Review Article

Rating of Modern Color Image Cryptography: A Next-Generation Computing Perspective

Muhammad Samiullah,1 Waqar Aslam,1 Muhammad Asghar Khan,2 Haya Mesfer Alshahrani,3 Hany Mahgoub,4 Ako Muhammad Abdullah,5 M. Ikram Ullah,6 and Chien-Ming Chen7

1Department of Computer Science & IT, The Islamia University of Bahawalpur, Pakistan
2Hamdard University, Islamabad, Pakistan
3Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
4Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
5Computer Science Department, College of Basic Education, University of Sulaimani, Iraq
6Department of Information Sciences, University of Education, Lahore, Pakistan
7Shandong University of Science and Technology, Qingdao, China

Correspondence should be addressed to Chien-Ming Chen; chienmingchen@ieee.org

Received 27 December 2021; Revised 17 February 2022; Accepted 2 March 2022; Published 22 March 2022

Academic Editor: Shalli Rani

Copyright © 2022 Muhammad Samiullah et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Issues such as inefficient encryption architectures, nonstandard formats of image datasets, weak randomness of chaos-based Pseudorandom Number Generators (PRNGs), omitted S-boxes, and unconvincing security metrics leading to increased computational time and inadequate security level of chaos and Deoxyribonucleic Acid- (DNA-) based image encryption schemes need careful examination towards the development of more stable encryption schemes in terms of efficiency and reasonable security. A new taxonomy of image encryption based on chaotic systems, hyperchaotic systems, and DNA is propounded to assess the impact of these issues on the performance and security metrics. The primary emphasis of this research is to study various recent encryption architectures centered on a variety of confusion and diffusion methods. It is aimed at assessing the performance and security of various ciphers using a cipher rating criterion that categorizes ciphers into different classes. The parameters that are included in the rating criteria are information entropy, chi-squared goodness of fit test for histogram uniformity analysis, encryption efficiency, key space, differential attacks (Number of Pixels Change Rate and Universal Average Changing Intensity), key sensitivity analysis, encryption time, randomness tests such as NIST-R (a statistical suite for validating the randomness designed by the National Institute of Standards and Technology), correlation coefficient analysis, contrast analysis, energy analysis, homogeneity analysis, Mean Absolute Error, peak signal-to-noise ratio, and robustness to noise and occlusion attacks.

1. Introduction

Digital images are the most attractive and valuable type of data in social networks owing to the sufficient supply of information. The information about people, Electronic Patient Records (EPRs), things, places, and lifetime events can be documented in the form of images and are frequently used in the world of the internet for communicating sensitive and confidential data. Over the past few years, governments and organizations have taken serious concern for the confidentiality and integrity of data at rest or in transit. In this respect, cryptography as a solution is playing an eminent role. Modern chaos and DNA-based cryptography must guarantee security with low computational needs; otherwise, the proposed cryptosystems would be discarded by the potential users. Chaotic systems are nonlinear
dynamical systems having sensitive dependence on initial conditions. The properties of chaotic systems such as sensitive dependence on initial conditions, randomness in the generated sequence, and complex behaviors have been attracting the researchers to implement it in encrypting and decrypting the images, and its efficient implementation with efficient encryption architectures produces excellent results as compared to existing cryptographic algorithms such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES). To improve the security and encryption efficiency, numerous gray and color image cryptosystems have emerged recently with excellent results. The work presented by [1] uses 2D alteration models to encrypt images, audios, and videos. This scheme provides high security features with low correlation, ideal entropy value, and faster encryption speed for gray-level image encryption. An image encryption scheme by [2] uses Piecewise Linear Chaotic Map (PWLCM) and Hyperchaotic Lorenz System (HLS) for DNA encoding, permutation, and diffusion. The test results of this scheme have shown a reasonable level of security with faster encryption speeds for gray-level and small-sized color images. Another image encryption/decryption algorithm proposed by [3] uses two rounds of permutation-diffusion by using two chaotic systems, dynamic DNA coding and sequencing operations. This scheme can resist statistical, plaintext, brute force, and differential attacks, but the encryption efficiency is degraded for larger dimensions and sizes of color images. Novel chaos and bit-level permutation proposed by [4] has good security and faster encryption speed advantage. But the special formats and size of the color images are not mentioned in the experimental results.

In this study, a systematic review with new taxonomy of image encryption based on chaotic systems, hyperchaotic systems, and DNA computing is propounded to assess the impact of the mentioned issues on the performance and security metrics. Moreover, some criteria are also selected to judge and quantify the worthiness of any cryptosystem. Issues such as inefficient encryption architectures, nonstandard formats of image datasets, weak randomness of chaos-based PRNGs, omitted S-boxes, and unconvincing security metrics leading to increased computational time and inadequate security level of chaos and DNA-based image encryption schemes need careful examination towards the development of a more stable encryption scheme in terms of efficiency and reasonable security. Additionally, there is a need to quantify and classify the encryption schemes into different classes by using some criteria. To this end, our specific contribution investigates the encryption architectures along with the findings of various symmetric image ciphers; a taxonomy of image encryption and cipher rating criteria to judge and quantify the worthiness of any cryptosystem is propounded.

The rest of the paper is structured as follows. Section 2 deals with definitions depicted in the taxonomy. Related work comprising encryption architectures of various image encryption schemes is given in Section 3. The encryption efficiency of some recently published cryptosystems is presented in Section 4. A review of chaotic and biometric-based substitution box is given in Section 5. And some proposed criteria to judge the cryptosystems are given in Section 6. Conclusion with future directions is given in Section 7.

2. Definitions and Taxonomies

In this section, definitions related to modern cryptography are presented. An extended taxonomy of modern cryptography is shown in Figure 1. Modern cryptography is comprised of asymmetric, symmetric, quantum cryptography, and hash functions, while symmetric cryptography is further decomposed into block and stream cipher. Block cipher is further divided into chaotic, hyperchaotic, and cosine/sine transform-based cryptography. And stream cipher can be subdivided into synchronous, asynchronous, and one-time pad.

2.1. Asymmetric Cryptography. In asymmetric cryptography, two different keys are created for encryption and decryption, i.e., at the sender’s side, the sender encrypts the plaintext with a key called public key and sends it to the communication network. The receiver on the other side decrypts the encrypted text with another key called secret key which is only known to the receiver (see Figure 2). Examples of asymmetric cryptography include Diffie-Hellman and RSA.

2.2. Symmetric Cryptography. In symmetric cryptography, a single key (same key) is used to encrypt and decrypt the data (see Figure 3). In order to safeguard the symmetric key, the asymmetric cipher can be used to share it among sender and receiver. Symmetric cryptography is further divided into block ciphers and stream ciphers. Block ciphers encrypt and decrypt the plaintext by taking a block of data, e.g., 32-bit and 64-bit, while stream ciphers process a single bit or byte at a time. Stream ciphers are further subdivided into synchronous ciphers, self-synchronizing (asynchronous), and one-time pad (OTP). In synchronous ciphers, an independent keystream is produced from the plaintext and ciphertext. Any character modification in the ciphertext does not influence the decryption process for the rest of the ciphertext, but insertion or deletion of character from the ciphertext will result in the failure of synchronization as well as the decryption process. In contrast, asynchronous ciphers generate their keystream from a particular number, say p, of former ciphertext digits and the key. Therefore, this scheme can handle the insertion or deletion of ciphertext character problems as was present in synchronous cipher. One-time pad is also called one-time encryption.

2.3. Chaotic Cryptography. It is the efficient implementation of mathematical chaos theory in the form of chaotic maps or systems to encrypt and decrypt the data (text, image, audio, and video) to transmit or preserve it in a secure way. The control parameters and initial conditions of chaotic maps are used as secret keys that are shared between transmitter and receiver. The secret key can then be again encrypted by using stream ciphers such as RSA for secure communication. The initial conditions can be generated by some mechanism from the input data. Many chaotic systems with varying dimensions until now have been implemented for the encryption of gray and color images. Chaotic systems
can be subdivided into continuous and discrete time chaotic systems. For example, Chua’s circuit (continuous time chaotic physical system) is the simplest electronic circuit that reveals chaotic behavior. Other continuous time chaotic systems are Duffing equation, folded-towel hyperchaotic map, Hadley chaotic circulation, Rossler attractor, etc. While the discrete time chaotic maps include logistic map, Arnold’s cat map, Baker’s map, Bagdonov map, and Henon map. The chaotic maps generate a random sequence that can further be improved to make it PRNGs. The intrinsic random sequence generated by the chaotic map is used for confusion or diffusion of the input image. Various cryptographic algorithms have been developed since 1989 to ensure the security of data at rest or in transit. Till 1995, cryptography used one-time pad with a chaotic system, though it is not suitable for encryption of image, audio, and video data. Later, the ergodicity property of chaotic maps is the focus of researchers towards designing cryptographic algorithms.
However, cryptosystems were not considered better due to being less efficient and less secure [5].

2.4. Hyperchaotic Cryptography. The tasks of cryptography are done through hyperchaotic systems. Hyperchaotic systems show complex dynamical behavior and high sensitive dependence on initial conditions with more than one positive Lyapunov exponents ($\lambda$) as compared to chaotic systems. Sensitive dependence is quantified by calculating Lyapunov exponents. The sequence generated by hyperchaotic systems has better randomness as compared to chaotic systems and can be used for image scrambling and diffusion [6]. Some hyperchaotic systems’ sequences can be used as PRNGs. Therefore, give better encryption results [7], a hyperchaotic map with higher dimensions has better ergodicity, more complex dynamic behavior, better randomness, and more than one positive Lyapunov exponents than low-dimensional hyperchaotic systems [8].

