IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 18, 2021, accepted August 23, 2021, date of publication August 30, 2021, date of current version September 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3108789

A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step

WANG JI JUN [1,2] AND TAN SOO FUN [1], (Member, IEEE)
[1]Faculty of Computing and Informatics, Universiti Malaysia Sabah (UMS), Kota Kinabalu, Sabah 88400, Malaysia
[2]Faculty of Information and Statistics, Guangxi University of Finance and Economics, Nanning, Guangxi 530003, China

Corresponding author: Tan Soo Fun (soofun@ums.edu.my)

This work was supported in part by the Ministry of Higher Education Malaysia and Universiti Malaysia Sabah through the Fundamental Research Grant Scheme under Grant FRG0530-2020 and Skim Dana Khas Grant SDK0165-2020, in part by the Research Fund of National Natural Science Foundation under Grant 62162006, in part by Guangxi Key Laboratory of Multi-Source Information Mining and Security under Grant MIMS18-05, and in part by the Young and Middle-Aged Teachers' Ability Improvement Project of Guangxi under Grant 2020KY16021 and Grant 2021KY0650.

ABSTRACT Chaotic-based S-box image encryption schemes promise to be a practical solution for securing digital images. However, the high-dimensional continuous chaotic has increased the algorithm's complexity. Recent alternatives that focused on double or multiple S-boxes approaches, on the other hand, have been proven vulnerable to differential attacks. This paper presents an efficient and secure chaotic-based S-box image encryption scheme. Firstly, a single S-box with a size of 10×26 was constructed by using a low-dimensional chaotic system. Without a complex mathematical operation, the constructed single S-box has obvious efficiency advantages and achieved a higher image entropy rate than recent double or multiple S-boxes. Secondly, a new dynamic encryption step method is proposed to solve the high correlation and deterministic problems in multiple S-box encryptions. Under the control of the dynamic encryption step algorithm, it effectively destroys the correlation between the source image's pixels. The experimental results and security analysis show that the proposed scheme enjoys higher security and is more efficient to secure digital images in real-world applications.

INDEX TERMS Image encryption, substitution box (S-box), chaotic systems, dynamic step.

I. INTRODUCTION

With the growing popularity of digital images in thriving social media and their importance in supporting medical and surveillance industries, the increased security breaches have promoted the need for a practical solution to protect digital image privacy. As a result, various image encryption schemes have been proposed recently, with their approaches classified as chaotic system approach [3]–[15], DNA encryption [16]–[28], compressive sensing encryption [29]–[36], wavelet transform encryption [37]–[45] and Substitution-box (S-box) approach [46]–[53].

A. CHAOTIC ENCRYPTION

A chaotic system's intrinsic characteristics, such as pseudo-randomness, instability, and sensitivity to the system's initial conditions and parameters, make the chaotic system have the requisite security conditions. The core principle of chaotic encryption depends on the chaotic framework's capacity to generate a sequence of random numbers that are uncorrelated, similar noise and renewable. Subsequently, a sequence is applied to guide image scrambling. The verifiable properties of sequence reconstruction and prediction resulted in a higher security level in chaotic encryption. Recent chaos-based image encryption techniques can be further categorized into true random numbers [3], [4], cyclic shift [5], chaotic logistic map [6], hyperchaos [7]–[9], fuzzy cellular neural networks [10], coupling map lattices with mixed multi-chaos [11], dynamic chaos and matrix convolution [12], and generalized Fibonacci chaos [13] and Fractional calculus [14], [15]. Chaotic encryption is common in image encryption literature; however, the confusion and diffusion process in some studies are vulnerable to security flaws.

B. DNA ENCRYPTION

Some researchers adopted biological and algebraic operations based on DNA sequences with the rapid

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

development of DNA computing. For example, DNA sequence addition and subtraction operations are derived from the conventional binary addition and subtraction. In recent years, many achievements have been made in DNA-based image encryption, includes DNA computing and chaotic system [16]–[22], DNA based probability and two-dimensional logistic map [23], DNA level permutation with 3D Latin cubes [24], FSM–DNA Rule Generator and FSBI [25], 3D DNA level permutation and substitution [26], CML system and DNA encoding [27], Zigzag-like transform and DNA-like coding [28]. The main advantages of DNA-based image encryption are that all sorts of entropy and differential attacks can be resisted. However, DNA encryption is still in its infancy, and there are other issues such as complexity of encoding process, high biological operation error and costly experimental need to be addressed.

C. COMPRESSED SENSING (CS) ENCRYPTION

Compressed Sensing (CS) is a new sampling theory. The CS sampling process extracts useful information from sparse signals by simply correlating sparse signals with a set of projection bases. The core concepts of CS consist of two parts: uncorrelated feature and sparse structure, which involves the sparse representation of the signal, projection measurement of signal, and reconstruction of the original signal. CS-based image encryption has dimensionality reduction and random projection characteristics. CS-based image encryption thus enjoys a high compression rate and is widely used in image encryption. However, it is hard to meet the security requirements of image encryption. As a result, subsequent researchers [29]–[36] have taken a hybrid approach to improve CS-based encryption security by utilizing chaos and optics' security properties.

D. WAVELET TRANSFORM ENCRYPTION

Compared to the typical image encryption in the spatial domain, wavelet transform encryption focuses on the frequency domain. The frequency domain has advantages of strong sensitivity and resistance to security attacks. The key concept of wavelet transform encryption is to decompose the original image to get each component's image, including approximate image, low-frequency horizontal and vertical components, and high-frequency components. After that, each component of the image is encrypted, and the complete encrypted image is reconstructed using each component's encrypted image. Various variants of wavelet transform-based encryption methods have been proposed recently, include traditional wavelet transform [37], discrete wavelet transform [38], Fresnel wavelet transform [39], fractional wavelet transform [38], chaotic trigonometric haar wavelet transform [39], quantum haar wavelet packet transform [42], lifting wavelet [43], [44], chaos and wavelet transform [45].

E. SUBSTITUTION-BOX (S-BOX)

S-box is one of the most important ingredients in blocks encryption algorithms because of its unique nonlinear element. It has been widely applied in classical encryption algorithms, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The image encryption algorithm based on the S-box approach enjoys faster processing speed but achieved a lower security level. The implementation results of the S-box in the substitution phase of image encryption observed a high correlation between the image pixels and high similarity features among encrypted image and source image, thus reducing its security properties.

In recent years, scholars have directed hybrid S-Box with chaotic encryption in hardening the security resistance of S-box-based image encryption. Jahangir *et al.* [46] constructed S-box based on finite algebraic structures and proposed a colour image encryption technology using permutation key and S-box. Jahangir *et al.* [46] scheme can resist statistical analysis and differential analysis. Considered CS encryption of the chaotic measurement matrix has a strong sensitivity to plaintext, Zhu *et al.* [47] hybridized the CS-based image encryption with S-box. Hasanzadeh *et al.* [48] use Julia fractal set to generate a fractal image, then apply Hilbert fractal to construct S-box. Combining fractal, S-box, and hyperchaotic dynamics, Hasanzadeh *et al.*'s scheme [48] has a larger keyspace and good encryption effect. On the other hand, Farah *et al* [49] optimized S-box by using chaotic Jaya optimization algorithm and Shanon's confusion and diffusion concepts. The good randomness and sensitivity of chaotic mapping make Farah *et al.* 's algorithm [49] resist different cryptanalysis attacks. Çavuşoğlu *et al.* [50] proposed a chaos-based S-Box that has low complexity and high security. Lu *et al* [51] proposed a new discrete compound chaotic Logistic Sine System (LSS) with a wider chaotic range and better chaotic performance. Their scheme improved password security and efficiency significantly with the embedded key strategy associated with the image content during the encryption process. Wang *et al.* [52] introduced a non-equilibrium system with chaos. The constructed S-box enjoys higher security features, but it takes more time to generate multiple S-boxes. Zhang *et al.* [53] focused on the security aspect by introducing an image encryption scheme based on asynchronous substitution and diffusion. The scheme belongs to the double S-box method and adopts forward and backward encryption to synchronize pixel scrambling and pixel diffusion.

Recent literature [43]–[53] demonstrated that chaotic-based S-box image encryption has significantly improved security. However, the high-dimensional continuous chaotic increased the algorithm's complexity [54], [55]. Several researchers applied double S-Box and multiple S-boxes approaches to tackle the complexity of high-dimensional continuous chaos. However, these approaches [49]–[53] target a relatively simple image encryption application and are limited to support S-box sizes of 4×16 or 16×16. Furthermore, the high correlation between the grey image pixels and the achievement of low rate in Number of Pixels Change Rate (NPCR), Unified Average Change Intensity (UACI) and entropy analysis resulted in these schemes [49]–[53]

cannot resist well to the differential attack and direct attack.

This paper aimed to address these research gaps by proposing an S-box with a low-dimensional chaotic system. The contributions of this paper are summarized by:

- A new technique in constructing a secure chaotic-based S-Box image encryption, called 'Dynamic Encryption Step', significantly reduced the high correlation between the pixels of source image, thus improve the security level of S-Boxed based image encryption.
- We use the low dimensional chaotic sequence to construct a single S-box to achieve a better chaotic degree (measured in entropy rate). The row-column transform process does not need complex mathematical operations and has obvious efficiency advantages.
- Pixel diffusion is used to increase the security of the proposed 'Dynamic Encryption Step' approach by changing the statistical characteristics of the encrypted image. Therefore, the proposed algorithm is robust against differential attacks.
- We extended S-box sized to 10×26 to support more complex image encryption applications without sacrificing the security and algorithm complexity.

The rest of this paper is organized as follows. Section II introduces the S-box construction with a low dimensional chaotic sequence. The proposed dynamic encryption step method and chaotic-based S-box image encryption algorithm are presented in Section III. Section IV discussed the experimental results and compared them with recent chaotic-based S-box algorithms. Section V concludes.

II. THE NEW S-BOX CONSTRUCTION WITH LOW DIMENSIONAL CHAOTIC SEQUENCE

A. LOGISTIC MAP

Logistic map is a classical model to study the dynamical system, chaos, fractal, and other complex systems behaviours. Logistic map, also called logistic iteration, is essentially a time-discrete dynamic system. Its formula is:

$$x_{k+1} = \mu x_k (1 - x_k) \tag{1}$$

where $0 \leq \mu \leq 4$ is called the branching parameters, when $x_k \in (0, 1)$ and $3.56 \leq \mu \leq 4$. The logistic map is in a chaotic state and can generate a low dimensional chaotic sequence from elementary nonlinear dynamical equations. From the probability density function, mean value, and cross-correlation function of chaotic sequence, we know that logistic map has the characteristics of certainty, pseudo randomness, non-periodic and non-convergence, the sensitivity of initial value, unpredictability and fast generation speed, which ensures the randomness and security of sequence generation.

Compared to recent hyperchaos [7]–[9], coupling map lattices with mixed multi-chaos [11], dynamic chaos and matrix convolution [12], and generalized Fibonacci chaos [13], the chaotic logistic mapping can be significantly less computationally. We chose a one-dimensional chaotic logistic map with low dimensions and high security as a trade-off between efficiency and security.

B. CONSTRUCTION OF THE NEW SINGLE S-BOX

The construction of a new Single S-box, denoted as $\mathbf{S}$ should meet the following conditions:

- The size of $\mathbf{S}$ is 26×10 or 10×26, which accommodate at least 256 elements.
- All elements in $\mathbf{S}$ must be integers between 0 and 255, such that $\mathbf{S}(i, j) \in [0, 255]$.
- All elements in $\mathbf{S}(i, j)$ are not equal to each other, and 256 values should cover the continuous range of 0∼255.

STEP 1: Set initial parameters x_0 and μ, use Eq. (1) to generate a low dimensional chaotic sequence P_i with 256 distinct elements, for $i \in [0, 255]$.

