IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 March 2023, accepted 29 May 2023, date of publication 1 June 2023, date of current version 7 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3282160

RESEARCH ARTICLE

Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map of Fractional-Order and Hybrid DNA Coding

WASSIM ALEXAN[1,2], (Senior Member, IEEE), MOHAMED GABR[3], (Member, IEEE), EYAD MAMDOUH[4], RIMON ELIAS[5], (Senior Member, IEEE), AND AMR ABOSHOUSHA[4,6]

[1]Communications Department, Faculty of Information Engineering and Technology, German University in Cairo (GUC), New Cairo 11835, Egypt
[2]Mathematics Department, German International University (GIU), New Administrative Capital, Cairo 13507, Egypt
[3]Computer Science Department, Faculty of Media Engineering and Technology, German University in Cairo (GUC), New Cairo 11835, Egypt
[4]Physics Department, Faculty of Basic Sciences, German University in Cairo (GUC), New Cairo 11835, Egypt
[5]Digital Media Department, Faculty of Media Engineering and Technology, German University in Cairo (GUC), New Cairo 11835, Egypt
[6]Physics Department, Science Faculty, Cairo University, Giza 12613, Egypt

Corresponding author: Wassim Alexan (wassim.alexan@ieee.org)

ABSTRACT With advancements in computer and communication technologies, the production, utilization and applications of digital images is at an unprecedented rate. Recent applications include military communications, remote sensing, novel engineering designs storage and communications, as well as medical imaging. In most cases, such images convey highly sensitive or confidential information, which creates a strong need for the design of secure and robust color image cryptosystems. Recent literature has shown that fractional-order functions exhibit improved performance over their corresponding integer-order versions. This is especially true in their use in image processing applications. In this research work, we make use of a four-dimensional (4D) hyperchaotic Chen map of fractional-order, in conjunction with a sine chaotic map and a novel hybrid DNA coding algorithm. A thorough numerical analysis is presented, showcasing the security performance and efficiency of the proposed color image cryptosystem. Performance is gauged in terms of resilience against visual, histogram, statistical, entropy, differential, as well as brute-force attacks. Mean values of the metrics computed are as follows. MSE of 9396, PSNR of 8.27 dB, information entropy of 7.997, adjacent pixel correlation coefficient of 0, NPCR of 99.62%, UACI of 33, MAE of 80.57, and a very large key space of 2^{744}. The proposed image cryptosystem exhibits low computational complexity, as it encrypts images at a rate of 4.369 Mbps. Furthermore, it passes the NIST SP 800 suite of tests successfully. Comparison of the computed metrics of the proposed image cryptosystem against those reported in the state-of-the-art by counterpart algorithms show that the proposed cryptosystem exhibits comparable or superior values.

INDEX TERMS Chaos theory, chen hyperchaotic map, DNA coding, fractional-order, image cryptosystem, image encryption.

I. INTRODUCTION

In a parallel manner to the massive advances and complexity of modern wireless communication networks [14], [15] and big data applications [42], security issues have become of paramount importance [49]. Thus, developing and implementing protective data measures, such as cryptography [18], steganography [7], [20], watermarking [8], as well as their combinations [4], [58] has become at the core of current research efforts. Over the years, well-established cryptosystems were designed and deployed to protect all sorts of private and sensitive data. The Data Encryption System (DES), Triple DES, and Advanced Encryption Standard (AES) were among the most utilized and trusted

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

cryptographic algorithms. Nevertheless, it became apparent over the years that not all cryptosystems are suitable for multimedia like 2D and 3D images and videos. In essence, because images and videos have large amounts of data, high redundancy, and significant pixel cross-correlation. Thus, the field of image and video encryption has seen an expansive outburst in the literature of recent years. This literature on image encryption algorithms repeatedly shows the utilization of mathematical operations and constructs originating from chaos theory [5], [34], [37], [60], cellular automata [6], [22], DNA encoding [28], [44], [53], [54] and electric circuits [12], [38].

For the most part, techniques for encrypting color images follow Shannon's ideas of data security, carrying out confusion and diffusion of pixels. Confusion is the process of altering the arrangement of pixels without altering their value. On its own, this process does not produce adequate encryption results. Recent literature shows a typical scenario, where bit-confusion is paired with a bit-diffusion process, which modifies the pixel values based on particular mathematical operations to enhance security. A confusion stage causes each bit in an encrypted image to depend on many sections of the key, thus concealing the relationship between the two [47]. However, a diffusion stage adds an avalanche effect, in which a change of a single bit in the plain input image results in a change of approximately half of all the bits in its encrypted version. The goal of diffusion is to eradicate any statistical association between a plain input image and its encrypted version. Chaotic functions come into play during the construction of these 2 stages of encryption. Primarily, because a number of inherent qualities of chaotic functions make their application desirable in relation to communication and data security. These features include, among others, sensitivity to initial conditions, ergodicity, pseudo-randomness, control parameters, and periodicity [35]. In addition, the key space created by the many chaotic systems is vast. Because of their ability to enhance the effectiveness of encryption techniques, several chaotic systems are frequently found to be used in color image encryption literature. In principle, chaotic functions are categorized as either low-dimensional (LD) or high-dimensional (HD). The selection of one class of chaotic functions over the other for use in image cryptosystems is always a compromise between complexity and security. Low-dimensional chaotic functions offer simple software and hardware implementations with an adequate level of security. This makes them an optimum choice for applications requiring real-time image encryption efficiency. High-dimensional chaotic functions, on the other hand, provide enhanced security at the expense of more complex designs and implementations [23].

To a great extent, cryptosystems designed utilizing LD chaotic functions employ multiple such functions, in a concatenated or iterated fashion. For example, the authors of [52] combine the 3 principal channels, Red, Green, and Blue, to convert a color image into a single bit-level image. The resulting image was then distorted using a skew tent map. A chaotic coupled-sine map was developed by the authors of [59]. Their proposed map is employed to scramble colored images. But since LD chaotic systems are characterized by a basic structure, their key space is limited, resulting in a comparatively poor level of security. To overcome this, in [19], the authors propose utilizing a number of enhanced one-dimensional chaotic maps, including the logistic map, the sine map, and the Chebyshev map in conjunction with an improved Hill cipher, for the encryption of both grayscale and RGB images. Such an idea of designing cryptosystems that can handle different image types was also proposed in [31] for medical images, whereby the proposed algorithm is based on image blocks and the logistic chaotic map.

On the other hand, HD chaotic functions are distinguished by structures that are more complex, as well as having inherently numerous parameters. Such characteristics allow HD chaotic functions to overcome the shortcomings of LD functions. The authors of [38] carry out color image encryption with dynamic DNA and four-dimensional (4D) memristive hyper-chaos. In [62], a novel color image cryptosystem based on dynamic DNA coding, a six-dimensional (6D) hyperchaotic system, and image hashing is proposed. While the authors of [32] proposed a minimax differential evolution-based seven-dimensional (7D) hyperchaotic map to carry out color image encryption. The authors of [45] designed a novel three-dimensional (3D) chaotic map by combining piece-wise and logistic chaotic maps, which they employ in numerous applications of information security. An interesting work is proposed in [66], where chaos theory, in terms of a five-dimensional (5D) hyperchaotic system, is made use of in conjunction with quantum theory. The literature clearly shows a reliance on chaos theory for designing secure and robust image cryptosystems. However, it is also clear that for the most part, chaos theory is combined with one or more mathematical constructs, for improved security performance.

DNA cryptography utilizes both biological and computational features to offer additional confidentiality over standard cryptographic algorithms while encrypting data [46]. Traditional image encryption algorithms frequently provide one layer of security, and it is possible that their secrecy is destroyed as the underlying computational procedures are made public. On the contrary, DNA cryptography exploits the self-assembling characteristics of DNA bases in tandem with a cryptographic technique to offer various security measures that boost the degree of achieved data secrecy [28]. Using amino acid tables, for instance, the authors of [44] translate ciphertext to a genomic form. The tables' protein sequence composition add to the ciphertext's level of uncertainty. In [53], the authors present a DNA encoding technique that is based on a distinctive string matrix data structure yielding distinctive DNA sequences. They apply these sequences to encode plaintext as DNA sequences. Some scholars have also made use of DNA sequences in the design of S-boxes for image cryptosystems, such as in [3] and [46]. The next

paragraph discusses the importance of an S-box as a building block in image cryptosystems.

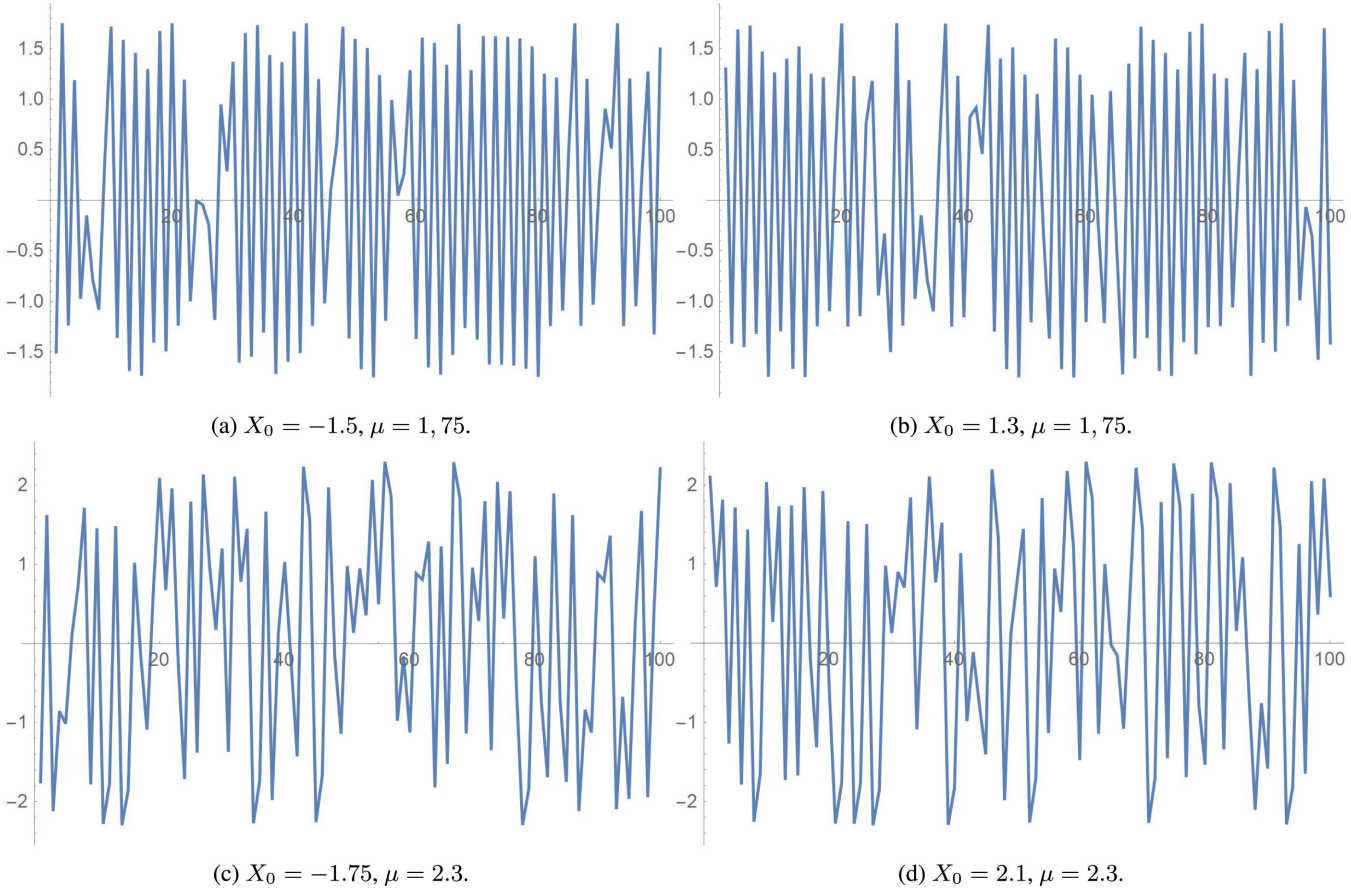
S-boxes are a fundamental component of modern block image encryption algorithms. An S-box facilitates the conversion of any given plaintext to ciphertext. Shannon's confusion property is provided by adding an S-box to a cryptosystem, which results in a non-linear translation between input and output data [47], as well as the removal of fixed points (thus, resisting any cryptanalysis efforts). The more uncertainty and variability provided by an S-box, the more secure it is. For many block image encryption algorithms, the level of security provided by one or more S-boxes correlates closely with their resistance to attacks. Although such algorithms may include multiple stages, an S-box is often the only non-linear stage that improves the security of confidential data. For an S-box to be acceptable for real-time data encryption, its design must be efficient and simple. Recent publications provide numerous examples of the design and implementation of S-boxes in image cryptosystems. For instance, the authors of [37] presented an S-box employing a nonlinear digital filter of the third order. Using a unique optimization strategy, its nonlinearity was improved. The authors of [51] proposed an optimization algorithm for a chaos-based entropy source to design their S-box. In [3], a DNA based S-box is constructed and utilized as part of AES. The conducted NIST analysis showcases its robustness and achieved level of security. A similar NIST analysis was conducted by the authors of [39] to gauge the robustness of their proposed S-box design. In [39], the design is based on a chaotic affine transformation. This involves the utilization of the nonlinear trajectories of the Logistic map to generate rotational matrices for the S-box generation. The authors of [40] propose a novel chaotic map, which they prove its chaotic behavior through various bifurcation and Lyapunov exponent plots, then utilize it to generate a robust S-box for image encryption.

To guarantee protection against known plaintext attacks, the literature provides multiple examples of image cryptosystems with several encryption stages [10], such that an S-box is always adopted as one of the inner stages, to ensure satisfying Shannon's concepts of confusion and diffusion. The authors of [21] propose one such instance of a 3-stage cryptosystem. In their proposed work, an S-box is the core stage, sandwiched between the application of 2 encryption keys. The first key is a Mersenne Twister-based pseudo-random number generator (PRNG), while the second key is a tan variant of the logistic map. The authors of [17] employ a similar strategy, constructing a PRNG-based S-box using Wolfram Mathematica® and employing the Rossler system and the Recaman's sequence for each encryption key. In [22], the first encryption stage involves the product of a plain image's pixel values with PRNG values, followed by an S-box application, and finally an XOR operation with a cellular automata generated key.

The integration of DNA cryptography with chaotic functions and S-boxes in image cryptosystems has attracted the interest of scientists and engineers in an effort to achieve better performance [67], either in terms of enhanced security or reduced computational complexity (thereby reducing encryption and decryption times). Based on a combination of chaotic maps and DNA sequences, the authors of [57] proposed a color image encryption algorithm that is shown to be highly resistant to statistical and brute force attacks. The authors of [13] proposed an image cryptosystem which combines the utilization of a 2D Henon-Sine map, DNA coding and an S-box. Their S-box is generated through random DNA coding operations. Parallel compressive sensing, chaos theory, and DNA encoding are jointly employed in an algorithm proposed in [54]. An iterative approach is utilized by the authors of [29] who provide a grayscale image encryption algorithm combining a 4D chaotic system with the hash algorithm SHA-2, DNA encoding, and the random movement of the Castle chess piece. A more advanced hashing protocol (SHA-512) is employed by the authors of [43], in conjunction with DNA encoding and numerous hyperchaotic maps. Moreover, their proposed algorithm also employs a logistic-tan map and a Zaslavskii map based pixel-shifting technique. A solid research work is presented in [46], where its authors proposed a novel S-box design that is based on DNA encoding and a 4D hyperchaotic system. In [23], the authors make use of a tan variation of the logistic map to carry out DNA encoding in the first encryption stage. Their second stage employs the numerical solution of the Lorenz chaotic system of differential equations, in conjunction with a linear descent algorithm to build an S-box. In their last stage, the logistic map in its original form is utilized to make a low-complexity encryption key.

Very recent literature on image processing in general, and on image cryptosystems more specifically, points out to the fact that the performance of fractional-order polynomials and functions is superior to their integer-order counterparts. This is discussed in [11], where the authors showcase better bacterial species recognition, in [33] where the authors describe improved plant disease recognition, as well as in [16] where the authors provide details of machine learning image-based COVID-19 diagnosis. More specifically, the authors of [27], propose an image cryptosystem that makes use of a 4D hyperchaotic Chen system of fractional-order combined with a Fibonacci Q-matrix. Their proposed algorithm is shown to exhibit exceptional security and robustness features, in addition to a large key space.

The previous paragraphs have attempted to summarize the importance and need for image cryptosystems, as well as provided a short and recent literature review on the topic. From this literature review, it can be summarized that recently proposed image encryption algorithms are characterized by: a) the utilization of bit-confusion or bit-diffusion stages, instead of both; b) A focus on increasing an algorithm's security at the expense of its efficiency, thus sacrificing its ability for real-time applications; and c) Mostly utilize integer-order instead of fractional-order hyperchaotic maps. In this research work,



(a) $X_0 = -1.5, \mu = 1,75.$ (b) $X_0 = 1.3, \mu = 1,75.$

(c) $X_0 = -1.75, \mu = 2.3.$ (d) $X_0 = 2.1, \mu = 2.3.$

FIGURE 1. First 100 elements in the recursive sequence produced by (1) for different X_0 and μ values.

the contributions of the proposed image cryptosystem are as follows:

1) A multistage RGB image cryptosystem is proposed. The first stage utilizes a simple Sine chaotic map. The second stage utilizes a 4D Chen hyperchaotic map of fractional-order, and the third stage utilizes a novel hybrid DNA coding algorithm.
2) The proposed cryptosystem is highly robust and secure, capitalizing on both security ideas of Shannon, bit-confusion and bit-diffusion [47].
3) The proposed cryptosystem is thoroughly tested against a plethora of visual, entropy, differential, statistical, known plain text and brute-force attacks, to gauge its performance in terms of security, efficiency, robustness and overall resilience against cryptanalysis.
4) Being built on multiple stages that in total utilize 14 variables, the key space is enlarged to 2^{744} effectively resisting brute-force attacks.
5) It is an efficient and fast encryption scheme, encrypting images in only 0.032 s for an image of dimensions of 256×256, achieving an average encryption rate of 4.369 Mbps.
6) The proposed image cryptosystem is shown to succeed at passing the NIST SP 800 full suite of randomness tests.

The rest of this research work is organized as follows. In Section II, we provide the preliminary mathematical constructs utilized in the proposed cryptosystem. In Section III, we describe the sequence of the proposed cryptosystem. In Section IV, we compute multiple performance evaluation metrics and present the results of the computations with respect to various visual and mathematical analyses. In Section V, we draw the conclusions of this research work and suggest a couple of future research directions.

II. PRELIMINARY OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The proposed image cryptosystem is based on a LD and HD chaotic maps, as well as a hybrid form of DNA cryptography. These are presented next.

A. THE SINE CHAOTIC MAP FOR KEY GENERATION

The sine chaotic map is a recursive map with a single dimension which generates sequences with chaotic behaviour [24]. The recursive formula for the sine chaotic map is given by the expression

$$X_{n+1} = \mu \sin(\pi X_n). \tag{1}$$

As a recursive definition, it comes as an inherited property that a generated sequence is highly affected by the scale factor

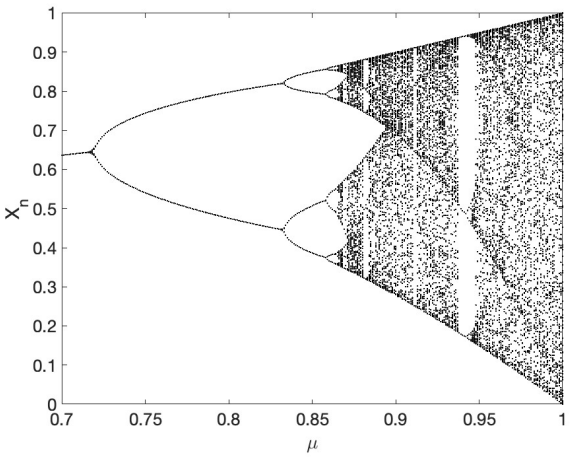


FIGURE 2. Bifurcation diagram of the Sine chaotic map.