2.5. DNA Cryptography. Deoxyribonucleic Acid (DNA) shown in Figure 4 is biological DNA which is located in the cell’s nucleus and carries genetic information about all the organisms. DNA is basically a double helix (double-stranded) structure formed by base pairs attached to the sugar-phosphate backbone. Replication is an important property of DNA. The 4 chemical bases, i.e., adenine (A), guanine (G), cytosine (C), and thymine (T), on a single strand form a specific sequence called a genetic code. These bases are connected to the bases of the opposite DNA strand, i.e., A with T and C with G called base pairs. The group of base, sugar, and phosphate is called a nucleotide. DNA can be used in cryptography for storing, encrypting, key generation, and transmitting the image data by using digital DNA datasets available on NCBI. Using biological DNA for storing, processing, and encrypting information demands higher technical laboratory requirements. To this end, cryptography based on biological DNA is still in its infancy and needs further theoretical discussions and experiments. For the sake of simplicity, digital DNAs are being used for encrypting and decrypting the data and information by mimicking the biological DNA operations such as Conservative Site-Specific Recombination (CSSR), DNA pairing, DNA annealing, and DNA replication (Figure 5). DNA-based cryptography is done by using the DNA mapping rules and DNA operations [9–16].

2.6. Sine and Cosine Chaotic Maps. Cosine or sine chaotic maps are considered more complex chaotic maps due to the simplicity in structure and high chaotic behavior with an infinite chaotic range thus leading to large key space and unpredictability. Sine- and cosine-based chaotic maps may be used as general frameworks for the existing chaotic maps. For example, a one-dimensional discrete cosine polynomial chaotic map (Equation (1)) is used for image encryption in two phases, i.e., row phase and column phase. Row and column phases do permutation-substitution based on pseudorandom sequence generated by 1D-DCP. The authors replaced the sequential permutation-substitution architecture with parallel permutation-substitution architecture and reduced the processing time while encrypting an image and showed better security metrics results [17]:

$$\{ f : [-1;1] \Rightarrow [-1;1] \} \ x_{n+1} = f(x_n) = \mu(x_n^3 + x_n) \} . \quad (1)$$

The DCP scheme is shown in Figure 6. According to this figure, the sequence generated by 1D-DCP is used for the permutation and substitution of row and column pixel values simultaneously in $T$ number of rounds. Similarly, the one-dimensional sine transform-based chaotic map (1D-STBCM) proposed by [18] gives a larger chaotic range and more complex behavior and gives excellent performance. 1D-STBCM (Equation (2)) [18] can be used as a general framework for any two existing chaotic maps:

$$x_{i+1} = \sin \left( \pi (f(a, x_i) + g(b, x_i)) \right), \quad (2)$$

where $f(a, x_i)$ and $g(b, x_i)$ are two existing chaotic maps also called seed maps which may or may not be the same. $a$ and $b$
are the control parameters, and $x_i$ signifies the input in each iteration. The input $x_i$ along with control parameters $a$ and $b$ is supplied to two seed maps, i.e., $f(a, x_i)$, and $g(b, x_i)$ in each iteration, and then, the sine-based transformation is executed. Last but not least, a large number of chaotic maps with different chaotic behaviors can be generated by extending Equation (2) to three or more seed maps. Therefore, the extended system may have a higher degree of randomness and unpredictable output sequences.

The author in [19] proposed a 3D sine map to permute an image and obtained high security, fast speed, and resistivity against some common attacks. A second-order nonlinear differential equation with cosine transform is employed to generate chaotic S-box which was found to be much better in Strict Avalanche Criterion (SAC) and nonlinearity and can be used for encrypting the input image by using some substitution processes such as the Rijndael substitution process [20].

2.7. Quantum Cryptography. Peter Shor’s 1994 algorithm for factoring large prime numbers is one of the main motives to divert the attention of security experts to make use of quantum computing towards quantum cryptography. Quantum cryptography is dependent on quantum computing which is still in its infancy stage and cannot be considered true quantum architectures. True quantum computing will further transform the current cryptography into new amazing dimensions. Quantum cryptography is based on the principles of quantum mechanics (quantum superposition, quantum annealing, and quantum entanglement) to encrypt...
Table 1: Different forms of permutation-substitution.

| Ref  | Encryption architecture                                                                 | Findings                                                                 |
|------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| [19] | 3D permutation method: in this architecture, 3D orthogonal Latin squares and matching   | It saves encryption time as Latin squares are composed of integers only.   |
|      | matrices generated from 3D sine map are combined to permute the plain image; then, each  | It has resistivity against various attacks, fast speed, and high security.|
|      | component of the permuted matrix is subdivided into subblocks of the same size. The     |                                                                         |
|      | corresponding blocks of each component are linked and shifted (cyclic shift) according   |                                                                         |
|      | to the sorted position matrix generated by 3D sine map chaotic sequence. In addition,     |                                                                         |
|      | singular value decomposition (SVD) is also applied on the 3rd chaotic sequence to        |                                                                         |
|      | produce three more matrices, namely, \( u_1, s_1, v_1 \). Finally, the cyclic shifted  |                                                                         |
|      | matrix is modulated with \( u_1 \) to produce the encrypted version of plain image.   |                                                                         |
| [20] | Chaotic S-box-based substitution: in this architecture, 2nd order nonlinear differential  | The rotation and addition of random columns increased the immunity against plaintext attacks (PTAs). The encrypted image passed most of the NIST randomness tests. |
|      | is employed to generate chaotic S-box which was found to be much better in Strict        |                                                                         |
|      | Avalanche Criterion (SAC) and nonlinearity. The input image is rotated clockwise by 90°, |                                                                         |
|      | a random column is added to the left of the rotated image, and values are substituted    |                                                                         |
|      | with S-box by using the Rijndael substitution process.                                   |                                                                         |
| [25] | Key substitution architecture (KSA): it includes one round of key scheming and novel      | Yielded satisfactory encryption performance, better security, and         |
|      | substitution method. The key scheming phase is based on a logistic chaotic map whose    | computational efficiency as compared to traditional substitution-         |
|      | initial conditions are calculated from the weighted summation method. And the          | permutation architectures. But encryption time increases for large-sized |
|      | substitution is composed of random grouping, chaotic S-box construction, and random      | color images.                                                           |
|      | substitution.                                                                             |                                                                         |
| [26] | Cross-plane permutation and nonsequential diffusion process: in cross-plane, a single   | The encryption speed is rapid as it employs simple implementations of     |
|      | operation shuffles randomly all the RGB pixel positions. And in nonsequential         | encryption structures and chaotic map. It can mitigate the data losses    |
|      | diffusion process, the pixels are permuted according to the chaotic sequence             | and noises, i.e., robust against noise attacks and resists differential,   |
|      | generated by using 2D-Logistic Tent Modular Map (LTMM). Nonsequential diffusion          | chosen-plaintext attacks, and statistical attacks and is extremely        |
|      | process takes two rounds for good diffusion.                                             | sensitive to its secret key. It can serve real-time applications in      |
|      |                                                                                            | an efficient way.                                                        |
| [27] | Cyclic shift-based scrambling and diffusion based on household decomposition method: in  | The encryption speed is not mentioned in the paper. It has better entropy, |
|      | this architecture, the number of left shifts for the rows and columns is determined     | NPCR, UACI, and correlation coefficients and is robust to occlusion       |
|      | by the chaotic sequence; then, the cyclic shift algorithm is performed on rows and     | attacks up to 25% and salt & pepper noise attacks up to 0.01.            |
|      | columns. After this, diffusion is employed by using household orthogonal decomposition.   |                                                                         |
|      | In the end, XOR operation is performed between the chaotic sequence and the output of   |                                                                         |
|      | diffusion based on household orthogonal decomposition.                                   |                                                                         |
| [28] | Lorenz-based diffusion and Rossler-based confusion: Lorenz chaotic map is used to       | The encryption time is not mentioned in the paper. It has better entropy, |
|      | scramble the input image. In scrambling, RGB pixel positions are rearranged by using    | NPCR, UACI, and correlation coefficient results and is robust to          |
|      | the histogram equalized Lorenz chaotic sequence. And pixel substitution                 | classical attacks to some extent. The encrypted image also passed the    |
|      | based on Rossler system is achieved through XOR operation.                             | NIST SP 800-22 randomness tests; therefore, it can be used as PRNG.     |
| [29] | Latin square-based confusion and diffusion: in diffusion phase, pixel permutation is    | Although the cryptosystem demands less computational complexity, the      |
|      | achieved in two steps: step 1: shuffle the pixel rowwise to a new coordinate (x, LSQ(x, y)), where LSQ is a Latin square | cryptosystem can be broken by chosen-plaintext attack (CPA) combined with  |
|      | intermediate permuted image is produced in this step; step 2: similarly, shuffle the   | chosen-ciphertext attack (CCA) [29]. Moreover, the cryptosystem used the  |
|      | pixels of the intermediate permuted image columnwise to new coordinate (LSQ(x, LSQ(x, y)), LSQ(x, y)), while in the confusion phase, the pixel values are modified according to this equation \( c(n) = k(n) \oplus \{ [p(n) + k(n)] \mod 256 \} \oplus c(n - 1) \), where \( k(n), p(n), c(n), c(n - 1) \) are the current key value, current pixel, cipher pixel, and previous cipher pixel. | same key in each round of encryption.                                   |
| [30] | Logistic map-based permutation: in this cryptosystem, the architecture for              | The cryptosystem gave high probability of resisting brute force attacks   |
|      | permuting the input color image is based on 1D logistic map. A chaotic sequence is       | and better encryption effect and is able to recover images that were      |
|      | first generated by using initial values, sequence is sorted, and finally, the input     | 25% covered with some other pixels.                                      |
|      | image is scrambled using the sorted sequence.                                           |                                                                         |
Table 1: Continued.

