IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 9, 2020, accepted January 21, 2020, date of publication January 31, 2020, date of current version February 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970981

An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems

MUHAMMAD SAMIULLAH[1], WAQAR ASLAM[1], HIRA NAZIR[1], M. IKRAMULLAH LALI[2], BASIT SHAHZAD[3], MUHAMMAD RAFIQ MUFTI[4], AND HUMAIRA AFZAL[5]

[1]Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[2]Department of Computer Science and IT, Division of Science and Technology, University of Education, Lahore 54770, Pakistan
[3]Department of Engineering, Faculty of Engineering and Computer Science, National University of Modern Language, Islamabad 44000, Pakistan
[4]Department of Computer Science, COMSATS University Islamabad–Vehari, Vehari 45550, Pakistan
[5]Department of Computer Science, Bahauddin Zakariya University, Multan 60000, Pakistan

Corresponding author: Waqar Aslam (waqar.aslam@iub.edu.pk)

ABSTRACT A number of techniques for securing plaintext, images and video frames have been developed in cryptography using jointly DNA computing and Chaos Theory. With the advancement of DNA/quantum computing, the threats of security breaches to information have an increasing possibility. In this paper, we propose a symmetric encryption algorithm for color images by extending the current encryption/decryption techniques. Our encryption algorithm is based on three chaotic systems (PWLCM, Lorenz and 4D Lorenz-type), a Secure Hash Algorithm, a scrambler, a chaotic generator and DNA sequence based Linear Feedback Shift Register. We introduce multilevel security to increase the degree of diffusion and confusion. Through experiments, we present security analysis for key irreproducibility and sensitivity, Gray Level Co-occurrence Matrix based analysis, maximum deviation, irregular deviation, entropy, histogram, variance and correlation, number of pixel change rate, unified average cipher intensity, known/chosen-plaintext attacks, mean absolute error, robustness against noises of various types using PSNR and occlusion attacks. It is demonstrated that mostly our proposed encryption algorithm has enhanced performance as compared to contemporary works in information security, while comparable in other cases.

INDEX TERMS Bit scrambling, chaotic generator, DNA sequence based linear feedback shift register, DNA encoding, hypechaos, secure hash algorithm.

I. INTRODUCTION

The significance of information security is increasing with digitization. Cryptography plays a vital role in confidentiality, integrity and availability of information. With growing computability, the digital security stakes are higher than ever. A strong protection is required to tackle data cracking. DNA (Deoxyribo Nucleic Acid) and chaotic system based joint cryptography is an emerging area due to achieving new levels of security, especially that of color images and videos. In order to effectively and efficiently utilize the security as provided by this joint cryptography, its understanding is an emergent and open challenge. This paper undertakes this research case for the security of color images. Their richness of colors renders them as a popular choice for capturing realistic expressions, whether they are natural scenes or artifacts. Security concern of color images is highly desired for ensuring their privacy in various application domains, hence cannot be undermined. To this end, we present an encryption algorithm and analyze its security performance.

Efficiency in the bonding of DNA molecular structure enables parallelism and extra ordinary storage, promising bright future for cryptography. DNA is a hereditary material of living organisms and consists of double strands moving antiparallel to each other. It is a long polymer consisting of small units of nucleotides, with each nucleotide made up of nitrogenous base, 5-carbon sugar and at least one phosphate group. Depending upon the type of nitrogenous base, there are four different nucleotides called adenine (A), cytosine (C), guanine (G) and thymine (T) [1]. Pairs of these bases are connected to each other in specific sequences through hydrogen bonds, thus keeping the two strands connected. A gene is a distinct sequence of nucleotides that contains genetic information of all living organisms.

DNA computing towards information security is promising. Digital DNAs available from public genetic databases

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

have billions of nucleotides, thus enable a huge space with an increased uncertainty. If used effectively by following the DNA sequencing, synthesis, recombination and hybridization operations, it leverages generation of strong cryptographic keys.

DNA based cryptography benefits from techniques such as One Time Pad (OTP), DNA fragmentation and DNA amplification through Polymerase Chain Reaction (PCR) [2]. As it can be generally noted, information randomization is the fundamental process for securing data. Multiple and independent randomization processes applied to data, introduce multiple security barriers. Though cryptography methods are majorly based on randomization, they tend to be application area specific. For instance, plaintext can be encrypted using DNA microdots [3], [4], a technique which is not directly applicable for securing images. Images can be encrypted by processing them in a breadth first pattern. The processing is based on the Chaos Theory and includes scrambling, permutation, shuffling and dynamic diffusion [5], and 3D permutation [6]. Other than breadth first pattern (row-wise), column-wise and diagonal-wise are also possibilities. Cryptography can be done using digital watermarking, canny edge detection and visualization [7]. A plain image can be encrypted by fragmenting it into non-overlapping blocks for adding watermarks that are followed by DNA addition and complementation using a Logistic Map. The Logistic Map generates the DNA matrix and encoding rules for the plain image. DNA addition on a DNA encoded image and DNA matrix gives additive DNA. The information entropy of additive DNA is diffused through Logistic Map, which increases the degree of confusion and diffusion. Visual encryption scheme is demonstrated by transforming a plain image into Visually Meaningful Encrypted Image (VMEI) using a Logistic Map and a Gray S-Box [8]. Other than encrypting images offline, there is a possibility of real time encryption. For instance, in a live communication setup, encryption with a low computation overhead is possible using a chaotic map [9].

A highly secured encryption system can be achieved by combining two chaotic systems and four cryptographic phases, namely, diffusion based on XOR, substitution based on S-boxes, diffusion based on a chaotic map and block permutation for reinforcement of the statistical results [10], [11]. Diffusion in multiple rounds based on bit permutation generator and bit diffusion generator has yielded promising encryption results [12]. These generators rely on SHA-256. In this scheme, an input plain image is divided into small blocks and the blocks having high correlation coefficients are XORed with the threshold values produced by a skew tent map. Finally the entire image is shuffled using two random sequences generated from Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS).

