

A lightweight symmetric image encryption cryptosystem in wavelet domain based on an improved sine map

Baichi Chen(陈柏池), Linqing Huang(黄林青), Shuting Cai(蔡述庭), Xiaoming Xiong(熊晓明), and Hui Zhang(张慧)

Citation: Chin. Phys. B, 2024, 33 (**3**): 030501. DOI: 10.1088/1674-1056/ad1030
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

A chaotic hierarchical encryption/watermark embedding scheme for multi-medical images based on row-column confusion and closed-loop bi-directional diffusion

Zheyi Zhang(张哲祎), Jun Mou(牟俊), Santo Banerjee, and Yinghong Cao(曹颖鸿)
Chin. Phys. B, 2024, 33 (**2**): 020503. DOI: 10.1088/1674-1056/ad0775

Enhancing visual security: An image encryption scheme based on parallel compressive sensing and edge detection embedding

Yiming Wang(王一铭), Shufeng Huang(黄树锋), Huang Chen(陈煌), Jian Yang(杨健), and Shuting Cai(蔡述庭)
Chin. Phys. B, 2024, 33 (**1**): 010502. DOI: 10.1088/1674-1056/ad01a1

Asymmetric image encryption algorithm based on a new three-dimensional improved logistic chaotic map

Guo-Dong Ye(叶国栋), Hui-Shan Wu(吴惠山), Xiao-Ling Huang(黄小玲), and Syh-Yuan Tan
Chin. Phys. B, 2023, 32 (**3**): 030504. DOI: 10.1088/1674-1056/ac7dbb

A color image encryption algorithm based on hyperchaotic map and DNA mutation

Xinyu Gao(高昕瑜), Bo Sun(孙博), Yinghong Cao(曹颖鸿), Santo Banerjee, and Jun Mou(牟俊)
Chin. Phys. B, 2023, 32 (**3**): 030501. DOI: 10.1088/1674-1056/ac8cdf

Lossless embedding: A visually meaningful image encryption algorithm based on hyperchaos and compressive sensing

Xing-Yuan Wang(王兴元), Xiao-Li Wang(王晓丽), Lin Teng(滕琳), Dong-Hua Jiang(蒋东华), and Yongjin Xian(咸永锦)
Chin. Phys. B, 2023, 32 (**2**): 020503. DOI: 10.1088/1674-1056/aca149

A lightweight symmetric image encryption cryptosystem in wavelet domain based on an improved sine map

Baichi Chen(陈柏池)[1,†], Linqing Huang(黄林青)[1,†], Shuting Cai(蔡述庭)[2], Xiaoming Xiong(熊晓明)[2], and Hui Zhang(张慧)[3,‡]

[1] *School of Advanced Manufacturing, Guangdong University of Technology, Jieyang* 522000, *China*
[2] *School of Integrated Circuits, Guangdong University of Technology, Guangzhou* 510006, *China*
[3] *School of Automation, Guangdong University of Technology, Guangzhou* 510006, *China*

(Received 21 October 2023; revised manuscript received 20 November 2023; accepted manuscript online 28 November 2023)

In the era of big data, the number of images transmitted over the public channel increases exponentially. As a result, it is crucial to devise the efficient and highly secure encryption method to safeguard the sensitive image. In this paper, an improved sine map (ISM) possessing a larger chaotic region, more complex chaotic behavior and greater unpredictability is proposed and extensively tested. Drawing upon the strengths of ISM, we introduce a lightweight symmetric image encryption cryptosystem in wavelet domain (WDLIC). The WDLIC employs selective encryption to strike a satisfactory balance between security and speed. Initially, only the low-frequency-low-frequency component is chosen to encrypt utilizing classic permutation and diffusion. Then leveraging the statistical properties in wavelet domain, Gaussianization operation which opens the minds of encrypting image information in wavelet domain is first proposed and employed to all sub-bands. Simulations and theoretical analysis demonstrate the high speed and the remarkable effectiveness of WDLIC.

Keywords: image encryption, discrete wavelet transform, 1D-chaotic system, selective encryption, Gaussianization operation

PACS: 05.45.–a, 43.60.Hj **DOI:** 10.1088/1674-1056/ad1030

1. Introduction

With the Internet diffusion, images have become the most significant carrier of multimedia information. However, images are susceptible to illegal interception and tampered by attackers when it is distributed on public servers, causing great losses and harm to users. In this context, to secure the image transmission, some technologies like image encryption, image hiding[1,2] and image watermarketing[3] have been widely studied.

In recent decades, chaotic systems have been extensively used in cryptography because of the inherent properties like unpredictability, aperiodicity, complexity and can generate pseudo-random sequences rapidly. Therefore, image encryption algorithms based on chaotic systems have been continuously proposed and improved.[4–21] Compared with high dimensional chaotic system, a one-dimensional (1D) chaotic map is easier to implement and widely used to develop image encryption pursuing high encryption speed. For example, in Ref. [7], the technology of total shuffling was used to develop a linear–nonlinear–linear structure which was then applied in producing permutation position matrix and the diffusion matrix involved in image encryption. In 2014, Zhou[8] combined with two existing 1D chaotic maps (seed maps) to construct a new chaotic system with more complex chaotic behaviors. Then four rounds of encryption are performed to enhance the robustness and security against various attacks. For most image encryption algorithms, the encryption operation is performed in spatial domains combining diverse technologies such as deoxyribonucleic acid (DNA) coding,[9–13] elliptic curve,[14–16] quantum theory,[17,18] neural network,[19] and so on. DNA computing is widely used in image encryption due to its advantages such as enormous parallelism, high information density, and low power consumption. In Ref. [11], Wu *et al.* presented a content-aware module to design a DNA computing system that can be employed to permute and diffuse the encoded medical image. Compared to RSA encryption, elliptic curve cryptography (ECC) which can mitigate the performance overhead in computation processes, is especially suitable for applications in scenarios with constrained device resources. With the application of ECC, Sasikaladevi *et al.*[14] introduced a hybrid multilayered hyper-chaotic hyper-elliptic curve to encrypt image losslessly. DNA bit scrambling was applied in original image during hyper chaotic encoding process and then the curve function was used to obtain valid points to diffuse the image. Quantum walk, a random walk model based on quantum mechanics, has good randomization and unpredictability, which enables its application in cryptography. In 2022, a controlled alternated quantum walks scheme was proposed by Gao *et al.*[18] to construct substitution boxes. Three-quarters of the image which was scrambled by the quan-

[†]These authors contributed equally to this work.
[‡]Corresponding author. E-mail: zh2008@gdut.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

tum Arnold block transform were divided into 32 blocks substituted with different S-boxes. Memristor has unique memory function and is utilized as an artificial nerve synapse. In Ref. [19], a memristive Hopfield neural network (HNN) processing complex dynamical behaviors was proposed by Lai *et al*. and applied to image encryption.

Image encryption based on transform domains is another research direction and have been studied by many researchers.[22–28] For example, in Ref. [22], an XOR operation is performed between the DNA matrix transformed by the plain image and a random phase mask, and then employing the fractional Fourier transform three times in the substituted image before further encryption. To minimize the transmission load, a two-dimensional (2D) discrete cosine Stockwell transform was utilized to compress the image.[23] Then DNA-level modulus diffusion was performed on the compressed image to gain confusion and diffusion effects simultaneously. Wavelet transform is a mathematical tool for image decomposition. In some image encryption schemes based on wavelet transform, the image in spatial domain was firstly converted to wavelet domain and then undergone further processing and encryption operations. For example, the wavelet transform is used to sparsify the image before compression sensing.[29–32] In Ref. [31], after wavelet transform and compression sensing, the original image was compressed into a smaller size image that was encrypted using confusing and singular value decomposition, which harvested the less time complexity compared to other techniques. In some other image encryption schemes, encryption operations are performed directly in wavelet domain.[33–35] Since the low-frequency coefficients contain most of the information of the oringin image, while the high-frequency coefficients contain more details, to obtain higher encryption efficiency, some sub-bands are selected to encrypt. In Ref. [33], a plaintext was decomposed into four sub-bands by discrete wavelet transform. According to their weights, the low-frequency image was confused firstly and then four sub-bands was encrypted under the feedback from the confused low-frequency image. This scheme uses dynamic keys generated by message-digest algorithm 5 that uses plaintext image as input. It means that the keys needed to be transmitted to receiver when encrypting a new image, which reduces the value of application. In Ref. [34], only the low-low frequecy component decomposed by two level discrete wavelet transform was shuffled and diffused only one round. The author claims that the proposed scheme have high plaintext sensitivity but the analysis results are difficult to support the conclusion.

