IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 October 2023, accepted 19 October 2023, date of publication 23 October 2023, date of current version 1 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3326848

RESEARCH ARTICLE

R^3–Rescale, Rotate, and Randomize: A Novel Image Cryptosystem Utilizing Chaotic and Hyper-Chaotic Systems

MOHAMED GABR[1], (Member, IEEE), YOUSEF KORAYEM[1], (Senior Member, IEEE), YEN-LIN CHEN[2], (Senior Member, IEEE), POR LIP YEE[3], (Senior Member, IEEE), CHIN SOON KU[4], AND WASSIM ALEXAN[5,6], (Senior Member, IEEE)

[1]Computer Science Department, Faculty of Media Engineering and Technology, German University in Cairo (GUC), Cairo 11835, Egypt
[2]Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei 106344, Taiwan
[3]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[4]Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia
[5]Communications Department, Faculty of Information Engineering and Technology, German University in Cairo (GUC), Cairo 11835, Egypt
[6]Mathematics Department, German International University (GIU), New Administrative Capital, Cairo 13507, Egypt

Corresponding authors: Yen-Lin Chen (ylchen@mail.ntut.edu.tw), Por Lip Yee (porlip@um.edu.my), and Chin Soon Ku (kucs@utar.edu.my)

This work was supported in part by the National Science and Technology Council in Taiwan under Grant NSTC-112-2221-E-027-088-MY2 and Grant NSTC-111-2622-8-027-009; in part by the Ministry of Education of Taiwan titled "The Study of Artificial Intelligence and Advanced Semiconductor Manufacturing for Female STEM Talent Education and Industry-University Value-Added Cooperation Promotion" under Grant 1122302319; and in part by the Universiti Tunku Abdul Rahman (UTAR) Financial Support for Journal Paper Publication Scheme through Universiti Tunku Abdul Rahman, Malaysia.

ABSTRACT This work proposes a novel image encryption algorithm that integrates unique image transformation techniques with the principles of chaotic and hyper-chaotic systems. By harnessing the unpredictable behavior of the Chua system and the hyper-chaotic nature of the Chen system, the algorithm carries out rescaling, rotation, and randomization on the target image. The intrinsic unpredictability and sensitivity to initial conditions of these chaotic systems endow the encryption algorithm with an expansive key space of 2^{5208}. This feature not only bolsters its resilience against brute-force attacks but also magnifies its overall security profile. The algorithm's efficiency is evident in its rapid computational speed and lean resource consumption, making it suitable for real-time applications. To gauge its robustness, a battery of rigorous tests and analyses, spanning differential attacks, statistical attacks, and brute-force assaults, were employed. The results validate its ability to resist a diverse spectrum of threats. With its expansive key space, exceptional efficiency, and sturdy defenses, the proposed algorithm emerges as a potential cornerstone for safeguarding digital images in arenas like secure communication, data storage, and multimedia transmission. In sum, this research pushes the boundaries of high-security image encryption methodologies, catering to the burgeoning demands of the digital age.

INDEX TERMS Chaos theory, Chen hyper-chaotic system, Chua chaotic system, image cryptosystem, image encryption, rotation.

I. INTRODUCTION

With multimedia data transmission over public networks growing exponentially in recent years, the criticality of efficient image encryption techniques has surged. These techniques are vital for safeguarding images from unauthorized access [1]. While the Advanced Encryption Standard (AES) is adept at text encryption [2], adapting it for image data poses challenges, given the unique properties of images, such as vast data capacity and significant pixel correlation. Recent literature has presented image encryption methods rooted in chaos theory [3], compressive sensing [4], and deep

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

learning [5]. However, these often grapple with inadequate security, computational intricacy, and less-than-optimal real-time performance [6]. This backdrop has fueled the pursuit of streamlined image encryption algorithms that promise potent security while sidestepping these limitations. In response, this paper unveils an innovative image encryption scheme that interweaves permutation and diffusion operations, adhering to Shannon's secure communication tenets [7]. This scheme is engineered to deliver staunch encryption with modest computational demands, positioning it as a prime candidate for real-time secure image transmission.

The ensuing discussion expounds on the significance of rotation techniques in sculpting pseudo-random number generators (PRNGs). This discourse segues into the pivotal role of chaos theory in image encryption. Furthermore, substitution boxes (S-boxes) are spotlighted as quintessential nonlinear elements in image encryption. Recognizing the gaps in existing research, we present our novel R^3 algorithm as a robust remedy for prevalent real-time image encryption challenges.

Rotation techniques are pivotal in contemporary image cryptosystems, predominantly amplifying the complexity and randomness of sequences generated by PRNGs, attributes that are essential for image encryption algorithms [8]. Despite the promise of these techniques, it is paramount to realize that their efficacy is not standalone. Several variables, including the initial seed, PRNG's caliber, and the meticulous integration of cryptographic strategies, exert significant sway over the encryption's fortitude.

The chaotic behavior and initial condition sensitivity inherent in chaos theory render it a linchpin for robust image encryption algorithms [9], [10]. Chaotic maps, with their intricate dynamics and expansive parameter spaces, augment encryption strength. The myriad benefits they offer, from extensive key sensitivity to resistance against a diverse attack spectrum, spotlight chaos theory as an enthralling research domain [11], [12].

Solving chaotic and hyper-chaotic systems of differential equations at a fractional-order, rather than an integer-order can significantly enhance unpredictability and system dynamics complexity [13], [14]. When applied to image cryptosystems, this increased complexity can potentially bolster the security of such algorithms [15], providing a larger key space and enhancing unpredictability and nonlinearity, thereby improving diffusion and confusion properties.

The literature review also underscores the importance of S-boxes in image encryption algorithms [13], [16], [17], [18], [19], and [20]. Incorporating an S-box into the proposed R^3 algorithm enhances the image encryption process's security. An S-box provides a non-linear transformation of the input data, making it significantly harder for an attacker to decipher the encrypted image [13]. In this research, S-boxes contribute to the proposed R^3 algorithm's robustness against various attacks, thereby improving digital image security.

Drawing insights from the above discussions, this paper champions the efficacy of PRNG rotation and fractional-order solutions to chaotic systems. As outlined in the subsequent section (Section II), despite noteworthy strides in image encryption, achieving a harmonious blend of security, efficiency, and real-time performance remains elusive. Our endeavor, through the R^3 (Rescale, Rotate, and Randomize) algorithm, is to bridge this chasm. By hinging on the unpredictable facets of the Chua and Chen systems, R^3 aspires to redefine the paradigms of image encryption efficiency and security. Its offerings span an expansive key space, staunch defenses against a plethora of attacks, and potential applications in secure communication, data storage, and multimedia transmission. The salient contributions of our proposed image cryptosystem encompass:

1) A 2-stage image encryption predicated on fractional-order chaotic and hyper-chaotic system solutions.
2) Enhanced security and robustness through rotation, rescaling, and randomization algorithms.
3) Enhanced encryption efficiency via advanced parallel processing, achieving an average rate of 2.13 Mbps.
4) A colossal key space of 2^{5208}, renders brute-force attacks futile.
5) Unyielding resistance against an array of cryptanalyses, spanning from visual to differential.
6) Conformity with all NIST SP 800 − 22 randomness tests, along with TestU01 analyses.

The remainder of this article is structured as follows: In Section II: Related Works, a literature review of related image cryptosystems is presented. Section III: Preliminary Studies introduces the chaotic and hyper-chaotic systems of differential equations used in the proposed image cryptosystem. Section IV: Proposed Scheme details the encryption and decryption procedures, complete with their algorithms and flowcharts. Section V: Performance Analysis showcases the results of various analyses conducted to evaluate the performance of the proposed image cryptosystem. Lastly, Section VI: Conclusions and Future Work concludes the article and suggests potential directions for future research.

II. RELATED WORKS

This section attempts to delve into the significant prior research and developments in the field of image encryption. It examines various methodologies and techniques that have been proposed, highlighting their strengths and limitations. This review not only provides context for our study but also underscores the innovation and necessity of our proposed image encryption algorithm. The following studies were instrumental in shaping the research direction and methodology of this work:

The authors of [21] propose an image encryption algorithm based on chaos theory, the use of the hash functions SHA-256 and SHA-512, as well as an image rotation matrix. While a limited security analysis is provided in their work, their proposed algorithm is shown to perform well. In [22],

an image encryption algorithm that carries out permutation and substitution based on 4 Chebyshev chaotic maps and rotation equations is proposed. Their proposed algorithm is shown to be highly efficient, encrypting 512 × 512 images in only 290 ms. Multiple rounds of DNA coding are carried out in an image cryptosystem proposed by the authors of [23], where they generate a 16 × 16 rotational DNA Playfair matrix using the chaotic logistic map. While their proposed algorithm is shown to pass various security analyses, it is very inefficient, encrypting 256 × 256 images in only 7 to 9 s. The work proposed in [24] makes use of a bit-plane matrix rotation, the Lorenz hyper-chaotic system, as well as a 6D hyper-chaotic system, in addition to the MD5 hash function, to carry out image encryption. A large key space of 2^{544} is the strongest metric computed and presented in the work of [24]. The authors of the work described in [25] carry out a rotational mechanism in a very interesting manner by rotating the axes of the 3 employed chaotic systems (Newton-Leipnik, Liu, and Financial) by an angle θ. Furthermore, their work applies a dynamic switched synchronized scheme. However, a limited security analysis is offered, and no mention of the algorithm's efficiency is made therein. The authors of [26] propose a medical image cryptosystem that is based on chaotic functions, block rotation, and DNA coding. In their cryptosystem, several chaotic maps under the sine transform framework are utilized to produce seeds for block rotation. Next, DNA coding is carried out. The proposed cryptosystem is shown to be resistant to various cryptanalyses. An interesting work is proposed in [27], where the rotation of pixels is related to the idea of the rotation of planets around their orbits. This is achieved by the authors by viewing the changes in the locations of planets around their orbits and associating them with the pixel shuffling technique. Further, they combine the rotations with chaotic sequences to scramble the pixel positions in plain images. Novel S-boxes are constructed in [28], where the authors realize the importance of introducing non-linearity into an image cryptosystem and the effectiveness of S-boxes at achieving just that. In their work, they employ the Hindmarsh-Rose system to generate S-boxes of chaotic nature. Two S-boxes are proposed in [28]. The first is based on a rotation algorithm in relation to the rows and columns, while the other is based on a zigzag transform. The proposed S-boxes are tested using the commonly utilized metrics found in the literature and are shown to perform well in an image cryptosystem. A gray-scale image encryption algorithm is proposed in [29] that is based on the scrambling rotations in a Rubik's cube to emulate pixel position permutations. Moreover, the work in [29] makes use of the quantum XOR operation and the quantum SWAP operation. The main advantage of this work is the improved efficiency achieved through the use of quantum methods over traditional ones. A very recent work by the authors of [30] develops an unsupervised deep learning algorithm trained on chaotic maps to build a generative adversarial network (GAN). This GAN is then utilized to provide encryption keys as input to newly designed S-boxes and P-boxes. The proposed GAN-based algorithm in [30] is shown to carry out encryption both at the bit-level and byte-level, performing very well in comparison to counterpart algorithms from the literature. In [31], the authors re-imagine 2D images as circular objects, or rotors, which can be rotated in clockwise or anti-clockwise directions, such that these rotations can be used to substitute the image pixels. The adopted rotation mechanism in [31] is jointly applied with a permutation that is based on a logistic sequence. Next, a Piece-wise Linear Chaotic Map (PWLCM) and the Chen system of differential equations are utilized to induce further rotations. Moreover, the seeds for the Chen system are based on the SHA-512 of the plain images input to the algorithm. Various performance analyses are conducted, showcasing the superior security of the work in [31].

In conclusion, the body of existing literature clearly indicates the increasing significance of robust and efficient image encryption techniques in the age of ubiquitous multimedia data transmission. While there have been numerous methodologies proposed, many of them have been found to exhibit significant shortcomings, such as susceptibility to various types of attacks, high computational complexity, and inadequate real-time performance. Notably, the exploration of chaotic and hyper-chaotic systems in the context of image encryption has shown promising results due to their inherent unpredictability and high sensitivity to initial conditions. However, there remains a wide scope for further improvement and innovation in this domain, particularly in terms of leveraging advanced concepts like fractional-order solutions and rotation mechanisms to enhance security. The subsequent sections of this article will introduce and detail a novel image cryptosystem that aims to address the existing gaps in the field by employing a unique combination of image transformations and the principles of chaotic and hyper-chaotic systems.

III. PRELIMINARY STUDIES

The proposed image cryptosystem is mainly divided into 2 main stages. Each stage utilizes a dynamical system (Chen and Chua) and consists of 3 main subroutines, namely, rotation, S-box, and XOR. Each of the HD systems and the subroutines utilized in the cryptosystem are discussed below.

A. CHEN SYSTEM

The Chen system is characterized as a hyper-chaotic system with more than one positive Lyapunov exponent. For such a characterization, it presents itself as a sufficient candidate for PRNG sequence generation, which is later utilized in 3 separate encryption subroutines (rotation, S-box, and XOR, as later discussed). Moreover, as a system in 4D space, many variables and coefficients present themselves as control parameters. The role of these control parameters is to change the behavior of the solution of the system, which changes the resulting PRNG sequence generated in the process. Alongside that, from the perspective of image encryption,

it is beneficial to construct a cryptosystem with a large key space.

The hyper-chaotic 4D Chen system is equated as per the following 4 differential equations (for x, y, z, and u, respectively) [32], [33]:

$$\begin{cases} D^{\alpha_x}x = a(y-x)+u, \\ D^{\alpha_y}y = \gamma x - xz + cy, \\ D^{\alpha_z}z = xy - bz, \\ D^{\alpha_u}u = yz + du, \end{cases} \tag{1}$$

In (1), the control variables are divided into 3 groups. The first group is the initial values for x, y, z, and u (or x_0, y_0, z_0, and u_0). The second group, a, b, c, γ, and d, are the scale coefficients. The last group, α_x, α_y, α_z, and α_u are values of fractional-order differentiation. These 3 groups combined introduce 13 variables, contributing a total of 52 variables to the overall cryptosystem (as this system is utilized 4 times). For demonstration, Fig. 1 shows an example plot for the 4D Chen system in (1). Hue colors are utilized in Fig. 1, where warmer colors present initial values and cooler colors present terminal ones.

Bifurcation diagrams of the system in (1) are plotted in Figs. 2, 3, and 4 for changing values of the variables b, c, and d, respectively. These diagrams present a visual representation of the transitions or bifurcations the system in (1) undergoes as a parameter is varied. Such diagrams are a powerful tool for analyzing the complex behavior of the Chen system. In the context of a 4D hyper-chaotic system, a bifurcation diagram can reveal a multitude of dynamical behaviors, including fixed points, periodic orbits, bifurcations, chaos, and hyperchaos. More specifically, a bifurcation happens when a small, smooth change made to the system parameters causes a sudden 'qualitative' or topological change in its behavior. In Figs. 2, 3, and 4, the horizontal axes represent the varied parameters (b, c, and d), while the vertical axes show the possible long-term values (equilibrium values or periodic orbits) of the Chen system in (1) for each value of those parameters.

Lyapunov exponents are a measure of the rate at which nearby trajectories in a system diverge or converge over time. In a 4D system, there are 4 Lyapunov exponents. A positive Lyapunov exponent indicates that trajectories diverge exponentially over time, which is a signature of chaotic behavior. Conversely, a negative exponent suggests that trajectories converge, indicating stable behavior. The 4D Chen system in (1) is shown to be hyper-chaotic in Fig. 5, displaying positive Lyapunov exponents.

B. CHUA SYSTEM

Another system that exhibits chaotic behavior is the Chua system [34]. As in the case with the Chen system, the chaotic behavior along with the large number of control variables enlarges the potential benefit of utilizing the Chua system as a component of image cryptosystems, as in this work. The Chua, as a 3D system, is equated as follows:

$$\begin{cases} D^{\alpha_x}x = p(y - x - f(a,b,x)), \\ D^{\alpha_y}y = x - y + z, \\ D^{\alpha_z}z = -qy, \end{cases} \tag{2}$$

given that,

$$f(a,b,x) = bx + \frac{1}{2}(a-b)(|x+1| - |x-1|) \mid a < b < 0. \tag{3}$$

As presented in (2), there are a total of 10 control variables, which can be divided into 3 groups. The first group contains the initial values for x, y, and z (or x_0, y_0, and z_0). The second group consists of scale factors: p and q for the main axis equations (2), and a and b for (3). The last group contains the fractional-order differential values α_x, α_y, and α_z. All 3 groups combined contribute a total of 40 variables to the overall cryptosystem (as they are utilized 4 times). As an illustration, Fig. 6 displays an example plot for the fractional-order 3D Chua system. As earlier, hue colors are utilized in Fig. 6, such that warmer colors present initial values and cooler colors present terminal ones. To test for and showcase the chaotic behavior of the 3D Chua system in (2), bifurcation diagrams are plotted and shown in Figs. 7, 8, and 9, while a Lyapunov characteristic exponents' plot is shown in Fig. 10.

C. SYSTEMS' SOLUTION PRIME ROTATION EXPANSION

As discussed earlier, the utilization of fractional-order differential equations has had a great effect on the field of image encryption. In this work, to add an extra layer of confusion to the systems' solution, a novel approach is proposed. In this approach, instead of solving the system for the full length needed (the image size, for example), only a subset of that is generated. For the remaining sequence length in demand, the generated set is recursively duplicated post-rotation by a changing prime factor. Given a required sequence length l, a prime seed p, and a PRNG sequence s of length less than l, Algorithm 1 is used to generate a PRNG sequence of the required length.

