Babylonian Journal of Networking
Vol.2024, **pp**. 148–161
DOI: https://doi.org/10.58496/BJN/2024/015; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Robust Color Image Encryption Using 3D Chaotic Maps and S-Box Algorithms

Jenan Ayad [1,*], Mustafa A Jalil [2]

[1] *Electro-mechanical Engineering dep, University of Technology, Baghdad, Iraq.*

[2] *Andalusian Research Institute in Data Science and Computational Intelligence (DaSCI), University of Cordoba, Campus Universitario de Rabanales, Cordoba, 14071, Spain.*

ARTICLE INFO

Article History

Received 11 May 2024
Accepted 12 Jul 2024
Published 05 Aug 2024

Keywords

S-box
encryption
decryption
chaotic map
PRNG
secure color image transmission

ABSTRACT

Chaos' key qualities, such as initial state sensitivity and unpredictability, make it an ideal contender for cryptography applications. This study presents an encryption scheme for efficient and secure image encryption. The encryption scheme includes two ciphering stages and a substitution stage. In this work, an algorithm for key generation has been proposed. The design of a Pseudo-random number generator that used for key generation is based on chaotic algorithms. The chaotic map will be utilised in encryption systems due to its high security. To evaluate the proposed PRNG randomness, NIST tests are used for these sequences. In the following subsection, security analysis of the proposed image encryption technique has been made to know the efficiency of the proposed technique. The statistical analysis now reaffirms that the technique is secure and efficient for and encrypting simple or complex images, be it in shades of black and white or, colorful. By a comparison with past chaotic investigations, demonstrating that our algorithm is competitive with earlier work.

1. INTRODUCTION

Thus, since the present approach is based on the image processing and the data transmission, the improvement is observable in recent years. Securing important data while transferring it in real-time from one point to another in wired and wireless networks is a requirement that has gained much significance [1]. Technology has risen impacting and changing all fronts through the application of multimedia and objects of visual communication such as the military and medical fields that use data transfer. Earlier methods of encryption that were applied for image encryption have failed to cope with large database images [2]. Therefore, the focus has been placed on advancing image encryption algorithms, with attention being given to algorithms using chaos as the main encryption basis [3, 4].

Chaotic systems and cryptology are closely linked [5,6], as the features of chaotic systems, such as randomness, control sensitivity, ergodicity, and deterministic yet highly unpredictable values, align well with the requirements of encryption [7]. These advantageous characteristics have led to further exploration of chaos-based encryption through additional experiments [8]. Random number sequences play an important part in encryption, and the unpredictability of these produced numbers strongly correlates with encryption strength. To achieve this, PRNG based on chaos have become a common application of chaotic systems in encryption [9]. The S-Box is a vital component in block encryption methods, as it performs confusion to improve encryption security. The design of a robust S-Box structure is crucial, as it must possess high cryptographic features, be resistant to attacks, and withstand differential cryptanalysis to be effective in encryption [10].

*Corresponding author. Email: jinan.a.namuq@uotechnology.edu.iq

2. RELATED WORKS

The complex structures of modern encryption algorithms, which require a great deal of computing power, have a negative impact on the efficiency of image encryption operations. As for the usage of chaotic systems in encryption methods, it is crucial to notice that although these approaches are actively investigated in academia, it has been shown that none of the encryption methods that solely uses chaotic systems can provide satisfactory security.

In reference [11], a chaotic sequence was generated using a sine map. To improve system security, an elliptic curve point and dynamic permutation table were used. The study in [12] reduced the number of iterations of the hyperchaotic system from WH/4 to 2W, a significant reduction for an image with dimensions W×H. A novel post-processing technique for generating a key matrix enabled this improvement. A new approach was presented in [13], offering a low time order, high output complexity, and a simple algorithm using 3D logistic maps. Reference [14] described a new approach of encrypting medical pictures using a 2D Logistic-Gaussian hyperchaotic map. In [15], image encryption was accomplished with the aid of 3D and 4D Arnold Cat maps, and the model incorporated the secure Elliptic Curve. In [16], a unique picture encryption technique using a combination of three modified and augmented chaotic one-dimensional maps was suggested. In [17], an encryption method for 3D models was proposed using a 2D chaotic system constructed by coupling the logistic map with infinite collapse (2D-LAIC) and the semi-tensor product (STP) theory. Reference [18] introduced a bit-level permutation and hyper-chaotic system as the foundation for an encryption scheme, while [19] proposed intra bitplane scrambling for parallel image encryption. In [20], a new four-dimensional and multi-scroll hyperchaotic system was developed. In [21], a visually secure image encryption scheme was proposed by combining the adaptive-threshold sparsification compression sensing model with a novel design memristive chaotic map. In [22], a chaotic oscillator was generated using a second-order differential equation.

Novel suggestions for a key generation were proposed in [23]. The study in [24] described a collection of one-dimensional quadratic chaotic maps based on topological conjugate theory. In [25], a new framework utilising finite precision was introduced for generating chaotic signals to improve image encryption is presented. The encryption process was enhanced using S-BOX, an algorithm based on chaotic processes, which provided a high level of security and efficiency. In [26], the encrypted data consisting of S-Boxes generated from a chaotic logistic map was compressed before encryption. The authors in [27] suggested a 3D chaotic map using highly nonlinear S boxes for encryption, followed by a data concealing strategy based on the Lah transform. A low-dimensional chaotic scheme was employed in [28] to create an S-box with dimensions of 10 by 26. In [29] the efficacy of encryption was increased, and secure transmission was promoted they used a 3D chaotic map-based symmetric technique. In [30], the combination of various chaotic map types with an S-box was hypothesised to achieve a fast method for scrambling and encrypting colour images. In [31], the Henon map was utilized to propose new image cryptosystem key-dependent bijective S-Boxes. In [32], Combining quantum walks with the generation of ciphertexts with visual meaning, a new approach of image encryption has been introduced.

This research seeks to design an efficient and secure image encryption system through simple procedures and a robust strong key. The study proposes method for encrypting images using chaotic maps and S-box algorithm. To enhance the confusion, the presented encryption method uses an S-box appended to the chaotic maps and ensures improved security while maintaining the favourable statistical characteristics of the approach.

The contribution of this work is proposing new method for key generation based on multi-stage 3D chaotic maps.

The remaining parts of this work are structured as described below. Section 2 contains the existing chaotic maps used in this work. In section three, the key generation method and S-box construction are introduced, and also, we will discuss the image encryption algorithms that have been suggested. The results of the experiments and an appraisal of their effectiveness are presented in Section 4. In the end, the conclusions are discussed in the final section.

3. CHAOTIC MAPS

The most famous 3D chaotic system, maps are Logistic and 3D Henon map, has been considered for key generation in the proposed systems. The mathematical models of the chaotic systems used in this study are defined in Table 1.

