PENINSULA PUBLISHING LLC

SHIFRA
Vol. **(2023)**, 2023, **pp.** 95–107
ISSN: 3078-3186

Research Article

Encryption of Color Images utilizing cascading 3D Chaotic Maps with S-Box Algorithms

Jenan Ayad[1,*], Guma Ali[2], Waheed Ullah[3], Wamusi Robert[4]

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

[2] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[3] *University of the Witwatersrand, South Africa*

[4] *Department of Computing and Technology, Faculty of Engineering Design and Technology, Uganda Christian University Arua Campus, P.O Box 356, Arua, Uganda*

ARTICLEINFO

Article History
Received 15 May 2023
Revised: 3 Jul 2023
Accepted 3 Aug 2023
Published 25 Aug 2023

Keywords
Encryption,
chaotic map,
decryption,
S-box,
PRNG.

ABSTRACT

The fundamental characteristics of chaos, including sensitivity to beginning conditions and unpredictability, render it a prime candidate for cryptographic applications. This research introduces an encryption methodology for effective and safe image encryption. The encryption system has two ciphering phases and a substitution phase. This study proposes a method for key creation. The design of a pseudo-random number generator utilized for key generation is founded on chaotic algorithms. The chaotic map will be employed in encryption systems owing to its superior security. NIST tests are employed to assess the randomness of the proposed PRNG sequences. The subsequent part presents a security study of the suggested picture encryption approach to evaluate its efficacy. The statistical analysis now confirms that the technique is secure and efficient for encrypting both basic and complicated images, whether in monochrome or color. Through a comparison with previous chaotic investigations, it is evident that our method is competitive with earlier efforts.

1. INTRODUCTION

Consequently, while the current methodology relies on picture processing and data transmission, enhancements have been seen in recent years. The protection of critical data during real-time transmission across wired and wireless networks has become increasingly vital. Technology has advanced, influencing and transforming several domains through the utilization of multimedia and visual communication tools, particularly in the military and medical sectors that employ data transmission. Previous encryption techniques utilized for image encryption have been inadequate for managing huge database images [1, 2]. Consequently, emphasis has been directed towards the enhancement of picture encryption algorithms, particularly those utilizing chaos as the primary encryption foundation [3, 4].

Chaotic systems and cryptology are intricately connected, as the characteristics of chaotic systems such as randomness, sensitivity to initial conditions, ergodicity, and deterministic yet extremely unexpected outcomes correspond effectively with the demands of encryption. These beneficial traits have prompted further investigation of chaos-based encryption via supplementary experiments [8]. Random number sequences are crucial in encryption, and the unpredictability of these generated numbers is closely linked to the strength of the encryption. To do this, pseudorandom number generators (PRNG) based on chaos have emerged as a prevalent application of chaotic systems in cryptography [9]. The S-Box is an essential element in block encryption techniques, as it introduces confusion to enhance encryption security. The construction of a resilient S-Box structure is essential, as it must exhibit superior cryptographic attributes, resist attacks, and endure differential cryptanalysis to function effectively in encryption [10].

Associated literature

*Corresponding author email: jinan.a.namuq@uotechnology.edu.iq
DOI: https://doi.org/10.70470/SHIFRA/2023/011

The intricate architectures of contemporary encryption methods, necessitating substantial computational resources, adversely affect the efficacy of picture encryption processes. Regarding the application of chaotic systems in encryption techniques, it is essential to recognize that, despite ongoing academic research, none of the encryption methods that exclusively utilize chaotic systems can deliver adequate security.

A chaotic sequence was produced utilizing a sine map in reference [11]. An elliptic curve point and a dynamic permutation table were employed to enhance system security. The research in [12] decreased the iterations of the hyperchaotic system from WH/4 to 2W, representing a substantial reduction for a picture of size W×H. An innovative post-processing method for constructing a key matrix facilitated this enhancement. A novel methodology was introduced in [13], featuring low time complexity, high output complexity, and a straightforward algorithm utilizing 3D logistic maps. Reference [14] outlined a novel method for encrypting medical images via a 2D Logistic-Gaussian hyperchaotic map. In [15], picture encryption was achieved using 3D and 4D Arnold Cat maps, and the model integrated the secure Elliptic Curve. A distinctive image encryption method utilizing a mix of three modified and enhanced chaotic one-dimensional maps was proposed in [16]. In [17], a method for encrypting 3D models was introduced, utilizing a 2D chaotic system formed by linking the logistic map with infinite collapse (2D-LAIC) with the semi-tensor product (STP) theory. Reference [18] presented a bit-level permutation and hyper-chaotic system as the basis for an encryption strategy, whereas [19] suggested intra bitplane scrambling for parallel picture encryption. A novel four-dimensional multi-scroll hyperchaotic system was established in [20]. A visually secure picture encryption system was suggested in [21] by integrating the adaptive-threshold sparsification compression sensing model with an innovative memristive chaotic map design. A chaotic oscillator was produced in [22] utilizing a second-order differential equation.

