Received: May 27, 2023. Revised: July 22, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Encryption in IOT Using Hyper-chaotic System

Rawia Abdulla Mohammed[1]* **Maisa'a Abid Ali Khodher[2]** **Ashwak Alabaichi[3]**

[1]*Department of Computer Science, University of Technology, Baghdad, Iraq*
[2]*Department of Computer Engineering, University of Technology, Baghdad, Iraq*
[3]*Department of Biomedical Engineering, University of Kerbala, Iraq*
* Corresponding author's Email: rawiaaljubori@gmail.com

Abstract: The rapid development of IOT and the ease of capturing and transmitting digital images have increased the demand for image encryption. Despite the availability of various encryption methods, chaos-based image encryption is the most suitable method for image applications due to its sensitivity to initial conditions and control parameters. Many image encryption schemes have been developed to enhance the security of images by using chaotic maps, but they cannot combat all possible threats from the cryptanalysis community. This study presents a new chaos-based substitution box (S-box) and its application for securing images. The construction of the presented S-box approach is based on a new five-dimensional hyper-chaotic system, and the experimental results prove that the suggested S-box approach has high nonlinearity and good cryptographic characteristics. In addition, we utilize the effectiveness of the presented S-box approach in designing a novel lightweight image encryption/decryption scheme. Results demonstrate that this scheme has a sufficient peak signal-to-noise ratio, a low correlation, and a large key space. These factors make it more efficient than its classical counterpart and allow it to resist statistical and differential attacks. The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) values were 99.623 and 33.532, respectively. The entropy oscillates from 7.9965 to 7.9971 for the tested encrypted images. These criteria indicate an efficient, fast, and robust scheme that can be used for secure image transmission via public channels.

Keywords: Chaos, Lightweight, S-box, Image encryption, Diffusion.

1. Introduction

The IOT enables multimedia data exchange across various applications, including smart buildings, smart transportation, smart health, etc. [1]. With the Internet of Things, all the data collected is transmitted over the Internet [2], bringing various security risks into this background, especially image data and video [3]. Data encryption methods are the first remedy that comes to mind for data protection. A cryptographic algorithm designed for a device with low resources (IOT) will have different design criteria than the one commonly used. Modern cryptography has evolved from this particular area into lightweight cryptography [2]. Cyber-physical systems' low energy, compute, and memory capacities should be compatible with lightweight cryptography. Additionally, it must provide optimum security, cost, and performance trade-offs [4]. On the other hand, the conventional methods of image encryption could not satisfy the requirements of good digital image encryption because of the inherent characteristics of digital images, such as bulk data capacity, high redundancy, and robust correlation [5]. The chaotic system exhibits various features such as initial conditions sensitivity, pseudo-randomness, non-periodicity, great entropy, complexity, etc. Therefore, they have been widely employed in image encryption, S-box design, hash functions, and steganography algorithms [6]. There are two classes of chaotic maps: one-dimensional (1D) and high-dimensional hyper-chaotic systems. Researchers have discovered that many 1D chaotic maps have inherent limitations [7] such as low complexity, limited system parameters, and a fair *Lyapunov* value [8] that make them unsuitable for developing a robust security system [7]. Therefore, using the

hyper-chaotic system to encrypt digital images is becoming a popular research direction[9]. These systems perform better than the low ones in terms of nonlinearity, randomness, unpredictability, and have a big keyspace [10].

S-boxes play a crucial role in determining the effectiveness of block cryptosystems [11]. Their utilization in image encryption enhances security by introducing confusion, as S-boxes ensure this crucial aspect [12]. The strength of S-boxes directly impacts block cipher security [11]. Literature reports several S-box generation studies using chaotic systems. In [13], *F. Özkaynak et al.* proposed an S-box design based on a 3D continuous-time Lorenz system as the chaotic system. In [14], *M. Khan et al.* proposes the use of a nonlinear functional chaos-based substitution process that employs a 3D continuous time Lorenz system. The method of *M. Khan et al.* [15] explored multiple systems (6D), namely 3D Lorenz and Rössler chaotic systems, to randomly generate all possible elements of an 8× 8 S-box. In [16], Q. Lu et al. a new algorithm for constructing S-Boxes based on a new compound chaotic system (tent–logistic system) is presented. In [17], *G. Hanchinamani et al.* proposed a method that employs a 4D chaotic map by mixing two 1D Logistic maps and a 2D Henon map. The mixed chaotic sequence is used to generate an S-box. In [18], *H. Nasry et al*. suggested an S-box image cryptosystem based on a 3D Lorenz and a 2D Henon map. However, existing S-boxes generation based on (discrete or continuous) chaotic methods does not lead to good nonlinearity and other performance parameters.

Sensitive and important images require secure transmission. Here's a concise literature review based on S-box and chaotic maps: In [9], *Mengmeng et al.* proposed a digital image encryption algorithm based on dynamic deoxyribonucleic acid coding and hyper digital chaos in the frequency domain. However, this method not suitable for IOT devices. In [19], *Ying et al.* proposed an image encryption based on S-boxes, and a fractional-order logistic map was proposed. In [20], *Hui et al.* suggested a lightweight image encryption scheme based on a message-passing algorithm with a chaotic external message and S-box. However, this method required high processing time. In [21] *Bedir et al.* suggested a technique for image encryption based on combining several chaotic maps to create more durable chaotic maps (5D) to maximize the security and privacy required by using changeable keys. In [22] *Jannatul et al.* proposed a chaotic-based lightweight image encryption method using Arnold and logistic maps to generate new (4D) chaos maps. In [23] *Yousef et al.* presents a lightweight, secure, and efficient image encryption algorithm based on logistic map, permutations, and AES S-box. In [3], *Wang et al.* introduced image encryption scheme based on S-box and cascaded chaos model that combines 2D and 1D chaos mappings to generate new chaos maps. In [24], *A. Ullah et al.* introduced presented a lightweight image encryption scheme using multiple chaotic maps (4D) to generate random keys.