For the fact that, the statistical properties of every sub-bands in the wavelet domain of a random information source follow Gaussian distribution. In this research, a new image encryption structure was proposed according to the statistical characteristics. A brief summary of the overall contribution of the work is as follows:

(i) An improved sine map was designed and extensively tested to possess a larger chaotic region, more complex chaotic behavior and greater unpredictability.

(ii) Different from existing spatial-domain and wavelet-domain image encryption systems, according to the statistical properties of a true random information source in wavelet domain, a noval encryption framework based on ISM was proposed.

(iii) Complete simulations and theoretical analysis were conducted to demonstrate the high speed and the remarkable effectiveness of WDLIC.

The remainder of this paper is as follows: an introduction to the discrete wavelet transform (DWT) and statistical properties of a true random information source in wavelet domain are presented in Section 2. Section 3 presents the improved sine map. Section 4 gives a complete description of the lightweight symmetric image cryptosystem in wavelet domain. Section 5 delivers the simulation and security analysis results of the algorithm. Eventually, we draw a conclusion in Section 6.

2. Related work

2.1. Discrete wavelet transform

DWT can be used to decompose an image into four sub-bands, namely high-frequency–high-frequency (HH), high-frequency–low-frequency (HL), low-frequency–high-frequency (LH), and low-frequency–low-frequency (LL) as illustrated in Fig. 1. Figure 2 shows the one level decomposition of Lena. Most of the image energy is concentrated in the low-frequency band and the three high-frequency bands depict the image details in horizontal, vertical and diagonal directions respectively. So in this research, the low-frequency band was chosen as the cryptographic object.

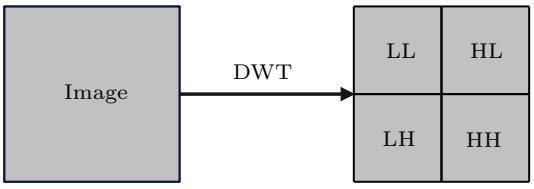


Fig. 1. One level wavelet decomposition.

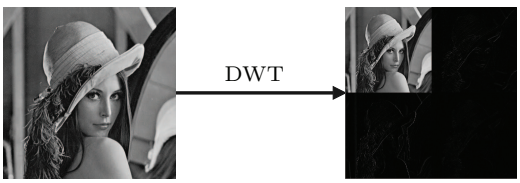


Fig. 2. One level wavelet decomposition of Lena.

The detailed processing of the Haar wavelet transform for an image is as follows:[33]

$$\mathrm{LL}(x,y) = \frac{p(x,y)+p(x,y+1)+p(x+1,y)+p(x+1,y+1)}{2},$$

$$\begin{aligned}\mathrm{LH}(x,y) &= \frac{p(x,y)+p(x,y+1)-p(x+1,y)-p(x+1,y+1)}{2},\\ \mathrm{HL}(x,y) &= \frac{p(x,y)-p(x,y+1)+p(x+1,y)-p(x+1,y+1)}{2},\\ \mathrm{HH}(x,y) &= \frac{p(x,y)-p(x,y+1)-p(x+1,y)+p(x+1,y+1)}{2},\end{aligned} \tag{1}$$

where $p(x,y)$, $p(x,y+1)$, $p(x+1,y)$, and $p(x+1,y+1)$ are four neighboring pixels in the original image.

2.2. Statistical properties in wavelet domain

For a random image, the occurrence probability of each gray level is $1/256$. According to Eq. (1), because p follows a uniform distribution $x \sim U(256)$ where $P(x=i)=1/256$ $(i=0,1,2,\ldots,255)$, LL approximately matches the Gaussian distribution $x \sim N(255, 5.4613\times 10^3)$ and other three sub-bands follow $x \sim N(0, 5.4613\times 10^3)$, which are demonstrated in Fig. 3.

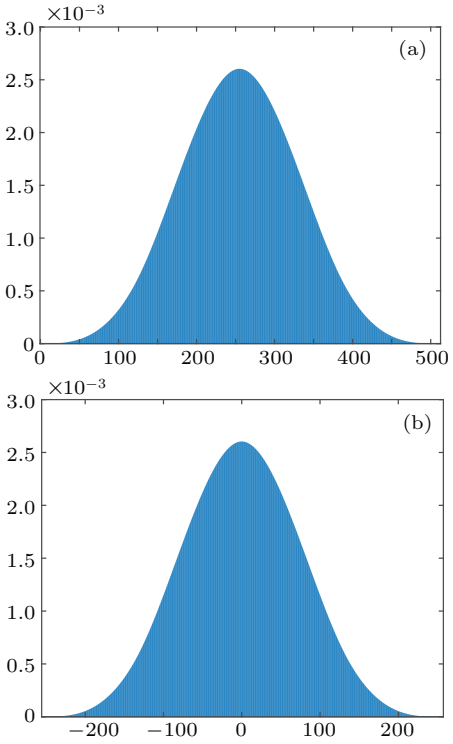


Fig. 3. Statistical properties of (a) LL, (b) HH, HL, and LH.

3. Improved sine map

Sine map is a well-known 1D chaos map and can be represented by

$$x_{n+1} = \frac{1}{4}\gamma \sin(\pi x_n). \tag{2}$$

The simple map has limited chaotic range as illustrated in Fig. 6(b). In our work, an improved sine map is proposed and defined by

$$x_{n+1} = (r+2)\sin\left(\frac{\pi}{x_n^3}\right), \tag{3}$$

where r is a control parameter.

In order to verify its chaotic performance, Lyapunov exponent test, bifurcation analysis, sample entropy, 0–1 test, and NIST test are performed in the following subsections.

3.1. Lyapunov exponent test

Lyapunov exponent (LE) characterizes the average exponential rate of convergence or divergence between neighboring orbits of the system in phase space and is given by

$$\lambda = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|, \tag{4}$$

where n is the size of the generated time series $f(x_n)$.

A positive value of LE indicates that in the phase space, a small initial distance between the two trajectories will increase exponentially with the evolution of time. A comparative analysis of ISM and other chaotic maps including logistic-sine-cosine,[36] 1-DFCS,[37] 1-DSP,[38] and sine map is given and its result is shown in Fig. 4. We can observe that the proposed ISM map has larger LE values over a larger parameter range than other recently proposed chaotic systems. In order to visually assess the sensitivity of ISM to the initial values and control parameters, figure 5 plots the output chaotic sequences generated with different initial values or control parameters.

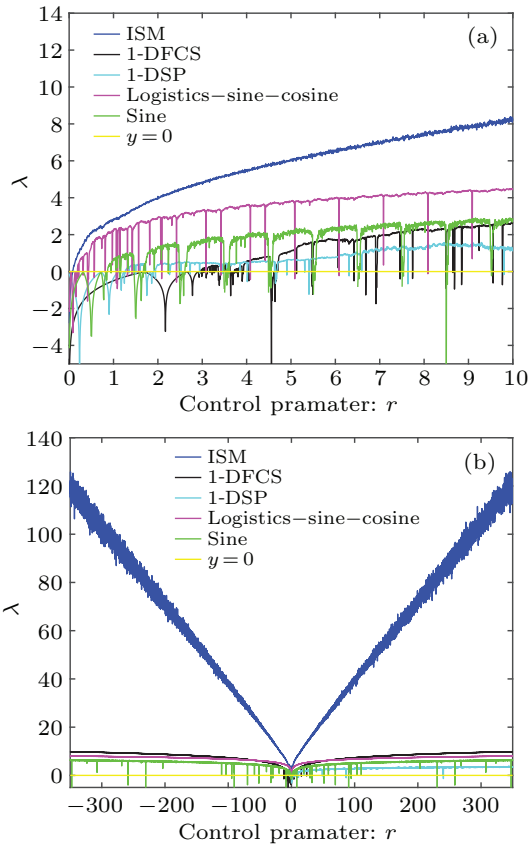


Fig. 4. Lyapunov exponent of different chaotic maps.

