IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Mapping

ZAID AMEEN ABDULJABBAR[1,2], IMAN QAYS ABDULJALEEL[3], JUNCHAO MA[4], MUSTAFA A. AL SIBAHEE [4,5], VINCENT OMOLLO NYANGARESI [6], DHAFER G. HONI [1], AYAD I. ABDULSADA[1], AND XIANLONG JIAO [7]

[1]Computer Science Department, College of Education for Pure Science, University of Basrah, Basrah, 61004, Iraq
[2]Shenzhen Institute of Huazhong University of Science and Technology, Shenzhen, 518118, China
[3]Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, 61004, Iraq
[4]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, 518118, China
[5]Computer Technology Engineering Department, Iraq University College, Basrah, 61004, Iraq
[6]Faculty of Biological and Physical Sciences, Tom Mboya University College, Homabay, 40300, Kenya
[7]College of Computer Science, Chongqing University, Chongqing, 400044, China

Corresponding author: Junchao Ma (e-mail: majunchao@sztu.edu.cn).

ABSTRACT The World Wide Web is experiencing a daily increase in data transmission because of developments in multimedia technologies. Consequently, each user should prioritize preventing illegal access of this data by encrypting it before moving it over the Internet. Numerous color image encryption schemes have been developed to protect data security and privacy, indifferent to the computation cost. However, most of these schemes have high computational complexities. This research proposes a fast color image scrambling and encryption algorithm depending on different chaotic map types and an S-box that relies on a hyperchaotic map principle. The first step involves converting color image values from decimal representation to binary representation in the scrambling stage by changing the location of the bits according to a proposed swapping algorithm. Next, in the second scrambling stage, the same process occurs after returning color image values from binary representation to decimal representation and generating an S-box with the assistance of two types of chaotic map, namely, a 2D Zaslavsky map and a 3D Hénon map. Thus, this S-box is relied upon to swap the locations of the pixels in the color image. The encryption procedure begins with the production of three key matrices using a hybrid technique that employs two low-complexity types of chaotic map, namely, a 1D Logistic map and a 3D Hénon map, followed by an XORed as a lightweight process between each key generated for the three matrices and the corresponding red, green, and blue image channels. According to the findings, the proposed scheme demonstrates the most efficiency in terms of lowering the computational cost and shows its effectiveness against a wide range of cryptographic attacks.

INDEX TERMS *Pixel mixing*, *Chaos, Fast Encryption*, *S-Box, Zaslavsky map*, *Color image*.

I. INTRODUCTION

RECENT years have seen numerous advancements within computer networks and information technology related to multimedia technologies. Digital images employed in different domains, such as biology, medical, military and daily life, are applied and play an essential role in multimedia transmission [1] [2]. Moreover, studies indicate that occasionally harmful activities directed at identifying viable information through sharing features have negatively affected the interests of communication performances and network openness [3]. Consequently, image security has become a crucial study field [4] [5]. Researchers has suggested several approaches to secure image information, including data hiding, encryption and watermarking. Image encryption technology represents the most basic means for creating a noise image out of an original image [6]. Cryptography has had significant applications throughout history. Noted users of information encryption have included governments and military personnel. However, the history of data encryption traces back to the Roman and Egyptian civilizations [7], [8].

Cryptography encrypts secret data using an algorithm that changes data so that unauthorized users cannot access it [1] [3].

In terms of image encryption, most existing techniques also use permutation and diffusion, and they either apply permutation first, then diffusion, or vice versa. That is to say: they use permutation and diffusion to encrypt images independently [3] [9]. Traditional text encryption algorithms like RSA, DES, and AES show their immaturity of image encryption due to the large size and variety of image data storage structures [10] [11]. Thus, an efficient image encryption strategy presents a digital image as a bitstream; the bitstream then undergoes encryption using standard data encryption techniques. On the other hand, a digital image has specific intrinsic properties in comparison to a bitstream, such as data redundancy and high pixel correlations. We overlook these features when approaching a digital image as a bitstream for encryption using conventional data encryption methods. Consequently, these methods encounter numerous significant challenges, such as weak encryption efficiency. Therefore, developing new image encryption algorithms that consider the characteristics of digital images can potentially improve image protection efficiency [12].

Following the encryption procedure, the image becomes information comparable to the channel's random noise, preventing eavesdropping during network transmission and successfully protecting image data in transit. Current image encryption technologies include image pixel scrambling technology, encryption technology based on secret segmentation and secret sharing, encryption technology based on modern cryptography systems and encryption technology based on chaotic systems. Additionally, the properties of the image signal may undergo examination from a different perspective when it transforms from the spatial domain to the frequency domain [4].

The usage of chaotic image encryption methods has gained increased interest in recent years. For example, these systems have a sensitive reliance on the initial stages and system parameters, randomness and ergodicity, making them ideal for image encryption. When employed in image encryption, these complex dynamic characteristics accomplish the requisite diffusion and mixing of data to increase security. Studies have shown that numerous data encryption methods based on chaotic sequences have been developed in recent years [3], [13]. Current chaotic maps have certain weaknesses. For instance, chaotic deterioration occurs on a platform with limited accuracy and non-uniform output distribution, resulting in a lack of dynamic complexity when attempting to assess their trajectories [6] [8]. Furthermore, research indicates that numerous encryption techniques based on existing chaotic maps are vulnerable to attack [6]. The Substitution Boxes (S-Boxes) in the structure of permutation ciphers constitute critical nonlinear features that ensure block ciphers maintain their confusion features. Some S-boxes are based on chaotic maps, while others are based on algebraic structures [14]. Chaotic maps are adopted due to the low computational complexity for the generating S-boxes and random numbers in image encryption schemes [15] [16] [17].

This paper proposes a method for scrambling color image data at two levels. The first aims to modify the positions of bits within the pixel data, and the second involves changing the positions of pixels in the original image based on the S-box. The encrypting step aligns with the generation of two lower mathematical complexity chaos maps, including the 1D logistic map [18] and the 3D Hènon map [19], which have merged to form hybrid chaos divided into three matrices. Following the execution of the XORed low-complexity operation between the image data obtained by the scrambling stage and the matrix data generated by the hybrid chaos generator, each of the three matrices produces the encrypted image.

This paper seeks to make a contribution by providing a low-complexity and fast image encryption technique for encrypting color images utilizing hyperchaotic systems. Obtaining the most thorough encryption security involves key parameters generating each chaotic map formula, which, in turn, increases the key space and impedes attackers' attempts to access data. In addition to increasing key space, this approach also ensures that each image's key is generated once. An image's key depends on the scrambling method boosting unpredictability, which also impacts growing entropy values. The pixel scrambling approach uses an S-box based on two chaotic mapping matrices and a specific scrambling algorithm to scramble the input binary values of each pixel, successfully breaking the relationship between neighboring pixels in an image. Fusing the pixel's low-bit information to update the image's details can avoid differential attacks and modern cryptanalysis. Finally, the system can work on all types of color images and all sizes as well as, to the best of our knowledge, representing the lowest computational complexity to date.

The article is divided into six sections. Section 2 features a literature survey of related works, section 3 has a brief background, section 4 discusses the proposed methods, section 5 contains results and discussion, and section 6 offers a conclusion.

II. RELATED WORKS

Image information comprises privacy and security, which indicates the importance of securing the online transmission of digital images. Thus, such images require encryption before they are sent [20]. Numerous image encryption techniques are in use, providing varying levels of security, but this article will focus on chaos-based encryption and S-boxes. One of the fundamental aspects of symmetric-key cryptography is the S-box, the design of which aims to break the bond between the encrypted message and the unidentifiable symmetric-key [21].

Using a hidden attractor chaotic system and the Knuth-Durstenfeld method, an author constructed an image encryption technique in paper [3]. Since it is an internal mixing algorithm, the Knuth-Durstenfeld approach has the least randomness and a simple design despite a low algorithmic space complexity. Finally, DNA sequence methods distribute image pixel values. The proposed method is designed on grayscale image data. However, when extended to a color image, it will extend execution time. Moreover, according to the results obtained by the authors, the resulting randomness in the image encoded by the entropy coefficient is considered low in comparison to the others. A 2D-SCMCI hyperchaotic map based on Cascade Modulation Couple (CMC) and two 1D chaotic maps was proposed in [6]. The significant dynamic performance and randomness in the 2D-SCMCI hyperchaotic map show that it is better suited for the image encryption method, although it only works with grayscale images. Modifying such a method to deal with color images will most likely multiply the encryption period many times because of forward and backward diffusion in this stage. Broumandnia [22] used diffusion and permutation of image pixels to develop an image encryption technique. The author proposes reversible chaotic maps for each of the two-dimensional and three-dimensional depending on modular mathematics. In this paper the cost of creating calculations and sequences goes up in ratio because it has complex topologies that include more parameters and variables. Moreover, the computational complexity has increased dramatically as a result of many chaos image encryption techniques confuses pixels by sorting chaotic series. The chaotic image encryption scheme is based on Galois fields shown in [23]. This method initially diffuses the original image using matrix multiplication operations, then scrambles the pixels using two chaotic maps. The expected consuming time will be higher when this approach is used on a color image.