Considering the advancement of DNA/quantum computing, it is increasingly becoming likely to breach highly secured information, whether it is text, image or videos. Security methods based on one or multiple chaotic systems mainly rely on PWLCM (piecewise linear chaotic map) and Lorenz [5], [6], [10], [13]–[17]. Still there is little or no work done using 4D Lorenz-type chaotic systems [18]. Also, though multistage encryption methods are proposed but there is a lack of such method that relies on a real DNA sequence based Linear Feedback Shift Register (DLFSR), which itself is supported by a chaotic generator. We hypothesize that such encryption systems will bring security to another level, especially when multiple security aspects are considered. Our specific research question is

"How to enhance the color image encryption performance using three chaotic systems (PWLCM, Lorenz and 4D Lorenz-type), a Scrambler, a chaotic generator and DLFSR?"

Due to exponential increase in usage of social media, secure transmission of images over public networks is one of the prime concerns that have evolved gravely. The current state of affairs in enhanced computability renders the security measures susceptible to potential security breaches. Thus, the security requirements on sensitive images and video frames of public/private organizations are stringent than ever. To this end, we aim to keep the protection intact as much as practically possible.

Motivated by image encryption schemes and cryptanalysis [19], we contribute by designing and proposing a symmetric image encryption algorithm. It is based on three chaotic systems (PWLCM and Lorenz for permutations, and 4D Lorenz-type for key generation), a Scrambler for image jumbling and DLFSR that is supported by a chaotic generator. It also uses a technique to convert binary data to nucleotides bases and vice versa [20]. The proposed encryption algorithm fulfills the requirements of a strong cipher as reflected by its promising results. The algorithm computes the initial hash using a key space and adds this hash to the three chaotic systems to generate new initial conditions. Using initial conditions, PWLCM and Lorenz chaotic systems iterate on RGB components individually, generating processed RGB components. These RGB components are further processed using three different keys that are generated from a 4D Lorenz-type system for DNA encoding the RGB components. Decoding the RGB components generates a first stage encrypted image, which is post processed using a key for enhanced security. The post processing key depends on two seed values. The first is a DNA seed taken from the NCBI database containing DNA sequences of animals or human genomes. It has also been used for watermarking the DNA sequences [21]. The second is a chaotic seed. Both seeds are fed to DLFSR and a chaotic generator, respectively. DLFSR and the chaotic generator give two keys, which are XORed to get the final key. The final key is XORed with the first stage encrypted image to produce the final encrypted image. Specifically, our contribution is enhanced security performance, as demonstrated by results.

The rest of this paper is organized as follows. Section 2 contains the related work. Section 3 presents our proposed algorithm and necessary details explaining it. Section 4 contains the results when our algorithm is applied on some reference images and corresponding security analysis. Section 5 provides fundamental performance of our

algorithm. Section 6 holds our final judgments and directions for future research.

II. RELATED WORK

For consistency, we introduce our notation to represent all chaotic systems, whether they are referred to or our proposed. Let x_i^n, y_i^n, z_i^n, w_i^n denote an $i^{\text{th.}}$ $(i = 1, 2, 3, \ldots)$ chaotic system with $n^{\text{th.}}$ $(n = 1, 2, 3, \ldots)$ initial condition. $j^{\text{th.}}$ $(j = 1, 2, 3, \ldots)$ coefficient of the i^{th} chaotic system is denoted by $c_{i.j}$.

A. HYPERCHAOS FOR SECURITY

Hyperchaotic systems show more randomness and unpredictability when compared with simple chaotic systems. We use 4D Lorenz-type [18], which is very sensitive to initial conditions used for the key generation,

$$\begin{cases} \dot{x}_1 = c_{1.1}\,(y_1 - x_1) \\ \dot{y}_1 = c_{1.2}x_1 - c_{1.3}y_1 - x_1 z_1 \\ \dot{z}_1 = -c_{1.4}z_1 + x_1 y_1 + w_1 \\ \dot{w}_1 = -c_{1.5}w_1 + c_{1.6}z_1. \end{cases} \tag{1}$$

(1) refers to the first hyperchaotic system in this paper with $c_{1.1}$, $c_{1.2}$, $c_{1.3}$, $c_{1.4}$, $c_{1.5}$, $c_{1.6}$ the system parameters and x_1, y_1, z_1 and w_1 four nonlinear state variables. Notation overdots represent corresponding time derivatives. When $c_{1.1} = -21.7$, $c_{1.2} = 7.3$, $c_{1.3} = 6.6$, $c_{1.4} = -2$, $c_{1.5} = 0.1$, $c_{1.6} = 0.9$ and the initial conditions are $x_1^{(0)} = 1.1625$, $y_1^{(0)} = 0.1392$, $z_1^{(0)} = -0.0003$, $w_1^{(0)} = -28.3942$, the 4D Lorenz-type chaotic system is in the chaotic state [18]. A mathematical model called the Lorenz system has been employed to yield the chaotic response for weather forecasting [22],

$$\begin{cases} \dot{x}_2 = -c_{2.1}x_2 + c_{2.1}y_2 \\ \dot{y}_2 = c_{2.2}x_2 - y_2 - x_2 z_2 \\ \dot{z}_2 = -c_{2.3}z_2 + x_2 y_2. \end{cases} \tag{2}$$

(2) refers to the second hyperchaotic system in this paper. The coefficient in (2), $c_{2.1}$, $c_{2.2}$, $c_{2.3}$ represent the physical characteristics of air flow, while x_2, y_2, z_2 represent amplitude of convective current, temperature difference and temperature deviation respectively. The system goes into a chaotic state for $c_{2.3} > 24$, $c_{2.1} = 10$ and $c_{2.2} = \frac{8}{3}$

Hyperchaotic systems of higher dimensions have received considerable attention for random bit generation, communications and information security due to their significant properties such as unpredictability and sensitivity to initial conditions. Low dimensional chaotic maps have small key spaces leading to low security, while 4D hyperchaotic systems have large key space, producing multiple chaotic sequences with unpredictable behavior, a desired property to achieve high security [23].