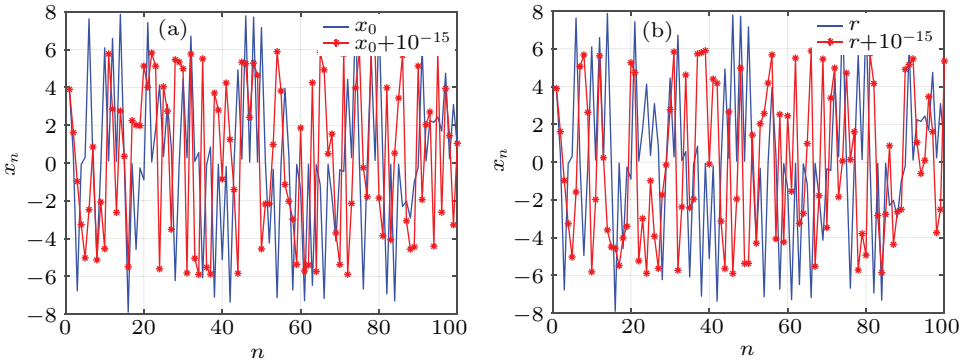


Fig. 5. Initial value and pramater sensitivity of ISM.

3.2. Bifurcation analysis

The period-doubling bifurcation path is one of the common paths to chaos. Figure 6 shows the bifurcation diagrams of ISM, logistic–sine–cosine, 1-DFCS, 1-DSP, and sine map. Relative to other chaotic mappings, the bifurcation diagram exhibits that ISM possesses a much larger chaotic range.

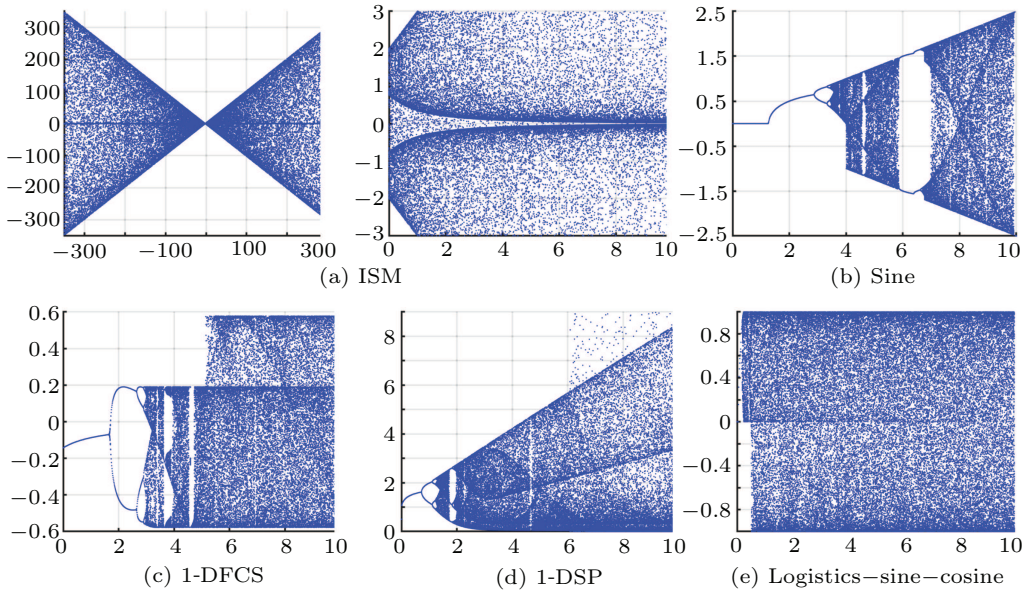


Fig. 6. Bifurcation diagram.

3.3. Sample entropy

The regularity of the time series generated by dynamic systems can be measured by sample entropy (SampEn).[39] A larger SampEn value indicates less self-similarity of the time series, which means the dynamic system has a higher complexity. In Eq. (5), the template vector $D_m(i)$ with a length of m is taken from the time series $\{X(i), X(i+1), \ldots, X(i+m-1)\}$. The SampEn of the time series X is calculated in Eq. (6).

$$D_m(i) = [X(i), X(i+1), \ldots, X(i+m-1)], \tag{5}$$

$$\mathrm{SampEn}(m, r, N) = -\ln \frac{A}{B}, \tag{6}$$

where r denotes tolerance. A and B are the total numbers of vectors satisfying the conditions $d[X_{m+1}(i), X_{m+1}(j)] < r$ and $d[X_m(i), X_m(j)] < r$ respectively. $d[X_m(i), X_m(j)]$ is the Chebyshev distance between $X(i)$ and $X(i+m-1)$. In our test, m and r are set to 2 and $0.2 \times$ std. The results of SampEn comparison experiments are shown in Fig. 7 which demonstrates that the time series generated by ISM has higher randomness.

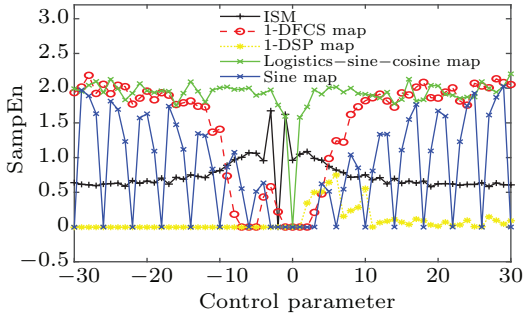


Fig. 7. SampEn comparative experiment.

3.4. The 0–1 test

The 0–1 test can be used to determines the presence of chaos in a dynamical system by calculating the linear growth

rate Kc of the discrete data transformation variables and defined by

$$K = \frac{\log M(n)}{\log n}, \tag{7}$$

$$M(n) = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{n}[p(i+n)-p(i)]^2 + [s(i+n)-s(i)]^2, \tag{8}$$

$$p(n) = \sum_{i=1}^{n} X(i)\cos(ir), \tag{9}$$

$$s(n) = \sum_{i=1}^{n} X(i)\sin(ir), \tag{10}$$

where X is a time series with the size of N and is generated by ISM. The constant r is set to 2. If the output results close to 1, the dynamical system exists chaotic behaviors. The test results of the four different mappings are illustrated in Fig. 8. The test result of ISM is close to 1 when $r \in (-350, 350)$. Therefore, we can conclude that ISM has better chaotic properties compared to the other four 1D chaotic maps.

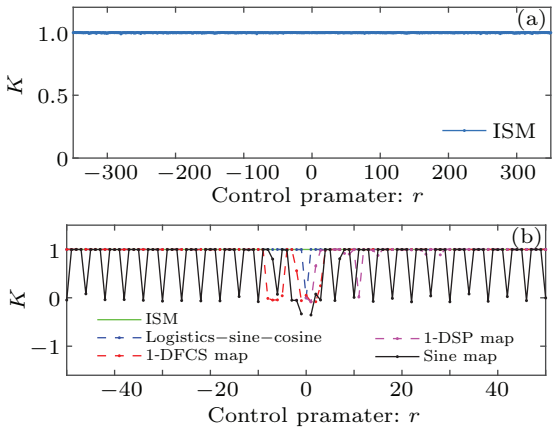


Fig. 8. The 0–1 test.