Innovative proposals for key generation were presented in [23]. The research in [24] delineated a series of one-dimensional quadratic chaotic maps grounded in topological conjugate theory. A novel approach employing finite accuracy for the generation of chaotic signals to enhance image encryption is provided in [25]. The encryption technique was improved through the utilization of S-BOX, an algorithm grounded in chaotic processes, which offered elevated security and efficiency. In [26], the encrypted data, comprising S-Boxes produced from a chaotic logistic map, was compressed prior to encryption. The authors in [27] proposed a three-dimensional chaotic map employing highly nonlinear S-boxes for encryption, succeeded by a data concealment technique utilizing the Lah transform. A low-dimensional chaotic technique was utilized in [28] to generate an S-box measuring 10 by 26. In [29], the effectiveness of encryption was enhanced, and secure transmission was facilitated with the implementation of a 3D chaotic map-based symmetric approach. In [30], it was proposed that the integration of several chaotic map types with an S-box could facilitate a rapid technique for scrambling and encrypting color images. In [31], the Henon map was employed to introduce novel key-dependent bijective S-Boxes for an image cryptosystem. In [32], a novel method of picture encryption has been developed by integrating quantum walks with the production of visually meaningful ciphertexts.

This project aims to develop an efficient and safe image encryption system utilizing straightforward methods and a resilient key. The research presents a methodology for image encryption utilizing chaotic maps and the S-box technique. The proposed encryption method incorporates an S-box in conjunction with chaotic maps, so augmenting security while preserving the advantageous statistical properties of the technique.

This paper proposes a novel method for key creation utilizing multi-stage 3D chaotic maps.

The subsequent sections of this work are organized as outlined below. Section 2 comprises the current chaotic maps utilized in this study. Section three introduces the key generation process and S-box construction, then discusses the proposed picture encryption algorithms. Section 4 presents the experimental data and an evaluation of their efficacy. The conclusions are addressed in the concluding section.

2. CHAOTIC MAPS

The renowned 3D chaotic systems, specifically the Logistic map and the 3D Henon map, have been evaluated for key generation in the suggested systems. The mathematical models of the chaotic systems utilized in this work are delineated in Table I.

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

3. THE PROPOSED IMAGE ENCRYPTION SCHEME

This section presents a chaotic approach for generating random numbers and examines the resulting chaotic system. Upon establishing that the chaotic system possesses adequate dynamic characteristics, a random number generator may be devised. Random numbers produced by a random number generator are utilized in tests conducted by the National Institute of Standards and Technology (NIST). An S-box is generated to enhance the efficacy of the proposed encryption techniques.

1. Key Generation

   The key generation of the suggested method relies on the PRBG algorithm. Due to the intricacy of prior works, a compromise must be established between the security of the cryptosystem and its efficiency. This study utilized a 4*1 multiplexer for key generation, employing four distinct chaotic maps, as illustrated in Figure 1. Figure 2 illustrates a block design for a 3D-Quantization and Decimal-to-binary converter, utilized to transform the output of the chaotic map into 8-bit binary format.

   The key generation proposal P2Sel looks like a 4*1 multiplexer with four different chaotic maps as an input and another chaotic map as a selector. The 3D chaotic maps used for the input are 3D-CM, 3D-FCM, 3D-HM, and 3D-SCM with their initial values. The procedure starts with the 3D-CSM with initial values xcs(0), ycs(0), and zcs(0), and then xoring xcs(i) and ycs(i) to get S0 selector, while the second selector S1= zcs(i) directly. The mathematical expression for the selection process is:

$$K_{P2}(R,G,B) = \begin{cases} Xc, Yc, Zc & , \quad if \quad S_0S_1 = 00 \\ Xf, Yf, Zf & , \quad if \quad S_0S_1 = 01 \\ Xh, Yh, Zh & , \quad if \quad S_0S_1 = 10 \\ Xsc, Ysc, Zsc & , \quad if \quad S_0S_1 = 11 \end{cases} \qquad (1)$$