To encrypt a color image, article [9] suggested a technique that Jointly Permutes and Diffuses (JPD) the pixels. Encryption methods are always constructed virtually by generating sequences from 4D hyperchaotic systems with positive Lyapunov exponents. Studies have shown that the JPD can withstand numerous types of attack, as evidenced by experimental results and security analysis. Although research has focused on separate permutation and diffusion methods, the findings have indicated that they pose a significant risk since they make it easier for attackers to crack the two processes independently. The JPD technique creates three auxiliary matrices, two index matrices and one mask array, to ascertain which pixels to process and how to process them. Such a requirement complicates the process and increases the time required to identify the pixel in question. Then, based on the auxiliary matrices, a feasible joint permutation and diffusion technique for color image coding are given.

A scrambling technique based on two chaotic sequences created via logic-sine coupling mapping in [24]. The transformation of a scrambled image into a one-dimensional series and then fusing the low-order bits between every two pixels to modify the detailed information of the image is feasible. Iterative logical mapping generates chaotic sequences for pixel replacement and ciphertext diffusion, respectively. The technique is safe and only works on grayscale images measuring 256×256. Although such a method increases the image's resistance against differential attacks, it is generally complicated and increases encryption time.

In [12], in this study, the LTMM-CIEA is built on a Two-Dimensional Logistic Tent Modular Map (2DLTMM) using a novel Color Image Encryption Algorithm (CIEA). The 2D-LTMM has more randomly distributed trajectories than previous chaotic maps utilized for image encryption. LTMM-CIEA comprises three processes: peripheral pixel blurring, cross-plane permutation and non-sequential scattering, resulting in a long consumption time. [25] Deals with a chaotic-based technique that aligns with chaotic map and wavelet transform features. This method uses a two-stage encryption technique. The initial step involved executing a process known as image diffusion. Moreover, by using the wavelet transform, hyperchaotic sequences could minimize the number of computations in confusion. The incompatibility with other file formats for encrypting, such as a color image or video and audio files, is a constraint of this work.

Using the Choquet Fuzzy Integral (CFI) and DNA methods, the paper [14] presents a unique strategy to develop the cryptographic characteristics of S-boxes. In terms of majority logic criteria, such as correlation, homogeneity, energy, entropy and contrast, the presented DNAFZ S-boxes have viable statistical characteristics. The limited number of DNA coding rules and DNA coding operations means numerous schemes fail to take full advantage of these rules, which, in turn, reduces the usefulness of employing DNA coding. Using the chaotic system, DNA computing, and a chess piece, [8] creates a unique image encryption method. Images are scrambled as they are entered, with random addresses being used for pixel shifts. Image Scrambler Using Castle (ISUC) routine is responsible for scrambling process. The castle moves at random on a hypothetical checkerboard of infinite size, with its location in each iteration determined by shifting pixels from the original image to its addresses in a scrambled image. Furthermore, it is DNA-encoded, so it is no longer a plain image. However, employing a chess piece for the scrambling operation can prove to be a hindrance because it limits the impact of eliminating the correlation that typically occurs between neighboring pixels in encrypted images.

[26] Uses a Binary Search Tree (BST) to construct a novel image encryption method. Using BST, which has adjustable length capabilities that improve security, can generate local and global encryption keys. Such a method is viable, but it expands the encryption process. Implementing Shannon's idea of diffusion and confusion required the sharing of the entire image contents to encrypt any byte of the original image. An image-encryption system based on triangle scrambling, DNA encoded data and the chaotic map has been implemented in [27]. The use of a master key of 320 bits generates a collection of sub-keys of 32 and 128 bits to encrypt the image blocks. Utilizing this approach shows its effectiveness because it protects the images from possible interception and misuse by foreign entities. However, the chaotic system

and DNA encryption approaches have numerous limitations, such as limited space and the inability to resist differential cyberattacks [25].

However, the aforementioned schemes do not always provide low computation cost or meet security requirements. This paper offers a simple color image encryption scheme with excellent security and low complexity to solve the computational cost concerns that exist in the literature. The algorithm uses color image data, S-box and hyperchaotic mapping. Such an approach not only increases the key space but also ensures that the key of each image is once generated. Moreover, the image encrypted in our way is unpredictable, making it impervious to differential attacks, thus ensuring the security of the encrypted image. In particular, our work presents a more lightweight encryption scheme compared to related work because it uses two low-processing complexities, a 1D Logistic map and 3D Hénon chaotic map to generate three key matrices in the encryption algorithm. The next step involves an XOR as lightweight process between each generation key matrix and the color image channels.

III. BACKGROUND

A. S-BOXES

Shannon first introduced the S-box design in 1949. An insecure nonlinear component also compromises the encryption standard. The ability of block ciphers is supported by the power of the S-box, which has been the subject of numerous attempts to improve its quality. Moreover, cryptographers have spent much time studying literature to analyze the characteristics of S-boxes.

In the block cipher structure architecture, the S-box is a crucial nonlinear module that confuses the relationship between ciphertext and secret keys [28]. In these cryptographic systems, the security is principally affected by the characteristics of the employed S-boxes. It must satisfy the following criteria: bijection, nonlinearity, output Bit Independence Criterion (BIC) and the Strict Avalanche Criterion (SAC). Viable S-boxes are those that meet the above criteria. Sensitivity to linear and differential cryptanalysis attacks represents another essential quality. In order to build cryptographically secured dynamic S-boxes, cryptography researchers have been interested in this topic [29].

S-boxes were employed in the structure of permutation encryption methods to play the role of fundamental nonlinear components and ensure that cryptosystems retain their confusing qualities [14]. The creation of S-boxes encompasses numerous conventional strategies. For instance, the random search procedure is a simple technique that generates S-boxes with lower cryptographic traits [30]. Nevertheless, the S-box has a crucial role in converting plain text or an understandable message into an encrypted form. Therefore, the creation of powerful S-boxes constitutes a significant source of concern for security analysts [28].

Remark 1: The primary aim of an S-box in this method is to cause confusion between the cipher image and the encryption key. In symmetric-key cryptosystems, reversible S-boxes play an influential part. Studies have found that in block ciphers (Substitution and Permutation), the stage is critical: a poor S-box means the encryption quality suffers.

B. CHAOTIC MAP THEORY

Matthew invented the chaos-based encryption approach in 1989. He explained the generation of chaotic series of random integers by using a simple nonlinear iterative function. Nine years later, in 1998, Fridrich used the Baker map to present a meristic block image encryption system, which was the first time parameters were introduced and discretized into a finite rectangular lattice of points to create a two-dimensional chaotic map [31]. Their instability and sensitivity to initiating conditions mean chaotic systems are used for randomization in cryptography [28]. Image cryptography uses different chaotic maps, and they are sensitive to seeds and control factors [32]. The following are examples of these types used in this paper:

1) Logistic map

The logistic map is a relatively manageable chaotic map with the following mathematical formula (1) [18]:

$$X_{n+1} = \partial X_n (1 - X_n), \tag{1}$$

Where $\partial\varepsilon$ [0,4] is called the logistic parameter, the logistic map works in a chaotic condition and presents a nonperiodic sequence when $\partial\epsilon$ [3.569946,4]. With (2), the map is quadratic and hence nonlinear [18]:

$$X_{n+1} = C X_n (1 - X_n), \tag{2}$$

Where C is the chaos behaviour control parameter, and to ensure X_n in the range [0, 1], parameter C must be in the range [0, 4] [18]. The X_n sequence is random and ranges between 0 and 1. X_0 = 0.1 and C = 3.9999 seem to be the initial values.