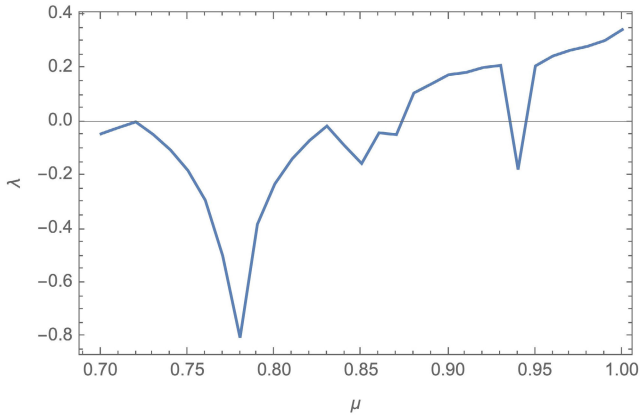


FIGURE 3. Lyapunov exponent diagram of the Sine chaotic map.

present in the definition, and the initial value. In the case of this definition, the scale factor, namely μ, should be assigned a value greater than 1. Accordingly, the initial value X_0 is to be assigned a value within the range $[-\mu, \mu]$. Fig. 1 shows some examples for the first 100 iterations of the sine map given different values for μ, and X_0.

In addition to the previously demonstrated examples, further confirmations are performed through plotting the bifurcation diagram and the Lyapunov exponent, as shown in Fig. 2 and Fig. 3, respectively. It is worth noting that the shape and bifurcation behavior is rather similar to that of the Logistic map, both in its original form, as well as in its tan variant (that is utilized in [23]).

Considered to be a LD chaotic system, as previously established, such a system comes with a small key space, which is resulting from having only 2 control variables, μ and X_0. In order to compensate for this drawback, as demonstrated later in more detail, the other components (used in other stages forming the overall proposed encryption technique) contribute to yielding a large key space as a result of using more control parameters. However, as such a system relies only on a single dimension producing well-evaluated chaotic sequences (as discussed above), it proves to be advantageous to produce such sequences (performing a full stage in the encryption technique) in a low cost manner. In other words, since the calculation of a sequence relies on a single-dimension recursive definition, the time and space complexities for such a process are linear with respect to the size of the sequence needed. Such linear correlation proves to be useful as the demanded sequence is of the same size of an image's bit-stream size, which is usually considerably large ($1,572,864$ bits for an RGB image of dimensions 256×256) [55].

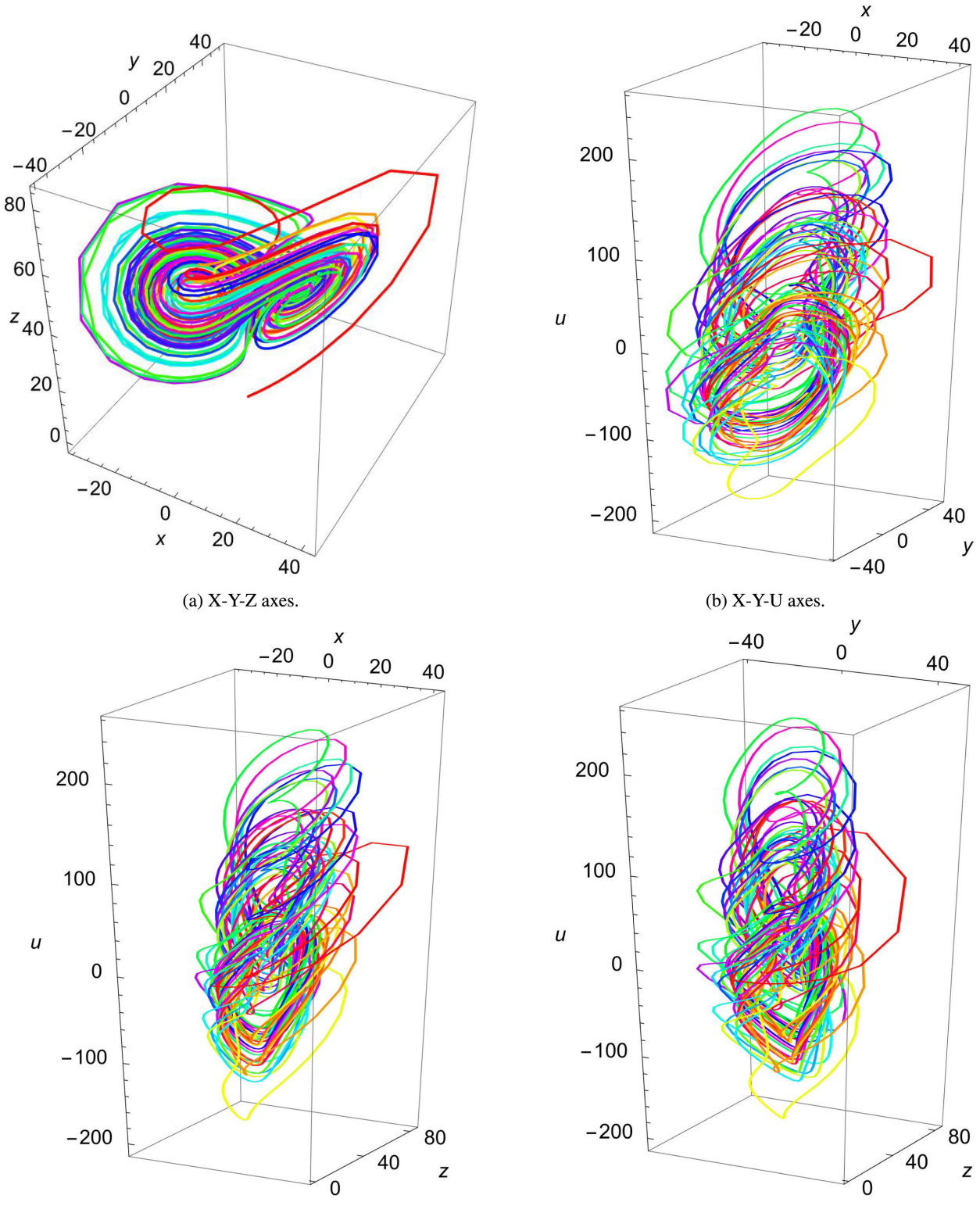
B. THE 4D HYPERCHAOTIC CHEN SYSTEM OF FRACTIONAL-ORDER FOR S-BOX GENERATION

As confusion is demanded in any image encryption procedure, the involvement of an S-box comes as a natural step. Beside confusion, in this work, this step is accompanied by an additional improvement to the quality of the overall encryption technique. Such improvement comes in terms of increasing the key space of the encryption as a whole. Hence, a seed-based randomly generated S-box using the 4D hyperchaotic Chen System of a fractional order is utilized. Since chaotic functions are preferred for creating PRNG sequences (later transformed into an S-box), hyperchaotic functions are a logical next step of evolution. This is evident as hyperchaotic systems are typically characterized as chaotic systems with more than one positive Lyapunov exponent. Beside that, the fractional order 4D Chen system introduces the involvement of many control variables, serving the target of increasing the key space. Moreover, the Chen system allows for a good balance in terms of possessing a high ergodicity and an improved distribution in phase space, while still exhibiting an acceptable computational complexity. These qualities become very clear upon comparing the Chen system to, for example, the Lorenz system [6] which possesses a comparatively poor ergodicity, or even the hyperchaotic memristor circuit with its transcendental non-linearities and complexity in terms of software implementations [41].

The hyperchaotic fractional order 4D Chen system is equated as per the following four equations (for x, y, z, and u respectively) [26]:

$$D^{\alpha}x = a(y - x) + u \tag{2}$$
$$D^{\alpha}y = \gamma x - xz + cy \tag{3}$$
$$D^{\alpha}z = xy - bz \tag{4}$$
$$D^{\alpha}u = yz + du \tag{5}$$

In (2), (3), (4), and (5), the control variables are divided into 3 groups. The first group, the initial values for x, y, z, and u, (or x_0, y_0, z_0, and u_0), are the start values assigned to each axis separately. The second group, a, b, c, γ, and d, are the scale coefficients for the equations. Finally, α is the differential order. These 3 groups combined introduce a total of 10 variables. For demonstration, Fig. 4 shows an example plot for the fractional order 4D Chen system. Moreover, the system's hyperchaotic behavior may be analyzed by visually



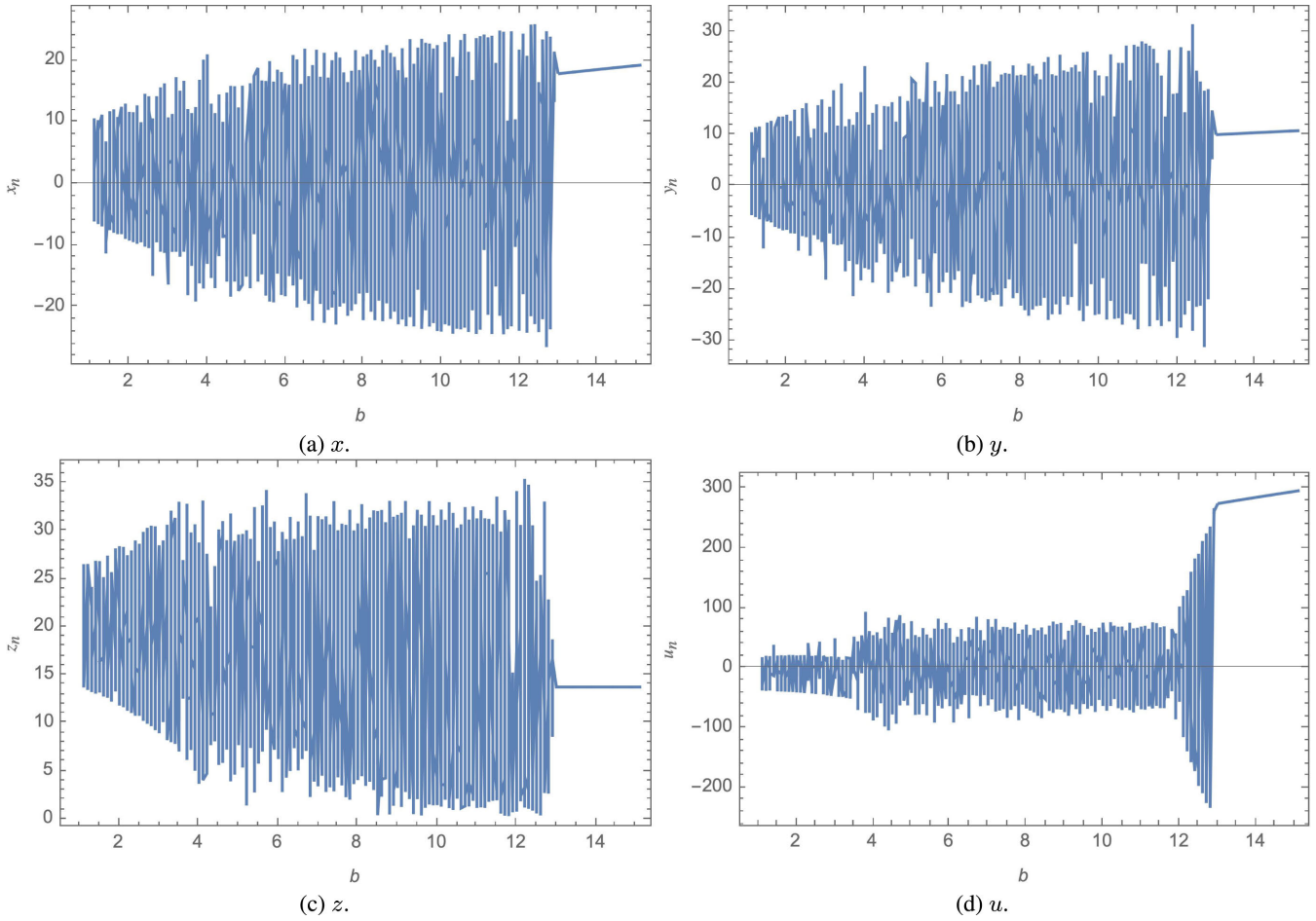
(a) X-Y-Z axes.

(b) X-Y-U axes.

(c) X-Z-U axes.

(d) Y-Z-U axes.

FIGURE 4. 3D plots for the fractional order 4D Chen system over different combinations of axes where $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$ (the system is calculated in the 4D space, hence initial values are needed for the four axes. However, for plotting purposes, one axis is ignored in each illustration).



(a) x. (b) y. (c) z. (d) u.

FIGURE 5. Bifonal order 4D Chen system for x, y, z and u against b.

Algorithm 1 Generate S-Box Given S and L

1) $L = [0 - 255]$
2) $n = 0$
3) $i = S_n\%Length(L)$
4) append $L[i]$ to S-box
5) delete $L[i]$ from L
6) $n = n + 1$
7) if $n <= 256 : GoTo(2)$

examining its corresponding bifurcation plots against different parameters, as respectively shown in Fig. 5 and Fig. 6, for b and c. Furthermore, the 4 Lyapunov characteristic exponents (LCEs) are plotted in Fig. 7. These showcase the rate of exponential divergence from perturbed initial conditions.

Towards generating an S-box given a set of 10 keys, the fractional order 4D Chen system is numerically solved, resulting in a 4D geometry, as demonstrated in Fig. 4. Next, the x, y, z, and u coordinates of each point in the solution are flattened into a single 1D array as follows:

$$\{\{x_0, y_0, z_0, u_0\}, \{x_1, y_1, z_1, u_1\}, \{x_2, y_2, z_2, u_2\}, \ldots\} \rightarrow \{x_0, y_0, z_0, u_0, x_1, y_1, z_1, u_1, x_2, y_2, z_2, u_2, \ldots\}. \quad (6)$$

Given this flattened sequence, the median is calculated, which is then used to turn the sequence into a bit-stream by using:

$$bitStream_i = \begin{cases} 1, & \text{if } sequence_i \geq median \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

Using a set of 2048 bits, each 8-bits are used to form a decimal number in the range [0, 255], forming a list of size equal to 256. Given a list L of 256 numbers (unsorted and containing repeated numbers), alongside a sorted set S $\{0 - 255\}$, the S-box is constructed in constant time using the procedures of Algorithm 1. For example, using the keys $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$, the first 8 bits in our generated bit stream are given by $\{0, 0, 0, 0, 1, 1, 1, 0\}$. On converting them into a decimal number, we get 14, which is the first entry in the S-box, shown in Table 1.

As an example, given seed values of $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$, the generated S-box is as shown in Table 1.

As a 4D system, it is expected that the computation cost of such a system would be high in terms of time and required memory allocation [55]. In the scope of this work, this is

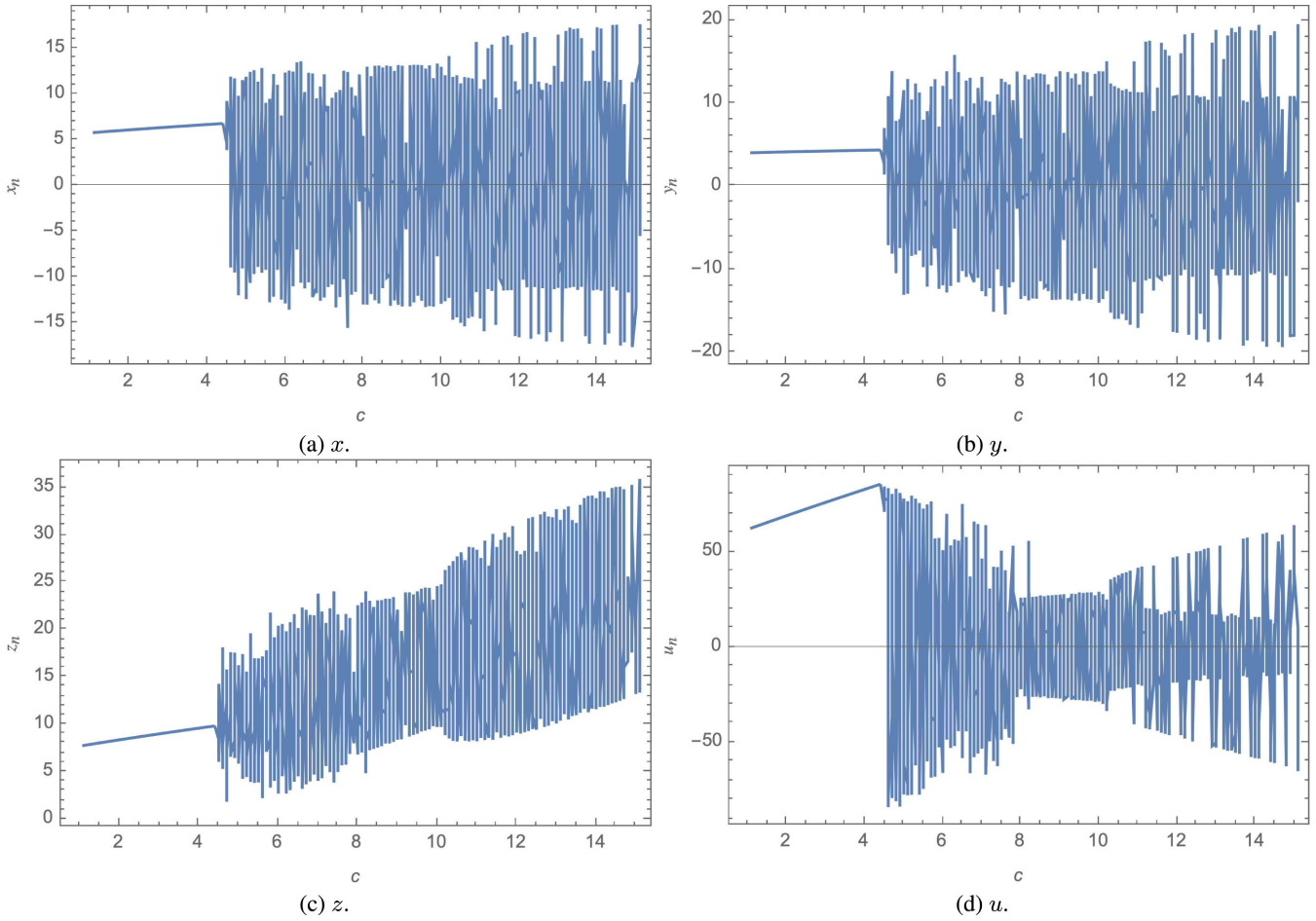


FIGURE 6. Bifurcation plots of the fractional order 4D Chen system for x, y, z and u against c.

TABLE 1. 4D hyperchaotic Chen system of fractional-order based S-Box using the keys $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$.

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

not the case, as it is used to generate a fixed-size set of bits (precisely, 2048 bits). Accordingly, the computation of such a step comes at a constant cost. On the other hand, the main advantage presented by this representation of the S-box is the addition of 10 keys, which in turn vastly improves the key space of the overall image cryptosystem. A full security analysis of the proposed Chen system based S-box is provided in detail in Section IV-M, alongside a comparison with state-of-the-art S-boxes.