Algorithm 1 Prime Rotation Expansion for a Sequence s, Using Prime Seed p, to Reach Length l

$s' \leftarrow s \ll p$
Appendto(s, s')
$p \leftarrow$ *NextPrime*(p)
if *Length*$(s) < l$ **then**
    GoTo 1
else
    return the first l elements of s
end if

D. KEY APPLICATION USING ROTATION

Aside from the common mechanism of key application using the logical XOR operator, in this work, a different approach

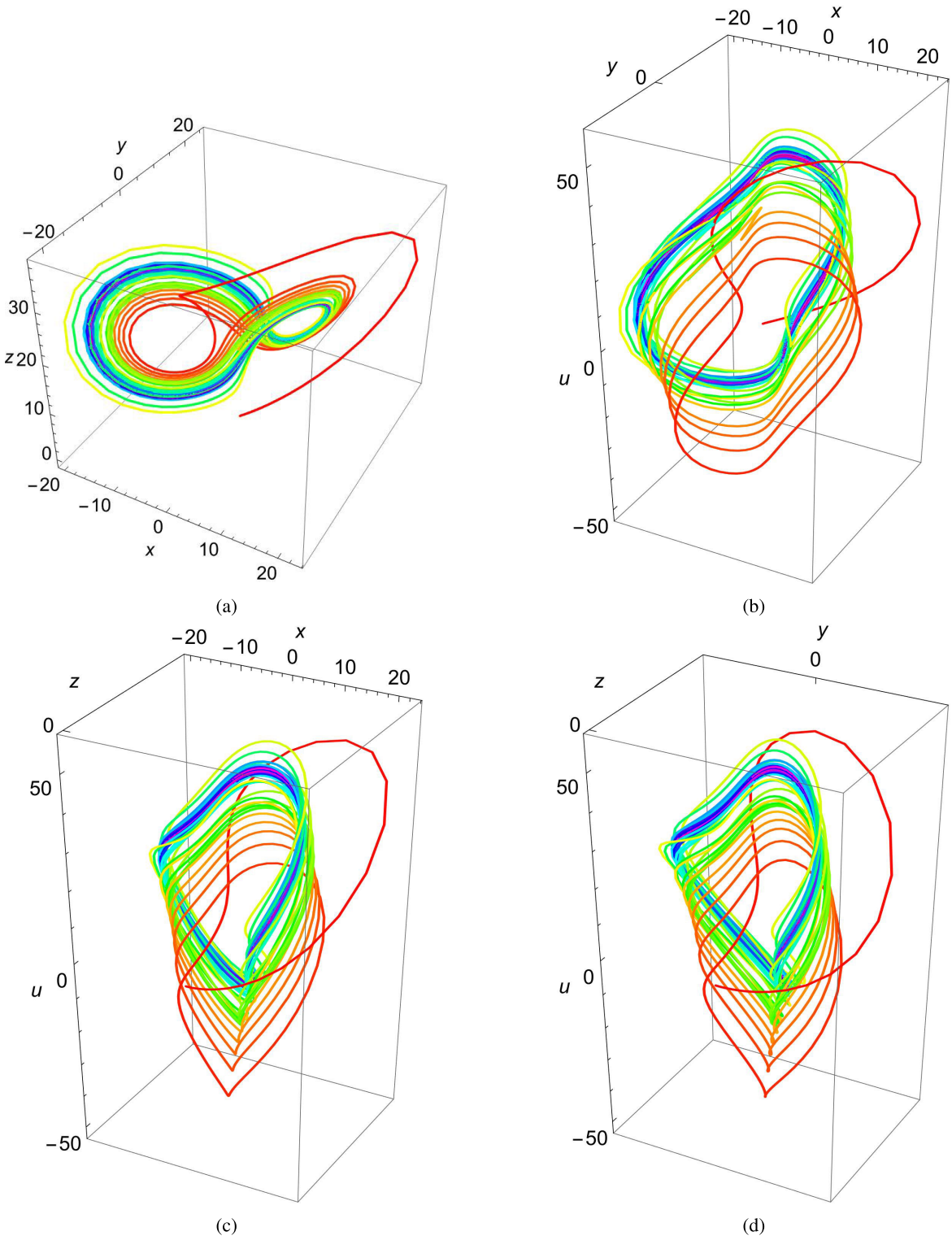


FIGURE 1. The fractional-order 4D Chen system is numerically solved and plotted here in various 3D spaces for $\{x_0, y_0, z_0, u_0\} = 0.3$, $a = 35$, $b = 3$, $c = 12$, $\gamma = 7$, $d = 0.5$, and $\{\alpha_x, \alpha_y, \alpha_z, \alpha_u\} = 0.97$ (a) X-Y-Z space; (b) X-Y-U space; (c) X-Z-U space; (d) Y-Z-U space.

is applied. As this approach is based on bit-wise rotation, transforming the image into a higher numerical base than bit-level, performed by forming subsets of the bit set of an image, becomes a necessity. In this perspective, the direction of the rotation (left or right) can be changed independently from one subset of bits to the other, utilizing a bit stream as a

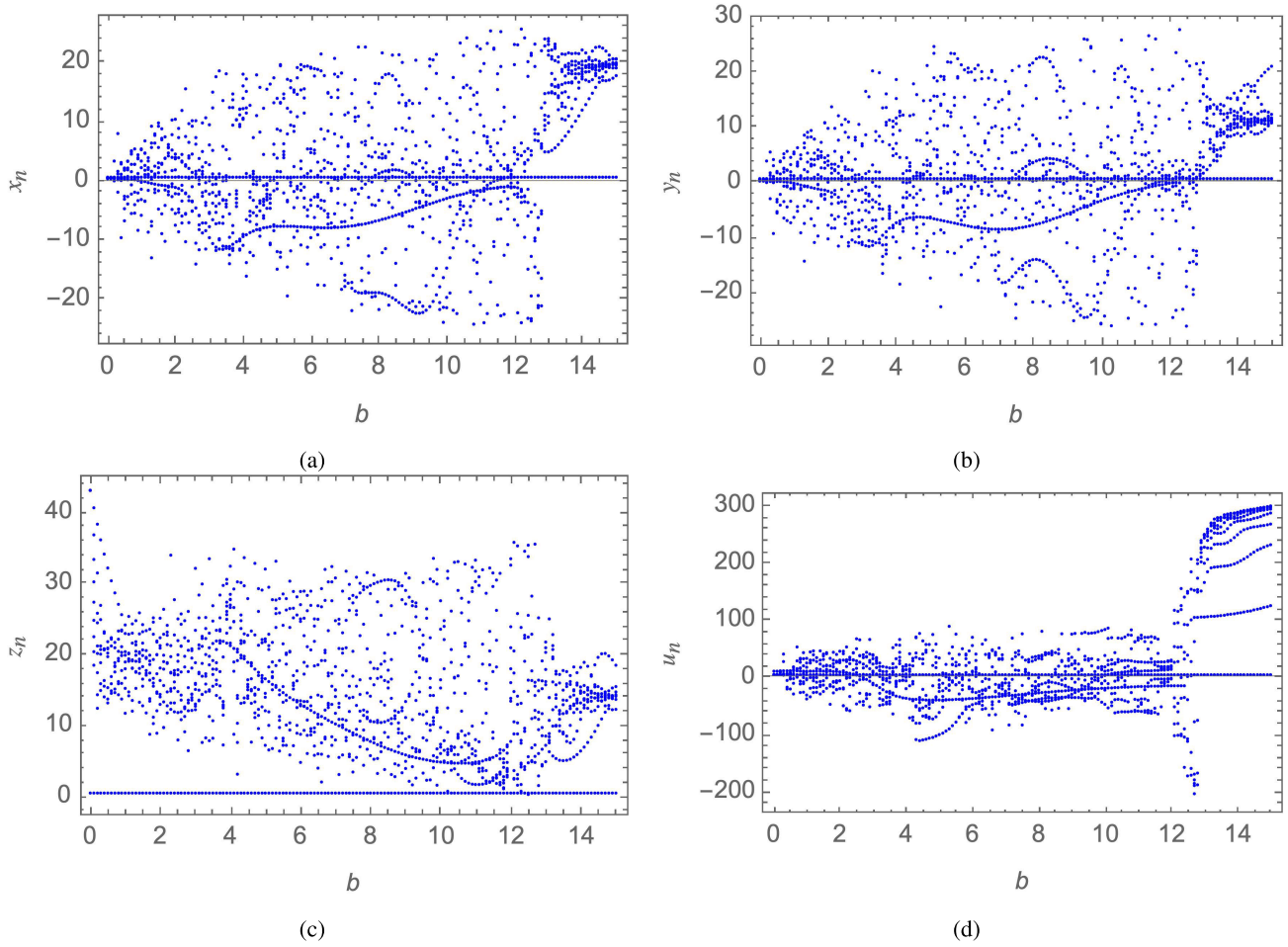


FIGURE 2. Bifurcation diagrams of the fractional-order 4D Chen hyper-chaotic system in (1) with changing b values over the different axes (a) x; (b) y; (c) z; (d) u.

direction selection factor (0 for left and 1 for right). Moreover, for a certain base of rotation, rot, a PRNG sequence of values $rotKey \in [1, rot - 1]$ is demanded as well. Given a flattened system's solution, such a PRNG sequence can be acquired by:

$$rotKey_{\alpha_1'}^{\alpha_2'}(i) = \left(\frac{rotKey_{\alpha_1}^{\alpha_2}(i) - \alpha_1}{\alpha_2 - \alpha_1} \times (\alpha_2' - \alpha_1') \right) + \alpha_1', \quad (4)$$

such that α_1 and α_2 are the old minimum and maximum values (retrieved from the system's solution), and α_1' and α_2' are the new minimum and maximum values (1 and $rot - 1$ in this case). Accordingly, given an image I, a rotation key $rotKey$, and a bit-stream d, Algorithm 2 demonstrates the encryption process that is used to generate encrypted image I'. Respectively, Algorithm 3 showcases the decryption process.

Algorithm 2 Encryption for Image I Using Rotation Given a Base of Rotation rot, List of Rotation Keys $rotKey$, and Set of Directions d, Generating I'

```
Irot ← TransformBase(I, 8, rot)
for each Irot_i in Irot and d_i in d do
    if d_i = 0 then
        Irot'_i ← Irot_i ≪ rotKey_i
    else
        Irot'_i ← Irot_i ≫ rotKey_i
    end if
end for
I' ← TransformBase(Irot', rot, 8)
```

IV. PROPOSED SCHEME

A. THE ENCRYPTION PROCESS

In the proposed approach, the encryption process is distributed among 2 stages, with 3 subroutines for each stage, resulting in a total of 6 encryption steps. Within each step, the performed process subsumes the involvement of a seed with the output of the step prior. Accordingly, the following steps showcase the sequence followed to produce the encrypted image:

1) Stage 1: Chen.
    a) Rotation:
        i) First, the input color image, I, of dimensions $M \times N$, is converted into a 1D bit-stream to

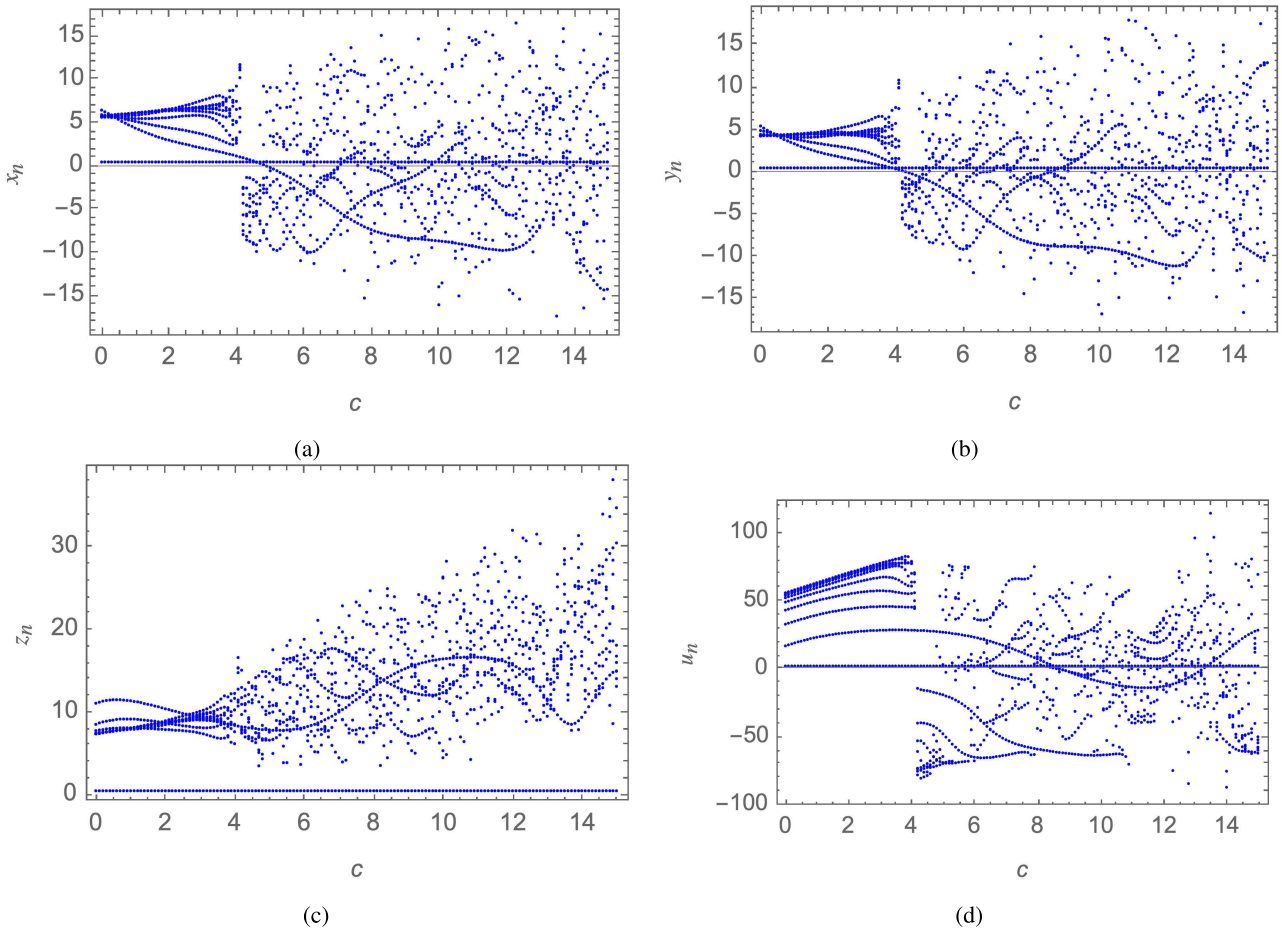


FIGURE 3. Bifurcation diagrams of the fractional-order 4D Chen hyper-chaotic system in (1) with changing c values over the different axes (a) x; (b) y; (c) z; (d) u.

Algorithm 3 Decryption for Image I' Using Rotation Given a Base of Rotation rot, a List of Rotation Keys $rotKey$, and Set of Directions d, Generating I

$Irot' \leftarrow TransformBase(I', 8, rot)$
for each $Irot'_i$ in $Irot'$ and d_i in d **do**
  if $d_i = 0$ **then**
    $Irot_i \leftarrow Irot'_i \ll rotKey_i$
  else
    $Irot_i \leftarrow Irot'_i \gg rotKey_i$
  end if
end for
$I \leftarrow TransformBase(Irot, rot, 8)$

produce I'_1, alongside calculating the length of this bit-stream:

$$BitStreamLength = M \times N \times 24 \quad (5)$$

ii) Given the rotation base $rot1$, I'_1 is divided into subsets of size $rot1$, generating I_{rot1}.
iii) Given a seed for the Chen rotation, a sequence of numbers, $seq_{ChenRot}$, is generated, with a length less than $BitStreamLength/rot1$.
iv) Given a prime rotation seed, Algorithm 1 is used, generating $seq_{ChenRot}$.
v) Each Element in $seq_{ChenRot}$ is scaled to the range of $rot1$ using (4) such that α_1 and α_2 are the old minimum and maximum values retrieved from $seq_{ChenRot}$, and α'_1 and α'_2 are 1 and $rot1 - 1$, generating $Chen_{rot1}$.
vi) Given a seed for the Chen direction selection, a bit-stream $dir_{ChenRot}$ is generated.
vii) Using Algorithm 2, I'_1 is encrypted using $Chen_{rot1}$ and $dir_{ChenRot}$.
viii) The resulting set is then flattened into a 1D bit stream $I'_{1.1}$

b) S-box:

i) The set $I'_{1.1}$ is converted to base 8 by grouping each consecutive 8 bits and transforming them to decimals.
ii) Given a seed for the S-box, a solution of the Chen system of length 256 is computed, then scaled using (4) with $\alpha'_1 = 0$ and $\alpha'_1 = 256$, resulting in a list $S1 \in [0, 255]$, and $|S1| = 256$.

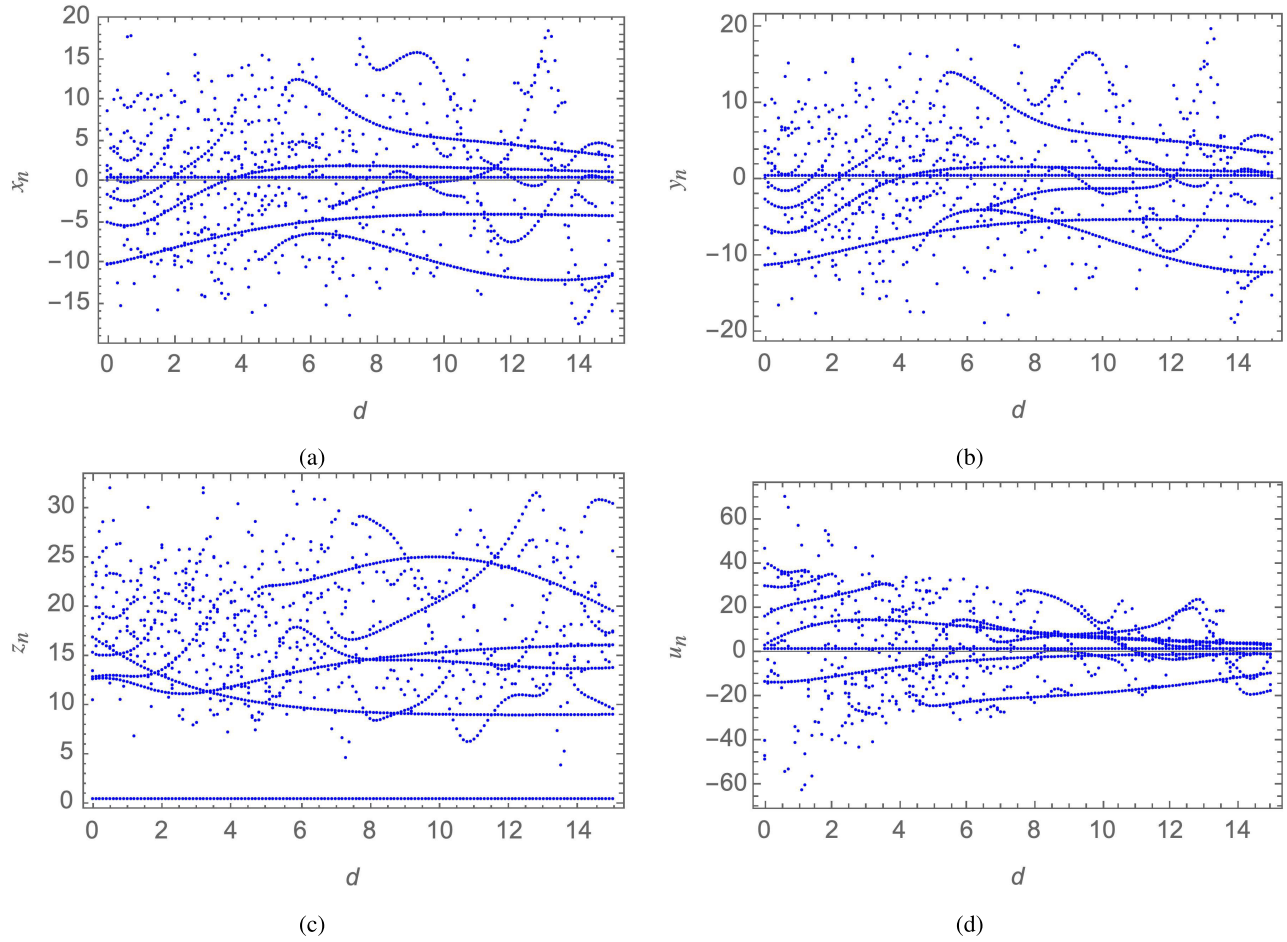


FIGURE 4. Bifurcation diagrams of the fractional-order 4D Chen hyper-chaotic system in (1) with changing d values over the different axes (a) x; (b) y; (c) z; (d) u.