Remark 2: Although using one-dimensional logistic chaotic maps increases the efficiency of image cryptography algorithms, the approach has numerous drawbacks, such as simple chaotic actions and limited key space. A more complicated chaotic quality means more than one chaotic map was employed or mixed. Consequently, we used essential parameter values from a 1D Logistic chaotic map to reconstruct the 3d Hénon map.

2) Zaslavsky Map

George M. Zaslavsky (1978) first introduced this Two-Dimensional (2D) chaotic map [33]. The map exhibits deterministic dynamic behavior, which constitutes an integral part of the contemporary data encryption algorithms [34]. The 2D Zaslavsky map is defined as [35]:

$$X_{n+1} = mod(X_n + \beta(1 + \mu Y_n) + \alpha\beta\cos(2\pi X_n), 1), \tag{3}$$

$$Y_n = e^{-\Gamma}(Y_n) + \alpha\cos(2\pi X_n), \tag{4}$$

$$\mu = \frac{1 - e^{-\Gamma}}{\Gamma}, \tag{5}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3151174, IEEE Access

Whereβ, Γ, and α: are control parameters and e is exponentiation. The parameters setting values are: β =12.6695, Γ =3.0, α = 9.1 [35].

Remark 3: Increasing the number of parameters and the complexity of the 2D Zaslavsky map's structure heightens the quality of encoding because it enlarges the Lyapunov and improves its image encoding capacity. Consequently, the cryptographic procedure employed a 2D Zaslavsky map as part of the suggested S-boxes.

3) Hénon map

The Hénon map works with initial values, and it is extremely sensitive to those values, and using different parameters and initial values will generate different chaotic sequences with significant translations. Moreover, such circumstances indicate its suitability for generating cryptographic functions due to its ability to create viable chaotic sequences. It is also periodic and non-convergent, indicating its pseudo-randomness and unpredictability. For image encryption, the Hénon map can produce confusion and histogram uniformity [36]. The Hénon map exists in Three Dimensions (3D) as it relates to system equations (6), (7) and (8) [19]:

$$Y_{n+1} = a - Y_n^2 - bZ_n \tag{6}$$

$$Y_{n+1} = X_n \tag{7}$$

$$Z_{n+1} = X_n \tag{8}$$

This paper uses a=1.76 and b=0.1 [18], [37].

Remark 4: The three-dimensional Hénon map is used to enhance complexity during the key generation stage or S-box creation.

IV. PROPOSED SCHEME

The paper adopts two principles. Firstly, an S-box is created based on the Zaslavsky and Hénon maps. Secondly, a hyperchaotic key sequence is made by combining the Hénon map equation with obtained values by the Logistic map equation. The symmetric secret key production contained a hybrid form based on the 3D Hénon map and the Logistic map parameters. The sequence of the HyperLogVarHénon map was saved as a matrix. The matrix has split into three similar matrices. Finally, performing XOR generates a cipher image that acts as a lightweight operation between the scrambling image channels and the randomly created HyperLogVarHénon matrices.

A. S-BOX GENERATION

This work provides a novel way to block cipher inconsistency. The strong interdependence between chaos theory and cryptanalysis requires the creation of a new substitution box using two principal replacement chaotic maps. This technique will provide 256 keys for encryption. The S-box produced in this proposal is as follows: a hybrid S-box of two chaotic maps is created by generating the first half of the S-box (128 elements) from a 2D Zaslavsky map and the second half of the S-box (128 elements) from a 3D Hénon map.

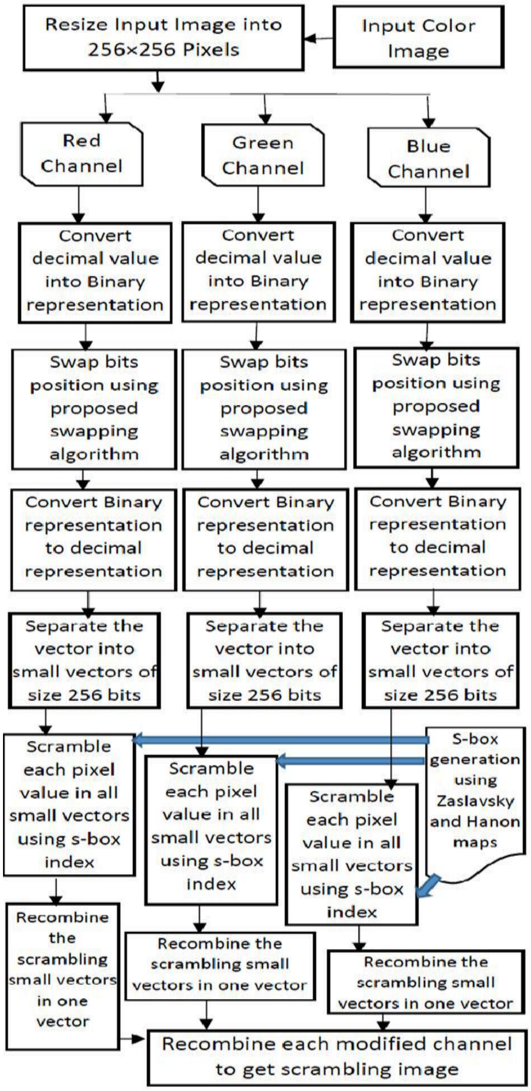

Resize Input Image into 256×256 Pixels
Input Color Image
Red Channel
Green Channel
Blue Channel
Convert decimal value into Binary representation
Swap bits position using proposed swapping algorithm
Convert Binary representation to decimal representation
Separate the vector into small vectors of size 256 bits
Scramble each pixel value in all small vectors using s-box index
S-box generation using Zaslavsky and Hanon maps
Recombine the scrambling small vectors in one vector
Recombine the scrambling small vectors in one vector
Recombine the scrambling small vectors in one vector
Recombine each modified channel to get scrambling image

FIGURE 1: **Scrambling image scheme**.

The secret key production was symmetric and contained a hybrid form based on the 3D Hénon map and the Logistic map parameters. The sequence of the key HyperLogVarHénon map is saved as a matrix split into three similar matrices. Finally, conducting an XOR operation between the scrambling image channels and the randomly created HyperLogVarHénon matrices obtains a cipher image.

Remark 5: In generating S-box values, we used 2D Zaslavsky map and 3D Hénon chaotic maps to add complexity during the development of these components and enhance the number of fundamental factors used to create the value stream while retaining a viable S-box generation time.

B. SCRAMBLING ALGORITHM

The scrambling is completed in two ways: the first involves scrambling each pixel's binary representation (bits), and the second involves scrambling each pixel's location using the S-box index (byte). Fig. 1 represents the Scrambling schema. A set of scramble steps is shown in algorithm 1:

Algorithm 1: Scrambling Algorithm

Begin

Input: Input color image of size $m \times n \times 3$.

Output: Scrambling image of size 256×256×3.

1) Resize the image to 256×256×3 pixels.
2) Divide the image into red, green, and blue channels.
3) Repeat the proposed swapping algorithm to the red, green and blue channels:
    - Convert each pixel value from decimal to binary representation
    - Combine all bits for each channel into a single vector
    - Separate the vector into small vectors of size 16 bits
    - Invert the first four values of the vectors (positions 1-4) by replacing them with the final four values (positions 13-16)
    - Recombine the small vectors to get a single vector
    - Convert the binary representation to decimal representation for every eight bits to obtain the pixels' value
    - Separate the vector into small vectors of 256 bits
    - Scramble each small vector value using an S-box index using the proposed S-box generation
    - Recombine the scrambling of small vectors to get a single scrambling vector
4) Recombine each modified channel to get a scrambling image.
5) Save the scrambling image of size 256×256×3.

End

C. ENCRYPTION ALGORITHM

The encryption process algorithm is shown in Fig. 2. Encrypting the scrambling color image first requires calculating the image's 256 hyperchaotic matrix value based on the Logistic and Hénon maps as the secret key.

The next step involves encrypting the scrambling image based on the XORed operation between the hyperchaotic matrix keys and scrambling image matrix. The specific steps are as follows (shown in algorithm 2):

Algorithm 2: Encryption Algorithm

Begin

Input: Scrambling image of size 256×256×3.

Output: An encrypted image of size 256×256×3.