C. HYBRID-OPERATIONAL DNA CODING

Research on DNA computing, in which DNA is used as an information carrier, gave rise to the innovative field of DNA cryptography. Within the DNA domain, the image will

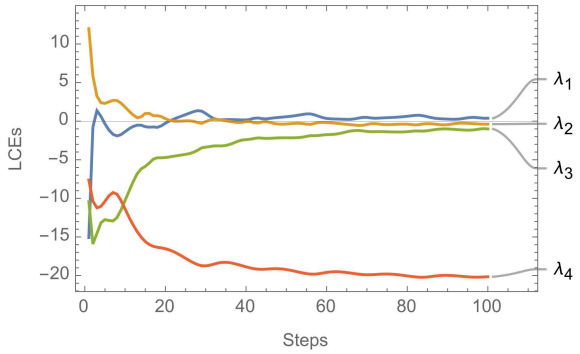


FIGURE 7. A plot of the 4 Lyapunov characteristic exponents of the fractional order 4D Chen system.

TABLE 2. DNA to bit pairs assignment permutations.

Rule	1	2	3	4	5	6	7	8
A	00	00	11	10	01	10	01	11
T	11	11	00	01	10	01	10	00
G	10	01	10	11	00	00	11	01
C	01	10	01	00	11	11	00	10

TABLE 3. Simple arithmetic and logical operations on DNA bases (here, {Addition, Subtraction, XOR, XNOR}).

	A	T	C	G
A	$\{A,A,A,G\}$	$\{T,G,T,C\}$	$\{C,C,C,T\}$	$\{G,T,G,A\}$
T	$\{T,T,T,C\}$	$\{C,A,A,G\}$	$\{G,G,G,A\}$	$\{A,C,C,T\}$
C	$\{C,C,C,T\}$	$\{G,T,G,A\}$	$\{A,A,A,G\}$	$\{T,G,T,C\}$
G	$\{G,G,G,A\}$	$\{A,C,C,T\}$	$\{T,T,T,C\}$	$\{C,A,A,G\}$

be altered (in a reversible way) in order to get a variant encryption domain, other than the bit level [2]. In order to perform that, each pair of succeeding bits is joined during the DNA encoding of an image, which produces a different representation than the bit-stream. Afterwards, the diffusion process is performed in that domain. Given the output, the diffusion activity carried out would appear to be performed as a bit-level operation, however, it is not traceable back using bit-level analyses. Fig. 8 displays a 3D plot of a DNA strand, to provide context.

DNA encoding is performed (in most cases) in a sequence of steps. First, creating a DNA sequence from bit-stream sequences by merging every 2 bits into a single DNA base. Given 4 DNA bases (A, T, C, and G), and 4 permutations of pairs of bits (00, 01, 10, 11), beside the lack of binding constraints between DNA bases and bit pairs, there are 24 possible permutations of which only 8 are possible, as listed in Table 2. In this work, permutation 1 is used, as per the following relation:

$$\{(00 \rightarrow A), (01 \rightarrow T), (10 \rightarrow C), (11 \rightarrow G)\}. \quad (8)$$

Second, being provided a key as a DNA sequence (of the same size as the DNA sequence of the image), a DNA-level (reversible) operation is to be performed. (A DNA sequence is produced be converging a PRNG bit-stream into a DNA sequence using one of the permutations in Table 2.) For

Algorithm 2 Encryption: Image I Given $Seed_D$ and $Seed_O$

1) $I_D = toDNA(I)$
2) $K_D = toDNA(PRNG_{[0-1]}(Seed_D))$
3) $K_O = PRNG_{[0-2]}(Seed_O)$
4) $I'_D(i) = \begin{cases} Add(I_D(i), K_D(i)), & \text{if } K_O(i) = 0 \\ XOR(I_D(i), K_D(i)), & \text{if } K_O(i) = 1 \\ XNOR(I_D(i), K_D(i)), & \text{otherwise} \end{cases}$
5) $result = toBits(I'_D)$

Algorithm 3 Decryption: Image I' Given $Seed_D$ and $Seed_O$

1) $I'_D = toDNA(I')$
2) $K_D = toDNA(PRNG_{[0-1]}(Seed_D))$
3) $K_O = PRNG_{[0-2]}(Seed_O)$
4) $I_D(i) = \begin{cases} Sub(I'_D(i), K_D(i)), & \text{if } K_O(i) = 0 \\ XOR(I'_D(i), K_D(i)), & \text{if } K_O(i) = 1 \\ XNOR(I'_D(i), K_D(i)), & \text{otherwise} \end{cases}$
5) $result = toBits(I_D)$

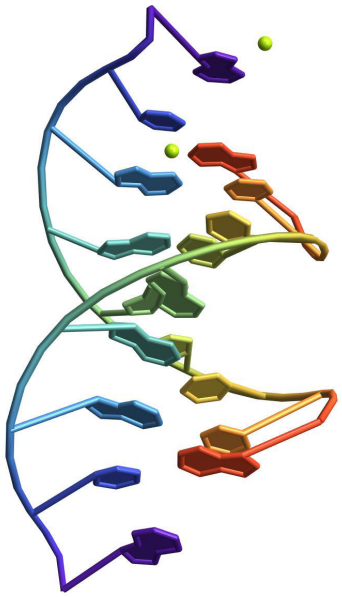


FIGURE 8. 3D plot of a DNA strand.

the implementation of a hybrid approach, instead of using a single operation, 2 operations will be applied in an interleaved manner. For the first reversible operation, addition and subtraction (as reverses of one another) are the operations of choice, while the second operation is DNA XOR (or XNOR). DNA addition, subtraction, XOR, and XNOR are performed according to Table 3. As a last step, the formed DNA sequence is turned back into a bit-stream.

In more detail, for this process to be performed, 2 keys (PRNG seeds) are needed. The first is used to generate a bit-stream which is equal in size to the image bit-stream, (where both bit-streams are converted into DNA sequences afterwards). The second seed is used to generate a sequence

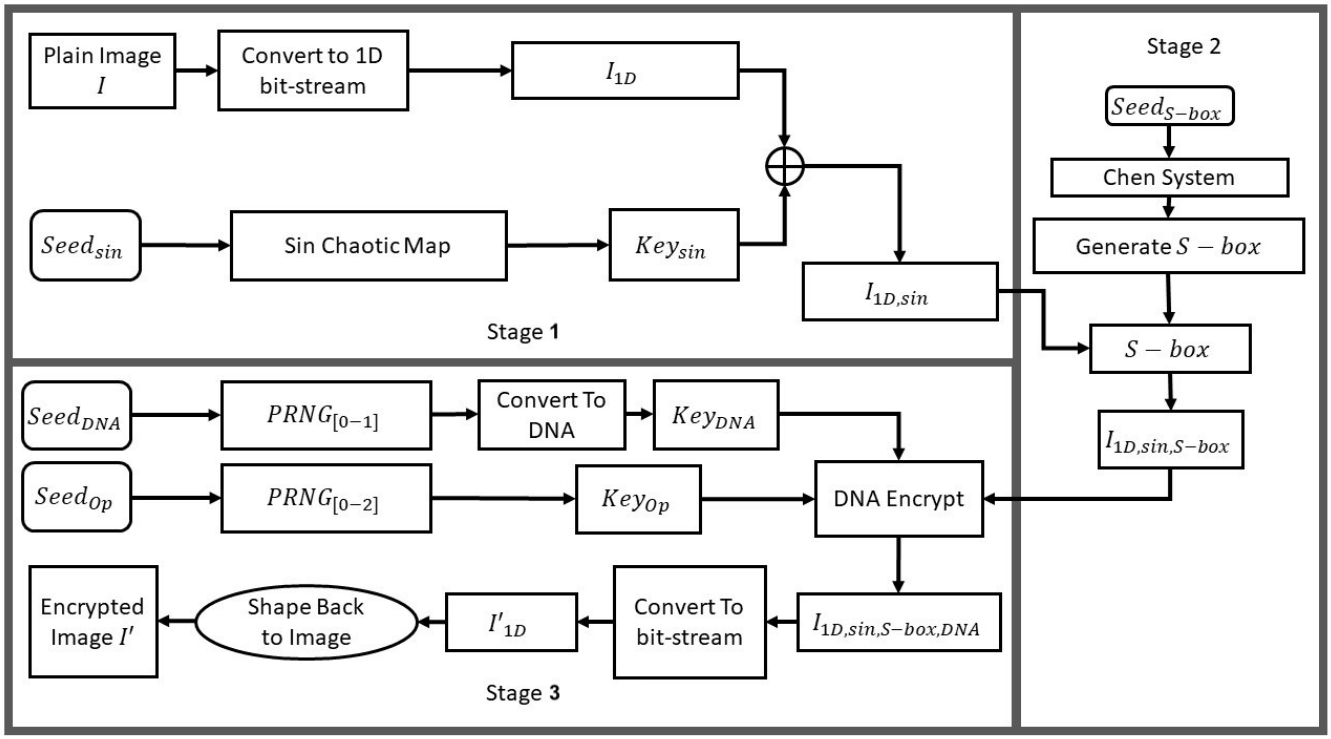


FIGURE 9. Flowchart of the encryption algorithm of the proposed image cryptosystem.

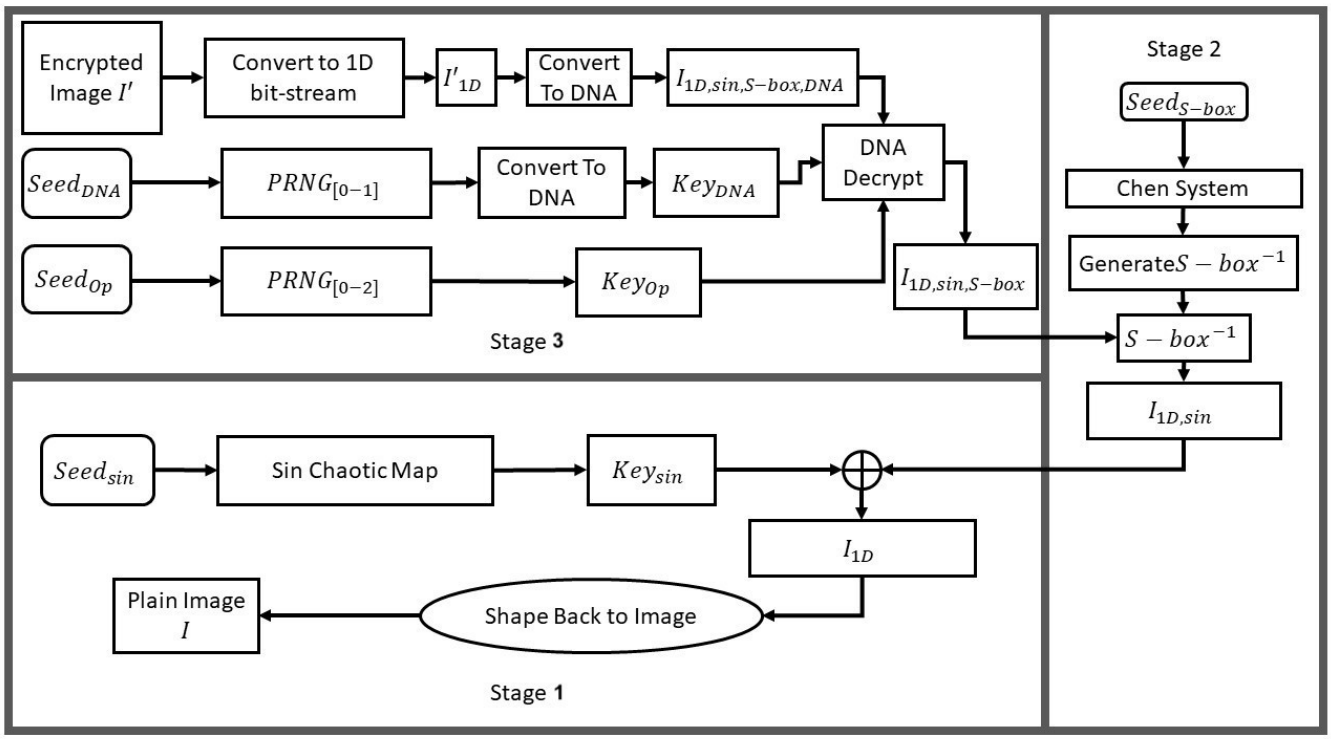
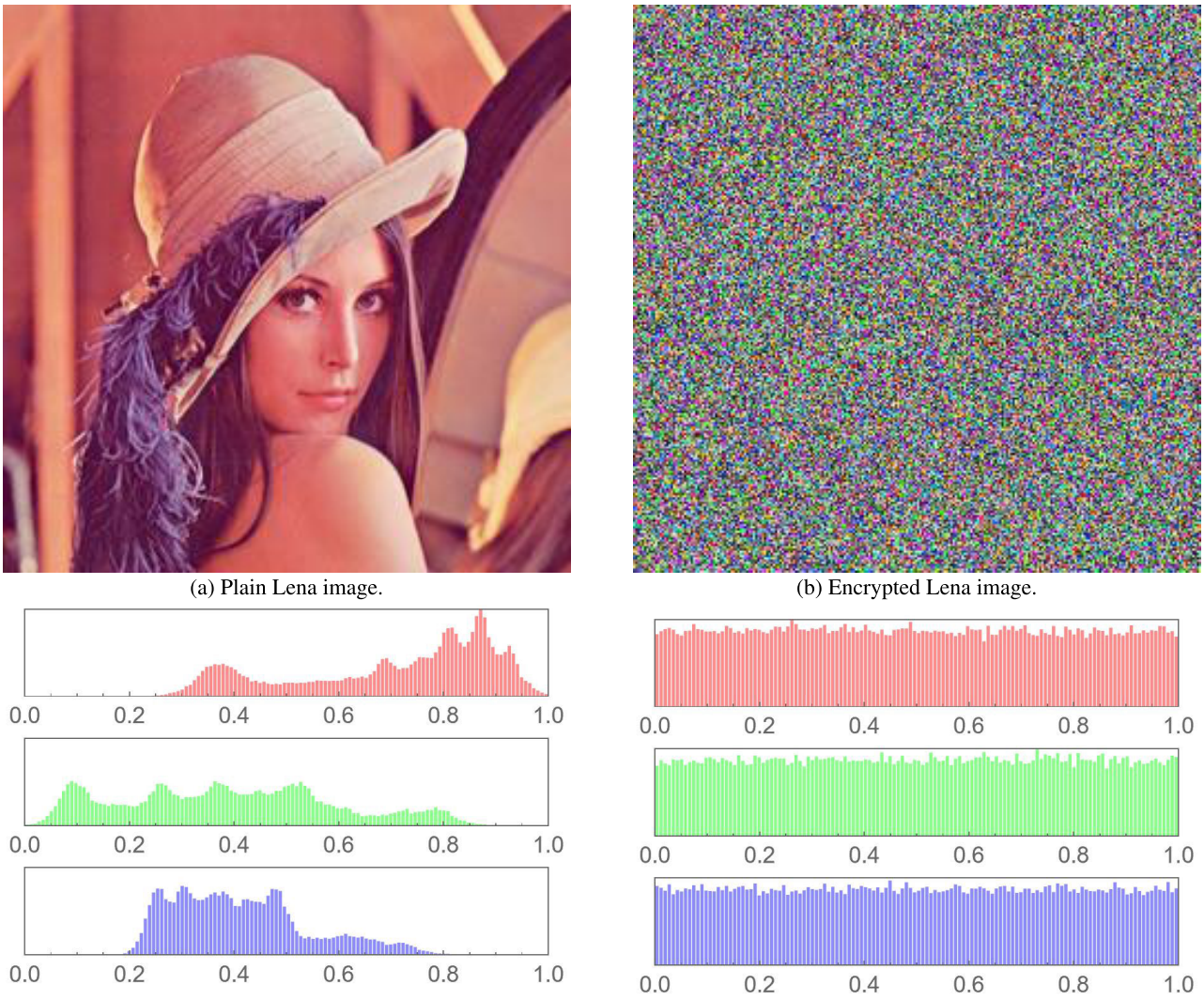


FIGURE 10. Flow chart of the decryption algorithm of the proposed image cryptosystem.

of size equal to the DNA sequence of the image (half the size of its bit-stream), such that this sequence is within the range [0, 2], which is used as an operation selection criterion. As per that, the encryption process is performed as per Algorithm 2,



(a) Plain Lena image.
(b) Encrypted Lena image.
(c) Histogram of plain Lena image.
(d) Histogram of encrypted Lena image.

FIGURE 11. Plain and encrypted versions of the Lena image, and their respective histogram plots.

and the decryption is performed as per Algorithm 3. Accordingly, at a small cost of run-time, there are 2 added benefits. The first being is the increase in the key space as an extra key is needed (for the operation selection). Second, the confusion of operations assures the difficulty of the traceability of the process.

III. METHODOLOGY OF THE PROPOSED COLOR IMAGE CRYPTOSYSTEM

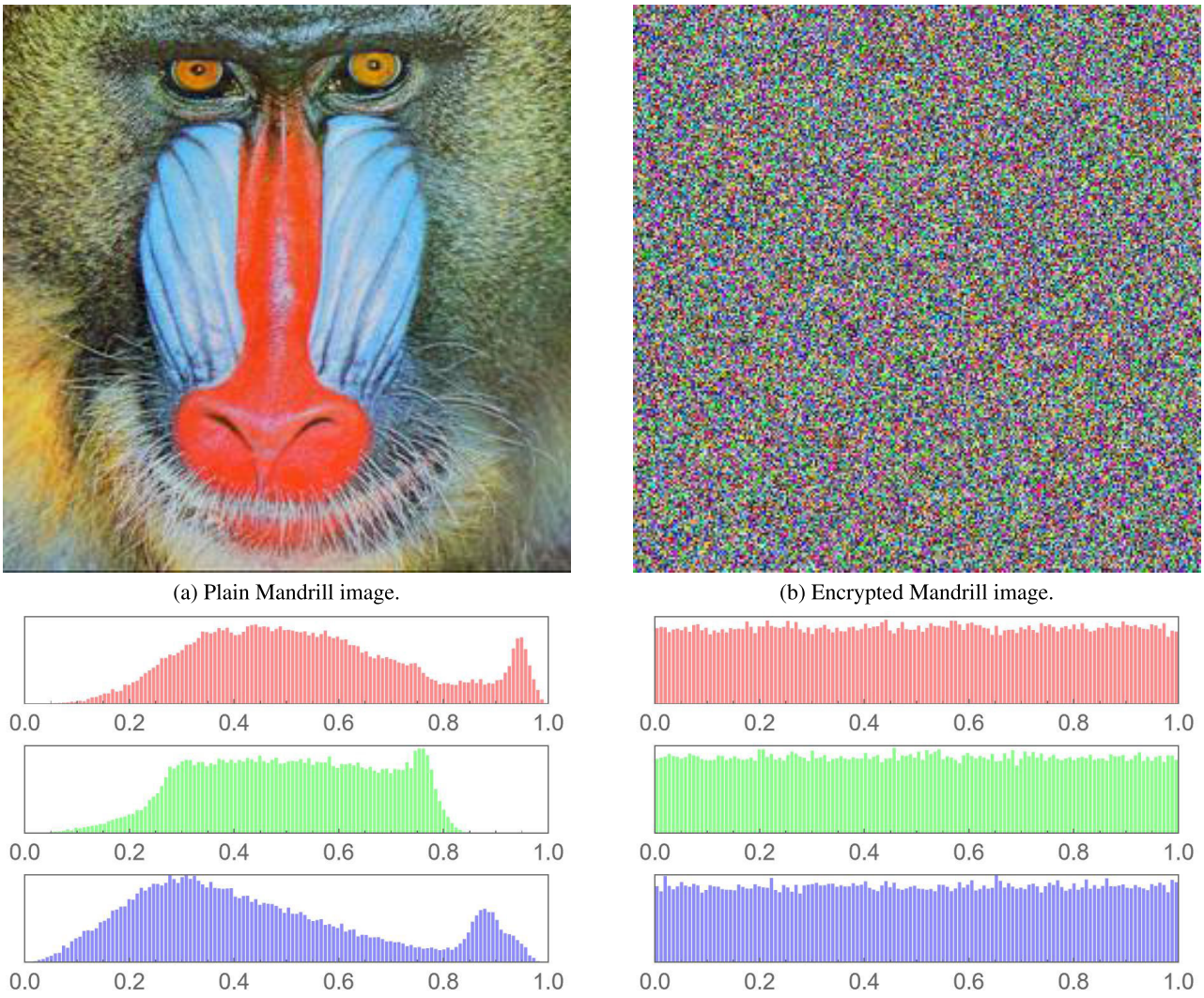
A. THE ENCRYPTION PROCESS

There are 3 stages to the encryption process. Each stage depicts how the input image interacts with the seed-based key used to produce the final output, which is the encrypted image. Additionally, each stage is carried out in a number of phases. This process can be broken down into the following steps for clarification:

1) Stage 1: Sine Chaotic Map.
   a) First, the input color image, I, of dimensions $M \times N$, is converted into a 1D bit-stream to produce I_{1D}, alongside calculating the length of this bit-stream:

$$BitStreamLength = M \times N \times 24 \tag{9}$$

   b) Given a seed for the sine chaotic map $Seed_{sin} = X_0, \mu$, a sequence of numbers is generated (Seq_{sin}) using (1), which is equal in length to the bit-stream length.
   c) Forming the Key_{sin}, the median (mid) of the sequence is generated, and each element is compared against this median value, converting the sequence into a bit-stream. The main target behind comparing to the median value ensures that the bit-stream will produce an equal number



(a) Plain Mandrill image.