TABLE I. CHAOTIC MAPS

Chaotic map	Mathematical model	Initial values	Control parameters
3D Cat map 3D CM [33]	$x_{n+1} = (3x_n + y_n + 4z_n) mod\ 1$ $y_{n+1} = (6x_n + 3y_n + 11z_n) mod\ 1$ $z_{n+1} = (6x_n + 2y_n + 9z_n) mod\ 1$	x_0=0.7467 y_0=0.3394 z_0=0.65758	
3D Henon map 3D-HM [30]	$x_{n+1} = a - {y_n}^2 - bz_n$ y_{n+1}=x_n z_{n+1}=y_n	x_0=0.17 y_0=0.45456 z_0=0.9434	a=1.76 b=0.1
3D Sine-Cosine 3D CSM [29]	$x_{n+1} = W^m \sin(x_n) + y_n - H^m \cos(z_n)$ $y_{n+1} = \sin(x_n)\cos(y_n) + x_n + \tan(z_n)$ $z_{n+1} = y_n\, cos(x_n) + B^m x_n \sin(z_n)$	x_0=-0.0005 y_0=0.300001 z_0=-0.38	W=0.66 H=1.33332 B=15.13 m=5
3D Sine map 3D-SCM [35]	$x_{n+1} = \sin\left(a_1 \sin^{-1}\sqrt{x(i-1)}\right)^2$ $y_{n+1} = \sin\left(a_1 \sin^{-1}\sqrt{y(i-1)}\right)^2$ $z_{n+1} = \sin\left(a_1 \sin^{-1}\sqrt{z(i-1)}\right)^2$	$x_0 = \sin(\theta_1 \pi a_1)^2$ $y_0 = \sin(\theta_2 \pi a_2)^2$ $z_0 = \sin(\theta_3 \pi a_3)^2$	θ_1=60, a_1=4 θ_2=70, a_2=3 θ_3=80, a_3=a_1*a_2
3D-FCM [45]	$x_{n+1} = {Lx_n}/{\lvert 1 - y_n \rvert!}$ $y_{n+1} = {My_n}/{\lvert 1 - z_n \rvert!}$ $z_{n+1} = {Nz_n}/{\lvert\lvert 1 - x_n \rvert\rvert!}$	x_0=1.5 y_0=2.756 z_0=3.4	L=6. 5 M=4. 6 N=9. 3

4. THE PROPOSED IMAGE ENCRYPTION SCHEME

In this section, we provide a chaotic method for random number generator and investigate the ensuing chaotic system. After it is determined that the chaotic system has sufficient dynamic features, a random number generator can be developed. In tests administered by the National Institute of Standards and Technology (NIST), random numbers generated using a random number generator are employed. Then S-box is generated to improve the performance of the proposed encryption schemes.

1- Key Generation

The originality of the proposed method is based on an efficient PRBG method for the key. Given the nature of the previous studies, both the level of security and the feasibility of the cryptosystem must be optimized. As for this work, a specific generation methodology is proposed as follows: two forward waves, that is, a 3D chaotic map, and a 3D chaotic map of the feedback part called the Proposal with FeedBack method (P1FB) shown in figure 1. Figure 2 demonstrates a block diagram of 3D-Quantization and Decimal-to-binary converter which is used to convert the output of chaotic map in to 8-bit binary form. The key generation proposal P1FB employed chaotic maps of three types, for the 3D-FCM the first initial value is set to be xf0, yf0, and zf0 while the 3D-CM employs initial value xc0=Xf, yc0=Yf, and zc0=Zf, the output of the former supplies the next map. The output of this stage includes both the feedback streams and ciphering key, where the latter is used for encrypting the color image in a binary format. In this case, the ciphering key as, K_P1_R for the red vector of the image, K_P1_G for the green vector of the image and K_P1_B for the blue vector of the image. The feedback streams become the initial values in the third stage, 3D-HM, with xh0 = Xc, yh0 = Yc, and zh0 = Zc. In the next iteration, the 3D-HM outcomes are internalized to the 3D-FCM with reinforcement of the clustering by setting xf1=Xh, yf1=Yh, and zf1=Zh until all pixels in the image are encrypted.

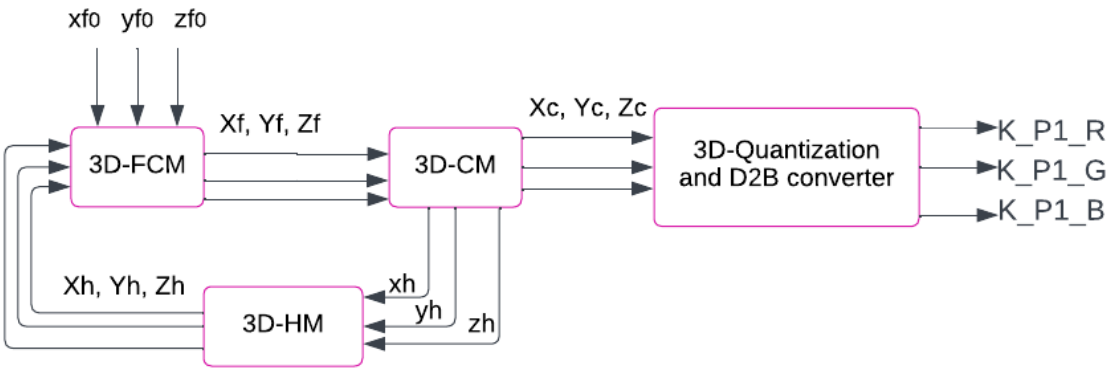


Fig .1. Key generation Proposal, FeedBack method (P1FB)

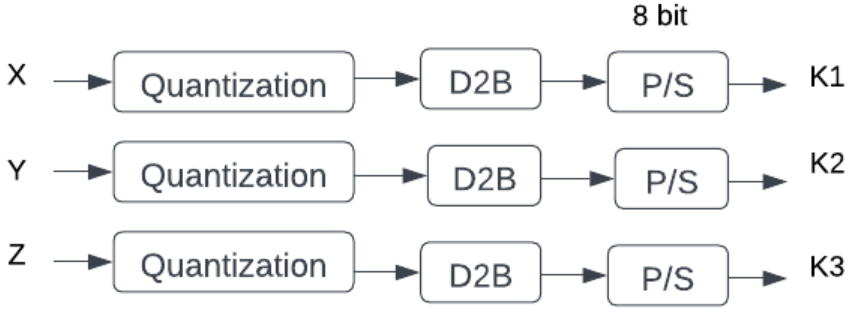


Fig. 2. 3D-Quantization and Decimal-to-binary converter block diagram

NIST is a regularly utilized test suite when evaluating the stochastic performance of a time series [34, 37]. The NIST requires multiple sequences and largely relies on two key performance metrics: P-value and pass rate, to measure the random performance of time series [38]. The pseudo-random properties of the new chaotic signals were demonstrated using NIST testing. The standard procedure was used to assess the randomness of the x, y, and z sequences. The NIST test results for 15 tests are presented in table 2, showing that all values are consistently below 0.01 in each trial. The results of all the tests for randomness suggest that the sequences generated by the key are suitably unpredictable for the purpose of image encryption.