1) Provide the 1D Logistic map's initial and parameter values.
2) Set the initial parameter values of the 3D Hénon map and adopt the Logistic map sequence as the 3D Hénon map's primary parameter values.
3) Compare the value location generated in a hybrid form based on the logistic equation (1) according to the following:

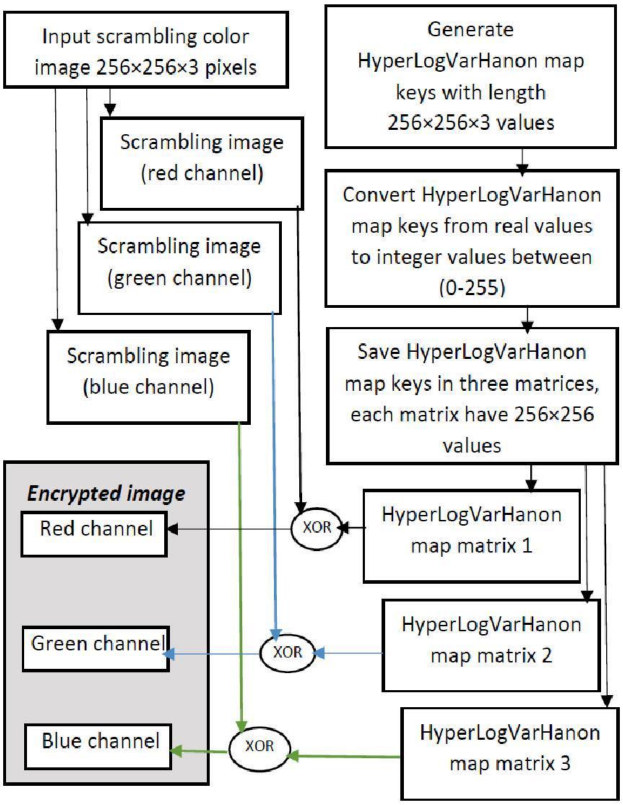
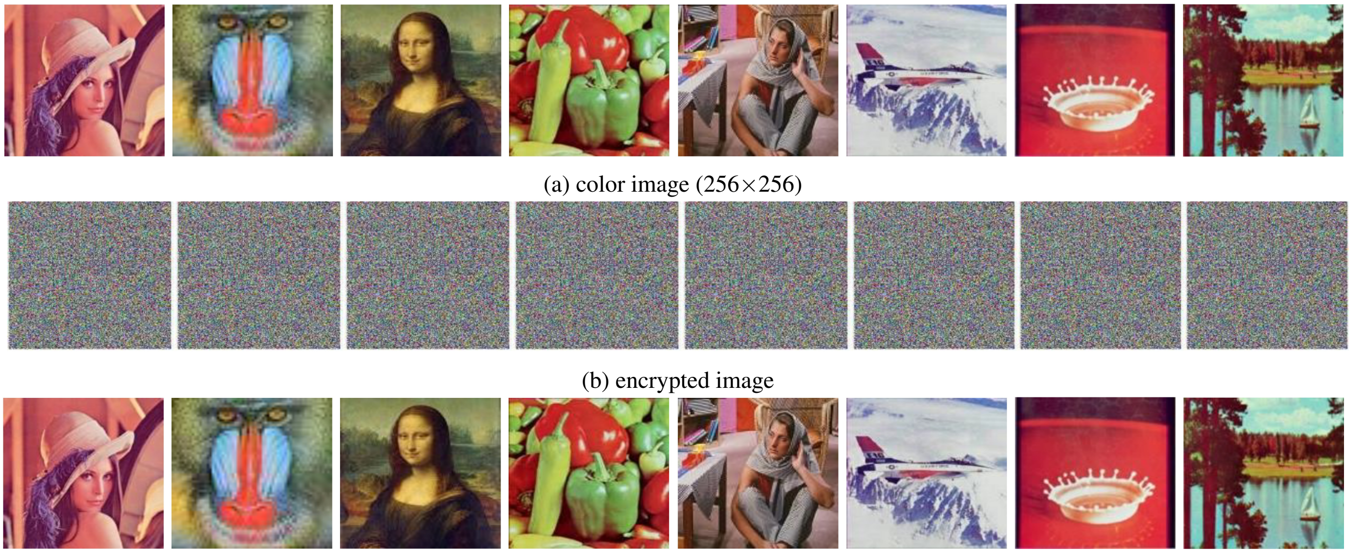

Input scrambling color image 256×256×3 pixels
Generate HyperLogVarHanon map keys with length 256×256×3 values
Scrambling image (red channel)
Convert HyperLogVarHanon map keys from real values to integer values between (0-255)
Scrambling image (green channel)
Scrambling image (blue channel)
Save HyperLogVarHanon map keys in three matrices, each matrix have 256×256 values
Encrypted image
Red channel
XOR
HyperLogVarHanon map matrix 1
Green channel
XOR
HyperLogVarHanon map matrix 2
Blue channel
XOR
HyperLogVarHanon map matrix 3

FIGURE 2: **Encryption image scheme**.

    - An odd position of value in the chaotic sequence requires adopting the output of the logistic map in (7)
    - An even position of value in the chaotic sequence requires adopting the output of the logistic map in (8)
4) Save the generating sequence keys in a matrix-named HyperLogVarHénon map with the length of 256×256×3 values. Further, the keys of the X_i result sequence are converted to an unsigned integer by multiplying components in the range 0 to 255 of the X_i by 255. Then the elements of the X_i value are rounded to the nearest decimal value. As a result, the acquired series is used to generate the primary key sequence.
5) Divide the HyperLogVarHénon map matrix into three matrices with a length of 256×256 values so that there is a key matrix for the red, green and blue channels.
6) A scrambling color image *I* of size 256×256 is read.
7) Split the image into red, green and blue channels, each of size 256×256 pixels.
8) Use XORs to scramble image channels with the randomly generated HyperLogVarHénon matrices matching the exact dimensions of the original image.
9) Convert the output into the standard value of RGB to resemble an encryption image.

End



(a) color image (256×256)

(b) encrypted image

(c) decrypted image

FIGURE 3: Simulation result.

D. DECRYPTION ALGORITHM

Deciphering, or decryption, fulfils the opposite role of encryption. The required key for use on the decipher side undergoes transmission via a secure channel. Creating the decipher series involves a similar process as the encryption phase pre-decryption. Algorithm 3 illustrates the method of producing the decryption image.

Algorithm 3: Decryption Algorithm

```
Begin
Input: An encrypted image of size 256×256×3.
Output: A decrypted image of size 256×256×3.

  1) Split the encrypted image into red, green and blue channels.
  2) XORs each encrypted image channel with the Hyper-LogVarHénon matrices of the original image.
  3) Repeat the proposed swapping algorithm to the red, green, blue channel:
      • Convert each pixel value from decimal to binary representation
      • Combine all bits for each channel into a single vector
      • Separate the vector into small vectors of size 16 bits
      • Invert the first four values of the vectors (positions 13-16) by replacing them with the final four values (positions 1-4)
      • Recombine the small vectors to obtain a single vector
      • Convert binary representation to decimal representation for every eight bits to obtain the pixels' value
      • Separate the vector into small vectors of size 256 bits
      • Descramble each small vector value using the S-box index and the proposed S-box generation
      • Recombine the descrambling of small vectors to obtain a single scrambling vector
  4) Recombine each modified channel to get a descramble image.
  5) Save the descrambling image of size 256×256×3.
End
```

V. RESULTS AND DISCUSSION

This part used eight 256×256×3 standard color images as input digital images to ensure the efficiency of the image encryption method. Fig. 3 shows eight sample images (Lina, Baboon, Mona Liza, Peppers, Barbara, Airplane, Splash and Sailboat) to illustrate the experimental results. The cipher image is an identical noise-like image, according to tests described and proven in subsections V.C (Histogram Analysis) and V.E (Information Entropy Analysis). Additionally, the original image and the cipher image that have no relationship are described and proven in subsections V.B (Correlation Coefficient Analysis) and V.G (Differential Attack Analysis). Moreover, the decrypted image shows high similarities to the original image. The findings indicate the proposed method's efficiency in reducing the average execution time of the encryption and decryption processes.

All tests were performed on MATLAB R2018a, while the encryption and decryption processes run on a computer with an Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz 2.59 GHz, with 16.0 GB RAM and 64-bit Windows 10 operating system. The use of correlation coefficients, differential analysis, entropy and histograms key space analysis in the

TABLE 1: **Key space comparison of the proposed scheme with the related work**.

Encryption Algorithm Scheme	Proposed Algorithm	[9]	[11]	[31]	[38]
Key Space	2^{430}	2^{186}	2^{326}	2^{600}	2^{497}

next subsections can help evaluate the proposed scheme's performance.