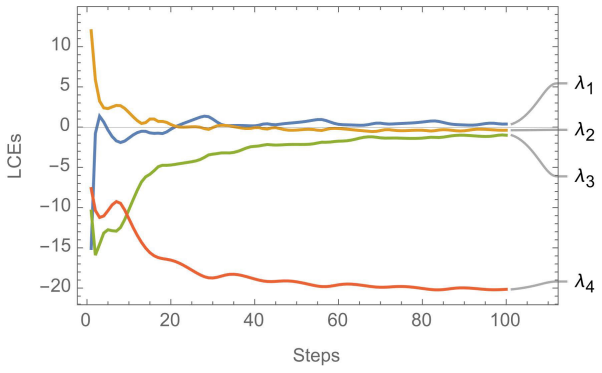


FIGURE 5. Lyapunov characteristic exponent plot of the fractional-order 4D Chen hyper-chaotic system in (1).

iii) List $S1$ is provided as input to Algorithm 4, producing the S-box; following that, the S-box gets evaluated.
iv) For the same S-box seed, the next 256 values in the Chen system's solution are calculated and used in repeating the previous steps until a target set of evaluation values is achieved.
v) After n attempts, if the target set of evaluation values is not achieved, the S-box with the best evaluation values is used.
vi) After deciding on an S-box (as shown in Table 1), it is applied to $I'_{1.1}$ producing $I'_{1.2}$.

c) Bit XOR:
i) The set $I'_{1.2}$ is converted into a 1D bit-stream.
ii) Given a seed for the Chen system's XOR step, the system's solution is calculated, generating a sequence $seq_{ChenXor}$, which is further expanded using Algorithm 1 and a prime seed to be equal in length to the 1D bit-stream of $I'_{1.2}$.
iii) The median μ of $seq_{ChenXor}$ is calculated, then used to convert $seq_{ChenXor}$ into a bit-stream using:

$$seq_{ChenBits}[i] = \begin{cases} 1, & \text{if } seq_{ChenXor}[i] \geq \mu \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

iv) The XOR operator is used on $seq_{ChenBits}$ and $I'_{1.2}$ producing $I'_{1.3}$.

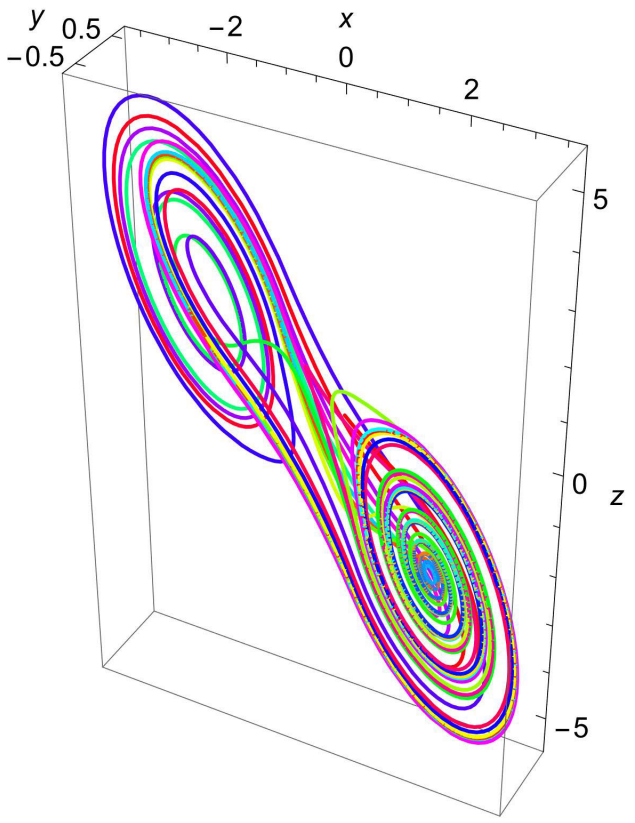


FIGURE 6. The fractional-order 3D system is numerically solved and plotted here for $\{x_0, y_0, z_0, u_0\} = 0.3$, $a = -1.3$, $b = -0.7$, $p = 10$ and $q = 14.87$.

2) Stage 2: Chua.
   a) Rotation:
      i) First, $I'_{1.3}$ is converted into a 1D bit-stream generating I'_2.
      ii) Given the rotation base $rot2$, I'_2 is divided into subsets of size $rot2$, generating I_{rot2}.
      iii) Given a seed for the Chua rotation, a sequence of numbers $seq_{ChuaRot}$ is generated, with a length less than $BitStreamLength/rot2$.
      iv) Given a prime rotation seed, Algorithm 1 is used to generate $seq_{ChuaRot}$.
      v) Each element in $seq_{ChuaRot}$ is scaled to the range of $rot2$ using (4) such that α_1 and α_2 are the old minimum and maximum values retrieved from $seq_{ChuaRot}$, and α'_1 and α'_2 are 1 and $rot2 - 1$, generating $Chua_{rot2}$.
      vi) Given a seed for the Chua direction selection, a bit-stream $dir_{ChuaRot}$ is generated.
      vii) Using Algorithm 2, I'_2 is encrypted using $Chua_{rot2}$ and $dir_{ChuaRot}$.
      viii) The resulting set is then flattened into a 1D bit-stream $I'_{2.1}$
   b) S-box:
      i) The set $I'_{2.1}$ is converted to base 8 by grouping each consecutive 8 bits and transforming them to decimals.

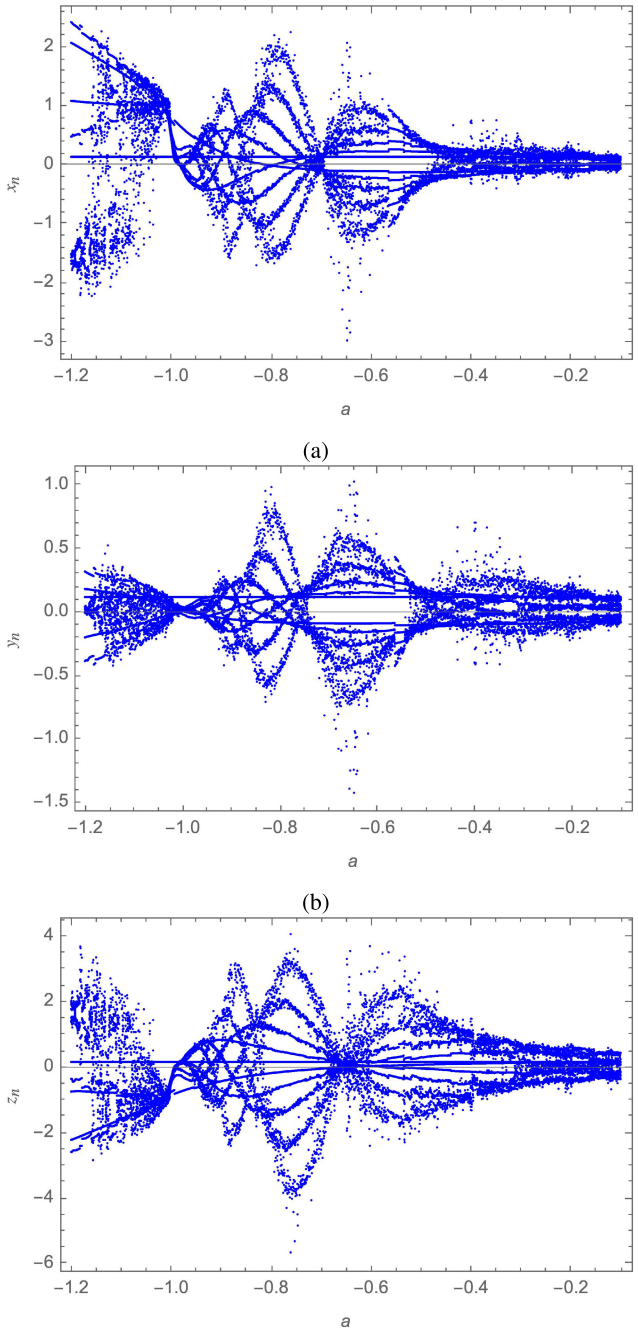


FIGURE 7. Bifurcation diagrams of the fractional-order 3D Chua chaotic system in (2) with changing a values over the different axes (a) x; (b) y; (c) z.

      ii) Given a seed for the S-box, a solution of the Chen system of length 256 is computed, then scaled using (4) with $\alpha'_1 = 0$ and $\alpha'_1 = 256$, resulting in a list $S2 \in [0, 255]$, and $|S2| = 256$.
      iii) List $S2$ is provided as input to Algorithm 4, producing the S-box; following that, the S-box gets evaluated.

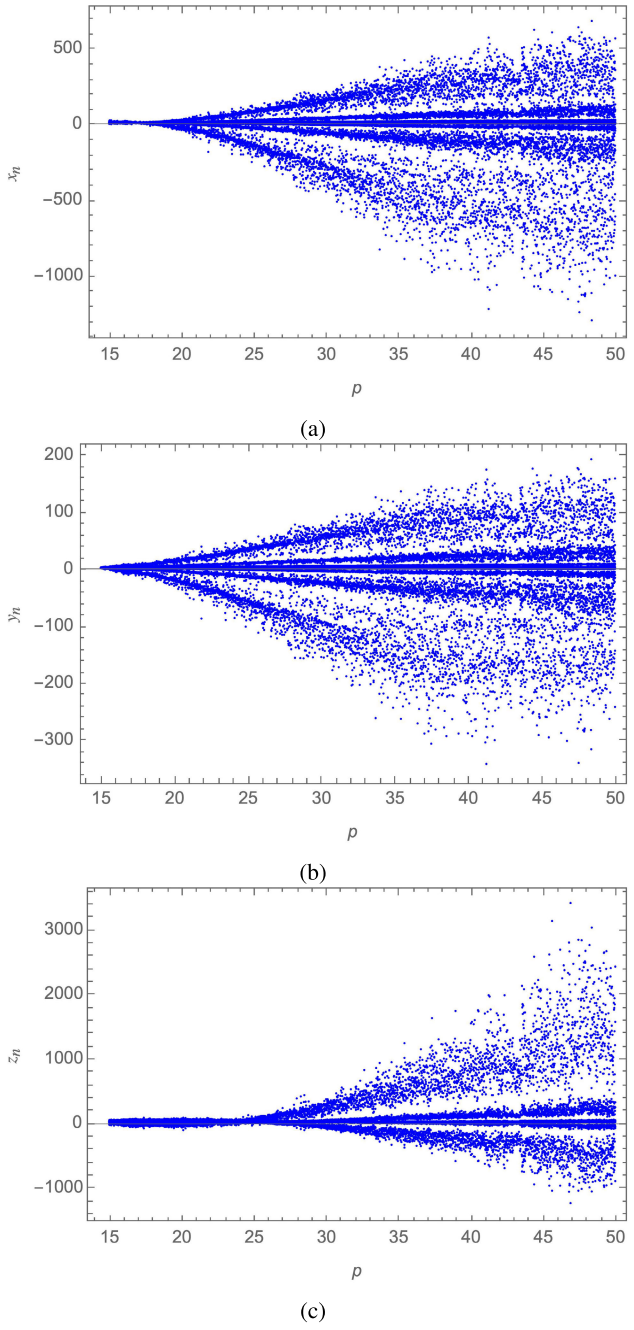


FIGURE 8. Bifurcation diagrams of the fractional-order 3D Chua chaotic system in (2) with changing p values over the different axes (a) x; (b) y; (c) z.

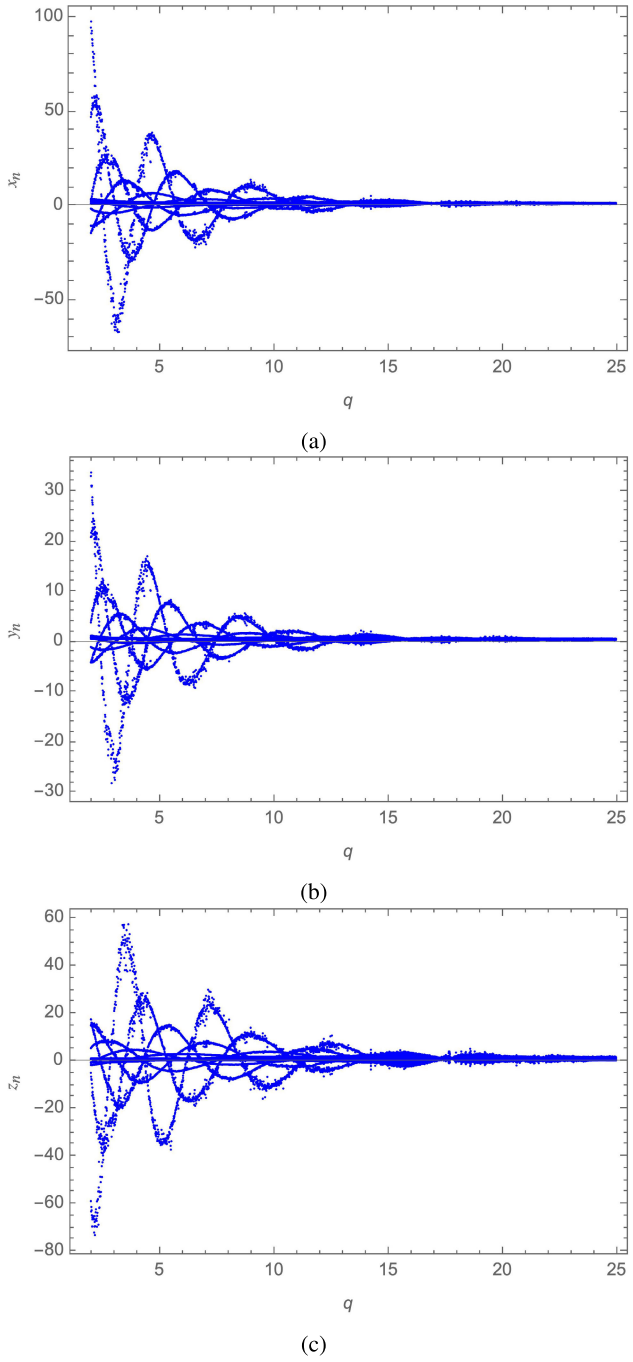


FIGURE 9. Bifurcation diagrams of the fractional-order 3D Chua chaotic system in (2) with changing q values over the different axes (a) x; (b) y; (c) z.

iv) For the same S-box seed, the next 256 values in the Chen system's solution are calculated and used in repeating the previous steps until a target set of evaluation values is achieved.
v) After n attempts, if the target set of evaluation values is not achieved, the S-box with the best evaluation values is used.
vi) After deciding on an S-box (as shown in Table 2), it is applied to $I'_{2.1}$ producing $I'_{2.2}$.

c) Bit XOR:
i) The set $I'_{2.2}$ is converted into a 1D bit-stream.
ii) Given a seed for the Chua system XOR step, the system's solution is calculated, generating a sequence $seq_{ChuaXor}$, which is further expanded using Algorithm 1 and a prime seed to be equal in length to the 1D bit-stream of $I'_{2.2}$.

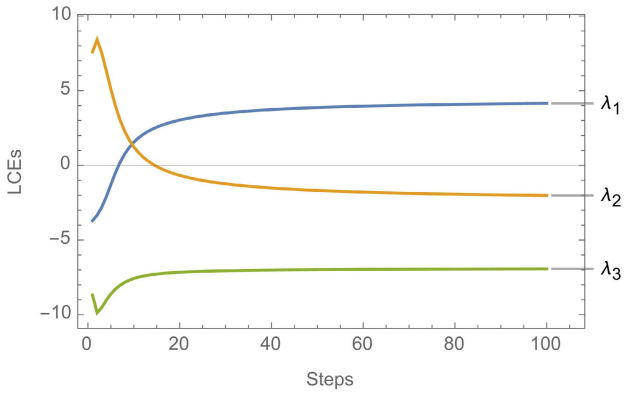


FIGURE 10. Lyapunov characteristic exponents plot of the fractional-order 3D Chua chaotic system in (2).

iii) The median μ of $seq_{ChuaXor}$ is calculated, then used to convert $seq_{ChuaXor}$ into a bit-stream (6).
iv) The XOR operator is used on $seq_{ChuaBits}$ and $I'_{2.2}$ producing $I'_{2.3}$, which is later converted back into an image, forming I'.

Fig. 11 demonstrates a flow chart for the encryption procedure.

B. THE DECRYPTION PROCESS

Starting with I' and the set of keys and S-boxes (generated in the same way as discussed in Subsection IV-A), the decryption procedure is as follows:

1) Stage 2: Chua.
   a) Bit XOR:
      i) The image I' is converted into a 1D bit-stream $I'_{2.3}$.
      ii) The XOR operator is used on $seq_{ChuaBits}$ and $I'_{2.3}$ producing $I'_{2.2}$.
   b) S-box:
      i) The set $I'_{2.2}$ is converted to base 8 by grouping each consecutive 8 bits and transforming them to decimal.
      ii) The inverse of Chua S-box is applied on $I'_{2.2}$ producing $I'_{2.1}$.
   c) Rotation:
      i) Given rotation base $rot2$, $I'_{2.2}$ is divided into subsets of size $rot2$, generating I_{rot2}.
      ii) For each set in I_{rot2}, given the rotation direction selection set $dir_{ChuaRot}$, and $Chua_{rot2}$, Algorithm 3 is used.
      iii) The resulting set is then flattened into a 1D bit-stream $I'_{1.3}$
2) Stage 1: Chen.
   a) Bit XOR:
      i) The set $I'_{1.3}$ is converted into a 1D bit-stream.
      ii) The XOR operator is used on $seq_{ChenBits}$ and $I'_{1.3}$ producing $I'_{1.2}$.
   b) S-box:
      i) The set $I'_{1.2}$ is converted to base 8 by grouping each consecutive 8 bits and transforming them to decimal.
      ii) The inverse of Chen S-box is applied on $I'_{1.2}$ producing $I'_{1.1}$.
   c) Rotation:
      i) Given rotation base $rot1$, $I'_{1.1}$ is divided into subsets of size $rot1$, generating I_{rot1}.
      ii) For each set in I_{rot1} given the rotation direction selection set $dir_{ChenRot}$, and $Chen_{rot1}$, Algorithm 3 is used.
      iii) The resulting set is then converted back into an image, re-producing the input image I.

Fig. 12 demonstrates a flow chart for the decryption procedure.