TABLE II. NIST RESULT TEST

	Proposed algorithms
NIST tests	P1 FB
Frequency Test	0.50669
Frequency within a Block Test	0.24187
Runs Test	0.8333
Longest Run of Ones in a Block Test	0.25027
Binary Matrix Rank Test	0.1713
Non overlapping Template Matching Test	0.3691
Overlapping Template Matching Test	0.7237
Universal Statistical “Maurer’s” Test	0.1211
Linear Complexity Test	0.3208
Serial Test	P-value1 : 0.78499 P-value2 : 0.8352
Approximate Entropy Test	0.79556
Cumulative Sums Test	P-value Forward: 0.7402 P-value Reverse: 1
Random Excursions Test	0.2153
Random Excursions Variant Test	0.309

2- The S-Box construction

Substitution-Box is primarily made up of a variety of mathematical procedures. This encryption algorithm takes the plaintext block and a key as the inputs to produce an encrypted block as the output. This is followed by S-box transformations to produce the ciphertext and then multiple rounds of S-box transformations. Decryption is, therefore, done by using the inverse of the S-box transformations in the reverse order using the same key [39].

The operation that is performed on a pixel value p using an S-box matrix s is called a nonlinear transformation and is suggested mathematically using the substitution function sb(s, p). The output of this function provides the transformed ciphertext pixel value. A strategy for creating some reliable S-boxes based on the chaotic maps (3D-CM, 3D-HM, 3D-FCM), and the proposed scheme (P1FB) has been developed. The resulting 3D chaotic sequences are ordered by rising values, and the ordered values' indices are recorded in one-dimensional arrays. It is necessary for the production of the S-box from the preceding sorting phase. The sorted indices are then placed into a 16x16 matrix, with each column representing the identity of the values in the sorted sequence and each row representing an S-box, known as the Sbox_matrix. This transformation applies to each pixel in the provided image, with the pixel's value serving as the index of the S-box. This retrieved value is the new pixel value in the altered picture known as Sbox_Imag depicting the cipher text pixel value.
The building of an S-box comprises three phases:
Step 1: To generate a chaotic sequence, use one of the chaotic maps using the methods described above.
Step 2: Randomise the sequence of indices.
Step 3: Convert the indices to decimal and produce the last S-box with a dimension of 16 × 16.
Algorithm 1 illustrates the precise procedure for constructing an S-box and chaotic sequences.

Algorithm1: Substitution box construction
Input: the chaotic sequences (xi,yi,zi), and m×n image. **Output:** The substituted image Sbox_Imag. 1. Sort the chaotic sequence x by its indices to get [xs]. 2. Generate a 16×16 substitution matrix Sbox_matrix using the index vector from the sorted sequence. 3. For each column $k1$ from 1 to n: 4. For each row $k2$ from 1 to m: 5. Substitute the pixel value in the image by the corresponding index in the substitution matrix and store it in Sbox_Imag.

The S-box (S) must satisfy the following conditions:
It is 16×16 and can hold up to 256 items.
It is also needed that all of the elements of S be integers and fall inside the interval [0, 255], thus S(i, j) [0, 255]. S(i, j) should not have any duplicates, and all entries should be between 0 and 255, so it falls inside the range [0, 255]. The study used a heuristic method to develop S_box using Henon map, Cat map, Factorial map, and the proposed scheme. More specifically, the x sequence was coded with blue vector of the image, the y sequence was coded with red vector of the image and the z sequence was linked with green vector of the image.
To decrypt, define the S-box inverse transform function, sb Inverse(s, q). As previously stated, s is the current state of the stream cypher, and q represents the first q bits of the cypher text block. The second method covers the technique for S-Box Inverse.

Algorithm2: Inverse S-Box
Input: Substituted image Sbox_Imag of size m×n and a 16×16 S-Box matrix. **Output:** m×n image InvSBox_Imag. **1.** For each *i* from 1 to 256: For each *j* from 1 to 256: If the index *x* equals *i*: Assign the value of *j* to the index *y*. **2.** For each column $k1$ from 1 to n: For each row $k2$ from 1 to m: Retrieve the image pixel value from the index and subtract 1, storing it in InvSBox_Imag.

3- Theproposed image encryption scheme

The image encryption scheme involves three stages: two stages of ciphering with the help of chaotic maps using PRNG and one stage of substitution by means of an S-box. The block diagram of entire image encryption scheme is depicted in the Figure 3. Then, the original color image is decomposed into the RGB channels, and then the ciphering process takes place. Following that, a diffusion operation is carried out using three of the S-box techniques for the RGB channels separately. The final data processing operation of ciphering is then done with respect to the RGB channels after the diffusion operation is performed. Last of all the three channels are combined to give the final color ciphertext image. The specific encryption steps are as follows:

Algorithm of Encryption

The following steps are listed in the encryption algorithm:

1- Take the original image I and enter it into the program and find the dimensions to be [m,n]×3=size(I).
2- Split the color plaintext image I to its RGB channels with dimensions M×N. Transform the RGB channel matrices into one dimensional binary streams and these are referred to as; B_R, B_G, B_B.
3- Define the parameters to be used in a chaotic map and obtain three chaotic matrices to form the first stage ciphering key.
4- XOR the obtained vectors in step 2 with the chaotic matrices x, y, z.
5- Transform the obtained ciphered binary vectors into matrices of the dimensions [m,n] for the second encryption stage.
6- It is important to carry out the S-box process as the last diffusion step for permuting the ciphered image on the basis of the index value to reach the second encryption stage image referred as to imagesb.
7- Perform step 2 for the encrypted imagesb obtained from the S-box output of the selected image. Note that for the next ciphering stage, replace the sine logistic map with a logistic chaotic map.
8- Convert the obtained binary vectors into the final encrypted image E_I, which will be in the form of [m,n]×3 decimal matrices.

The decryption algorithm essentially reverses the operations of the encryption algorithm.