A number of chaotic systems have been used in information security for securing gray and color images. These include PWLCM, Chen's, Lorenz, other similar high dimension hyperchaotic systems, chaotic maps and double chaotic systems [5], [6], [10], [13]–[17]. Two chaotic systems (skew tent map and PWLCM) based on decimal quantification have been widely used to improve the performance of image encryption algorithms. Another approach is defining permutations based on cyclic group properties for image encryption instead of a chaotic system [24]–[26]. In a two phases image encryption system, secret key is generated using a novel chaotic map, followed by image cryptography [27].

Recent color image encryption algorithm proposals based on DNA and chaos have comparable results [28], [29]. We deem it important to point out the need of benchmarks for algorithms with source codes along with images and results. Availability of this data publically will support concrete advancement in the field of information security.

B. DNA FOR SECURITY

Due to its immense space of sequences, DNA is well suited for achieving new levels of security in digital world. DNA is made up of four types of nucleotides called Adenin (A), Guanine, Cytosine (C) and Thymine (T). The nucleotides are linked together chemically and are the carrier of inherited traits. DNA exists in double stranded form twisted around each other, i.e., two strands of DNA are hydrogen bonded between complementary nucleotides, while the nucleotides within the strand are linked through phosphate [30]. Complementary nucleotides are AT and GC pairs. DNA rules [31] and DNA-XOR algebraic operation, shown in Table 1, can be used for DNA encoding and decoding. DNA based text and image security is significant though the computational complexity easily explodes with size of the DNA sequence. This issue is addressed by taking a 2-bit coding rule [10]. Diversity based boosting algorithm can be implemented in accurate classifications of DNA nucleotides of some specific length such as ACTTGGCTGT, AACCTCTGGG, etc., [32].

TABLE 1. XORing between DNA symbols [10].

$\oplus$	**A**	**G**	**C**	**T**
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

DNA usage leverages a broad canvas of confusion and diffusion that can effectively enhance the robustness of a security algorithm. Any such approach can follow the DNA encoding rules, especially the dynamic DNA encoding rules combined with chaos [33]. Thus, the serious threats due to the promising DNA computing can be countered by powerful encryption schemes realized by DNA combined with chaotic systems. This is demonstrated by the resistance created against differential attacks due to a game based chaos method of diffusion in which keys based on DNA sequences are generated for image diffusion.

Algebraic-Geometric (AG) codes [34] are still in their infancy stage, offering attractive applications in point to point communication and system security. DNA nucleotides may

be replaced with AG codes to secure wireless communication systems from different attacks detected by different Intrusion Detection Systems (IDS). IDS are used to detect the attacks imposed by sharp attackers [35].

Color images can also be secured by transforming their RGB components to DNA symbols according to DNA rules [36]. Joint usage of real DNA sequences, DNA complementary rules and 1D Logistic Chaos Mapping to compute each pixel value for encryption creates high chaos [37].

C. CHAOTIC GENERATOR AND LINEAR FEEDBACK SHIFTREGISTER / RANDOM BIT GENERATOR

Randomness has a fundamental role in strengthening a security mechanism. Unpredictability in the output of a random bit generator is a fundamental requirement in cryptography. Keeping the output of a random bit generator indeterministic is highly desired even if its design is disclosed somehow. To this advantage, a aperiodic random bit sequence generator (analog chaos circuit) based on a chaotic generator and Linear Feedback Shift Register (LFSR) is proposed [38]. An efficient entropy source exploits Chaos Theory and LFSR to generate random bits [39]. It is estimated that appropriate cryptanalysis can reveal the security weakness of an encryption method [40]. A general recommendation is to design content-aware encryption methods. For instance, encryption of a color image should consider critical factors such as special properties of multimedia, computation load and the concrete application scenario with specified constraints [40].

A combination of chaotic system and multiple DNA rules increases resistance to security attacks [13]. Thus, a multi barrier security approach comprising of a double chaotic system using a Coupled Map Lattice (CML), DNA encryption and optical chaos offers increased security [17]. In contrast to using a CML and optical chaos, we use three chaotic systems, SHA, a chaotic generator and DLFSR. We generate a final post processing key using our proposed random bit generator, DLFSR (based on a real DNA sequence) and a chaotic generator (based on a floating point seed value). Our chaotic generator uses Lorenz chaotic system for key sequence generation. The output of the chaotic generator and DLFSR are XORed to get the final post processing key, *fkey*.

III. PROPOSED ALGORITHM

We propose a symmetric key DNA extended chaotic encryption algorithm, hereafter called SDC-Encryption (SHA DNA Chaotic Encryption) that aims at improving the information security (refers Algorithm SDC-Encryption). DNA is considered a high speed cryptography technique, which is suitable to encrypt large volume of data [41]. SDC-Encryption is applied on plain color image. Its flowchart is shown in Fig. 1.