Algorithm 4 Generate an S-Box Given a Scaled System's Solution Sol, the Number of S-Box Trials n, and Target Performance Metrics $M_{Evls} = \{NL, SAC, BIC, LAP, DAP\}$ (an Adaptation From That Proposed in [18])

$Seq \leftarrow Partition(Sol, 256)$
$SB \leftarrow []$
$M \leftarrow M_{Evls}$
for each $Seq_i \in Seq$ (total of n) **do**
  $Sorted \leftarrow [0 - 255]$
  $SB_i \leftarrow []$
  for each $s_j \in Seq_i$ **do**
    $Loc_j \leftarrow Mod(s_j, Length(Sorted))$
    $Append(Sorted[Loc_j], SB_i)$
    $Delete(Sorted[Loc_j], Sorted)$
  end for
  $M_i \leftarrow \{NL_i, SAC_i, BIC_i, LAP_i, DAP_i\}$
  if $|M_i - M_{Evls}| < M$ **then**
    $M \leftarrow |M_i - M_{Evls}|$
    $SB \leftarrow SB_i$
  end if
end for
return SB

V. PERFORMANCE ANALYSIS

To ensure the security and efficiency of the proposed encryption scheme, a series of statistical and mathematical tests are applied to images passed through the proposed R^3 encryption algorithm. These tests output metrics that are commonly utilized and cited in image encryption research. Each test is discussed and described before the results relevant to the proposed R^3 encryption algorithm are displayed and commented on. Those results are also compared to the results from similar research in order to gain an understanding of just how effective the algorithm is when compared to its counterparts.

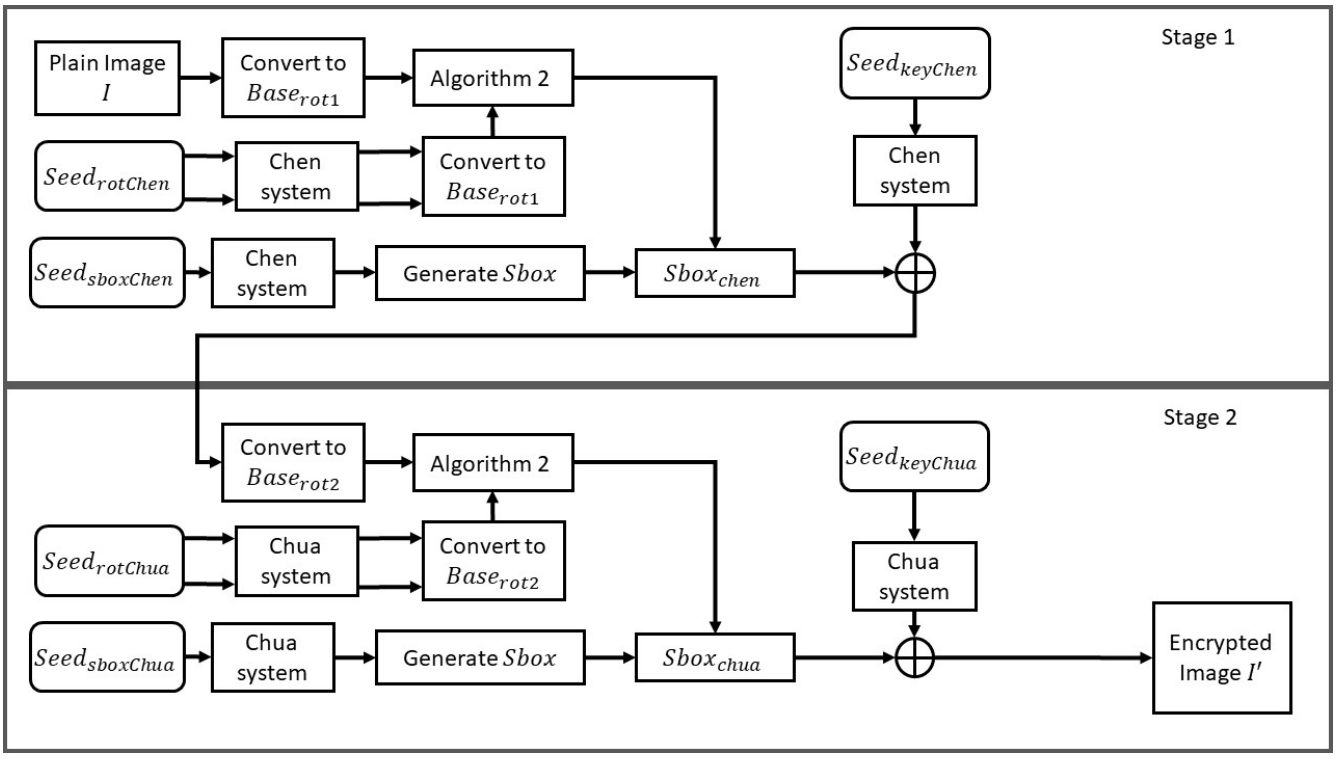


FIGURE 11. Flow chart of the encryption algorithm of the proposed image cryptosystem.

TABLE 1. Proposed Chen-based S-box.

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

A. EXPERIMENTAL ENVIRONMENT

All the images tested in this section are from the University of Southern California's Signal and Image Processing Institute (USC-SIPI)'s miscellaneous image database. These images are commonly cited in research and make comparisons straightforward. All the taken images are compared at a size of 256 × 256, unless mentioned otherwise. To maintain consistency in comparing across the different metrics, the following 5 studies are used as sources of comparison for the proposed scheme in this section: [18], [22], [25], [31], and [23]. However, it should be noted that not all researchers report the same metrics. For this reason, some of the evaluation tables may have empty cells without values, and in the case of subsections like V-B15, where little to no comparison is available, other research is used for comparison.

The machine employed for testing is characterized by the following specifications: An AMD® Ryzen™ 5600H Mobile CPU with a maximum frequency of 3.3 GHz and 16 GB of RAM. The software of choice is Wolfram Mathematica® v.13.1. This allowed for the parallelization of code wherever possible.

B. RESULTS AND DISCUSSION

1) VISUAL AND HISTOGRAM ANALYSES

The first measure taken to ensure the security of an encryption system is a basic visual analysis of its performance. Figures 13 – 15 all show the plain, encrypted and decrypted

TABLE 2. Proposed Chua-based S-box.

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

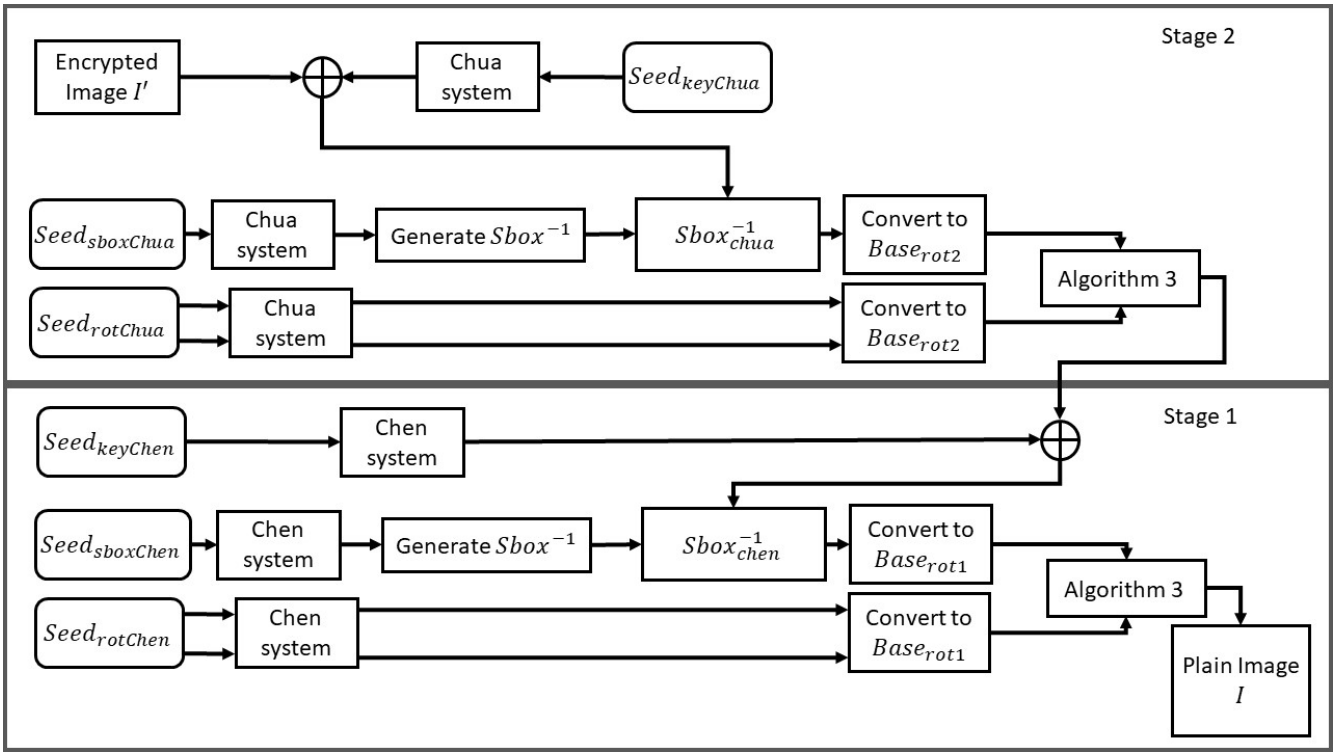


FIGURE 12. Flow chart of the decryption algorithm of the proposed image cryptosystem.

versions of the Lena, F16, and House images, respectively. A basic visual comparison of each image with its encryption reveals no visual symmetry or correlation. No features from the original images, be they colors, edges, or structures, appear in the encrypted images, at least not in a way that is visible to the human eye. This indicates that, at the very least, the contents of the original image are scrambled and altered enough by the encryption scheme that an accidental interceptor of the image data would be unable to access it without employing additional methods of decryption. On the contrary, a visual comparison between the encrypted and decrypted images reveals no differences, indicating the ability of the proposed algorithm to carry out lossless image decryption.

Figures 13 – 15 also contain the color histograms of the presented images, their encryptions and decryptions. While the original images' color histograms display the unique color "fingerprint" of the original image, the encrypted images fail to communicate any such information. An image's color distribution is another piece of information about that image. The proposed encryption scheme completely normalizes any unique peaks and troughs in the color histograms of the input images, forming histograms that are completely uniform and homogenized. This is useful because certain statistical

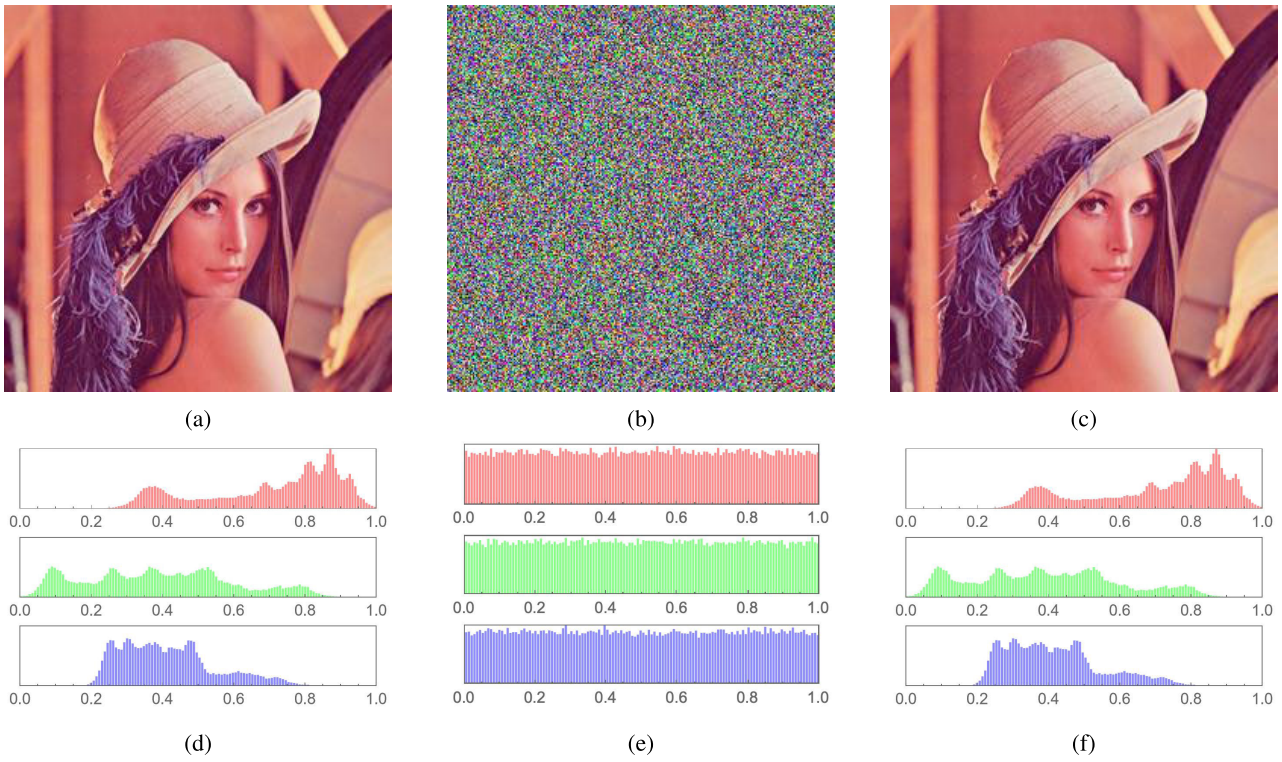


FIGURE 13. Plain, encrypted and decrypted versions of the Lena image and their respective histogram plots (a) Plain Lena image; (b) Encrypted Lena image; (c) Decrypted Lena image; (d) Histogram of plain Lena image; (e) Histogram of encrypted Lena image; (f) Histogram of decrypted Lena image.

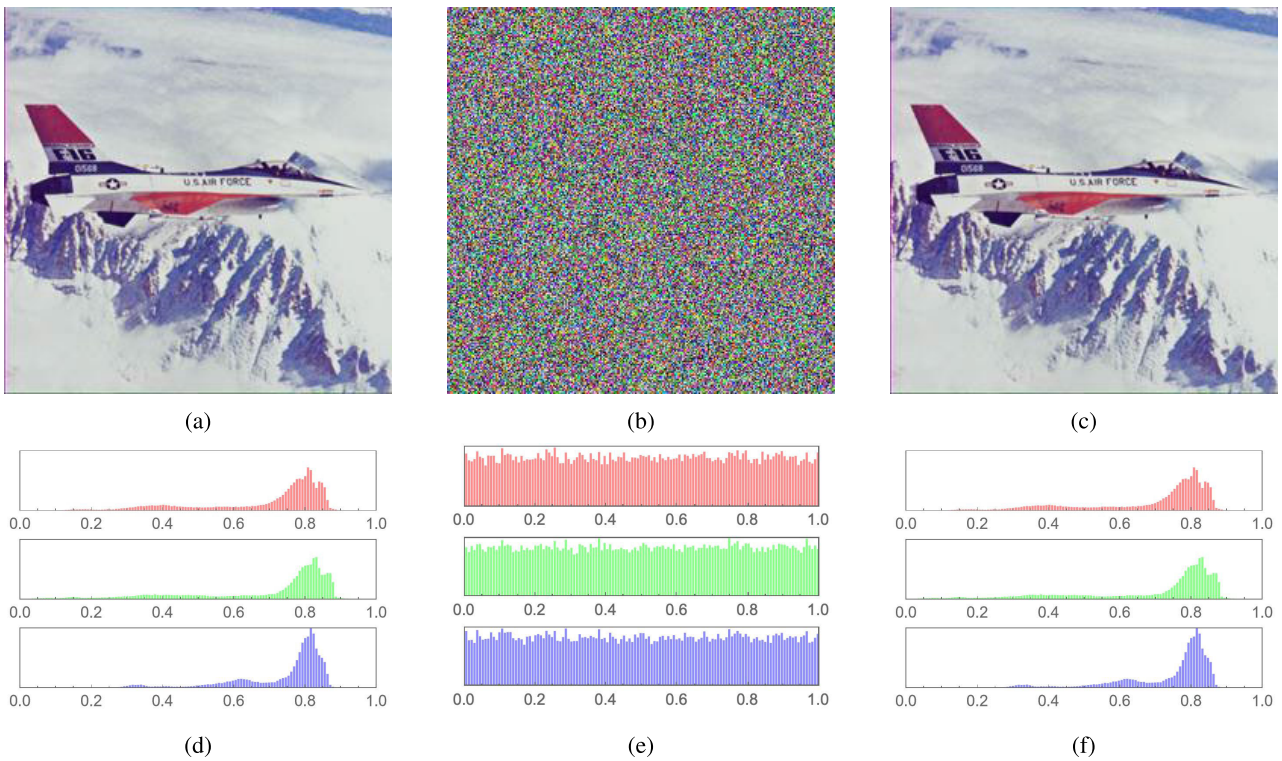


FIGURE 14. Plain, encrypted and decrypted versions of the F16 image and their respective histogram plots (a) Plain F16 image; (b) Encrypted F16 image; (c) Decrypted F16 image; (d) Histogram of plain F16 image; (e) Histogram of encrypted F16 image; (f) Histogram of decrypted F16 image.

cryptanalysis techniques may take advantage of the unique features of a color distribution, if not homogenized by the encryption, to glean information about the source image. All such properties have been eradicated by the proposed scheme.

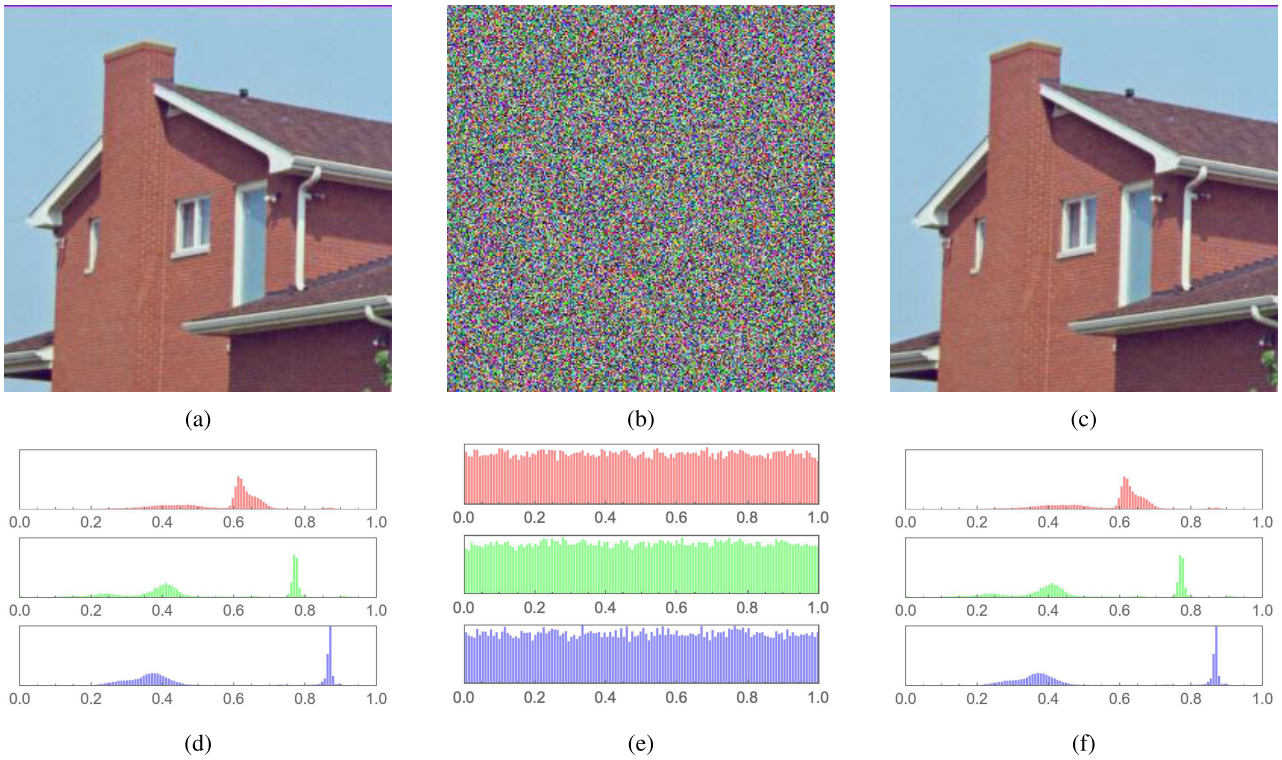


FIGURE 15. Plain, encrypted and decrypted versions of the House image and their respective histogram plots (a) Plain House image; (b) Encrypted House image; (c) Decrypted House image; (d) Histogram of plain House image; (e) Histogram of encrypted House image; (f) Histogram of decrypted House image.