| Ref     | Encryption architecture                                                                 | Findings                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| [31]    | Random permutation-substitution based on modular function: in this lightweight encryption architecture, a set of random permutation-substitutions through modular function at bit level followed by image rotations is performed. The encryption structure is scalable, i.e., any number of key sizes with any number of rounds may be used. | The smaller overhead with minimum number of rounds and simple structure reduces encryption time and energy consumption without reducing security level. |
| [32]    | $12 \times 12$ S-box-based substitution with linear permutation: $12 \times 12$ S-box is constructed through chain ring method $R_{12}$; then, it is extended to 24-bit extended lookup table. The 24-bit lookup table is decomposed into three cells of 8 bit each called L, M, R. Red, green, and blue components of input image are substituted with L, M, and R. Then, linear permutation is applied to produce permuted matrices. In the end, XOR is applied between permuted matrices and L, M, and R to get the encrypted image. | The ciphered image passed the NIST randomness tests. Less computational complexity and near to 8 bit/pixel entropy and resistance to some common attacks are the encouraging features of this encryption architecture. |
| [33]    | Lifting scheme-based permutation and substitution: pseudorandom chaotic sequence ($S$) of about half the size of the input image is generated and is circularly shifted called as A and substituted with S-box called as B. Then, input image after splitting, repeat predicting and updating steps of lifting scheme by making use of B for the purpose of permutation and substitution. The prediction and update repeat four times. |                                                                                                                                                 |
| [34]    | Kronecker product-based confusion-diffusion: input image is mapped to finite fields called P; then, scrambling and diffusion of P based on Kronecker product over finite field is done to produce R. Then, DNA operations based on Chen’s hyperchaotic system are applied on R to produce an encrypted image. | Permutation-substitution over finite fields using Kronecker product makes the cryptosystem capable of resisting known-plaintext attacks and chosen-plaintext attacks. The cryptosystem also has a good randomness, uniform histograms, and better entropy, NPCR, and UACI values. |
| [35]    | Fusion of two maps and transformation: a new chaotic map is produced by the fusion of two maps. The chaotic sequence of new map is exploited in the mathematical transformation function to convert the plain image into cipher image. | The obtained results in terms of NPCR, UACI, PSNR, entropy, histogram variances, correlation, and attacks are comparable to most of the recent studies. |
| [36]    | Image scrambling by using a mix of random, rotation, and zigzag permutation: in this approach, plain image is split into nonoverlapping subblocks. These subblocks are permuted by zigzag, rotation, and random fashion. Finally, XOR operation is performed between a key and scrambled image to get the encrypted image. Here, key is generated by using logistic map. | The simulation on 170 images of JPG type each having dimensions $512 \times 512$ reveals the efficiency of the proposed approach in terms of security and time complexity. The time complexity of the proposed approach comes out to be $O(M \times N)$. |

and decrypt the messages with guaranteed security. The cryptographic tasks require a quantum computer. The quantum computer with its immense power can break the RSA’s 2048-bit asymmetric algorithm in a few seconds on a mature quantum architecture; otherwise, it will take billions of years on classical computing architecture [21]. Quantum computing uses qubits to encode the information. Unlike a classical bit, the qubit is the basic building block in quantum computing (see Figure 7). The quantum superposition principle is used to set a qubit to form a quantum state. Several combinations of 0’s and 1’s can be processed on quantum architectures at the same time at a very less computational time. A qubit can exist in a state of $|0\rangle$, $|1\rangle$ and in a combined state of 0 and 1 called a superposition state and is denoted by $|\psi\rangle = a|0\rangle + b|1\rangle$. The qubit’s superposition state can be entangled with another quantum bit to make a new valid state. The qubits in quantum architecture are probabilistic as compared to classical bits which are deterministic [22]. The branches of quantum cryptography including Quantum Secret Sharing (QSS), Quantum Key Distribution (QKD), Quantum Secure Direct Communication (QSDC), Quantum Signature (QS), Quantum Private Query (QPO), Quantum Anonymous Voting (QAV), Quantum Sealed bid Auction (QSA), Quantum Public Key (QPK) cryptosystem, Quantum Key Agreement (QKA), and Quantum Identity Authentication (QIA) needs further development, review, and experiments to mature the field of quantum cryptography [23].

3. Related Work

In this section, the encryption architectures along with their findings of various image encryption schemes are presented. Various improvements in permutation-substitution...
architecture and permutation only architecture have been done after the classical chaos-based architectures [24]. Encryption architecture is a way or a method of doing substitutions, permutations, and transformations in the encryption algorithms by exploiting an encryption key. The key can be generated from a chaotic or hyperchaotic system. While encrypting an image whether color or gray, a good encryption algorithm strictly follows the principles of confusion and diffusion. Encryption architectures include substitution-permutation network (SPN), Feistel Network

| Ref | Image Size (kB) | ET | Entropy | NPCR, UACI | Corr (Avg) | KS | NCPB |
|-----|----------------|----|---------|------------|------------|----|------|
| [38] | 256 × 256 | 111 | 0.021 s | 7.9971 | 99.56, 33.28 | <0.01 | 314.0836 |
|      | 512 × 512 | 284 | 0.093 s | — | — | — | 543.6427 |
|      | 1024 × 1024 | 768 | 0.387 s | — | — | — | 1147.879 |
| [39] | 256 × 256 | 111 | 0.0759 | 7.9971 | 99.55, 33.27 | -0.0026 | 1135.188 |
|      | 512 × 512 | 284 | 0.3156 s | 7.9971 | 99.59, 33.28 | 0.0082 | 2277 | 1844.878 |
|      | 1024 × 1024 | 768 | 1.3153 s | — | — | — | 3899.292 |
| [17] | 256 × 256 | 111 | 0.0111 s | 7.9992 | 99.62, 33.45 | 0.0057 | 2392 | 210.4423 |
|      | 512 × 512 | 284 | 0.036 s | 7.9993 | 99.66, 33.45 | — | 2104 | 5396.677 |
|      | 1024 × 1024 | 768 | 0.1342 s | 7.9989 | — | — | 3972.102 |
| [33] | 256 × 256 | — | 49.18 Mbps | 7.997 | 99.60, 33.46 | <0.001 | 2512 | 276.8842 |
|      | 512 × 512 | — | — | — | — | — | — |
|      | 1024 × 1024 | — | — | — | — | — | — |
| [41] | 256 × 256 | 111 | 0.0491 s | 7.9942 | 99.50, 33.32 | — | 734.3574 |
|      | 512 × 512 | 284 | 0.0921 s | 7.9951 | 99.45, 33.34 | <0.0063 | 21773 | 538.3817 |
|      | 1024 × 1024 | 1238 | 2.3541 s | 7.9841 | — | — | 6978.882 |
| [42] | 256 × 256 | 111 | — | 7.9977 | 99.60, 33.35 | 0.0102 | 2256 | 6231.583 |
|      | 512 × 512 | 263 | 0.9872 s | 7.9990 | 99.59, 33.42 | -0.0165 | 2256 | 6231.583 |
|      | 1024 × 1024 | 1238 | — | — | — | — | — |
| [38] | 256 × 256 | 268 | 0.079 s | 7.9971 | 99.56, 33.28 | <0.01 | 2231 | 488.755 |
|      | 512 × 512 | 768 | 0.096 s | — | — | — | 210.978 |
|      | 1024 × 1024 | 1238 | 1.212 s | — | — | — | 2832.189 |
| [43] | 256 × 256 | 268 | — | — | — | — | 2256 |
|      | 512 × 512 | — | 44.93 Mbps | 7.9991 | 99.60, 33.46 | <0.0005 | 302.6931 |
|      | 1024 × 1024 | 1238 | — | — | — | — | — |
| [44] | 256 × 256 | 268 | — | — | — | — | 2170 |
|      | 512 × 512 | — | 31.97 Mbps | 7.9977 | 99.59, 33.46 | <0.0003 | 425.3988 |
|      | 1024 × 1024 | 1238 | — | — | — | — | — |
| [45] | 256 × 256 | — | 0.097 s | 7.9992 | — | — | 2200 | 147.3328 |
|      | 512 × 512 | 768 | 0.276 s | 7.9993 | 99.62, 33.68 | -0.0003 | 583.6487 |
|      | 1024 × 1024 | 1238 | 0.664 s | 7.9993 | — | — | 890.4231 |
| [46] | 256 × 256 | 260 | 8.2 s | 7.9992 | 99.64, 33.4 | 0.00106 | (2 × 10^{47} × 256^{5536×5}) | 52358.77 |
|      | 512 × 512 | 768 | 16.43 s | 7.9998 | — | — | 35516.1 |
|      | 1024 × 1024 | 1238 | 38 s | — | — | — | 37547.96 |
Generalized Feistel Structure (GFS), and its different variants. Different forms of improved permutation-substitution techniques proposed by various researchers are listed in Table 1.