   When the selectors are (00), the multiplexor will allow the stream of the first chaotic map 3D-CM at the output; therefore, the key stream K_P2(00) = (Xc, Yc, Zc). When the selectors are (01), the multiplexor will allow the stream of the second chaotic map 3D-FCM at the output; therefore, the key stream K_P2(01) = (Xf, Yf, Zf). When the selectors are (10), the multiplexor will allow the stream of the third chaotic map 3D-HM at the output; therefore, the key stream K_P2(10) = (Xh, Yh, Zh). Finally, when the selectors are (11), the multiplexor will allow the stream of the fourth chaotic map 3D-SCM at the output; therefore, the key stream K_P2(11) = (Xsc, Ysc, Zsc).

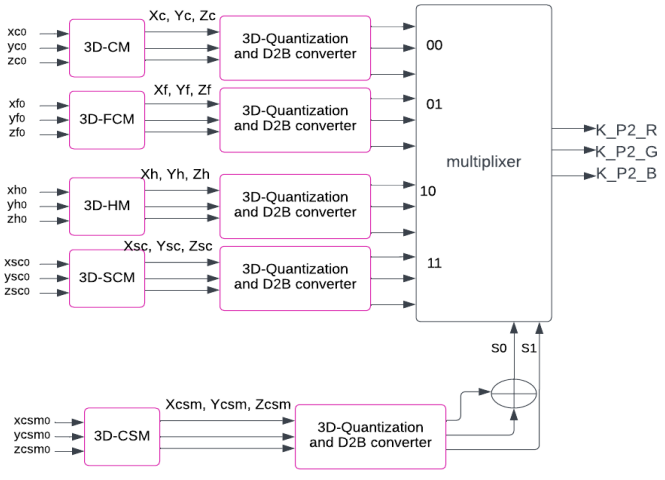


Fig. 1. Key generation Proposal, selection method (P2Sel)

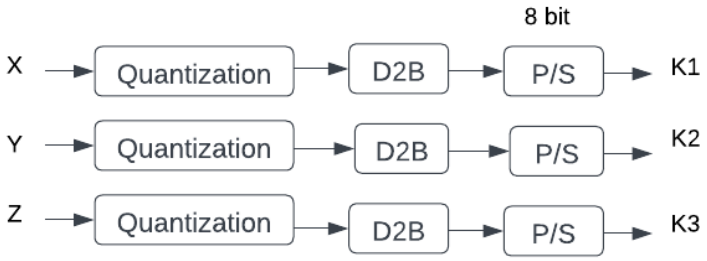


Fig. 2. 3D-Quantization and Decimal-to-binary converter block diagram

NIST is a commonly employed test suite for assessing the stochastic performance of a time series [34, 37]. The NIST mandates various sequences and primarily depends on two essential performance metrics: P-value and pass rate, to evaluate the random performance of time series [38]. The pseudo-random characteristics of the novel chaotic signals were validated through NIST testing. The established protocol was employed to evaluate the randomness of the x, y, and z sequences. The NIST test results for 15 trials are displayed in table II, indicating that all values consistently remain below 0.01 in each instance. The outcomes of all randomness tests indicate that the sequences produced by the key are enough unpredictable for picture encryption purposes.

TABLE II. NIST RESULT TEST

	Proposed algorithms
NIST tests	P2 Sel
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

The Substitution-Box consists mostly of various mathematical processes. This encryption algorithm utilizes a plaintext block and a key as inputs to generate an encrypted block as output. This is succeeded by S-box transformations to generate the ciphertext, followed by several iterations of S-box transformations. Decryption is executed by applying the inverse of the S-box modifications in reverse sequence with the identical key [39].

The process applied to a pixel value p utilizing an S-box matrix s is termed a nonlinear transformation, formally represented by the substitution function sb(s, p). This function outputs the modified ciphertext pixel value. A technique for generating trustworthy S-boxes utilizing chaotic maps (3D-CM, 3D-HM, 3D-FCM) and the proposed scheme (P1FB) has been formulated. The resultant 3D chaotic sequences are arranged in ascending order, and the indices of the ordered values are documented in one-dimensional arrays. The production of the S-box from the prior sorting process is essential. The ordered indices are subsequently arranged into a 16x16 matrix, where each column denotes the identity of the values in the sorted sequence and each row signifies an S-box, referred to as the Sbox_matrix. This transformation is applied to every pixel in the given image, utilizing the pixel's value as the index for the S-box. The recovered result represents the new pixel value in the modified image referred to as Sbox_Imag, which illustrates the encrypted text pixel value.