A. KEY SPACE

A well-designed encryption system should have sufficient key space to make brute-force cyberattacks impossible. The user-defined initial value of 1D logistic chaotic maps parameters is labelled C, an initial value of the 1D logistic chaotic map is marked Xn. The initial value of the 2D Zaslavsky map parameters is labelled Yn, and the control parameters are labelled β, Γ and α. Additionally, the 3D Hénon map initial value contains Zn, while the control parameters are named a and b.

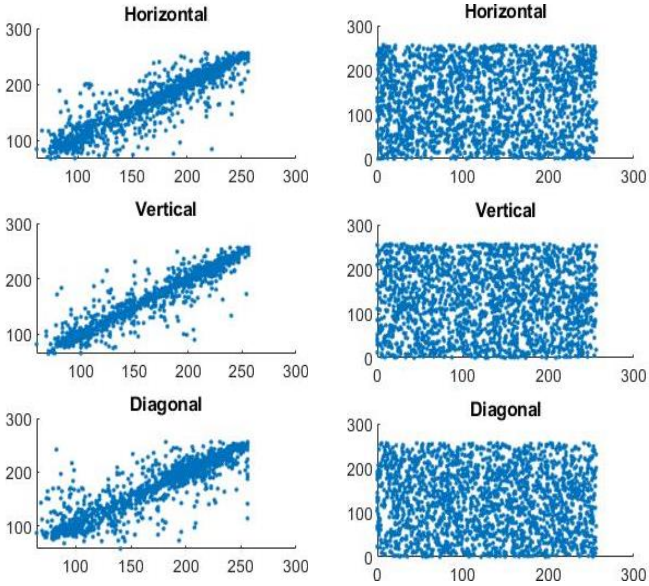
The proposed algorithm gives each of the nine values listed above a role as a major contribution to the security key. In this work, each floating-point number has a precision of 10^{-14}; thus, it contributes $10^{14} \times 9 = 10^{126}$ to the key space. The second contribution to increase the key space is made by the user key. The proposed system consists of eight subparts known as user keys. These user keys will be XORed with series keys called HyperLogVarHénon map. The user key is 256 bits long. It contributes 2^{11} to the key space. As a result, the suggested cipher's total key space would be as ample as $2^{11} \times 10^{126} \approx 2^{430}$. More time is taken by brute force attackers, the larger the key space. According to the existing research, if the size of the key space of a cryptosystem exceeds 2^{100}, it can effectively resist brute-force attacks by modern computers [8]. Thus, the proposed algorithm has sufficient key space to resist brute-force attacks. Table 1 lists the key space size of different available chaos cryptographic techniques.

According to the findings, the encryption method's key space is achieved as recommended in [8], although reference [31] has a higher key space, our proposed method achieves much lower encryption and decryption time as will be shown later in detail in the subsection V.F (Speed Analysis and Complexity).

B. CORRELATION COEFFICIENT ANALYSIS

The correlation coefficient covers the connection of two neighbors available at a particular bearing. A closer link between these two variables sees the correlation coefficient approach 1. Conversely, the value of the correlation coefficient approaches zero when they have a weaker relationship. The following formulae determine the correlation coefficient of neighboring pixels [27]:

$$Cr = cov_{x,y}/\sqrt{D_x}\sqrt{D_y}, \tag{9}$$



(a) input color image (b) cipher image

FIGURE 4: The correlation coefficient analysis.

$$cov_{x,y} = \frac{1}{T}\sum_{i=1}^{T}(X_i - E(X))(Y_i - E(Y)), \tag{10}$$

$$E(X) = \frac{1}{T}\sum X_i, D(X) = \frac{1}{T}\sum(X_i - E(X))^2, \tag{11}$$

X, Y indicate the corresponding pixels in the two images, cov(x, y), E(x) and D(x) refer to covariance, mean and variance, separately, and T represents the total number of image pixels. Fig. 4 shows the horizontal, vertical and diagonal correlations of the Lena unencrypted and ciphertext images using the described encryption technique to emphasize the correlation of adjacent pixels. It also shows before and after encryption, the correlation coefficients of different channels. As such, Fig. 4 illustrates the original and encrypted image adjacency pixels correlation. As shown in Fig. 4, the adjacency pixels correlation in the cipher image is sparse and in the input color image is almost linear. As a result, the suggested technique is impenetrable to various attacks. Table 2 summarizes the results.

C. HISTOGRAM ANALYSIS

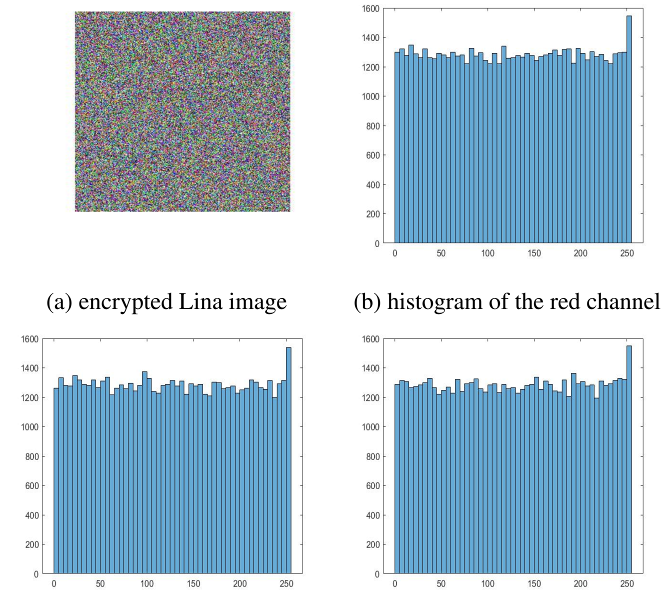
The image's histogram shows the distribution of intensity levels across its pixels. A histogram delineates the pixel distribution values, meaning the encrypted image's histogram requires an even distribution to avert statistical attacks [33]. Fig. 5 features the histograms for several images, including the ciphering image. The pixels in the ciphering images are uniformly well-distributed, resulting in a probability of occurrence for each intensity level closer to the equivalent.

D. SENSITIVITY TO SECURITY KEYS

Both encryption and decryption keys thwart incursions by third parties or neuromas that seek to decrypt the correctly

TABLE 2: **Image correlation coefficients**.

Image	Direction	Plain Image	Cipher Image	[27]
Lina	Horizontal	0.9460	0.0033	0.0012
Lina	Vertical	0.9720	0.0070	-0.0056
Lina	diagonal	0.9212	0.0027	0.0027
Baboon	Horizontal	0.9694	0.0025	0.0054
Baboon	Vertical	0.9635	0.0064	0.0006
Baboon	diagonal	0.9437	0.0035	0.0018
MonaLiza	Horizontal	0.9932	-0.0055	0.0096
MonaLiza	Vertical	0.9927	0.0051	0.0027
MonaLiza	diagonal	0.9866	0.0022	0.0014
Peppers	Horizontal	0.9715	-0.0020	0.0040
Peppers	Vertical	0.9774	0.00008	-0.0016
Peppers	diagonal	0.9479	-0.0064	0.0015
Barbara	Horizontal	0.9041	-0.00005	-
Barbara	Vertical	0.9259	0.0061	-
Barbara	diagonal	0.8830	0.0019	-
Airplane	Horizontal	0.9041	0.0034	-
Airplane	Vertical	0.9259	0.0013	-
Airplane	diagonal	0.8830	0.0019	-
Splash	Horizontal	0.9852	0.0062	-
Splash	Vertical	0.9871	0.0017	-
Splash	diagonal	0.9743	0.0023	-
Sailboat	Horizontal	0.9581	-0.0046	-
Sailboat	Vertical	0.9704	0.0049	-
Sailboat	diagonal	0.9352	0.0003	-



(a) encrypted Lina image

(b) histogram of the red channel

(c) histogram of the green channel

(d) histogram of the blue channel

FIGURE 5: Histogram analysis.

encrypted image. We set the parameters of the 1D Logistic map, 2D Zaslavsky map and 3D Hénon map by using a small handful for each one while keeping the other parameters of the keys constant in each test. Table 3 summarizes the results, which show the NPCR and UACI measures studied between the original image and the cipher image with the altered key. The Lina image was used to perform the test, and the result has been presented in Table 3. According to the findings, a tiny adjustment in the security keys' values produces randomized images indistinguishable as instructive objects. Consequently, we may infer that the suggested schema is sensitive to a minor change in the keys, resulting in different keys and encryption and decryption outcomes.