4. Encryption Efficiency of Cryptosystems

Another most important criterion of analyzing the cryptographic algorithms is encryption efficiency, especially for evaluating the cryptosystems for real-time internet applications. Based on the encryption time (ET), the encryption efficiency [37] in terms of encryption throughput (ETₜₜ) and number of cycles per byte (NCPB) is calculated by

\[ ETₜₜ = \frac{PI_{size}}{ET}, \]

\[ NCPB = \frac{CPU_{speed}}{ETₜₜ}, \]

where PI_{size}, ET, and CPU_{speed} are the plain image size in bytes, encryption time in seconds, and processor speed in Hertz, respectively, while NCPB is the number of cycles per byte. For example, 1-DCPIE proposed by [17] takes 36.1 ms to encrypt a $512 \times 512$ grayscale image of size 263 kB. Its encryption efficiency in terms of NCPB according to the abovementioned formulas will be 228 cycles per byte.

In this section, some recently published cryptosystems with minimum encryption time and encryption efficiency in terms of minimum number of cycles per byte (NCPB) are focused, and NCPB is computed. NCPB is computed on a 1.7 GHz processor with 2 GB RAM. The basic purpose is to identify the cryptosystems for real-time internet applications. The identified cryptosystems having better NCPB may be selected as lightweight ciphers, and improvements in these cryptosystems can be done.

The effort to attain a desired state or value of any cryptanalysis metric may affect the other cryptanalysis metrics such as encryption speed and robustness against noise attacks. Too much trade-off among security metrics may be caused by inefficient encryption architectures having multiple rounds and extensive formatting operations and using multiple chaotic systems, extensive DNA encoding, decoding, inefficient looping structures, inefficient source codes, etc.

A good cipher maintains a balance among these metrics by keeping an eye on the encryption architecture, type and size of input data, etc.; for example, the author in [9] proposed a hybrid model of DNA computing for encrypting the grayscale images of different sizes. The experimental results indicate that the proposed cryptosystem gives a good encryption effect, resists against known attacks, and is sufficiently fast for practical applications. In this regard, we have implemented this algorithm for color images of different sizes. The experimental results for color images of larger sizes greater than or equal to $512 \times 512$ degrade the performance of the algorithm in terms of encryption time by keeping the security level maximum. Therefore, it is not suitable in terms of speed for practical real-time applications especially in IoT. Therefore, the scrutinizing of the cryptosystems based on minimum encryption time (ET) by considering other cryptanalysis metrics such as entropy, NPCR, UACI, encryption efficiency (EE), correlation (Corr), key space (KS), and robustness is done and listed in Table 2.
| Analysis metrics | Class | Condition | Weight |
|------------------|-------|-----------|--------|
| ET (s)           | VH    | >50 and <100 |        |
|                  | H     | >20 up to 50  |        |
|                  | M     | ≥10 and ≤20   | VH = 1, H = 2, M = 3, L = 4, VL = 5 |
|                  | L     | ≥1 and ≤9    |        |
|                  | VL    | <1          |        |
| EE (NCPB)        | H     | <1000       |        |
|                  | M     | ≥1000 and ≤10000 |        |
|                  | L     | >ten thousand and <25000 |        |
|                  | VL    | >25000      | H = 4, M = 3, L = 2, VL = 1 |
| NIST-R           | P     | ≥50%        |        |
|                  | F     | <50%        | P = 1, F = 0 |
| Entropy          | H     | ≥99% and ≤100% |        |
|                  | M     | ≥98% and <99% |        |
|                  | L     | >95% and <98% |        |
| Corr             | S     | Close to 1  |        |
|                  | W     | Close to 0  | S = 0, W = 1 |
| HistU            | U     | ≥99% and <100% |        |
|                  | NU    | ≥98% and <98% |        |
| NPCR             | H     | ≥33%        |        |
|                  | M     | ≥30% and <33% |        |
|                  | L     | >28% and <30% |        |
| UACI             | H     | ≥80         |        |
|                  | M     | ≥70         | H = 3, M = 2, L = 1 |
|                  | L     | ≥65         |        |
| MAE              | H     | ≥2^{100}    |        |
|                  | M     | ≥2^{100}    |        |
|                  | L     | ≥2^{80} and <2^{100} |        |
| KS               | H     | ≥0.5        |        |
|                  | M     | ≥0.45       | H = 3, M = 2, L = 1 |
|                  | L     | >0.38 and <0.45 |        |
| KSn/avalanche    | H     | PSNR > 30   |        |
|                  | M     | PSNR > 20   |        |
|                  | L     | PSNR > 10 and ≤20 |        |
|                  | VL    | PSNR ≥ 8 and ≤10 |        |
| RbN (up to 10%)  | H     | PSNR > 30   |        |
|                  | M     | PSNR > 20   |        |
|                  | L     | PSNR > 10 and ≤20 |        |
|                  | VL    | PSNR ≥ 8 and ≤10 |        |
| RbO (up to 50%)  | H     | PSNR > 30   |        |
|                  | M     | PSNR > 20   |        |
|                  | L     | PSNR > 10 and ≤20 |        |
|                  | VL    | PSNR ≥ 8 and ≤10 |        |
| PSNR (E-D)       | H     | PSNR > 30   |        |
|                  | M     | ≥80         | H = 4, M = 3, L = 2, VL = 1 |
|                  | L     | ≥70         |        |
|                  | VL    | ≥50 and <70 |        |
Table 4: A quantified comparison of some recently published gray-level image cryptosystems based on Table 3.

| Ref | ET (5) | EE (4) | NIST-R (5) | Entropy (3) | Corr (1) | HistU (1) | NPCR (3) | UACI (3) | MAE (4) | KS (4) | Avalanche (3) | RbN (4) | RbO (4) | PSNR (E-D) (4) | Scores |
|-----|--------|--------|-------------|--------------|----------|-----------|-----------|----------|---------|--------|-----------------|--------|--------|-----------------|--------|
| 9   | VL (5) | H (4)  | P (5)       | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | H (4)   | M (2)  | L (2)            | M (3)  | H (4)  | 45/48          |
| 34  | L (4)  | H (4)  | P (5)       | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | M (3)   | H (4)  | L (2)            | M (3)  | H (4)  | 42/48          |
| 65  |        |        |             |              |          |           |           |          |         |       |                 |        |        |                 |        |
| 66  |        |        |             |              |          |           |           |          |         |       |                 |        |        |                 |        |
| 67  | L (4)  | M (3)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | H (3)            | L (2)  | L (2)  | H (4)          | 25/30  |
| 65  |        |        |             |              |          |           |           |          |         |       |                 |        |        |                 |        |
| 68  | VL (5) | M (3)  | —           | H (3)        | H (3)    | U (1)     | H (3)     | M (3)    | H (4)   | M (2)  | L (2)            | M (3)  | H (4)  | 39/43          |
| 69  | L (4)  | L (2)  | P (5)       | H (3)        | H (3)    | U (1)     | H (3)     | H (3)    | M (3)   | H (4)  | M (2)            | L (2)  | ND    | H (4)          | 39/44  |
| 27  |        |        |             |              |          |           |           |          |         |       |                 |        |        |                 |        |
| 70  | L (4)  | M (3)  | P (5)       | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | M (2)            | L (2)  | L (2)  | H (4)          | 37/44  |
| 2   | L (4)  | L (2)  | P (5)       | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | H (3)            | —      |        | H (4)          | 29/36  |
| 30  | VL (5) | H (4)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | M (2)            | H (4)  | —     | H (4)          | 34/37  |
| 71  | VL (5) | VL (1) | P (5)       | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | H (3)            | —      | —     | H (4)          | 33/36  |
| 72  |        |        |             |              |          |           |           |          |         |       |                 |        |        |                 |        |
| 73  | VL (5) | H (4)  | —           | W (1)        | U (1)    | H (3)     | H (3)    | M (3)    | M (3)   | H (3)  | L (2)            | L (2)  | H (4)  | 28/34          |
| 74  | VL (5) | H (4)  | P (5)       | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | H (3)            | —      | —     | H (4)          | 36/40  |
| 75  | VL (5) | H (4)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | M (3)  | H (3)            | L (2)  | —     | H (4)          | 32/35  |
| 76  | L (4)  | L (2)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | M (2)            | M (3)  | L (2)  | H (4)          | 32/39  |
| 77  | L (4)  | M (3)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | H (4)  | M (2)            | L (2)  | L (2)  | H (4)          | 32/39  |
| 78  | L (4)  | L (2)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | M (3)  | M (2)            | —      | —     | H (4)          | 28/31  |
| 79  | M (3)  | L (2)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | H (3)    | —       | M (3)  | M (2)            | —      | —     | H (4)          | 25/31  |
| 80  | M (3)  | L (2)  | —           | H (3)        | W (1)    | U (1)     | H (3)     | M (3)    | H (4)   | M (2)  | L (2)            | L (2)  | M (3)  | 32/43          |
Table 5: A quantified comparison of some recently published color image cryptosystems based on Table 3.