However, It is important to design a cryptographically strong S-box to design secure systems; most of the suggested techniques have sluggish encryption speeds or compromise encryption security for speed. This study enhances the nonlinearity of the new S-box by employing a proposed 5D hyper-chaotic system. By integrating the Hénon and Lorenz systems into a cascaded model, the parameter count of the system increases, leading to improved complexity and larger key spaces. The main contributions of this paper are as follows:

- Present a new lightweight colour image encryption and decryption based on chaotic systems. Therefore, a new high-dimensional hyper-chaotic system is proposed in this paper which is found to have rich dynamics.
- The new 5D hyper-chaotic system is explored to generate an initial 8 × 8 S-box, which is evaluated and compared with current methods.
- Propose a new IP permutation.
- Evaluating the proposed algorithm with many metrics.

This paper is organized as follows: chaos theory; designing a chaotic hybrid system; performance of the proposed S-Box algorithm; the proposed S-box algorithm and its performance; security analyses; and conclusion.

2. Chaos theory

Chaos describes certain dynamical systems' long-term aperiodic behavior, which is highly sensitive to initial conditions. Applying minor input adjustments greatly alters the systems' outputs [26]. Systems based on chaos theory are more secure for image encryption; unauthorized individuals cannot predict the chaos sequence if they are unaware of the proper control parameters and initial values [27].

3. Designing a chaotic hybrid system

This system utilizes two chaotic systems, the Hénon and Lorenz systems, in a cascaded model.

This integration increases the parameter count and key space size, resulting in increased complexity, improved randomness, and heightened uncertainty. The following equations define the system:

$$x_s = \left(x_s + (s \times (\mathrm{y}_s + \mathrm{k}_s))\right)\%1 \quad (1)$$

$$\mathrm{y}_s = \left(\mathrm{y}_s + \left((x_s \times (\mathrm{r} - \mathrm{z}_s + \mathrm{p}_s))\right)\right)\%1 \quad (2)$$

$$\mathrm{z}_s = \left(\mathrm{z}_s + (\mathrm{p}_s \times \mathrm{y}_s - b \times \mathrm{k}_s)\right)\%1 \quad (3)$$

$$\mathrm{k}_s = (1 - (\mathrm{L} \times \mathrm{k}_s \times x_s) + \mathrm{p}_s)\%1 \quad (4)$$

$$\mathrm{p}_s = (\mathrm{M} \times \mathrm{k}_s)\%1 \quad (5)$$

Where s, r, b, L, M are system control parameters. If the parameters are assigned as $s = 0.01, r = 2.8, b = 2.66, L = 1.4, M = 0.3,$ the proposed is chaotic and could produce five sequences. Having a greater number of system parameters results in more diverse output data, as the system parameters directly influence the output. This characteristic significantly enhances the resistance of the encryption technique against brute-force cryptographic attacks. The proposed model is demonstrated to be superior to the Hénon and Lorenz systems through statistical analyses conducted by the national institute of standards and technology (NIST) and the calculation of the Lyapunov exponent.

3.1 Lyapunov exponent

The Lyapunov exponent plays a crucial role in assessing the practicality of a chaotic map for cryptography. It indicates the sensitivity of seed parameters, including initial conditions and control parameters. By utilizing the correlation coefficient, we can determine if a system exhibits chaotic behavior and whether there is any relationship with the original parameters [28]. A Lyapunov exponent can be defined as a number that depicts the dynamic movement of trajectory evolution. The *Lyapunov* exponent's positive value computes sensitive dependence on starting points by displaying the mean at which two closely spaced points diverge over time. Recent research considers many dynamical systems that produce at least one positive *Lyapunov* exponent as chaos. In this work, the hyper-chaotic system has four positive and one negative *Lyapunov* exponent, which is 1.484909, 0.046229, 0.017563, 0.000117, and -1.4044959 as the system maps' order.

Table 1. Results of the NIST

Test Name	p-value	Result
Frequency	0.447884	Success
Block frequency's	0.324625	Success
Runs	0.511745	Success
Longest runs of ones in a block	0.600557	Success
Binary matrix ranks	0.778728	Success
Discrete Fourier transform	0.299755	Success
Non- overlapping templates	0.000413	Success
Overlapping template of all one's	0.060034	Success
Maurer's universal statistical	0.031841	Success
Linear complexity	0. 709060	Success
Serial	0.421822	Success
Approximate Entropy	0.999789	Success
Cumulative sums	0.483072	Success

3.2. Randomness test

The unpredictable nature, or an incomprehensible pattern in a data series, is known as randomness. The *NIST* standard is used to assess how random the results are. Each of the fifteen tests at *NIST* yields a p-value, a real number between zero and one. The statistical test is judged to have been passed if the p-value exceeds a predetermined threshold known as the significance level (equal to0.01) and there is 99% confidence that the generator is random [29]. NIST results are shown in Table 1.

4. Proposed S-box algorithm and its performance

The new S-box generation scheme based on the dynamics of our 5D hyper-chaotic system has been discoursed in Section Three presented. as illustrated in Algorithm 1. Its performance evaluation and compare it with other chaos-based S-boxes. Table 2 lists the generated S-box.

Algorithm 1: S-box construction

Input: initial values map (x_0 , y_0 , z_0, p_0, k_0, n) of proposed hybrid chaotic system and its parameters (b, r, s, u, dt), result array= Null, arr_list array= Null, W, H are width and height of input image

Output: S-Box (16 × 16)

Step 1: $[x_s , y_s , z_s, p_s, k_s] \longleftarrow$ chaotic system (x_0 , y_0 , z_0, p_0, k_0) // to generate random numbers

Step 2: For each value in $x_s , y_s , z_s, p_s, k_s$ that's generated from the proposed 5D hybrid chaotic system

Step 2.1: Get only five digits from the index (3 to 7) and convert it to an integer