On the contrary, a comparison of the histogram plots of the plain and decrypted images reveals no differences, indicating excellent lossless decryption.

2) CHI SQUARE TEST

The Chi-Square (χ^2) test is a statistical test that is used to determine if the observed frequencies of a categorical variable match the expected frequencies. In the context of analyzing the pixel distribution in an encrypted image, the χ^2 value can be computed using the following formula:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i}, \tag{7}$$

where O_i and E_i represent the observed and expected frequencies of the i^{th} pixel value, respectively.

For an ideal encrypted image with a uniform distribution, each pixel value from 0 to 255 (for an 8-bit grayscale image) should occur with equal probability. Therefore, the expected frequency E_i for each pixel value is $N/256$, where N is the total number of pixels in the image. The χ^2 value is then computed by summing up the squared differences between the observed and expected frequencies, each divided by the expected frequency, over all pixel values.

A χ^2 value close to 256 for an 8-bit grayscale image suggests that the pixel values in the encrypted image are uniformly and randomly distributed, indicating a high degree of security offered by the encryption algorithm. Table 3 displays the computed χ^2 values for the RGB color channels of a number of encrypted images. It is clear from the table that the computed values are close enough to the ideal value of 256.

TABLE 3. χ^2 values of various encrypted images.

Image	R	G	B	Average
Lena	279.1484	238.9141	258.5859	258.8828
Peppers	313.0078	292.1797	297.7422	300.9766
Mandrill	287.5859	301.1953	336.1406	308.3073
Girl	401.5156	345.4609	411.7500	386.2422
Sailboat	307.6875	299.0547	259.6250	288.7891
Average	317.789	252.361	312.769	308.653

3) MEAN SQUARED ERROR

A simple visual analysis of the differences between an image and its encryption is not quite enough to determine the efficacy of an encryption scheme. To ensure that the differences that exist are great enough to show strong encryption, additional mathematical metrics are computed. One such metric, often utilized in image encryption literature, is the mean squared error (MSE), which is typically expressed as follows:

$$MSE = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P_{(i,j)} - E_{(i,j)})^2}{M \times N}. \tag{8}$$

In the equation, $P_{(i,j)}$ and $E_{(i,j)}$ represent pixels located in the plain and encrypted images, respectively, at the locations denoted by (i, j). The images are both of the same dimensions $M \times N$. The MSE calculates the mean squared difference between respective pixels in both images, giving an idea of just how different the encrypted image is from its source. Ideally, this value would be as high as possible, showing a minimal relationship between the source image and its encryption. Table 4 shows the results computed for encryptions produced by the proposed scheme as well as those in comparable literature. Although the compared literature does not represent much in terms of MSE, the values presented by [25] are definitely comparable to the equivalent encryption presented by the proposed scheme.

4) PEAK SIGNAL-TO-NOISE RATIO

Another metric used to measure image differences is the peak signal-to-noise ratio (PSNR). It measures the ratio between the MSE and the maximum intensity of a pixel (I_{max}) in that image. The PSNR is generally expressed as:

$$PSNR = 10 \log \left(\frac{I_{max}^2}{MSE} \right). \tag{9}$$

Typically, I_{max} is taken as 255, which is the maximum value a grayscale pixel can take in the encrypted image. Because of the use of the MSE in inverse form in the equation, lower PSNR values are considered ideal for image encryption. Table 5 shows the PSNR values calculated for encryptions produced by the proposed algorithm, as well as some of those produced by similar schemes in modern research. The table clearly shows that the proposed scheme, although somewhat inferior, generally performs comparably, in terms of PSNR, to the compared literature's encryptions. A complete comparison of PSNR is hard to make given the limited number of images tested in the adjacent literature.

5) INFORMATION ENTROPY

Evaluating the difference between the encrypted image and its source input is useful, but metrics that analyze the encrypted image directly can also assess the effectiveness of the encryption scheme. One such measurement is an analysis of the Shannon Information Entropy of the encrypted image's three separate color channels. Typically a measurement of the amount of randomness in a dataset, the Information Entropy of a grayscale image is typically calculated as follows:

$$H(m) = \sum_{i=1}^{M} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{10}$$

where $p(m_i)$ represents the probability of occurrence of each symbol m in the total number of M symbols in an image. In essence, the entropy of an image gives an idea of just how random its contents are by giving an idea of how many bits are needed on average to encode the data in each pixel. A completely uniform image would require no bits, while a completely, truly random image would require exactly 8 bits, the maximum value [35]. This is generally impossible, but strong encryption schemes will approach this value, as can be seen in Table 6. The proposed encryption scheme performs very well, generally exceeding the entropy values shown by other encryption schemes in the literature, which indicates that the images produced by the proposed encryption scheme show high properties of randomness.

6) CORRELATION COEFFICIENT ANALYSIS

Another metric used to analyze the contents of an encrypted image alone is the correlation coefficient r. By analyzing the correlations between adjacent pixels in an image, it becomes possible to determine whether any natural structures–like edges, boundaries, and color gradients–from the original image are preserved in the image. In this research, correlations between adjacent pixels are calculated for the three directions: horizontal (H), vertical (V), and diagonal (D). The equations (11)–(14) show the process of calculating the coefficient r. First, (14) calculates the mean distribution, $E(x)$, of the pixels in each image. Equation (13) then calculates the dispersion, $D(x)$, in each image, which is followed by (12) calculating the linear direction similarity in the chosen direction for each of the images' distributions, $cov(x, y)$. These values are then used by (11) to calculate the correlation coefficient, r_{xy}. Since the correlation coefficient represents the strength of the relationships between adjacent pixels, the ideal value in an encrypted image is 0 for all directions, indicating no correlation whatsoever. Values close to ± 1 are expected from source images, which indicate the maximum possible correlation between adjacent pixels.

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{11}$$

where

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{12}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2, \tag{13}$$

and

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i). \tag{14}$$

Here, the variables x and y represent 2 images, and N is the length of the bit-stream representing their pixels. That bit-stream's length is calculated by multiplying the number of pixels in the image by the number of bytes per pixel. For our tested RGB images, that would output a stream of length $256 \times 256 \times 3 \times 8 = 1572864$.

Tables 7 and 8 show the correlation coefficient values for a number of plain and encrypted images. The tables clearly show that while the plain images have relatively high values of r (as shown in 7), with most values approaching the maximum values of ± 1, the respective encrypted values of

TABLE 4. MSE values comparison of different images.

	Proposed	[25] (Sc. 3)	[18]	[22]	[23]	[31]
Lena	8887.52	8868.4	8912.4	N/A	N/A	N/A
Peppers	10013.3	N/A	10,065.4	N/A	N/A	N/A
Mandrill	8337.54	N/A	8320.41	N/A	N/A	N/A
Girl	12120.9	N/A	12,104.2	N/A	N/A	N/A
Sailboat	10012.6	N/A	10,071.9	N/A	N/A	N/A
Average	9874.49	8868.4	9894.862	N/A	N/A	N/A

TABLE 5. PSNR values comparison of different images.

	Proposed	[25] (Sc. 3)	[18]	[22]	[23]	[31] RGB		
Lena	8.643	8.7117	8.63086	N/A	N/A	7.8882	8.6081	9.6660
Peppers	8.12503	N/A	8.10248	N/A	N/A	N/A	N/A	N/A
Mandrill	8.92043	N/A	8.92936	N/A	N/A	8.9588	9.4883	8.5673
Girl	7.29545	N/A	7.30144	N/A	N/A	N/A	N/A	N/A
Sailboat	8.12533	N/A	8.0997	N/A	N/A	N/A	N/A	N/A
Average	8.221848	8.7117	8.212768	N/A	N/A	8.4235	9.0482	9.11665

TABLE 6. Comparison of the entropy values of the combined Lena image of the proposed cryptosystem and various algorithms from the literature.

Algorithm	Entropy value
Proposed	7.99901
[25] (Sc. 3)	7.9972
[18]	7.99887
[22]	7.999357
[23]	7.9967
[31]	7.9976

TABLE 7. 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
Girl	0.974013	0.974013	0.965671
Sailboat	0.950138	0.919872	0.950138

TABLE 8. Correlation coefficients of adjacent pixels in encrypted images. Shown here in 3 directions: horizontal, diagonal and vertical.

Enc. image	H	D	V
Lena	0.00591782	0.00107969	0.000194493
Peppers	0.00430376	−0.00544425	−0.00181753
Mandrill	0.00509484	0.00356122	−0.00101199
Girl	0.00459616	−0.000727385	0.00497798
Sailboat	−0.00152584	−0.000564933	−0.00071081

r are all close to the ideal value of 0. This indicates little to no correlation between adjacent pixels in all directions in the encrypted images. Figure 16 shows those values visually for the plain Lena image and its encrypted counterparts. Figures 16a, 16b, and 16c show strong central streaks, indicating high levels of correlation among adjacent pixels in all three directions of the plain image, while 16d, 16e, and 16f all show a uniform distribution of points. Such a scrambled distribution of values indicates a lack of correlation. Similar plots can be seen for the red, green, and blue channels of the plain and encrypted Lena images, shown respectively in Figs. 17, 18, and 19.

TABLE 9. Correlation coefficient comparison between plain and encrypted Lena images.

Direction	Horizontal	Diagonal	Vertical
Plain	0.938611	0.913175	0.96833
Proposed	0.00591782	0.00107969	0.000194493
[25] (Sc. 3)	0.0007832	−0.0028532	−0.0018442
[18]	0.0064113	0.0015143	0.000568333
[22]	−0.003761	0.000686	0.001775
[23]	0.0005	0.0032	0.0014
[31]	−0.0107	0.00067	−0.027067

Table 9 shows the calculated correlation coefficient values when compared to some of the values produced by algorithms in similar research. The table shows comparable performance in terms of correlation coefficients for the proposed algorithm.

7) FOURIER TRANSFORMATION ANALYSIS

Another technique useful for measuring the destruction of artifacts from the input image in the encryption is the analysis of the Fourier transform of the image contents. By comparing the Discrete Fourier Transform (DFT) of a plain image and its encryption, the presence of common frequencies can be determined and compared between the image and its encryption. The DFT of an image $f(i, j)$ with size $N \times N$ in the frequency domain is calculated as follows:

$$F(k, l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) e^{-i2\pi(\frac{ki}{N} + \frac{li}{N})}, \tag{15}$$

where $f(a, b)$ is the image representation in the spatial domain, such that the exponential term is the basis function that matches every point $F(k, l)$ in the Fourier space. From this calculation, it is seen that $F(0, 0)$ is the component of the image that translates into average brightness, and $F(N - 1, N - 1)$ translates into the highest frequency.

Figure 20 shows the effect of applying the DFT to the plain and encrypted versions of the Mandrill image. It is clear from Fig. 20a that the plain image contains large bands of

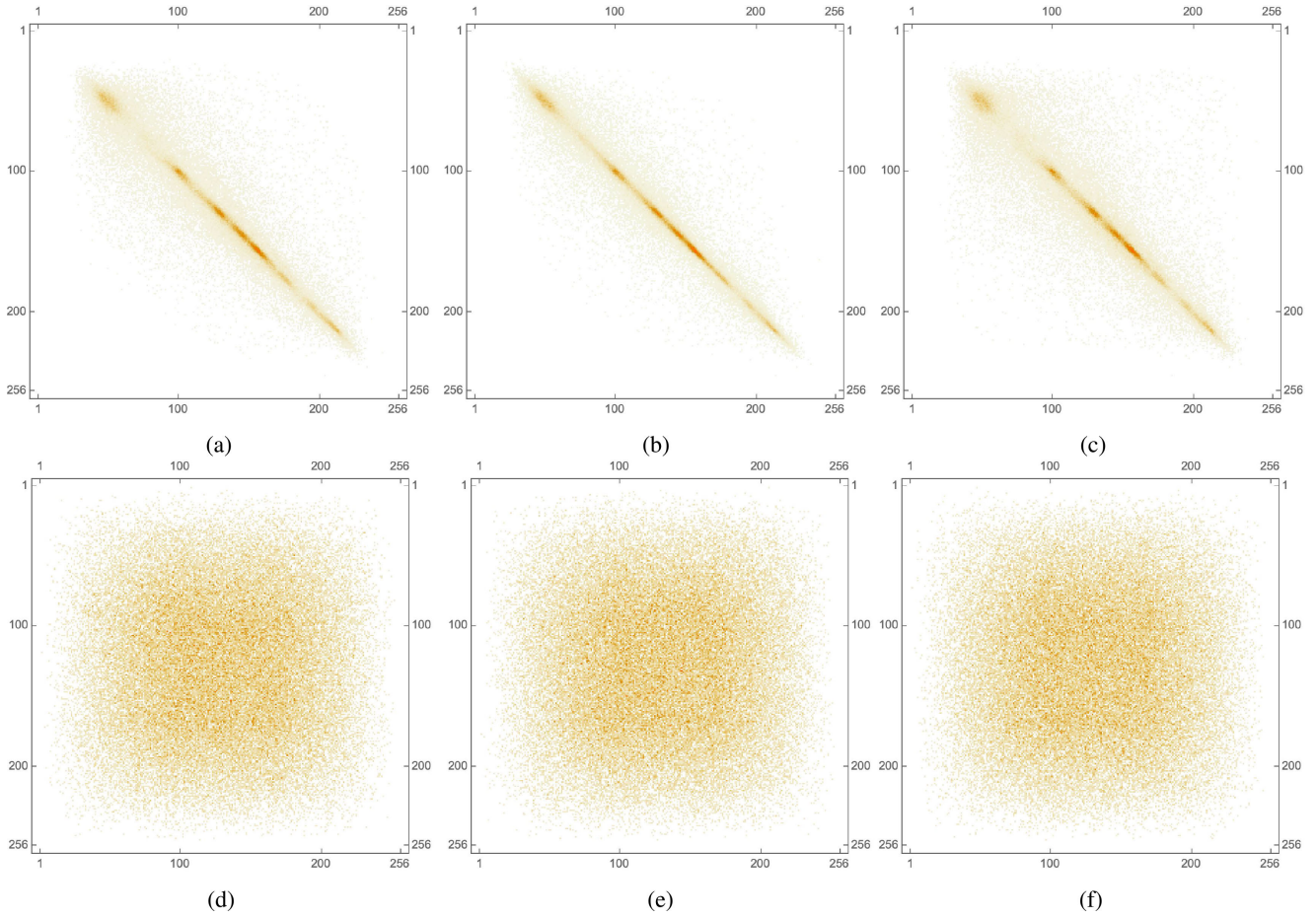


FIGURE 16. Correlation coefficient diagrams of the plain and encrypted Lena images (a) Horizontal, plain; (b) Vertical, plain; (c) Diagonal, plain; (d) Horizontal, encrypted; (e) Vertical, encrypted; (f) Diagonal, encrypted.

frequencies with the same brightness, a property typical of real images. This manifests as a large cross-like object in the center of the DFT. Applying the DFT to the encryption of the Mandrill image, however, reveals a completely uniform field where all such frequencies are distributed evenly. This indicates that, where the original image had special features like edges, vertices, and fields of uniform coloring, the encryption of the image lacks those features, which is a desirable outcome for any strong encryption system.

8) HISTOGRAM DEPENDENCY TESTS

Although Section V-B1 briefly displayed and examined the color histograms of the plain images and their encrypted counterparts, a more thorough analysis of those graphs is warranted to ensure a complete lack of dependency between them. To ensure that this is the case, a number of linear dependency tests are carried out on those color histograms, namely Blomqvist β, Goodman-Kruskal γ, Kendall τ, Spearman ρ, and Pearson correlation r. These tests all measure the linear dependency between 2 histograms, producing a value that ranges from 1, indicating a strong positive correlation, to -1, which indicates a strong negative correlation. The ideal value is 0, which indicates no relation. The 5 tests are defined as follows:

- The Blomqvist metric assesses the correlation between 2 histogram distributions (X and Y) as a medial correlation coefficient (for medians $\overline{x}$ and $\overline{y}$). Blomqvist correlation is equated as follows:

$$\beta = \{(X - \overline{x})(Y - \overline{y}) > 0\} - \{(X - \overline{x})(Y - \overline{y}) < 0\}, \tag{16}$$

  where X and Y are the two distributions, with their medians $\overline{x}$ and $\overline{y}$, respectively.
- The Goodman-Kruskal measure works cumulatively, identifying whether subsequent elements in both histograms either promote or regress the linear correlation between the 2 histograms. This is done by comparing pairs of values from the 2 histograms. The Goodman-Kruskal correlation is defined as:

$$\gamma = \frac{n_c - n_d}{n_c + n_d}, \tag{17}$$

  where n_c is the number of pairs of cases ranked in the same order on both variables, while n_d is the number of pairs of cases ranked in reversed order on both variables.