3.5. NIST SP 800-22 test

SP 800-22 developed by the National Institute of Standards and Technology (NIST) was utilized to validate the randomness of the sequences generated by ISM.[40] SP 800-22 consists of 15 subtests and uses a set of binary sequences as input. Then each subtest result, namely P-values serves as a measure of randomness of the system. In our test, ISM generates a total of 1.25×10^5 bit binary numbers as input and all the test results fall into $(0.01, 1)$ as shown in Table 1, which proves that the sequences generated by ISM iterations boast a higher degree of randomness and are suitable for image encryption.

Table 1. NIST SP 800-22 test of ISM.

Test	P-value	State
Frequency (monobit) test	0.739918	PASS
Frequency test within a block	0.494392	PASS
Cumulative sums (cusums) test	0.590983	PASS
Runs test	0.574903	PASS
Longest run of ones in a block test	0.759756	PASS
Binary matrix rank test	0.236810	PASS
Discrete fourier transform (spectral) test	0.153763	PASS
Non-overlapping template matching test	0.451530	PASS
Overlapping template matching test	0.019188	PASS
Maurers universal statistical test	0.153763	PASS
Approximate entropy test	0.401199	PASS
Random excursions test	0.504436	PASS
Random excursions variant test	0.361067	PASS
Serial test	0.821464	PASS
Linear complexity test	0.983453	PASS

4. The proposed image cryptosystem

In this section, we construct a lightweight symmetric image encryption cryptosystem in wavelet domain. Figure 9 depicts the encryption and decryption flowchart of our proposed cryptosystem.

In the following, we describe the proposed encryption cryptosystem in details:

Step 1 Alice's fingerprint image Fin is fed into SHA-256 to generate a 256-bit hash value f which is used as the secret key.

Step 2 The plaintext P with the size of $M\times N$ is used as input to SHA-512 hash function to produce a 512-bit binary number h. f and h are first processed by Eq. (11).

$$\begin{aligned} R_1(i) &= \text{bin2dec}(h(8i-7:8i)),\\ R_2(i) &= \text{bin2dec}(h(8i+249:8i+256)),\\ f_1(i) &= \text{bin2dec}(f(8i-7:8i)), \end{aligned} \tag{11}$$

where $i = 1,2,\ldots,32$ and the function bin2dec can convert binary numbers to decimal numbers.

Then in Eq. (12), pairwise XOR operations are performed on R_1, R_2, and R to obtain H which is used to generate two plaintext-related parameter arrays h_1 and h_2. h_1 and h_2 are subsequently used to generate the random image and use in diffusion process.

$$\begin{aligned} &R(i) = R_1(i)\oplus R_2(i), && i = 1,2,\ldots,32,\\ &H(i) = R(i)\oplus R(i+16), && i = 1,2,\ldots,16,\\ &h_1 = H(1:8),\\ &h_2 = H(9:16). \end{aligned} \tag{12}$$

For the purpose of improving the plaintext sensitivity, f_1 is used to obtain chaotic initial values x_0, y_0, z_0, and N_0 by

$$\begin{aligned} x_0 &= \frac{f_1(1)}{f_1(2)},\\ y_0 &= \text{mod}(\text{sum}(f_1(3:17)),350),\\ z_0 &= \text{mod}(\text{sum}(f_1(18:32)),350),\\ N_0 &= f_1(1)\times f_1(2). \end{aligned} \tag{13}$$

Step 3 By using x_0, y_0, and z_0 as initial values respectively, the ISM is iterated to generate three random sequences x, y, and z as

$$x = \{x_1, x_2, \ldots, x_{N_0+M+N}\},$$

$$y = \{y_1, y_2, \ldots, y_{N_0+1}\},$$
$$z = \{z_1, z_2, \ldots, z_{N_0+1}\}. \quad (14)$$

It is worth noting that the former N_0 elements are discarded. In Eq. (15), y_1 and z_1 are used to preprocess the random sequence x to obtain a new sequence X

$$X(i) = x_i \times y_1 \times z_1, \quad i = 1, 2, \ldots, (M+N). \quad (15)$$

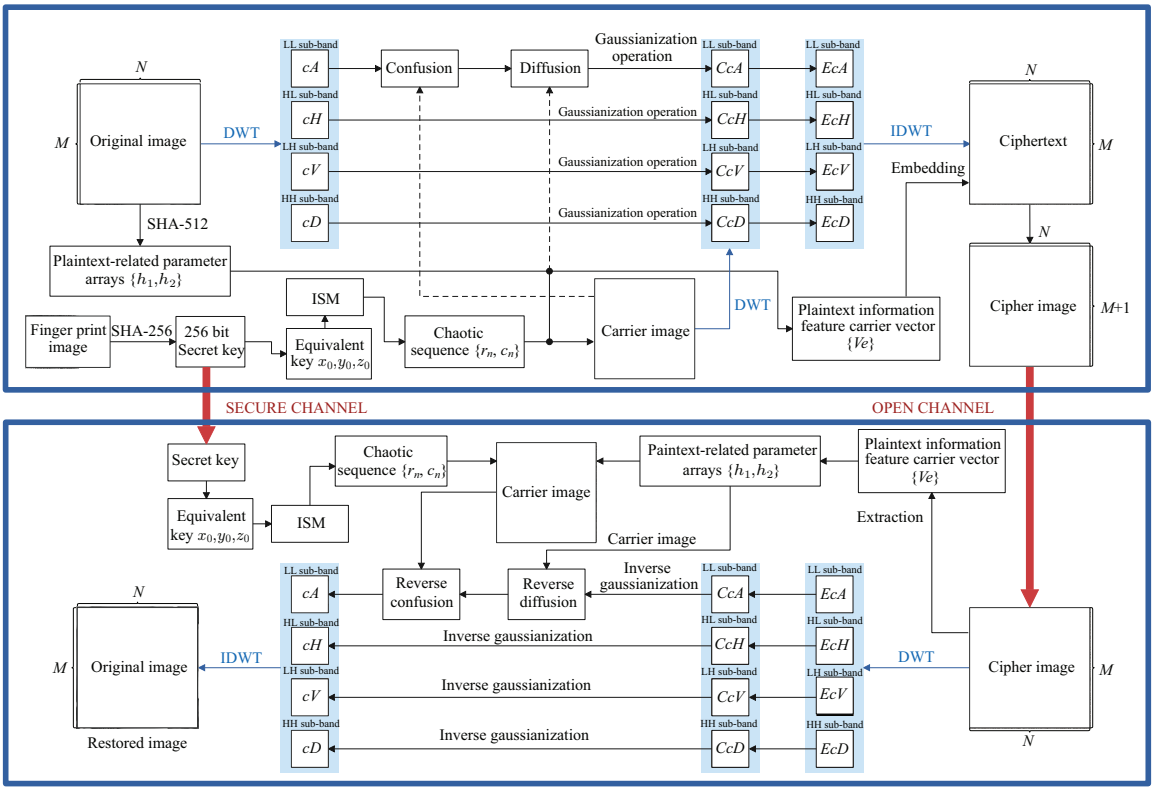


Fig. 9. The proposed image cryptosystem.