Table 2. The S-box1 generated by the proposed algorithm

173	232	65	1	15	78	176	47	242	233	157	120	80	147	84	247
208	67	119	83	214	17	34	183	41	134	50	160	76	40	7	23
25	150	2	253	91	131	11	4	130	149	166	187	102	145	108	146
106	254	124	227	202	236	255	168	29	6	81	164	194	210	70	109
193	231	203	98	237	205	96	212	60	177	93	128	204	105	127	238
213	101	89	59	182	140	46	114	53	77	207	239	43	86	245	220
184	125	56	172	217	219	163	141	45	161	71	87	175	99	116	72
97	243	148	44	178	216	121	12	111	20	252	38	137	209	195	180
240	251	73	170	230	79	200	154	0	152	113	222	174	30	32	235
49	218	223	191	35	215	139	155	159	3	132	179	21	122	169	68
186	57	142	31	64	189	156	62	5	8	61	36	69	110	14	95
33	165	52	10	82	115	129	92	229	117	58	246	190	185	248	42
88	241	27	196	48	197	90	28	135	55	206	112	138	153	226	224
201	133	104	103	54	18	51	188	143	19	250	151	249	126	198	85
75	199	171	100	181	144	107	26	37	66	228	221	167	136	13	9
158	94	24	39	63	192	211	22	225	244	16	118	234	162	123	74

Table 3. Dependency matrix—SAC value

0.500	0.406	0.469	0.500	0.469	0.547	0.453	0.563
0.516	0.453	0.500	0.453	0.484	0.500	0.531	0.516
0.469	0.484	0.516	0.484	0.438	0.469	0.563	0.469
0.531	0.547	0.516	0.594	0.531	0.516	0.469	0.469
0.547	0.469	0.500	0.563	0.453	0.484	0.563	0.547
0.453	0.500	0.531	0.547	0.438	0.484	0.531	0.469
0.516	0.484	0.500	0.406	0.531	0.453	0.516	0.453
0.579	0.469	0.500	0.531	0.422	0.422	0.516	0.469

Table 4. BIC nonlinearity

0	106	98	102	106	108	106	102
106	0	104	100	104	106	102	106
98	104	0	104	106	102	104	106
102	100	104	0	102	106	104	94
106	104	106	102	0	104	100	104
108	106	102	106	104	0	104	106
106	102	104	104	100	104	0	100
102	106	106	94	104	106	100	0

Step 2.2: Mod 256 to generate values between 0-255 and save the result in x_s , y_s , z_s, p_s, k_s
Step 3: Generate an S-box based on the value of x_s values from the chaotic system as follows and based on the size of the input image (W, H)
Step 3.1: for i= 1 to 62500
m= x_s [i] mod 256 to generate values between 0-255 $arr\_list \longleftarrow$ convert (m) to the integer
Step 3.2: For each element (m) in arr_list
Step 3.3: If (m) is not found in the Result array
Step 3.4: Append (m) in the Result array
Step 3.5: S-box= Result array
Step 4: Generate a new matrix (V) is 16 × 16 based on the values of y_s and z_s Form chaotic system
Step 4.1:Permutation rows for (S-box) based on (V) matrix
Step 5: Generate a new matrix (W) is 16 × 16 based on the value of k_s the chaotic system
Step 5.1:Permutation columns for (S-box) based on (W) matrix
Step 6: Get the final S-box

4.1. Performance analysis of proposed S-box

In this section, the performance tests of the generated S-box are performed and compared with the studies in the literature in Table 5. These assessments include the following:
a) Bijectivity : The proposed S-box has different output values from the interval [0,255] with no repetition. Therefore, S-box satisfies the bijectivity property.

Table 5. Performance comparison of high dimensional /hyper-chaotic S-box adopted for 8×8

References	SAC ($ave.$)	NL ($ave.$)	BIC-NL ($ave.$)
[13]	0.5048	103.2	104
[14]	0.4930	105	100.357
[15,32]	0.4978	103	104.07
[16]	4.990	104	103.8
[17]	0.4975	103.2	-
Proposed S-box	0.4993	104	104.429

b) Balanced: to achieve the principle of balance as the number of ones is a near-equal number of Zeros [18]; therefore, the proposed S-box is balanced.

c) Avalanche Effect: If half of the output bits are changed by changing a single input bit, this is the avalanche effect [30]. The avalanche effect of the proposed S-box is 0.5.

d) Strict avalanche criterion (SAC): The boolean function is said to satisfy SAC if a change in an input bit causes a change in half of the boolean function's output bits [31]. The SAC of an S-box is checked by employing a dependency matrix in Table 3, and the *average* value is 0.4956, which is close to the ideal value of 0.5. Therefore, the proposed S-box meets the strict avalanche criteria.

e) Bit independence criterion *(BIC):* This is a very important property of the security of cryptographic systems. It becomes more difficult to attack the cryptosystem as the independence between bits increases [12]. The $BIC(f)$ takes the values between [0, 1]; in the worst situation, it equals zero [31]. Table 4 shows the BIC nonlinearity criterion of the generated S-box.

i) Nonlinearity: is defined for functions; the function's nonlinearity should be sufficiently large to withstand linear cryptographic assaults [15]. The nonlinearity results of the generated S-box are listed in Table 5, SAC, and BIC.

j) Fixed and opposite fixed points: S-box fixed points are often undesirable since they indicate that the output and input are equal. The suggested S-box's fixed points tested out as one, whereas the opposing fixed points tested as zero. As seen, the suggested S-box has extremely few fixed points. Analyzing the fixed points of the suggested S-boxes makes it hard to attack the cryptosystem.

In Table 5, our S-box technique outperformed state-of-the-art S-boxes except [14]. It showed high nonlinearity (score: 104) and strong resistance against linear cryptanalysis and related attacks, It also achieved the highest BIC-NL criterion score (104.429) and met the SAC criterion, with a remarkable nonlinearity score of 0.4993, second only to [13].

5. Proposed image encryption algorithm

The primary objective of this suggestion is to design a secure, lightweight, and fast symmetric encryption scheme with a block size equal to 256 bits and a key size equal to 128 bits for image encryption. The proposed algorithm is a mixture of the Feistel and SPN structures. This scheme depends on a proposed hybrid chaos system in designing all its needed tools, such as S-Box, keys, and a table of permutations (IP). The different encryption keys are used to change the pixel value for all components of the color image, where (x_s , y_s , z_s, p_s, k_s) keys are generated from a hybrid chaotic system in a buffer of equal size. In the proposed image encryption algorithm, as illustrated in Fig. 1, the color image is separated into three channels: red, green, and blue. After that, each channel will be processed as follows:

1- We are generating hash-padding by sha-512 from channel R and $XORed$ each channel with Generating hash-padding.

