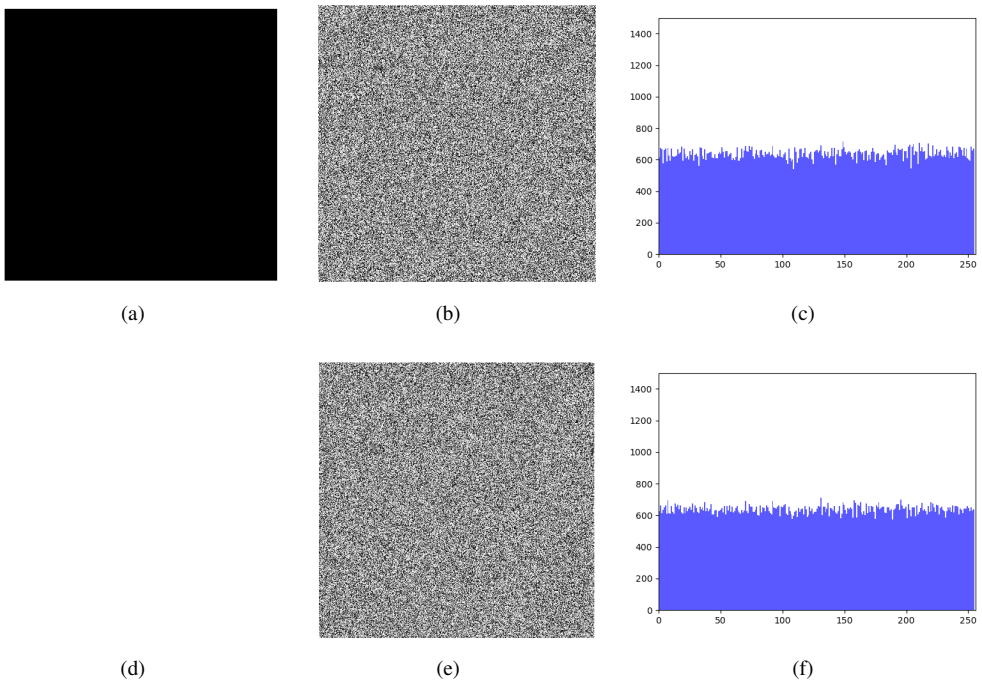


Fig. 15: Encryptions and histograms of all black image and white image

[5] H. Lu, Y. Zhang, Y. Li, C. Jiang, and H. Abbas, "User-oriented virtual mobile network resource management for vehicle communications," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2020.

[6] Y. Sun, J. Liu, K. Yu, M. Alazab, and K. Lin, "Pmrss: Privacy-preserving medical record searching scheme for intelligent diagnosis in iot healthcare," *IEEE Transactions on Industrial Informatics*, vol. PP, pp. 1–1, 04 2021.

[7] K. Yu, Z. Guo, Y. Shen, W. Wang, and T. Sato, "Secure artificial intelligence of things for implicit group recommendations," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2021.

[8] H. Li, K. Yu, B. Liu, C. Feng, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics*, vol. PP, no. 99, 2021.

[9] C. Feng, K. Yu, M. Aloqaily, M. Alazab, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent iov," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 784–13 795, 2020.

[10] Z. Hua and Y. Zhou, "Image encryption using 2d logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[11] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory," *Information Sciences*, vol. 507, pp. 16–36, 2020.

[12] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation," *Optics & Laser Technology*, vol. 121, p. 105777, 2020.

[13] W. Shi, F. Jiang, S. Liu, and D. Zhao, "Image compressed sensing using convolutional neural network," *IEEE Transactions on Image Processing*, vol. 29, pp. 375–388, 2019.

[14] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22 023–22 043, 2019.

[15] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on dna sequence operations and chaotic systems," *Neural Computing and Applications*, vol. 31, no. 1, pp. 219–237, 2019.

[16] A. Kulsoom, D. Xiao, A. ur Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 1–23, 2016.

[17] Z. Hua, F. Jin, B. Xu, and H. Huang, "2d logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[18] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Optics and Lasers in Engineering*, vol. 134, p. 106202, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0143816619315969

[19] X. Y. Wang, S. X. Gu, and Y. Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering*, vol. 68, pp. 126–134, 2015.

[20] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[21] Y. Q. Zhang and X. Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[22] N. A. Abbas, "Image encryption based on independent component analysis and arnold' s cat map," *Egyptian informatics journal*, vol. 17, no. 1, pp. 139–146, 2016.

[23] J. Zhang, "An image encryption scheme based on cat map and hyperchaotic lorenz system," in *2015 IEEE International Conference on Computational Intelligence & Communication Technology*. IEEE, 2015, pp. 78–82.

[24] A. B. Joshi, D. Kumar, A. Gaffar, and D. Mishra, "Triple color image encryption based on 2d multiple parameter fractional discrete fourier transform and 3d arnold transform," *Optics and Lasers in Engineering*, vol. 133, p. 106139, 2020.

[25] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[26] F. Svanström, "Properties of a generalized Arnold's discrete cat map," p. 36, 2014.

[27] E. Buben í kov á , M. Franekov á , and A. Kan á likov á , "Modern methods of image processing in safety-critical applications within intelligent transportation system," in *International Conference on Transport Systems Telematics*, 2017.