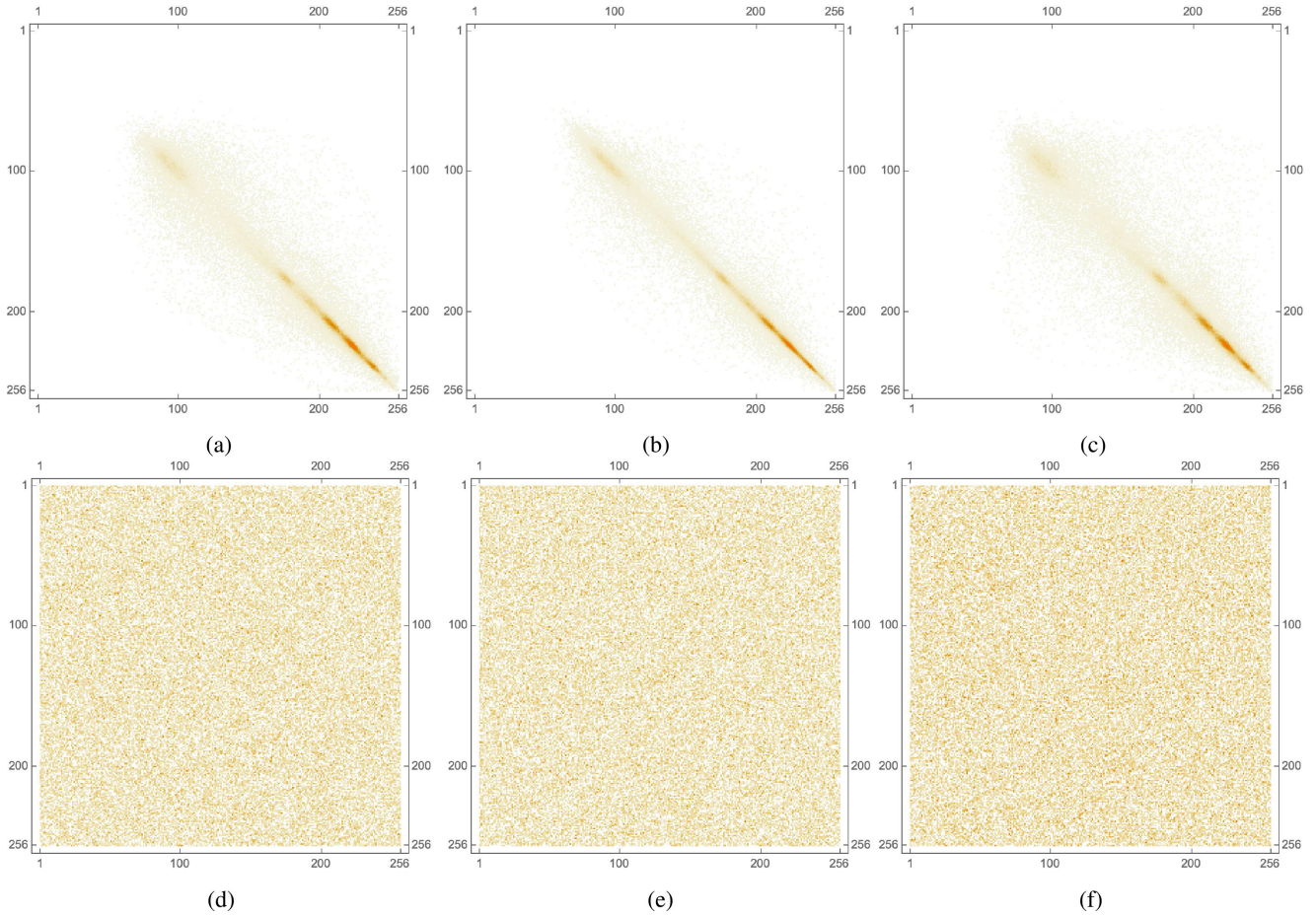


FIGURE 17. Correlation coefficient diagrams of the red channels of the plain and encrypted Lena images (a) Horizontal, plain; (b) Vertical, plain; (c) Diagonal, plain; (d) Horizontal, encrypted; (e) Vertical, encrypted; (f) Diagonal, encrypted.

- Kendall's τ evaluates correlation in relation to sample size by using a similar concept reliant on concordant and discordant pairs. The correlation is defined as:

$$\tau = \frac{n_c - n_d}{\frac{n(n-1)}{2}}. \tag{18}$$

- 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:

$$\rho = \frac{\sum(R_{ix} - \overline{R}_x)(R_{iy} - \overline{R}_y)}{\sqrt{\sum(R_{ix} - \overline{R}_x)^2 \sum(R_{iy} - \overline{R}_y)^2}}, \tag{19}$$

  where x and y are the two distributions, R_{il} is the rank of element i in list l, and $\overline{R}_l$ is the mean of the ranks of l.
- The Pearson correlation, which is generally the most ubiquitous and straightforward correlation metric, simply connects components of the distributions to their mean averages. The Pearson correlation can be calculated as:

$$r = \frac{\sum(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum(X_i - \overline{X})^2 \sum(Y_i - \overline{Y})^2}}. \tag{20}$$

where $\overline{X}$ and $\overline{Y}$ are the means of the distributions X and Y, respectively.

Table 10 contains the outcomes for applying all 5 of the above tests to various plain and encrypted images' histograms. All of the produced values are very close to 0, indicating a very weak correlation between the color histograms of the plain and encrypted images, as discussed in Subsection V-B1.

9) DIFFERENTIAL ATTACK ANALYSIS

One type of malicious attack that a strong encryption system needs to protect against is the differential attack. Differential attacks rely on comparing encryptions made to slightly modified images to retrieve information about the encryption key using analytical techniques. A strong encryption system would be able to resist attacks by having its encryption system widely alter its encryption with even the smallest of modifications to its input. Two metrics are useful in measuring an encryption system's resistance to differential attacks: the number of pixel changing rate (NPCR) and the unified average change intensity (UACI). The NPCR is calculated as follows:

$$NPCR = \frac{\sum_{i,j} D_{i,j}}{M \times N} \times 100, \tag{21}$$

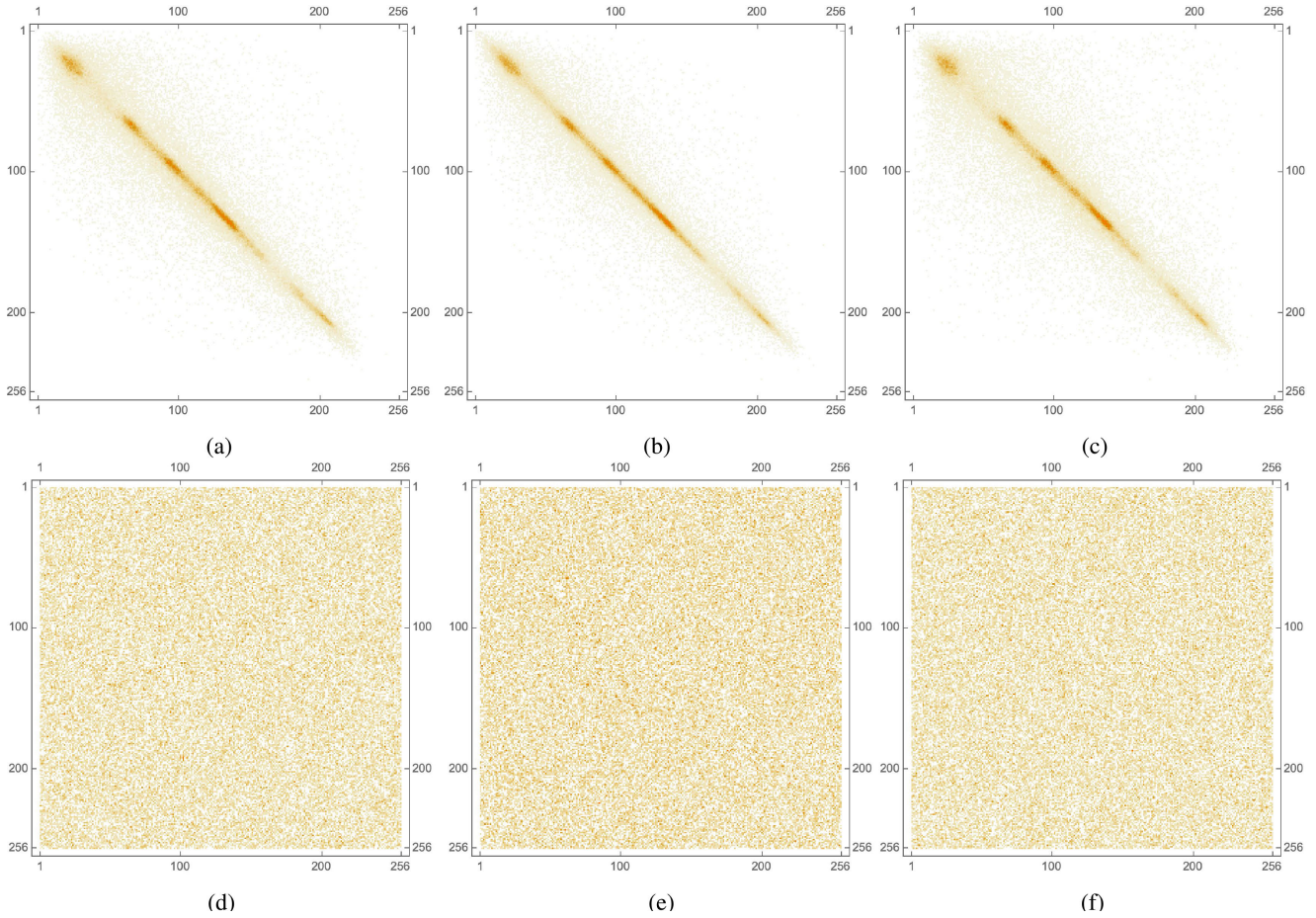


FIGURE 18. Correlation coefficient diagrams of the green channels of the plain and encrypted Lena images (a) Horizontal, plain; (b) Vertical, plain; (c) Diagonal, plain; (d) Horizontal, encrypted; (e) Vertical, encrypted; (f) Diagonal, encrypted.

TABLE 10. Histogram dependency tests for various images.

Image	Color	β (16)	γ (17)	τ (18)	ρ (19)	r (20)
Lena	Red	0.0594233	0.0397646	0.0384909	0.05723168	−0.00872151
	Green	−0.0357936	0.0380455	0.0375543	0.0574823	0.0769809
	Blue	0.0199778	−0.0551999	−0.0519275	−0.0756834	−0.0451689
	Combined	0.023916	0.0196115	0.0195021	0.0296231	0.0365851
Peppers	Red	−0.063496	−0.0129422	−0.0126723	−0.0228809	−0.0208279
	Green	0.00397681	−0.0134277	−0.0132851	−0.0173865	−0.038918
	Blue	0.0278483	−0.00903519	−0.0088976	−0.00743829	−0.0224383
	Combined	−0.011835	0.000557759	0.000554599	−0.0000141284	−0.0276875
Mandrill	Red	0.0512881	−0.000781714	0.000773781	0.00218615	0.00384019
	Green	−0.0673337	−0.0337814	−0.033168	−0.0479362	−0.0416112
	Blue	−0.0591786	−0.0208379	−0.0206664	−0.0319658	−0.0154122
	Combined	−0.0862752	−0.0197242	−0.0196354	−0.0331432	−0.0451568
Girl	Red	0.020404	−0.0834336	−0.0704424	−0.0919205	−0.128357
	Green	−0.0235593	−0.0706575	−0.0585565	−0.0779061	−0.0558211
	Blue	0	−0.0155551	−0.0126184	−0.0169687	−0.0250975
	Combined	0.03125	0.00526545	0.00503263	0.00772016	0.0449592
Sailboat	Red	−0.015625	0.0269194	0.025861	0.0366697	0.043668
	Green	0.123766	0.102216	0.101336	0.15038	0.142923
	Blue	0	0.0200584	0.0198153	0.0323054	0.0135318
	Combined	0.118585	.102804	0.102335	0.150245	0.141763

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

$$D_{i,j} = \begin{cases} 0 & C_{1(i,j)} = C_{2(i,j)}, \\ 1 & C_{1(i,j)} \neq C_{2(i,j)}. \end{cases} \tag{22}$$

The NPCR effectively calculates the proportion of an encrypted image that is different from its input. The UACI is mathematically expressed as:

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255}, \tag{23}$$

where $C_{1(i,j)}$ and $C_{2(i,j)}$ are 2 images of dimensions $M \times N$. The UACI calculates the difference in the average pixel

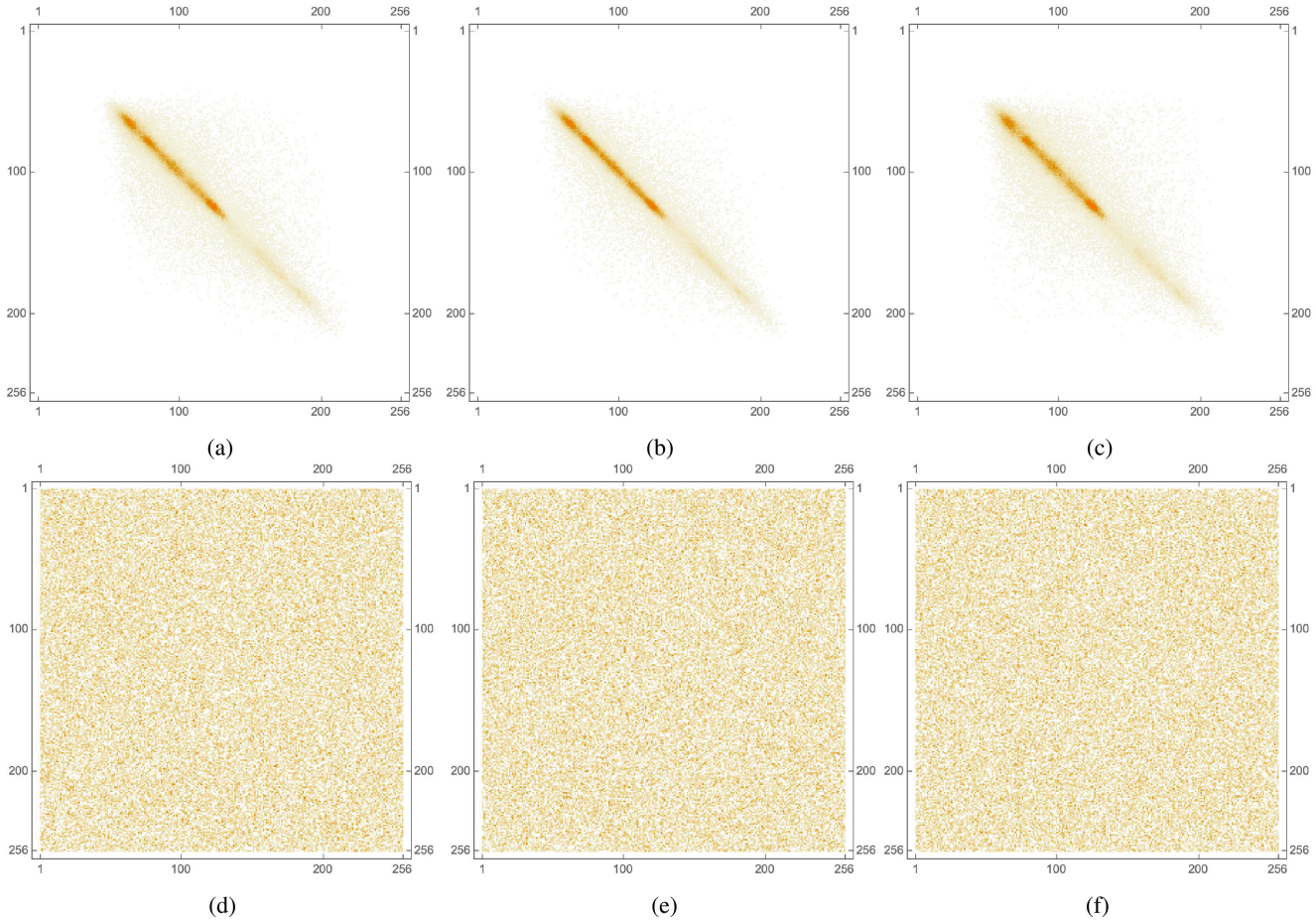


FIGURE 19. Correlation coefficient diagrams of the blue channels of the plain and encrypted Lena images (a) Horizontal, plain; (b) Vertical, plain; (c) Diagonal, plain; (d) Horizontal, encrypted; (e) Vertical, encrypted; (f) Diagonal, encrypted.

TABLE 11. NPCR values of the encrypted Lena image in comparison with other research.

Algorithm	NPCR
Proposed	99.6282
[25] (Sc. 3)	99.6216
[18]	99.5855
[22]	99.6042
[23]	99.6033
[31]	99.6129

TABLE 12. UACI values of the encrypted Lena image in comparison with other research.

Algorithm	UACI
Proposed	30.3379
[25] (Sc. 3)	33.5218
[18]	30.3873
[22]	33.515567
[23]	33.375
[31]	33.5623

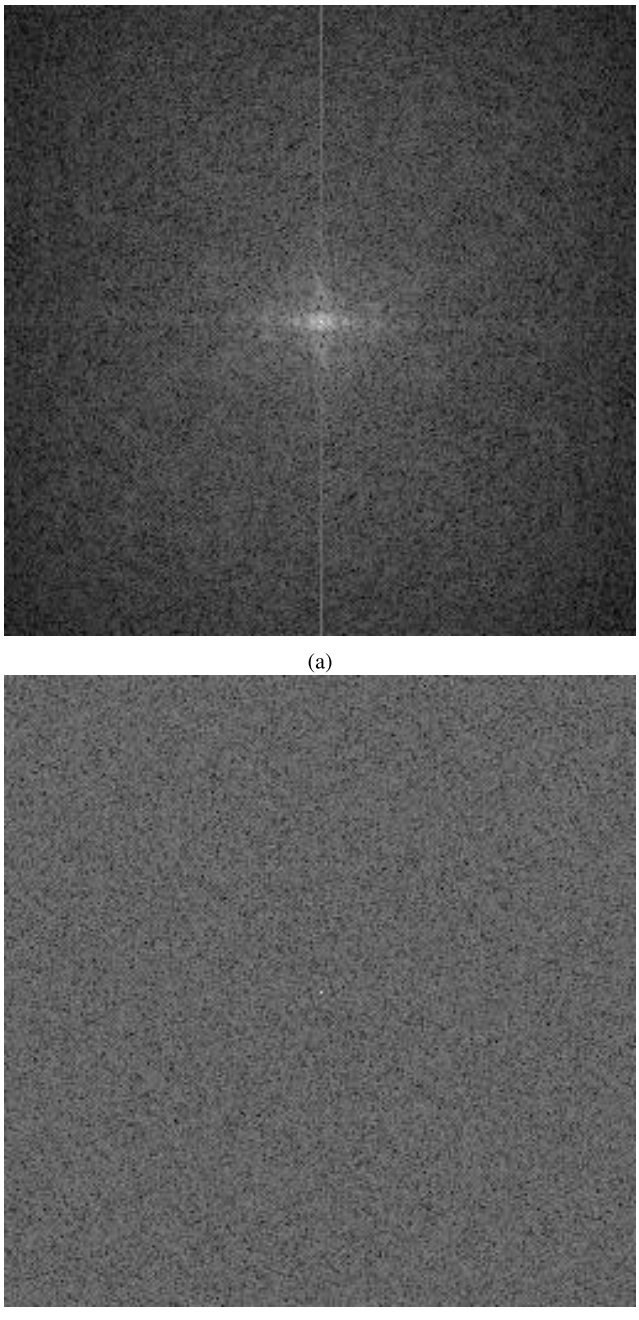
values between the plain image and its encrypted counterpart. Both the NPCR and UACI of the encrypted Lena image are presented in Tables 11 and 12, and compared to the NPCR and UACI values in similar research. While the NPCR values are found to be quite high, all above 99%, the UACI values are somewhat low, never approaching the ideal value of 33.35% as close as some of the compared research has.