(b) Encrypted Mandrill image.

(c) Histogram of plain Mandrill image.

(d) Histogram of encrypted Mandrill image.

FIGURE 12. Plain and encrypted versions of the Mandrill image, and their respective histogram plots.

of 0s and 1s without compromising the PRNG component. This step is performed as per the following equations:

$$C(n) = \begin{cases} 1, & n > mid \\ 0, & otherwise \end{cases} \tag{10}$$

$$Key_{sin} = \bigcup_{i=0}^{BitStreamLength} C(Seq_{sin}) \tag{11}$$

d) Both bit-streams I_{1D} and Key_{sin} are given as inputs to the XOR operation as follows:

$$I_{1D,sin} = I_{1D} \oplus Key_{sin}. \tag{12}$$

2) Stage 2: 4D Chen S-box Application.

a) Given a seed for the S-box, which consists of the 4D Chen system inputs (the 10 keys), a solution of the Chen system is computed, then converted into a 1D sequence of length 2048 (to form 256 numbers, 8 bits each).

b) As performed with the sin sequence, the median value will be utilized in combination with (10) in order to convert the Chen 1D sequence into a bit-stream. Next, each 8 bits are further converted into decimal, resulting in a list $S \in [0, 255]$, and $|S| = 256$.

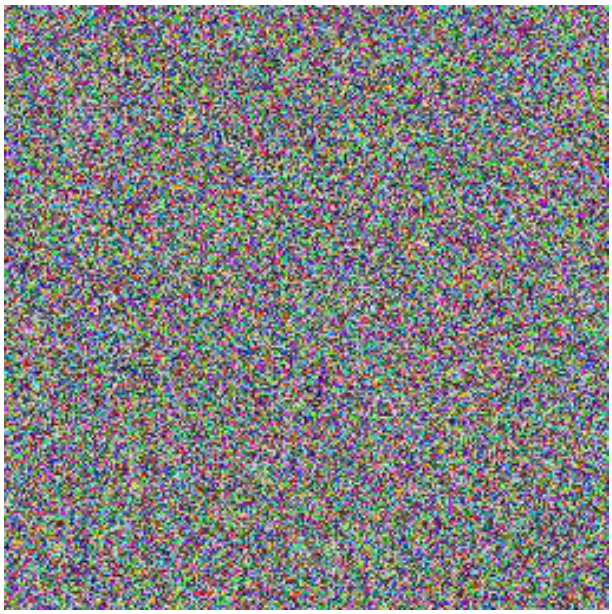
c) List S is provided as input to Algorithm 1, producing the S-box. Finally, the S-box is applied as:

$$I_{1D,sin,S-box} = S - box(I_{1D,sin}). \tag{13}$$

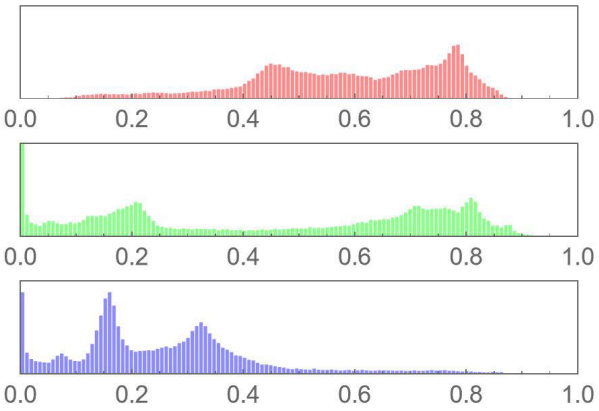
3) Stage 3: Hybrid DNA Encoding.

a) Given a seed for the hybrid DNA encoding, which consists of values for both $Seed_{DNA}$ and $Seed_{Op}$, 2 sequences of numbers are generated, the first, Key_{DNA} which is a PRNG bit-stream equal in size

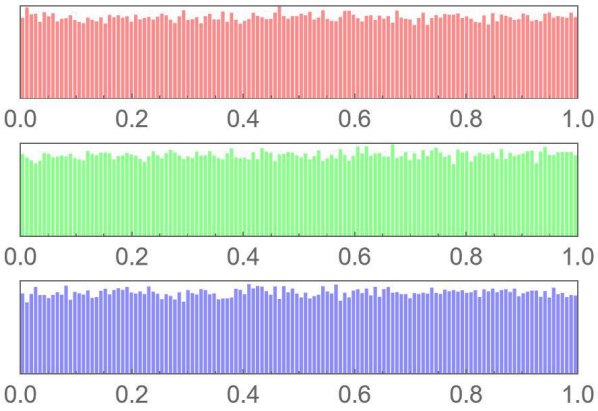
(a) Plain Peppers image.



(b) Encrypted Peppers image.



(c) Histogram of plain Peppers image.



(d) Histogram of encrypted Peppers image.

FIGURE 13. Plain and encrypted versions of the Peppers image, and their respective histogram plots.

to the bit-stream of the image, and the second, Key_{Op}, which is a PRNG sequence of 0s, 1s and 2s, of half the size of the Key_{DNA} (as it is used to control operations on the DNA level, which is half the size of the bit-level).

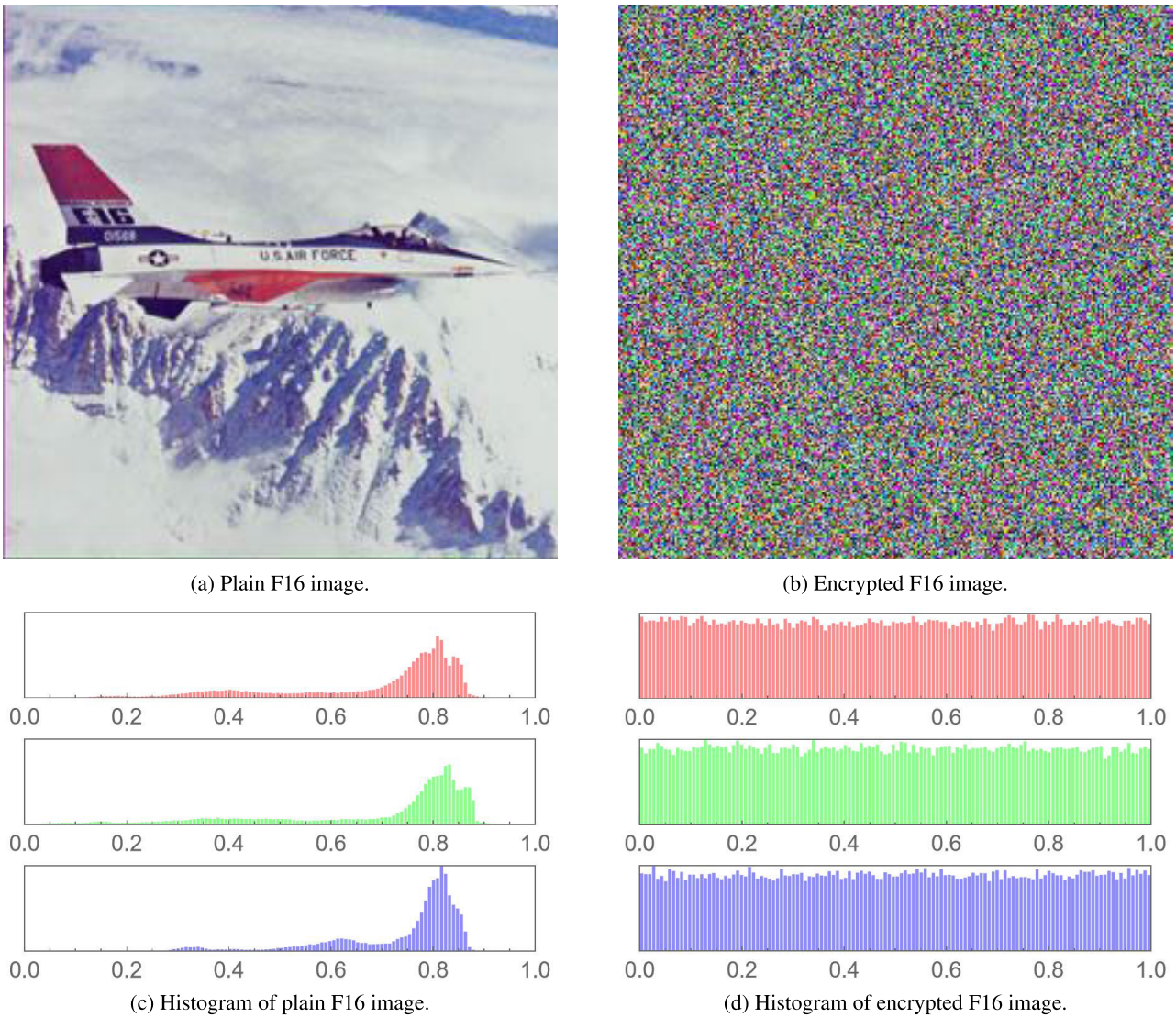
b) Both bit-streams $I_{1D,sin,S-box}$ and Key_{DNA} are converted into DNA-streams using (8). Alongside Key_{Op}, the 3 sequences are passed to Algorithm 2 forming $I_{1D,sin,S-box,DNA}$.

After performing the 3 stages, reshaping $I_{1D,sin,S-box,DNA}$ back into a 2D image (of dimensions $M \times N$) results in the encrypted image I'. Fig. 9 demonstrates a flow chart for the encryption procedure.

B. THE DECRYPTION PROCESS

Decryption, which is the opposite of encryption, is the process of removing the encryption layers in order to recover the original image. Therefore, it is necessary to carry out the aforementioned processes in reverse (as a series of stages), and in a regressive order (as inverse of each performed process). Therefore, the decryption process starts with the encrypted image I', alongside the seeds ($Seed_{sin}$, $Seed_{S-box}$ and $Seed_{DNA}$). Since the process of generating keys out of seeds is performed exactly the same way as in the encryption process, the decryption steps elaborated next are demonstrated in terms of keys instead of seeds. The decryption procedure as follows:

1) Stage 3: Hybrid DNA Decoding.
   a) Image I' of dimensions $M \times N$, is converted into a 1D bit-stream to reproduce $I_{1D,sin,S-box,DNA}$.
   b) Given $I_{1D,sin,S-box,DNA}$, Key_{DNA}, and Key_{Op}, to retrieve $I_{1D,sin,S-box}$, Algorithm 3 is performed.



(a) Plain F16 image.

(b) Encrypted F16 image.

(c) Histogram of plain F16 image.

(d) Histogram of encrypted F16 image.

FIGURE 14. Plain and encrypted versions of the F16 image, and their respective histogram plots.

2) Stage 2: 4D Chen S-box Application.
   a) Given $S-box$, the inverse $S-box$ is calculated, namely $S-box^{-1}$.
   b) The inverse S-box is applied as:

$$I_{1D,sin} = S-box^{-1}(I_{1D,sin,S-box}). \tag{14}$$

3) Stage 1: Sine Chaotic Map.
   a) The XOR operation is performed on the bit-stream $I_{1D,sin}$, and Key_{sin} in order to retrieve I_{1D}.

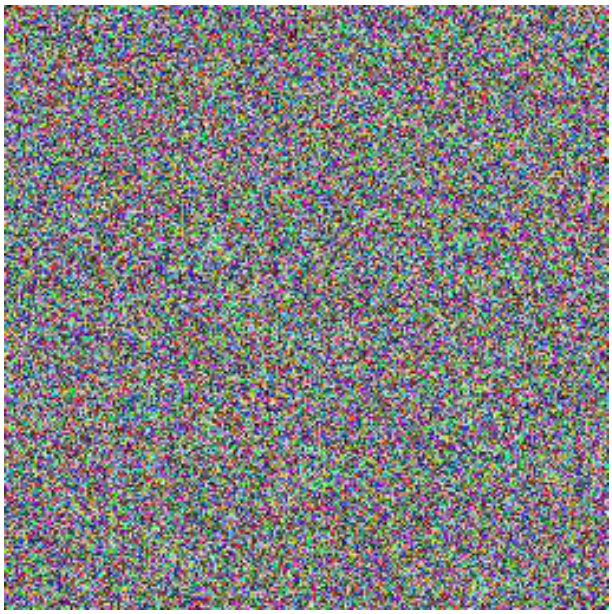
Finally, I_{1D} is to be reshaped back into a 2D image (of dimensions $M \times N$) resulting in the input image I. Figure 10 demonstrates a flow chart for the decryption procedure.

IV. SECURITY ANALYSIS AND NUMERICAL RESULTS

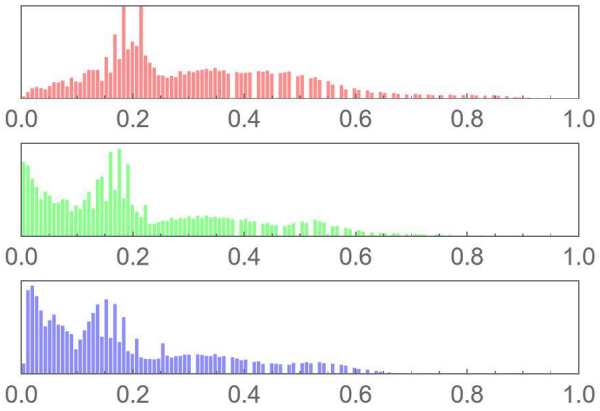
In this section, the performance of the proposed cryptosystem is gauged. This is carried out in terms of computing a number of metrics that are commonly utilized in the image encryption literature, as well as relatively novel ones. Next, appropriate commenting is provided on each computed metric, as well as comparison to counterpart algorithms from the literature. Images popular in the image processing community are employed, all having dimensions 256×256, unless otherwise stated. The performed tests and computed metrics are:

- Visual and Histogram Analyses (Section IV-A)
- Mean Squared Error (Section IV-B)
- Peak Signal-to-Noise Ratio (Section IV-C)
- Information Entropy (Section IV-D)
- Correlation Coefficient (Section IV-E)
- Fourier Transformation Analysis (Section IV-F)
- Histogram Dependency Tests (Section IV-G)
- Differential Attack Analysis (Section IV-H)
- Mean Absolute Error (Section IV-I)
- Key Space Analysis (Section IV-J)
- Execution Time Analysis (Section IV-K)

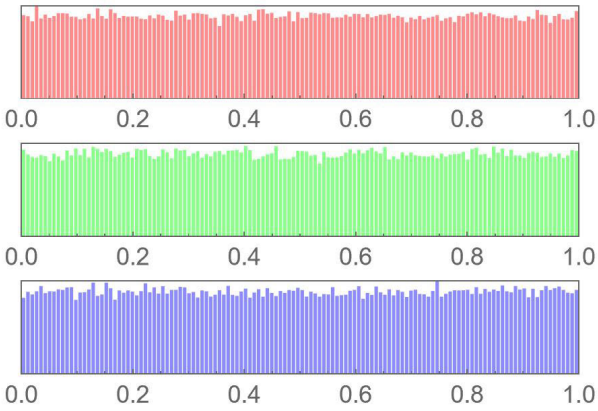
(a) Plain Girl image.



(b) Encrypted Girl image.



(c) Histogram of the plain Girl image.



(d) Histogram of the encrypted Girl image.

FIGURE 15. Plain and encrypted versions of the Girl image, and their respective histogram plots.

- The National Institute of Standards and Technology Analysis (Section IV-L)
- S-Box Performance Analysis (Section IV-M)

A. VISUAL AND HISTOGRAM ANALYSES

The simplest measure of how well an image cryptosystem performs is evaluation by the human visual system (HVS). Subfigures (a) and (b) in Fig. 11–Fig. 19, provide plain and encrypted image versions of Lena, Mandrill, Peppers, F16, Girl, House, House2, Sailboat, Tree, respectively. On visually comparing each of the plain and encrypted versions of the same image, one can find absolutely no visual symmetry or correlation whatsoever.

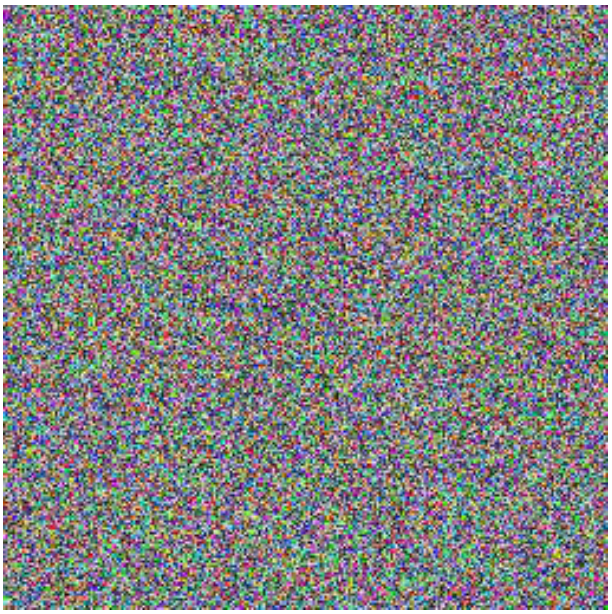
An image histogram is another metric that involves the HVS in addition to its statistical nature. Simply put, the histogram of an image provides information on the probability density function of its pixels. Unlike the histogram of a plain image which can take on any form, that of an encrypted image should be as uniform as possible. On examining Subfigures (c) and (d) in Fig. 11–Fig. 19, which show the histogram plots of the plain and encrypted versions of Lena, Mandrill, Peppers, F16, Girl, House, House2, Sailboat, Tree, respectively, one easily sees that the statistical pixel properties of each of the plain images are completely lost in their encrypted counterparts.