| Ref | ET (5) | EE (4) | NIST-R (5) | Entropy (3) | Corr (1) | HistU (1) | NPCR (3) | UACI (3) | MAE (4) | KS (4) | Avalanche (3) | RbN (4) | RbO (4) | PSNR (E-D) (4) | Scores |
|-----|--------|--------|------------|-------------|----------|-----------|----------|----------|---------|-------|--------------|---------|---------|---------------|--------|
| [81]| —      | —      | —          | H (3)       | W (1)    | U (1)     | H (3)    | H (3)    | M (3)   | H (4) | M (2)        | VL (1)  | VL (1)  | H (4)         | 27/34  |
| [82]| H (2)  | L (2)  | P (5)      | H (3)       | W (1)    | U (1)     | H (3)    | H (3)    | M (3)   | H (4) | M (2)        | L (2)   | L (2)   | H (4)         | 37/48  |
| [3]| L (4)  | L (2)  | —          | H (3)       | H (3)    | U (1)     | H (3)    | H (3)    | —       | H (4) | M (2)        | L (2)   | L (2)   | H (4)         | 34/43  |
| [72]| —      | —      | —          | H (3)       | H (3)    | U (1)     | H (3)    | H (3)    | M (3)   | H (4) | M (2)        | L (2)   | L (2)   | H (4)         | 31/34  |
| [83]| VL (5) | M (3)  | —          | H (3)       | H (3)    | U (1)     | H (3)    | H (3)    | L (2)   | H (4) | M (2)        | L (2)   | M (3)   | H (4)         | 38/43  |
| [84]| L (4)  | M (3)  | —          | H (3)       | H (3)    | U (1)     | H (3)    | H (3)    | ND      | H (4) | H (3)        | L (2)   | L (2)   | H (4)         | 35/39  |
| [68]| VL (5) | M (3)  | —          | H (3)       | H (3)    | U (1)     | H (3)    | H (3)    | M (3)   | H (4) | M (2)        | L (2)   | M (3)   | H (4)         | 39/43  |
| [69]| L (4)  | L (2)  | P (5)      | H (3)       | H (3)    | U (1)     | H (3)    | H (3)    | M (3)   | H (4) | M (2)        | L (2)   | ND     | H (4)         | 39/44  |
Table 6: Proposed CRT of some recently published image cryptosystems.

| Ref | Scaling factors | Key space | Key sensitivity | Histogram | Visual analysis (PSNR (plain-decrypted)) | Correlation analysis | Contrast analysis | Energy analysis | Homogeneity analysis | NPCR | UACI | Brute force attack | Information entropy | NRT: randomness | CPA | MAE | Robustness against noise | Robustness against occlusion | Encryption time | Decryption time | Encryption efficiency |
|-----|----------------|-----------|----------------|-----------|------------------------------------------|---------------------|------------------|-----------------|---------------------|-------|------|-----------------|-------------------|-----------------|-----|-----|---------------------|---------------------|-----------------|-----------------|---------------------|
|     |                |           |                |           |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
| [85] | Rating (1-5)  | 4         | 4              | 3           | 5                                        | 5                   | 3                | 3               | 4                   | 4     | 4    | 5               | 5                 | 3               | 3   | 1  | 1                    | 1                    |                |                 |                 |
|      | Marking factor | 2         | 2              | 2           | 2                                        | 2                   | 1                | 2               | 2                   | 2     | 2    | 2               | 2                 | 3               | 3   | 2  | 2                    | 2                    |                |                 |                 |
|      | Total marks    | 10        | 10             | 10          | 10                                       | 10                  | 5                | 5               | 10                  | 10    | 10   | 10               | 10                | 10              | 15  | 15 | 15                    | 15                   |                |                 |                 |
|      | Obtained marks | 8         | 8              | 10          | 10                                       | 10                  | 3                | 6               | 8                   | 8     | 8    | 10               | 10                | 12              | 15  | 6  | 3                    | 3                    |                |                 |                 |
|      | Sum Percentage |           |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
|      | obtained marks | 157       |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
|      | total marks    | 157       |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
| [86] | Rating (1-5)  | 4         | 4              | 5           | 5                                        | 5                   | 2                | 3               | 4                   | 5     | 5    | 5               | 5                 | 5               | 4   | 4  | 3                    | 4                    |                |                 |                 |
|      | Marking factor | 2         | 2              | 2           | 2                                        | 2                   | 1                | 2               | 2                   | 2     | 2    | 2               | 2                 | 3               | 3   | 2  | 2                    | 2                    |                |                 |                 |
|      | Total marks    | 10        | 10             | 10          | 10                                       | 10                  | 5                | 10              | 10                  | 10    | 10   | 10               | 10                | 15              | 15  | 10 | 10                    | 10                   |                |                 |                 |
|      | Obtained marks | 8         | 8              | 10          | 10                                       | 10                  | 2                | 6               | 8                   | 10    | 10   | 10               | 10                | 15              | 12  | 8  | 6                    | 12                   |                |                 |                 |
|      | Sum Percentage |           |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
|      | obtained marks | 187       |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
| [87] | Rating (1-5)  | 4         | 4              | 5           | 5                                        | 5                   | 2                | 3               | 4                   | 5     | 5    | 5               | 5                 | 5               | 4   | 4  | 3                    | 4                    |                |                 |                 |
|      | Marking factor | 2         | 2              | 2           | 2                                        | 2                   | 1                | 2               | 2                   | 2     | 2    | 2               | 2                 | 3               | 3   | 2  | 2                    | 2                    |                |                 |                 |
|      | Total marks    | 10        | 10             | 10          | 10                                       | 10                  | 5                | 10              | 10                  | 10    | 10   | 10               | 10                | 15              | 15  | 10 | 10                    | 10                   |                |                 |                 |
|      | Obtained marks | 8         | 8              | 10          | 10                                       | 10                  | 2                | 6               | 8                   | 10    | 10   | 10               | 10                | 15              | 12  | 8  | 6                    | 12                   |                |                 |                 |
|      | Sum Percentage |           |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
|      | obtained marks | 184       |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
| [88] | Rating (1-5)  | 3         | 4              | 5           | 5                                        | 5                   | 2                | 4               | 4                   | 5     | 5    | 5               | 5                 | 5               | 4   | 4  | 3                    | 4                    |                |                 |                 |
|      | Marking factor | 2         | 2              | 2           | 2                                        | 2                   | 1                | 2               | 2                   | 2     | 2    | 2               | 2                 | 3               | 3   | 2  | 2                    | 2                    |                |                 |                 |
|      | Total marks    | 10        | 10             | 10          | 10                                       | 10                  | 5                | 10              | 10                  | 10    | 10   | 10               | 10                | 15              | 15  | 10 | 10                    | 10                   |                |                 |                 |
|      | Obtained marks | 6         | 8              | 10          | 10                                       | 10                  | 2                | 8               | 8                   | 10    | 10   | 10               | 10                | 15              | 12  | 8  | 6                    | 12                   |                |                 |                 |
|      | Sum Percentage |           |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
|      | obtained marks | 185       |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
| [89] | Rating (1-5)  | 4         | 5              | 5           | 5                                        | 5                   | 4                | 4               | 4                   | 5     | 5    | 5               | 5                 | 5               | 4   | 4  | 3                    | 4                    |                |                 |                 |
|      | Marking factor | 2         | 2              | 2           | 2                                        | 2                   | 1                | 2               | 2                   | 2     | 2    | 2               | 2                 | 3               | 3   | 2  | 2                    | 2                    |                |                 |                 |
|      | Total marks    | 10        | 10             | 10          | 10                                       | 10                  | 2                | 8               | 8                   | 10    | 10   | 10               | 10                | 15              | 12  | 8  | 6                    | 12                   |                |                 |                 |
|      | Obtained marks | 6         | 8              | 10          | 10                                       | 10                  | 2                | 8               | 8                   | 10    | 10   | 10               | 10                | 15              | 12  | 8  | 6                    | 12                   |                |                 |                 |
|      | Sum Percentage |           |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
|      | obtained marks | 185       |                |             |                                          |                     |                  |                 |                     |       |      |                 |                   |                 |     |     |                     |                     |                |                 |                 |
Table 6: Continued.