The building of an S-box comprises three phases:

Step1: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.
All members of S must be integers inside the interval [0, 255], so S(i, j) ∈ [0, 255]. S(i, j) must be devoid of duplicates, with all entries constrained inside the interval [0, 255]. The research employed a heuristic approach to construct the S_box utilizing the Henon map, Cat map, Factorial map, and the proposed methodology. The x sequence was encoded with the blue vector of the image, the y sequence was encoded with the red vector of the image, and the z sequence was associated with the green vector of the image.
To decrypt, specify the inverse S-box transformation function, sb Inverse (s, q). As previously mentioned, s denotes the current state of the stream cipher, while q signifies the initial q bits of the ciphertext block. The second method delineates the procedure for S-Box Inversion.
It is essential that all elements of S are integers inside the interval [0, 255], therefore S(i, j) ∈ [0, 255]. S(i, j) must be devoid of duplicates, with all entries constrained inside the interval [0, 255]. The research employed a heuristic approach to construct the S_box utilizing the Henon map, Cat map, Factorial map, and the proposed methodology. The x sequence was encoded with the blue vector of the image, the y sequence with the red vector, and the z sequence with the green vector. To decrypt, specify the inverse S-box transformation function, sb Inverse(s, q). As previously mentioned, s denotes the current state of the stream cipher, while q signifies the initial q bits of the ciphertext block. The second way addresses the technique for S-Box Inversion.

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.

The suggested picture encryption methodology
The picture encryption system comprises three phases: two phases of ciphering utilizing chaotic maps with a pseudorandom number generator (PRNG) and one phase of substitution employing an S-box. Figure 3 illustrates the block diagram of the whole picture encryption system. The original color image is subsequently split into its RGB channels, followed by the encryption procedure. A diffusion operation is subsequently executed employing three distinct S-box algorithms for each RGB channel independently. The final data processing operation of encryption is conducted concerning the RGB channels subsequent to the execution of the diffusion operation. The three channels are ultimately merged to produce the final color ciphertext image.
The decryption algorithm fundamentally inverts the processes of the encryption algorithm.