Algorithm SDC-Encryption

Input: A plain color image ($m \times n$), initial conditions for three chaotic systems (PWLCM, Lorenz and 4D Lorenz-type) and seeds for the chaotic generator and the Shift Register.
Output: An encrypted image ($m \times n$).
// Initial conditions generation
Step 1: Choose the SHA based on the average value of first four pixels of the plain color image and generate new initial conditions (details in Section III A).
// Dual Permutation: Steps 2-8
Step 2: Take transpose of the plain color image (details in Section III B).
Step 3: Generate two fake images (of same size as the plain color image) and split them into their R, G and B components.
Step 4: The found R, G and B components are passed to a PWLCM system for iterations, producing three processed R, G and B components that are concatenated to form a processed image whose pixel values are then sorted.
Step 5: Generate a new image by permuting the pixel values of Step 2 image. Permutation is done by considering the pixel values of Step 4 image as indices into Step 2 image.
Step 6: Step 5 image is split into R, G and B components.
Step 7: Step 6 R, G and B components are passed to a Lorenz chaotic system, producing three R, G and B components whose pixel values are then sorted individually.
Step 8: Generate three new R, G and B components by permuting the R, G and B components of Step 6. Permutation is done by considering Step 7 component pixel values as indices into Step 6 corresponding R, G and B components.
// Scrambling and key generation
Step 9: A Scrambler function maps each of Step 8 components and corresponding keys to new R, G and B components. The corresponding keys are generated using Fourth Order Runge-Kutta method, a hyperchaotic system (details in Section III C).
// DNA encoding
Step 10: The R, G and B components of Step 9 undergo DNA sequence encoding, which is based on DNA encoding rules, DNA complementing and DNA XORing.
// DNA decoding
Step 11: Symbols in the DNA encoded chain of Step 10 undergo DNA sequence decoding. The result is considered as encrypted R, G and B components, which are concatenated to form an encrypted image.
// Final post processing key generation
Step 12: The final post processing key, *fkey*, is generated by XORing the output of the Logistic Map based chaotic generator and DLFSR. The DLFSR is activated by the real DNA sequence. The encrypted image of Step 11 is XORed with *fkey* to get the final encrypted image (details in Section III D).

A. INITIAL CONDITIONS AND CHAOS

SDC-Encryption uses a chaotic system to increase randomness in the encryption image. Let pI denote the plain RGB image ($m \times n$). Initial conditions for the chaos are set as follows. The average of first row, first four pixel values, $p_{i,j}$ $(i = 1, j = 1, 2, 3, 4)$, $AVG = avg\left(p_{i,j}\right)$ determines the hash algorithm for generating the hash digest. For AVG within 0-50, MD5 is chosen, within 51-100, SHA-1 is chosen,

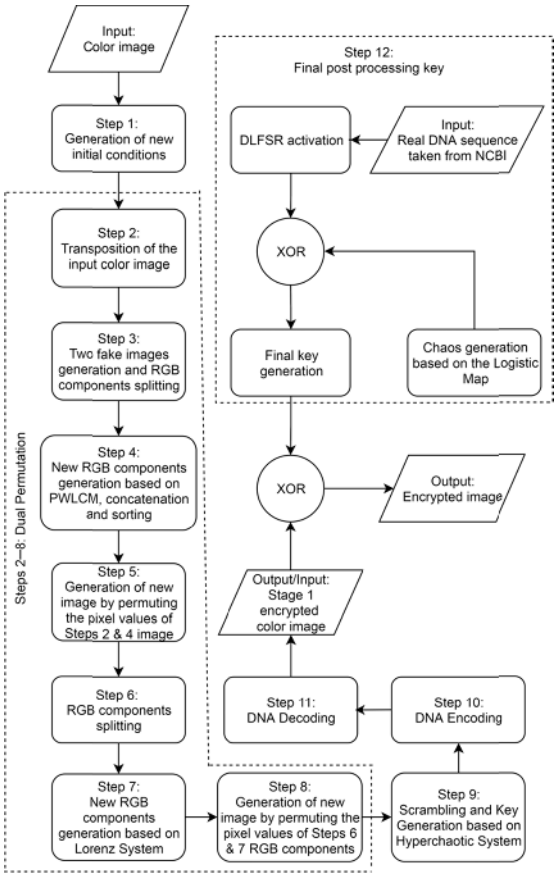


FIGURE 1. The flowchart of SDC-Encryption algorithm.

within 101-150, SHA-256 is chosen, within 151-200, SHA-384 is chosen and above 200, SHA-512 is chosen. The digest is generated regardless of the size of the plain color image. The quotient of the digest, d, is determined as $q = hex2dec(d)/ks$, where the keyspace, $ks = 2^{kl}$ depends on the keylength, kl. Inclusion of q in 4D Lorenz-type (refers (1)) and Lorenz chaotic system (refers (2)) is used for generating the new initial conditions and different from the previous works to ensure secrecy.

Let the seed values for the 4D Lorenz-type, given in (1), be $x_1^{(0)}, y_1^{(0)}, z_1^{(0)}, w_1^{(0)}$ so the new initial conditions are

$$\begin{cases} x_1^{(1)} = x_1^{(0)} + q + gk \\ y_1^{(1)} = y_1^{(0)} + q + gk \\ z_1^{(1)} = z_1^{(0)} + q + gk \\ w_1^{(1)} = w_1^{(0)} + q + gk. \end{cases} \tag{3}$$

Three more seeds for Lorenz chaotic system (refers (2)) are

$$\begin{cases} x_2^{(1)} = x_2^{(0)} + q + gk \\ y_2^{(1)} = y_2^{(0)} + q + gk \\ z_2^{(1)} = z_2^{(0)} + q + gk. \end{cases} \tag{4}$$

New values for PWLCM [42] are computed as

$$\begin{cases} x_3^{(1)} = x_3^{(0)} + q + gk \\ y_3^{(1)} = y_3^{(0)} + q + gk. \end{cases} \tag{5}$$

(5) is the third hyperchaotic system that we considered in this paper. The gk term is the common key generated by adding the initial conditions to the three chaotic systems (PWLCM, Lorenz and 4D Lorenz-type), $gk = (x_1^{(0)} + y_1^{(0)} + z_1^{(0)} + w_1^{(0)} + x_2^{(0)} + y_2^{(0)} + z_2^{(0)} + x_3^{(0)} + y_3^{(0)}) mod 1$.