STEP 2: Sort P_i in descending order, such that $P'_i = Rank(P_i)$ and $i \in [0, 255]$. Subsequently, define a new chaotic sequence, P''_j by finding the x that corresponding to all y in ascending order of P'_i, such that x and y are the position index sequence of the identical value in P_i and P'_i respectively, ($x \in [0, 255]$, $y \in [0, 255]$). All elements in the sequence P''_j are integers in the continuous interval 0∼255, which are not omitted or repeated.

STEP 3: The chaotic sequence P''_j is transformed into a single S-box matrix sized of 26×10 or 10×26. Four generated values (6, 25) (7, 25) (8, 25) (9, 25) can be filled with any value not ending in [0, 255], order by $\boldsymbol{S} = reshape(P''_j, 10, 26)$.

Table 1 illustrates the example of the constructed S-box with initial parameters $\mu = 3.95$ and $x_0 = 0.32568$.

C. HIGH CORRELATION PROBLEM IN S-BOX BASED IMAGE ENCRYPTION

Let $\mathbf{A}$ be an original image with a size of $m \times n$ and $\mathbf{A}(i, j) \in [0, 255]$. Each pixel $\mathbf{A}(i, j)$ is expressed as a three-digit numeral. Conduct vacancy filling process if necessary, so that the numeral is always three digits, such as $000, 001, 002, \ldots, 254, 255$. The first two digits of each pixel $\mathbf{A}(i, j)$ are used to index the S-Box column position, denoted as col, and the third digit represents the index position of rows, denoted as row, then:

$$\begin{aligned} col &= [\mathbf{A}(i, j) - rem(\mathbf{A}(i, j), 10)]/10 \\ &\quad row \in [0, 25] \ \& \ row \in \mathbf{Z}^+. \end{aligned} \tag{2}$$

$$\begin{aligned} row &= rem(\mathbf{A}(i, j), 10) \\ &\quad col \in [0, 9] \ \& \ col \in \mathbf{Z}^+, \quad 1 \leq i \leq m, \ 1 \leq j \leq n. \end{aligned} \tag{3}$$

where $rem(x, y)$ is the remainder operation, $rem(x, y) = x - y \times round(x/y)$, and $round$ () function rounds a division result to zero. The corresponding col and row can be obtained through the pixel-wise decomposition by giving any pixel $\mathbf{A}(i, j)$.

Let $\mathbf{S}$ is the matrix of constructed single S-Box and $\boldsymbol{S} = [S\,(row, col)]$. Then, conduct index search process by

TABLE 1. The constructed S-box with low dimensional chaotic sequence ($\mu = 3.95, x_0 = 0.32568$).

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	91	112	182	176	191	29	207	35	57	87	116	56	206	61	80	45	90	253	130	6	63	223	22	228	255	38
1	172	202	46	21	54	121	2	164	189	162	64	66	251	158	218	136	171	181	1	216	160	144	79	180	210	246
2	17	214	98	219	49	133	110	212	52	236	235	193	224	83	20	239	16	226	139	122	85	25	19	197	5	78
3	77	4	196	81	148	33	140	238	123	65	161	43	145	53	175	11	244	198	242	30	149	102	174	99	215	18
4	245	209	179	59	84	129	153	135	119	187	86	237	26	190	94	71	154	100	14	126	50	60	93	47	203	173
5	37	254	227	101	159	131	243	44	31	117	150	163	128	40	8	213	141	48	74	204	55	157	177	183	113	92
6	155	72	199	24	62	27	15	194	127	106	107	88	32	248	68	201	229	147	34	186	192	82	96	138	231	—
7	142	12	69	37	104	146	170	67	205	234	118	169	120	221	178	165	111	184	256	105	42	39	10	241	167	—
8	166	240	9	249	185	225	89	7	108	115	51	152	124	23	195	36	3	28	211	114	168	247	70	13	143	—
9	230	137	95	41	125	252	75	217	151	233	188	109	103	58	97	76	208	132	134	232	250	220	200	73	156	—

searching the *row* and *col* index value in $\boldsymbol{S}(row, col)$. The one-time S-box encrypted image denoted as $\mathbf{C}_1$, such that:

$$\begin{aligned}\mathbf{C}_1(i,j) &= \mathbf{S}(row, col)\\ &= \mathbf{S}([\mathbf{A}(i,j) - rem(\mathbf{A}(i,j), 10)]/10 + 1,\\ &\quad rem(\mathbf{A}(i,j), 10) + 1)\end{aligned} \tag{4}$$

Each pixel $\mathbf{A}(i,j)$ in the original image $\mathbf{C}_1(i,j)$ can be obtained by a one-time pixel-wise decomposition and index search process. For example, given the pixel, add leading zero to pixel '19' to form a three-digit numeral $\boldsymbol{A}(i,j) =$ '019'. Then, obtain the index position of column and row respectively, $col = 01$ and $row = 9$ by decomposing '019' into '01' and '9'. Subsequently, use column position index '01' and row position index '9' to search and substitute the value in the constructed single S-box matrix $\mathbf{S}$, such that $\boldsymbol{S}(9, 01) = 137$. The encryption diagram is shown in Figure 1.

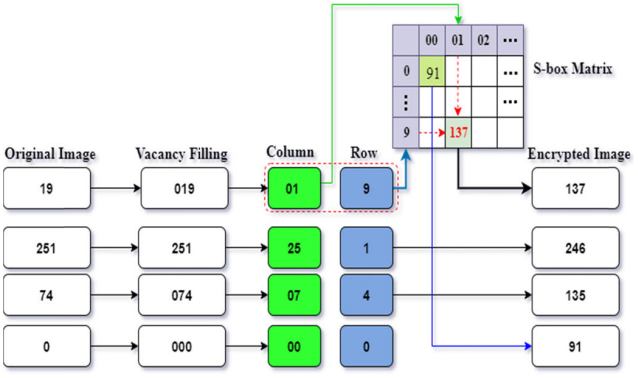

FIGURE 1. S-box encryption diagram.

Few researchers applied multiple S-Box encryptions techniques in hardening the security of S-box based image encryption. Let $\boldsymbol{C}_n$ be the output of n-th round encrypted image, $n + 1$ multiple-times S-Box encryption can be achieved by using Eq.(4) such that $\boldsymbol{C}_{n+1} = \boldsymbol{C}_n(i,j) = \boldsymbol{S}(row, col)$. Figure 2 illustrates the output of multiple-S-Box encryptions with $n = 8$.

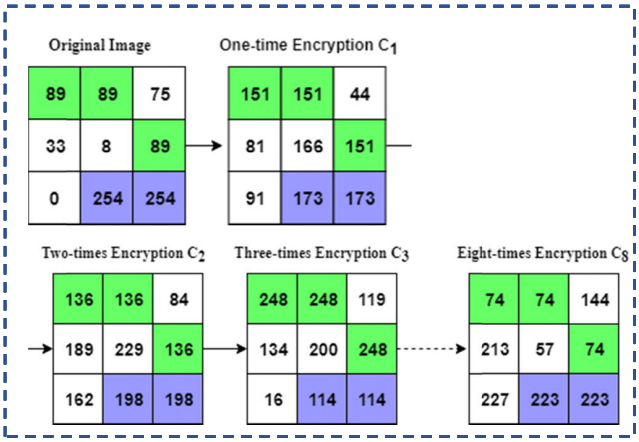

FIGURE 2. High correlation and deterministic problems in multiple-times S-box encryption ($n = 8$).

The multiple S-box encryptions do not effectively destroy the correlation between the pixels with the increased numbers of S-box encryption. As illustrated in Figure 2, the pixel value of 89 (highlighted in green colour) and 254 (highlighted in purple colour) in the original image returns the same sequence of states in encrypted images, $\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_n$. The deterministic properties of multiple S-Box encryptions caused them vulnerable to chosen-plaintext attacks and differential attacks.

Several double S-boxes, three S-boxes, or multiple S-boxes approaches Ref. [49]–[53] have recently been proposed to overcome high correlation and deterministic issues. However, these approaches generate distinct S-boxes to support multiple S-box encryptions, thus increasing computing workloads and not effectively solving the root problem.

III. THE PROPOSED METHOD

This section presents the proposed dynamic step encryption and S-box image encryption algorithm to address S-box image encryption's high correlation and deterministic issues.

A. DYNAMIC STEP ENCRYPTION

Let T as the total encryption times and t is a random number in $1 \sim T$, $(1 \le t \le T)$, we construct a dynamic encryption step matrix that makes each pixel $\mathbf{A}(i,j)$ correspond to a randomly assigned encryption step t. Firstly, use Eq. (1) to generate a chaotic sequence ET with a size of $m \times n$. Then perform the following operations to generate a dynamic encryption step matrix T':

$$T' = \text{mod}\ (fix(ET(i) \times 1000),\ T) + 1, \quad 1 \le i \le m \times n. \tag{5}$$

$$T' = reshape(T', m, n), \quad 1 \le i \le m,\ 1 \le j \le n. \tag{6}$$

where $1 \le T' \le t$. T' is the encryption step matrix, the encryption step t corresponding to a pixel $\mathbf{A}(i,j)$ is denoted $t = \mathbf{T}(i,j)$.

The complete process of dynamic step S-box encryption can be realized by Eq. (7):

$$\mathbf{C_{t+1}}(i,j) = \begin{cases} \mathbf{S}'(\,[\mathbf{C}_t(i,j) - rem(\mathbf{C}_t(i,j), 10)]/10 + 1, \\ rem(\mathbf{C}_t(i,j), 10) + 1\,) & if\ t < T'(i,j) \\ \mathbf{C}_t(i,j) & if\ t \ge T'(i,j) \end{cases} \tag{7}$$

where t is the number of encryption times, and $t \le T$. Figure 3 illustrates the process of the proposed dynamic step S-box encryption.

B. PIXEL DIFFUSION

To further improve the security of the proposed method, the pixel diffusion technique is used to change the encrypted image's statistical characteristics, thus preventing the attacker from obtaining valuable information by comparing the pair of plaintexts and ciphertexts. Apply Eq. (1) to generate a random chaotic sequence $\boldsymbol{Q}$ and transform it into a $m \times n$ size pixel diffusion matrix $\mathbf{Q}'$.

$$Q = \text{mod}\ (fix(ET(i) \times 1000),\ 256), \quad 1 \le i \le m \times n, \quad 0 \le Q \le 255. \tag{8}$$

$$\mathbf{Q}' = reshape(Q, m, n). \quad 1 \le i \le m,\ 1 \le j \le n. \tag{9}$$

where $1 \le \mathbf{Q}'(i,j) \le t$.

The encrypted image after pixel diffusion is $\mathbf{C}'$,

$$\mathbf{C}' = \mathbf{C} \oplus \mathbf{Q}'. \tag{10}$$

C. DECRYPTION

Given the encrypted image $\mathbf{C}'$, first input the password to get x_0 and μ, then use Eq. (1) to generate the sequence P, sequence Q, sequence ET. Next, apply Eq. (5)(6)(8)(9) to obtain the pixel diffusion matrix $\mathbf{Q}'$ and S-box matrix $\mathbf{S}$. Let $\mathbf{C} = \mathbf{C}' \oplus \mathbf{Q}'$, for each pixel $C(i,j)$ in the encrypted image $\mathbf{C}$ has corresponding decryption step t, such that $t = T'(i,j)$. Then, search the $\mathbf{S}(u_1, v_1)$ equivalent to the pixel value $C(i,j)$ in the S-box matrix $\mathbf{S}$ and record the position of the row as u_1 and column as v_1 such that $\mathbf{C}(i,j) = \mathbf{S}(u_1, v_1)$.