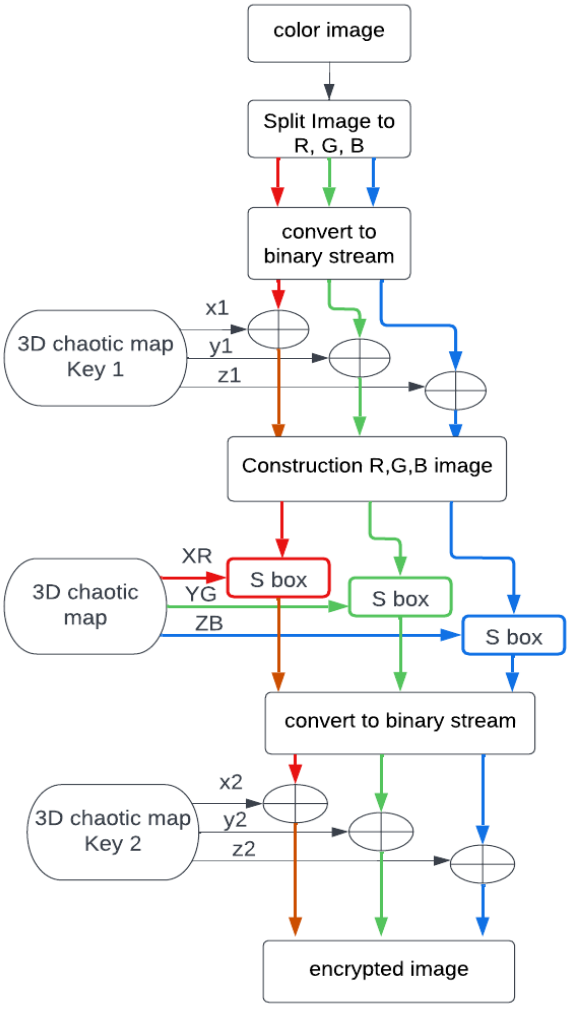


Fig .3. encryption process

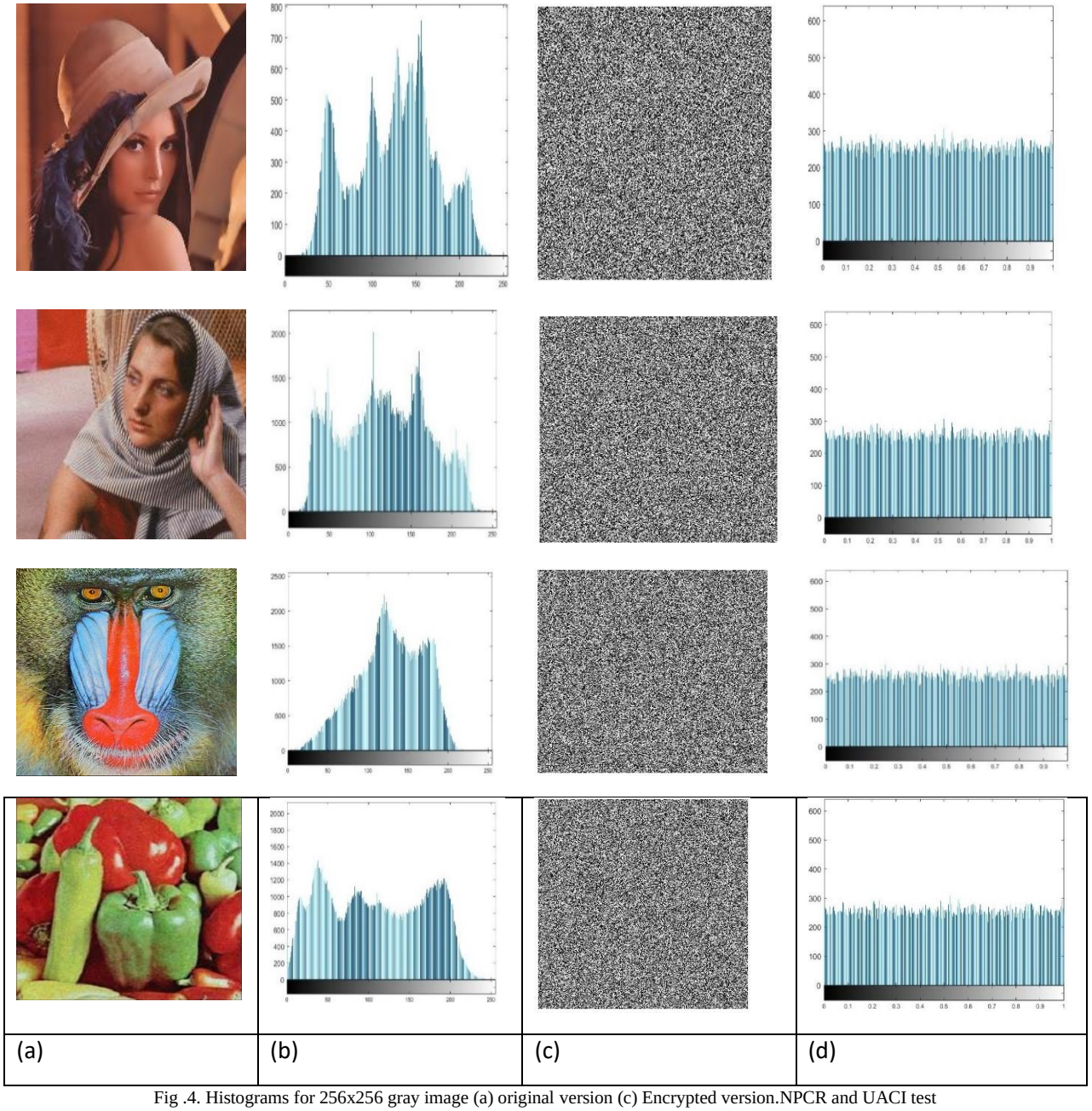
4. EXPERIMENTAL RESULTS

A comprehensive analysis was conducted on the outcomes and weaknesses of the proposed algorithms. The outcomes included histogram evaluations, correlation coefficients, information entropy, keyspace, and resistance to differential attacks. All experiments were conducted meticulously, followed by signal analysis utilizing Matlab. An essential criterion for developing an effective picture encryption technique is its ability to mitigate various attacks. Statistical analysis was conducted, including differential attack analysis (change intensity and change rates, both average and uniform) and key analysis (key-space and key-sensitivity). Additionally, correlation coefficients, information entropy, and histograms were also examined. A specific emphasis is placed on comparing the proposed solution with alternative approaches to the same problem.