| Ref | Scaling factors | Key space | Key sensitivity | Histogram | Visual analysis (PSNR (plain-decrypted)) | Correlation analysis | Contrast analysis | Energy analysis | Homogeneity analysis | NPCR | UACI | Brute force attack | Information entropy | NRT- randomness | CPA | MAE | Robustness against noise | Robustness against occlusion | Encryption time | Decryption time | Encryption efficiency |
|-----|----------------|-----------|----------------|-----------|-----------------------------------------|----------------------|------------------|-----------------|---------------------|-------|-------|-------------------|---------------------|------------------|-----|-----|-------------------------|-------------------------|---------------|---------------|---------------------|
|     | Marking factor |          |                |           |                                         |                      |                  |                 |                     |       |       |                   |                      |                 |    |     |                         |                         |              |               |                     |
|     | Total marks    | 10        | 10             | 10         | 10                                      | 10                   | 5                | 10              | 10                  | 10     | 10    | 15                | 15                  | 10              | 10            | 15                | 15                | 15              | 15            | 15                |
|     | Obtained marks | 8         | 10             | 10         | 10                                      | 10                   | 4                | 8               | 8                   | 10     | 10    | 15                | 15                  | 8               | 8             | 6                | 12                | 12              | 9             |
|     | Sum Percentage count | 193     |                   |             |                                          |                      |                  |                 |                     |        |       |                   |                      |                 |    |     |                         |                         |              |               |                     |
|     | Rating (1-5)   | 4         | 5               | 5           | 5                                       | 5                    | 3                | 3               | 3                   | 5      | 5     | 5                 | 5                    | 4               | 4             | 3                | 3                | 5              | 5             | 3                |
|     | Marking factor | 2         | 2               | 2           | 2                                       | 2                    | 1                | 2               | 2                   | 2      | 2     | 2                 | 2                    | 3               | 2             | 2                | 2                | 3              | 3             | 3                |
|     | Total marks    | 10        | 10             | 10         | 10                                      | 10                   | 5                | 10              | 10                  | 10     | 10    | 15                | 15                  | 10              | 10            | 15                | 15                | 15              | 15            | 15                |
|     | Obtained marks | 8         | 10             | 10         | 10                                      | 10                   | 3                | 6               | 6                   | 10     | 10    | 15                | 15                  | 8               | 6             | 6                | 15                | 15              | 9             |
|     | Sum Percentage count | 189     |                   |             |                                          |                      |                  |                 |                     |        |       |                   |                      |                 |    |     |                         |                         |              |               |                     |
|     | Rating (1-5)   | 5         | 5               | 5           | 5                                       | 5                    | 3                | 3               | 3                   | 5      | 5     | 5                 | 5                    | 4               | 4             | 3                | 4                | 4              | 4             | 4                |
|     | Marking factor | 2         | 2               | 2           | 2                                       | 2                    | 1                | 2               | 2                   | 2      | 2     | 2                 | 2                    | 3               | 2             | 2                | 2                | 3              | 3             | 3                |
|     | Total marks    | 10        | 10             | 10         | 10                                      | 10                   | 5                | 10              | 10                  | 10     | 10    | 15                | 15                  | 10              | 10            | 15                | 15                | 15              | 15            | 15                |
|     | Obtained marks | 10        | 10             | 10         | 10                                      | 10                   | 3                | 6               | 6                   | 10     | 10    | 15                | 15                  | 8               | 6             | 6                | 12                | 12              | 12            | 12                |
|     | Sum Percentage count | 191     |                   |             |                                          |                      |                  |                 |                     |        |       |                   |                      |                 |    |     |                         |                         |              |               |                     |
|     | Rating (1-5)   | 5         | 5               | 5           | 5                                       | 5                    | 3                | 3               | 3                   | 5      | 5     | 5                 | 5                    | 4               | 3             | 3                | 4                | 4              | 3             | 3                |
|     | Marking factor | 2         | 2               | 2           | 2                                       | 2                    | 1                | 2               | 2                   | 2      | 2     | 2                 | 2                    | 3               | 2             | 2                | 2                | 3              | 3             | 3                |
|     | Total marks    | 10        | 10             | 10         | 10                                      | 10                   | 5                | 10              | 10                  | 10     | 10    | 15                | 15                  | 10              | 10            | 15                | 15                | 15              | 15            | 15                |
|     | Obtained marks | 10        | 10             | 10         | 10                                      | 10                   | 3                | 6               | 6                   | 10     | 10    | 15                | 15                  | 8               | 6             | 6                | 12                | 12              | 9             |
|     | Sum Percentage count | 188     |                   |             |                                          |                      |                  |                 |                     |        |       |                   |                      |                 |    |     |                         |                         |              |               |                     |
|     | Rating (1-5)   | 3         | 4               | 5           | 5                                       | 5                    | 3                | 3               | 3                   | 5      | 5     | 5                 | 5                    | 4               | 3             | 3                | 3                | 3              | 3             | 4                |
|     | Marking factor | 2         | 2               | 2           | 2                                       | 2                    | 1                | 2               | 2                   | 2      | 2     | 2                 | 2                    | 3               | 2             | 2                | 2                | 3              | 3             | 3                |
|     | Total marks    | 10        | 10             | 10         | 10                                      | 10                   | 5                | 10              | 10                  | 10     | 10    | 15                | 15                  | 10              | 10            | 15                | 15                | 15              | 15            | 15                |

87.727273 (upper middle class)

85.909091 (upper middle class)

86.818182 (upper middle class)

85.454545 (upper middle class)
| Ref | Scaling factors | Key space | Key sensitivity | Histogram | Visual analysis (PSNR (plain-decrypted)) | Correlation analysis | Contrast analysis | Energy analysis | Homogeneity analysis | NPCR | UACI | Brute force attack | Information entropy | NIST-randomness | CPA | MAE | Robustness against noise | Robustness against occlusion | Encryption time | Decryption time | Encryption efficiency |
|-----|----------------|-----------|----------------|-----------|------------------------------------------|----------------------|------------------|----------------|-------------------|-------|------|-------------------|-------------------|-----------------|-----|-----|----------------------|----------------------|----------------|----------------|----------------------|
|     | Total marks    | 6         | 8              | 10        | 10                                       | 10                   | 3                | 6              | 6                 | 10    | 10   | 10                | 10                | 15              | 15  | 8   | 6                   | 9                  | 9               | 12             |
|     | Obtained marks |           |                |           |                                          |                      |                  |                |                   |       |      |                   |                   |                 |     |     |                      |                    |                |
|     | Sum            | 179       |                |           |                                          |                      |                  |                |                   |       |      |                   |                   |                 |     |     |                      |                    |                |
|     | Percentage count |          |                |           |                                          |                      |                  |                |                   |       |      |                   |                   |                 |     |     |                      |                    |                |
| [78] | Rating (1-5)   | 3         | 4              | 5          | 5                                        | 5                    | 3                | 3              | 4                 | 5     | 5    | 5                 | 5                 | 4              | 4   | 4   | 4                   | 4                  |                |
|     | Marking factor | 2         | 2              | 2          | 2                                        | 2                    | 1                | 2              | 2                 | 2     | 2    | 2                 | 2                 | 3              | 3   | 2   | 2                   | 2                  |                |
| [78] | Total marks    | 10        | 10             | 10         | 10                                       | 10                   | 5                | 10             | 10                 | 10    | 10   | 10                | 10                | 15             | 15  | 10  | 10                  | 10                 | 15             | 15  | 15  | 15                  |
| [78] | Obtained marks | 6         | 8              | 10         | 10                                       | 10                   | 3                | 6              | 8                 | 10    | 10   | 10                | 10                | 15             | 15  | 8   | 8                   | 6                  | 12             | 12  | 12  | 12                  |
| [78] | Sum            | 187       |                |           |                                          |                      |                  |                |                   |       |      |                   |                   |                 |     |     |                      |                    |                |
| [78] | Percentage count |          |                |           |                                          |                      |                  |                |                   |       |      |                   |                   |                 |     |     |                      |                    |                |

Total marks obtained: 187
Percentage count: 85 (upper class)
5. Novel S-Boxes

No doubt, S-box as a nonlinear lookup table plays a pivotal role in obscuring the relationship between the key and ciphertext. Although it has been adopted in some chaos-based ciphers, it is very rarely adopted in DNA-based image ciphers [47]. Numerous researchers have seriously neglected the importance of S-boxes in their chaos and DNA-based image encryption algorithms [26, 39, 48–51]. Uniqueness of the values and no correlation between the values in S-box are the indicators of a good S-box. The methods such as heuristic, Pseudorandom Number Generators (PRNGs), finite field inverse, and finite field exponent have been used for generating S-boxes to further enhance the security level of image cryptographic algorithms [52]. Chaos theory has also been implemented in designing S-box. For example, 8 × 8 S-box based on chaotic maps is used in an image cryptographic algorithm [53]. The design of dynamic S-box by using the Zhangtang chaotic system is proposed in [54]. A 3D controlled chaotic plasma-based algorithm is presented in [55] to generate S-box. Artificial Bee Colony (ABC) and 6D hyperchaotic system are utilized in the generation of S-box [56]. An optimal S-box based on the firefly algorithm and discrete chaos is created in [57]. Multiple chaotic systems can be exploited in designing optimal S-boxes. The author in [58] used two chaotic systems, i.e., Chen’s and Henon maps for creating chaotic S-box with improved randomness. The chaotic system called Logistic Sine System (LSS) having a wider chaotic range and better chaotic properties is employed in creating a single S-box of size 16 × 16 [59].

Biometric subdivisions are shown in Figure 8. The biometric subdivisions such as face, fingerprint, iris, and DNA can be utilized to generate initial conditions for hyperchaotic systems and to generate cryptographic keys that will aid in constructing the novel S-boxes in the cryptographic algorithms. To this end, fingerprint-based S-box with minimum execution time is generated in [52] by using ridge ending features of the fingerprints. The iris dataset is used by [60], to create the initial conditions for logistic map and sine map for creating crypto S-box. The crypto S-box contains unique values.

Similarly, biological DNA can be converted into digital DNA, and digital DNA can be used in designing S-boxes. A 16 × 16 S-box generated from the two DNA sequences (DS1 and DS2) taken from GenBank is proposed in [61]. The DS1 is converted into 16 × 16 S-box where each cell consists of four nucleotide bases equivalent to 1 byte. The DS2 is used to compute (row, col) pair. The DS1 DNA values are picked sequentially and placed in the third empty S-box according to the (row, col) pair computed from DS1. The S-box is generated by splitting the numbers (0-255) into four sets, and each set is independently coded into a DNA strand. In this way, four DNA strand sets are obtained. Perform the reverse Watson Crick on all the DNA strand sets. Another DNA strand is taken from GenBank, and XOR operation between DNA strand sets and GenBank DNA strand is performed. And finally, central dogma is applied to get the entries of DNA-based S-box [62]. Another approach to construct an S-box with nonrepeating values is composed of DNA coding, DNA addition and subtraction, XOR and arithmetic operations, and finally, the search procedure to eliminate the duplicate values [63]. In order to increase the level of confusion in cryptographic algorithms, the concept of multiple DNA or RNA-based S-boxes has also been proposed by the researchers. For example, [64] accomplished this task in three steps: (1) user string is converted into DNA string by using DNA mapping/coding rules, (2) DNA string is transformed into mRNA by simulating the biological replication and transcription processes, (3) mRNA size is reduced by splitting, addition, subtraction, and XOR operations, and (4) the reduced mRNA is used to construct S-box with 256 different hexadecimal values.