Let $C_1(i,j) = u_1 \times 10 + v_1$, $t = t - 1$, if $t > 0$, continue to search $C_1(i,j)$ in the S-box matrix $\mathbf{S}$, and record the row position as u_2 and column position as v_2 in $\mathbf{S}$, such that $\mathbf{C}_1(i,j) = \mathbf{S}(u_2, v_2)$. Let $C_2(i,j) = u_2 \times 10 + v_2$ $t = t - 1$ and repeat the same operation until $t = 0$ to recover the original image $\mathbf{A}$. The decryption algorithm can be summarized as (11), shown at the bottom of the page.

D. THE PROPOSED CHAOTIC-BASED S-BOX IMAGE ENCRYPTION SCHEME

The encryption and decryption process of the proposed chaotic-based S-box image encryption scheme is presented as follows:

1) ENCRYPTION ALGORITHM

Step 1: Input the original image $\mathbf{A}$ and define the image size $[m, n] = size(\mathbf{A})$.

Step 2: Set the password, convert the password into initial security parameters x_0, μ and encryption times T. Then, generate a chaotic sequence P, Q and ET respectively with the Eq. (1).

Step 3: Sort P_i such that $P'_i = Rank\ (P_i)$ and $i \in [0, 255]$. Subsequently, define a new chaotic sequence, P''_j by finding the x that corresponding to all y in ascending order of P'_i, such that x and y are the position index sequence of the identical value in P_i and P'_i respectively. Let $\boldsymbol{S} = reshape(P''_j, 10, 26)$, then generate the single S-box matrix $\mathbf{S}$.

Step 4: Use sequence ET and Eq. (5)(6) to get the dynamic encryption step matrix T'.

Step5: Execute T times of Eq. (7) on the original image $\mathbf{A}$ to obtain the $T - times$ encrypted image $\mathbf{C}_t$.

Step 6: Use Eq. (8)(9) and sequence ET to generate a diffusion matrix $\mathbf{Q}'$, then can obtain the final encrypted image $\mathbf{C}'$ by Eq. (10).

2) DECRYPTION ALGORITHM

Step 1: Get the size of the encrypted image $\mathbf{C}'$, $[m, n] = size(\mathbf{C}')$.

Step 2: Input the password $\mathbf{K}$ and generate the initial parameters x_0, μ and encryption times T. Then, generate a chaotic sequence P, Q and ET respectively with the Eq. (1).

Step 3: Obtain the single S-box matrix $\mathbf{S}$ by the sequence $P_{original}$ and the encryption step matrix T' by the sequence ST.

Step 4: Obtain the image $\mathbf{C}$ through the operation of Eq. (10) on the image $\mathbf{C}'$.

Step 5: Execute T times Eq. (11) on the image $\mathbf{C}$ to restore the original image $\mathbf{A}$.

$$\mathbf{B}_{t+1}(i,j) = \begin{cases} u_t \times 10 + v_t, & t = t - 1 \quad if\ \mathbf{C}_{t-1}(i,j) = \mathbf{S}(u_t, v_t)\ \ \&\ \ t < T'(i,j) \\ \mathbf{B}_t(i,j), & t = t - 1 \quad if\ \mathbf{C}_{t-1}(i,j) = \mathbf{S}(u_t, v_t)\ \ \&\ \ t \ge T'(i,j) \end{cases} \tag{11}$$

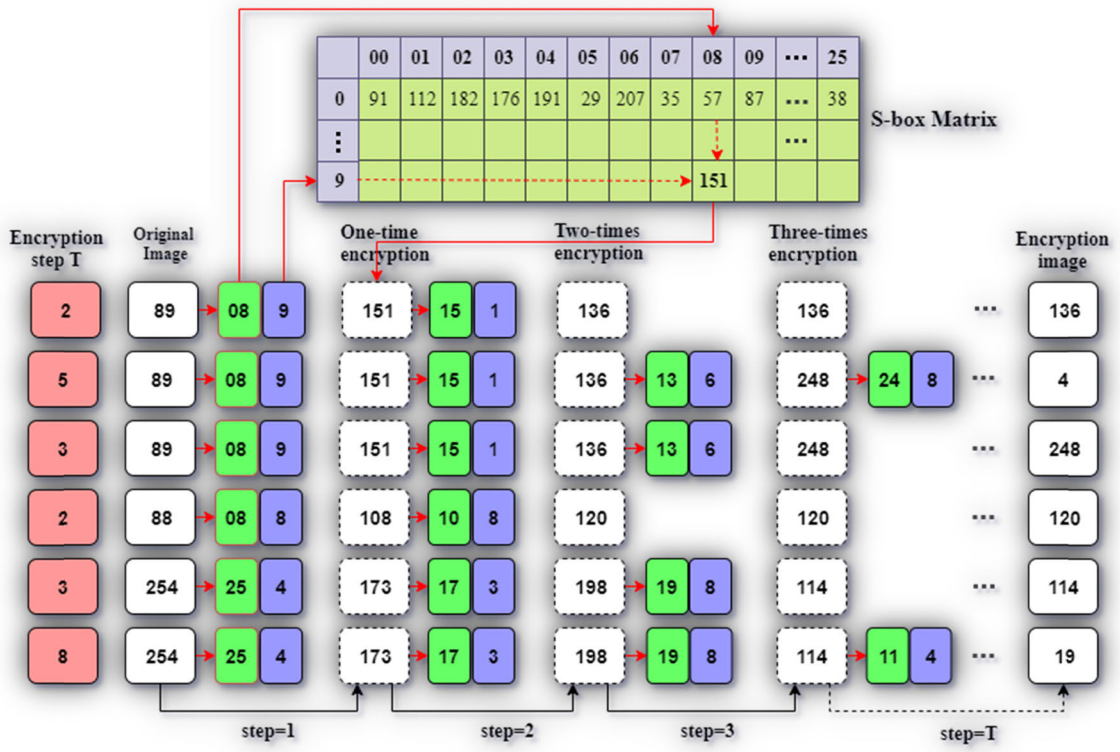

FIGURE 3. Dynamic step S-box encryption.

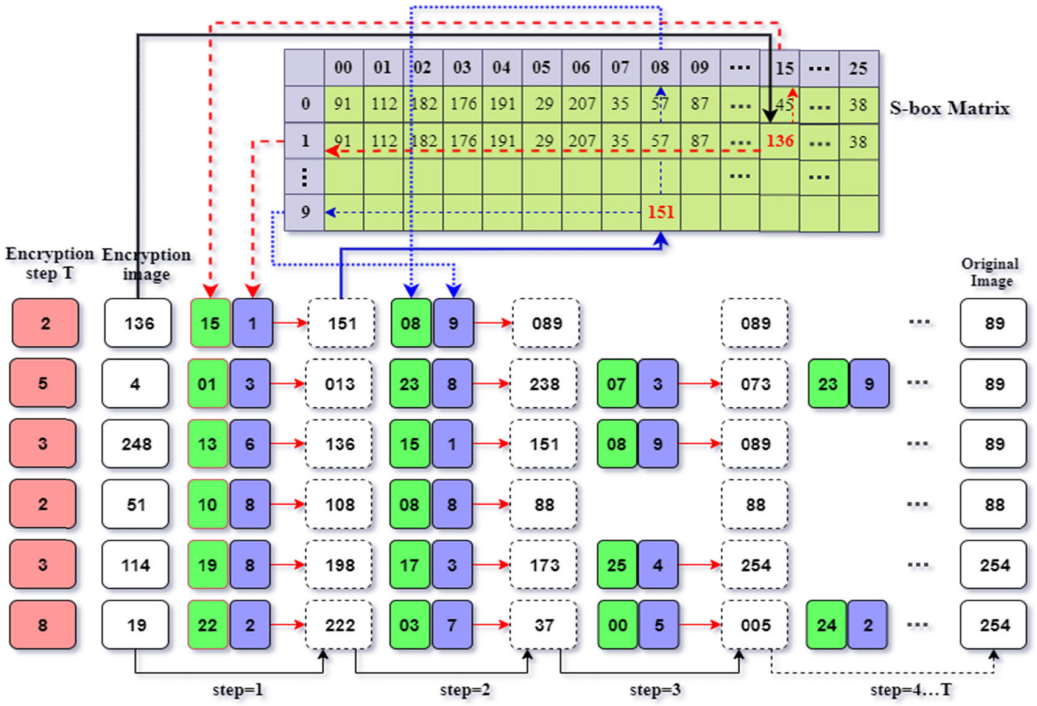

FIGURE 4. Decryption method of dynamic step S-box encryption.

IV. EXPERIMENT RESULT ANALYSES

Several experimental tests have been carried to examine the performance and security properties of the proposed chaotic-based S-box encryption scheme. The experiments are configured and performed on a Windows 10 desktop with an AMD Ryzen 5, CPU 2.10 GHz, 8 GB RAM and the platform

is MATLAB 2018a. The experimental images are standard grey images from the USC-SIPI image dataset, as illustrated in Figure 5.

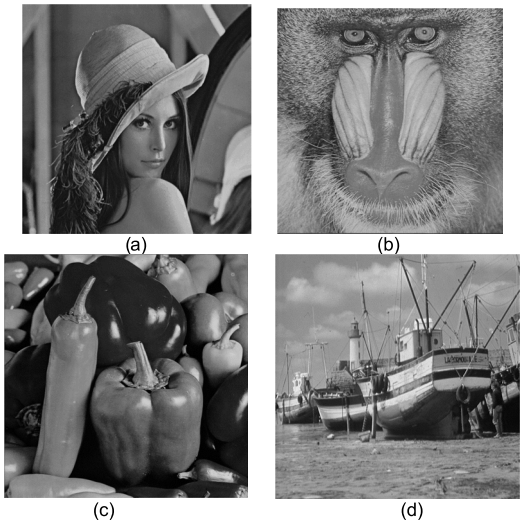

FIGURE 5. Original images. (a) Lena; (b) Baboon; (c) Peppers; (d) Boat.

A. HISTOGRAM ANALYSIS

An image histogram is mainly used to describe the distribution of grey values. In general, the more uniform the distribution of grey values in the encrypted image, the stronger the ability to resist statistical analysis. Figure 6 shows the histogram distribution of the original image and their corresponding encrypted image for different encryption times, T. It can be seen that the grey value distribution of the original image is not uniform and has obvious peaks and changes, illustrated in Figure 6 (b)(j)(n)(r). On the other hand, the histogram distributions are more uniform for their corresponding encrypted image in Figure 6 (d)(h)(l)(p)(t) and tend to be horizontal. The results show that our encryption algorithm can obtain a statistically secure encrypted image.

B. CHI-SQUARE TEST

We apply the quantitative grey uniformity Chi-square test to verify further the uniformity of histogram distribution of the encrypted image, as the greyscale values in histogram analysis are inconsistent. The Chi-square formula is as follows:

$$\chi^2 = \sum_{i=1}^{m\times n} \frac{(A_{ij} - E)^2}{E} \tag{12}$$

where A_{ij} denotes the actual amount of each grey level of the original image and represents the desired amount of each grey level. A smaller experimental Chi-square value implies the ciphertext images are distributed more uniformly, thus improves security defences. Table 2 summarizes the experimental result of the Chi-square test.