This study employed compound configurations of chaotic maps to generate a key for the application type utilized in the research. The layouts were designated using the following abbreviations: Factorial chaotic map (F), Henon chaotic map (H), Cat chaotic map (C), Proposal method (P2), and S-box (S). For example, H_SP2_F indicates that the authors utilized the Henon chaotic map for the initial key, an S-box for the subsequent key according to the proposed technique with an intrinsic selection algorithm, and the production of the third key via 3DFCM.

1. Analyzing a Histogram

   Histograms illustrate the quantity of pixels in an image corresponding to a certain shade of gray. This study furnishes cryptanalysts with substantial information regarding the image. To eliminate any residual traces of the original image, the histogram of the fully encrypted image must exhibit uniformity, contrasting significantly with the histogram of the original image. Figure 4 displays the test picture, its histogram, the encrypted image, and the histogram of the encrypted image, utilizing the (P1_SF_H) arrangement for various test images. The histogram of the encrypted image provides no valuable information. The proposed method effectively obstructs the recognition of the original information in the provided image, as the altered image seems entirely distinct and exhibits uniform intensity values.



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

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

$$NPCR = \frac{\sum_{a=0}^{M-1}\sum_{b=0}^{N-1} D_{a,b}}{M*N} * 100\% \quad (2)$$

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 $D_{a.b} \in B^{M\times N}$.

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:

$$UACI = \left[\sum_{a=0}^{M-1}\sum_{b=0}^{N-1}\frac{|I_1(a,b)-I_2(a,b)|}{255}\right] * \frac{100\,\%}{M*N} \quad (3)$$

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 III. 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 IV. 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 UACI 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_SP2_F	99.6536	33.3930	99.6017	33.3408	99.6231	33.4074	99.6201	33.3287	99.5987	33.5013
F_SH_P2	99.5804	33.4704	99.6643	33.2293	99.5575	33.3834	99.5743	33.4345	99.6353	33.3719

TABLE IV COMPARISON FOR UACI 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

2. 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:

$$H(X) = -\sum_{j=1}^{K} P_r(\chi_j) \log_2 P_r(\chi_j) \quad (4)$$

$$P_r(X = \chi_j) = \frac{1}{IS} \quad (5)$$

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 V. The entropy values here derived are slightly higher than the theoretical values that would have been expected. As presented in Table VI, 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_SP2_F	7.99762	7.99751	7.99742	7.99693	7.99730
F_SP2_P2	7.9971	7.99750	7.99691	7.99751	7.99732
P2_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

3. 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:

$$CC = \frac{\sum_{j=1}^{Q}(\alpha_j - E(\alpha))(\beta_j - E(\beta))}{\sqrt{\sum_{j=1}^{Q}(\alpha_j - E(\alpha))^2}\sqrt{\sum_{j=1}^{Q}(\beta_j - E(\beta))^2}} \quad (6)$$

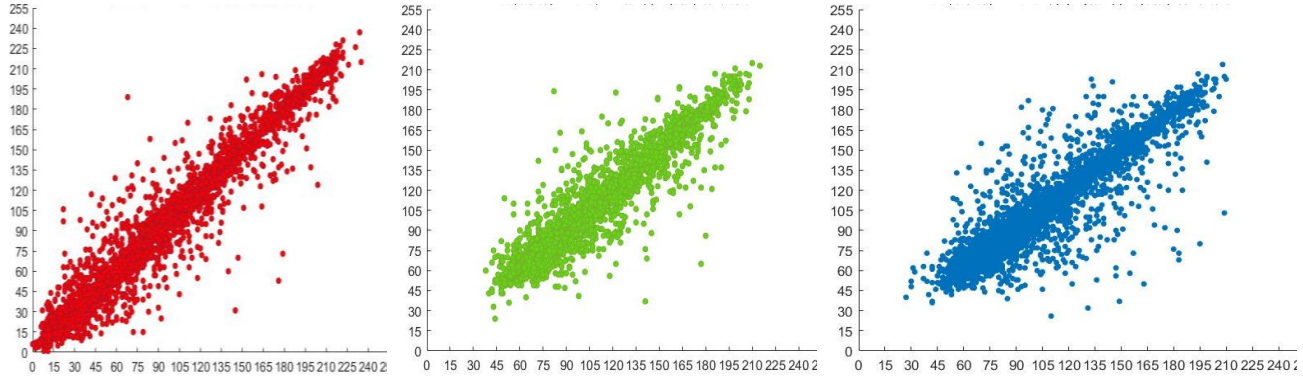
Where E(.) is the mean value function, (α , β) are two neighboring pixels. The performance of the proposed system on the three-directional encrypted images for the correlation coefficient is shown in the Table VII. In Table VIII, which includes previous work, the proposed methods documented have CC values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