Cryptography based on physical and behavioral biometrics can be called as biocryptography. Biometric parameters (iris, DNA, fingerprint, etc.) can be exploited to generate a secret key while designing cryptographic algorithms. Biometric-based secret keys can lessen the demand for key storage and generation. Another concept of biohashing can be used to make secret keys in which biometric parameters are combined with hash algorithms such as MD5 and SHA-512.

6. Proposed Criteria to Evaluate Cryptosystems

Comparing cryptosystems’ performance and cryptanalysis parameters without noting image size and format is not rational. To the best of our knowledge, criteria to quantify the cryptosystems are not proposed. In this section, some criteria to quantify some recently published color image cryptosystems are proposed which are indicated in Table 3. Based on these criteria, we allocate weights to various cryptanalysis parameters, and overall scores of a cipher in the sense of security and robustness can be computed. The criteria include encryption time (ET), encryption efficiency (EE) in terms of NCPB, National Institute of Science and Technology-Randomness Test (NIST-R), entropy, correlation (Corr), histogram uniformity (HistU), Number of Pixels Change Rate (NPCR), Universal Average Changing Intensity (UACI), Mean Absolute Error (MAE), key space (KS), key sensitivity (KSn), robustness against noise (RbN), robustness against occlusion (Rbo), and peak signal-to-noise ratio between encrypted and decrypted images (PSNR (E-D)). The proposed judgement criteria given in Table 3 can be used for gray-level and color images and can be extended by including other metrics as well. The scores of some recently published ciphers based on the chosen criteria of Table 3 are given in Tables 4 and 5.

Similarly, Cipher Rating Taxonomy (CRT) to rate various ciphers is designed as a next proposal that can facilitate security researchers to assess the trustworthiness of their ciphers in double figures. The ratings of cryptanalysis parameters given in Table 3 can be extended, i.e., from 1 to 5 or 1 to 3. For example, to rate the entropy, we can rate it as ≥7.9999 (rating 5), ≥7.999 (rating 4), ≥7.99 (rating 3), ≥7.9 (rating 2), and <7.9 (rating 1). We have also introduced a critical marking factor or weight, which represents the significance of the cryptanalysis parameter, and it ranges from
1 (least significant) to 3 (most significant). Other than cryptanalysis parameters, other vulnerabilities such as Insecure Data Storage, Broken Cryptography, Insecure Data Transport, Cryptographic Flaw, and Privacy Concerns (secret key sharing, key management, etc.) can be added in the proposed CRT to assess the cryptosystems. Furthermore, CRT is an effort to further classify the past, present, and future ciphers and security systems in different classes and to bolster the transparent examination system. The proposed CRT shown in Table 6 presents the ratings and classifications of some recently published ciphers. We have divided the ciphers into 5 classes, namely, lower class, working class, lower middle class, upper middle class, and upper class. The criteria to classify the ciphers are the following: percentage count (pc) of a cipher is \( \geq 90 \) (upper class), \( \geq 80 \) (upper middle class), \( \geq 75 \) (lower middle class), \( \geq 70 \) (working class), and below 70 (lower class). Like so, lightweight ciphers can also be categorized by using the similar rating or modified rating method. The potential benefit of proposing CRT is that we can judge the cipher in a single shot, i.e., to (i) which class it belongs, (ii) which test metrics it has passed and which test metrics it has not passed, and (iii) which test metrics it has not performed. For example, a stakeholder needs a security algorithm for some application scenarios and demands moderate-level security with higher encryption speed to encrypt the bulk of image data. So, in this case, he/she can consult the CRT chart to match his/her demands.

7. Conclusions and Future Directions

We have covered the various aspects of chaotic and DNA-based cryptography. Assessment of various recently published cryptosystems based on encryption architectures, encryption efficiency, average encryption time, and number of cycles per byte is also done. Moreover, Cipher Rating Taxonomy (CRT) to rate various ciphers is also proposed that can facilitate security researchers to classify and assess the trustworthiness of their ciphers. For example, a stakeholder needs a security algorithm for some application scenarios and demands moderate-level security with higher encryption speed to encrypt the bulk of image data. So, in this case, the organization can consult the CRT chart to match its demands by considering its resources. The inclusion of hyperchaos-based confusion and diffusion in the cryptographic algorithms produces excellent security results but needs optimization to create an optimal trade-off between security and encryption efficiency and to make it lightweight. Moreover, hyperchaos coupled with genetic codes may advance the security of cryptographic practical applications besides the stoppage of side channel attacks.

No doubt, modern cryptography has transformed human existence and will continue to do so in communications, e-commerce, smart phones, digital signatures, and digital rights management (DRM) in the most advanced forms. Moreover, the proposed criteria may be extended, refined, and modified according to the classes of performance and cryptanalysis metrics under study.

**Data Availability**

All data generated or analyzed during this study are included in this article.

**Conflicts of Interest**

The authors declare no conflict of interest.

**Acknowledgments**

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under grant number (RGP 2/46/43) and Princess Nourah Bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R237), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia.

**References**

[1] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, “A chaotic-based encryption / decryption framework for secure multimedia communications,” *Entropy*, vol. 22, no. 11, pp. 1–23, 2020.

[2] Z. Li, C. Peng, W. Tan, and L. Li, “A novel chaos-based image encryption scheme by using randomly DNA encode and plaintext related permutation,” *Applied Sciences (Switzerland)*, vol. 10, no. 21, p. 7469, 2020.

[3] S. Zhou, P. He, and N. Kasabov, “A dynamic DNA color image encryption method based on SHA-512,” *Entropy*, vol. 22, no. 10, pp. 1–23, 2020.

[4] Z. Li, C. Peng, W. Tan, and L. Li, “A novel chaos-based color image encryption scheme using bit-level permutation,” *Symmetry*, vol. 12, no. 9, p. 1497, 2020.

[5] J. Gayathri and S. Subashini, “A survey on security and efficiency issues in chaotic image encryption,” *International Journal of Information and Computer Security*, vol. 8, no. 4, pp. 347–381, 2016.

[6] F. Yang, J. Mou, Y. Cao, and R. Chu, “An image encryption algorithm based on BP neural network and hyperchaotic system,” *China Communications*, vol. 17, no. 5, pp. 21–28, 2020.

[7] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, “An overview of encryption algorithms in color images,” *Signal Processing*, vol. 164, pp. 163–185, 2019.

[8] S. Sun, Y. Guo, and R. Wu, “A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping,” *IEEE Access*, vol. 7, pp. 28539–28547, 2019.

[9] E. Z. Zefreh, “An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions,” *Multimedia Tools and Applications*, vol. 79, no. 33-34, pp. 24993–25022, 2020.

[10] S. Kalsi, H. Kaur, and V. Chang, “DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation,” *Journal of Medical Systems*, vol. 42, no. 1, 2018.

[11] X. Aqul-ul-Rehman, M. Liao, A. Hahsmi, and R. Haider, “An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos,” *Optik*, vol. 153, pp. 117–134, 2018.

[12] X. Wu, J. Kurths, and H. Kan, “A robust and lossless DNA encryption scheme for color images,” *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 12349–12376, 2018.
X. Zhang, F. Han, and Y. Niu, “Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding,” *Computational Intelligence and Neuroscience*, vol. 2017, 11 pages, 2017.

B. Wang, Y. Xie, S. Zhou, X. Zheng, and C. Zhou, “Correcting errors in image encryption based on DNA coding,” *Molecules (Basel, Switzerland)*, vol. 23, no. 8, 2018.

G. Bachira and N. Khan, “A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI,” *IEEE Access*, vol. 7, pp. 81333–81350, 2019.

L. Sharp, DNA Sequencing and Sorting: Identifying Genetic Variations, COMAP, Bedford, USA, 2015.

M. Z. Talhaoui, X. Wang, and M. A. Midoun, “A new one-dimensional cosine polynomial chaotic map and its use in image encryption,” *The Visual Computer*, pp. 1–11, 2021.

Z. Hua, B. Zhou, and Y. Zhou, “Sine-transform-based chaotic system with FPGA implementation,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2557–2566, 2018.

J. Zhou, N.-R. Zhou, and L.-H. Gong, “Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix,” *Optics & Laser Technology*, vol. 131, article 106437, 2020.

A. Javeed, T. Shah, and A. Attaullah, “Lightweight secure image encryption scheme based on chaotic differential equation,” *Chinese Journal of Physics*, vol. 66, pp. 645–659, 2020.

C. R. Logan, O. Mailloux, C. D. Lewis II, and M. R. Grimaila, “Post-quantum cryptography what advancements in quantum computing mean for IT professionals logan,” *Cybersecurity And Privacy*, vol. 18, no. 5, pp. 42–47, 2016.

A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, “A computing perspective of quantum cryptography [energy and security],” *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 57–59, 2018.