And then two 1D arrays r_n, c_n with the length of M and N respectively are obtained by the following operation:

$$r_n = X(1:M),$$
$$c_n = X(M+1:M+N). \quad (16)$$

Step 4 The vectors h_1, h_2, r_n, and c_n are utilized to generate a random image Pc with the same size of the plaintext image by

$$\begin{aligned} &Pc(i,j) \\ &= \lfloor \mathrm{mod}(\mathrm{mod}((r_n(i) \times h_1(\mathrm{mod}(i \times j, 8) + 1) \times 10^{10}), 256) \\ &\quad + c_n(j) \times h_2(\mathrm{mod}(i \times j, 8) + 1) \times 10^{10}, 256) \rfloor. \end{aligned} \quad (17)$$

Step 5 DWT is performed on the plaintext image P and the random image Pc to obtain their corresponding four sub-bands, which is expressed as Eq. (18). Four sub-bands cA, cH, cV, and cD correspond to low-frequency–low-frequency (LL), high-frequency–low-frequency (HL), low-frequency–high-frequency (LH), and high-frequency–high-frequency (HH) respectively.

$$[cA, cH, cV, cD] = dwt2(P, 'haar'),$$
$$[CcA, CcH, CcV, CcD] = dwt2(Pc, 'haar'). \quad (18)$$

And then converts the coefficients' values of HL, LH, and HH into positive ones as

$$\begin{aligned} cH &= cH + 256, \\ cV &= cV + 256, \\ cD &= cD + 256, \\ CcH &= CcH + 256, \\ CcV &= CcV + 256, \\ CcD &= CcD + 256. \end{aligned} \quad (19)$$

Step 6 Because the low frequency component contains the basic information of the image, the cA is chosen to encrypt in our work. Two random sequences SC_1 and SC_2 with the size of $M/2$ and $N/2$ respectively are generated using Pc by applying Eq. (20). SC_1 and SC_2 are utilized to permute cA to obtain cA' which is then transformed into a one-dimensional vector.

$$\begin{cases} SC_1(i) = \lfloor \mathrm{mod}(Pc(i,1) \times 10^8, M/2) \rfloor + 1, & i = 1, 2, 3 \ldots, M/2, \\ SC_2(i) = \lfloor \mathrm{mod}(Pc(1,i) \times 10^8, N/2) \rfloor + 1, & i = 1, 2, 3 \ldots, N/2. \end{cases} \quad (20)$$

Step 7 Performing the diffusion on cA' to obtain a vector En_cA which is then reshaped to a matrix with the size of $M/2 \times N/2$. The complete encryption process is detailed in Algorithm 1.

Algorithm 1 Encryption algorithm

Input: A sub-band of plaintext image cA and its size $(M/2, N/2)$, two random sequences SC_1 and SC_2, two plaintext correlation parameter arrays h_1 and h_2, an empty vector temp.

Output: Encrypted sub-band of plaintext image En_cA.

for $i = 1 : M/2$
  temp $= cA(i,:)$
  $cA(i,:) = cA(SC_1(i),:)$
  $cA(SC_1(i),:) =$ temp
end for
for $i = 1 : N/2$ **do**
  temp $= cA(:,i)$
  $cA(:,i) = cA(:,SC_2(i))$
  $cA(:,SC_2(i)) =$ temp
end for
$cA' = \text{reshape}(cA, [1, M/2 \times N/2])$
for $i = 1 : M/2 \times N/2$ **do**
  $En_cA(i) = \text{mod}(\text{mod}(cA'(i) + h_1(\text{mod}(i,8)+1) \times h_2(\text{mod}(i,8)+1) \times 10^7, 512), 512)$
end for
$En_cA = \text{reshape}(En_cA, [M/2, N/2])$

Step 8 According to the statistical properties in the wavelet domain discussed in Section 2, the distributions of sub-bands of the ciphertext should be as close as possible to the ones in a random image. The complete Gaussianization process is detailed in Algorithm 2.

Algorithm 2 Gaussianization of sub-bands

Input: The encrypted sub-band En_cA, three sub-bands of plaintext image cH, cV, cD, four sub-bands of random image CcA, CcH, CcV, CcD.

Output: Four sub-bands of ciphertext EcA, EcH, EcV, EcD

for $i = 1 : M/2$
  for $j = 1 : N/2$ **do**
    $EcA(i,j) = \text{mod}\left(\frac{(En_cA(i,j)+999\times CcA(i,j)}{1000}\right), 512)$
    $EcH(i,j) = \text{mod}\left(\frac{(cH(i,j)+999\times CcH(i,j)}{1000}\right), 512) - 256$
    $EcV(i,j) = \text{mod}\left(\frac{(cV(i,j)+999\times CcV(i,j)}{1000}\right), 512) - 256$
    $EcD(i,j) = \text{mod}\left(\frac{(cD(i,j)+999\times CcD(i,j)}{1000}\right), 512) - 256$
  end for
end for

Step 9 Perform inverse discrete wavelet transformation on the four sub-bands EcA, EcH, EcV, EcD to obtain cipher image E.

Step 10 In Eqs. (21) and (22), we construct the plaintext information feature carrier vector Ve and the position vector I_{n1} using the random array c_n.

$$Ve(i) = \lfloor \text{mod}(c_n(i) \times 10^4, 256) \rfloor, \quad i = 1, 2, 3 \ldots, N, \tag{21}$$

$$I_{n1}(i) = \lfloor \text{mod}(c_n(i) \times 10^8, N-1) + 1 \rfloor, \quad i = 1, 2, 3 \ldots, 16. \tag{22}$$

Then according to the position vector I_{n1}, we embed plaintext-related parameter array H into the vector Ve as

$$Ve(I_{n1}(i)) = H(i), \quad i = 1, 2, 3 \ldots, 16. \tag{23}$$

Step 11 The position to insert the vector Ve into the cipher image E is calculated in Eq. (24). Finally, the cipher image with the size of $(M+1) \times N$ is obtained.

$$I_{n2} = \lfloor \text{mod}(y_1 \times z_1 \times 10^8, M-1) + 1 \rfloor. \tag{24}$$

On the receiving end, the same secret keys are utilized to iterated ISM to generate the same random sequences r_n, c_n firstly. Then the plaintext information feature carrier vector Ve us extracted from the cipher image and the plaintext-related parameter arrays h_1, h_2 are obtained. After that, using Eq. (15), h_1 and h_2 are used for the random image Pc generation. Finally, the decryption process detailed in Algorithm 3 is performed to obtain the decrypted image.

Algorithm 3 Decryption algorithm

Input: Four sub-bands of cipher image EcA, EcH, EcV, EcD, sub-bands of random image CcA, CcH, CcV, CcD, two random sequences SC_1 and SC_2, two plaintext correlation parameter arrays h_1 and h_2, an empty vector temp.

Output: The decrypted image D.

for $i = 1 : M/2$
  for $j = 1 : N/2$
    $En_cA(i,j) = \text{mod}(EcA(i,j) - 999 \times CcA(i,j) + 512, 512) \times 1000$
    $cH(i,j) = \text{mod}(EcH(i,j) - 999 \times CcH(i,j) + 768, 512) \times 1000$
    $cV(i,j) = \text{mod}(EcV(i,j) - 999 \times CcV(i,j) + 768, 512) \times 1000$
    $cD(i,j) = \text{mod}(EcD(i,j) - 999 \times CcD(i,j) + 768, 512) \times 1000$
  end for
end for
$En_cA = \text{reshape}(En_cA, [1, M/2 \times N/2])$
for $i = 1 : M/2 \times N/2$
  $cA'(i) = \text{mod}(En_cA(i) - h_1(\text{mod}(i,8)+1) \times h_2(\text{mod}(i,8)+1) \times 10^7, 512)$
end for
$cA = \text{reshape}(cA', [M/2, N/2])$
for $i = M/2 : -1 : 1$
  temp $= cA(i,:)$
  $cA(i,:) = cA(SC_1(i),:)$
  $cA(SC_1(i),:) =$ temp
end for
for $i = N/2 : -1 : 1$
  temp $= cA(:,i)$
  $cA(:,i) = cA(:,SC_2(i))$
  $cA(:,SC_2(i)) =$ temp 23: **end for**
$D = idwt(cA, cH - 256, cV - 256, cD - 256, 'haar')$

5. Experimental simulation results and security analysis

Aiming to evaluate the performance of WDLIC, in this section various simulations are performed on Matlab 2022a. The experiments are conducted on a personal computer with Core(TM) i7-11800H CPU 2.30 GHz, 16 GB RAM and Windows 10 operating system.