E. INFORMATION ENTROPY ANALYSIS

Information entropy assesses the image's confusion and can explain the variability of the source, as well as the average amount of information of all targets. Information entropy has an experimental value of 8, as mentioned in [36]. Indeed, the information entropy of pixel channels of the three colors is listed in Table 4, and the values achieved are all close to 8. Thus, the study found that the encrypted image is sufficiently random. Table 5 presents the entropy values of different encryption methods. Furthermore, the study shows that the encryption method presented in this work could approximate a random image in terms of encryption. We notice that the proposed work has an entropy value closest to 8 when compared to the references [11], [27], [31], [38], [39]. Such a situation occurs because the scrambling algorithm increases both the randomness and the entropy values.

F. SPEED ANALYSIS AND COMPLEXITY

The encryption algorithm's speed analysis represents a suitable method of determining the proposed technique's viability and assessing its performance in the field of image encryption. Table 6 displays the computed time for various images based on the encrypting and decrypting time of 256×256 color images. Table 7 describes the speed of the proposed encryption with most related reference methods.

We conclude that our methods have achieved the least time for encrypting and decrypting processed compared to the related methods, this achievement with the least possible complexity came from using 1D Logistic map, 3D Hénon map, and an XORed.

G. DIFFERENTIAL ATTACK ANALYSIS

A viable encryption algorithm should not be susceptible to various attacks, according to cryptography concepts. Consequently, when assessing the image encryption algorithm's sensitivity to differential attacks, the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) have become significant indicators [36]. They reflect the degree of change after adjusting a specific pixel value of the plaintext image at random and show the link between the number of changes in the encrypted image's pixel values and the change degree. Even the slightest change in the plaintext image's pixel value can substantially alter the ciphertext image, which indicates that the encryption technique has a high resistance to differential attacks [40]. Table 8 demonstrates that the use of three color images evaluated the performance of opposing various attacks, and the findings suggest that this work is highly reliant on the input original image to deal with differential attacks. The NPCR is higher than 99%, but the UACI is greater than 33%. Table 9 shows that our image encryption results are better than other encryption techniques. This work shows extreme sensitivity to the original image

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3151174, IEEE Access

TABLE 3: **Key sensitivity result (uses Lina image).**

Key	C=4$\times$10^{-12}	β=β $\times$ 10^{-12}	Γ=$\Gamma$$\times$10^{-12}	α=$\alpha$$\times$10^{-12}	a=a$\times$10^{-12}	b=b$\times$10^{-12}
NPCR	99.59411	99.60021	99.59564	99.59411	99.62056	99.58445
UACI	30.46642	30.39244	30.36747	30.51093	30.45054	30.37768

TABLE 4: **Information entropy result.**

Image Name	Lina	Baboon	MonaLiza	Peppers	Barbara	Airplane	Splash	Sailboat
Plain Image Entropy	7.75994	7.61280	7.38081	7.77491	7.64546	6.79310	7.34609	7.766048
Cipher Image Entropy	7.99918	7.99907	7.99910	7.99890	7.99910	7.99904	7.9992	7.99897

TABLE 5: **Comparison of entropy with another scheme.**

Encrypted Scheme	proposed algorithm	[11]	[27]	[31]	[38]	[39]
Entropy In Lina	7.99913	7.99750	7.94368	7.90263	7.99716	7.9987
Entropy In Peppers	7.99903	7.9973	7.95264	7.9999	7.99735	7.9987
Entropy In Baboon	7.99911	7.9970	7.98655	7.9999	-	7.9988

TABLE 6: **Encryption and decryption time.**

Image Name	Lina	Baboon	MonaLiza	Peppers	Barbara	Airplane	Splash	Sailboat
Encryption Time	0.3493	0.3495	0.3525	0.3493	0.3040	0.3011	0.3064	0.3207
Decryption Time	0.4411	0.3910	0.3992	0.4179	0.4101	0.4002	0.3771	0.4061

TABLE 7: **Speed analysis of proposed encryption with alternative reference strategies. (used Lina image).**

Operation	Image (256$\times$256) In Proposed Algorithm	Image (256$\times$256) In [9]	Image (256$\times$256) In [7]	Image (256$\times$256) In [31]
Encryption stage (second)	0.3493	0.42125	1.0612	0.8314
Decryption stage (second)	0.4411	2.12740	1.6291	4.2531

TABLE 8: **NPCR and UACI results of cipher images.**

Image Name	Lina	Baboon	MonaLiza	Peppers	Barbara	Airplane	Splash	Sailboat
NPCR	99.61937	99.62361	99.61344	99.60937	99.62158	99.61344	99.60886	99.61446
UACI	33.44153	33.82484	33.98317	33.83490	33.46354	33.55539	33.90233	33.15795

TABLE 9: **Comparison of the NPCR and UACI values of the Lina (256$\times$256) image.**

References	Proposed Algorithm	[11]	[27]	[31]	[38]	[39]
NPCR	99.6194	99.60	99.63	99.62	99.5965	99.59
UACI	33.4415	30.3348	30.51	33.52	33.4588	30.97

in dealing with differential attacks, as shown in Table 8 and Table 9.

H. NOISE ATTACK ANALYSIS

The encoded image frequently encounters various kinds of noise because it travels across realistic communication channels. Introducing this noise into the encrypted image causes significant issues, including the impossibility of rebuilding the original image from the transmitted encrypted image. Accordingly, the suggested algorithm should resist noise and find a solution to such issues. PSNR (peak signal-to-noise ratio) is employed. To assess the quality of the decrypted image following the assault, PSNR may be determined using the following formula [31]:

$$PSNR = 10 \times \log_{10}(\frac{MAX_1}{\sqrt{MSE}}) \tag{12}$$

$$MSE = \frac{1}{qp}\sum_{j=0}^{q-1}\sum_{k=0}^{p-1} \parallel M(j,k) - N(j,k) \parallel^2 \tag{13}$$

MSE is the mean squared error between the original and generated images; MAXI is the maximum image point colour value, displaying M(j,k) and N(j,k) pixel values for the plain and recovered images, respectively.

Table 10 computes and presents the PSNR value between the encrypted and plain images. The lower the digital in-

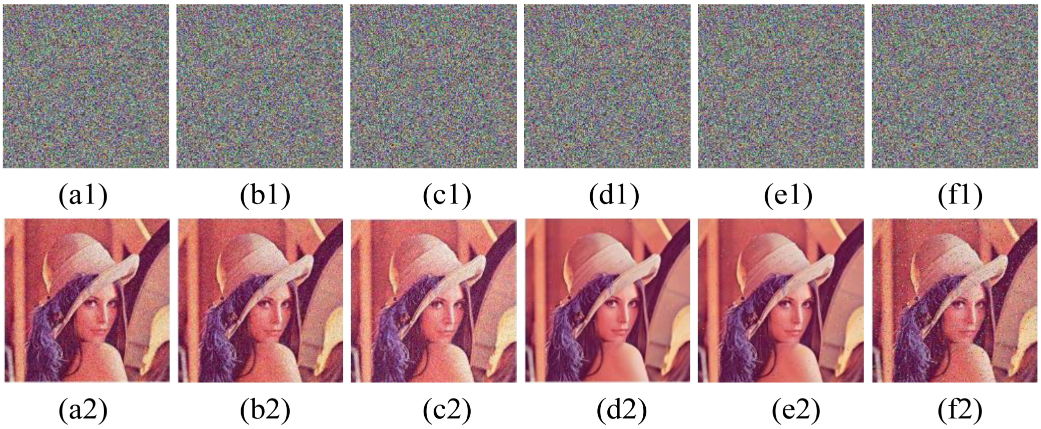


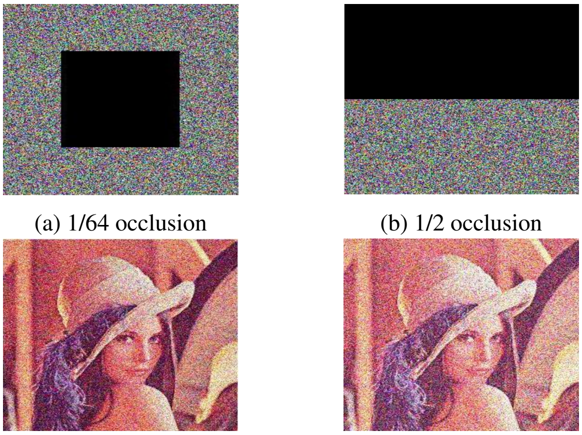
FIGURE 6: **(a1) Cipher image under 0.0005 Gaussian noise, (b1) Cipher image under 0.005 Gaussian noise, (c1) Cipher image under 0.05 Gaussian Noise, (d1) Cipher image under 0.0005 Salt and Pepper noise, (e1) Cipher image under 0.005 Salt and Pepper noise, (f1) Cipher image under 0.05 Salt and Pepper noise, (a2) Decipher image under 0.0005 Gaussian noise, (b2) Decipher image under 0.005 Gaussian noise, (c2) Decipher image under 0.05 Gaussian noise, (d2) Decipher image under 0.0005 Salt and Pepper noise, (e2) Decipher image under 0.005 Salt and Pepper noise, (f2) Decipher image under 0.05 Salt and Pepper noise**.