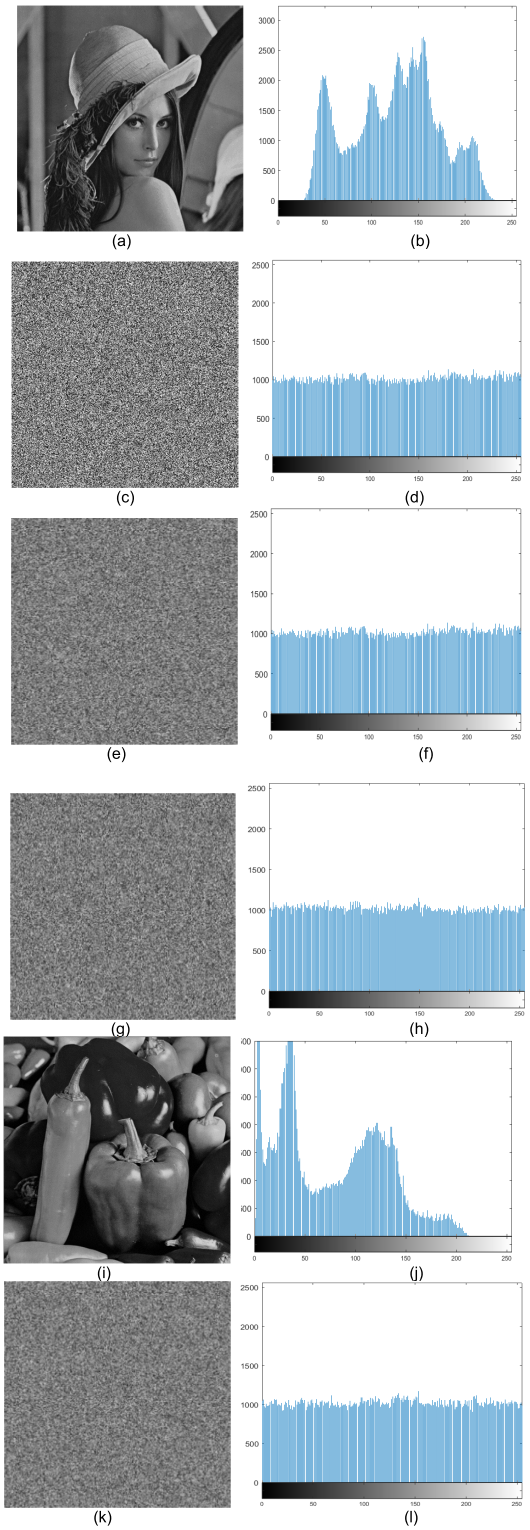

FIGURE 6. Histogram analysis for original image and encrypted image (a) Original image–Lena; (b) Histogram of image–Lena; (c) Encrypted image of Lena for T = 1; (d) Histogram of encrypted image in (c); (e) Encrypted image of Lena for T = 20; (f) Histogram of encrypted image in (e); (g) Encrypted image of Lena for T = 50; (h) Histogram of encrypted image in (g); (i) Original image–Pepper; (j) Histogram of image–Pepper; (k) Encrypted image of Pepper for T = 50; (l) Histogram of encrypted image in (k).

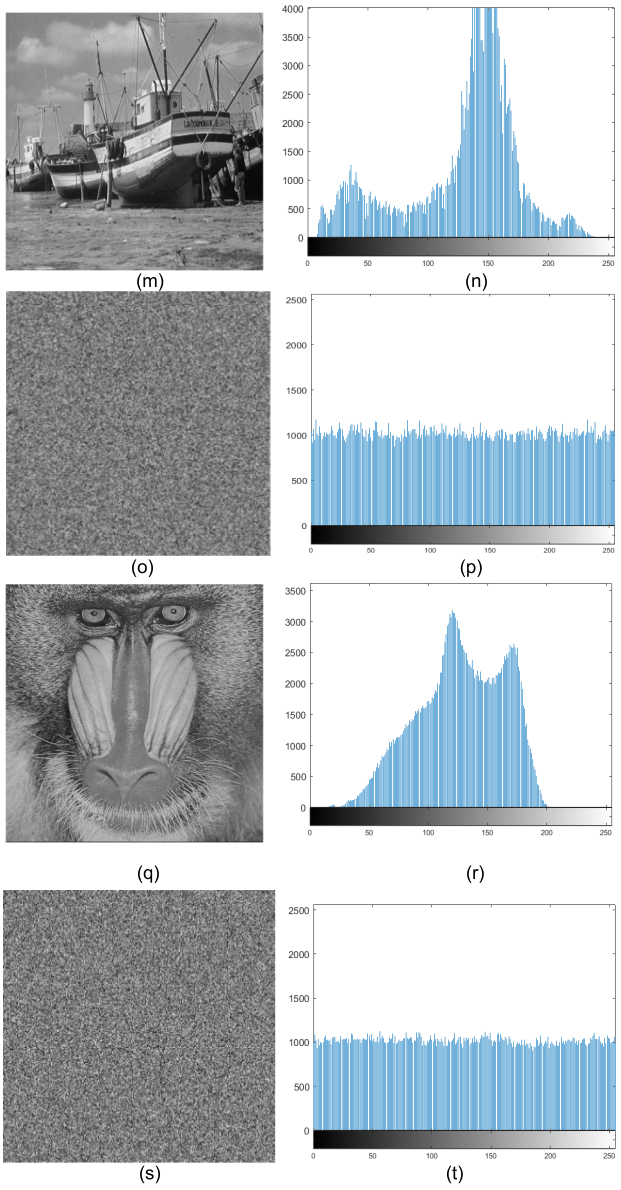

FIGURE 6. *(Continued.)* **Histogram analysis for original image and encrypted image (m) Original image–Pepper; (n) Histogram of image–Boat; (o) Encrypted image of Boat for T = 50; (p) Histogram of encrypted image in (o); (q) Original image–Baboon; (r) Histogram of image–Baboon; (s) Encrypted image of Baboon for T = 50; (t) Histogram of encrypted image in (s).**

When the confidence interval is 95%, i.e. significant level value P = 0.05, the corresponding Chi-square critical value is 293.2478. In this experiment, the corresponding Chi-square test for different carrier images is evaluated when T = 1, T = 20 and T = 50, as discussed in Table 1. The experimental results show that the histogram distribution of the ciphertext image is uniform, and we can conclude that the proposed chaotic-based S-box encryption scheme provides a sophisticated security level.

C. CORRELATION COEFFICIENT ANALYSIS

The correlation coefficient reflects the degree of correlation between adjacent pixel values of an image and is often used to measure the security level of the image encryption scheme. The original image has a high correlation coefficient in general. However, if the encrypted image remains a high correlation, it is bound to the risk of being cracked. Therefore, a secure image encryption algorithm should have a low correlation coefficient and nonlinear distribution, preferably zero correlation or negative correlation relevant. We randomly select 5000 pairs of two adjacent pixels in different directions: horizontal, vertical, and diagonal from the original and encrypted images. The correlation coefficient formula is shown in Eq. (13) and Eq. (14):

$$r(x, y) = \frac{|Cov(x, y)|}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

$$\text{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{14}$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))$, x and y are two adjacent pixel values in the image, N represent the total number of pixels in the sample.

Figure 7 shows the correlation between two adjacent pixels of an image. The original image shows a high correlation in the horizontal, vertical and diagonal directions, and their correlation distribution is linear. The adjacent pixels in the encrypted image are randomly dispersed in three directions, and the distribution correlation is scattered almost randomly.

Table 3 compares the correlation coefficients of our scheme and recent chaotic-based S-box image encryption schemes [49]–[53]. The results of the experiment are based on an average of 50 measurements. We can see that the correlation coefficients of the original image in three directions are close to 1, which indicates the original image pixels are highly correlated. On the other hand, the correlation

TABLE 2. Chi-square test results of images.

Image	Plaintext	Encryption Times	Ciphertext	Decision
Lena	3.9428×10^4	T=1	289.5996	Pass
		T=20	283.3984	Pass
		T=50	274.7188	Pass
Baboon	6.4971×10^4	T=1	289.4609	Pass
		T=20	281.5625	Pass
		T=50	275.7813	Pass
Pepper	5.5865×10^4	T=1	289.0011	Pass
		T=20	272.5000	Pass
		T=50	261.1406	Pass
Boat	9.6281×10^4	T=1	291.4219	Pass
		T=20	266.0469	Pass
		T=50	278.1641	Pass

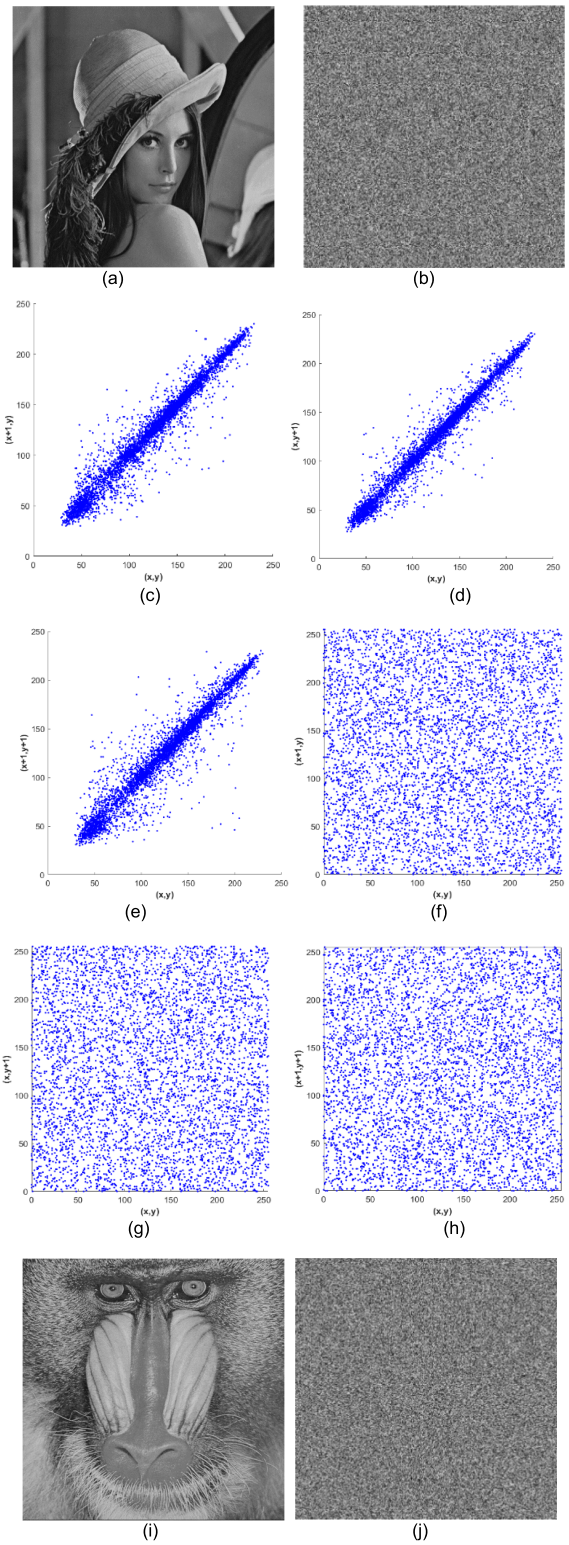

FIGURE 7. Three direction correlation of image adjacent pixels (a)(i): original images; (b)(j): horizontal direction correlation coefficient of original images; (c)(k): vertical direction correlation coefficient of original images; (d)(l): diagonal direction correlation coefficient of original images; (f)(n): horizontal direction correlation coefficient of encrypted images; (g)(o): vertical direction correlation coefficient of encrypted images; (h)(p): diagonal direction correlation coefficient of encrypted images.