B. MEAN SQUARED ERROR

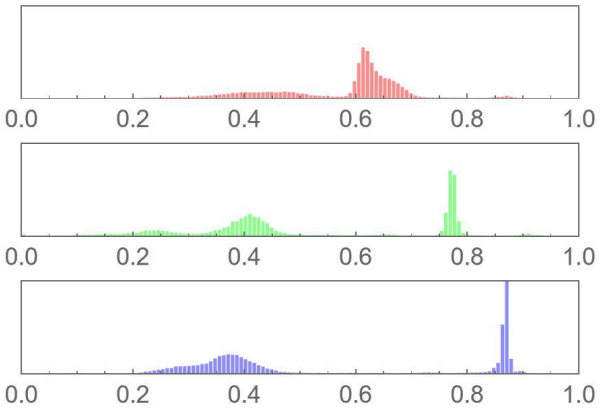
To evaluate the reliability of an image cryptosystem, the mean squared error (MSE) is one of most utilized metrics in the literature. It is expressed as follows:

$$MSE = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P_{(i,j)} - E_{(i,j)})^2}{M \times N}, \tag{15}$$

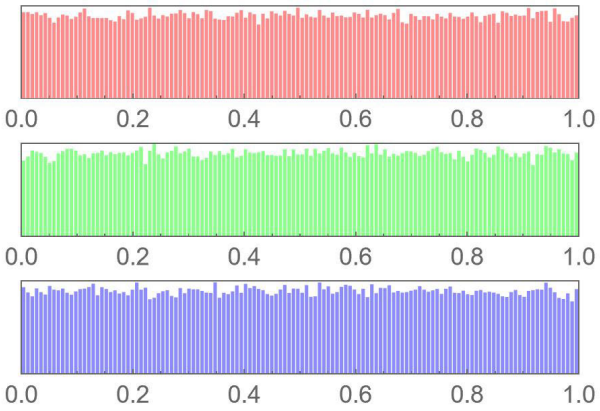
(a) Plain House image.



(b) Encrypted House image.



(c) Histogram of the plain House image.



(d) Histogram of the encrypted House image.

FIGURE 16. **Plain and encrypted versions of the House image, and their respective histogram plots.**

where $P_{(i,j)}$ and $E_{(i,j)}$ are pixels from the plain and encrypted images, respectively, at location (i, j), in an image of dimensions $M \times N$. The larger the computed MSE value between a plain image and its encrypted image, the better is the performance of an image cryptosystem, as this would reflect better resilience against statistical attacks. Table 4 displays the computed MSE values for the proposed cryptosystem, as well provides a comparison with those achieved by counterpart algorithms from the literature. It is clear that the achieved MSE values are comparable to those found in the literature.

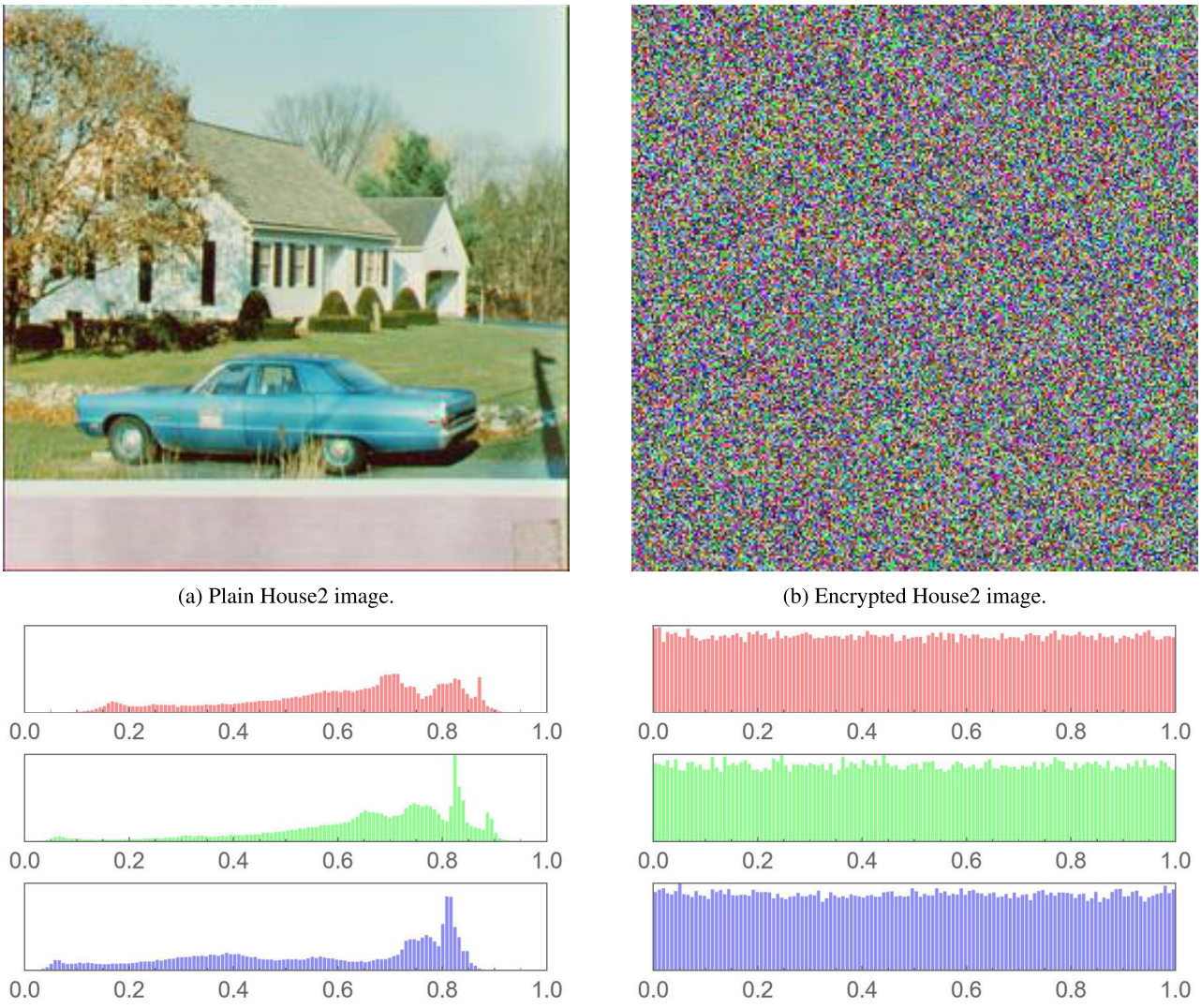
C. PEAK SIGNAL-TO-NOISE RATIO

The Peak Signal-to-Noise Ratio (PSNR) is a basic metric for evaluating image cryptosystems. Its calculation is based on the log value of the ratio between the square of the maximum pixel value I_{max} to the MSE. It is mathematically expressed as

$$PSNR = 10 \log \left(\frac{I_{max}^2}{MSE} \right), \tag{16}$$

where I_{max} is the maximum gray scale intensity, having a value of 255. Because of the inverse proportionality between PSNR and MSE, lower values of PSNR reflect improved encryption. Table 5 displays the computed PSNR values for the proposed cryptosystem, as well as provides a comparison with those achieved by counterpart algorithms from the literature. It is clear that the achieved PSNR values are comparable to those found in the literature.

Table 5 shows the computed PSNR values of our proposed image cryptosystem, alongside those reported for counterpart algorithms from the literature. It is clear that our computed values are comparable to the literature and even superior at times (much better than those of [60]).



(a) Plain House2 image.

(b) Encrypted House2 image.

(c) Histogram of the plain House2 image.

(d) Histogram of the encrypted House2 image.

FIGURE 17. Plain and encrypted versions of the House2 image, and their respective histogram plots.

TABLE 4. MSE values comparison of different images.

	Proposed	[34]	[60]	[6]	[24]
Lena	8966.97	10869.73	4859.03	8888.88	9112.1
Peppers	10049.4	–	6399.05	10092.3	10298.7
Mandrill	8333.14	10930.33	7274.44	8295.21	8573.38
F16	10352.3	–	–	–	–
Girl	12150.7	–	–	–	12450.9
House	8345.95	–	–	–	8427.04
House2	9149.54	–	–	–	9374.65
Sailboat	10021.4	–	–	–	–
Tree	9956.19	–	–	–	–

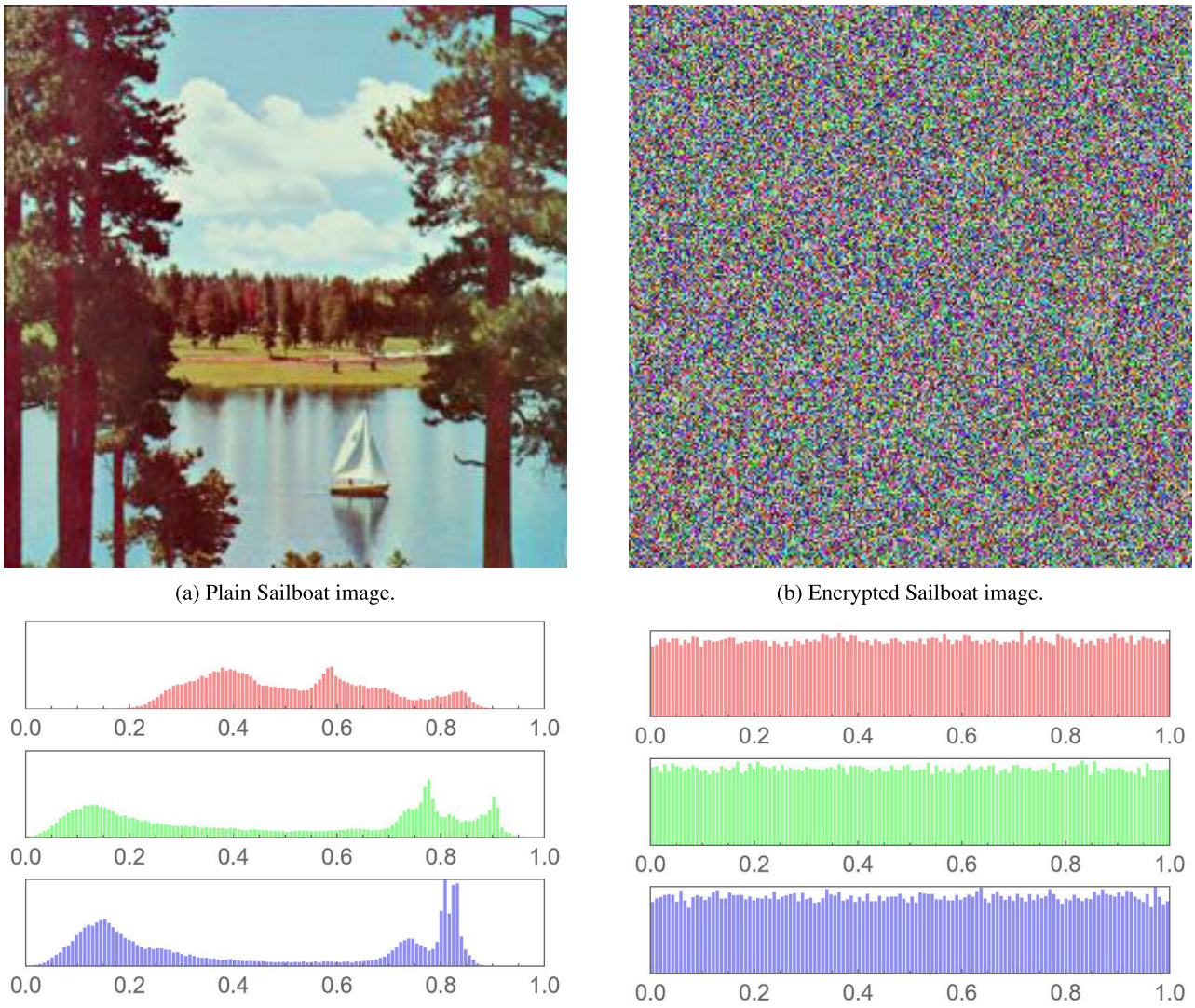
TABLE 5. PSNR values comparison of different images.

	Proposed	[34]	[60]	[6]	[24]
Lena	8.60435	7.7677	11.3	8.64233	8.53462
Peppers	8.10939	–	10.10	8.09089	8.00296
Mandrill	8.92272	7.7447	9.55	8.94253	8.79929
F16	7.98045	–	–	–	–
Girl	7.28478	–	–	–	7.17879
House	8.91604	–	–	–	8.87405
House2	8.51681	–	–	–	8.41125
Sailboat	8.12152	–	–	–	–
Tree	8.14987	–	–	–	–

D. INFORMATION ENTROPY

In order to evaluate the extent of the randomness of the distribution of the gray pixels in each of the 3 color channels of an image, the information entropy is the right metric to utilize. Its calculation is expressed as follows:

$$H(m) = \sum_{i=1}^{M} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{17}$$



(a) Plain Sailboat image.

(b) Encrypted Sailboat image.

(c) Histogram of the plain Sailboat image.

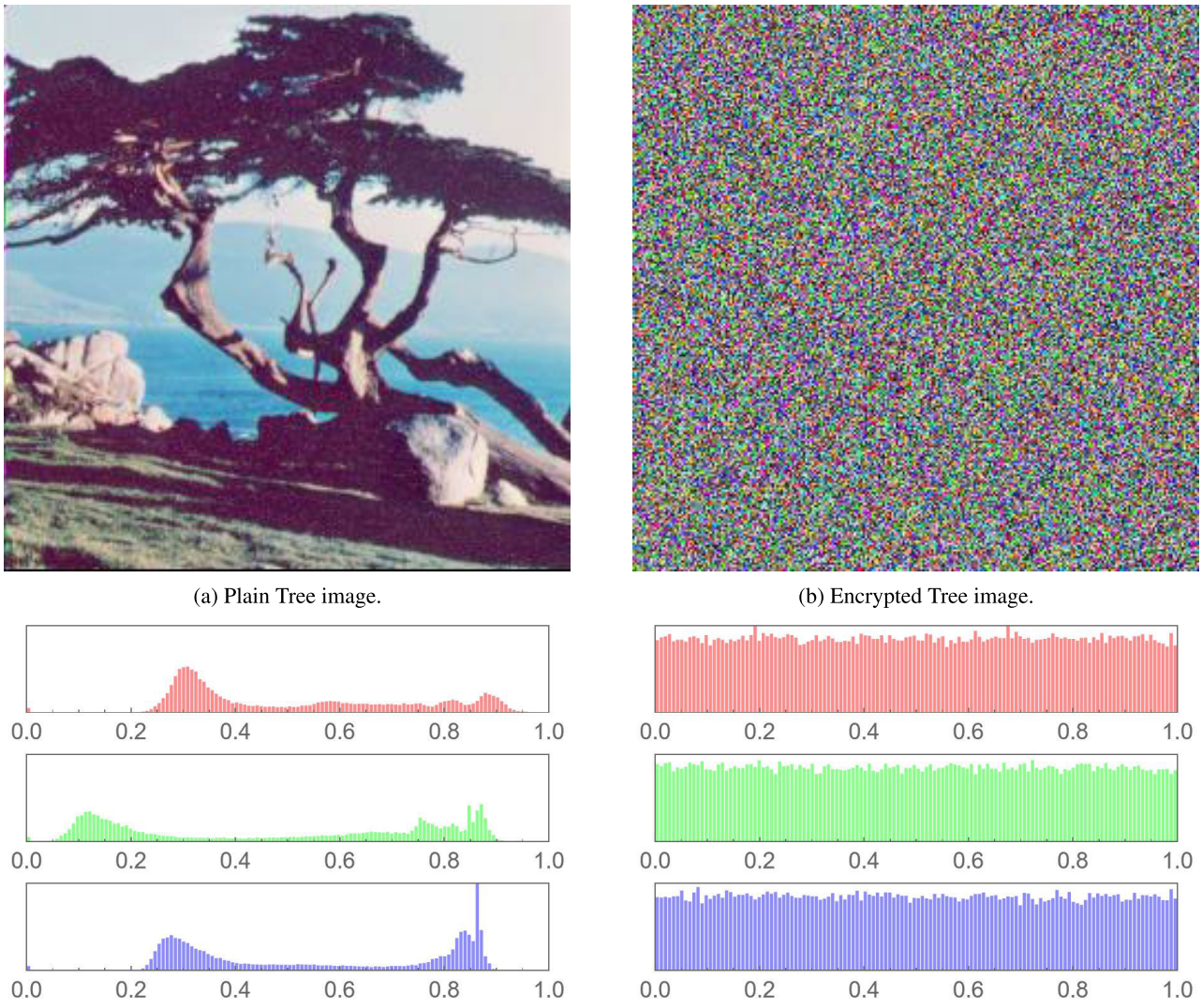
(d) Histogram of the encrypted Sailboat image.

FIGURE 18. Plain and encrypted versions of the Sailboat image, and their respective histogram plots.

where $p(m_i)$ represents the probability of occurrence of each symbol m in the total number of M symbols in an image. The ideal entropy value of a well-encrypted RGB image is 8 [63]. Table 6 displays the computed entropy values for each color channel of a number of images. It is clear that the achieved values are all higher than 7.99, close enough to the ideal value of 8, indicating that the proposed cryptosystem is resistant to entropy attacks. Furthermore, upon comparing the computed entropy value for the encrypted Lena image of the proposed cryptosystem with counterparts algorithms from the literature, in Table 7 and Table 8, it is shown to exhibit comparable performance.

E. CORRELATION COEFFICIENT ANALYSIS

The analysis of the correlation coefficient, r, is a crucial indicator for assessing the effectiveness of any image cryptosystem. In this analysis, the correlation between 2 adjacent pixels in 3 dimensions, horizontal (H), vertical (V) and diagonal (D), is computed. This is mathematically carried out using (18) to (21) in the following manner. First off, (21) is used to calculate the mean average of the distribution of pixels in each image. Next, (20) is used to calculate the dispersion (or level of uncertainty of the distribution) in each image. This is then followed by the utilization of (19) to calculate the linear direction similarity (i.e. the covariance) in each of the images' distributions. Finally, (18) calculates the correlation coefficient, r. For a well-encrypted image, the resulting r value should be as close to zero as possible, to indicate the absence of any sort of pixel correlation. On the other hand, r values close to ± 1 would indicate a strong positive or negative pixel correlation, a characteristic of plain images where adjacent pixels are often of the same color.



(a) Plain Tree image.

(b) Encrypted Tree image.

(c) Histogram of the plain Tree image.

(d) Histogram of the encrypted Tree image.

FIGURE 19. Plain and encrypted versions of the Sailboat image, and their respective histogram plots.

The ability of a robust image cryptosystem to eradicate any pixel correlation directly translates into eradicating statistical attacks by cryptanalysts.