10) MEAN ABSOLUTE ERROR

A third test that can be employed to check the effectiveness of an encryption strength against differential attacks is the mean absolute error (MAE). Just like the MSE, the MAE determines the average difference between the respective pixels in an encrypted image when compared to its plaintext counterpart. However, instead of relying on the square of those differences, the MAE uses the absolute value to aggregate the difference values. For a plain image $P_{(i,j)}$ and its encryption $E_{(i,j)}$ for all its pixels that range from i to j, the MAE can be calculated as follows:

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} P_{(i,j)} - E_{(i,j)}. \tag{24}$$

As with the MSE, higher values of MAE indicate greater differences between the input images and their encryptions, making them preferable. Computed MAE values



(a) (b)

FIGURE 20. DFT of the plain and encrypted Mandrill images (a) The plain Mandrill image after DFT; (b) The encrypted Mandrill image after DFT.

are presented in Table 13, alongside values reported from similar algorithms in modern research.

11) KEY SPACE ANALYSIS

The proposed image encryption system requires a total of 98 variables to operate. The Chen and Chua systems are both instantiated 4 times each, with each instantiation of the Chen system needing 13 inputs and each call of the Chua system needing 10. Additionally, 2 input keys are needed as bases for the rotations, and 4 seed values are required for generating the rotation prime base values. This adds up to a total of 98 variables, and with the maximum machine precision for real numbers being 10^{-16}, the effective key space of the proposed algorithm is $10^{98\times16} = 10^{1568} \approx 2^{5208}$. This makes the proposed encryption system resistant to brute-force attacks, according to [36]. Table 14 shows that this value is superior to most encryption schemes found in similar literature.

TABLE 13. MAE values comparison of various images.

Image	Proposed	[25]	[18]	[22]	[23]
Lena	77.3617	N/A	77.4877	N/A	N/A
Peppers	81.718	N/A	81.9832	N/A	N/A
Mandrill	75.2894	N/A	75.1632	N/A	N/A
Girl	90.0213	N/A	89.9807	N/A	N/A
Sailboat	81.7741	N/A	82.1003	N/A	N/A
Average	81.2329	N/A	81.34302	N/A	N/A

TABLE 14. Key space values comparison.

Scheme	Key space
Proposed	$10^{1568} \approx 2^{5208}$
[18]	2^{1658}
[22]	2^{298}
[23]	2^{128}
[31]	2^{232}
[37]	10^{128}
[38]	2^{299}
[39]	2^{372}
[40]	2^{256}
[41]	10^{169}
[42]	2^{219}
[43]	2^{128}
[44]	2^{187}
[45]	10^{94}
[46]	2^{256}
[25]	2^{128}

12) ENCRYPTION TIME ANALYSIS

The efficiency of the proposed encryption algorithm is a critical factor in its practical applicability. Encryption time, in particular, plays a crucial role in real-time applications where timely data transmission is essential. In this context, the proposed R^3 algorithm is specifically designed to prioritize computational efficiency, and its implementation is optimized to further enhance this attribute.

At the heart of the R^3 algorithm lie three core phases: rescaling, rotation, and randomization. These phases are built upon relatively straightforward mathematical operations, which inherently minimize the time complexity of the algorithm. The simplicity of these computations allows for swift execution, thus ensuring that the encryption process is as efficient as possible. This design choice was intentional, emphasizing computational efficiency to meet the demands of real-time applications.

To further enhance the computational efficiency of the proposed encryption algorithm, we implemented the R^3 algorithm using a variety of optimized programming

TABLE 15. Encryption time comparison of the Lena image of dimensions 256 × 256.

Scheme	Time [s]	Machine specifications (CPU and RAM)
Proposed	0.752824	AMD® Ryzen™ 5600H Mobile 3.3 GHz, 16 GB
AES	0.838	AMD® Ryzen™ 5600H Mobile 3.3 GHz, 16 GB
[18]	0.426243	2.9 GHz Intel® Core™ i9, 32 GB
[37]	2.582389	2.9 GHz Intel® Core™ i9, 32 GB
[39]	1.42545	2.9 GHz Intel® Core™ i9, 32 GB
[38]	0.25	N/A
[47]	1.1168	3.4 GHz Intel® Core™ i7, 8 GB
[42]	3.45	N/A
[48]	4.98	2.5 GHz AMD®, 4 GB
[49]	1.112	3.4 GHz Intel® Core™ i3, 4 GB
[39]	1.42545	2.9 GHz Intel® Core™ i9, 32 GB

techniques and tools. For instance, efficient data structures and algorithms are employed to ensure that the underlying computations are carried out as quickly and effectively as possible. Moreover, the power of computational parallelism is leveraged, splitting tasks into sub-tasks that can be computed simultaneously. This strategy is particularly effective for operations that can be performed concurrently, significantly reducing the overall computation time.

The proposed R^3 algorithm is programmed in Mathematica® 13.1, and while most of the steps were executed quite efficiently, the central rotation step bottlenecked the performance of the algorithm somewhat, accounting for over half of the encryption time. Regardless, the actual encryption time and its comparison to similar schemes are presented in Table 15. The table clearly shows that, despite the programming issues, the algorithm performs better than all the compared algorithms except one, with a sub-1-second encryption time for a 256 × 256 image. It should be noted that this comparison is not absolute: the actual encryption time of an image will depend highly on software and hardware implementation, making these values difficult to compare overall. Furthermore, AES is also employed to encrypt an image of the same dimensions on the same machine to showcase that the proposed scheme is more efficient, as shown in Table 15.

13) THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ANALYSIS

The United States' National Institute of Standards and Technology (NIST) has a statistical analysis suite designed specifically for assessing the effectiveness of pseudo-random number generators. While not exactly designed for encryption schemes, applying the testing suite to the encryption of a test image can yield some information about the overall efficacy of the encryption scheme. Mostly, passing all of the tests in the NIST SP 800 − 22 test suite can confirm that the output of the encryption scheme is of high randomness–high enough, in fact, to work as a pseudo-random number generator in its own right. Table 16 shows the result of a NIST analysis performed on the bit-stream of

TABLE 16. NIST analysis of the image-data bit-stream from the encrypted Sailboat image of size 256 × 256.

Test Name	p-value	Remarks
Frequency	0.888395	Success
Block Frequency	0.747756	Success
Runs	0.025998	Success
Longest run of ones	0.602116	Success
Rank	0.387851	Success
FFT	0.561257	Success
Non overlapping T.M. (000000001)	0.273642	Success
Overlapping T.M.	0.811479	Success
Maurer's Universal	0.938364	Success
Linear complexity	0.463095	Success
Serial 1	0.843083	Success
Serial 2	0.866173	Success
Approx. entropy	0.238354	Success
Cum. sums forward	0.724428	Success
Cum. sums reverse	0.851699	Success
Random ex. 1	0.351210	Success
Random ex. 2	0.767811	Success
Random ex. 3	0.083782	Success
Random ex. 4	0.082888	Success
Random ex. 5	0.411272	Success
Random ex. 6	0.926426	Success
Random ex. 7	0.842099	Success
Random ex. 8	0.983662	Success
Random ex. var. 1	0.901591	Success
Random ex. var. 2	0.826341	Success
Random ex. var. 3	0.887553	Success
Random ex. var. 4	0.817641	Success
Random ex. var. 5	0.571068	Success
Random ex. var. 6	0.579574	Success
Random ex. var. 7	0.812266	Success
Random ex. var. 8	0.902387	Success
Random ex. var. 9	0.766160	Success
Random ex. var. 10	0.431874	Success
Random ex. var. 11	0.564319	Success
Random ex. var. 12	0.939418	Success
Random ex. var. 13	0.840912	Success
Random ex. var 14	0.853931	Success
Random ex. var. 15	0.739089	Success
Random ex. var. 16	0.540048	Success
Random ex. var. 17	0.359677	Success
Random ex. var. 18	0.322557	Success

the encrypted 256 × 256 Sailboat image. The table shows that all of the tests passed, and are statistically significant, with p-values greater than 0.01. Thus, it can be concluded that the output of the encryption scheme is random enough to act as a PRNG independently.

14) TestU01 FOR RANDOMNESS

The randomness of the output encrypted images produced by the proposed R^3 image encryption algorithm was evaluated using the TestU01 suite, which includes the federal information processing standards (FIPS) 140 − 2, Alphabit, and Rabbit tests. The FIPS 140 − 2 test suite, consisting of the Monobit, Poker, Runs, and Longest Run of Ones in a block tests, was passed successfully by the R^3 algorithm, indicating a balanced distribution of zeros and ones, an equivalent frequency of all possible 4-bit sequences, an acceptable range of total runs, and a non-significant length of the longest run of ones. Furthermore, the Alphabit and Rabbit tests were also passed, demonstrating excellent randomness of the generated bit sequences in both 32-bit integer and

TABLE 17. Analysis of TestU01.

Battery	Length	Remarks
FIPS $140-2$	10^5	Success
Rabbit	10^7	Success
Alphabit	10^7	Success

floating-point representations. The results are shown in Table 17. These results affirm the effectiveness and security of the R^3 algorithm, showcasing its ability to produce highly random and unpredictable encrypted images, a crucial characteristic for resisting potential attacks.

15) S-BOX PERFORMANCE ANALYSIS

Substitution boxes are key components of any encryption scheme, including the one proposed here. Several metrics exist to measure the efficiency of an S-Box at operating as a component of an encryption scheme, namely the following 5 tests:

- Nonlinearity (NL) [50] tests the S-Box to check how many bits in a Boolean function's truth table need to be changed to approach the nearest affine function.
- Linear approximation probability (LAP) [51] determines the likelihood for an S-box to be biased.
- Differential Approximation Probability (DAP) [52] measures the effect of some changes to the inputs on the output.
- Bit Independence Criterion (BIC) [53] assesses the relationship between the encryption and patterns in the encrypted output.
- Strict Avalanche Criterion (SAC) [53] measures the rate of change in the encryption relative to the rate of change in the input on a bit-by-bit basis.

Both the Chen and Chua systems were used to generate S-boxes. The results of the 5 S-box evaluation tests discussed are found in Table 18. While one of the metrics, namely the DAP, showed outputs equal to the ideal DAP value, the other tests did not fare quite as well, falling somewhat short of the ideal values. This can be attributed mainly to the dynamic method of generating S-boxes applied in the research, where pseudo-randomness is used as a source input for the S-box. Typical S-boxes are purposely designed to ensure a wide distribution of values, not necessarily a random one, making some of the tests look for qualities not apparent in an S-box generated using a random sequence. In any case, this method of generating S-boxes serves to create dynamic S-boxes of acceptable performance and increases the key space by an additional 13 variables per Chen S-box and 10 variables per Chua S-box, working to protect the system as a whole from brute-force interference.

Table 19 shows the computed S-box evaluation metrics for 2 of the sample S-boxes used in the proposed scheme in comparison to S-boxes taken from a number of other sources, including the AES encryption. While not the worst-performing S-boxes, especially when compared to some other

TABLE 18. Evaluation metrics for the S-box generated using the 4D hyper-chaotic Chen system of fractional-order (shown in Table 1) and the Chua-based S-box (shown in Table 2).

Evaluation Method	Optimal Score	Score of Chen S-box	Score of Chua S-box
NL	112	110	108
SAC	0.5	0.5056	0.4958
BIC	112	108	104
LAP	0.0625	0.0781	0.0937
DAP	0.0156	0.0156	0.0156

TABLE 19. Comparison between the proposed S-boxes and those provided in the literature.

S-Box	NL	SAC	BIC	LAP	DAP
Chen Table 1	110	0.5056	108	0.0781	0.0156
Chua Table 2	108	0.4958	104	0.0937	0.0156
[54] AES	112	0.5058	112	0.0625	0.0156
[55]	111	0.5036	110	0.0781	0.0234
[56]	107	0.497	103.5	0.1560	0.0390
[18] TM	108	0.503662	92	0.140625	0.015625
[18] OpenSSL	108	0.499023	112	0.0625	0.015625
[18] MKL	108	0.499268	104	0.09375	0.015625

S-boxes generated in the wake of chaotic encryption systems, the generated S-boxes still fail to match the performance of dedicated, non-dynamic S-boxes, like those used in AES [54], for example.

16) FURTHER TESTS

This subsection discusses and showcases the ability of the proposed image cryptosystem to fend off some further types of attacks, including known text attacks, occlusion attacks, and various noise attacks.

In relation to known text attacks, either a known plaintext attack (KPA) or a known ciphertext attack (KCA), the proposed image cryptosystem is provably semantically secure. In a KPA, an attacker has access to both the plain image and its encrypted version. The attacker's goal is to analyze the pairs of plain and encrypted images to derive the encryption key or discover the encryption algorithm. In a KCA, the attacker has access to the encrypted image but not its corresponding plain image. The goal of the attacker is to derive the plain image or the encryption key from the known encrypted image. Since the proposed image cryptosystem has 2 stages of data XORing and the application of S-boxes, an attacker is not able to derive the encryption key in either attack. The utilization of 2 S-boxes provides the needed non-linearity, thus completely eradicating the relationship between a plain image and its corresponding encrypted output version.

In relation to chosen plaintext attacks (CPA), an attacker can choose arbitrary plain images and obtain the corresponding encrypted versions. The goal is to obtain the encryption key or learn more about the encryption algorithm. Such an attack assumes that the attacker has full knowledge of the cryptosystem. Even in such a case, without knowledge of the encryption keys, the vast key space that the proposed cryptosystem possesses prohibits such an attack from ever

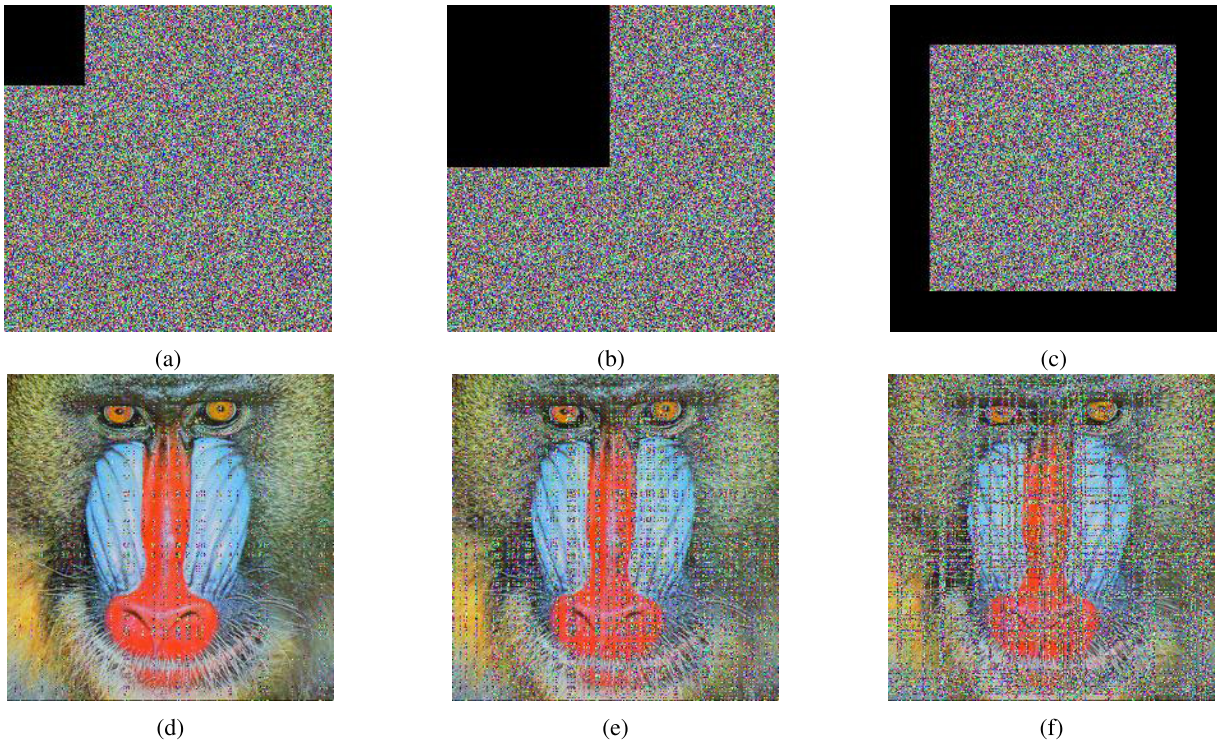


FIGURE 21. Various occlusion attacks on encrypted images (a) 12.5%; (b) 25%; (c) 56.25% and the resulting decrypted ones (d) 12.5%; (e) 25%; (f) 56.25%.