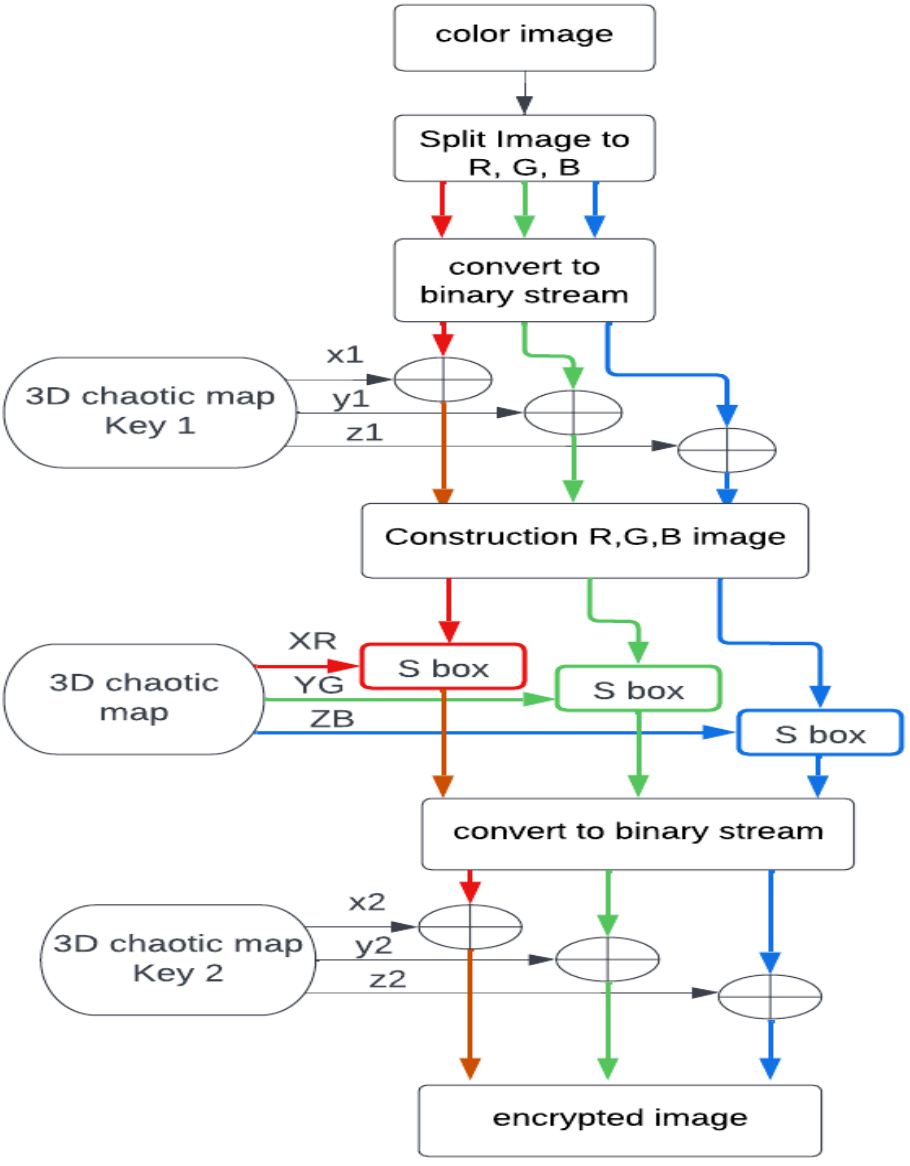


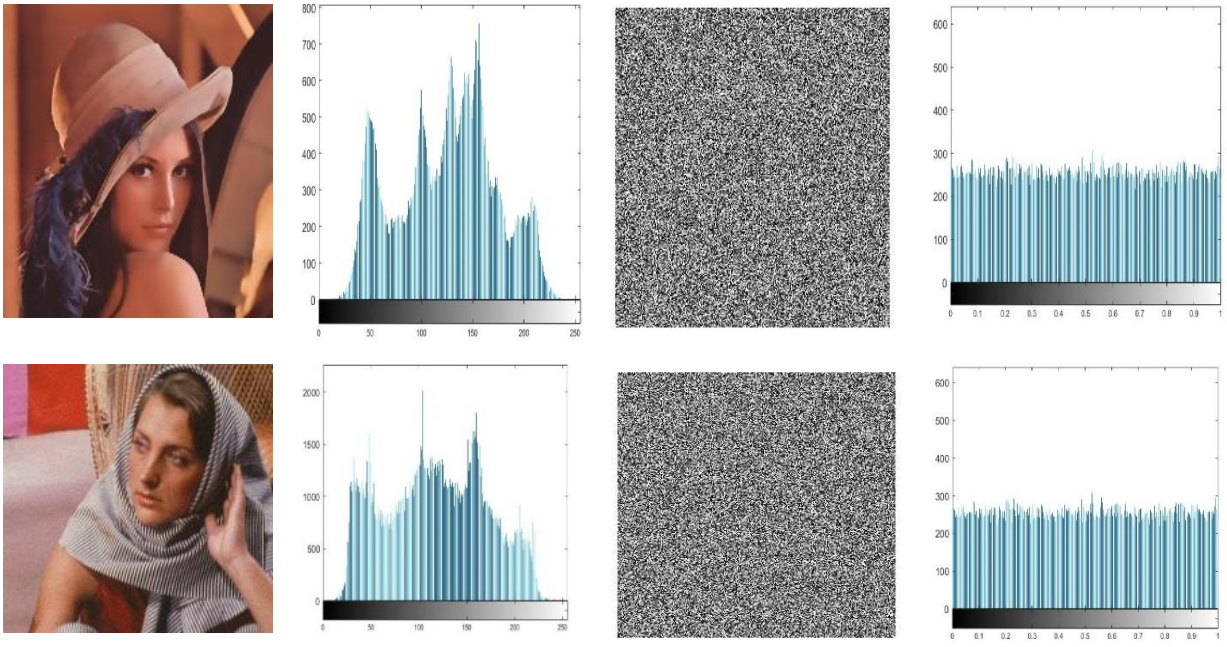
Fig. 3. encryption process

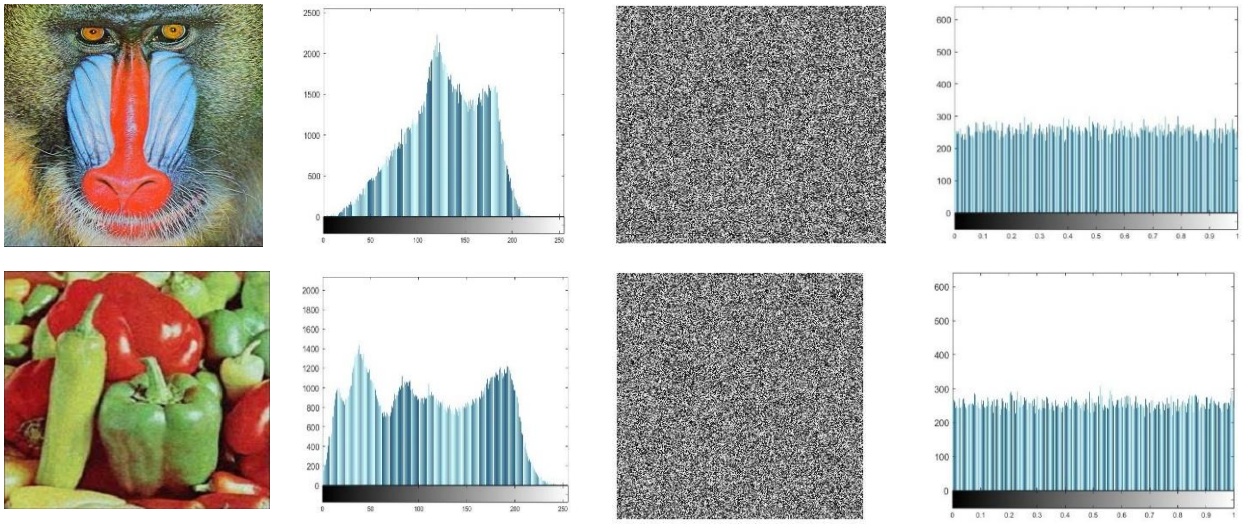
5. EXPERIMENTAL RESULTS

A detailed investigation was done with respect to the results and vulnerability of the suggested algorithms. These were histogram evaluation results, correlation coefficients, information entropy, keysRpace, and resistance against differential attacks. All experiments were very carefully performed and afterwards signal analysis was done with the help of Matlab.
The first requirement for designing a good image encryption technique is that it must counter a number of threats. Some statistical analysis was done, for instance; differential attack analysis (change intensity and change rates where both are average and uniform), key analysis (key-space and key-sensitivity). Besides, correlation coefficients, information entropy, and histograms were as well considered. As in many cases, a particular emphasis is placed on the comparison of the proposed technique with the other approaches to the same problem.
In this study, compound arrangements of chaotic maps were used to create a key for the type of application we used in the study. These arrangements were identified using abbreviations: These are Factorial chaotic map (F), Henon chaotic map (H), Cat chaotic map (C), Proposal algorithm with feedback algorithm (P1), and S-box (S). For instance, H_SP1_F implies that the authors have employed Henon chaotic map for the first key, S-box for the subsequent key based on proposal 1 with selection algorithm inherent to the system besides the generation of the third key through 3DFCM.