B. DUAL PERMUTATION

We increase the randomness within the plain color image by shuffling the pixels. Let the transpose of the plain color image pI be pI^T. Now, generate two fake images fI_1 and fI_2 of same size as of pI and split them into their R, G and B components, which are passed to PWLCM system for iterations producing three processed R, G and B components. These are concatenated, resultant image pixel values sorted and used to permute the pixel values of pI^T. Let the permuted image be rI. Permutations are carried out by considering the sorted pixel values as indices into pI^T. rI is split into R, G and B components, which are passed to a Lorenz chaotic system, producing three new R, G and B components. Their pixel values are sorted individually and used as indices into the corresponding R, G and B components of rI to produce permuted R, G and B components, say, uR, uG and uB.

C. DNA ENCODING AND DECODING

DNA encoding and decoding is applied to a space that is generated using a scrambler function, mapping each of uR, uG and uB components and their corresponding keys to new R, G and B components, say uR′, uG′ and uB′ . The keys are mapped by fourth order Runge-Kutta method applied on (1) with $c_{1.6}$ within [0, 9.5] to produce four chaotic sequences, which are combined into a single array.

DNA encoding on uR′, uG′ and uB′ is applied in three stages. One, DNA rule is applied to convert binary digits to DNA Nucleotide symbols (A, C, G, T). The rule is 00→A, 01→C, 10→G, 11→T [31]. Two, the complements of these symbols are taken. Three, DNA symbols and their complements are XORed according to Table 1.

DNA decoding is applied to the XORed output to obtain encrypted R, G and B components, which are concatenated to form first stage encrypted image, denoted by eI'.

D. GENERATING THE FINAL POST PROCESSING KEY

To increase security, the first stage encrypted image is XORed with the final post processing key, $fkey$, to generate the final encrypted image as $eI = fkey \oplus eI'$. $fkey$ is computed using a DNA seed of length 128 and q value determined in Section 3.1. DNA seed is taken randomly from the NCBI database [43]. DNA seed is mapped to a binary seed of length 256 using the same rule as applied for DNA encoding. Binary seed and q value are mapped using DLFSR and the Logistic Map based chaotic generator, respectively, to two keys, called $cfsrk_1$ and $cfsrk_2$ each of size pI. Thus, $fkey = cfsrk_1 \oplus cfsrk_2$ with size equal to pI.

To evaluate the randomness of $fkey$, NIST SP800-22 test suite [44], [45], consisting of 15 tests listed in Table 2,

is performed with significance level $\alpha = 0.01$. Three binary sequences, each of length 10^6 are generated and their minimum p-value is recorded. The binary sequence is considered random whenever p-value is larger than $\alpha = 0.01$, otherwise non-random. Our p-values are cases of good randomness.

TABLE 2. Randomness results of fkey using NIST-800-22 test suite.

NIST parameters	Min p-value	Result
Frequency	0.4128	Passed
Block Frequency	0.0682	Passed
The Run test	0.5631	Passed
Longest run of Ones	0.0720	Passed
Binary Matrix Rank	0.0665	Passed
DFT Spectral	0.0622	Passed
Non Overlapping Template Matching	0.0824	Passed
Maurer's Universal Statistical Test	0.1923	Passed
Linear Complexity	0.0843	Passed
Serial Test	0.3422	Passed
Approximate Entropy	0.1222	Passed
Cummulative Sums	0.2870	Passed
Random Excursions	0.0650	Passed
Random Excursions Variant	0.1423	Passed

Corresponding to SDC-Encryption, we also propose a decryption algorithm, hereafter called SDC-Decryption (SHA DNA Chaotic Decryption), which is applied on an encrypted image to produce a plain color image.

Algorithm SDC-Decryption

Input: An encrypted image ($m \times n$).
Output: A decrypted image ($m \times n$).
Steps: Inverse steps of image encryption are carried out in the reverse order.

IV. RESULTS AND SECURITY ANALYSIS

We applied SDC-Encryption to four color images. A comparison between plain, encrypted and decrypted is shown in Fig. 2. It is clearly noted that the encrypted images completely conceal information contained therein plain color images to keep maximum visual disparity. The decrypted images are almost replicas of the plain color images, reflecting minimal information losses, as also reflected by the peak signal-to-noise ratio (PSNR). PSNR can be defined in terms of mean squared error (MSE) between the plain image ($m \times n$) and the encrypted/decrypted image ($m \times n$) [46]. Denoting a processed (encrypted/decrypted) image by sI, we have

$$psnr(pI, sI) = 10log_{10}\left(\frac{MAX^2}{mse(pI, sI)}\right), \tag{6}$$

where

$$mse(pI, sI) = \frac{\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} [pI(i,j) - sI(i,j)]^2}{m \times n}. \tag{7}$$

MAX is the maximum possible intensity of a pixel in the plain color image pI. (6) assumes $mse(pI, sI) > 0$.

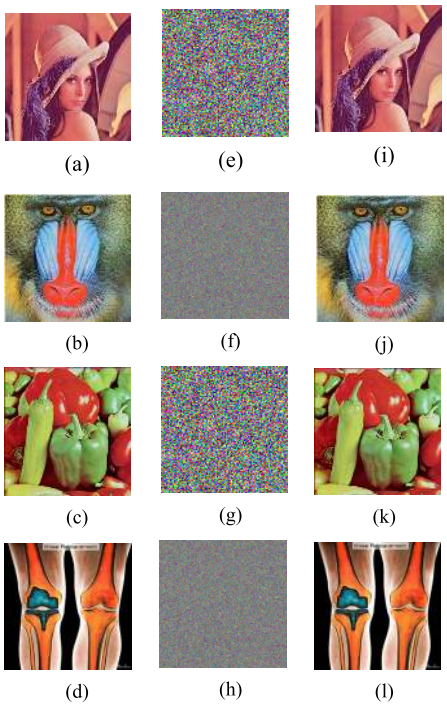


FIGURE 2. SDC-Encryption performance for the color images, Lena (256×256), Baboon (512×512), Peppers (256×256) and Knee (460×555): (a)-(d) the plain images. (e)-(h) the corresponding encrypted-images, and (i)-(l) the corresponding decrypted images.