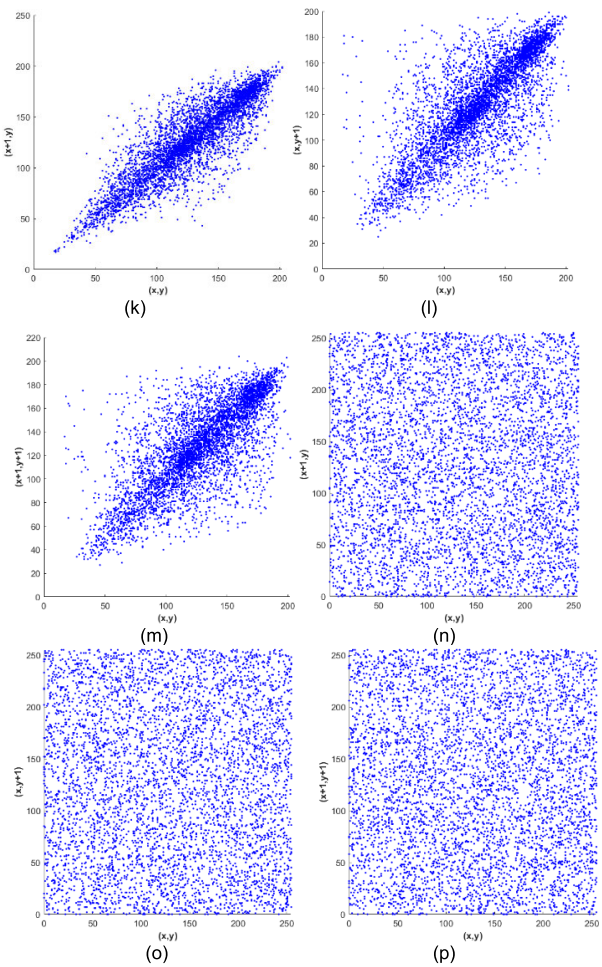

FIGURE 7. *(Continued.)* Three direction correlation of image adjacent pixels (a)(i): original images; (b)(j): horizontal direction correlation coefficient of original images; (c)(k): vertical direction correlation coefficient of original images; (d)(l): diagonal direction correlation coefficient of original images; (f)(n): horizontal direction correlation coefficient of encrypted images; (g)(o): vertical direction correlation coefficient of encrypted images; (h)(p): diagonal direction correlation coefficient of encrypted images.

coefficients of the encrypted image fluctuated around 0, indicating that there is almost no correlation between the source image and the encrypted image. Compared to recent chaotic-based S-box [49]–[53] that generate distinct double or multiple S boxes to achieve a high correlation coefficient, the proposed dynamic step encryption resulted in our scheme enjoys a higher correlation in all directions (Horizontal, Vertical, Diagonal). The correlation coefficient between adjacent pixels of the proposed image encryption scheme is close to zero, indicating that the proposed scheme has higher security by effectively destroying the correlation between the pixels of the original image and the encrypted image.

D. DIFFERENTIAL ANALYSIS

A secure image encryption algorithm should be able to against the differential attacks with its non-deterministic

TABLE 3. Comparison of correlation coefficients between our scheme and related works.

Image	Direction	Plain image	Our Scheme			[47]	[48]	[49]	[50]	[51]
			T=10	T=30	T=50					
Lena	Horizontal	0.9848	–0.0020	–0.0000	**–0.0059**	0.0118	0.0009	–0.0056	0.0044	–0.0005
	Vertical	0.9719	–0.0046	–0.0041	**–0.0064**	–0.0173	0.0876	0.0006	0.0088	0.0013
	Diagonal	0.9588	–0.0044	0.0003	–0.0003	0.0080	0.0040	0.0018	–0.004	**–0.0046**
Baboon	Horizontal	0.7585	**–0.0040**	0.0018	–0.0014	0.0046	0.0018	–0.0007	–0.0000	–0.0037
	Vertical	0.8666	–0.0012	–0.0003	0.0032	**–0.0029**	0.0139	–0.0004	0.0123	–0.0027
	Diagonal	0.7274	**–0.0069**	0.0029	0.0010	0.0091	0.0045	–0.0001	0.0015	–0.0007
Peppers	Horizontal	0.9816	0.0001	–0.0037	–0.0026	**–0.0159**	0.0002	–0.0075	–0.0044	0.0006
	Vertical	0.9798	–0.0036	–0.0052	–0.0012	0.0035	0.0022	0.0041	0.0038	0.0035
	Diagonal	0.9684	–0.0000	–0.0072	–0.0050	–0.0096	0.0004	–0.0016	0.0060	–0.0021
Boat	Horizontal	0.9716	–0.0057	–0.0018	–0.0020	0.0094	0.0036	0.0080	–0.0046	**–0.0080**
	Vertical	0.9381	**–0.0076**	–0.0009	–0.0047	0.0044	0.0042	–0.0015	0.0013	0.0029
	Diagonal	0.9226	–0.0027	**–0.0064**	–0.0018	–0.0103	–0.0006	–0.0004	–0.0015	–0.0041
Bridge	Horizontal	0.9287	–0.0035	–0.0017	–0.0064	–0.0034	0.0020	**–0.0084**	0.0023	0.0015
	Vertical	0.9408	–0.0051	–0.0012	–0.0002	0.0019	**–0.0054**	–0.0027	0.0066	0.0016
	Diagonal	0.8974	–0.0031	–0.0006	–0.0032	–0.0005	0.0019	–0.0009	–0.0006	–0.0023
Camera man	Horizontal	0.9902	0.0011	0.0016	**–0.0079**	0.0029	0.0043	0.0029	0.0074	–0.0031
	Vertical	0.9836	–0.0014	**–0.0059**	0.0018	–0.0016	0.0087	–0.0007	0.0139	–0.0039
	Diagonal	0.9734	**–0.0065**	–0.0064	–0.0017	–0.0019	0.0018	–0.0010	–0.0031	–0.0004
Average	Horizontal	0.9359	–0.00233	–0.00063	**–0.00437**	0.001567	0.002133	–0.00188	0.00085	–0.00220
	Vertical	0.9468	**–0.00392**	–0.00293	–0.00125	0.00106	0.018533	–0.00010	0.00778	0.00045
	Diagonal	0.9080	**–0.00393**	–0.00290	–0.00183	–0.00086	0.00200	–0.00037	–0.00028	–0.00237

TABLE 4. Comparison of differential analysis (UACI and NPCR) between our scheme and related works.

Image	NPCR & UACI	Our Scheme			[47]	[48]	[49]	[50]	[51]
		T=10	T=30	T=50					
Lena	NPCR %	**99.6269**	99.6220	99.6197	99.6083	99.6208	99.6216	99.5784	99.6106
	UACI %	32.6523	32.6540	33.0443	33.1312	31.8345	33.0941	31.7584	**33.1823**
Baboon	NPCR %	**99.6212**	99.6006	99.6082	99.6118	99.6117	99.6220	99.6033	99.6104
	UACI %	32.2105	32.1233	32.1316	**33.1431**	31.7399	32.0669	32.0005	33.1408
Peppers	NPCR %	**99.6235**	99.6147	99.6124	99.6223	99.6113	99.6194	99.5987	99.6102
	UACI %	33.2354	**33.2394**	33.1976	33.1420	32.0007	32.9312	32.8451	33.0534
Boat	NPCR %	**99.6254**	99.6059	99.6159	99.6099	99.6220	99.6132	99.5975	99.6105
	UACI %	32.5399	32.4069	32.3799	33.0410	31.9675	33.0047	32.6984	**33.0696**
Bridge	NPCR %	99.5941	99.6056	**99.6269**	99.6109	99.6052	99.5941	99.6077	99.6016
	UACI %	32.8451	32.7152	32.9693	32.8976	31.9581	32.6059	**32.9995**	32.9539
Average	NPCR %	**99.61822**	99.60976	99.61662	99.61264	99.6142	99.61406	99.59712	99.60866
	UACI %	32.69664	32.62776	32.74454	33.07098	31.90014	32.74056	32.46038	**33.080**

properties. The non-deterministic properties of the image encryption scheme can be determined by analyzing the sensitivity of the encryption scheme in responding to the slight changes of the original image, includes the Number of Pixels Change Rate (NPCR) and the Unified Average Change Intensity (UACI) techniques. NPCR is used to measure the ability to resist the known-plaintext selection attack and the plaintext selection attack, and the ideal value is 100%. The closer

TABLE 5. Comparison of image entropy rate between our scheme and related works.

Image	Original image	Our Scheme			[49]	[50]	[51]	[52]	[53]
		T=10	T=30	T=50					
Lena	7.4492	7.9961	7.9965	7.9971	7.9970	7.9932	7.9972	7.9969	7.9969
Baboon	7.1393	7.9969	7.9962	7.9961	7.9973	7.9955	7.9972	7.9970	7.9970
Peppers	7.3564	7.9975	7.9967	7.9970	7.9972	7.9958	7.9973	7.9961	7.9971
Boat	7.1913	7.9970	7.9967	7.9967	7.9973	7.9961	7.9970	7.9965	7.9969
Bridge	5.7056	7.9954	7.9958	7.9961	7.9936	7.9955	7.9947	7.9938	7.9943
Average	–	7.99658	7.99638	**7.99660**	7.99648	7.99522	**7.99668**	7.99606	7.99644

to 100%, the more sensitive the ciphertext is to plaintext changes. UACI is used to measure the ability to resist differential attacks. The higher the value of UACI, the stronger the ability to resist differential attack. For two plaintext images with an only one-pixel value different, the corresponding ciphertext images are marked as C_1 and C_2 respectively, then the calculation formula of NPCR and UACI is as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \tag{15}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{16}$$

where $D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) = C_2(i,j), \end{cases}$

M and N are the width and height of the image respectively.

We selected different carrier images and tested them 50 times by changing their different pixels. Table 4 summarizes the analysis result of UACI and NPCR. From the data, we can see that the NPCR value is between 99.5941 and 99.6269, with an average of 99.61487, which is very close to 100%. Meanwhile, the value of UACI is concentrated between 32.1233 and 33.2394, with an average value of 32.68925. Comparing UACI and NPCR values with rent chaotic-based S-Box encryption schemes, our scheme performs better than other schemes [47]–[51] in NPCR analysis. The UACI of reference [51] is the highest, with an average of 33.080. Our scheme is relatively close to their achievement and has advantages over recent works [47]–[50]. The experimental results show that our scheme has good robustness against differential attacks.

E. IMAGE ENTROPY ANALYSIS

Entropy is used to describe the chaotic degree of a system. The image entropy is used to describe the average number of bits in the grey level set of an image, which can reflect the average amount of information in the image. When the probability of the occurrence of each grey value in the image is completely equal, the entropy reaches the ideal value of 8. Theoretically, the higher the entropy, the less likely the information is to be leaked. Therefore, the image encryption method with good performance should make the image as much as possible the image entropy is close to 8, and the calculation formula of image entropy is as follows:

$$H(s) = \sum_{s} p(s_i)\ \log_2 P(s_i)^{-1} \tag{17}$$

$$p_{ij} = f(i,j) / \sum_{i=1}^{M} \sum_{j=1}^{N} f(i,j) \tag{18}$$

where $p(s_i)$ is the probability of occurrence of grey value s_i, $f(x, y)$ as the grey value of the pixel (i, j) in the image.

If $M \times N$ is the local window of the image, then the field is called the local entropy of the image. Each pixel of the image is represented by the local entropy value of its window, and the local entropy description of the image is obtained.

1) IMAGE ENTROPY ANALYSIS

The entropy of our scheme and related works [49]–[53] for different encrypted images is given in Table 5. We can see that the corresponding entropy of our scheme exceeds 7.995, with an average value of 7.996362, which is very close to the ideal value of 8. Thus, our scheme is better than recent chaotic-based S-box encryption schemes [49]–[51], [53], and it is only 0.00008 less than the average value of entropy in Ref. [51]. Through experiments, we infer that our scheme can effectively resist the direct attack.