TABLE 10: **Quantitative measurement of Gaussian noise and Salt and Pepper noise attack resistance)**.

Noise Type	Gaussian Noise	Gaussian Noise	Gaussian Noise	Salt and Pepper Noise	Salt and Pepper Noise	Salt and Pepper Noise
Noise Intensity	0.0005	0.005	0.05	0.0005	0.005	0.05
PSNR In Proposed Schema	20.2103	20.1970	19.3401	37.2551	28.2713	18.0792
PSNR In [31]	20.2230	20.1964	19.3710	38.5802	27.9578	18.1261

TABLE 11: **After a data loss attack, the PSNR of the decrypted image**.

Occlusion	1/64	1/32	1/16	1/8	1/4	1/2
PSNR In Proposed Schema	26.1644	23.8930	20.8524	17.7929	14.6572	11.0323
PSNR In [31]	32.5454	21.8788	20.8054	15.6806	14.7826	7.7850



(a) 1/64 occlusion

(b) 1/2 occlusion

(c) decrypted image with 1/64 occlusion

(d) decrypted image with 1/2 occlusion

FIGURE 7: The encrypted images and their decrypted images after data loss.

formation loss, the greater the PSNR. According to Table 10, the encryption system can successfully counter a noise assault. Fig. 6 presents the outcome of adding two kinds of noise, Gaussian noise and Salt and Pepper noise, with varying intensities to the encrypted image, allowing retrieval of the original image. The decrypted images share a close association, and comparisons provide extremely positive findings, suggesting a strong connection between the deciphered and original images. Accordingly, it is possible to say that the proposed algorithm is anti-noise.

I. OCCLUSION ATTACK ANALYSIS

Employing the occlusion attack assesses recoveries of original images from encrypted images. Additionally, the use of statistical metrics, such as MSE and PSNR, can successfully estimate the original image from an encrypted image with a fixed amount of lost data. Fig. 7 depicts the multiple occlusions of the encrypted Lena image. Table 11 shows the statistical results of the recovery values per the recommended algorithm's occlusion assault. The approach shows its robustness and capacity to withstand occlusion assaults, as shown in Fig. 7 and Table 11.

VI. DISCUSSION

The experiments using eight color images referenced in [11], [27], [31], [38], [39] indicate a better value for the entropy coefficient in the proposed algorithm than the alternatives outlined in Table 5. Such a situation means the keys generated in the proposed scheme will add more randomness to their dependence on the hyperchaotic map during generation. The basis for this is that the chaotic maps employed in both types, namely, the Logistic 1D map and the Hénon 3D map, overlap. According to Table 9, the proposed technique can achieve a viable NPCR score in more test images than [11], [38], [39]. Additionally, the UACI scores are closer to the theoretical value of 33.4635% [14] in most images. Therefore, the proposed algorithm demonstrates its robust ability to defend the differential attack. Table 7 also shows the encryption and decryption speed provided by our work and techniques [7], [9], [31]. The findings show the significantly superior performance for the time calculated by the proposed algorithm. Such an occurrence results from the simplicity of the techniques employed in the coding stage represented by solely using S-box generation and exclusive OR operation. Of equal importance is the role played by the mixing stage in ensuring the removal of any link between the original image and the input image for the encryption process, which had the principal role of simplifying the proposed encryption stage.

VII. CONCLUSION

Transmitted images represent a significant problem in networking security. This security gap exposes many networks to attacks. The openness and vulnerability of the transmission to attacks show the importance of applying security to the transmitted image. Therefore, employing an image encryption technique secures this channel. Based on the hyperchaotic and S-box principles, the proposed method encrypts color images. Firstly, this study used the suggested swapping method to scramble each image binary pixel. The next step involved using a 2D Zaslavsky map and a 3D Hénon map to generate a new S-box that scrambles image pixels' positions. Lastly, the encrypted color image can be obtained using a XORed as a low-complexity operation between HyperLogVarHénon map keys (produced using a 1D Logistic map and a 3D Hénon map) and scrambling image pixels. The scrambling and encryption method can increase the anti-attacking capabilities, according to the performance test results.

Accordingly, the new chaotic system in the S-box and hyperchaotic keys generation mechanism described in this work behaves well in numerous tests and outperforms the encryption method. Moreover, the system can withstand extensive attacks and statistical analysis alongside being used to secure image information. Furthermore, it provides the lowest executing time compared with other related schemes. In future work, we want to apply DNA coding, a Quantum chaotic map of key sequence generating, with an encryption algorithm to further improve the efficiency of the encryption system.

ACKNOWLEDGMENT

This work is supported by Natural Science Foundation of Top Talent of SZTU(grant no.20211061010016).

REFERENCES

[1] A. A. Karawia and Y. A. Elmasry, "New encryption algorithm using bit-level permutation and non-invertible chaotic map," *IEEE Access*, vol. 9, p. 101357–101368, 2021.

[2] Z. A. Abduljabbar, H. Jin, A. Ibrahim, Z. A. Hussien, M. A. Hussain, S. H. Abbdal, and D. Zou, "Sepim: Secure and efficient private image matching," *Applied Sciences*, vol. 6, no. 8, 2016.

[3] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the knuth–durstenfeld algorithm," *Optics and Lasers in Engineering*, vol. 128, pp. 105–995, 2020.

[4] Y. Ma, N. Li, W. Zhang, S. Wang, and H. Ma, "Image encryption scheme based on alternate quantum walks and discrete cosine transform," *Optical Express*, vol. 29, no. 18, pp. 28–33, 2021.

[5] Z. A. Abduljabbar, A. Ibrahim, M. A. Hussain, Z. A. Hussien, M. A. A. Sibahee, and S. L. and, "Eeiri: Efficient encrypted image retrieval in iot-cloud," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 11, pp. 5692–5716, November 2019.

[6] J. Sun, "2d-scmci hyperchaotic map for image encryption algorithm," *IEEE Access*, vol. 9, p. 59313–59327, 2021.

[7] A. Momeni Asl, A. Broumandnia, and S. J. Mirabedini, "Scale invariant digital color image encryption using a 3d modular chaotic map," *IEEE Access*, vol. 9, no. 15, p. 102433–102449, 2021.

[8] N. Iqbal, "On the image encryption algorithm based on the chaotic system, dna encoding, and castle," *IEEE Access*, vol. 9, p. 118253–118270, 2021.

[9] T.Li, J. Shi, and D. Zhang, "Color image encryption based on joint permutation and diffusion," *J. Electron. Imag*, vol. 30, no. 01, p. 102433–102449, 2021.

[10] Y. Sha, Y. Cao, H. Yan, X. Gao, and J. Mou, "An image encryption scheme based on iavl permutation scheme and dna operations," 2021.

[11] S. Zhou, P. He, and N. Kasabov, "A dynamic dna color image encryption method based on sha-512," *Entropy*, vol. 22, pp. 964–975, 2020.

[12] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.

[13] R. M. Lin and T. Y. Ng, "Secure image encryption based on an ideal new nonlinear discrete dynamical system," *Mathematical Problems in Engineering*, vol. 18, p. 1–12, 2018.

[14] A. G. Mohamed, N. O. Korany, and S. E. El-Khamy, "New dna coded fuzzy based (dnafz) s-boxes: Application to robust image encryption using hyper chaotic maps," *IEEE Access*, vol. 9, p. 14284–14305, 2021.

[15] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[16] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[17] O. Reyad, Z. Kotulski, and W. M. Abd-Elhafiez, "Image encryption using chaos-driven elliptic curve pseudo-random number generators," *Applied Mathematics and Information Sciences*, vol. 10, pp. 1283–1292, 2016.