TABLE 3. The PSNR comparison of SDC-Encryption with the existing works, whenever data is available (shown in parenthesis). Whenever there are improvements due to SDC-Encryption, they are illuminated in bold.

Image	PSNR (plain-encrypted)	PSNR (plain-decrypted)
Lena (512×512)	**8.7048** (8.1293 [47])	∞ (∞ [47])
Baboon (512×512)	**9.0996** (8.7729 [47])	∞ (∞ [47])
Peppers (512×512)	**8.2003** (7.6393 [47])	∞ (∞ [47])
Knee (460×555)	6.5411	∞

The PSNR values for the plain-encrypted and the plain-decrypted images are listed in Table 3.

A. KEY IRREPRODUCIBILITY

Security analysis of SDC-Encryption is presented here. It has been pointed out that an intrusion attack on a DNA based encryption is successful if DNA reference sequence, coding rule for binary digits to DNA Nucleotide symbols and Least Significant Base (LSB) substituted permutations are known [28]. We assess the protection provided by different level barriers of SDC-Encryption.

First level barrier is leveraged by using DNA Nucleotide symbols for generating the post processing key. We evaluate two cases. One, given that the intruder knows of using a 128 DNA symbols key extracted from the NCBI database for encryption, the probability of choosing the correct DNA reference sequence is $\frac{1}{1.63\times10^8}$. There are about 163 million DNA sequences available publically [48]. Let the length of the i^{th} sequence is L_i, then there are $L_i - 128 + 1$ possibilities of generating 128 symbols sequences. Thus the combined

probability is $\frac{1}{1.63\times10^{8}} \times \frac{1}{L_i-128+1}$. Two, given that the intruder knows of using a 128 DNA symbols key not extracted from the NCBI database, the probability of generating the correct DNA reference sequence is $\frac{1}{4^{128}}$. Thus there are almost negligible chances of maliciously generating correct DNA based key.

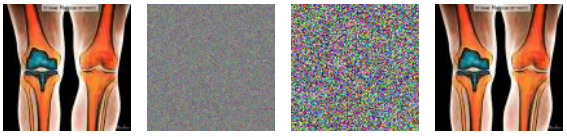
Second level barrier is provided by the chaotic systems and SHA-512/SHA-256. Given that the floating point precision for each input $(x_3^{(0)}, y_3^{(0)})$ to PWLCM is 10^{-12}, for each input $(x_1^{(0)}, y_1^{(0)}, z_1^{(0)}, w_1^{(0)})$ to 4D Lorenz-type is 10^{-10} and for each input $(x_2^{(0)}, y_2^{(0)}, z_2^{(0)})$ to Lorenz is 10^{-10}, total precision is $10^{-94} \cong 2^{-312}$. By including the SHA-512 (2^{512}) to 2^{312} will further increase the key space to 2^{824} which is enough to resist brute-force attacks.

Considering these two basic barriers together, the actual chances of a successful attack are much smaller than the existing minimum chances $\left(\frac{1}{2^{128}}\right)$ of protection [49]. Increasing the forgery resistance up to this level is significant, especially against birthday attacks [50] those may be performed by quantum computers [51]. They can breach cryptographic security systems by finding the likelihood of collisions between random attack attempts at some selected extent of permutations of a hash function.

B. KEY SENSITIVITY

A minor difference in the encryption key results in a significant modification in ciphertext. We tested the sensitivity of secret key of SDC-Encryption by encrypting the plain color image Knee (512×512) with the initial parameters and decrypting it with slight modifications in the initial parameters. The results shown in Fig. 3 clearly indicate absence of a relation between the plain color image and the decrypted image even after the initial conditions are slightly modified. We denote the plaintext by P, the key by $K^1 = k_0^1, k_1^1, ..., k_{MN-1}^1$, $K^2 = k_0^2, k_1^2, ..., k_{MN-1}^2$ and cipher image by $C^1 = c_0^1, c_1^1, ..., c_{MN-1}^1$, $C^2 = c_0^2, c_1^2, ..., c_{MN-1}^2$. Key sensitivity ($kS$), computed using the hamming distance [52] is

$$kS = \frac{1}{MN} \sum_{j=0}^{MN-1} \left(c_j^1 \oplus c_j^2\right), \tag{8}$$



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

FIGURE 3. Key sensitivity test for the color image Knee (460×555): (a) the plain image, (b) the encrypted image, (c) the decrypted image with different initial conditions, (d) the decrypted image with same initial conditions.

where C^1 and C^2 are given by

$$\begin{cases} C^1 = encrypt\left(P, K^1\right), \\ C^2 = encrypt\left(P, K^2\right). \end{cases}$$

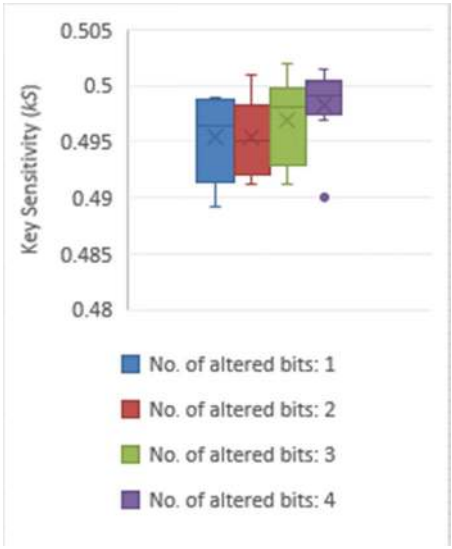


FIGURE 4. The key sensitivity of SDC-Encryption represented by a boxplot.