2) IMAGE LOCAL ENTROPY ANALYSIS

Image local entropy is the result of all pixels in the window, which has the capacity to resist noise interference and geometric distortion. The larger the window to calculate local entropy is, the stronger the ability to resist noise interference and geometric distortion is. Image local entropy reflects the difference of the grey value of pixels in the local window. The smaller the local entropy is, the more significant the difference of the grey value of pixels in the window is. As illustrated in Figure 8, the abscissa and ordinate are the

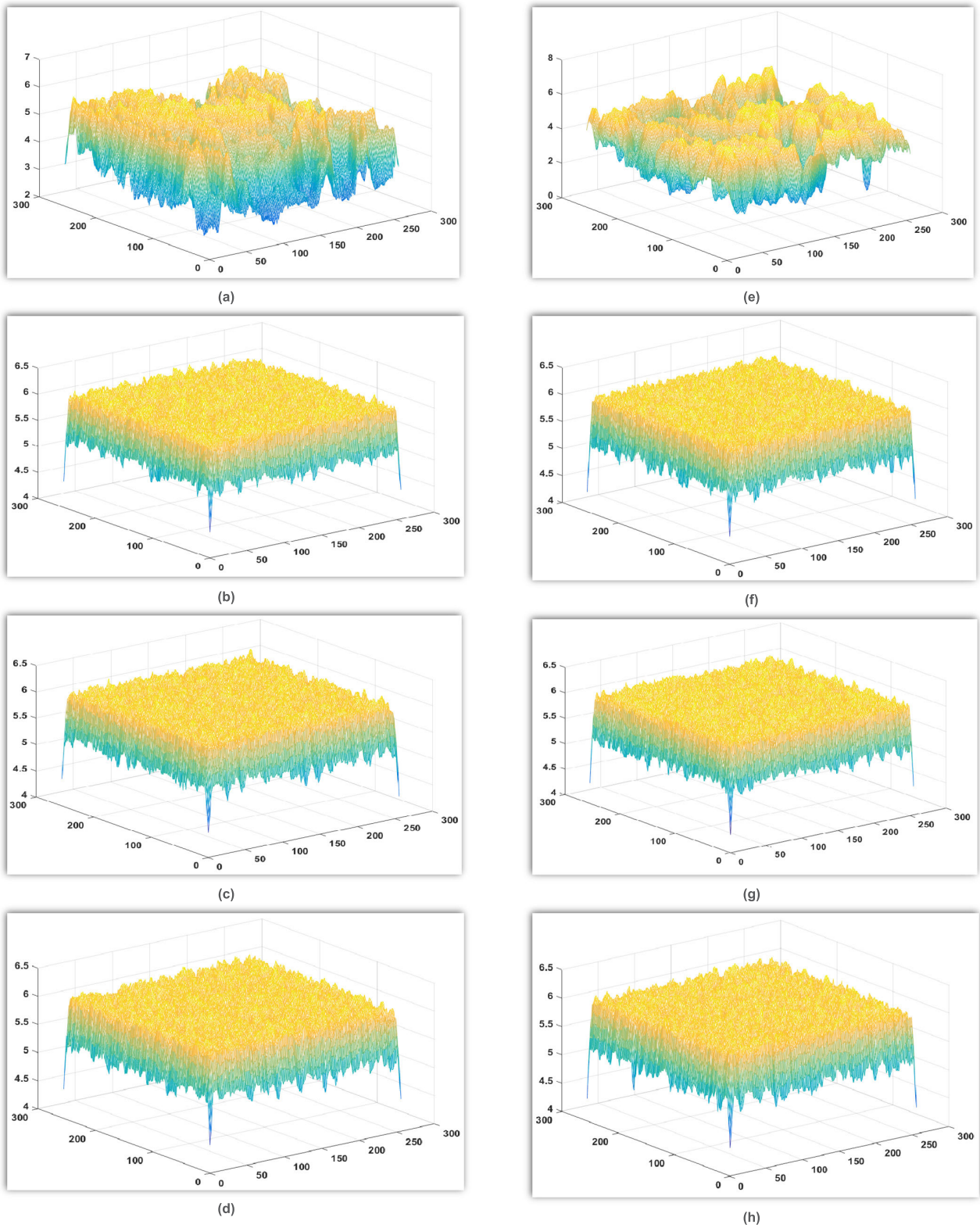

FIGURE 8. Image Local Entropy (a) Lena-local entropy; (b): Lena- encrypted image (T = 1) local entropy; (c): Lena- encrypted image (T = 20) local entropy; (d): Lena- encrypted image (T = 50) local entropy; (e): Peppers-local entropy; (f): Peppers - encrypted image (T = 1) local entropy; (g): Peppers - encrypted image (T = 20) local entropy; (h): Peppers - encrypted image (T = 50) local entropy.

image pixel positions, and the height coordinate is the local entropy value of the point. Compared with the local entropy of the original image, it can be clearly seen that the local entropy in the encrypted image window is larger, so the grey value difference of the pixels in the window is smaller, and the total entropy image looks smoother.

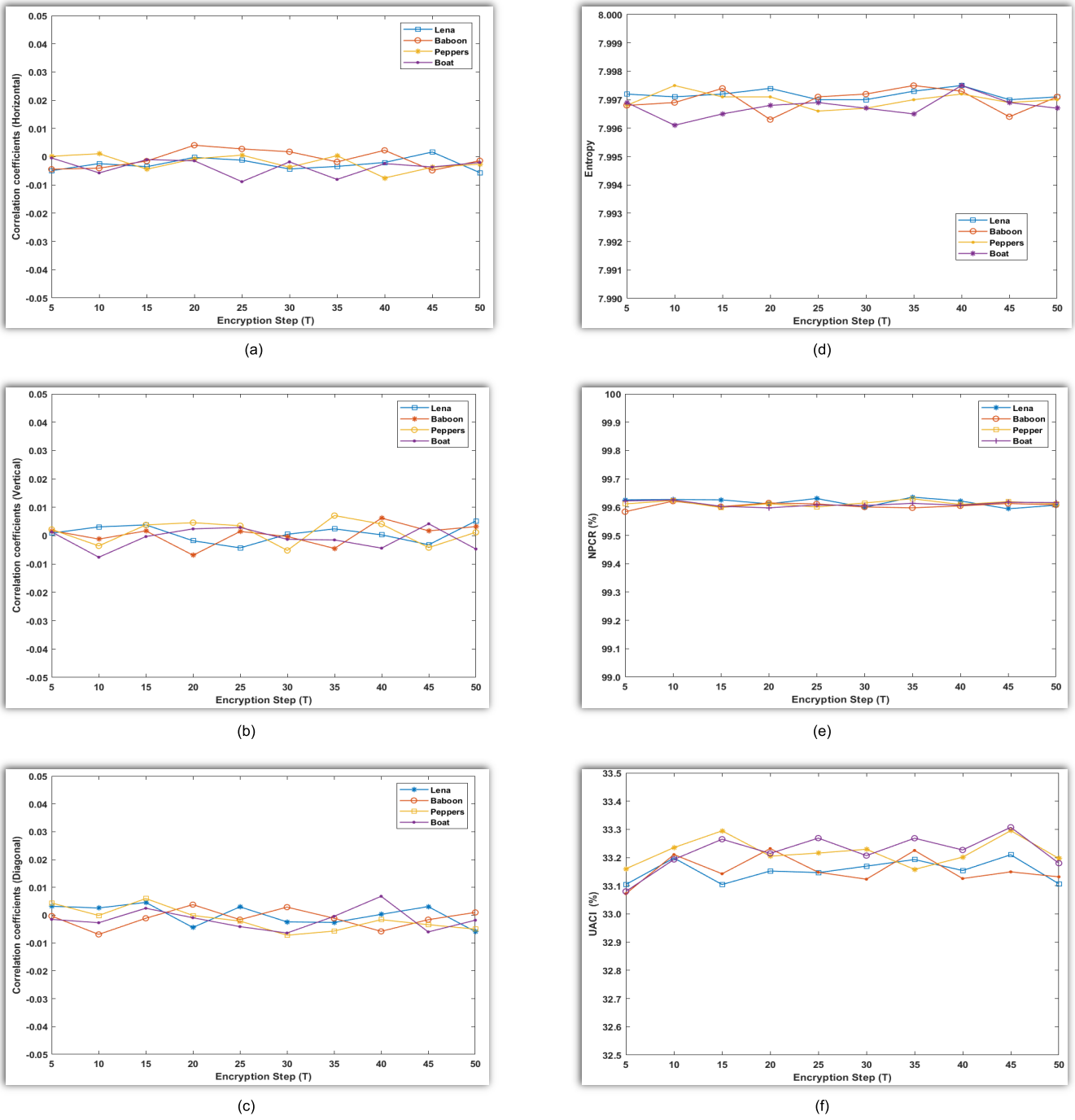

FIGURE 9. Relationship between encryption step and algorithm performance (a) Correlation coefficients (Horizontal); (b) Correlation coefficients (Vertical); (c) Correlation coefficients (Diagonal); (d) Entropy value; (e) NPCR; (f) UACI.

F. DYNAMIC ENCRYPTION STEP(T) AND ALGORITHM PERFORMANCE

We ran a series of experiments to verify the impact of the proposed dynamic encryption step on the chaotic-based S-box algorithm's performance, including correlation coefficients (horizontal, vertical, diagonal), differential analysis (UACI and NPCR) and entropy analysis. Figure 9 shows that all curves fluctuate in a small range, which shows that the encryption step size has no direct impact on the performance of the algorithm. Among them:

Horizontal correlation coefficients $\in [-0.0075,\ 0.0041]$,
Vertical correlation coefficients $\in [-0.0076,\ 0.0071]$,
Diagonal correlation coefficients $\in [-0.0072,\ 0.0088]$,
$NPCR \in [99.5838\%,\ 99.6353\%]$,
$UACI \in [33.0718\%,\ 33.3074\%]$,
$Entropy \in [7.9955,\ 7.9975]$.

According to different original images, the experimental comparison is carried out under different parameter data conditions from six aspects: horizontal correlation coefficients, vertical correlation coefficients, diagonal correlation coefficients, UACI NPCR, etc. The experimental results are shown in Figure 9.

The experiment result also shows that the algorithm's performance does not depend on the dynamic encryption step. Instead, it enables a relatively small encryption step, further reducing the computation and improving the algorithm's performance. Thus, our scheme has obvious advantages over recent works [49]–[53].

G. ROBUSTNESS ANALYSIS

This section implements the salt and pepper noise attacks, Gaussian noise attacks, and loss attacks to verify our algorithm's anti-interference capabilities against noise. We add Gaussian white noise and salt, and Pepper noise with different variance and zero mean value to encrypted Lena, Peppers, boat and Baboon images. After the encrypted image is attacked by noise, the decryption results are shown in Figure 10, Figure 11, and Figure 12.

1) SALT AND PEPPER NOISE ATTACKS
2) GAUSSIAN NOISE ATTACKS
3) LOSS ATTACKS

As illustrated in Figure 10 and Figure 11, the decrypted image becomes increasingly blurry as the noise intensity increases, but the contour and primary texture of the image remain apparent, indicating that our scheme can resist certain noise attacks. The experimental result of an encrypted image data loss attack is illustrated in Figure 12. The encrypted picture data missing area has no effect on the decryption of any other regions. As a result, the corresponding image area that cannot be appropriately decrypted is limited in the data loss area, and other regions can be decrypted accurately, indicating that our scheme has a certain resistance to the data loss attack. In a nutshell, the robustness test experimental results in Figure 10, Figure 11, and Figure 12 demonstrated that our scheme has strong robustness to noise and loss attacks.