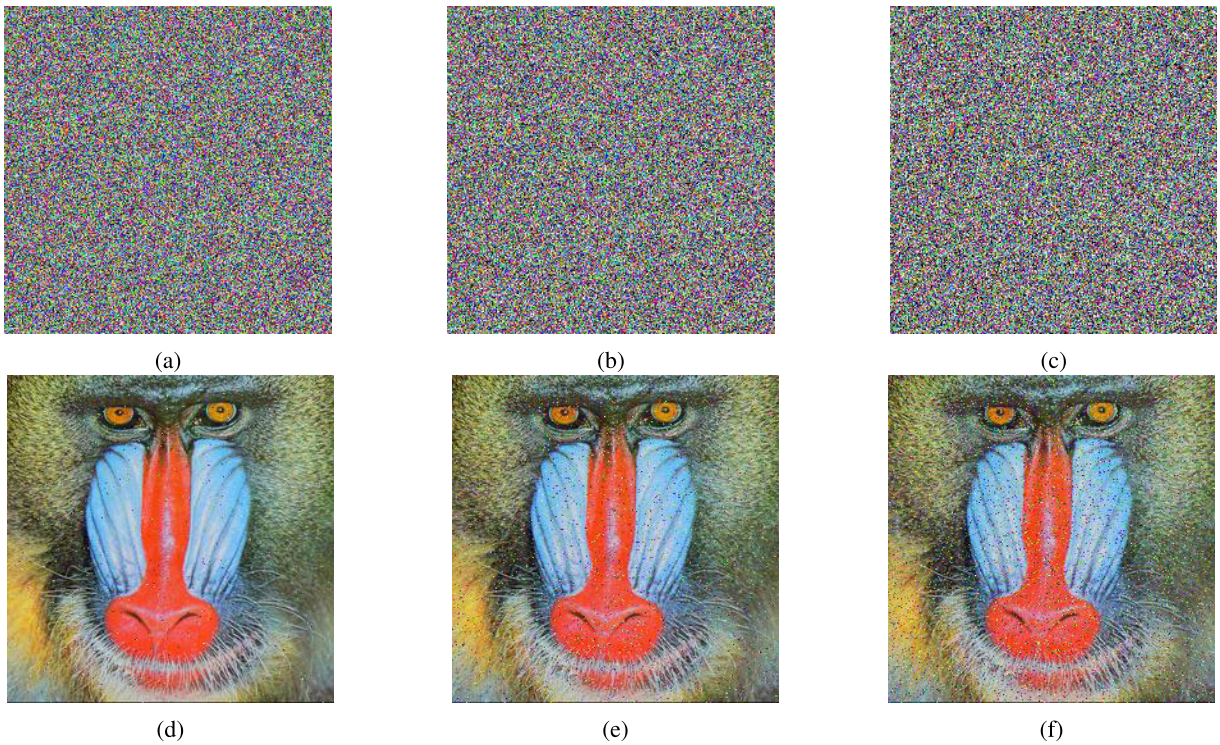


FIGURE 22. Various strengths of S&P attacks on encrypted images (a) 1%; (b) 5%; (c) 10% and the resulting decrypted ones (d) 1%; (e) 5%; (f) 10%.

being successful. It was shown in Subsection V-B11 that a key space of 2^{5208} is achieved. On the other hand, in a chosen ciphertext attack (CCA), an attacker can choose arbitrary encrypted images and learn their corresponding decrypted

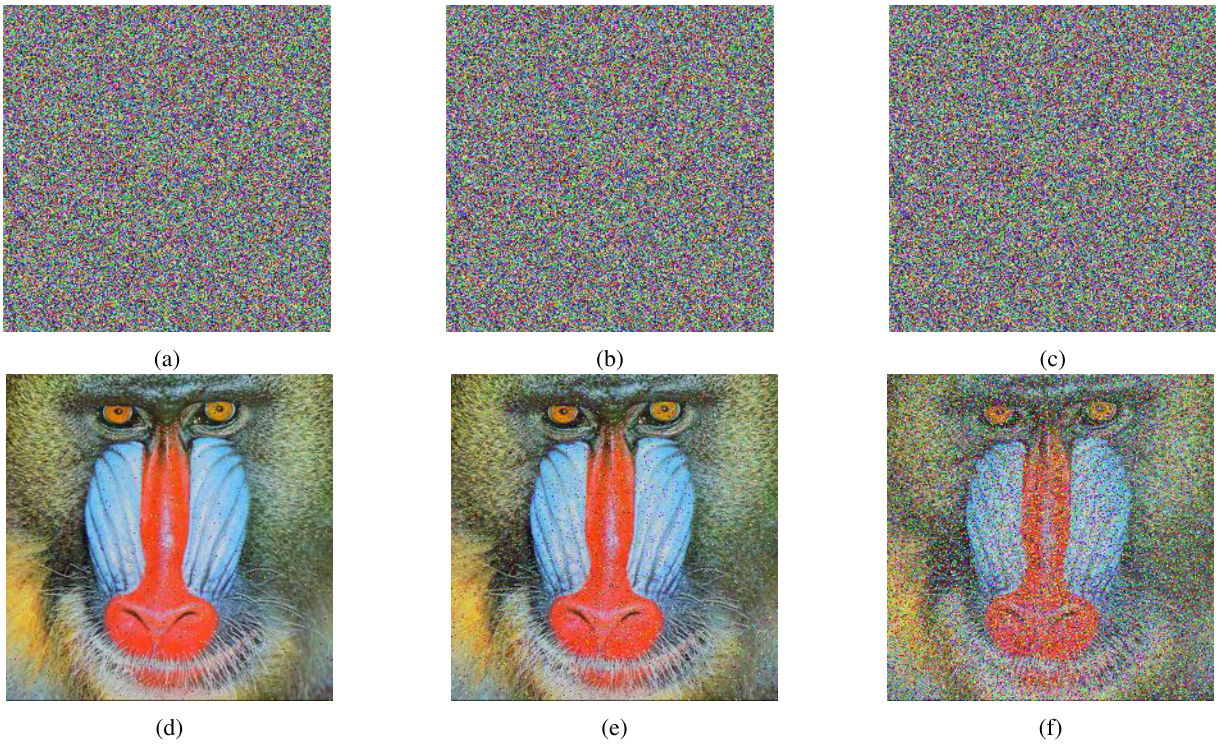


FIGURE 23. Various standard deviations of Gaussian noise attacks on encrypted images (a) $\sigma = 0.0008$; (b) $\sigma = 0.001$; (c) $\sigma = 0.002$ and the resulting decrypted ones (d) $\sigma = 0.0008$; (e) $\sigma = 0.001$; (f) $\sigma = 0.002$.

plain versions. However, this type of attack is particularly relevant for public-key cryptographic systems, which is not the case here as the proposed image cryptosystem depends on the use of symmetric encryption keys.

An occlusion attack is a type of attack where a portion of the encrypted image is deliberately altered or occluded to decipher the encryption algorithm's behavior or even retrieve the original image. The attacker can either remove or replace part of the encrypted image with arbitrary data and observe the effect on the decrypted image. The key reason for testing image encryption algorithms against occlusion attacks lies in the inherent structure of image data. Unlike text or other forms of data, images usually have strong correlations between neighboring pixels. If an encryption algorithm does not sufficiently randomize these correlations, an attacker might be able to exploit them. For example, an attacker could replace a region of an encrypted image with another part of the same image. If the algorithm does not sufficiently randomize the image, the decrypted image might show recognizable parts of the original image in the occluded region. This could potentially enable the attacker to retrieve parts of the original image or understand the behavior of the encryption algorithm, thereby compromising its security. Therefore, it's essential to test image encryption algorithms against occlusion attacks to ensure they sufficiently randomize the image and are resistant to these types of attacks. This enables the encryption algorithm to provide robust security for image data, ensuring its integrity and confidentiality even in the face of sophisticated attacks. Figure 21 provides examples of occlusion attacks carried out on different portions of encrypted images using the proposed cryptosystem. It is clear that the corresponding decrypted images are all still recognizable as those of the Mandrill image, albeit increasingly deteriorated with increases in the portion of their occluded encrypted versions.

In the context of cryptanalysis and rogue cyber operations, an attacker might introduce various types of noise to acquired encrypted images. The reasons for introducing such noise could be manyfold. First, the attacker may want to disrupt the viewing of the decrypted image, making it harder for the legitimate recipient to extract useful information from the image. Second, the attacker may introduce noise and observe its effect on the decrypted image. Depending on how the encryption algorithm handles noise, this could potentially give the attacker insights into the workings of the algorithm or the content of the original image. The literature on image cryptosystems mainly shows interest in 2 such types of noise: salt and pepper (S&P) noise and Gaussian noise.

Testing an image cryptosystem against noise attacks is important for a number of reasons. First, it helps evaluate the cryptosystem's robustness against noise. In real-world scenarios, images can be subject to various kinds of noise during transmission or storage. Therefore, it is important for an encryption algorithm to maintain the confidentiality and integrity of the image data in the presence of such noise. Second, by introducing noise and observing its effect on

the decrypted image, an attacker might gain insights into the encryption algorithm. Therefore, testing against this type of attack can help ensure the algorithm does not reveal any information about the original image or the encryption process when subjected to noise. Lastly, in some cases, noise in a small part of the encrypted image can lead to errors in a large part of the decrypted image due to the cryptosystem's error propagation characteristics. Testing against S&P noise can help evaluate and minimize this error propagation. Figure 22 showcases the effect of introducing a S&P noise to encrypted images of Mandrill with increasing strengths. It is clear that despite the deteriorating quality of the decrypted images as the S&P strength increases, the images are all clearly identifiable as those of Mandrill. Similar observations and conclusions can be drawn from Fig. 23 in relation to Gaussian noise attacks with increasing severity.

VI. CONCLUSION AND FUTURE WORK

This article has presented a novel image cryptosystem that harnesses the principles of chaotic and hyper-chaotic systems. By employing unique image transformation techniques, including rescaling, rotation, and randomization, the R^3 algorithm leverages the unpredictable behavior of the Chua system and the hyper-chaotic nature of the Chen system. The proposed algorithm has demonstrated significant robustness against various types of attacks, such as differential, statistical, and brute-force attacks. Moreover, its output was shown to satisfy a wide array of randomness tests, through passing both the NIST suite of tests as well as TestU01. The vast key space of 2^{5208} enhances its resistance to brute-force attacks and amplifies the overall security of the system. Importantly, the algorithm has shown remarkable efficiency in terms of computational speed and minimal resource consumption, making it ideal for real-time applications. With the rising demand for superior security in the digital information era, the proposed algorithm serves as a vital tool for securing digital images in diverse applications, including secure communication, data storage, and multimedia transmission. This research contributes significantly to the ongoing development and evolution of high-security image encryption methodologies.

Despite the promising results, there is still room for further exploration and enhancement of the proposed algorithm. Future work may focus on several aspects. First, while the proposed algorithm has shown robustness against several types of attacks, further testing against other potential threats could strengthen its overall security profile. This includes, but is not limited to, testing against adaptive and intelligent attacks that leverage machine learning techniques. Second, the practical implementation of this algorithm in real-world applications can be investigated. This includes integrating the algorithm into existing digital communication systems or storage solutions and conducting empirical studies to assess its performance in these environments. The proposed algorithm opens a new avenue in the field of image encryption. The underlying principles and techniques employed in the proposed algorithm could potentially be extended to other multimedia types, such as video and audio, thus broadening its applicability and impact.

REFERENCES

[1] S. Scherrer and A. Perrig, "Security, anonymity, privacy, and trust," in *Future Networks, Services and Management: Underlay and Overlay, Edge, Applications, Slicing, Cloud, Space, AI/ML, and Quantum Computing*. Cham, Switzerland: Springer, 2021, pp. 367–381.

[2] 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.

[3] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Logistic sine map based image encryption," in *Proc. Signal Process., Algorithms, Archit., Arrangements, Appl. (SPA)*, 2019, pp. 290–295.

[4] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, May 2017.

[5] X. Li, Y. Jiang, M. Chen, and F. Li, "Research on iris image encryption based on deep learning," *EURASIP J. Image Video Process.*, vol. 2018, no. 1, pp. 1–10, Dec. 2018.

[6] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing," *CAAI Trans. Intell. Technol.*, vol. 8, no. 2, pp. 440–452, Jun. 2023.

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

[8] I. Syafalni, G. Jonatan, N. Sutisna, R. Mulyawan, and T. Adiono, "Efficient homomorphic encryption accelerator with integrated PRNG using low-cost FPGA," *IEEE Access*, vol. 10, pp. 7753–7771, 2022.

[9] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical image cryptosystem using dynamic Josephus sequence and chaotic-hash scrambling," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022.

[10] 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.

[11] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, and X. Tang, "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Process.*, vol. 202, Jan. 2023, Art. no. 108745.

[12] W. Alexan, Y. Korayem, M. Gabr, M. El-Aasser, E. A. Maher, D. El-Damak, and A. Aboshousha, "AntEater: When Arnold's cat meets Langton's ant to encrypt images," *IEEE Access*, vol. 11, pp. 106249–106276, 2023.

[13] W. Alexan, M. Gabr, E. Mamdouh, R. Elias, and A. Aboshousha, "Color image cryptosystem based on sine chaotic map, 4D Chen hyperchaotic map of fractional-order and hybrid DNA coding," *IEEE Access*, vol. 11, pp. 54928–54956, 2023.

[14] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using multiple fractional-order moments and chaotic map," *Multimedia Tools Appl.*, vol. 81, no. 17, pp. 24347–24375, Jul. 2022.

[15] 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.

[16] M. Gabr, R. Elias, K. M. Hosny, G. A. Papakostas, and W. Alexan, "Image encryption via Base-n PRNGs and parallel base-n S-boxes," *IEEE Access*, vol. 11, pp. 85002–85030, 2023.

[17] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, "Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption," *Symmetry*, vol. 15, no. 5, p. 1081, May 2023.

[18] W. Alexan, N. Alexan, and M. Gabr, "Multiple-layer image encryption utilizing fractional-order Chen hyperchaotic map and cryptographically secure PRNGs," *Fractal Fractional*, vol. 7, no. 4, p. 287, Mar. 2023.

[19] A. Mazen, Y. Korayem, M. Gabr, and W. Alexan, "Three layered image encryption: An application of hyperchaos and cellular automata," in *Proc. Int. Telecommun. Conf. (ITC-Egypt)*, Jul. 2023, pp. 615–620.

[20] S. Khaled, M. Gabr, Y. Korayem, and W. Alexan, "Image encryption through cellular automata, S-box and tent chaotic map," in *Proc. Int. Telecommun. Conf. (ITC-Egypt)*, Jul. 2023, pp. 601–606.

[21] F. Budiman, P. N. Andono, and D. R. I. M. Setiadi, "Image encryption using double layer chaos with dynamic iteration and rotation pattern," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 2, pp. 57–67, 2022.

[22] B. Stoyanov and K. Kordov, "Image encryption using Chebyshev map and rotation equation," *Entropy*, vol. 17, no. 4, pp. 2117–2139, Apr. 2015.

[23] D. Ibrahim, K. Ahmed, M. Abdallah, and A. A. Ali, "A new chaotic-based RGB image encryption technique using a nonlinear rotational 16 × 16 DNA playfair matrix," *Cryptography*, vol. 6, no. 2, p. 28, Jun. 2022.

[24] C. Xu, J. Sun, and C. Wang, "A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 5573–5593, Mar. 2020.

[25] W. S. Sayed and A. G. Radwan, "Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems," *AEU Int. J. Electron. Commun.*, vol. 123, Aug. 2020, Art. no. 153268.

[26] J. Xiong, M. Ji'e, L. Wang, and S. Duan, "Fully chaotic medical image encryption scheme based on dynamic DNA and block rotation," *Phys. Scripta*, vol. 98, no. 7, Jul. 2023, Art. no. 075234.

[27] W. Ali, C. Zhu, R. Latif, M. Asim, and M. U. Tariq, "Image encryption scheme based on orbital shift pixels shuffling with ILM chaotic system," *Entropy*, vol. 25, no. 5, p. 787, May 2023.

[28] M. B. Savadkouhi, H. H. S. Javadi, and M. A. Tootkaboni, "Application of S-boxes based on the chaotic Hindmarsh-rose system for image encryption," *J. Math. Model.*, vol. 11, no. 2, pp. 277–300, 2023.

[29] H.-K. Wang, G.-B. Xu, and D.-H. Jiang, "Quantum grayscale image encryption and secret sharing schemes based on Rubik's cube," *Phys. A, Stat. Mech. Appl.*, vol. 612, Feb. 2023, Art. no. 128482.

[30] O. D. Singh, S. Dhall, A. Malik, and S. Gupta, "A robust and secure immensely random GAN based image encryption mechanism," *Multimedia Tools Appl.*, vol. 82, no. 13, pp. 19693–19743, May 2023.

[31] A. U. Rehman, A. Firdous, S. Iqbal, Z. Abbas, M. M. A. Shahid, H. Wang, and F. Ullah, "A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine," *IEEE Access*, vol. 8, pp. 172275–172295, 2020.

[32] Z. Yan, "Controlling hyperchaos in the new hyperchaotic Chen system," *Appl. Math. Comput.*, vol. 168, no. 2, pp. 1239–1250, Sep. 2005.

[33] 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.

[34] C. P. Li, W. H. Deng, and D. Xu, "Chaos synchronization of the Chua system with a fractional order," *Phys. A, Stat. Mech. Appl.*, vol. 360, no. 2, pp. 171–185, Feb. 2006.

[35] 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.

[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] 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.

[38] 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.

[39] 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.

[40] H. Gao and X. Wang, "Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position," *IEEE Access*, vol. 9, pp. 105627–105640, 2021.

[41] 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, Dec. 2019.

[42] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020.

[43] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on logistic map and dynatomic modular curve," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8911–8938, Apr. 2018.

[44] Y. Wang, C. Wu, S. Kang, Q. Wang, and V. I. Mikulovich, "Multi-channel chaotic encryption algorithm for color image based on DNA coding," *Multimedia Tools Appl.*, vol. 79, nos. 25–26, pp. 18317–18342, Jul. 2020.

[45] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018.

[46] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field ZN," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21803–21821, Aug. 2018.

[47] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.

[48] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[49] 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.

[50] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1989, pp. 549–562.

[51] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, and I. Cho, "Provable security against differential and linear cryptanalysis for the SPN structure," in *Proc. Int. Workshop Fast Softw. Encryption*. Cham, Switzerland: Springer, 2000, pp. 273–283.

[52] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.

[53] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1985, pp. 523–534.

[54] J. Daemen and V. Rijmen, *The Design of Rijndael*, vol. 2. Cham, Switzerland: Springer, 2002.

[55] 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.

[56] 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.

MOHAMED GABR (Member, IEEE) was born in Cairo, Egypt, in 1989. He received the B.Sc., M.Sc., and Ph.D. degrees in computer science and engineering from German University in Cairo (GUC), Egypt, in 2011, 2013, and 2023, respectively.

He has been with the Computer Science and Engineering Department, since 2011. He is currently teaching various courses in relation to computer vision, artificial intelligence, compilers, 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.

Dr. Gabr has been granted the Best Paper Award at the 26th IEEE Conference on Signal Processing Algorithms, Architectures, Arrangements and Applications, SPA'2023 in Poznan, Poland.

YOUSEF KORAYEM (Senior Member, IEEE) was born in Cairo, Egypt, in 2001. He received the B.Sc. degree in computer science and engineering from German University in Cairo (GUC), Egypt, in 2003. He has, as of yet, published a number of IEEE conference papers. His research interests include information security and image processing.

YEN-LIN CHEN (Senior Member, IEEE) received the B.S. and Ph.D. degrees in electrical and control engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2000 and 2006, respectively. From February 2007 to July 2009, he was an Assistant Professor with the Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan. From August 2009 to January 2012, he was an Assistant Professor with the Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei, Taiwan, where he was an Associate Professor, from February 2012 to July 2015. Since August 2015, he has been a Full Professor with the National Taipei University of Technology. His research interests include artificial intelligence, intelligent image analytics, embedded systems, pattern recognition, intelligent vehicles, and intelligent transportation systems. His research results have been published in over 100 journals and conference papers. He is a fellow of the IET and a member of ACM, IAPR, and IEICE.

POR LIP YEE (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from Universiti Malaya, Malaysia. He is currently an Associate Professor with the Faculty of Computer Science and Information Technology, Universiti Malaya. His research interests include neural networks (such as supervised and unsupervised learning methods, such as support vector machine and extreme learning machine), bioinformatics (such as biosensors and pain research), computer security [such as information security, steganography, and authentication (graphical password)], grid computing, and e-learning framework.

CHIN SOON KU received the Ph.D. degree from Universiti Malaya, Malaysia, in 2019. He is currently an Assistant Professor with the Department of Computer Science, Universiti Tunku Abdul Rahman, Malaysia. His research interests include AI techniques (such as genetic algorithm), computer vision, decision support tools, graphical authentication (authentication, picture-based password, and graphical password), machine learning, deep learning, speech processing, natural language processing, and unmanned logistics fleets.

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 a member of the Faculty of Information Engineering and Technology, GUC, teaching various courses in relation to wireless communications, modulation and coding, information theory, digital logic design, circuit theory, and mathematics. In 2023, he was promoted to the academic rank of an associate professor in electrical engineering and information technology. He has been an Associate Professor with the New Administrative Capital, Mathematics Department, German International University (GIU), Egypt, since 2019. He is the author or coauthor of more than 80 journal articles and conference papers. His research interests include wireless communications, information security, image and signal processing, mathematical modeling, and engineering education.

Dr. Alexan is also a member of the ACM and has been granted the Best Paper Award at the 19th and 26th IEEE Conference on Signal Processing Algorithms, Architectures, Arrangements and Applications (SPA'2015 and SPA'2023, respectively), 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.