TABLE VII CORRELATION COEFFICIENT TEST

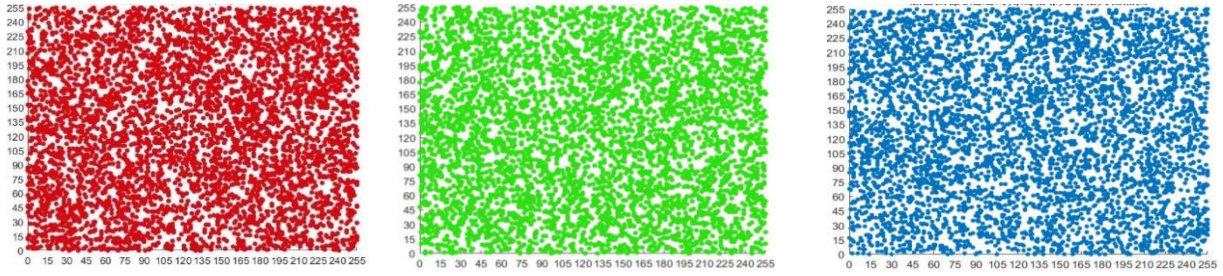
	Lena			Barbara			Camera man			Babon		
	Horiz.	Vert.	Diag.	Horiz.	Vert.	Diag.	Horiz.	Vert.	Diag.	Horiz.	Vert.	Diag.
H sh F	0.027	-0.037	-0.029	-0.024	0.074	0.059	0.0964	0.011	0.0136	-0.156	0.021	0.0692
F Sh C	-0.068	-0.010	-0.024	-0.023	-0.108	0.049	-0.0108	0.004	-0.0127	0.0432	-0.145	-0.0334
P2_SF_F	-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 SP2_P2	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_P2	-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 VIII 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.

4. 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.

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} [45]. Here, the mentioned 3D FCM applied to produce key-dependent S-Boxes. Table IX 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.

For this scheme the corresponding key space size will approximately about $(1015)6 \approx 2299$, P2 has four parameters, and each map has 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 $(1015)6\times(1015)6\times(1015)6$. 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 X 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	P2	F SP2 P2
Keyspace	10^{90}	10^{450}	10^{990}

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

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

In this section, two selected configurations (H-Sf_C and H-Sf_F) are presented; color photos are provided for security assessments.

The strategy defined effectively conceals the pixel distributions throughout all channels H-Sf_F, reflecting the outcomes of their evaluation utilizing colored images. To evaluate the algorithm's efficacy in practical image processing, entropy, NPCR, UACI, and correlation analyses were conducted on color images. The results in Table XI and the comparative statistics on the Lena image in Table XII demonstrate the method's efficacy. The results consistently indicate that the proposed image encryption is both secure and rapid for color and grayscale images, showcasing significant improvement over previous methods.

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 256X256 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

5. CONCLUSION

Proposals have been made for simple and secure 3D chaotic maps for picture encryption utilizing S-boxes. To diminish complexity and enhance the effectiveness of the encryption system, a new method has been introduced for encrypting grayscale and color photos; also, an innovative chaotic map has been suggested for key generation. We have developed a rapid and secure solution for image encryption by employing a multi-stage chaos-based key generator and utilizing Sbox. Various chaotic maps have been employed in diverse configurations during the key matrix creation phase, enhancing the randomness and unpredictability of the key matrix. Initially, we implement a ciphering phase to encrypt the image using

several keys. Moreover, employing a Sbox enables the distribution of both pixel and key information across the full cipher image, followed by the implementation of a second encryption stage. Experiments demonstrate that the suggested encryption approach may accommodate numerous keys, with a key space exceeding 10^180, contingent upon the configurations employed in the encryption system. Strong resistance to statistical, brute-force, differential, and other common attacks; elevated plaintext sensitivity; information entropy performance exceeds 7.999, NPCR approximates 99.6, UACI approximates 33.8. Furthermore, the outcomes of experiments conducted on color images suggest that this algorithm possesses a wide range of possible applications. The proposed image encryption method satisfies the security, efficiency, and robustness criteria for the majority of routine confidential image communications.

Funding:

No external funding or financial support was provided by any commercial or governmental agency for this study. The research was independently managed by the authors.