5.1. Key space

Key space means the total number of keys that a cryptosystem can select. It is generally accepted that a cryptosystem can resist brute-force attacks when the key space is greater than 2^{100}. In this paper, Alice's fingerprint image was utilized to generate three keys x_0, y_0, and z_0 via SHA-256. If the computer accuracy is 10^{15}, we can calculate the key space $= (10^{15})^3 > 2^{149}$. Therefore, the key space of WDLIC is large enough to invalidate brute-force attacks.

5.2. Histogram analysis

The histogram of an image reflects the distribution of pixels. In spatial domain, the more uniform of an encrypted image's histogram, the more challenging it is for an attacker to extract meaningful information from it. In wavelet domain, the distributions of sub-bands of the ciphertext should be as close as possible to Gaussian distribution. We tested the histograms of Lena and other five images with the size of 512×512 before and after decryption. As shown in Figs. 10 and 11, the WDLIC can resist the statistical attacks well.

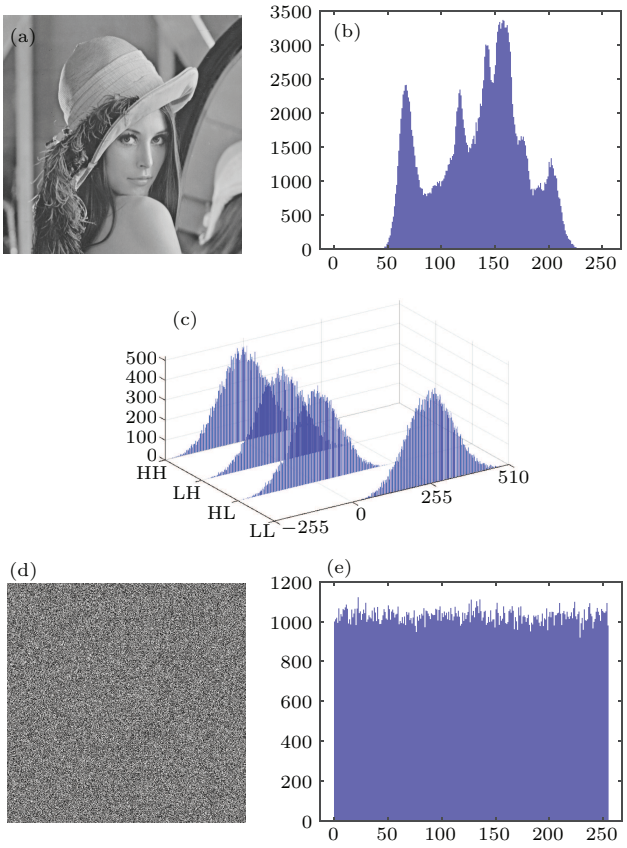


Fig. 10. Histogram. (a) Lena; (b) histogram of Lena; (c) histograms of four ciphertext sub-bands; (d) cipher image; (e) histogram of cipher image.

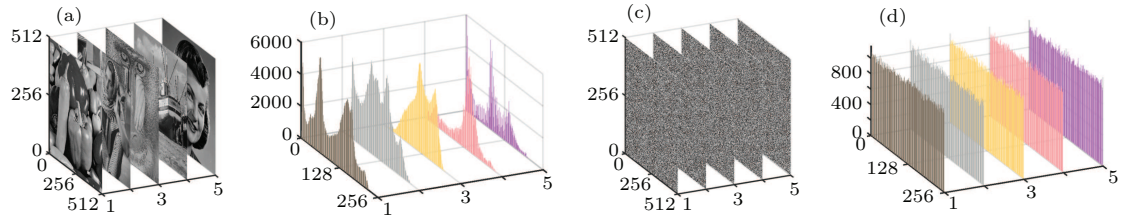


Fig. 11. Simulation results of five images, 1-Peppers, 2-Barbara, 3-Baboon, 4-Boat, 5-Girl. (a) Five plain images; (b) bistograms of five plain images; (c) five cipher images; (d) histograms of five cipher images.

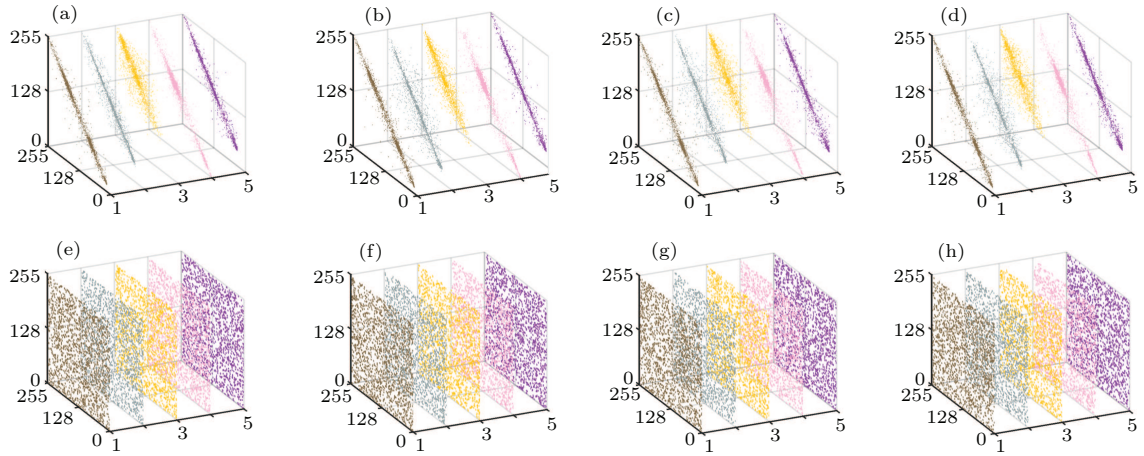


Fig. 11. Correlation analysis of five images, 1-Peppers, 2-Barbara, 3-Baboon, 4-Boat, 5-Girl: the first line is the correlation analysis of five images in four specified directions, (a) vertical; (b) horizontal; (c) diagonal; (d) anti-diagonal. The secord line is the correlation analysis of five cipher images in four specified directions.

5.3. Correlation analysis

Exploiting high correlation of neighboring pixels to attack encryption algorithms is a common tactic for attackers. A secure encryption algorithm should eliminate the correlations of images. The correlations between two adjacent pixels in four specified directions can be measured by the correlation coefficients (cc). The fomula of cc is given as

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{25}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))(y_i - E(y)), \tag{26}$$

$$E(x) = \frac{1}{N}\sum_{i=0}^{N} x_i, \tag{27}$$

where N is the number of pixels arbitrarily selecting from the image. x and y are two neighboring pixels. Figure 12 shows the correlation analysis in four specified directions and the results of correlation coefficients analysis are shown in Tables 2 and 3, which indicates that WDLIC is effective in eliminating the strong correlation.

Table 2. The results of correlations analysis.

Image	Original image				Cipher image			
	V	H	D	A	V	H	D	A
Lena	0.9852	0.9723	0.9554	0.9762	–0.0057	0.0021	0.0021	–0.0178
Peppers	0.9836	0.9803	0.9692	0.9627	0.0107	–0.0070	–0.0151	–0.0255
Barbara	0.9576	0.8619	0.8320	0.8897	0.0062	–0.0193	–0.0031	–0.0193
Baboon	0.7764	0.8805	0.7340	0.7393	0.0158	–0.0008	0.0039	–0.0407
Boat	0.9713	0.9203	0.9330	0.9292	0.0030	–0.0364	–0.0016	–0.0007
Girl	0.9874	0.9784	0.9770	0.9789	–0.0015	0.0107	0.0031	–0.0024

Table 3. The comparative correlation coefficients analysis of encrypted Lena.

Direction	Proposed	Ref. [33]	Ref. [34]	Ref. [41]	Ref. [42]	Ref. [43]
Horizontal	0.0021	0.0114	0.0105	0.0110	-0.0017	0.0010
Vertical	-0.0057	–0.0148	–0.0019	–0.0032	0.0011	–0.0053
Diagonal	0.0021	0.0096	–0.0019	–0.0001	0.0007	0.0069
Average	0.0005	0.0021	0.0022	0.0026	0.0001	0.0009

5.4. Information entropy

Information entropy reflects the uncertainty of an information source. For a 256-grey level image, the ideal information entropy of the cipher image should be as close as possible to 8. The mathematical formula of the information entropy is

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log\frac{1}{p(m_i)}, \tag{28}$$

where $p(m_i)$ is the probability of the appearance of the pixel m_i and 2^N represents the total number of m_i. As seen in Table 4, all the simulation results are extremely close to the desired value, which indicates that WDLIC can completely confuse the image information.