2- Generate an array of keys (x_s , y_s , z_s, p_s, k_s) using the proposed algorithm by the image size (M x H) and then preliminary treating the numbers generated by taking only a fraction of each number.

3- For each byte of the red channel (R-CH), it takes an XORed with each value of the fraction of the x_s array.

4- As well as taking the values of the green channel (G-CH) and making XORed them with values of y_s .

5- Also, the blue channel(B-CH), implement XOR between the value of (B-CH) and z_s an array of chaotic keys.

6- Applying the proposed S-box (16*16) to each of the data in the resulting three channels (after $XORed$ operation) to add the confusion effect.

7- The result from (step 5) is three new channels are R-CH, G-CH, *and* B-CH. Then, concatenate the G-CH with the B-CH in channel GB (CH-GB).

8- Generate the proposed IP-based proposed chaotic system with the size of a CH-GB channel.

9- The IP is used to permutation the CH-GB array by replacement of pixel positions to their new positions based on the proposed IP array. Thus, all pixel positions in a CH-GB are changed with permutation, and as a result, the strong correlations between all adjacent pixels having relative values are effectively broken.

10- The rotating process has been applied to increase the diffusion effect of the CH-GB. The result is put in the encrypted-GB. Also, rotate the position values by 180 degrees to the CH-R. All rotation processes are based on values of the first row in the IP array.

11- the rotated version of R-CH is concatenated with

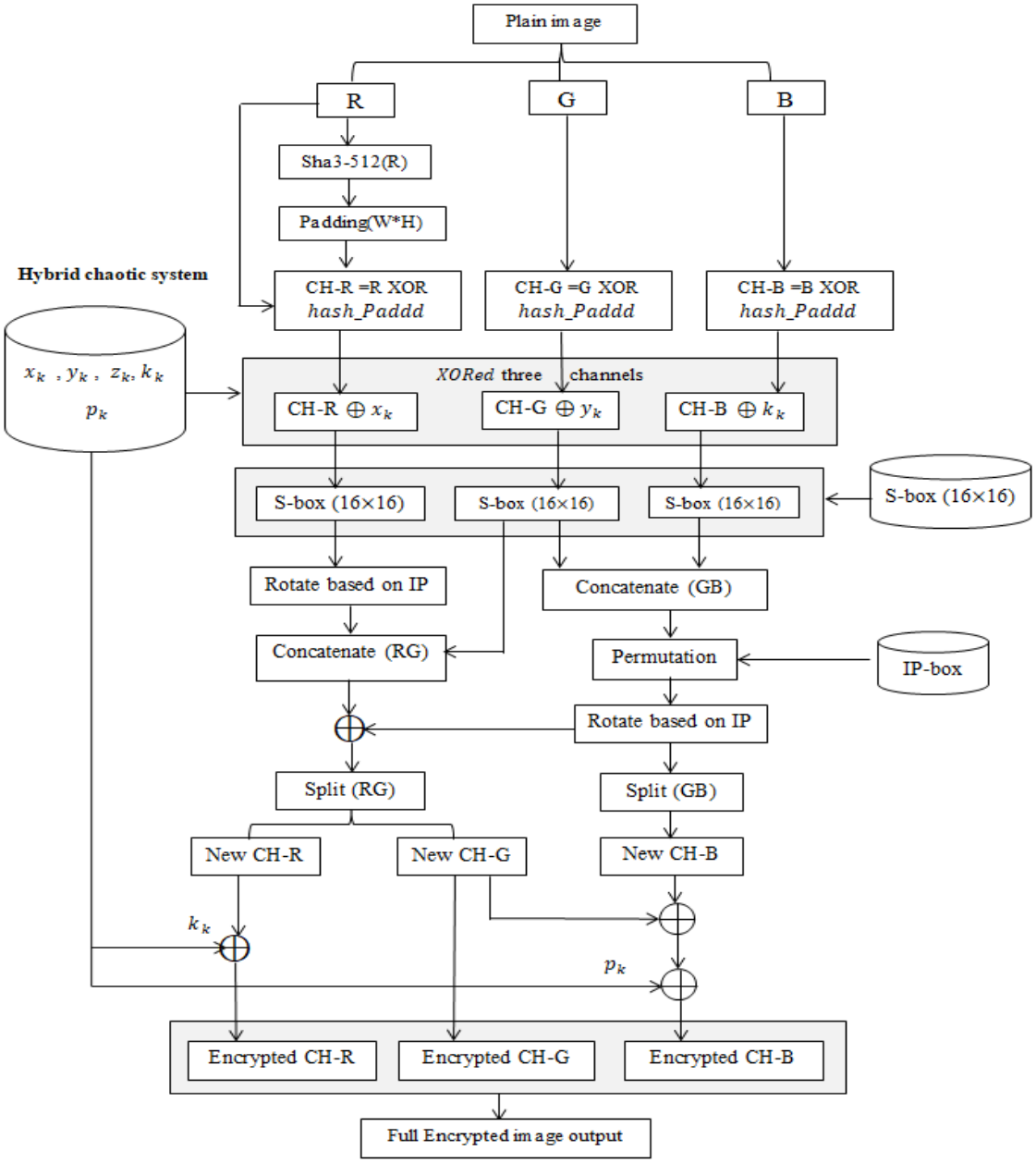


Figure. 1 Flow chart for the proposed algorithm

G-CH, namely RG-CH channel, and then this new RG-CH is applied XOR with rotated-GB-CH. The result $XORed$ operation is put in encrypted-RG.

12- The next step is splitting the encrypted-RG into new CH-R and new CH-G (where new CH-G is saved into Encrypted CH-G) and performing the following:

- A new CH-R $XORed$ with k_s A key and the result are put in the Encrypted CH-R.
- Split the encrypted-GB into new CH-G and new CH-B, then, $XORed$ new CH-B with new CH-G resulting from splitting the encrypted-RG.
- The result from the previous step $XORed$ with the key (p_s) and the output puts into Encrypted CH-B.
- After that, construct an image using three channels (Encrypted CH-R, Encrypted CH-G, and Encrypted CH-B).
- Finally, get the cipher unclear image.