[18] A. K. A. Hassan, "Proposed hyperchaotic system for image encryption," *ijacsa*, vol. 7, no. 1, pp. 15–27, 2016.

[19] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using henon map, dynamic s-boxes and elliptic curve cryptography," *IEEE Access*, vol. 8, p. 194289–194302, 2020.

[20] H. Hu, Y. Cao, J. Xu, C. Ma, and H. Yan, "An image compression and encryption algorithm based on the fractional-order simplest chaotic circuit," *IEEE Access*, vol. 9, no. 3, p. 22141–22155, 2021.

[21] 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, no. 11, p. 26583–26592, 2021.

[22] A. Broumandnia, "Designing digital image encryption using 2d and 3d reversible modular chaotic maps," *Journal of Information Security and Applications*, vol. 47, pp. 188–198, 2019.

[23] ——, "Image encryption algorithm based on the finite fields in chaotic maps," *Journal of Information Security and Applications*, vol. 54, p. 102553, 2020.

[24] G. Shengtao, W. Tao, W. Shida, Z. Xuncai, and N. Ying, "A novel image encryption algorithm based on chaotic sequences and cross-diffusion of bits," *IEEE Photonics*, vol. 13, no. 1, p. 1–15, 2021.

[25] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," vol. 23, no. 3, p. 341, 2021.

[26] M. A. F. Al-Husainy, H. A. A. Al-Sewadi, and B. Al-Shargabi, "Using the binary search tree structure as key to encrypt images," *International Journal of Advanced Science and Technology*, vol. 130, no. 1, pp. 21– 32, 2019.

[27] H. M. Al-Mashhadi and I. Q. Abduljaleel, "Color image encryption using chaotic maps, triangular scrambling, with dna sequences," in *in 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, 2017, p. 93–98.

[28] A. S. Alanazi, N. Munir, M. Khan, M. Asif, and I. Hussain, "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes," *IEEE Access*, vol. 9, p. 93795–93802, 2021.

[29] B. B. Cassal-Quiroga, "Generation of dynamical s-boxes for block ciphers via extended logistic map," *Mathematical Problems in Engineering*, vol. 22, pp. 1–12, 2020.

[30] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of s-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimed Tools Appl*, vol. 80, p. 7333–7350, 2021.

[31] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, no. 11, p. 61334–61345, 2021.

[32] A. Firdous, A. U. Rehman, and M. M. S. Missen, "A gray image encryption technique using the concept of water waves, chaos and hash function," *IEEE Access*, vol. 9, no. 11, p. 11675–11693, 2021.

[33] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the zaslavsky chaotic map," *Information Security Journal*, vol. 25, no. 4-6, p. 162–179, 2016.

[34] F. J. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," *Procedia Computer Science*, vol. 93, no. 6, p. 816–823, 2016.

[35] D. Riadh and R. Shaker, "Implementation of gray image encryption using multi-level of permutation and substitution," *IJAIS*, vol. 10, no. 1, p. 25–30, 2015.

[36] J. Hao, H. Li, H. Yan, and J. Mou, "A new fractional chaotic system and its application in image encryption with dna mutation," *IEEE Access*, vol. 9, no. 19464126, p. 52364–52377, 2021.

[37] E. A. Albahrani and T. Karam, "A new key stream generator based on 3d henon map and 3d cat map," *International Journal of Scientific and Engineering Research*, vol. 8, no. 1, pp. 2114–2120, 2017.

[38] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and dna level," *Optics and Lasers in Engineering*, vol. 125, no. 1, p. 105851, 2020.

[39] I. Q. Abduljaleel, S. A. Abdul-Ghani, and H. Z. Naji, "An image of encryption algorithm using graph theory and speech signal key generation," *J. Phys*, vol. 1804, no. 1, p. 012005, 2021.

[40] P. Fang, H. Liu, and C. Wu, "A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks," *IEEE Access*, vol. 9, no. 18, p. 18497–18517, 2021.

ZAID AMEEN ABDULJABBAR received the bachelor's and master's degrees in computer science from University of Basrah, Iraq, in 2002 and 2006, respectively, and the Ph.D. degree in computer engineering from the Department of Computer Science and Technology, Huazhong University of Science and Technology, China, in 2017. His research interests include cloud security, searchable encryption systems, similarity measures, Internet of Things, secure computation, biometric, and soft computing. He has published regular articles for more than 40 IEEE International Conferences and High-quality articles in SCI journals, and he holds 3 international patents and 2 International Computer Software Copyright. He has always served as a Reviewer for several prestigious journals, and has served as the PC Chair/PC member for more than 25 international conferences. He has got the Best Paper Award that published in the 11th International Conference on Green, Pervasive, and Cloud Computing (GPC16), Xian, China, in May 2016. Also, he participated as a visiting scholar programme for international researchers to Huazhong University of Science and Technology and Shenzhen Institute in 2018 and 2019.

IMAN QAYS ABDULJALEEL received a B.Sc. degree in computer science from University of Basrah, Iraq, in 2002. She received an M.Sc. degree in computer science from University of Basrah, Iraq, in 2006. Her research interests the speech processing, data mining, and data hidden. She has been a professor in Departments: Computer Science, Computer Science and Information Technology College, University of Basrah-Iraq from 2003 to the present time.

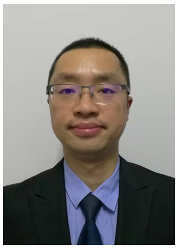
JUNCHAO MA is an associate professor in Shenzhen Technology University. He received B.Eng in Automation from Zhejiang University, China in 2006. He received M.Eng. in Department of Electronic and Information Engineering from The Hong Kong Polytechnic University, Hong Kong in 2007. He received Ph.D degree in Department of Computing from The Hong Kong Polytechnic University, Hong Kong in 2013. He worked in Huawei as a senior engineer from 2013 to 2020. His research interests are broadly in the fields of big data, interest of things, and wireless ad hoc and sensor networks.

MUSTAFA A. AL SIBAHEE is an Researcher at College of Big Data and Internet, Shenzhen Technology University, Shenzhen-China. Received his, Ph.D. 2018, from Huazhong University of Science and Technology, Wuhan-China. From April-2019 to March-2021, was a postdoctor at Shenzhen Huazhong University of Science and Technology, Research Institute, Shenzhen-China. His research interests include Computer Networks and Information Security, Internet of Things and Wireless Sensor Networks (WSNs).

VINCENT OMOLLO NYANGARESI received his bachelors degree in telecommunication and information engineering in 2010 and a masters degree in information technology security and audit in 2018. His first doctorate degree is in information technology security and audit. He is currently pursuing his second doctorate degree in computer science. His research interests include machine learning, computer networks and security protocols, telecommunication engineering and systems modeling. He has published over 40 research articles in peer reviewed journals, conferences and symposiums.

DHAFER G. HONI received the Bachelor's in 2013 and Master's degree in 2016 from University of Thi-Qar , iraq. His research interest in artificial intelligence, machine learning, deep learning, neural networks , computer vision, information security and medical image processing. He published many articles that indexed in Scientific Citation Index (SCI)and Scopus. Now He works as a rapporteur in Computer Sciences Department College of Education for Pure Science- University of Basrah, iraq.

AYAD I. ABDULSADA is a doctor in computer science. He was awarded the PhD degree in computer science from HUST University in 2013, his research is about searching the encrypted cloud data. He awarded the master degree in 2005 from Basrah University. The B.E degree was awarded in 2002. His research interests are: cryptography, searchable encryption systems, similarity search, information retrieval, record linkage, privacy preserving and data mining. He published many a regular scientific papers in the Computer Journal and the IEEE International Conference.



XIANLONG JIAO received the B.E., M.E. and Ph.D. degrees in computer science and technology from National University of Defense Technology, Changsha, China, in 2003, 2005 and 2011 respectively. He was an exchanging student with the Department of Computing, The Hong Kong Polytechnic University, Hong Kong, from 2009 to 2010. He was a post-doctor with the College of Information System and Management, National University of Defense Technology, Changsha, China, from 2012 to 2015, and was a lecturer with the Information and Navigation College, Air Force Engineering University, Xi'an, China, from 2015 to 2019. He is currently an assistant professor with the College of Computer Science, Chongqing University, Chongqing, China. His current research interests include the Internet of Things and information security. He is a member of the IEEE.

• • •