H. Zhang, Z. Ji, H. Wang, and W. Wu, “Survey on quantum information security,” *China Communications*, vol. 16, no. 10, pp. 1–36, 2019.

J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1299–1284, 1998.

Y. Song, Z. Zhu, W. Zhang, H. Yu, and Y. Zhao, “Efficient and secure image encryption algorithm using a novel key-substitution architecture,” *IEEE Access*, vol. 7, pp. 84368–84400, 2019.

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

X. Wang, W. Xue, and J. An, “Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household,” *Chaos, Solitons and Fractals: the interdisciplinary journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena*, vol. 141, pp. 110309–110317, 2020.

D. S. Malik and T. Shah, “Color multiple image encryption scheme based on 3D-chaotic maps,” *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.

G. Hu, D. Xiao, Y. Wang, and X. Li, “Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion,” *Nonlinear Dynamics*, vol. 88, no. 2, pp. 1305–1316, 2017.

A. Hadji Brahim, A. Ali Pacha, and N. Hadj Said, “Image encryption based on compressive sensing and chaos systems,” *Optics and Laser Technology*, vol. 132, article 106489, 2020.
maps, and diffusion,” *Optics and Lasers in Engineering*, vol. 103, pp. 9–23, 2018.

A. Adeel, J. Ahmad, H. Larijani, and A. Hussain, “A novel real-time, lightweight chaotic-encryption scheme for next-generation audio-visual hearing aids,” *Cognitive Computation*, vol. 12, no. 3, pp. 589–601, 2019.

X. Zhang and X. Wang, “Digital image encryption algorithm based on elliptic curve public cryptosystem,” *IEEE Access*, vol. 6, pp. 70025–70034, 2018.

R. Ge, G. Yang, J. Wu, L. Luo, and S. Member, “A novel chaos-based symmetric image encryption using bit-pair level process,” *IEEE Access*, vol. 7, pp. 99470–99480, 2019.

O. Sengel, M. A. Aydin, and A. Serthas, “An efficient generation and security analysis of substitution box using fingerprint patterns,” *IEEE Access*, vol. 8, pp. 160158–160176, 2020.

G. Chen, “A novel heuristic method for obtaining _S_-boxes,” *Chaos, Solitons & Fractals*, vol. 36, no. 4, pp. 1028–1036, 2008.

Ü. Savusoglu, A. Zengin, I. Pehlivan, and S. Kasar, “A novel approach for strong _S_-box generation algorithm design based on chaotic scaled Zhongtang system,” *Nonlinear Dynamics*, vol. 87, no. 2, pp. 1081–1094, 2017.

N. M. G. Al-saidi, “A new _S_-box generation algorithm based on multistability behavior of a plasma perturbation model,” *IEEE Access*, vol. 7, pp. 124914–124924, 2019.

Y. Tian and Z. Lu, “_S_-box: six-dimensional compound hyperchaotic map and artificial bee colony algorithm,” *Journal of Systems Engineering and Electronics*, vol. 27, no. 1, pp. 232–241, 2016.

H. A. Ahmed, M. F. Zolkipi, and M. Ahmad, “A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map,” *Neural Computing and Applications*, vol. 11, pp. 1–18, 2019.

F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Computing and Applications*, vol. 31, no. 8, pp. 3317–3326, 2019.

Q. Lu, C. Zhu, and X. Deng, “An efficient image encryption scheme based on the LSS chaotic map and single _S_-box,” *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

F. Özkaynak, “From biometric data to cryptographic primitives: a new method for generation of substitution boxes,” in *Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics*, pp. 27–33, Bangkok, Thailand, 2017.

A. H. Al-wattar, R. Mahmood, Z. A. Zukarnain, and N. I. Udzir, “A new DNA-based _S_-box,” *International Journal of Engineering & Technology*, vol. 15, no. 4, pp. 1–10, 2015.

A. H. S. Al-Wattar, R. Mahmood, Z. A. Zukarnain, and N. I. Udzir, “Generating a new _S_-box inspired by biological DNA,” *International Journal of Computer Science and Application*, vol. 4, no. 1, pp. 32–42, 2015.

F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, “Proposal new _S_-box depending on DNA computing and mathematical operations,” in *15th International Conference on Multidisciplinary in IT and Communication Techniques Science and Applications, AIC-MITCSA 2016*, pp. 142–147, 2016.

A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, “A new approach to generate multi _S_-boxes based on RNA computing,” *International Journal of Innovative Computing, Information and Control*, vol. 16, no. 1, pp. 331–348, 2020.

T. Wang and M. H. Wang, “Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding,” *Optics and Laser Technology*, vol. 132, article 106355, 2020.

A. A. Abd El-Atif, B. Abd-El-Atty, and M. Talha, “Robust encryption of quantum medical images,” *IEEE Access*, vol. 6, pp. 1073–1081, 2018.

Y. Luo, X. Ouyang, J. Liu, and L. Cao, “An image encryption method based on elliptic curve Elgamal encryption and chaotic systems,” *IEEE Access*, vol. 7, pp. 38507–38522, 2019.

B. Arpaci, E. Kurt, and K. Çelik, “A new algorithm for the colored image encryption via the modified Chaś circuits,” *Engineering Science and Technology, an International Journal*, vol. 23, no. 3, pp. 595–604, 2020.

R. Anandkumar and R. Kalpana, “Designing a fast image encryption scheme using fractal function and 3D Henon map,” *Journal of Information Security and Applications*, vol. 49, p. 102390, 2019.

A. Sahasarabudhe and D. S. Laiphrakpam, “Multiple images encryption based on 3D scrambling and hyper-chaotic system,” *Information Sciences*, pp. 1–31, 2021.

A. Banik, Z. Shamsi, and D. S. Laiphrakpam, “An encryption scheme for securing multiple medical images,” *Journal of Information Security and Applications*, vol. 49, article 102398, 2019.

X. Wang and S. Gao, “Application of matrix semi-tensor product in chaotic image encryption,” *Journal of the Franklin Institute*, vol. 356, no. 18, pp. 11638–11667, 2019.

C. L. Li, Z. Y. Li, W. Feng, Y. N. Tong, J. R. Du, and D. Q. Wei, “Dynamical behavior and image encryption application of a memristor-based circuit system,” *AEU - International Journal of Electronics and Communications*, vol. 110, article 152861, 2019.

W. Gao, J. Sun, W. Qiao, and X. Zhang, “Digital image encryption scheme based on generalized Mandelbrot-Julia set,” *Optik*, vol. 185, pp. 917–929, 2019.

H. Liu, A. Kadir, and J. Liu, “Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system,” *Optics and Lasers in Engineering*, vol. 122, pp. 123–133, 2019.

H. Wu, J. Wang, Z. Zhang, X. Chen, and Z. Zhu, “A multi-image encryption with super-lager-capacity based on spherical diffraction and filtering diffusion,” *Applied Sciences*, vol. 10, no. 16, p. 5691, 2020.

L. Ding and Q. Ding, “A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyper-chaos,” *Electronics (Switzerland)*, vol. 9, no. 8, p. 1280, 2020.

W. Hou, S. Li, J. He, and Y. Ma, “A novel image-encryption scheme based on a non-linear cross-coupled hyperchaotic system with the dynamic correlation of plaintext pixels,” *Entropy*, vol. 22, no. 7, pp. 1–21, 2020.

J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, “Image encryption using block cipher and chaotic sequences,” *Signal Processing: Image Communication*, vol. 79, pp. 24–31, 2019.

Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, “Image encryption scheme by combining the hyper-chaotic system with quantum coding,” *Optics and Lasers in Engineering*, vol. 124, article 105836, 2020.

A. Alghaih, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, “An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing,” *Mathematics and Computers in Simulation*, vol. 177, pp. 441–466, 2020.
[82] M. Samiullah, W. Aslam, H. Nazir et al., "An image encryption scheme based on DNA computing and multiple chaotic systems," IEEE Access, vol. 8, pp. 25650–25663, 2020.

[83] W. Xingyuan, Z. Junjian, and C. Guanghui, "An image encryption algorithm based on ZigZag transform and LL compound chaotic system," Optics and Laser Technology, vol. 119, 2019.

[84] L. L. Huang, S. M. Wang, and J. H. Xiang, "A tweak-cube color image encryption scheme jointly manipulated by chaos and hyper-chaos," Applied Sciences (Switzerland), vol. 9, no. 22, p. 4854, 2019.

[85] Y. Khedmati, R. Parvaz, and Y. Behroo, "2D hybrid chaos map for image security transform based on framelet and cellular automata," Information Sciences, vol. 512, pp. 855–879, 2020.

[86] M. Gafsi, M. A. Hajjaji, J. Malek, and A. Mtibaa, "Efficient encryption system for numerical image safe transmission," Journal of Electrical and Computer Engineering, vol. 2020, Article ID 8937676, 12 pages, 2020.

[87] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A new image encryption scheme based on hybrid chaotic maps," Complexity, vol. 2020, 23 pages, 2020.

[88] M. Gafsi, N. Abbassi, M. A. Hajjaji, J. Malek, and A. Mtibaa, "Improved chaos-based cryptosystem for medical image encryption and decryption," Scientific Programming, vol. 2020, 22 pages, 2020.

[89] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," Signal Processing, vol. 167, p. 107280, 2020.

[90] K. K. Butt, G. Li, F. Masood, and S. Khan, "A digital image confidentiality scheme based on pseudo-quantum chaos and Lucas sequence," Entropy, vol. 22, no. 11, pp. 1–20, 2020.