5.1 Decryption process

The opposite of the encryption process is the decryption process. The receivers decipher the cipher image using the secret keys using the encryption algorithm′s reverse operations. Also, hashed R

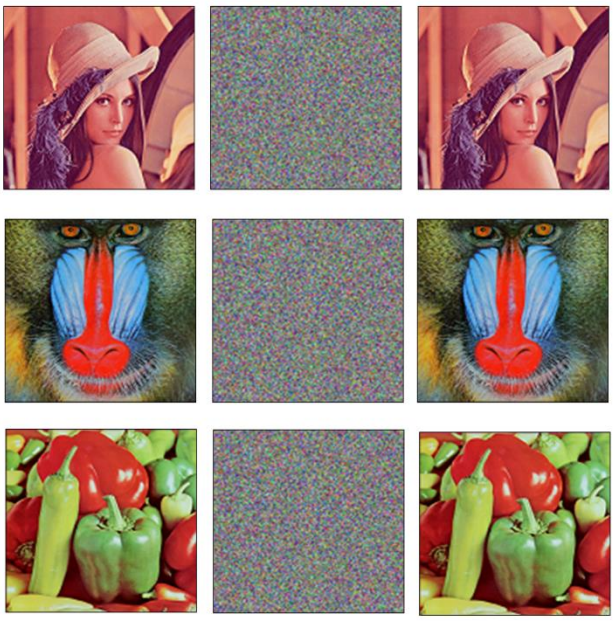
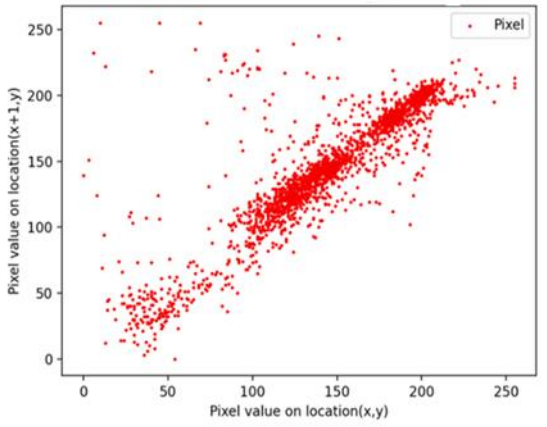
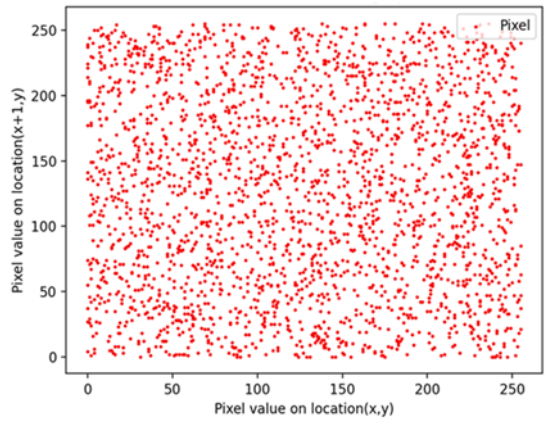


Figure. 2 The left column is plain images; the Middle column is encrypted images, and the Right column is decrypted images



(a)



(b)

Figure. 3 (a) is correlation plots of the Lena plain image, and (b) is correlation plots of the Lena encrypted image

channels received from the encryption side have been used.

6. Security analysis

The experiment was conducted on a personal computer with an Intel Core i7, 2.70 GHz CPU, 12 GB RAM, Windows 10, and Python 3.7.4. The test images (Lena, Baboon, Barbara, Airplane, Goldhill, and Pepper) have dimensions of 256×256 with 24-bit color. Fig. 2 shows that some of the cipher images are noise-like, which makes it impossible to infer anything valuable from them. The security analysis includes the following:

6.1 Correlation coefficient

Correlation in image processing refers to the similarity between two images. It can also be analyzed by examining the correlation between neighboring pixels through random pairings. For the best encryption process, there must be a low correlation. Eq. (6) represents the correlation mathematically[36]:

$$r = \frac{Covariance(x,y)}{S_x \times S_y} \tag{6}$$

where S_x and S_y Are standard deviation at pixel positions x and y.

From Table 6, the correlation average in the horizontal direction of the six images is close to zero, i.e. no correlation seems in the neighbor pixels in the six encrypted images, this indicating increased robustness.

6.2 Information entropy

The most significant indicator for measuring randomness is information entropy. To calculate the information entropy, we can use the following equation: [37]:

$$H(s) = -\sum_{i=0}^{n-1} p(s_i) \log_2 p(s_i) \tag{7}$$

where $\boldsymbol{s}$ is the source of information, $\boldsymbol{n}$ is the bit value required for the symbol $\boldsymbol{s_i}$, and $\boldsymbol{p(s_i)}$ denotes the probability of the symbol $\boldsymbol{s_i}$. For increased security, the information entropy of a ciphered image should be close to eight. Table 6 displays the average information entropy for the tested images, and it is found to be close to eight. This observation suggests that the proposed scheme exhibits high-security characteristics.