1. Analyzing a Histogram

Histograms displays the number of the pixels in an image at a specific shade of gray. This analysis provides cryptanalysts with a lot of information on the image. To avoid even faint traces of the original image, the histogram of the end encrypted image should be uniform which is quite different from the histogram of the original image. The test image along with the histogram of the test image and the encrypted image and its histogram are shown in figure 4 using (P1_SF_H) arrangement for different testing images. This figure shows that the histogram of the encrypted image does not give any useful information. It can be noted that the proposed method adequately hinders the identification of the original content in the given image, as the given scrambled image looks completely different in terms of appearance and has equalized intensity values.





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

Fig . 4. Histograms for 256x256 gray image (a) original version (c) Encrypted version.

2. NPCR and UACI test

The robustness of this method to the differential attacks is established using two of the most common measures. One of these is NPCR, which gives the number of pixels with differences in two images divided by the total number of pixels. Two different encrypted images are described as I_1(a,b) and I_2(a,b) where a varies from 0 to M-1 and b from 0 to N-1. Importantly, each of these images is one-pixel different from its corresponding plaintext image. The NPCR percentage is calculated using the following formula:

$$\text{NPCR} = \frac{\sum_{a=0}^{M-1} \sum_{b=0}^{N-1} D_{a,b}}{M * N} * 100\% \quad (1)$$

where $D_{a.b}$ is a (0, 1) matrix calculated by $I_1(a, b)$ and $I_2(a, b)$. If $I_1(a, b)$=$I_2(a, b)$, then $D_{a.b}$ = 0; otherwise, $D_{a.b}$= 1, and $D_{a.b} \in \mathrm{B}^{M \times N}$.

The other parameter was therefore UACI which essentially measures the mean intensity of differences between two images most especially when the variations between images are negligible and the images consequently are close to plaintext images. The UACI is computed using the following formula:

$$\text{UACI} = \left[\sum_{a=0}^{M-1} \sum_{b=0}^{N-1} \frac{|I_1(a,b) - I_2(a,b)|}{255} \right] * \frac{100\,\%}{M * N} \quad (2)$$

A suitable level of performers for image encryption confidence is the adequate values of UACI that, according to the established calculations should be around 33. Multiple Filter sizes are to be tested using the performance measures of NPCR and UACI, the value 99.604 is the ideal NPCR. [23]. The encryption scheme applied for the encrypted grey images are and the respective UACI and NPCR are mentioned below in Table 3. The methods shown, illustrate NPCR values which are either greater or comparable to the standard values and hence better or equivalent security is established with higher values. The issued NPCR and UACI will accordingly fluctuate depending on the applied format and size of the image. The values calculated by these methods are provided in the table and compared to previous methods using the Lena test image, which is shown in table 4. Comparing the result, it is concluded that the NPCR and UACI of the proposed systems are higher than those of previous research, which means that the procedures have better protection against various attacks and transmission security and efficiency of images in addition to safety.

TABLE III. UACL AND NPCR TESTS

	Lena		Barbara		Camera man		Babon		Pepper	
	NPCR	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**
H_sh_F	99.6414	33.4513	99. 6323	33.5219	99.6185	33.4256	99.6094	33.4999	99.5819	33.6261
F__Sh_C	99.649	33.726	99.626	33.379	99.620	33.424	99.5499	33.5676	99.6002	33.4364
H_SP1_F	99.6536	33.3930	99.6017	33.3408	99.6231	33.4074	99.6201	33.3287	99.5987	33.5013
F_SH_P1	99.5804	33.4704	99.6643	33.2293	99.5575	33.3834	99.5743	33.4345	99.6353	33.3719

TABLE IV. COMPARISON FOR UACL AND NPCR TESTS WITH PREVIOUS WORKS FOR LENA IMAGE.

Ref. no.	[21]	[29]	[36]	[37]	[16]	[25]	[15]	[38]	[39]	[40]	[41]	[41]	[13]
NPCR	99.60	99.6	99.622	99.61	99.6078	99.6185	99.6	99.61	99.61	99.6	99.606	99.617	99.6032
UACI	99.60	33.47	32.654	33.55	33.4599	33.4671	33.42	33.34	33.46	33.47	33.4689	33.4749	33.5986

1. Entropy

in the case of statistical tests, information entropy is one of the parameters, which assesses the degree of image's randomness. In a grayscale image with size of 256 by 256, the total no of shades would be 256 I/p levels. If the probability at each level is considered to be the same then the entropy value is 8 bits. The mathematical expression for entropy is:

$$H(X) = -\sum_{j=1}^{K} P_r(\chi_j) \log_2 P_r(\chi_j) \quad (3)$$

$$P_r(X = \chi_j) = \frac{1}{IS} \quad (4)$$

where X is the original image, $\Pr(\chi_j)$ is the probability of $X = \chi_j$, χ_j is j-th possible value in X, K indicates the number of levels present in an image, and S stands for "intensity sequence number," which is related to the format of the image. The entropy values of encrypted test images through the encryption schemes are shown in Table 5. The entropy values here derived are slightly higher than the theoretical values that would have been expected. As presented in Table 6, this approach experienced an entropy increment compared to Lena grey image in the prior work.

TABLE V. ENTROPY TEST.

	Lena	**Barbara**	**Cameraman**	**Babon**	**Pepper**
H_Sh_F	7.99751	7.99760	7.99721	7.99701	7.99691
F__Sh_C	7.99743	7.99711	7.99720	7.99690	7.99643
H_SP1_F	7.99762	7.99751	7.99742	7.99693	7.99730
F_SP1_P1	7.9971	7.99750	7.99691	7.99751	7.99732
P1_SF_F	7.99742	7.99711	7.99740	7.99742	7.99751

TABLE VI. COMPARISON WITH PREVIOUS WORKS FOR ENTROPY TEST OF LENA IMAGE.