Table 4. Information entropy analysis results.

Image	Type	Size	Plain-image	Cipher-image
Lena	gray	512×512	7.2185	7.9990
Peppers	gray	512×512	7.5715	7.9985
Barbara	gray	512×512	7.4664	7.9987
Baboon	gray	512×512	7.1391	7.9986
Boat	gray	512×512	7.1914	7.9985
Girl	gray	512×512	7.0818	7.9988
Lena in Ref. [33]	gray	512×512	7.2185	7.9994
Lena in Ref. [34]	gray	512×512	7.2185	7.9987
Lena in Ref. [41]	gray	512×512	-	7.9973
Lena in Ref. [42]	gray	512×512	7.5151	7.9979
Lena in Ref. [43]	gray	512×512	7.4455	7.9994

5.5. Sensitivity analysis

A superior encryption algorithm should have strong key sensitivity and plaintext sensitivity to defend against differential attacks and chosen plaintext attacks. In general, the number of pixels changing rate (NPCR) and the unified average changed intensity (UACI) are exploited to to evaluate the sensitivity. Mathematically, NPCR and UACI are calculated by

$$\begin{cases} \mathrm{NPCR} = \sum_{i=0}^{H}\sum_{j=0}^{W} D(i,j)\times 100\%, \\ \mathrm{UACI} = \frac{1}{W\times H}\sum_{i=0}^{H}\sum_{j=0}^{W}\frac{|P_1(i,j)-P_2(i,j)|}{255}\times 100\%, \end{cases} \tag{29}$$

where

$$D(i,j) = \begin{cases} 0, & P_1(i,j) = P_2(i,j), \\ 1, & P_1(i,j) \neq P_2(i,j). \end{cases} \tag{30}$$

5.5.1. Key sensitivity

In our work, the secret key generated from Alice's fingerprint image is used to produce the initial values of ISM. A subtle change in the key can result in a significant difference in the cipher image. Take standard image Lena as an example, figure 13 illustrates the decrypt results with the correct and wrong key. And Table 5 lists the corresponding NPCR and UACI test results. One can see that the encryption and decryption process of WDLIC are very sensitive to the key.

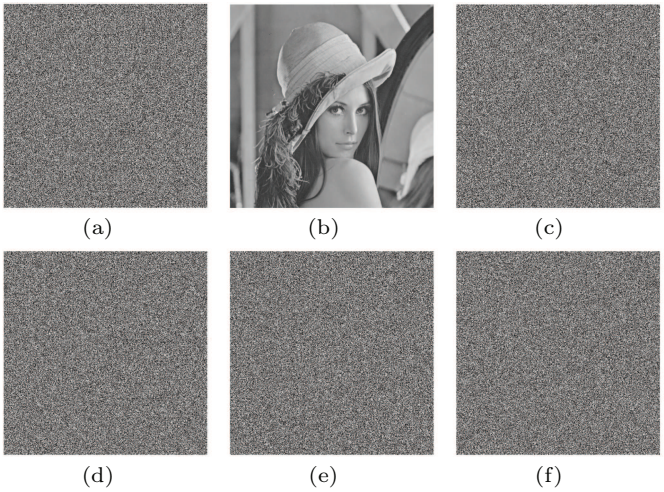


Fig. 13. Visualization tests for key sensitivity. (a) The encrypted image with the security key $\text{key}_1 = [N_0, x_0, y_0, z_0]$; (b) the decrypted image using correct key; (c) the decrypted image using $\text{key}_1 = [N_0, x_0, y_0, z_0]$; (d) the decrypted image using $\text{key}_2 = [N_0+1, x_0, y_0, z_0]$; (e) the decrypted image using $\text{key}_3 = [N_0, x_0+10^{-15}, y_0, z_0]$; (f) the decrypted image using $\text{key}_4 = [N_0, x_0, y_0+10^{-15}, z_0]$; (g) the decrypted image using $\text{key}_5 = [N_0, x_0, y_0, z_0+10^{-15}]$.

Table 5. NPCR and UACI performance of key sensitivity analysis.

Image	Index	N_0+1	x_0+10^{-15}	y_0+10^{-15}	z_0+10^{-15}
Lena	NPCR	99.9320	99.9331	99.9345	99.9343
	UACI	33.4412	33.4338	33.4313	33.4348
Baboon	NPCR	99.9400	99.9383	99.9399	99.9377
	UACI	33.4367	33.4428	33.4315	33.4253
Peppers	NPCR	99.9372	99.9363	99.9418	99.9317
	UACI	33.4391	33.4253	33.4424	33.4205

5.5.2. Plaintext sensitivity

Plaintext sensitivity analysis seeks to determine whether a slight change of plaintext will have a significant impact on ciphertext. Table 6 lists the average UACI and NPCR analysis results of WDLIC and other algorithms. The results of the study reveal that WDLIC exhibits robustness against differential attacks and chosen plaintext attack.

Table 6. NPCR and UACI performance of plaintext sensitivity analysis.

Image	Type	Size	NPCR(99.6094)	UACI(33.4635)
Lena	gray	512×512	99.7735	33.4037
Peppers	gray	512×512	99.7677	33.3807
Barbara	gray	512×512	99.7833	33.3800
Baboon	gray	512×512	99.7781	33.4031
Boat	gray	512×512	99.7780	33.4255
Girl	gray	512×512	99.7753	33.3792
Lena in Ref. [33]	gray	512×512	99.8430	33.4283
Lena in Ref. [34]	gray	512×512	99.8100	33.3995
Lena in Ref. [41]	gray	512×512	99.5720	33.3724
Lena in Ref. [42]	gray	512×512	99.6103	33.4658
Lena in Ref. [43]	gray	512×512	100	33.6941

5.6. Running time efficiency analysis

The speed of encryption is an important indicator for cryptosystem, especially for some application scenarios with limited resource or need real-time encryption. In our work, we select some standard images with the size of 256×256 and 512×512 as the test images. Table 7 lists the running time of different algorithms in MATLAB programming environment. Obviously, the proposed WDLIC achieves a significant advantage in terms of speed.

Table 7. Time consumption comparisons with other methods (in seconds).

	Proposed	Ref. [33]	Ref. [34]	Ref. [41]	Ref. [42]	Ref. [43]
512×512	0.1158	0.5748	0.3474	0.2570	0.2010	0.5409
256×256	0.0285	0.1430	0.1229	0.1810	0.0550	0.1351

5.7. Noise attack and data loss

A strong cryptosystem should have the robustness of noise attack and data loss. In this subsection, as shown in Fig. 14, the cipher image is added with different intensities salt-and-pepper noise or malicious cut. One can see that the decrypted image contains most visual information of original image. Peak signal to noise ratio (PSNR) is used to evaluate the decrypted image quality and the results shown in Table 8 prove that WDLIC has strong robustness to resist noise attack and data loss.