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{18}$$

where

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{19}$$

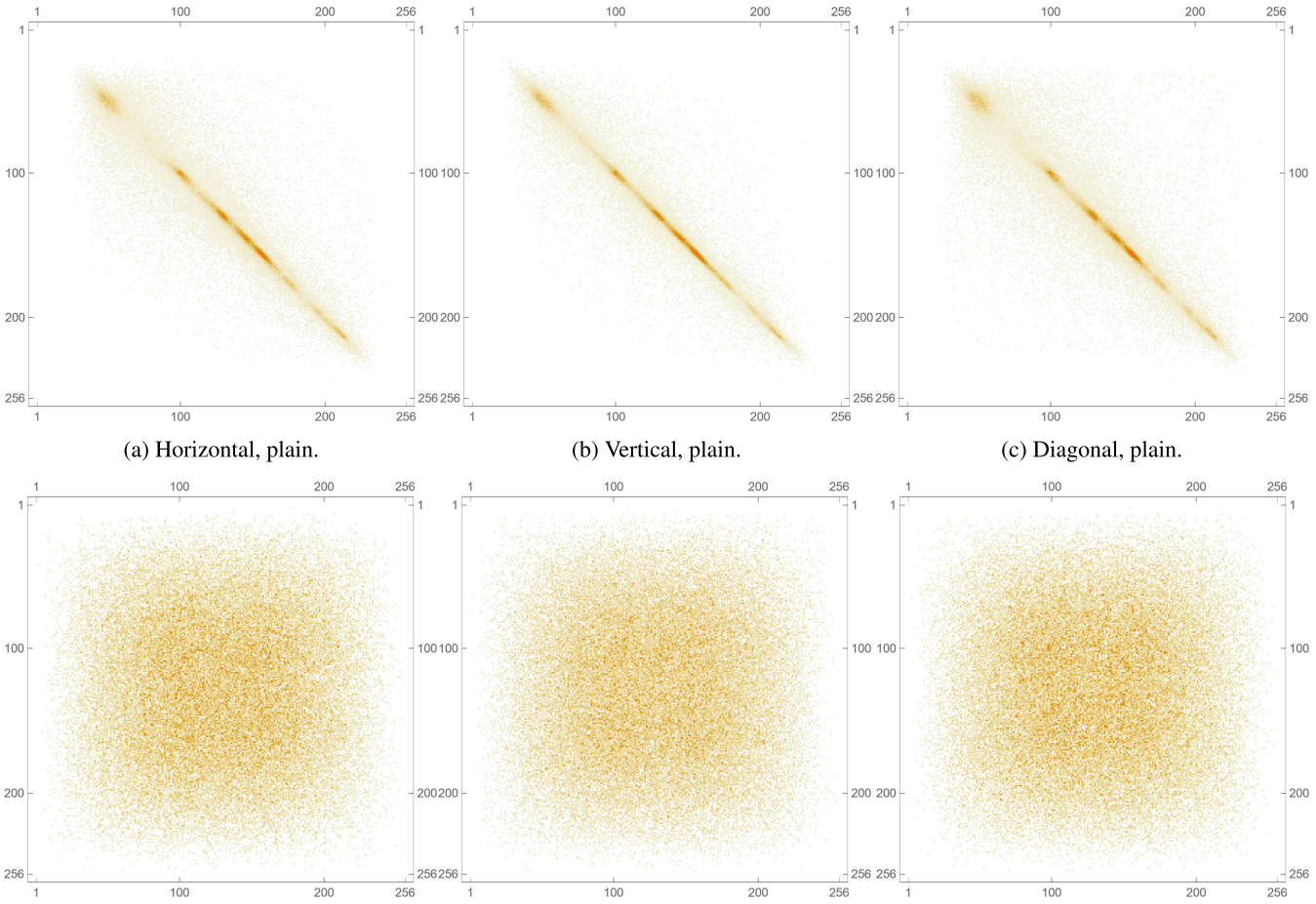
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{20}$$

and

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i). \tag{21}$$

where x and y are 2 images, while N is the length of the bitstream representing their pixels. For example, for RGB images each of dimensions 256×256, N would be $256 \times 256 \times 3 \times 8 = 1572864$.

Tables 9 and Table 10 display r values for various plain and encrypted images, respectively. It is clear that values in Table 9 exhibit a high correlation among adjacent pixels, in the various directions, where most of the computed values are higher than 0.9. On the other hand, the values computed and displayed in Table 10 are close to 0, signifying no correlation among adjacent pixels, which is the desired situation for encrypted images. Additionally, these differences are visually more apparent in the Fig. 20, where sub-figures (a), (b) and (c) depict typical pixel behavior of plain images, and appear as a cluster of points taking on the form of a diagonal line. This is unlike the scattered plot shown in sub-figures (d), (e) and (f),



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain.

(d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 20. Correlation coefficient diagrams of the plain and encrypted Lena images.

which is typical of encrypted images having no correlation among their adjacent pixels. Similar plots are generated and displayed in Fig. 21, Fig. 22 and Fig. 23, for the red, green and blue color channels of the Lena image, respectively. Furthermore, 3D plots of the correlation coefficient matrices of the plain and encrypted Lena images are displayed in Fig. 24. The same diagonal behavior can be seen in the case of the plain Lena image (Fig. 24a), while a random distribution of values is seen for its encrypted version (24b).

Table 11 and Table 12 display the computed correlation coefficient values in comparison with those reported by counterpart algorithms from the literature. It is clear that a comparable performance is exhibited by all the shown algorithms.

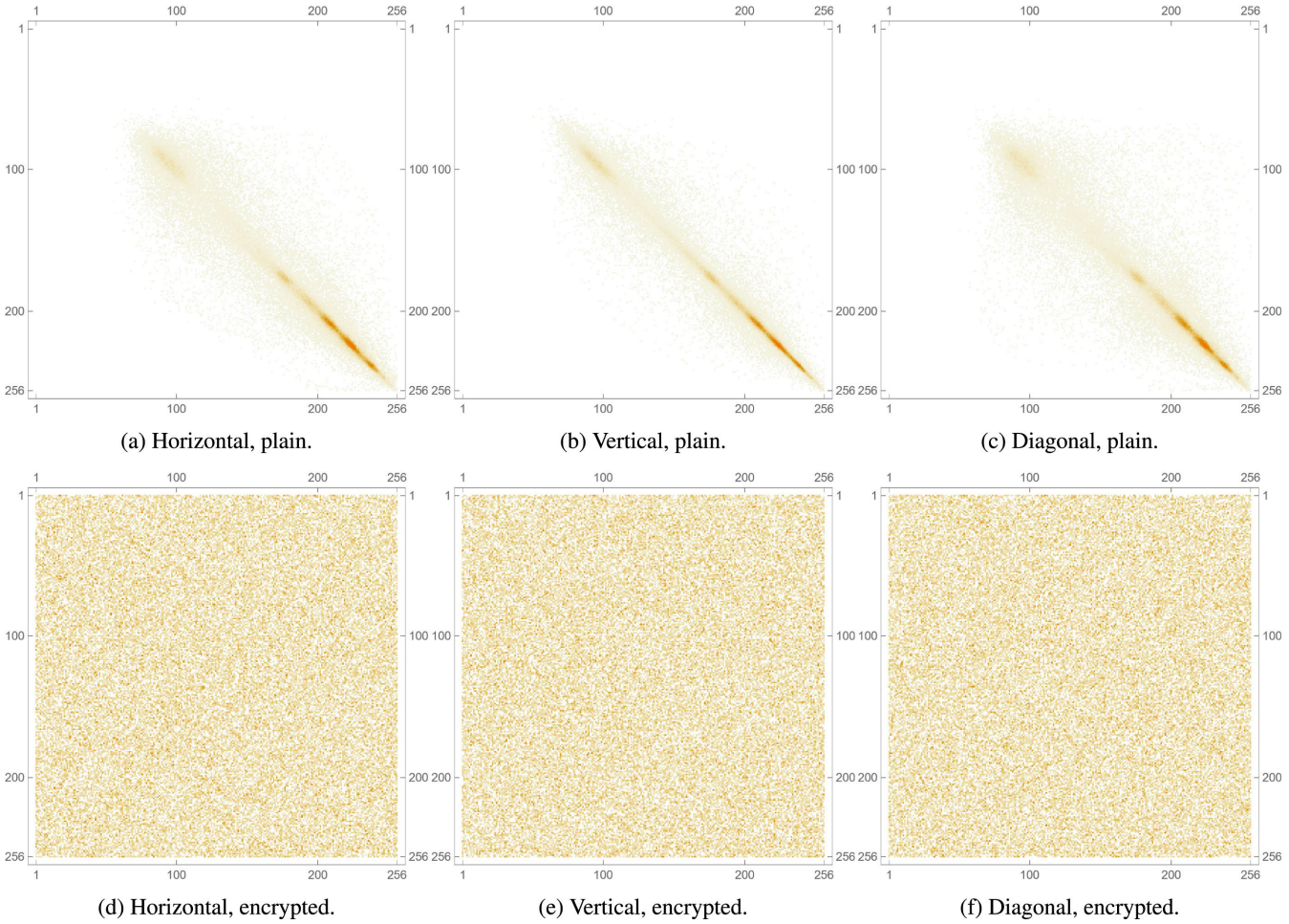
F. FOURIER TRANSFORMATION ANALYSIS

While the loss of correlation among adjacent pixels is usually gauged through the correlation coefficient, r, described in Section IV-E, there is however another interesting measure for that same property. By comparing the Discrete Fourier Transform (DFT) of the plain and encrypted version of the same image, one can assess whether an image cryptosystem is really successful at eradicating any correlation among adjacent pixels. Mathematically, the DFT of an $N \times N$ image $f(i, j)$ into the frequency domain is expressed as follows

$$F(k, l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) e^{-i2\pi(\frac{ki}{N} + \frac{li}{N})}, \tag{22}$$

where $f(a, b)$ is the image representation in the spatial domain, such that the exponential term is the basis function that matches to every point $F(k, l)$ in the Fourier space. In (22), the basis functions are trigonometric waves with increasing frequencies. Ultimately, this means that $F(0, 0)$ is the DC-component of the image and therefore translates into average brightness. On the other hand, $F(N - 1, N - 1)$ translates into the highest frequency.

Fig. 25 displays the application of the Fourier Transform to plain and encrypted versions of the Mandrill image. It is easily seen in Fig. 25 that at the image's center represents pixels with high correlation. This is observed in the appearance of a plus-sign feature in the image's center, with decreasing brightness levels as we move away radially from the center. A plain image has special features, including edges and corners, and such features can be recognized in the Fourier



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain.

(d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 21. Correlation coefficient diagram of the plain and encrypted red channel of Lena image.

Transform. However, on applying the Fourier Transform to the encrypted image of Mandrill, as in Fig. 25a, we observe a rather uniform distribution of values. This is because no special features are available in an encrypted image. All edges and corners are lost upon encrypting the image, signifying the eradication of any correlation among adjacent pixels.

G. HISTOGRAM DEPENDENCY TESTS

To showcase the absence of any correlation between the plain and the encrypted images, linear dependency between the histograms of images before and after encryption is evaluated using various methods [23]. The dependency level is an effective encryption method should be as minimal as possible. As a result, it is preferable for the dependency coefficient to be as near to 0 as feasible when calculated as a value in the range $[-1, 1]$. In such evaluation perspective, 1 means strong dependency, -1 means strong inverse dependency, and 0 means no present dependency. Five different linear correlation evaluation techniques are applied: Blomqvist β, Goodman-Kruskal γ, Kendall τ, Spearman ρ, and Pearson correlation r.

Blomqvist assesses the correlation between two histogram distributions (X and Y) as a medial correlation coefficient (for medians $\bar{x}$ and $\bar{y}$). Blomqvist correlation is equated as follows:

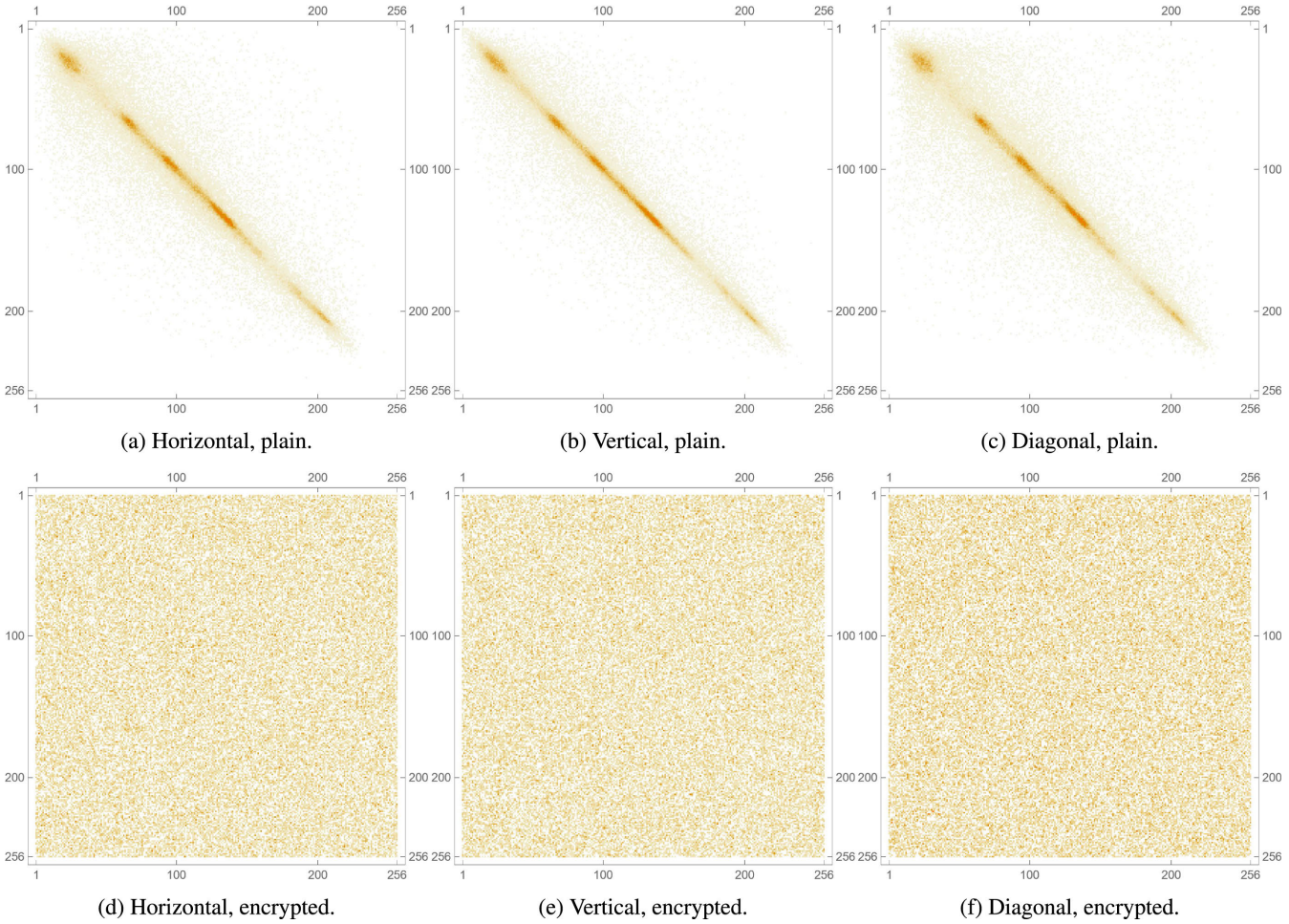
$$\beta = \{(X - \bar{x})(Y - \bar{y}) > 0\} - \{(X - \bar{x})(Y - \bar{y}) < 0\}. \quad (23)$$

The evaluation of the Goodman-Kruskal pairwise measure of monotonic association is based on the relative order of subsequent elements in the 2 histogram. When comparing two pairs after combining the 2 histograms into a single set of pairs in a 1 to 1 construction, they are either promoting or inhibiting the linear correlation. Goodman-Kruskal correlation is equated as:

$$\gamma = \frac{n_c - n_d}{n_c + n_d}. \quad (24)$$

Kendall assesses correlation in relation to sample size using the same idea of concordant pairs and discordant pairs, equating the correlation as:

$$\tau = \frac{n_c - n_d}{\frac{n(n-1)}{2}}. \quad (25)$$



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain.

(d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 22. Correlation coefficient diagram of the plain and encrypted green channel of Lena image.

When conducting a rank-based correlation test, the Spearman rank correlation test compares the position of the element in the sorted list of elements forming the histogram to the mean rank value. Spearman rank correlation is equated as:

$$\rho = \frac{\sum(R_{ix} - \overline{R}_x)(R_{iy} - \overline{R}_y)}{\sqrt{\sum(R_{ix} - \overline{R}_x)^2 \sum(R_{iy} - \overline{R}_y)^2}}. \tag{26}$$

Conclusively, the most common and straightforward correlation method, Pearson correlation, simply connects components of the distributions to their mean averages. An equivalent of Pearson correlation is:

$$r = \frac{\sum(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum(X_i - \overline{X})^2 \sum(Y_i - \overline{Y})^2}}. \tag{27}$$

The outcome of applying the 5 tests to various test images are displayed in Table 13. There is very little dependence between the input and encrypted counterparts of images in terms of histograms across all color channels since all scores are getting very close to 0.

H. DIFFERENTIAL ATTACK ANALYSIS

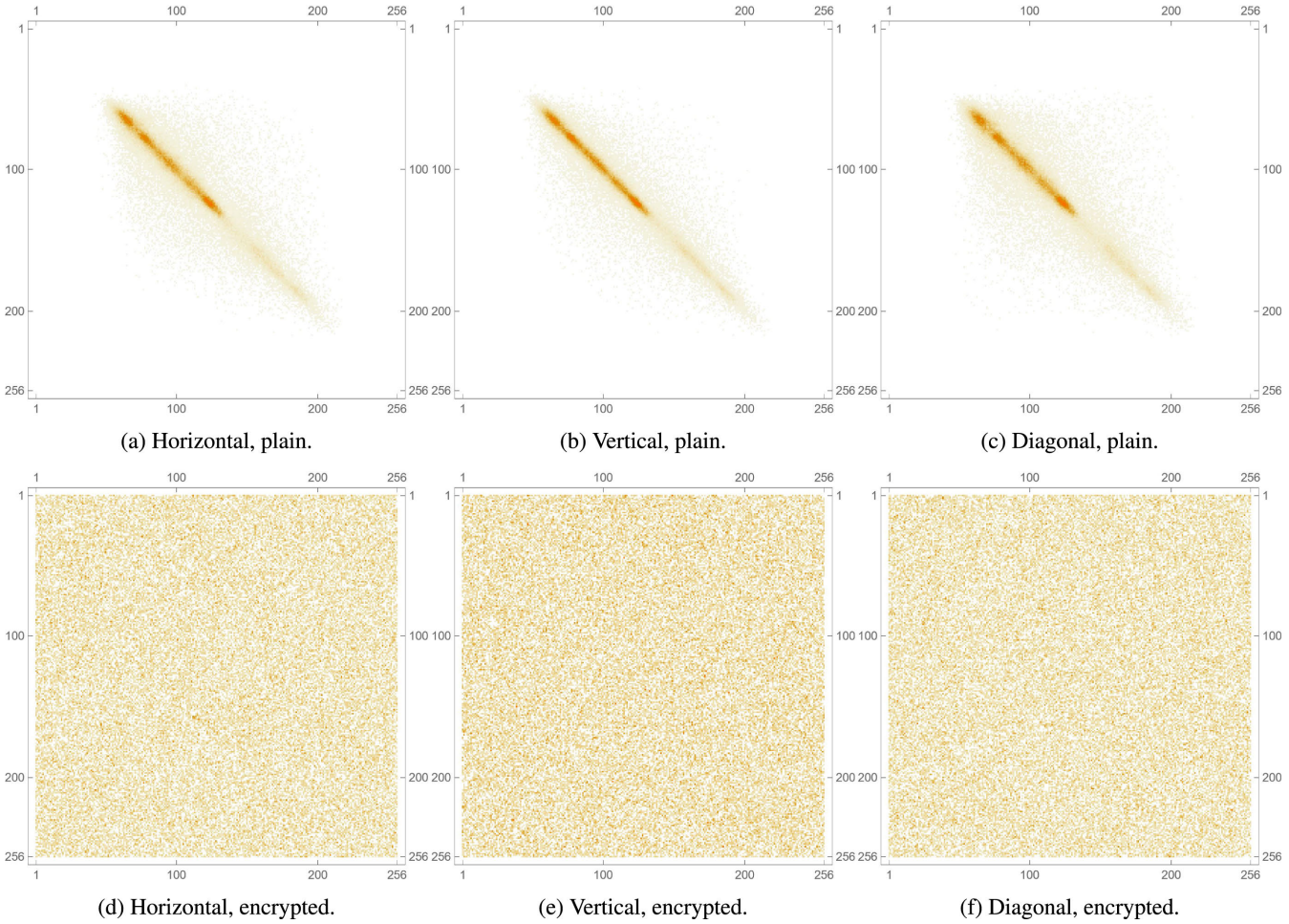
Differential attacks are performed by making minute modifications to a plain image and then retrieving the matching encrypted image, both before and after the alteration. Next, an effort is made to calculate the key via cryptanalysis. This means that a secure image cryptosystem should let even the smallest modifications to the plain image to result in a substantial alteration of the encrypted image. The Number of Pixel Changing Rate (NPCR) and the Unified Average Change Intensity (UACI) are the 2 measures most useful for determining an image cryptosystem's resilience to differential attacks. The NPCR is mathematically expressed as

$$NPCR = \frac{\sum_{i,j} D_{i,j}}{M \times N} \times 100, \tag{28}$$

where $D_{i,j}$ is given by

$$D_{i,j} = \begin{cases} 0 & C_{1(i,j)} = C_{2(i,j)} \\ 1 & C_{1(i,j)} \neq C_{2(i,j)}. \end{cases} \tag{29}$$

Simply put, the NPCR is a computation resulting in the number of differing pixels between a plain image and its



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain.