Ref. no.	[13]	[29]	[36]	[37]	[16]	[25]	[15]	[38]	[39]	[40]	[41]
entropy	7.9962	7.9965	7.9971	7.999312	7.9969	7.9977	7.9993	7.997	7.9974	7.9914	7.9992

2. Correlation Coefficient analysis(CC)

A correlation coefficient is an essential parameter for examining the relationship between pixels in three-dimension horizontal, vertical, and diagonal. The pixels that comprise the plain text image have a solid association in all directions. In a secure system, the data are uncorrelated and random; thus, the value tends toward zero, and the encrypted plaintext image preserves all of its original features. If Q random pairings of the surrounding pixels of an image with the values (α_j, β_j), where j might vary from 1 to Q, are chosen. The equation of CC is:

$$CC = \frac{\sum_{j=1}^{Q}(\alpha_j - E(\alpha))(\beta_j - E(\beta))}{\sqrt{\sum_{j=1}^{Q}(\alpha_j - E(\alpha))^2}\sqrt{\sum_{j=1}^{Q}(\beta_j - E(\beta))^2}} \quad (5)$$

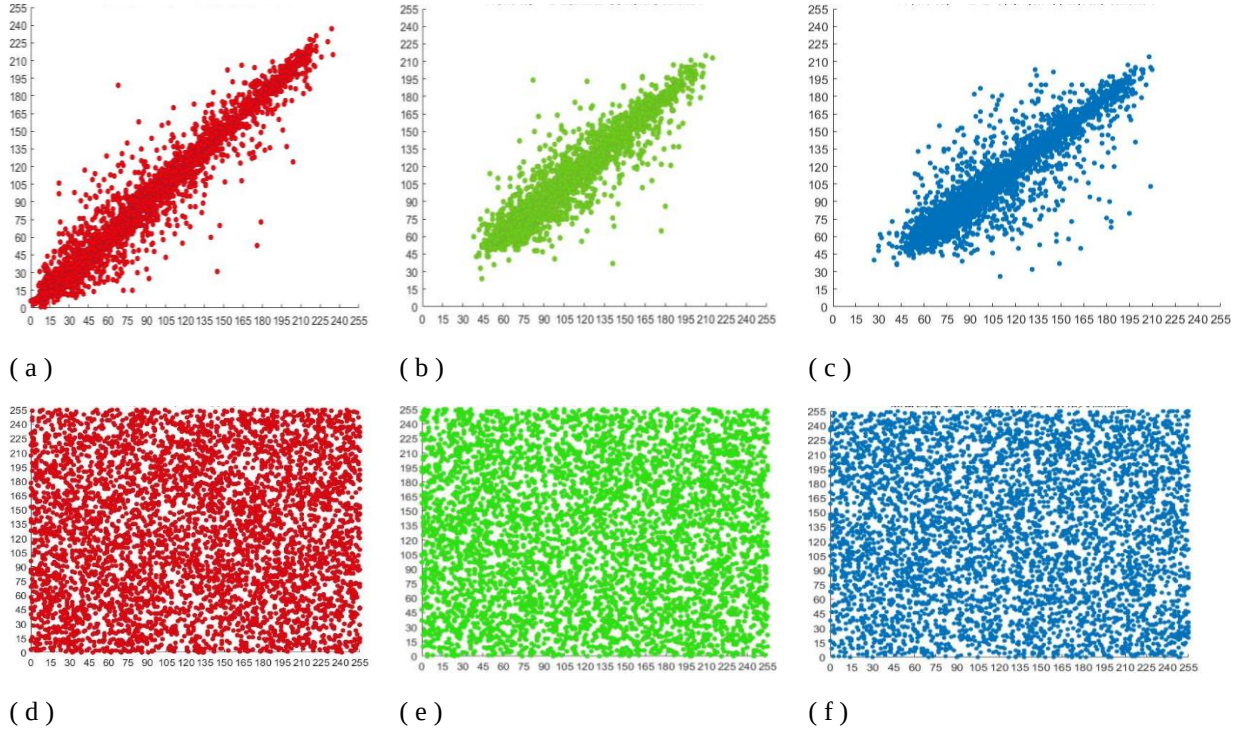
Where E(.) is the mean value function, $(\alpha \ , \beta)$ are two neighboring pixels. The performance of the proposed system on the three-directional encrypted images for the correlation coefficient is shown in the Table 7. In Table 8, which includes previous work, the proposed methods documented have CC values higher than the one shown in Table 6. Barbara plaintext images and their corresponding encrypted images are shown in figure 5, it shows the three correlation directions.

TABLE VII. CORRELATION COEFFICIENT TEST.

	Lena			**Barbara**			**Camera man**			**Babon**		
	Horiz.	**Vert.**	**Diag.**	**Horiz.**	**Vert.**	**Diag.**	**Horiz.**	**Vert.**	**Diag.**	**Horiz.**	**Vert.**	**Diag.**
H sh F	0.027	-0.037	-0.029	-0.024	0.074	0.059	0.0964	0.011	0.0136	-0.156	0.021	0.0692
F Sh C	-0.068	-0.010	-0.024	-0.023	-0.108	0.049	-0.0108	0.004	-0.0127	0.0432	-0.145	-0.0334
P1_SF_F	-0.045	-0.143	0.097	-0.11	-0.091	-0.017	-0.0187	-0.09	0.0001	0.0414	-0.035	-0.0381
F SP1_P1	0.0378	-0.006	-0.0346	-0.0091	-0.108	-0.042	-0.0577	0.001	-0.0079	0.0551	0.010	0.0698
H Sh_P1	-0.040	-0.107	-0.027	-0.011	0.020	-0.100	-0.0601	0.067	0.0144	-0.075	0.001	0.0669

TABLE VII. CORRELATION COEFFICIENT TEST FOR PREVIOUS WORKS FOR LENA IMAGE.

Reference	**Horizontal**	**Vertical**	**Diagonal**
[29]	0	-0.004	0.00030
[36]	−0.001	−0.001	−0.00030
[37]	0.001	0.001	0.00051
[16]	0.0028	−0.001	0.0021
[25]	0.00070	0.00060	0.00031
[15]	0.001	0.001	0.001
[38]	0.002	0.001	0.00081
[39]	0.002	0.006	0.00051
[40]	0.00162	0.00027	0.00062
[41]	0.00006	0.00001	-0.00002
[42]	0.005	0.001	0.006



(a) (b) (c)

(d) (e) (f)

Fig . 5. Pixels correlation in all directions of Lena color image and encrypted image respectively; (a,d)red, (e,b) green, (c,f) blue.

3. Key Analysis

A secure encryption system is one that cannot succumb to any comprehensive key attack hence the need to implement key sensitivity. When it becomes impossible to recover the original data if a slight difference occurs between the encryption, decryption keys then the technique is said to be "keys sensitive", that too even if the difference between the keys is in the order of 10^{-15} then the resulting sequence would be entirely different [47].

The key space is the number of keys that can be possibly used in a particular cryptographic method. This is why to counter brute-force attacks, it is encouraged that the total key search space is greater than 2^{100} [47]. Here, the mentioned 3D FCM applied to produce key-dependent S-Boxes. Table 9 represents the key space of the 3DFCM and the proposed scheme used in this paper. The parameters of the 3DFCM include x_0, y_0, z_0, L, M and N, which makes the key space measuring up to a level that will bar any attempt at a brute force.

P1 consists of three chaotic maps, each with six parameters. These maps can be used as key1 or key2 and are also useful in constructing the S-Boxes while completing the procedure of the encryption. As for the F_SF_F pattern, the determined size of the key will be $(10^{15})^6\times(10^{15})^6\times(10^{15})^6$. Our method defines a key space big enough that resume all types of brutal force attacks. Comparisons of the sizes of keys have been presented in table 10 and it is revealed that the proposed image encryption has a key space bigger and more invincible than other researches done.