Table 6. Entropy and correlation average of the proposed encryption algorithm

Image Test	Correlation	Entropy
Plain images	0.9355	7.3794
Encrypted images	0.00123	7.9971

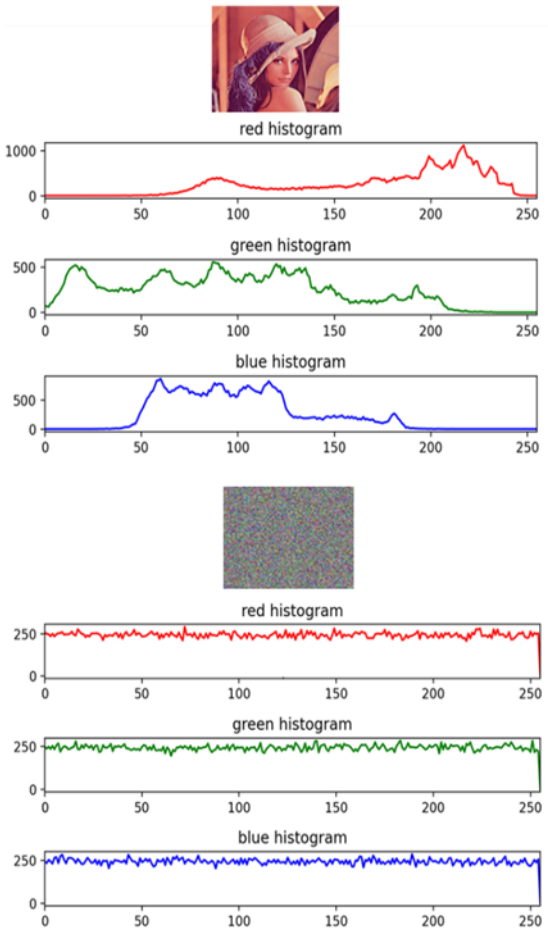


Figure. 4 Histogram of plain and encrypted Lena image

6.3 Histogram analysis

The histogram visually represents the statistical features of an image's pixel intensity distribution. A safe encryption system will ensure the encrypted image has a consistent histogram, making it resistant to statistical attacks [12]. Fig. 4 displays the histogram of the plain and encrypted Lena image. It illustrates that the color values of the encrypted images are well-distributed.

6.4 Differential analysis

A strong encryption technique must guarantee that even a minor change to the plain image will result in a noticeable difference in the ciphered images to protect against a differential attack. The proposed encryption scheme can make two ciphered images different completely, even if their plain images have only one different pixel. By applying eqs. 8 and 9, we can determine the actual value of the sensitivity to a small change in the plain image by comparing the ciphered images C_1 and C_2 [38].

$$\text{NPCR} = \sum_{i=1}^{N}\sum_{j=1}^{M}\left[\frac{D(i,j)}{M\times N}\right]\times 100\% \quad (8)$$

$$\text{UACI} = \sum_{i=1}^{N}\sum_{j=1}^{M}\left[\frac{abs\, C_1(i,j)-C_2(i,j)}{255\times M\times N}\right]\times 100\% \quad (9)$$

where $D(i,j) = 0$ if $C_1(i,j) = C_2(i,j)$. Otherwise, $D(i,j) = 1$. Without loss of generality, choose the Lena, Baboon and Pepper images as the test images and calculate the values of NPCR and UACI. The results of NPCR and UACI are listed in Table 7. As observed, the proposed algorithm obtains the mean (for six tested images) NPCR and UACI are 99.623%, 33.532% respectively. Therefore, the proposed encryption scheme is strong robustness against differential attack.

6.5 Encryption quality

When evaluating the effectiveness of an image encryption technology, encryption quality is a key consideration. Several tests are run on the plaintext and cipher images to gauge the effectiveness of encryption, including mean square error (MSE), peak signal-to-noise ratio ($PSNR$), maximum deviation (MD), and irregular deviation (ID) [17]. Below, a thorough discussion of these tests and their outcomes is provided.

6.5.1. Mean square error and peak signal-to-noise ratio

MSE is used to measure the average squared difference between the pixel values of plaintext and encrypting images. The $PSNR$ quantified the difference in peak error between plain and encrypted images. Plain and cipher images should have low PSNRs due to their large differences[17]. MSE and $PSNR$ outcomes are, respectively, 10134.48 and 0.00537. The suggested approach for image encryption works as intended.

6.5.2. Maximum deviation

It calculates the difference between ciphered and plain images, as shown in Table 8. When calculating MD, a larger number means a higher deviation. The MD is calculated by the following equation:

$$MD = \frac{HD_0+HD_{N-1}}{2} + \sum_{i=1}^{N-2} HD_i \quad (10)$$

where HD_i Is the difference histogram at index i

Table 7. Comparison of the NPSR, UACI, and Entropy scores of encryption algorithms

Test image		Ref. [9]	Ref. [16]	Ref. [18]	Ref. [19]	Ref. [20]	Ref. [21]	Ref. [22]	Ref. [24]	Proposed scheme
Lena	UACI	33.613	-	-	0.208	33.456	33.06	20.75	-	33.637
Baboo		33.207	-	-	0.238	-	33.08	23.77	-	33.657
Pepper		-	33.38	32.747	-	33.479	-	-	33.383	33.359
Lena	NPSR	99.639	-	98.7	99.37	99.609	99.46	99.37	-	100
Baboo		99.673	-	-	99.49	-	100	99.49	-	99.610
Pepper		-	99.613	-	-	99.609	-	-	99.613	99.362
Lena	Entropy	7.9923	-	7.9973	7.4077	7.9967	7.71	7.41	-	7.9972
Baboo		7.9925	-	-	7.9434	-	7.853	7.94	-	7.9972
Pepper		-	7.999	43.646	-	7.9963	-	-	7.999	7.9967

Table 8. Comparison of the MD and ID scores of encryption algorithms

Test image	Ref.[23]	Ref.[24]	Proposed scheme
MD	1.7×10^2	2.2×10^2	4.9×10^4
ID	9.1×10	-	2.1×10^4

Table 9. GLCM analysis

Test image	Energy	Contrast	Homogeneity
Lena	0.0127	9.406	0.098
Baboon	0.009	7.141	0.052
Barbara	0.009	9.623	0.079
Pepper	0.012	9.116	0.104
Airplane	0.031	5.819	0.198
Goldhill	0.012	4.439	0.116

6.5.3. Irregular deviation

Irregular deviation (ID) reveals the degree of irregularity in the deviation that the encryption technique caused in the cipher image. A lower value of ID represents good encryption quality [36,37].