[28] Y. Zhang, H. Wen, F. Qiu, Z. Wang, and H. Abbas, "ibike: Intelligent public bicycle services assisted by data analytics," *Future Generation Computer Systems*, 2018.

[29] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, and M. Guizani, "Heterogeneous information network-based content caching in the inter-

net of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 10 216–10 226, 2019.
[30] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing dicom image," *Computers in biology and medicine*, vol. 72, pp. 170–184, 2016.
[31] X. Zhang, H. Zhang, and C. Xu, "Reverse iterative image encryption scheme using 8-layer cellular automata," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 7, pp. 3397–3413, 2016.
[32] C. Yu, J. Li, X. Li, X. Ren, and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform , chaos and computer generated hologram," pp. 4585–4608, 2018.
[33] S. M. Pan, R. H. Wen, Z. H. Zhou, and N. R. Zhou, "Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional mellin transform," *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 2933–2953, 2017.
[34] X. D. Chen, Q. Liu, J. Wang, and Q. H. Wang, "Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction," *Optics & Laser Technology*, vol. 107, pp. 302–312, 2018.
[35] H. Liu, X. Wang *et al.*, "Image encryption using dna complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.
[36] G. Ye and J. Zhou, "A block chaotic image encryption scheme based on self-adaptive modelling," *Applied Soft Computing*, vol. 22, pp. 351–357, 2014.
[37] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.
[38] Z. l. Zhu, W. Zhang, K. w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.
[39] W. Wen, Y. Zhang, M. Su, R. Zhang, J. xin Chen, and M. Li, "Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 383–390, 2017.
[40] 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, 2019.
[41] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.

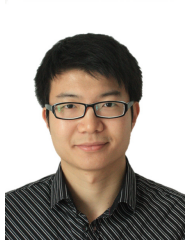
Yi SUN received the Ph.D. degree in Computer Science and Technology from Beijing University of Posts and Telecommunications, Beijing, China, in 2015. She is currently a lecturer at the School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications. She serves as the Associate Editor for Wireless Communications and Mobile Computing Journal and Journal of Circuits, Systems and Computers. She is a Guest Editor for Electronic Markets, ACM/Springer Mobile Networks & Applications, etc. She is the TPC of IEEE GLOBECOM 2021-WS01, PC of the ICME-2020&2021, DSC-2019, CAIML-2021, OC of the ICNCIS-2021. Her research interests include information security, secure multiparty computation, blockchain, artificial intelligence and internet of things.

Keping YU received the M.E. and Ph.D. degrees from the Graduate School of Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan, in 2012 and 2016, respectively. He was a Research Associate and a Junior Researcher with the Global Information and Telecommunication Institute, Waseda University, from 2015 to 2019 and 2019 to 2020, respectively, where he is currently a Researcher.

Dr. Yu has hosted and participated in more than ten projects, is involved in many standardization activities organized by ITU-T and ICNRG of IRTF, and has contributed to ITU-T Standards Y.3071 and Supplement 35. He received the Best Paper Award from ITU Kaleidoscope 2020, the Student Presentation Award from JSST 2014. He has authored 100+ publications including papers in prestigious journal/conferences such as the IEEE WirelComMag, NetMag, TFS, IoTJ, TII, T-ITS, TVT, TNSE, TGCN, CEMag, IoTMag, ICC, GLOBECOM etc. He is an Editor of IEEE Open Journal of Vehicular Technology (OJVT). His research interests include smart grids, information-centric networking, artificial intelligence, blockchain, and information security.

Ali Kashif Bashir received his Ph.D. in computer science and engineering from Korea University, South Korea. He is a Senior Lecturer/Associate Professor at the Department of Computing and Mathematics, Manchester Metropolitan University, UK. He is also with the National University of Science and Technology (NUST), Pakistan and with University of Electronics Science and Technology of China (UESTC) as visiting professor and Chief Advisor of Visual Intelligence Research Center, UESTC. He is a senior member of IEEE and Distinguished Speaker of ACM. His past assignments include University of the Faroe Islands, Denmark; Osaka University, Japan; Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea, and the Seoul Metropolitan Government, South Korea.

He has authored over 150 research articles; received funding from research bodies of South Korea, Japan, EU, UK and Middle East. His research interests include internet of things, wireless networks, distributed systems, network/cyber security, network function virtualization, machine learning, etc. He is serving as the Editor-in-chief of the IEEE FUTURE DIRECTIONS NEWSLETTER. He has served/serving as editors (associate or guest) for several journals like IEEE Transaction on Industrial Informatics, IEEE Internet of Things Magazine, IEEE Access, etc.



Xin LIAO received the B.E. and Ph.D. degree in information security from Beijing University of Posts and Telecommunications, in 2007 and 2012, respectively. He worked as a post-doctoral fellow at Institute of Software, Chinese Academy of Sciences, and also a research associate at The University of Hong Kong. From 2016 to 2017, he was a visiting scholar at University of Maryland, College Park, USA. He is currently an associate professor and doctoral supervisor at Hunan University, China. He is serving as the Associate Editor for IEEE Signal Processing Magazine. He is also a member of Technical Committee (TC) on Multimedia Security and Forensics of Asia Pacific Signal and Information Processing Association, TC on Computer Forensics of Chinese Institute of Electronics, and TC on Digital Forensics and Security of China Society of Image and Graphics. His current research interests include multimedia forensics, steganography and watermarking.