TABLE IX. KEY SIZE OF THE PROPOSED SCHEMES.

Method	3DFCM	P 1	H SP2 P3	F SP2 P2
Keyspace	10^{90}	10^{120}	10^{690}	10^{990}

TABLE X. A COMPARISON OF KEY-SIZE WITH PREVIOUS STUDIES.

Ref no.	[44]	[24]	[16]	[30]	[31]	[22]	[20]
Keyspace	2^{352}	2^{340}	10^{704}	2^{430}	2^{213}	2^{280}	2^{207}

In this part, two proposed arrangements had chosen (H-Sf_C and H-Sf_F); for evaluation purposes, color images are submitted for security checks.

The described method properly hides the pixel distributions across all channels H-Sf_F, indicating the results of their testing using colored images. To test the performance of the algorithm on real life image processing, entropy, NPCR, UACI and correlation analysis were carried out on the color images. The results presented in the Table 11 as well as the comparison data on the Lena image in the Table 12, prove the efficiency of the method. In all cases, the results demonstrate that the proposed image encryption is secure and fast for colour as well as grayscale pictures; also revealing a vast enhancement compared to prior approaches.

TABLE XI. TESTS FOR 256X256 COLOR IMAGES.

Lena	**Entropy**	**Correlation**	**NPCR**	**UACI**	**psnr**
H Sf C	7.99910	0.034 0.022 -0.056	99.611	33.406	7.957
H Sh f	7.99921	0.046 -0.101 -0.002	99.602	33.457	7.973
Baboon					
H Sf C	7.99910	0.003 -0.089 0.078	99.596	33.537	8.437
H Sh f	7.99910	0.031 0.036 -0.041	99.629	33.459	8.427
Barbara					
H Sf C	7.999	0.055 0.076 -0.033	99.571	33.502	8.953
H Sh f	7.998	-0.075 0.034 0.006	99.620	33.516	8.563
Pepper					
H Sf C	7.999	-0.004 -0.1186 0.055	99.605	33.506	8.587

TABLE XII.COMPARISON FOR 256 X 256 LENA COLOR IMAGE WITH PREVIOUS STUDIES.

	Entropy	Correlation	NPCR	UACI
[29]	7.9971	-0.0020 -0.0011 -0.0020	99.590	33.031
[15]	7.99921	0.0004 0.0061 -0.00020	99.621	33.2
[12]	7.99920	-0.00160 -0.00031 -0.00121	99.609	33.4
[19]		−0.0230 0.0041 0.0060	99.6021	33.46
[20]	7.9967 1	− 0.004 −0.017 0.004	99.625	33.4
[22]	7.98911		99.631	33.6
[31]	7.9990	0.00161 0.00670 0.00569	99.721	33.251
[43]	7.99911	0.003 0.0070 0.002	99.5941	30.46
[26]	7.99551	-0.002 0.002 -0.001	99.766	36.714

6. CONCLUSION

Simple and secure 3D chaotic maps have been proposed for encryption images with S-box. Aiming to reduce the complexity and increase the efficiency of the encryption system, a novel system has been proposed to encrypt gray and color images; moreover, a novel chaotic map is proposed for key generation. Using a multi-stage Chaos-based key generator and utilizing Sbox, we have devised a fast and secure algorithm for image encryption. During the key matrix generation step, many chaotic maps have been used in different arrangements, which can increase the randomness and unpredictability inside the key matrix. Firstly, we apply a ciphering stage to encrypt the image with different keys. Furthermore, by using an Sbox, It is feasible for both pixel and key information to be distributed throughout the entire cipher image, then we used a second ciphering stage. Experiments indicate that the proposed encryption method can contain many keys, with key space $>10^{180}$; it depends on the arrangements used in the encryption system. Robust resistance to statistical, brute-force, differential, and other prevalent assaults; high plaintext sensitivity; information entropy performance is superior to 7.999, NPCR close to 99.6, UACI close to 33.8. In addition, the results of tests done on color photographs indicate that this algorithm has a vast array of potential applications. The suggested picture encryption technique meets the security, efficiency, and resilience requirements for the vast majority of daily image-confidential communications.

Conflicts Of Interest

The author asserts that there are no conflicts of interest that could have affected the study design, methodology, or results.

Funding

The absence of acknowledgments or thank you notes to institutions or sponsors in the paper suggests no financial support was received.

Acknowledgment

The author appreciates the collaborative efforts of colleagues and research groups at the institution, which enriched the discussions and analysis in this study

References

[1] Z. Chen and G. Ye, "An asymmetric image encryption scheme based on hash SHA-3, RSA, and Compressive Sensing," Optik, vol. 267, p. 169676, 2022. [Online]. Available: https://doi.org/10.1016/j.ijleo.2022.169676.

[2] S. T. Kamal et al., "A new image encryption algorithm for Grey and color medical images," IEEE Access, vol. 9, pp. 37855–37865, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3063237.

[3] H. Imad Mhaibes, M. Hattim Abood, and A. Farhan, "Simple lightweight cryptographic algorithm to secure imbedded IOT devices," International Journal of Interactive Mobile Technologies (iJIM), vol. 16, no. 20, pp. 98–113, 2022. [Online]. Available: https://doi.org/10.3991/ijim.v16i20.34505.

[4] R. S. Ali et al., "Enhancement of the cast block algorithm based on novel S-box for image encryption," Sensors, vol. 22, no. 21, p. 8527, 2022. [Online]. Available: https://doi.org/10.3390/s22218527.

[5] J. Ayad, F. S. Hasan, and A. H. Ali, "Image encryption using One Dimensional Chaotic Map and transmission Through OFDM system," in Proc. 14th Int. Conf. on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-7. [Online]. Available: https://doi.org/10.1109/ICCCNT56998.2023.10308260.

[6] J. Ayad, F. S. Hasan, and A. H. Ali, "OFDM Transmission for encrypted Images based on 3D Chaotic Map and S-Box through Fading Channel," in Proc. Int. Conf. on Smart Systems for applications in Electrical Sciences (ICSSES), Tumakuru, India, 2023, pp. 1-6. [Online]. Available: https://doi.org/10.1109/ICSSES58299.2023.10199452.

[7] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, vol. 480, pp. 403–419, 2019. [Online]. Available: https://doi.org/10.1016/j.ins.2018.12.048.

[8] S. A. Elsaid, E. R. Alotaibi, and S. Alsaleh, "A robust hybrid cryptosystem based on DNA and hyperchaotic for images encryption," Multimedia Tools and Applications, vol. 82, no. 2, pp. 1995–2019, 2022. [Online]. Available: https://doi.org/10.1007/s11042-022-12641-5.

[9] R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," Annals of Data Science [Preprint], 2022. [Online]. Available: https://doi.org/10.1007/s40745-021-00364-7.

[10] C. Zhu et al., "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," Multimedia Tools and Applications, vol. 79, no. 11-12, pp. 7227–7258, 2019. [Online]. Available: https://doi.org/10.1007/s11042-019-08226-4.

[11] D. S. Laiphrakpam et al., "Encrypting multiple images with an enhanced chaotic map," IEEE Access, vol. 10, pp. 87844-87859, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3199738.