$kS = 0.5$ indicates a good cipher [52]. K^1 and K^2 have n bits difference. Boxplot in Fig. 4 shows the key sensitivity results for SDC-Encryption. Under this test, Lena (512×512) images are generated for 100 iterations by altering n bits. We can observe that on average 99.1% of kS values lie within $[0.47 - 0.501]$, which is quite close to 0.5, thus reflect that SDC-Encryption is highly sensitive to even minor changes in the key.

C. STATISTICAL ANALYSIS

1) MAXIMUM DEVIATION

It is a statistical parameter representing the deviation among pixel values of a plain image and an encrypted image [53]. It is calculated as

$$M_D = \frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i. \tag{9}$$

Here, d_i represents the difference between the $i^{th.}$ pixel intensity values of the plain color image and the encrypted image. Higher values of M_D represent large deviations in the encrypted image. results of M_D are listed in Table 4.

TABLE 4. The maximum deviation of color images.

Plain Color Image	Maximum Deviation
Lena (256×256)	**131,944** (54,894 [53])
Lena (512×512)	356,122
Peppers (200×200)	47,320
Peppers (512×512)	**79,408** (73,422 [53])
Peppers (512×512)	307368
Baboon (200×200)	68566

2) IRREGULAR DEVIATION

Irregular deviation can be used to assess the encryption quality of a cipher. It can be defined as the extent of closeness

between the histogram deviation distribution and uniform distribution [54]. Its smaller values imply uniform histograms and better ciphers.

$$I_D = \sum_{i=0}^{255} |H_i - M_h| . \tag{10}$$

H_i is the histogram deviation at the $i^{\text{th.}}$ pixel intensity and M_h is the mean value of histogram. Results of i_d are listed in Table 5.

TABLE 5. The irregular deviation of images.

Plain Color Image	Type	Irregular Deviation
Lena (128×128)	Gray	**38,075** (39,858 [54])
Lena (128×128)	Color	62,220 (43,506 [55])
Lena (256×256)	Color	247006
Peppers (256×256)	Color	220918
Panda (256×256)	Color	190008

3) GLCM BASED ANALYSIS

Gray-level co-occurrence matrix (GLCM) is a statistical measure showing different combinations of gray levels found within the image. The statistics such as contrast, energy and homogeneity can be derived from GLCM [55], [56].

a: CONTRAST ANALYSIS

It is a measure of the intensity contrast between a pixel and its neighbours spread over the whole image.

$$CA = \sum_{i=0}^{gt-1} \sum_{j=0}^{gt-1} |i-j|^2 \times G_{i,j}^2, \tag{11}$$

where i, j are the spatial coordinates, $g_{i,j}$ is the glcm of an encrypted image and gt is the gray tone. contrast analysis results are listed in Table 6. large values of contrast represent higher security.

b: ENERGY ANALYSIS

It is a measure of the sum of squared elements in GLCM.

$$EA = \sum_{i=0}^{gt-1} \sum_{j=0}^{gt-1} G_{i,j}^2, \tag{12}$$

where i, j are the spatial coordinateS, $G_{i,j}$ is the GLCM of an encrypted image and gt is the gray tone. Energy analysis results are listed in Table 6. Low values of EA indicate good encryption quality.

c: HOMOGENEITY ANALYSIS

It measures the closeness of the distribution of elements in GLCM.

$$HA = \frac{\sum_{i=0}^{gt-1} \sum_{j=0}^{gt-1} G_{i,j}}{1 + |i-j|}, \tag{13}$$

where i, j are the spatial coordinates, $G_{i,j}$ is GLCM of an encrypted image and gt is the gray tone. Low values of HA reflect better encryption quality. The results of HA are listed in Table 6.

TABLE 6. Results of Contrast, Energy and Homogeneity Analysis of color images.

Plain Color Image	CA	EA	HA
Peppers (128×128)	10.5186	0.0157	0.3893
Peppers (256×256)	10.4934	0.0156	0.3901
Peppers (512×512)	10.5060	0.0156	0.3890
Lena (256×256)	10.5434	0.0156	0.3894
Panda (256×256)	10.5161	0.0156	0.3894
Baboon (200×200)	10.4704	0.0156	0.3898
Average	**10.50798** (10.1098 [55], 10.1145 [9])	**0.015617** (0.165 [55])	**0.3895** (0.4110 [55])

d: HISTOGRAM AND VARIANCE

Histograms for the image Baboon are shown in Fig. 5. Histogram of the encrypted image is quite uniform as compared to the plain color image. Though not enough, but still it provides resistance against statistical attacks. It is pointed out that the variance of histogram and the uniformity of an encrypted image are reciprocal of each other [57]. Low variance gives high uniformity in the histogram of an encrypted image and vice versa. The variances for the images Peppers and Lena (512×512) shown in Table 7 , are lower than [42], which show higher uniformity in the histogram of the encrypted images. Hence SDC-Encryption is effective for the encryption of images.

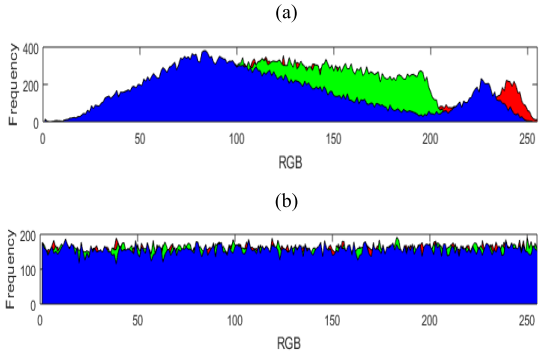


FIGURE 5. The histograms of the image Baboon (512×512): (a) plain, (b) encrypted.

e: CORRELATION

Correlation of an image, plain or encrypted, is measured between the pixels in vertical, horizontal and diagonal directions. Positive correlation exists in plain color images while highly secured image cryptography algorithms have zero or little correlation between the adjacent pixels [15]. Correlations plots for the plain and the encrypted images of Lena

TABLE 7. The variance comparison of SDC-Encryption with the existing works, whenever data is available. This comparison is made only for encrypted images aggregate pixels (last column) due to unavailability of component-wise (RGB) data in the existing works.