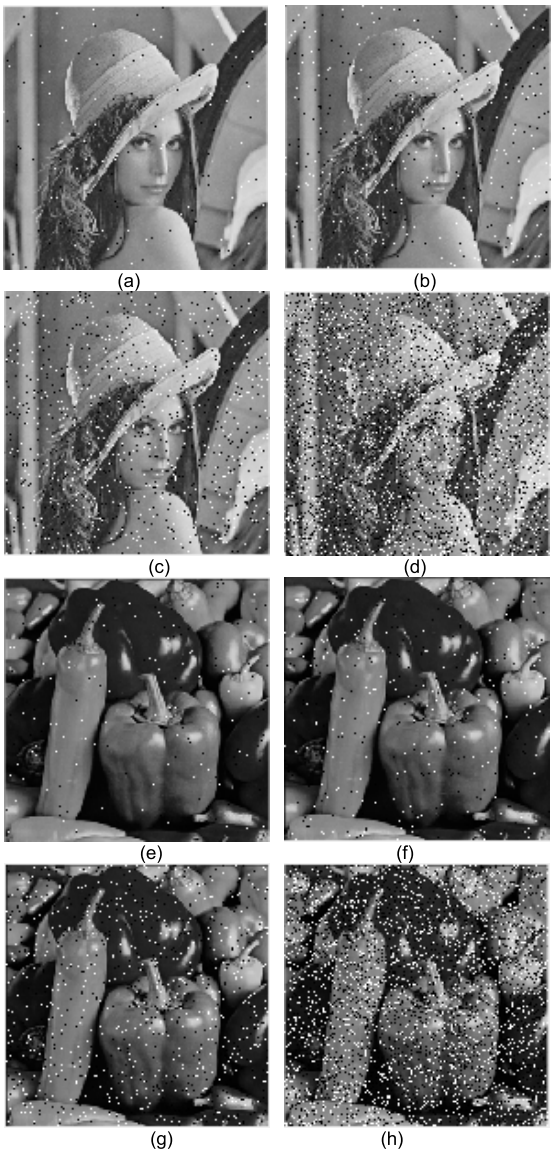

FIGURE 10. Test of adding salt & pepper noise (a) Lena encrypted image +1%; (b) Lena encrypted image +2%; (c) Lena encrypted image +5%; (d) Lena encrypted image +20%; (e) Peppers encrypted image +1%; (f) Peppers encrypted image +2%; (g) Peppers encrypted image +5%; (h) Peppers encrypted image +20%.

H. KEY SPACE AND SENSITIVITY ANALYSIS

To withstand an exhaustive attack, a secure encryption algorithm should be sensitive to the key. The term ''key sensitivity'' refers to the fact that if the decryption key and the encryption key change only slightly, the useful information cannot be recovered at all. The security of the proposed scheme is constructed based on the chaotic properties of the Logistic map. The security properties are highly sensitive to the initial value. When the initial value is 10^{-15} different, the generated sequence will be completely different. Therefore, the sensitivity of the chaotic system to initial values and parameters shows that the constructed S-box is extremely sensitive to the key K. Without the correct key K, it is difficult to reconstruct the correct S-box and the correct encryption step sequence. Furthermore, without an accurate S-box as a reference and accurate encryption step control, it is difficult for the destroyer to know the replacement relationship of each pixel, so it is difficult to decipher. The experimental result of key space and sensitivity testing are presented in Figure 13.

I. ENCRYPTION TIME TEST

Encryption speed is a key performance indicator of an encryption algorithm to ensure its practicability in supporting real-world applications. We implement recent S-box based image encryption algorithms [49]–[53] and compared their

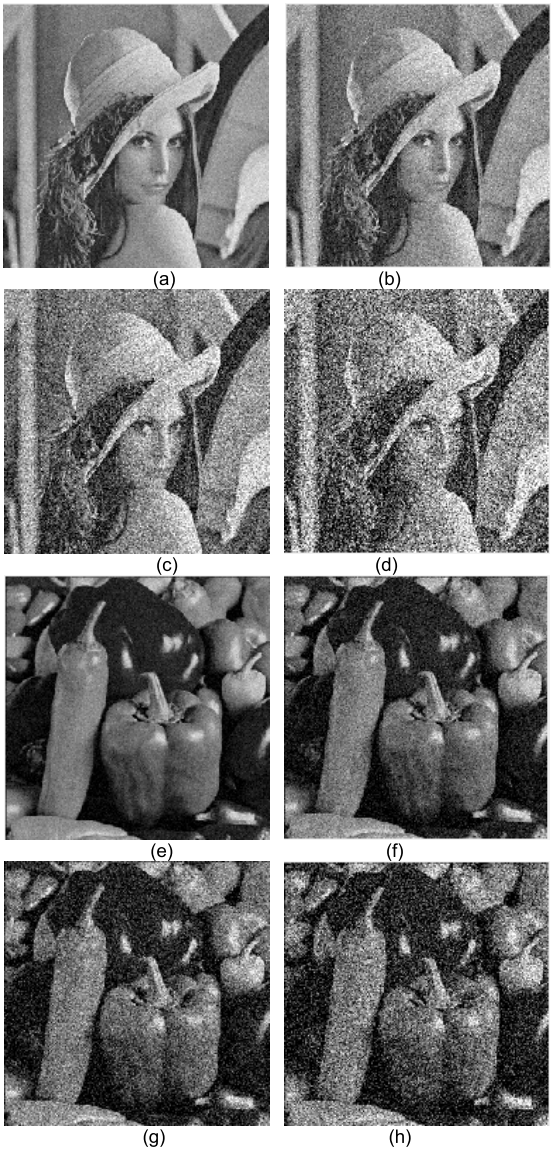

FIGURE 11. Test of adding Gaussian noise (a): Lena encrypted image (intensity = 0.05); (b): Lena encrypted image (intensity = 0.1); (c): Lena encrypted image (intensity = 0.2); (d): Lena encrypted image (intensity = 0.3); (e): Peppers encrypted image (intensity = 0.05); (f): Peppers encrypted image (intensity = 0.1); (g): Peppers encrypted image (intensity = 0.2); (h): Peppers encrypted image (intensity = 0.3).

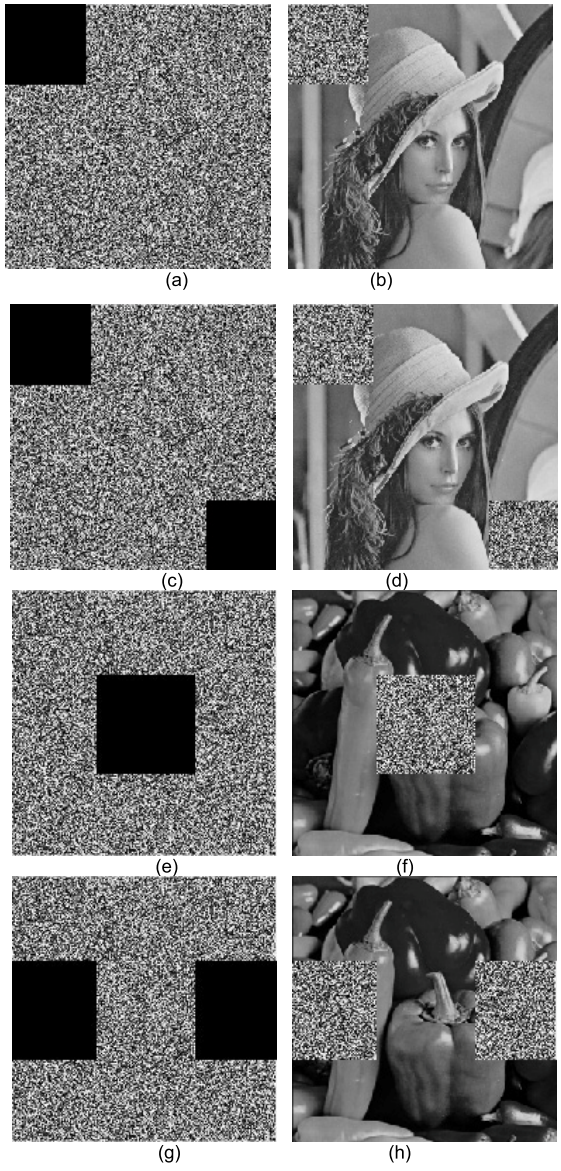

FIGURE 12. Test of loss attacks.

TABLE 6. Encryption time and comparisons (unit: second).

	Proposed	[49]	[50]	[51]	[52]	[53]
Average Time	0.3381	0.3633	0.7232	0.3458	0.5573	0.2758

performance with our scheme. The experiments are configured and performed on a Windows 10 desktop with an AMD Ryzen 5, CPU 2.10 GHz, 8 GB RAM. The measurement is taken based on the average of 100 runs, and encryption time is clocked for one round of encryption to achieve more accurate testing. The experimental and comparison results are illustrated in Table 6.

The time required for one-time encryption of the algorithm in this paper is slightly slower than Ref. [53], but more efficient than Ref. [49]–[52]. In fact, the image encryption algorithm based on the S-box approach is mainly spent on generating S-box, and the encryption time is shorter than other approaches. Compared to recent S-box based encryption schemes [49]–[52] that involve a complex, chaotic system, our scheme uses a one-dimensional chaotic system that enjoys a higher generation efficiency. Also, the usage of multiple S-box during the encryption increased the computation time. For instance, our scheme only needs to generate an S-box, but Ref. [52] needs to generate four S-Boxes.

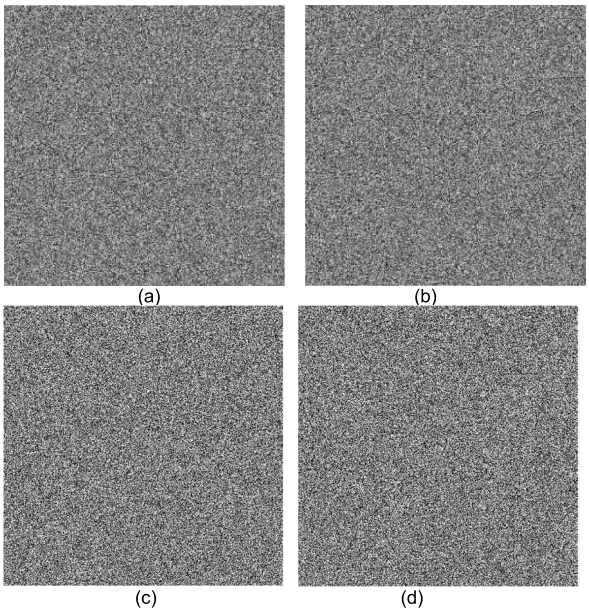

FIGURE 13. Key space and sensitivity testing (a) Decryption of S-box with x_0 a difference of 10^{-15}; (b) Decryption of S-box with μ a difference of 10^{-15}; (c) Decryption of encryption step with x_0 a difference of 10^{-15}; (d) Decryption of encryption step with μ a difference of 10^{-15}.

V. CONCLUSION

This paper presents a new chaotic-based S-box image encryption scheme, which employs a new low dimensional chaotic-based single S-box and dynamic encryption step. Compared to recent chaotic-based S-box image encryption schemes that rely on the high-dimensional continuous chaotic system to strengthen their S-box security, which increased their algorithm complexity, we directed to apply a logistic map to generate a low dimensional chaotic sequence in constructing S-box structure. Our scheme has obvious efficiency advantages since it only involves a simple row-column transform process and eliminates heavy mathematical operations. The image entropy analysis results show that our scheme can achieve a better chaotic degree than recent works. Next, we introduced a dynamic encryption step technique to address the high correlation and deterministic issues in multiple S-box encryptions. Subsequently, pixel diffusion is used to change the statistical characteristics of the encrypted image. The experimental results in correlation coefficient and differential analysis show that our scheme has significantly reduced the high correlation between the pixes of source images. Thus, our scheme has the advantages over the recent double or multiple S-boxes approaches that generate distinct S-boxes to support multiple S-box encryptions, which increased computing workloads and not effectively solving the root problem. Lastly, we extended S-box sized to 10×26 to support more complex image encryption applications without sacrificing the security and algorithm complexity. Experimental results and further security analysis verified the significance of our scheme in supporting real-time image encryption.

REFERENCES

[1] Z. Tang, X. Zhang, and S. Zhang, "Robust perceptual image hashing based on ring partition and NMF," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 3, pp. 711–724, Mar. 2014.

[2] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust image hashing with ring partition and invariant vector distance," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 200–214, Jan. 2016.