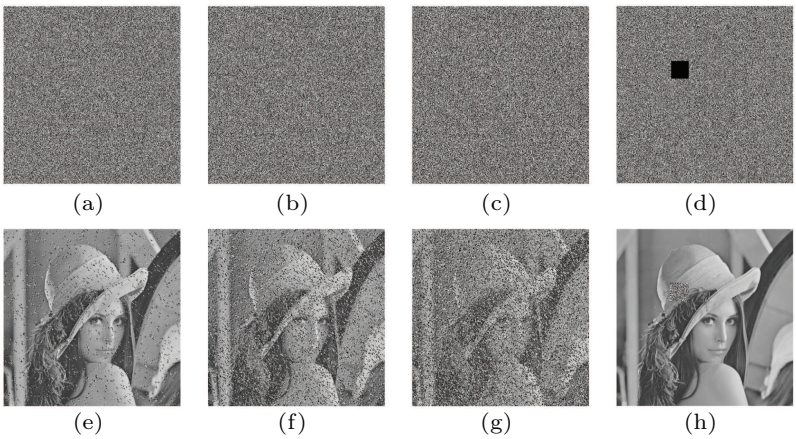


Fig. 14. Results of noise resistance and data loss. (a) The encrypted images contaminated by salt-and-pepper noise 1% density; (b) the encrypted images contaminated by salt-and-pepper noise 5% density; (c) the encrypted images contaminated by salt-and-pepper noise 10% density; panels (e)–(g) are the corresponding decrypted images. Panel (d) is the encrypted Lena with 50×50 data loss and panel (h) is the decrypted image of panel (d).

Table 8. Noise attack analysis using PSNR indicator.

Noise attacks or data loss	PSNR
Salt-and-pepper noise (1%)	20.9001
Salt-and-pepper noise (5%)	14.4095
Salt-and-pepper noise (10%)	12.1268
Data loss (50×50)	30.0494

6. Conclusion

This paper introduces an improved sine map. Extensive tests including Lyapunov exponent test, bifurcation analysis, sample entropy, the 0–1 test and NIST test indicate that ISM possesses a larger chaotic region, more complex chaotic behavior and greater unpredictability compared to the previous chaotic maps. Building upon ISM, we propose a lightweight image cryptosystem wherein only the low-frequency–low-frequency component is chosen to encrypt and then Gaussianization is employed across all sub-bands. Experimental simulation results and security analysis demonstrate that WDLIC achieves satisfactory security, encryption speed and robustness against various attacks. The robustness against noise and data loss of WDLIC is compromised due to the selective encryption employed. In the future, our efforts will focus on optimizing the selective encryption strategy to overcome the limitations and utilizing WDLIC to develop potential applications for multimedia data encryption like color images and even video on hardware.

Acknowledgements

Project supported by the Key Area Research and Development Program of Guangdong Province, China (Grant No. 2022B0701180001), the National Natural Science Foundation of China (Grant No. 61801127), the Science Technology Planning Project of Guangdong Province, China (Grant Nos. 2019B010140002 and 2020B111110002), and the Guangdong–Hong Kong–Macao Joint Innovation Field Project (Grant No. 2021A0505080006).

References

[1] Wu H, Ye G, Yap W S and Goi B M 2023 *Opt. Laser Technol.* **167** 109755
[2] Ye G, Wu H, Liu M and Huang X 2023 *Chaos, Solitons & Fractals* **171** 113469
[3] Gong L H and Luo H X 2023 *Opt. Laser Technol.* **167** 109665
[4] Lai Q and Liu Y 2023 *Expert Systems with Applications* **223** 119923
[5] Nestor T, Jacques K, Bassem A, Abdullah M I, Kaoru H and Ahmed A E 2020 *Information Sciences* **515** 191
[6] Wang X Y and Liu P B 2022 *IEEE Transactions on Circuits and Systems I: Regular Papers.* **69** 1291
[7] Pak C and Huang L L 2017 *Signal Processing* **138** 129
[8] Zhou Y C, Bao L and Chen L P 2014 *Signal Processing* **97** 172
[9] Wang S M, Peng Q Q and Du B X 2022 *Opt. Laser Technology* **148** 107753
[10] Zhu Y, Wang C H, Sun J R and Yu F 2023 *Mathematics* **11** 767
[11] Wu Y R, Zhang L L, Stefano B and Wan S H 2023 *IEEE Transactions on Industrial Informatics* **19** 2089
[12] Chai X L, Fu X L, Gan Z H, Lu Y and Chen Y R 2019 *Signal Processing* **155** 44
[13] Kang Y L, Huang L Q, He Y, Xiong X M, Cai S T and Zhang H Y 2020 *Symmetry-Basel* **12** 1393
[14] Sasikaladevi N, Geetha K, Sriharshini K and Aruna M D 2020 *Opt. Laser Technol.* **127** 106173
[15] Banik A, Laiphrakpam D S, Agrawal A and Patgiri R 2022 *Digital Signal Processing* **129** 103639
[16] Luo Y L, Ouyang X, Liu J X and Cao L C 2019 *IEEE Access* **7** 38507
[17] Luo Y L, Tang S B, Liu J X, Cao L C and Qiu S H 2020 *Opt. Lasers Eng.* **124** 105836
[18] Gao Y J, Xie H W, Zhang J and Zhang H 2022 *Physica A* **598** 127334
[19] Lai Q, Wan Z Q, Zhang H and Chen G R 2023 *IEEE Transactions on Neural Networks and Learning Systems.* **34** 7824
[20] Lai Q and Chen Z J 2023 *Chaos, Solitons & Fractals* **170** 113341
[21] Lai Q, Yang L and Chen G R 2023 *IEEE Transactions on Industrial Electronics* 1
[22] Farah M A B, Guesmi R, Kachouri A and Samet M 2020 *Opt. Laser Technol.* **121** 105777
[23] Huang Z W and Zhou N R 2022 *Opt. Laser Technol.* **149** 107879
[24] Wang M M, Zhou N R, Li L and Xu M T 2022 *Expert Systems with Applications* **207** 118067
[25] Huang Z J, Cheng S, Gong L H and Zhou N R 2020 *Opt. Lasers Eng.* **124** 105821
[26] Yu S S, Zhou N R, Gong L H and Nie Z 2020 *Opt. Lasers Eng.* **124** 105816
[27] Joshi A B, Kumar D, Gaffar A and Mishra D C 2020 *Opt. Lasers Eng.* **133** 106139
[28] Gurpreet K, Rekha A and Vinod P 2022 *Journal of King Saud University-Computer and Information Sciences* **2022** 5883
[29] Jiang D H, Liu L D, Zhu L Y, Wang X Y, Rong X W and Chai H X 2021 *Signal Processing* **188** 108220
[30] Chai X L, Bi J Q, Gan Z H, Liu X X, Zhang Y S and Chen Y R 2020 *Signal Processing* **176** 107684
[31] Ye G D, Pan C, Dong Y X, Shi Y and Huang X L 2020 *Signal Processing* **172** 107563
[32] Huo D M, Zhu Z L, Wei L S, Han C and Zhou X 2021 *Opt. Commun.* **492** 126976
[33] Wen H P, Chen Z F, Zheng J H, Huang Y M, Li S W, Ma L C, Lin Y T, Liu Z, Li R, Liu L H, Lin W X, Yang J Y, Zhang C F and Yang H D 2022 *Entropy* **24** 1332
[34] Oteko T L and Mbuyu S 2019 *IEEE Access* **7** 103463
[35] Zhou N R, Hu L L, Huang Z W, Wang M M and Luo G S 2024 *Expert Systems with Applications* **238** 122052
[36] Hua Z Y, Zhou Y C and Huang H J 2019 *Information Sciences* **480** 403
[37] Midoun M A, Wang X Y and Talhaoui M Z 2021 *Opt. Lasers Eng.* **139** 106485
[38] Talhaoui M Z, Wang X Y and Midoun M A 2021 *The Visual Computer* **37** 541
[39] Richman J S and Moorman J R 2000 *American Journal of Physiology-Heart and Circulatory Physiology.* **278** H2039
[40] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J and Vo S 2010 *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (Gaithersburg: National Institute of Standards and Technology)
[41] Chen H P, Bai E J, Jiang X Q and Wu Y 2022 *IEEE Access* **10** 116031
[42] Shen Y L, Huang J, Chen L L, Wen T, Li T Y and Zhang G D 2023 *Entropy* **25** 753
[43] Huang Q Y, Huang L Q, Cai S T, Xiong X M and Zhang H 2023 *Mathematics* **11** 4411