[12] B. Ge et al., "Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation," IEEE Access, vol. 9, pp. 137635-137654, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3118377.

[13] A. Shokouh Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," Pattern Analysis and Applications, vol. 22, no. 1, pp. 243-257, 2018. [Online]. Available: https://doi.org/10.1007/s10044-018-0765-5.

[14] Q. Lai et al., "High-efficiency medical image encryption method based on 2D logistic-gaussian hyperchaotic map," Applied Mathematics and Computation, vol. 442, p. 127738, 2023. [Online]. Available: https://doi.org/10.1016/j.amc.2022.127738.

[15] P. Parida et al., "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," IEEE Access, vol. 9, pp. 76191-76204, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3072075.

[16] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," Optik, vol. 272, p. 170316, 2023. [Online]. Available: https://doi.org/10.1016/j.ijleo.2022.170316.

[17] S. Gao et al., "A 3D model encryption scheme based on a cascaded chaotic system," Signal Processing, vol. 202, p. 108745, 2023. [Online]. Available: https://doi.org/10.1016/j.sigpro.2022.108745.

[18] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," Expert Systems with Applications, vol. 213, p. 119074, 2023. [Online]. Available: https://doi.org/10.1016/j.eswa.2022.119074.

[19] W. Song et al., "A parallel image encryption algorithm using intra bitplane scrambling," Mathematics and Computers in Simulation, vol. 204, pp. 71-88, 2023. [Online]. Available: https://doi.org/10.1016/j.matcom.2022.07.029.

[20] S. Yan et al., "Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image," Integration, vol. 88, pp. 203-221, 2023. [Online]. Available: https://doi.org/10.1016/j.vlsi.2022.10.002.

[21] L. Zhu et al., "A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map," Information Sciences, vol. 607, pp. 1001-1022, 2022. [Online]. Available: https://doi.org/10.1016/j.ins.2022.06.011.

[22] A. Javeed, T. Shah, and A. , "Lightweight secure image encryption scheme based on chaotic differential equation," Chinese Journal of Physics, vol. 66, pp. 645-659, 2020. [Online]. Available: https://doi.org/10.1016/j.cjph.2020.04.008.

[23] S. Bhowmik and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," Journal of Information Security and Applications, vol. 72, p. 103391, 2023. [Online]. Available: https://doi.org/10.1016/j.jisa.2022.103391.

[24] L. Liu and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," Mathematics and Computers in Simulation, vol. 204, pp. 89-114, 2023. [Online]. Available: https://doi.org/10.1016/j.matcom.2022.07.030.

[25] S. Zhou, X. Wang, and Y. Zhang, "Novel image encryption scheme based on chaotic signals with finite-precision error," Information Sciences, vol. 621, pp. 782-798, 2023. [Online]. Available: https://doi.org/10.1016/j.ins.2022.11.104.

[26] E. Setyaningsih, R. Wardoyo, and A. K. Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution," Digital Communications and Networks, vol. 6, no. 4, pp. 486-503, 2020. [Online]. Available: https://doi.org/10.1016/j.dcan.2020.02.001.

[27] A. S. Alanazi, "A dual layer secure data encryption and hiding scheme for color images using the three-dimensional chaotic map and Lah Transformation," IEEE Access, vol. 9, pp. 26583-26592, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3058112.

[28] W. J. Jun and T. S. Fun, "A new image encryption algorithm based on single S-box and dynamic encryption step," IEEE Access, vol. 9, pp. 120596-120612, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3108789.

[29] M. Tanveer et al., "Multi-images encryption scheme based on 3D chaotic map and Substitution Box," IEEE Access, vol. 9, pp. 73924-73937, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3081362.

[30] Z. A. Abduljabbar et al., "Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map," IEEE Access, vol. 10, pp. 26257-26270, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3151174.

[31] S. Deb and P. K. Behera, "Design of key-dependent bijective S-boxes for color image cryptosystem," Optik, vol. 253, p. 168548, 2022. [Online]. Available: https://doi.org/10.1016/j.ijleo.2021.168548.

[32] J. Wang et al., "Optical Image Encryption scheme based on quantum S-box and meaningful ciphertext generation algorithm," Optics Communications, vol. 525, p. 128834, 2022. [Online]. Available: https://doi.org/10.1016/j.optcom.2022.128834.

[33] X. Qian et al., "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," IEEE Access, vol. 9, pp. 61334-61345, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3073514.

[34] J. Namuq, F. Hasan, and A. Ali, "Image encryption based on S-box and 3D-chaotic maps and secure image transmission through OFDM in Rayleigh Fading Channel," Engineering and Technology Journal, vol. 42, no. 2, pp. 288-297, 2024. [Online]. Available: doi:10.30684/etj.2024.141722.1508.

[35] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," Microprocessors and Microsystems, vol. 65, pp. 1-6, 2019. [Online]. Available: https://doi.org/10.1016/j.micpro.2018.12.003.

[36] L. Liu and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," Mathematics and Computers in Simulation, vol. 204, pp. 89-114, 2023. [Online]. Available: https://doi.org/10.1016/j.matcom.2022.07.030.

[37] S. Bhowmik and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," Journal of Information Security and Applications, vol. 72, p. 103391, 2023. [Online]. Available: https://doi.org/10.1016/j.jisa.2022.103391.

[38] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," Signal Processing, vol. 168, p. 107340, 2020. [Online]. Available: https://doi.org/10.1016/j.sigpro.2019.107340.

[39] X. Wang et al., "A new image encryption algorithm based on Latin square matrix," Nonlinear Dynamics, vol. 107, no. 1, pp. 1277-1293, 2021. [Online]. Available: https://doi.org/10.1007/s11071-021-07017-7.

[40] L. Teng, X. Wang, and Y. Xian, "Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion," Information Sciences, vol. 605, pp. 71-85, 2022. [Online]. Available: https://doi.org/10.1016/j.ins.2022.05.032.

[41] Y. Xian et al., "Cryptographic system based on double parameters fractal sorting vector and new spatiotemporal chaotic system," Information Sciences, vol. 596, pp. 304-320, 2022. [Online]. Available: https://doi.org/10.1016/j.ins.2022.03.025.

[42] F. Musanna and S. Kumar, "Image encryption using Quantum 3-D Baker map and Generalized Gray Code coupled with fractional Chen's chaotic system," Quantum Information Processing, vol. 19, no. 8, 2020. [Online]. Available: https://doi.org/10.1007/s11128-020-02724-3.

[43] Z. A. Abduljabbar et al., "Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map," IEEE Access, vol. 10, pp. 26257-26270, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3151174.

[44] S. Zhu et al., "Secure image encryption scheme based on a new robust chaotic map and strong S-box," Mathematics and Computers in Simulation, vol. 207, pp. 322-346, 2023. [Online]. Available: https://doi.org/10.1016/j.matcom.2022.12.025.

[45] J. Ayad, F. S. Hasan, and A. H. Ali, "Efficient Transmission of Secure Images with OFDM using Chaotic Encryption," in Proc. 4th Int. Conf. on Circuits, Control, Communication, and Computing (I4C), Bangalore, India, 2022, pp. 391-396, doi: 10.1109/I4C57141.2022.10057774.