6.6. Gray-level co-occurrence matrix analysis (GLCM)

GLCMis a statistical study of texture measurement that depicts the spatial characteristics of image pixels. It provides valuable information about various aspects such as contrast, energy, and homogeneity [18]. The energy analysis quantifies the information of ciphered image and reflects the disorder degree of ciphered image. The lower energy value of ciphered image indicates the higher encryption quality. The energy value is calculated by eq. (11) [19].

$$E = \sum_{i,j}(i,j)^2 \tag{11}$$

where p(i, j) is given as the number of GLCM. The energy values of the cipher images are shown in Table 9, which shows that the energy values are minimal; this indicates higher randomness in image pixels. The contrast calculates the intensity difference between pixels and their adjacent pixels in a complete image [12]. The superiority of the suggested method is evidenced by the high contrast value, which can be calculated using the following equation [22]:

$$C = \sum_{i,j}|i-j|^2 \times p(i,j) \tag{12}$$

where $p(i,j)$ is given as the number of $GLCM$, The homogeneity analysis can measure the closeness of $GLCM$ elements in this proposal.

The homogeneity values should be lower the stronger the encryption technique. Eq. (13) to calculate the homogeneity [17]:

$$H_n = \sum_{i,j}\frac{p(i,j)}{1+|i-j|} \tag{13}$$

where $p(i,j)$ denotes the $GLCM's$ grey-level co-occurrence matrices. Table 9, also displays contrast and homogeneity values of the ciphered images given by the proposed encryption scheme. Table 10 compares encryption algorithms' Energy, Contrast, and homogeneity scores**.**

As shown in Table 10, the energy values are closer to zero and the contrast values are much smaller in the proposed scheme than in schemes [10]. Therefore, the proposed encryption scheme has high security.

6.7 Keyspace analysis

The strength of an encryption technique lies in secret key parameters. As a result, the key is a cryptosystem's most crucial component. A reduced keyspace might result in the key, or a portion of the key, being exposed. A wider keyspace in digital picture encryption denotes resistance to brute-force assault [36]. Due to the use of two chaotic maps and

Table 10. Security comparison

Test image		Ref. [10]	Ref. [19]	Ref. [23]	Proposed scheme
Lena	Energy	-	0.016	-	0.027
Baboon		0.016	-	0.0164	0.009
Pepper		0.016	-	0.0163	0.012
Lena	Contrast	-	10.460	-	9.406
Baboon		10.486	-	10.515	7.141
Pepper		10.484	-	10.489	9.116
Lena	Homogeneity	-	-	-	0.098
Baboon		0.389	-	-	0.052
Pepper		0.387	-	-	0.104

Table 11. Time comparison

Time (Mbit/s)	Ref.[20]	Ref.[22]	Proposed scheme
Encryption	-	4.75	2.33
Decryption	-	3.73	3.6
Total time	18.21	8.48	5.93

a total of ten initial conditions and parameters in this study, the key space is $(10^5)^{10} \approx 2^{150} > 2^{128}$. The keyspace analysis demonstrates that the suggested technique provides enough key space, and as a result, it is resistant to numerous exhaustive key search assaults and brute force attacks.

6.8. Time and space cost

The main evaluation criterion is the amount of time and space the cryptographic strategy takes to encrypt and decrypt any image. The encryption and decryption processes are simulated for 256 ×256 images seven times, and get the total time for encryption is 2.33 s ± 70.6 ms per loop (mean ± std. dev. of 7 runs, one loop each). The total time for decryption is 3.6 s ± 76.8 ms per loop (mean ± std. dev. of 7 runs, one loop each). Regarding space cost, the proposed algorithm needs 46.83 MiB for the encryption process and 18.11 MiB for the decryption process; throughput is 28.1270 Bms. The proposed algorithm performs with high encryption efficiency and is acceptable for IOT applications. Table 11, presents a comparison between our proposed solution and existing lightweight image encryption methods. The results indicate that our approach requires less overall execution time in seconds (s) compared to the current methods.

7. Conclusion

This first phase of the paper presents a new five-dimensional hyper-chaotic system. The analysis of the new 5D system showed that it has a good hyper-chaotic nature, where it has four positive Lyapunov exponents. High-dimensional/hyper-chaotic systems are considered better candidates for image encryption applications. Based on this fact, a cryptographically strong S-box construction method is proposed using the new 5D hyper-chaotic system in the second phase of the paper. The generated S-box was found to have excellent cryptographic security features to diminish the differential and linear assaults. The strong recital of the anticipated S-box makes it qualifiable as a successful nonlinear component candidate for use in block ciphers. Any lightweight block cipher based on the proposed S-box will make it robust and powerful to meet the requirements of IoT devices. Therefore, we presented a lightweight block cipher using the proposed S-boxes and a new 5D hyper-chaotic system.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The first author was responsible for methodology, software, validation, formal analysis, investigation, resources, data curation, writing original draft preparation, writing review and editing, and visualization, while the authors second and third were responsible for supervision and project administration

References

[1] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, “A Review of Security in Internet of Things”, *Wireless Personal Communications*, Vol. 108, No. 1, pp. 325-344, 2019.

[2] H. Dweik and M. Abutaha, “A Survey of Lightweight Image Encryption for IoT”, *Lightweight Cryptographic Techniques and Cybersecurity Approaches, IntechOpen*, 2022, doi: 10.5772/intechopen.104431

[3] J. Zheng and T. Bao, “An Image Encryption Algorithm Using Cascade Chaotic Map and S-Box”, *Entropy*, Vol. 24, No. 12, p. 1827, 2022.

[4] V. Thakor, M. Razzaque, and M. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities”, *IEEE Access*, Vol. 9, Article ID 527643161, pp. 28177-28193, 2021.

[5] S. Zhu, G. Wang, and C. Zhu, “A Secure and Fast Image Encryption Scheme Based on

Double Chaotic S-Boxes", *Entropy*, Vol. 21, No. 790, pp. 1-20, 2019.

[6] R. Mohammed, M. Khodher, and A. Alabaichi, "A Novel Lightweight Image Encryption Scheme", *Computers, Materials & Continua*, Vol. 75, No. 1, 2023.

[7] A. Alhudhaif, M. Ahmad, A. Alkhayyat, N. Tsafack, A. Farhan, and R. Ahmed, "Block Cipher Nonlinear Confusion Components Based on New 5-D Hyperchaotic System", *IEEE Access*, Vol. 9. pp. 87686-87696, 2021.