Conflicts of Interest:

The authors declare that there are no conflicts of interest.

Acknowledgment:

The authors would like to thank their institutions for the continuous moral and institutional support received during the course of this work.

References

[1] X. Wang and Y. Teng, "A novel S-box design based on chaotic systems for image encryption," *IEEE Access*, vol. 9, pp. 12345–12356, 2021, doi: 10.1109/ACCESS.2021.3056789.

[2] L. Zhang and Y. Liu, "Secure image transmission over OFDM systems using chaotic encryption under Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2339–2350, 2020, doi: 10.1109/TCOMM.2020.2967432.

[3] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2010, doi: 10.1016/j.imavis.2010.05.005.

[4] M. A. F. Al-Husainy, "Color image encryption based on chaotic maps and S-boxes," *Int. J. Comput. Appl.*, vol. 179, no. 15, pp. 15–21, 2018, doi: 10.5120/ijca2018916893.

[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. Comput. Commun. Netw. Technol. (ICCCNT)*, Delhi, India, 2023, pp. 1–7, doi: 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. Smart Syst. Appl. Electr. Sci. (ICSSES)*, Tumakuru, India, 2023, pp. 1–6, doi: 10.1109/ICSSES58299.2023.10199452.

[7] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, 2019, doi: 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 Appl.*, vol. 82, no. 2, pp. 1995–2019, 2022, doi: 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," *Ann. Data Sci.*, preprint, 2022, doi: 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 Appl.*, vol. 79, no. 11–12, pp. 7227–7258, 2019, doi: 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, doi: 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, doi: 10.1109/ACCESS.2021.3118377.

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

[14] Q. Lai *et al.*, "High-efficiency medical image encryption method based on 2D logistic-gaussian hyperchaotic map," *Appl. Math. Comput.*, vol. 442, p. 127738, 2023, doi: 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, doi: 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, doi: 10.1016/j.ijleo.2022.170316.

[17] S. Gao *et al.*, "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Process.*, vol. 202, p. 108745, 2023, doi: 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 Syst. Appl.*, vol. 213, p. 119074, 2023, doi: 10.1016/j.eswa.2022.119074.

[19] W. Song *et al.*, "A parallel image encryption algorithm using intra bitplane scrambling," *Math. Comput. Simul.*, vol. 204, pp. 71–88, 2023, doi: 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, doi: 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," *Inf. Sci.*, vol. 607, pp. 1001–1022, 2022, doi: 10.1016/j.ins.2022.06.011.

[22] A. Javeed, T. Shah, and A. *, "Lightweight secure image encryption scheme based on chaotic differential equation," *Chin. J. Phys.*, vol. 66, pp. 645–659, 2020, doi: 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," *J. Inf. Secur. Appl.*, vol. 72, p. 103391, 2023, doi: 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," *Math. Comput. Simul.*, vol. 204, pp. 89–114, 2023, doi: 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," *Inf. Sci.*, vol. 621, pp. 782–798, 2023, doi: 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," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 486–503, 2020, doi: 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, doi: 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, doi: 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, doi: 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, doi: 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, doi: 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," *Opt. Commun.*, vol. 525, p. 128834, 2022, doi: 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, doi: 10.1109/ACCESS.2021.3073514.

[34] J. AYAD, *Pulsed radar signals and intelligent system*. Saarbrücken, Germany: LAP Lambert Acad. Publ., 2020.

[35] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," *Microprocess. Microsyst.*, vol. 65, pp. 1–6, 2019, doi: 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," *Math. Comput. Simul.*, vol. 204, pp. 89–114, 2023, doi: 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," *J. Inf. Secur. Appl.*, vol. 72, p. 103391, 2023, doi: 10.1016/j.jisa.2022.103391.

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

[39] X. Wang *et al.*, "A new image encryption algorithm based on Latin square matrix," *Nonlinear Dyn.*, vol. 107, no. 1, pp. 1277–1293, 2021, doi: 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," *Inf. Sci.*, vol. 605, pp. 71–85, 2022, doi: 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," *Inf. Sci.*, vol. 596, pp. 304–320, 2022, doi: 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 Inf. Process.*, vol. 19, no. 8, 2020, doi: 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, doi: 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," *Math. Comput. Simul.*, vol. 207, pp. 322–346, 2023, doi: 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. Int. Conf. Circuits, Control, Commun. Comput. (I4C)*, Bangalore, India, 2022, pp. 391–396, doi: 10.1109/I4C57141.2022.10057774.