[3] V. M. S. Garcia, M. D. G. Ramirez, R. F. Carapia, E. Vega-Alvarado, and E. R. Escobar, "A novel method for image encryption based on chaos and transcendental numbers," *IEEE Access*, vol. 7, pp. 163729–163739, 2019, doi: 10.1109/access.2019.2952030.

[4] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Process.*, vol. 11, no. 5, pp. 324–332, Jan. 2017.

[5] X.-Y. Wang, S.-X. Gu, and Y.-Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Opt. Lasers Eng.*, vol. 68, pp. 126–134, May 2015.

[6] H. W. Safi and A. Y. Maghari, "Image encryption using double chaotic logistic map," in *Proc. Int. Conf. Promising Electron. Technol. (ICPET)*, Deir El-Balah, Palestine, Oct. 2017, pp. 66–70.

[7] L. Liu, Z. Zhang, and R. Chen, "Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos," *IEEE Access*, vol. 7, no. 8, pp. 126450–126463, 2019, doi: 10.1109/access.2019.2938181.

[8] W. Yuan, A. Sultan, and S. B. Hussain, "Robust hybrid plaintext-related image encryption using hyper chaos signal processing," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 9, pp. 49–56, Sep. 30 2019.

[9] W. Yuan, X. Yang, W. Guo, and W. Hu, "A double-domain image encryption using hyper chaos," in *Proc. 19th Int. Conf. Transparent Opt. Netw. (ICTON)*, Girona, Spain, Jul. 2017, pp. 1–4.

[10] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, and P. Raveendran, "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Process.*, vol. 140, no. 5, pp. 87–96, Nov. 2017.

[11] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Sci. Rep.*, vol. 10, no. 1, pp. 1–15, Dec. 2020.

[12] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020, doi: 10.1109/access.2020.2965740.

[13] Y. Guo, X. Xu, S. Jing, T. Jin, and M. Jin, "Optical image encryption based on spiral phase transform and generalized fibonacci chaos," *J. Electron. Inf. Technol.*, vol. 42, no. 4, pp. 988–996, Apr. 2020, doi: 10.11999/jeit190514.

[14] T. Liu, H. Yan, S. Banerjee, and J. Mou, "A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation," *Chaos, Solitons Fractals*, vol. 145, Apr. 2021, Art. no. 110791, doi: 10.1016/j.chaos.2021.110791.

[15] T. Liu, S. Banerjee, H. Yan, and J. Mou, "Dynamical analysis of the improper fractional-order 2D-SCLMM and its DSP implementation," *Eur. Phys. J. Plus*, vol. 136, no. 5, pp. 1–17, May 2021, doi: 10.1140/epjp/s13360-021-01503-y.

[16] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimedia Tools Appl.*, vol. 79, nos. 33–34, pp. 24993–25022, Sep. 2020, doi: 10.1007/s11042-020-09111-1.

[17] M. Samiullah, W. Aslam, H. Nazir, M. I. Lali, B. Shahzad, M. R. Mufti, and H. Afzal, "An image encryption scheme based on DNA computing and multiple chaotic systems," *IEEE Access*, vol. 8, pp. 25650–25663, 2020, doi: 10.1109/access.2020.2970981.

[18] Y. Liu and J. Zhang, "A multidimensional chaotic image encryption algorithm based on DNA coding," *Multimedia Tools Appl.*, vol. 79, nos. 29–30, pp. 21579–21601, Aug. 2020, doi: 10.1007/s11042-020-08880-z.

[19] M. Kar, A. Kumar, D. Nandi, and M. K. Mandal, "Image encryption using DNA coding and hyperchaotic system," *IETE Tech. Rev.*, vol. 37, no. 1, pp. 12–23, Jan. 2020, doi: 10.1080/02564602.2018.1544855.

[20] W. Yu, Y. Liu, L. Gong, M. Tian, and L. Tu, "Double-image encryption based on spatiotemporal chaos and DNA operations," *Multimedia Tools Appl.*, vol. 78, no. 14, pp. 20037–20064, Jul. 2019, doi: 10.1007/s11042-018-7110-2.

[21] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," *IET Image Process.*, vol. 13, no. 9, pp. 1535–1539, Jul. 2019, doi: 10.1049/iet-ipr.2019.0051.

[22] 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 Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019, doi: 10.1007/s00521-017-2993-9.
[23] H. Liu, B. Zhao, and L. Huang, "A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map," *IEEE Access*, vol. 7, pp. 65450–65459, 2019, doi: 10.1109/access.2019.2917498.
[24] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes," *Entropy*, vol. 21, no. 3, p. 319, Mar. 2019, doi: 10.3390/e21030319.
[25] S. Khan, L. Han, H. Lu, K. K. Butt, G. Bachira, and N.-U. Khan, "A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI," *IEEE Access*, vol. 7, pp. 81333–81350, 2019, doi: 10.1109/access.2019.2920383.
[26] C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7227–7258, Mar. 2020, doi: 10.1007/s11042-019-08226-4.
[27] H. Zhang, X. Wang, X. Wang, and P. Yan, "Novel multiple images encryption algorithm using CML system and DNA encoding," *IET Image Process.*, vol. 14, no. 3, pp. 518–529, Feb. 2020, doi: 10.1049/iet-ipr.2019.0771.
[28] X. Wang and H. Sun, "A chaotic image encryption algorithm based on zigzag-like transform and DNA-like coding," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 34981–34997, Dec. 2019, doi: 10.1007/s11042-019-08085-z.
[29] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Comput. Appl.*, vol. 32, no. 9, pp. 4961–4988, May 2020, doi: 10.1007/s00521-018-3913-3.
[30] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019, doi: 10.1016/j.optlaseng.2019.04.011.
[31] Y. Song, Z. Zhu, W. Zhang, L. Guo, X. Yang, and H. Yu, "Joint image compression–encryption scheme using entropy coding and compressive sensing," *Nonlinear Dyn.*, vol. 95, no. 3, pp. 2235–2261, Feb. 2019, doi: 10.1007/s11071-018-4689-9.
[32] R. Ponuma and R. Amutha, "Encryption of image data using compressive sensing and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 11857–11881, 2019, doi: 10.1007/s11042-018-6745-3.
[33] R. Ponuma and R. Amutha, "Image encryption using sparse coding and compressive sensing," *Multidimensional Syst. Signal Process.*, vol. 30, no. 4, pp. 1895–1909, Oct. 2019, doi: 10.1007/s11045-019-00634-x.
[34] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019, doi: 10.1016/j.optlastec.2019.01.039.
[35] D. Zhang, X. Liao, B. Yang, and Y. Zhang, "A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2191–2208, Jan. 2018, doi: 10.1007/s11042-017-4370-1.
[36] J. Wang, Q. H. Wang, and Y. Hu, "Image encryption using compressive sensing and detour cylindrical diffraction," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–14, Jun. 2018, doi: 10.1109/jphot.2018.2831252.
[37] W.-W. Hu, R.-G. Zhou, J. Luo, S.-X. Jiang, and G.-F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Inf. Process.*, vol. 19, no. 3, p. 82, Jan. 2020, doi: 10.1007/s11128-020-2579-9.
[38] N. Khalifa, R. L. Filali, and M. Benrejeb, "A fast selective image encryption using discrete wavelet transform and chaotic systems synchronization," *Inf. Technol. Control*, vol. 45, no. 3, pp. 235–242, Sep. 2016, doi: 10.5755/j01.itc.45.3.12650.
[39] H. Singh, "Cryptosystem for securing image encryption using structured phase masks in Fresnel wavelet transform domain," *3d Res.*, vol. 7, no. 11, p. 34, Dec. 2016, doi: 10.1007/s13319-016-0110-y.
[40] Q. Liu, Y. Wang, J. Wang, and Q.-H. Wang, "Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain," *Opt. Rev.*, vol. 25, no. 1, pp. 46–55, Feb. 2018, doi: 10.1007/s10043-017-0390-3.
[41] S. Ahadpour and Y. Sadra, "Chaotic trigonometric Haar wavelet with focus on image encryption," *J. Discrete Math. Sci. Cryptogr.*, vol. 20, no. 5, pp. 1217–1239, Jul. 2017, doi: 10.1080/09720529.2016.1187958.
[42] H.-S. Li, C. Li, X. Chen, and H. Xia, "Quantum image encryption based on phase-shift transform and quantum Haar wavelet packet transform," *Modern Phys. Lett. A*, vol. 34, no. 26, Aug. 2019, Art. no. 1950214, doi: 10.1142/s0217732319502146.
[43] J. Wang, W. Liu, and S. Zhang, "Adaptive encryption of digital images based on lifting wavelet optimization," *Multimedia Tools Appl.*, vol. 79, nos. 13–14, pp. 9363–9386, Apr. 2020, doi: 10.1007/s11042-019-7704-3.
[44] A. Belazi, A. A. A. El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Opt. Lasers Eng.*, vol. 88, pp. 37–50, Jan. 2017, doi: 10.1016/j.optlaseng.2016.07.010.
[45] H. Ga and W. Zeng, "Image compression and encryption based on wavelet transform and chaos," *Comput. Opt.*, vol. 43, no. 2, pp. 258–263, Apr. 2019, doi: 10.18287/2412-6179-2019-43-2-258-263.
[46] S. Jahangir and T. Shah, "Designing S-boxes triplet over a finite chain ring and its application in RGB image encryption," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 26885–26911, Oct. 2020, doi: 10.1007/s11042-020-08995-3.
[47] Z. Zhu, Y. Song, W. Zhang, H. Yu, and Y. Zhao, "A novel compressive sensing-based framework for image compression-encryption with S-box," *Multimedia Tools Appl.*, vol. 79, nos. 35–36, pp. 25497–25533, Sep. 2020, doi: 10.1007/s11042-020-09193-x.
[48] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7279–7297, Mar. 2020, doi: 10.1007/s11042-019-08342-1.
[49] M. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, pp. 3041–3064, Mar. 2020, doi: 10.1007/s11071-019-05413-8.
[50] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractal*, vol. 95, no. 2, pp. 91–92, 2017, doi: 10.1016/j.chaos.2016.12.018.
[51] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020, doi: 10.1109/access.2020.2970806.
[52] X. Wang *et al.*, "S-box based image encryption application using a chaotic system without equilibrium," *Appl. Sci.-Basel*, vol. 9, no. 4, pp. 781–798, Feb. 2019, doi: 10.3390/app9040781.
[53] X.-P. Zhang, R. Guo, H.-W. Chen, Z.-M. Zhao, and J.-Y. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chin. Phys. B*, vol. 27, no. 8, Aug. 2018, Art. no. 080701, doi: 10.1088/1674-1056/27/8/080701.

WANG JI JUN received the M.C.A. degree from Guangxi Normal University, in 2005 and 2008. He is currently pursuing the Ph.D. degree with the Faculty of Computing and Informatics, Universiti Malaysia Sabah (UMS).

He worked as an Associate Professor with the Faculty of Information and Statistics, Guangxi University of Finance and Economics. He has published over 20 papers, including book chapters, journals, technical reports, and proceedings. He received few research grants in the related fields. His research interests include data hiding, digital watermark, and image processing.

TAN SOO FUN (Member, IEEE) received the B.Tech. degree in e-commerce and the M.Sc. degree in computer science from Universiti Malaysia Sabah (UMS), in 2006 and 2009, respectively, and the Ph.D. degree from Universiti Sains Malaysia (USM), in 2017. She is currently a Senior Lecturer with the Faculty of Computing and Informatics, UMS. She has published over 40 papers, includes book chapters, journals, technical reports, and proceedings. She received ten research grants in the related field. She is a Certified IPv6 Network Engineer, Certified IPv6 Security Engineer, Huawei Certified ICT Professional (HCIP), Huawei Certified Academy Instructor (HCAI), and IBM Certified Academic Associate. Her research interests include post–quantum cryptography and information and network security.