[8] S. K. Hathal, H. M. Abdulhussein, and R. Ibrahim, "Lyapunov exponent testing for AWGN Generator system", *Communications and Network*, Vol. 6, No. 4, pp. 201-208, 2014.

[9] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding", *IET Image Processing*, Vol. 13, No. 9, pp. 1535-1539, 2019.

[10] A. Neamah, "An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix", *Journal of King Saud University – Computer and Information Sciences*, Vol. 35, No. 3, pp. 238-248, 2023.

[11] M. Ahmad, M. Doja, and M. Beg, "ABC Optimization Based Construction of Strong Substitution-Boxes", *Wireless Personal Communications*, Vol. 101, No. 3, pp. 1715-1729, 2018.

[12] A. E. Latifa, B. A. E. Attya, and S. V. Andraca, "A novel image steganography technique based on quantum substitution boxes", *Optics and Laser Technology*, Vol. 116, pp. 92-102, 2019.

[13] F. Özkaynak and A. Özer, "A method for designing strong S-Boxes based on chaotic Lorenz system", *Physics Letters A*, Vol. 374, No. 36, pp. 3733-3738, 2010.

[14] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems", *Nonlinear Dynamics*, Vol. 70, No. 3, pp. 2303-2311, 2012.

[15] [15] M. Khan, T. Shah, H. Mahmood, and M. Gondal, "An efficient method for the construction of block cipher with multi-chaotic systems," *Nonlinear Dynamics*, Vol. 71, pp. 489-492, 2017.

[16] Q. Lu, C. Zhu, and G. Wang, "A Novel S-Box Design Algorithm Based on a New Compound Chaotic System", *Entropy*, Vol. 21, No. 10, No. 1004, pp. 1-15, 2019.

[17] G. Hanchinamani, D. Narayan, and R. Savakknavar, "Construction of S-Box Based on Parametric Mixing of Chaotic Maps", In: *Proc. of International Conf. On Advances in Electrical, Computing, Communication and Sustainable Technologies*, Bhilai, India, 2021.

[18] H. Nasry, A. Abdallah, A. Farhan, H. Ahmed, and W. Sobky, "Multi Chaotic System to Generate Novel S-Box for Image Encryption", *Journal of Physics Conference Series*, Vol. 2304, No. 2022, pp. 1-11, 2022.

[19] Y. Zhang, J. Hao, and X. Wang, "An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map", *IEEE Access*, Vol. 8, pp. 54175-54188, 2020.

[20] H. Liu, B. Zhao, J. Zou, L. Huang, and Y. Liu, "A Lightweight Image Encryption Algorithm Based on Message Passing and Chaotic Map", *Security and Communication Networks*, Vol. 2020, Article ID 7151836, pp. 1–12, 2020.

[21] A. Yousif, F. Khalifa, and A. Makram, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps", *AIP Advances*, Vol. 10, No. 7, pp. 1-9, 2020.

[22] J. Ferdush, M. Begum, and M. Uddin, "Chaotic Lightweight Cryptosystem for Image Encryption", *Advances in Multimedia*, Vol. 2021, Article ID 5527295, pp. 1-16, 2021.

[23] Y. Alghamdi, M. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution", *Entropy*, Vol. 24, No. 10, No. 1344, pp. 1-25, 2022.

[24] A. Ullah, A. Shah, J. Khan, M. Sajjad, W. Boulila, A. Akgul, J. Masood, F. Ghaleb, S. Shah, and J. Ahmad, "An Efficient Lightweight Image Encryption Scheme Using Multichaos", *Security and Communication Networks*, Vol. 2022, Article ID 5680357, pp. 1-16, 2022.

[25] K. Zamli, A. Kader, F. Din, and H. Alhadawi, "Selective chaotic maps Tiki-Taka algorithm for the S-box generation and optimization", *Neural Computing and Applications*, Vol. 33, No. 23, pp. 16641-16658, 2021.

[26] A. Arab, M. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm", *Journal of Supercomputing*, Vol. 75, No. 10, pp. 6663-6682, 2019.

[27] R. Naik and U. Singh, "A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption", *Annals of Data Science*, ID: 246034034, pp. 1-27, 2022.

[28] A. Soleymani, M. Nordin, and E. Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map", *Scientific World Journal*, Vol. 2014, Article ID 536930, pp. 1-21, 2014.

[29] I. Hussain and T. Shah, "Literature survey on nonlinear components and chaotic nonlinear components of block ciphers", *Nonlinear. Dyn.*, Vol. 74, pp. 869-904, 2013.

[30] W. Sobky, A. Mahmoud, A. Mohra, and T. E. Garf, "Enhancing Hierocrypt-3 Performance by Modifying Its S- Box and Modes of Operations", *Journal of Communications*, Vol. 15, No. 12, pp. 905-912, 2020.

[31] F. Ishfaq, "A MATLAB Tool for the Analysis of Cryptographic Properties of S-boxes", *Faculty of Computing Department of Mathematics, M.S. thesis, Capital University of Science and Technology*, Islamabad, Pakistan, 2018.

[32] E. A. Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes", *Entropy*, Vol. 20, No. 525, pp. 1-17, 2018.

[33] Y. Ghadi, S. Alsuhibany, J. Ahmad, H. Kumar, W. Boulila, M. Alsaedi, K. Khan, and S. Bhatti, "Multi-Chaos-Based Lightweight Image Encryption-Compression for Secure Occupancy Monitoring", *Journal of Healthcare Engineering*, Vol. 2022, Article ID 7745132, pp. 1-14, 2022.

[34] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-Chaos", *IEEE Access*, Vol. 7, pp. 78367-78378, 2019.

[35] M. Ahmad, M. Doja, and M. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system", *Journal of King Saud University–Computer and Information Sciences*, Vol. 33, No.1, pp. 77–85, 2021.

[36] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption", *Multidimensional Systems and Signal Processing*, Vol. 30, No. 4, pp. 943-961, 2019.

[37] F. E. Samie, H. Ahmed, I. Elashry, M. Shahieen, O. Faragallah, E. E. Rabaie, and S. Alshebeili, "Image encryption: A communication perspective", *Taylor & Francis*, pp. 1–391, 2013.