(d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 23. Correlation coefficient diagram of the plain and encrypted blue channel of Lena image.

encrypted version. The UACI is mathematically expressed as

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255}, \tag{30}$$

where $C_{1(i,j)}$ and $C_{2(i,j)}$ are 2 images of dimensions $M \times N$. The UACI is a computation resulting in the difference in the average intensity between a plain image and its encrypted version. The computed NPCR and UACI of the proposed image cryptosystem for the Lena image are provided in Table 14 and Table 15, respectively. It is clear that the computed NPCR values are all above 99%, being very close to the ideal value. On the other hand, the computed UACI values are close enough to the ideal value of 33.35%, but not exactly reaching it. Furthermore, it is clear that the computed values are comparable to those of counterpart image encryption algorithms reported in the literature.

I. MEAN ABSOLUTE ERROR

A third metric that can also be utilized to measure the strength and robustness of an image cryptosystem against differential attacks is the Mean Absolute Error (MAE). In essence, the MAE attempts to compute the average difference between a pixel of the plain image $P_{(i,j)}$ and that of its encrypted version $E_{(i,j)}$ for all $M \times N$ pixels in an image. Its calculation is based on the following formula

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} P_{(i,j)} - E_{(i,j)}. \tag{31}$$

Of course, the larger the computed MAE value, the better indication of the robustness of an image cryptosystem against attacks of differential nature. The computed values of our proposed image cryptosystem are provided in Table 16, along with the reported values of those of counterpart algorithms from the literature. For the various tested images, the computed MAE values are in close agreement with the others.

J. KEY SPACE ANALYSIS

The proposed image cryptosystem is comprised of 3 stages, with 2, 10 and 2 variables for the keys used in each stage, respectively. For a machine precision of 10^{-16}, this means that the proposed image cryptosystem has an effective key space of $10^{14\times16} = 10^{224} \approx 2^{744}$, effectively rendering it robust against brute-force attacks according to [36]. Table 17

TABLE 6. Entropy values of the RGB channels of various encrypted images.

Image	Channels	Entropy values
Lena	Red	7.9971
	Green	7.99718
	Blue	7.99736
Peppers	Red	7.99692
	Green	7.99742
	Blue	7.99714
Mandrill	Red	7.99772
	Green	7.99717
	Blue	7.99741
F16	Red	7.99741
	Green	7.99672
	Blue	7.99683
Girl	Red	7.99731
	Green	7.99741
	Blue	7.99697
House	Red	7.99688
	Green	7.99678
	Blue	7.99729
House2	Red	7.99695
	Green	7.99689
	Blue	7.99718
Sailboat	Red	7.99732
	Green	7.99703
	Blue	7.99741
Tree	Red	7.99711
	Green	7.99753
	Blue	7.99701

TABLE 7. Comparison of entropy values of the Lena image RGB channels.

Algorithm	Entropy values of channels		
	Red	Green	Blue
Proposed	7.9971	7.99718	7.99736
[6]	7.9972	7.9973	7.9966
[25]	7.9994	7.9994	7.9993
[34]	7.9973	7.9972	7.9975
[50]	7.9991	7.9954	7.9963

TABLE 8. Comparison of the entropy values of the Lena image of the proposed cryptosystem and various algorithms from the literature.

Algorithm	Entropy value
Proposed	7.99901
[6]	7.9991
[9]	7.9984
[24]	7.9856
[30]	7.9992
[34]	7.9990

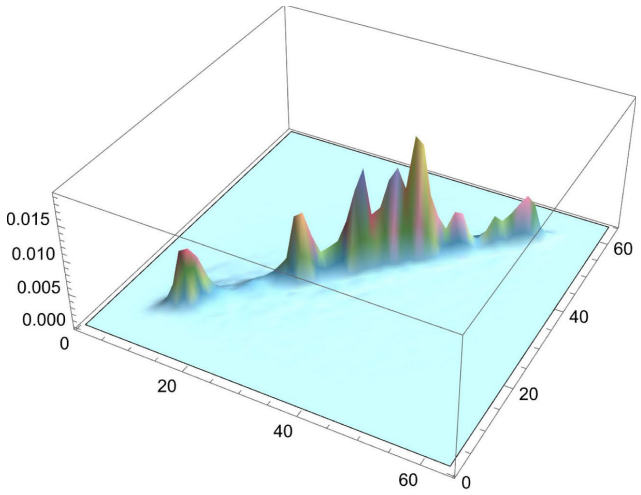
TABLE 9. Correlation coefficients of adjacent pixels in plain images. Shown here in 3 directions, horizontal, diagonal and vertical.

Plain image	H	D	V
Lena	0.959422	0.930426	0.79088
Peppers	0.959422	0.930426	0.966795
Mandrill	0.848778	0.750624	0.79088
F16	0.92752	0.868229	0.920783
Girl	0.974013	0.974013	0.965671
House	0.978232	0.952926	0.952926
House2	0.907074	0.907074	0.92309
Sailboat	0.950138	0.919872	0.950138
Tree	0.968153	0.929967	0.919872

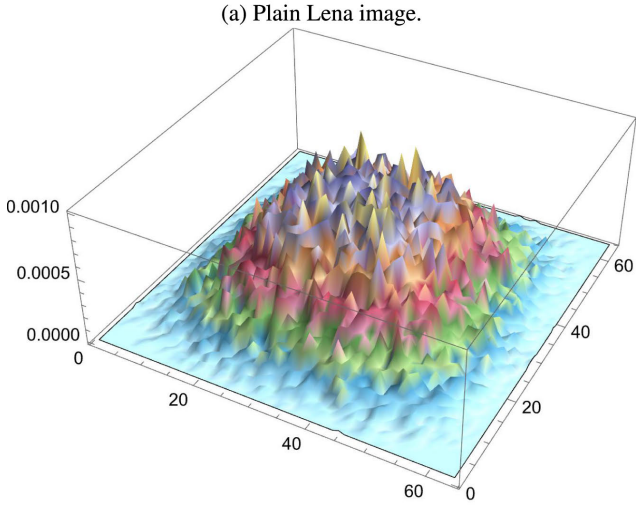
provides a comparison among the achieved key space values of the proposed image cryptosystem and its counterparts from the literature. With the exception of the image cryptosystem

TABLE 10. Correlation coefficients of adjacent pixels in encrypted images. Shown here in 3 directions, horizontal, diagonal and vertical.

Enc. image	H	D	V
Lena	0.0079784	−0.00012531	0.0011584
Peppers	−0.0020878	0.00065688	−0.0015191
Mandrill	0.0013408	−0.004713	−0.0019799
F16	−0.0022452	0.0013559	0.0017223
Girl	0.0041745	0.0083768	−0.000019129
House	−0.0030184	0.0052921	0.0032035
House2	−0.0043876	−0.0059352	0.0000076582
Sailboat	0.0013155	−0.0048803	0.00083999
Tree	0.0020466	−0.0035259	0.0024777



(a) Plain Lena image.



(b) Encrypted Lena image.

FIGURE 24. 3D plots of the correlation coefficient matrix of the plain and encrypted Lena image.

of [30], reportedly having a key space of $(2 \times 10^{15})^3 \times 10^2 \times 256^{65,536\times 3} \approx \infty$, our proposed image cryptosystem is shown to have a superior key space in comparison to its counterparts from the literature.

K. ENCRYPTION TIME ANALYSIS

In order for an image cryptosystem to be suitable for real-time applications and usage on portable wireless devices, its

TABLE 11. Correlation coefficient comparison of plain and encrypted Lena image color channels with the literature.

Schemes	R			G			B		
	H	D	V	H	D	V	H	D	V
Plain	0.952474	0.928029	0.975913	0.935628	0.910534	0.966647	0.917439	0.888482	0.947961
Proposed	−0.000322076	0.000326725	0.0041215	−0.00190115	−0.00310607	−0.00737188	0.00482435	0.00308685	0.00352459
[30]	0.0021	−0.0026	0.0018	−0.0006	0	0.0004	−0.005	−0.0104	0.001
[6]	−0.00364	0.00016	0.000697	0.000118	0.00177	−0.0011	−0.00164	−0.00523	0.006041
[24]	0.006559	−0.00145	0.002	0.00295	−0.001739	0.001745	−0.00278	0.000744	0.0051
[65]	0.001365	0.000232	0.004776	0.003294	0.004807	−0.000579	0.002060	−0.004043	0.000194

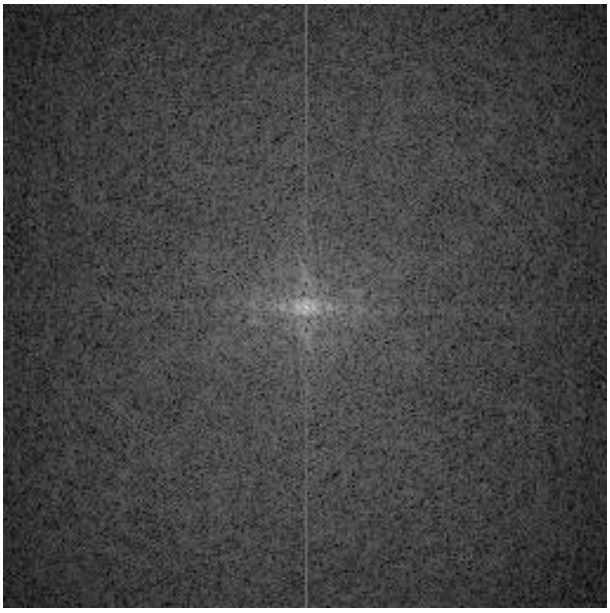
TABLE 12. Correlation coefficient comparison between plain and encrypted Lena images.

Direction	Horizontal	Diagonal	Vertical
Plain	0.938611	0.913175	0.96833
Proposed	0.00797842	−0.000125306	0.00115838
[6]	0.002287	−0.00132	−0.00160
[24]	0.003265	−0.00413	0.002451
[34]	0.0054	0.0054	0.0016
[56]	−0.0082	−0.0012	−0.0128

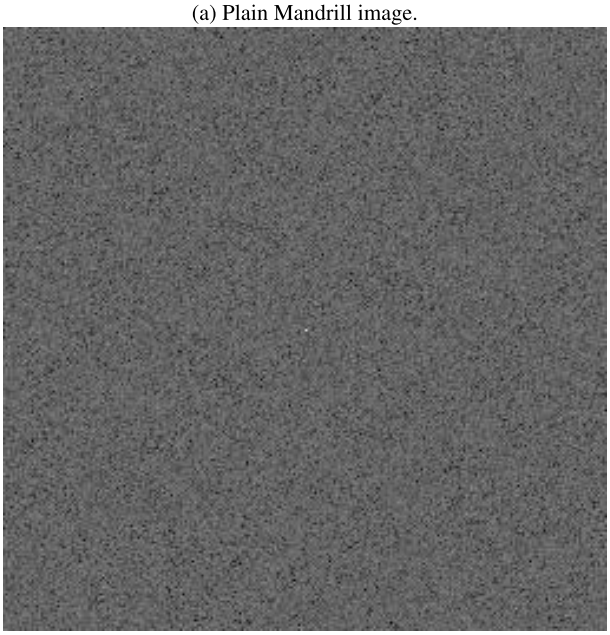
execution time needs to be relatively low. This is the case for the proposed cryptosystem, which carries out image encryption at an average of 4.369 Mbps. Table 18 displays the execution times needed for the proposed image cryptosystem at various image dimensions. For practical usage on portable devices, an image of dimensions 256×256 needs needs about one-third of a second to be encrypted or decrypted. Furthermore, upon comparing the execution time of the proposed cryptosystem with counterparts algorithms from the literature, Table 19 clearly showcases the superior real-time performance of the proposed image cryptosystem, as compared to counterpart algorithms from the literature. It is important to note that the measured and reported encryption times of the various algorithms are not solely due to an algorithm's inherent complexity, but they are in fact also functions of the characteristics of the machine on which the algorithm is processed, in terms of its processing power and available random access memory (RAM), as well as the software package or programming language on which the algorithm runs.

L. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ANALYSIS

The National Institute of Standards and Technology's (NIST) SP 800 analysis is a reliable method for measuring the randomness of encrypted images. It comprises a series of tests performed on a bitstream to evaluate its performance as a PRNG. To pass any of the tests, a bitstream's probability, or $p-$value, must be larger than 0.01. For our proposed image cryptosystem, we demonstrate that a long sequence of bits formed by concatenating the rows of a large encrypted image passes the NIST examination. Table 20 displays the results of a NIST analysis performed on each of the RGB color channels of a 256-by-256-pixel Mandrill image for illustrative purposes. All of the computed values in Table 20 are clearly more than 0.01, demonstrating that the proposed image cryptosystem passes the NIST examination.



(a) Plain Mandrill image.



(b) Encrypted Mandrill image.

FIGURE 25. Fourier transform of the plain and encrypted Mandrill images.

M. S-BOX PERFORMANCE ANALYSIS

As a consistent element that is nearly always at the heart of any image cryptosystem, and as it is responsible for applying

TABLE 13. Histogram dependency tests for various images.

Image	Color	β (23)	γ (24)	τ (25)	ρ (26)	r (27)
Lena	Red	−0.0790594	−0.0648197	−0.0648197	−0.0903261	−0.0903261
	Green	−0.0557897	−0.0145591	−0.0143864	−0.0192951	0.0167818
	Blue	−0.011835	0.00940461	0.00940461	0.0105536	0.0131596
	Combined	0.153245	0.112667	0.11203	0.160838	0.124326
Peppers	Red	0.00793775	0.0108023	0.0105619	0.0133232	0.0713354
	Green	0.0160067	−0.0322217	−0.0318883	−0.0402633	−0.028904
	Blue	0.015749	−0.0246168	−0.0242389	−0.0365687	−0.0231623
	Combined	0.015749	0.00201669	0.00200402	0.00419139	0.00795007
Mandrill	Red	0.015877	0.0640773	0.0634211	0.0948675	0.107755
	Green	−0.015944	0.0267866	0.0263019	0.0388898	0.0622873
	Blue	−0.0238155	−0.0127349	−0.0126171	−0.0197281	−0.028192
	Combined	0.078125	0.0630927	0.0627357	0.0932775	0.0817397
House	Red	0.019804	0.0146408	0.0142064	0.0206739	0.0481415
	Green	−0.0625	−0.00476429	−0.00471042	−0.00735313	−0.0420009
	Blue	−0.0524412	−0.0454195	−0.0434216	−0.061722	−0.121295
	Combined	0.078125	0.0502096	0.0498746	0.0717279	0.0381506
House2	Red	−0.03125	−0.0314876	−0.0309667	−0.0471004	−0.0570892
	Green	−0.0758962	−0.0124321	−0.0123122	−0.0179482	0.0186552
	Blue	−0.0881506	−0.0808928	−0.0795777	−0.117383	−0.0803996
	Combined	−0.078125	−0.0539779	−0.0536898	−0.0811651	−0.0508163
Girl	Red	0.030808	−0.0360147	−0.0303517	−0.045062	−0.0578528
	Green	0.0362369	0.00334836	0.00277394	0.00490064	0.0202396
	Blue	−0.0135084	−0.0020532	−0.00166414	−0.0019811	0.0240379
	Combined	−0.00396106	0.0140088	0.0133777	0.0194152	0.0518811
F16	Red	−0.111129	−0.0837964	−0.0818473	−0.114845	0.0355151
	Green	0.0517084	0.000470352	0.000464924	0.00679854	−0.0499089
	Blue	−0.0477673	−0.0479584	−0.0449149	−0.0659138	−0.042241
	Combined	0.015625	−0.0378026	−0.0375592	−0.057952	−0.0337486
Tree	Red	0.00797096	−0.0162066	−0.0158976	−0.0233341	−0.0716159
	Green	0.00397706	0.0698246	0.0688178	0.102906	0.0843898
	Blue	−0.0156864	−0.00477295	−0.00458907	−0.00851525	0.00497167
	Combined	−0.078745	−0.0368505	−0.0365771	−0.0552284	−0.0367142

TABLE 14. NPCR values for the RGB channels of the Lena image.

RGB	Proposed	[48]	[6]	[25]	[34]	[24]
R	99.636	99.635	99.611	99.606	99.58	99.626
G	99.591	99.625	99.611	99.615	99.56	99.62
B	99.638	99.615	99.637	99.623	99.64	99.695

TABLE 15. UACI values for the RGB channels of the Lena image.

RGB	Proposed	[48]	[6]	[25]	[34]	[24]
R	33.097	33.465	33.415	33.411	33.27	33.031
G	30.723	33.455	30.39	33.465	33.36	30.727
B	27.701	33.455	33.242	33.49	33.50	27.611

TABLE 16. MAE values comparison of various images.

Image	Proposed	[34]	[6]	[24]
Lena	77.7932	87	77.3752	78.3564
Peppers	81.8995	–	81.7740	82.3273
Mandrill	75.3317	92	75.1659	81.913
F16	83.1831	–	–	–
Girl	90.1524	–	–	–
House	75.2815	–	–	–
House2	78.4004	–	–	–
Sailboat	81.8042	–	–	–
Tree	81.6185	–	–	–

Shannon's property of confusion, an S-box should be assessed independently of the whole cryptosystem. In order to assess the confusion capabilities of an S-box, 5 tests are often

TABLE 17. Key space values comparison.

Scheme	Key space
Proposed	$10^{244} \approx 2^{744}$
[6]	10^{128}
[9]	2^{299}
[24]	2^{372}
[25]	10^{169}
[30]	∞

TABLE 18. Execution time of the proposed image cryptosystem, shown here in as encryption time, decryption time, and their added values, for the Lena image at various dimensions.

Image Dimensions	t_{Enc} [s]	t_{Dec} [s]	t_{Add} [s]
64×64	0.022	0.022	0.044
128×128	0.082	0.091	0.173
256×256	0.32	0.31	0.63
512×512	1.33	1.33	2.66
1024×1024	5.76	5.78	11.54

administered [39]. The first test is nonlinearity (NL), which is the number of bits in a Boolean function's truth table that must be altered to approach the nearest affine function. The second test is the linear approximation probability (LAP), which determines the likelihood of bias for a certain S-box. The third test is the differential approximation probability (DAP), which measures the effect of certain changes in inputs on the output. The fourth test is the bit independence

TABLE 19. Encryption time comparison of the Lena image of dimensions 256 × 256.

Scheme	Time [s]	Machine specifications (CPU and RAM)
Proposed	0.32	3.3 GHz AMD® Ryzen 9 5900HX, 32 GB
[6]	2.582389	2.9 GHz Intel® Core™ i9, 32 GB
[24]	1.42545	2.9 GHz Intel® Core™ i9, 32 GB
[9]	0.25	N/A
[63]	1.112	3.4 GHz Intel® Core™ i3, 4 GB

TABLE 20. NIST analysis on the RGB color channels of an encrypted Mandrill image.

Test Name	Red	Green	Blue	Remarks
Frequency	0.372954	0.056971	0.340499	Success
Block Frequency	0.704631	0.912734	0.068156	Success
Run	0.366008	0.823602	0.908698	Success
Long runs of ones	0.905041	0.395569	0.280846	Success
Rank	0.020980	0.823602	0.977743	Success
Spectral FFT	0.048540	1.000000	0.034399	Success
Non overlapping	0.801225	0.936962	0.872090	Success
Overlapping	0.756541	0.858086	0.461852	Success
Universal	0.424700	0.729189	0.607299	Success
Serial	0.626962	0.330943	0.289701	Success
Serial	0.102496	0.392653	0.777191	Success
Approx. entropy	0.029964	0.015296	0.481289	Success
Cum. sums forward	0.561173	0.082559	0.225777	Success
Cum. sums reverse	0.127064	0.100631	0.510922	Success

TABLE 21. Evaluation metrics for the S-box generated using the 4D hyperchaotic Chen system of fractional-order (shown in Table 1). The values used for the keys are $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$.

Evaluation Method	Optimal Score	Score of Proposed Cryptosystem
NL	112	106
SAC	0.5	0.472656
BIC	112	68
LAP	0.0625	0.234375
DAP	0.0156	0.01562

criterion (BIC), which assesses the relationship between the encryption technique and repeating patterns in the resulting encrypted output. The fifth test is the strict avalanche criteria (SAC), which assesses the rate of change in the encrypted output relative to the rate of change in the input on a bit-by-bit basis.

The proposed S-box, which is generated utilizing a 4D hyperchaotic Chen system of fractional-order with the keys $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$, is evaluated employing the 5 aforementioned tests, and the results are shown in Table 21. It is clear that not all optimal values were met. Our achieved DAP value is congruent with the optimal DAP score of 0.0156. This is followed by the NL and SAC, where both are in close proximity to the optimal scores of 112 and 0.5, respectively. However, a clear deviation from the optimal scores is noted for the BIC and LAP, with their optimal scores being 112 and 0.0625, while our achieved scores are 68 and 0.234375. Such a shortcoming in 2 out of 5 testing criteria can be explained as follows. In the design and development of our S-box, we make use of a hyperchaotic function which results in pseudo-randomness.

TABLE 22. Comparison between the proposed S-box (generated using keys $\{x, y, z, u\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 28$, $d = 0.5$, and $\alpha = 0.97$.) and those provided in the literature.

S-Box	NL	SAC	BIC	LAP	DAP
Proposed	106	0.47266	68	0.23438	0.015625
[1]	112	0.4998	112	0.0625	0.0156
[39]	112	0.500977	112	0.0625	0.015625
[40]	110	0.5034	103.5	0.133	0.039
[61]	107	0.497	103.5	0.1560	0.039

This is indeed one way to generate an S-box, however, it does not inherently take into consideration the 5 tests of S-box design. On the other side though, the utilization of this hyperchaotic system leads to the introduction of 7 keys, and thus an increase in the key space by 2^{372}, effectively contributing to the overall robustness and resilience of the proposed image cryptosystem against cryptanalysis.

V. CONCLUSION AND FUTURE WORK

In this research work, we proposed an image cryptosystem that is based on 3 stages. In the first stage, the data bits of a plain image are XORed with a secret key that is based on the Sine chaotic map. In the second stage, a 4D Chen hyperchaotic map of fractional order is used to generate an S-box and apply it to the output of the first encryption stage. In the third stage, a hybrid form of DNA coding is utilized, whereby different logical operations could be applied to the output of the second encryption stage. Finally, this results in an encrypted output image. We have subjected a number of such encrypted images from the image processing community to a plethora of tests to gauge the security and robustness performance of our proposed image cryptosystem. Those included computation and comparison with the state of the art algorithms in terms of visual checks, histogram checks, MSE, PSNR, information entropy, correlation coefficients, Fourier transformation, histogram dependency tests, differential attack analyses, key space analysis, execution time analysis, a NIST analysis, and finally an S-box performance analysis. The various conducted analyses showcase excellent encryption performance that is comparable and sometimes superior to counterpart algorithms from the literature. A future work could attempt to employ a HD chaotic map could be employed in the first stage of encryption, instead of the LD sine map. While this would improve the security and robustness of the proposed image cryptosystem even further, it would however invariably introduce more complexity in the design, and thus more complexity in software and hardware implementations.

REFERENCES

[1] J. A. Aboytes-González, J. S. Murguía, M. Mejía-Carlos, H. González-Aguilar, and M. T. Ramírez-Torres, "Design of a strong S-box based on a matrix approach," *Nonlinear Dyn.*, vol. 94, no. 3, pp. 2003–2012, Nov. 2018.

[2] F. Ahmed, M. U. Rehman, J. Ahmad, M. S. Khan, W. Boulila, G. Srivastava, J. C.-W. Lin, and W. J. Buchanan, "A DNA based colour image encryption scheme using a convolutional autoencoder," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 19, no. 3s, pp. 1–21, Oct. 2023.

[3] A. H. S. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "Generating a new S-box inspired by biological DNA," *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 32–42, 2015.

[4] W. Alexan, A. Ashraf, E. Mamdouh, S. Mohamed, and M. Moustafa, "IoMT security: SHA3–512, AES-256, RSA and LSB steganography," in *Proc. 8th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2021, pp. 177–181.

[5] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Image encryption through Lucas sequence, S-box and chaos theory," in *Proc. 8th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2021, pp. 77–83.

[6] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, S-box and the Lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, Feb. 2022.

[7] W. Alexan, A. Elkhateeb, E. Mamdouh, F. Al-Seba'Ey, Z. Amr, and H. Khalil, "Utilization of corner filters, AES and LSB steganography for secure message transmission," in *Proc. Int. Conf. Microelectron. (ICM)*, Dec. 2021, pp. 29–33.

[8] W. Alexan, E. Mamdouh, M. ElBeltagy, F. Hassan, and P. Edward, "Image feature-based watermarking," in *Proc. Int. Telecommun. Conf. (ITC-Egypt)*, Jul. 2022, pp. 1–6.

[9] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19853–19873, Jul. 2020.

[10] A. Arora and R. K. Sharma, "Known-plaintext attack (KPA) on an image encryption scheme using enhanced skew tent map (ESTM) and its improvement," *Optik*, vol. 244, Oct. 2021, Art. no. 167526.

[11] B. Chen, M. Yu, Q. Su, H. J. Shim, and Y. Shi, "Fractional quaternion Zernike moments for robust color image copy-move forgery detection," *IEEE Access*, vol. 6, pp. 56637–56646, 2018.

[12] J.-J. Chen, D.-W. Yan, S.-K. Duan, and L.-D. Wang, "Memristor-based hyper-chaotic circuit for image encryption*," *Chin. Phys. B*, vol. 29, no. 11, Nov. 2020, Art. no. 110504.

[13] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Inf. Sci.*, vol. 520, pp. 130–141, May 2020.

[14] A. El-Mahdy and W. Alexan, "A comparative study on the performance of LLR- and SNR-based hybrid relaying schemes," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–7, Jan. 2017.

[15] A. El Mahdy and W. Alexan, "A threshold-free LLR-based scheme to minimize the BER for decode-and-forward relaying," *Wireless Pers. Commun.*, vol. 100, no. 3, pp. 787–801, Jun. 2018.

[16] M. A. Elaziz, K. M. Hosny, A. Salah, M. M. Darwish, S. Lu, and A. T. Sahlol, "New machine learning method for image-based diagnosis of COVID-19," *PLoS ONE*, vol. 15, no. 6, Jun. 2020, Art. no. e0235187.

[17] M. ElBeltagy, W. Alexan, A. Elkhamry, M. Moustafa, and H. H. Hussein, "Image encryption through Rössler system, PRNG s-box and Recamán's sequence," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2022, pp. 0716–0722.

[18] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools Appl.*, vol. 81, pp. 25497–25518, Mar. 2022.

[19] M. Essaid, I. Akharraz, A. Saaidi, and E. A. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–187, Aug. 2019.

[20] S. Farrag and W. Alexan, "Secure 3D data hiding technique based on a mesh traversal algorithm," *Multimedia Tools Appl.*, vol. 79, nos. 39–40, pp. 29289–29303, Oct. 2020.

[21] M. Gabr, W. Alexan, K. Moussa, B. Maged, and A. Mezar, "Multi-stage RGB image encryption," in *Proc. Int. Telecommun. Conf. (ITC-Egypt)*, Jul. 2022, pp. 1–6.

[22] M. Gabr, H. H. Hussein, and W. Alexan, "A combination of decimal- and bit-level secure multimedia transmission," in *Proc. Workshop Microw. Theory Techn. Wireless Commun. (MTTW)*, Oct. 2022, pp. 177–182.

[23] M. Gabr, H. Younis, M. Ibrahim, S. Alajmy, I. Khalid, E. Azab, R. Elias, and W. Alexan, "Application of DNA coding, the Lorenz differential equations and a variation of the logistic map in a multi-stage cryptosystem," *Symmetry*, vol. 14, no. 12, p. 2559, Dec. 2022.

[24] J. Griffin, "The sine map," *Retrieved May*, vol. 4, p. 2018, May 2013.

[25] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools Appl.*, vol. 79, pp. 7279–7297, Mar. 2020.

[26] A. S. Hegazi and A. E. Matouk, "Dynamical behaviors and synchronization in the fractional order hyperchaotic Chen system," *Appl. Math. Lett.*, vol. 24, no. 11, pp. 1938–1944, Nov. 2011.

[27] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "Novel encryption for color images using fractional-order hyperchaotic system," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 2, pp. 973–988, Feb. 2022.

[28] M. A. Iliyasu, O. A. Abisoye, S. A. Bashir, and J. A. Ojeniyi, "A review of DNA cryptograhic approaches," in *Proc. IEEE 2nd Int. Conf. Cyberspac (CYBER NIGERIA)*, Feb. 2021, pp. 66–72.

[29] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, M. Hanif, S. Abbas, and D. Hussain, "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[30] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102428.

[31] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.

[32] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Appl. Phys. B*, vol. 126, no. 9, pp. 1–19, Sep. 2020.

[33] P. Kaur, H. S. Pannu, and A. K. Malhi, "Plant disease recognition using fractional-order Zernike moments and SVM classifier," *Neural Comput. Appl.*, vol. 31, no. 12, pp. 8749–8768, Dec. 2019.

[34] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Sep. 2019.

[35] M. Kumari and S. Gupta, "Performance comparison between chaos and quantum-chaos based image encryption techniques," *Multimedia Tools Appl.*, vol. 80, no. 24, pp. 33213–33255, Oct. 2021.

[36] H. Liu, X. Wang, and A. Kadir, "Chaos-based color image encryption using one-time keys and Choquet fuzzy integral," *Int. J. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 1, pp. 1–10, Feb. 2014.

[37] X. Liu, X. Tong, Z. Wang, and M. Zhang, "Efficient high nonlinearity S-box generating algorithm based on third-order nonlinear digital filter," *Chaos, Solitons Fractals*, vol. 150, Sep. 2021, Art. no. 111109.

[38] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019.

[39] M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.

[40] A. Manzoor, A. H. Zahid, and M. T. Hassan, "A new dynamic substitution box for data security using an innovative chaotic map," *IEEE Access*, vol. 10, pp. 74164–74174, 2022.

[41] S. M. Mohamed, W. S. Sayed, A. H. Madian, A. G. Radwan, and L. A. Said, "An encryption application and FPGA realization of a fractional memristive chaotic system," *Electronics*, vol. 12, no. 5, p. 1219, Mar. 2023.

[42] I. K. Nti, J. A. Quarcoo, J. Aning, and G. K. Fosu, "A mini-review of machine learning in big data analytics: Applications, challenges, and prospects," *Big Data Mining Analytics*, vol. 5, no. 2, pp. 81–97, Jun. 2022.

[43] L. Paul, C. Gracias, A. Desai, V. Thanikaiselvan, S. S. Shanthini, and A. Rengarajan, "A novel colour image encryption scheme using dynamic DNA coding, chaotic maps, and SHA-2," *Multimedia Tools Appl.*, vol. 81, pp. 37873–37894, Apr. 2022.

[44] S. Vinay, A. Pujar, H. A. Kedlaya, and V. S. Shahapur, "Implementation of DNA cryptography based on dynamic DNA sequence table using cloud computing," *Int. J. Eng. Res. Technol.*, vol. 7, pp. 1–8, Jun. 2019.

[45] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 723–744, Oct. 2018.

[46] H. R. Shakir, S. A. A. Mehdi, and A. A. Hattab, "A dynamic s-box generation based on a hybrid method of new chaotic system and DNA computing," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 20, no. 6, pp. 1230–1238, 2022.

[47] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[48] N. B. Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30993–31019, Dec. 2018.

[49] N. Sun, C. Li, H. Chan, B. Dung Le, M. Z. Islam, L. Y. Zhang, M. R. Islam, and W. Armstrong, "Defining security requirements with the common criteria: Applications, adoptions, and challenges," *IEEE Access*, vol. 10, pp. 44756–44777, 2022.
[50] M. Tanveer, T. Shah, A. Rehman, A. Ali, G. F. Siddiqui, T. Saba, and U. Tariq, "Multi-images encryption scheme based on 3D chaotic map and substitution box," *IEEE Access*, vol. 9, pp. 73924–73937, 2021.
[51] E. Tanyildizi and F. Özkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.
[52] L. Teng, X. Wang, and J. Meng, "A chaotic color image encryption using integrated bit-level permutation," *Multimedia Tools Appl.*, vol. 77, no. 6, pp. 6883–6896, Mar. 2018.
[53] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, "A novel string matrix data structure for DNA encoding algorithm," *Proc. Comput. Sci.*, vol. 46, pp. 820–832, Jan. 2015.
[54] D. Wei and M. Jiang, "A fast image encryption algorithm based on parallel compressive sensing and DNA sequence," *Optik*, vol. 238, Jul. 2021, Art. no. 166748.
[55] J. Wen, X. Xu, K. Sun, Z. Jiang, and X. Wang, "Triple-image bit-level encryption algorithm based on double cross 2D hyperchaotic map," *Nonlinear Dyn.*, vol. 11, pp. 6813–6838, Jan. 2023.
[56] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.
[57] A. Y. Niyat and M. H. Moattar, "Color image encryption based on hybrid chaotic system and DNA sequences," *Multimedia Tools Appl.*, vol. 79, nos. 1–2, pp. 1497–1518, Jan. 2020.
[58] S. Yasser, A. Hesham, M. Hassan, and W. Alexan, "AES-secured bit-cycling steganography in sliced 3D images," in *Proc. Int. Conf. Innov. Trends Commun. Comput. Eng. (ITCE)*, Feb. 2020, pp. 227–231.
[59] B. Y. Irani, P. Ayubi, F. A. Jabalkandi, M. Y. Valandar, and M. J. Barani, "Digital image scrambling based on a new one-dimensional coupled sine map," *Nonlinear Dyn.*, vol. 97, no. 4, pp. 2693–2721, Sep. 2019.
[60] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, Nov. 2018.
[61] A. Zahid, M. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, Mar. 2019.
[62] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13841–13864, Apr. 2021.
[63] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, Mar. 2019.
[64] X. Zhang, L. Wang, Y. Wang, Y. Niu, and Y. Li, "An image encryption algorithm based on hyperchaotic system and variable-step Josephus problem," *Int. J. Opt.*, vol. 2020, pp. 1–15, Oct. 2020.
[65] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106040.
[66] N. Zhou, W. Chen, X. Yan, and Y. Wang, "Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system," *Quantum Inf. Process.*, vol. 17, no. 6, pp. 1–24, Jun. 2018.
[67] S. M. U. Zia, M. McCartney, B. Scotney, J. Martinez, M. Abu-Tair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, pp. 917–935, Apr. 2022.

WASSIM ALEXAN (Senior Member, IEEE) was born in Alexandria, Egypt, in 1987. He received the B.Sc., M.Sc., and Ph.D. degrees in communications engineering and the M.B.A. degree from German University in Cairo (GUC), Egypt, in 2010, 2012, 2017, and 2019, respectively.

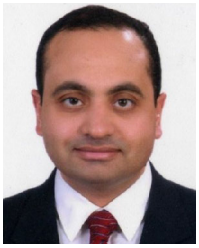
He was with the Mathematics Department, from 2010 to 2017. Since 2017, he has been an Assistant Professor with the Faculty of Information Engineering and Technology, GUC, teaching various courses in relation to wireless communications, modulation and coding, digital logic design, circuit theory, and mathematics. He is also an Adjunct Assistant Professor with the Mathematics Department, German International University (GIU), New Administrative Capital, Egypt, since 2019. He is the author or coauthor of more than 60 journal articles and conference papers. His research interests include wireless communications, information security, image, and signal processing.

Dr. Alexan is also a member of the ACM. He received the Best Paper Award at the 19th IEEE Conference on Signal Processing Algorithms, Architectures, Arrangements and Applications (SPA'2015), Poznan, Poland, the AEG Writer of the Year Award from the American University in Cairo (AUC), Egypt, in 2019, and the Best Poster Award at the 37th IEEE National Radio Science Conference, Cairo, Egypt, in 2020.

MOHAMED GABR (Member, IEEE) was born in Cairo, Egypt, in 1989. He received the B.Sc. and M.Sc. degrees in computer science and engineering from German University in Cairo (GUC), Egypt, in 2011 and 2013, respectively.

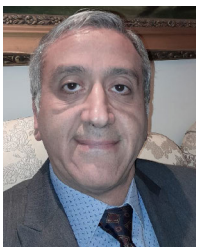
He has been with the Computer Science and Engineering Department, since 2011. He is teaching various courses in relation to computer vision, artificial intelligence, compilers, the theory of computation, and computer graphics. He is the author or coauthor of various journal articles and conference papers. His research interests include computer vision and information security.

EYAD MAMDOUH was born in Cairo, Egypt, in 1999. He received the B.Sc. degree in communication engineering from German University in Cairo (GUC), in 2022. Since 2022, he has been a Teaching Assistant with the Physics Department, GUC. He has published six conference papers in data security, including image encryption and 3D image steganography.



RIMON ELIAS (Senior Member, IEEE) received the M.C.S. and Ph.D. degrees in computer science from the University of Ottawa, Ottawa, ON, Canada, in 1999 and 2004, respectively.

He is the author of *Digital Media* (Springer) and *Modeling of Environments* (Lambert Academic Publishing), and several book chapters, encyclopedia, journal, and conference papers. His research interests include different image-related fields, including computer vision, image processing, computer graphics, and visualization.



AMR ABOSHOUSHA was born in Cairo, Egypt, in 1967. He received the B.Sc. degree (Hons.) in physics and the M.Sc. degree in theoretical physics from the Science Faculty, Cairo University, in 1988 and 1995, respectively, and the Dr. rer. nat. degree in theoretical physics from Friedrich Alexander University Erlangen-Nuerenberg, Germany, in 2001.

From 2002 to 2010, he was a Physics Lecturer with the Physics Department, Science Faculty, Cairo University. During this period, he instructed and supervised various physics courses, such as thermodynamics, electromagnetism, statistical mechanics, computational physics, and optical communications. From 2004 to 2005, he was a reviewer of the Physics Exam Committee of the High School Certificate, Ministry of Education. Since 2010, he has been an Assistant Professor with the Physics Department, Faculty of Engineering, German University in Cairo (GUC), teaching different physics related courses to engineering, biotechnology, and pharmacy students. His research interests include the applications of theoretical physics models in different areas, such as information technology and biophysics.