Image	Plain Color Image Components			Encrypted Image Components				Encrypted Image Aggregate
	R	G	B	R	G	B	Avg. (R,G,B)	
Lena (256×256)	1,021,300	457,510	1,382,800	1,057.6	1,101.2	1,005.5	1,054.76	1,052 (977.02 [59], 1079.20 [42])
Lena (256×256)	23,453	12,253	32,551	124.6902	138.6980	150.1961	137.8614	137.5020
Panda (256×256)	27,573	36,382	16,350	294.9804	282.9725	268.6039	282.1856	281.4498
Baboon (512×512)	1,976,200	3,204,000	1,160,000	1,087.3	925.9294	1030.8	1,014.67	1,012
Peppers (512×512)	888160 (852750 [15])	**647870** (1273500 [15])	**1698300** (1965700 [15])	**884.3216** (1077 [15])	**1043.3** (1059.6 [15])	**940.9020**, (1061.4 [15])	**956.1745** (1066 [15])	**953.6949** (1064 [15])

TABLE 8. The correlation coefficients comparison of SDC-Encryption with the existing works, whenever data is available. All images are (512×512).

Image	Plain			Encrypted		
	H	V	D	H	V	D
Lena	**0.9445** (0.974662 [25], 0.9778 [15])	**0.9328** (0.985274 [25], 0.9886 [15])	**0.9082** (0.964243 [25], 0.9878 [15])	**-0.0357** (0.000946 [25], 0.0031 [15])	0.00347 (0.000844 [25], 0.0005 [15])	**-0.0007** (0.002741 [25], -0.0041 [15])
Panda	0.9458	0.9458	0.9458	-0.0357	-0.0357	-0.0223
Baboon	0.9458	0.9458	0.9458	-0.0357	-0.0223	-0.0223
Pepper	0.9658 (0.9654 [24])	**0.9458** (0.9552 [24])	0.9458 (0.9243 [24])	**-0.0223** (-0.0012 [24])	**-0.0223** (-0.0213 [24])	**-0.0223** (0.0027 [24])

and Panda are shown in Fig. 6, while Table 8, lists the correlation results of plain and encrypted images along three directions, i.e., vertical, horizontal and diagonal. It is clear that correlation values are very low for encrypted images. We have compared our results to existing works, whenever data is available. Our diagonal correlation values of encrypted images are comparable to the results given in [15], [24], [25]. Therefore, SDC-Encryption resists a statistical attack.

4) DIFFERENTIAL ATTACK ANALYSIS

Number of Pixel Changing Rate (NPCR) and Unified Average Changing Intensity (UACI) are quantitative tests to evaluate the differential attack [10], [47]. In NPCR, a plain image and its variant is produced by varying its pixel values randomly. Both images are encrypted. Say, the encrypted variant is denoted by veI. Now, both eI and veI are compared to identify the rate of change of pixel values between them. Given that an NPCR lies between 0% and 100%, a secure cryptographic algorithm seeks maximal NPCR. For an image $(m \times n)$, NPCR [58] and UACI [58] are

$$npcr\left(eI, veI\right) = \frac{\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} d\left(i,j\right)}{m \times n} \times 100, \quad (14)$$

where $d\left(i,j\right) = \begin{cases} 0 \; if \; eI\left(i,j\right) = veI\left(i,j\right) \\ 1 \; if \; eI\left(i,j\right) \neq veI\left(i,j\right) \end{cases}$,

and

$$uaci\left(eI, veI\right) = \frac{1}{m \times n}\left[\frac{\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} \left|eI\left(i,j\right) - veI\left(i,j\right)\right|}{255}\right]. \quad (15)$$

NPCR and UACI results are listed in Table 9. The average values of NPCR and UACI (single run and multiple runs) of the proposed algorithm, given in Table 9, are better than [14] and are comparable to [10], [28], which clearly shows the resistance against the differential attacks.

5) INFORMATION ENTROPY ANALYSIS

Entropy, a thermodynamic quantity measures the degree of disorder or randomness within the system or encrypted image. A value close to 8 indicates the ideal score of an encrypted image and can be calculated as [60],

$$ent\left(eI\right) = -\sum_{i=0}^{2^k-1} p\left(int\left(el\right)\right) log_2\left(p\left(int\left(el\right)\right)\right), \quad (16)$$

where $ent\left(eI\right)$ and $int\left(el\right)$ are the entropy and intensity value of the encrypted image eI. $p\left(\cdot\right)$ is the probability function and k is the number of gray levels. Table 10, shows the entropy results which are very close to 8, hence the encrypted image has maximal randomness leading to information protection.

TABLE 9. The NPCR and the UACI comparison of SDC-Encryption with the existing works, whenever data is available. All images are (256×256).

Image	NPCR				UACI			
	Min	Max	Avg. (single run)	Avg. (multiple runs)	Min	Max	Avg. (single run)	Avg. (multiple runs)
Lena	99.6214	99.6596	**99.6294** (99.6 [28])	99.6269 (99.6314 [15], 99.6177 [10], 52.8244 [14])	33.3214	33.4252	**33.3514** (33.3 [28])	33.4076 (33.5513 [15], 33.6694 [10], 20.6665 [14])
Panda	99.6231	99.6345	99.6220	-	33.3802	33.4965	33.4518	-
Baboon	99.5964	99.6478	99.6278	-	33.3934	33.4142	33.3956	-
Peppers	99.5676	99.6543	99.6287	-	33.4222	33.4587	33.4316	-

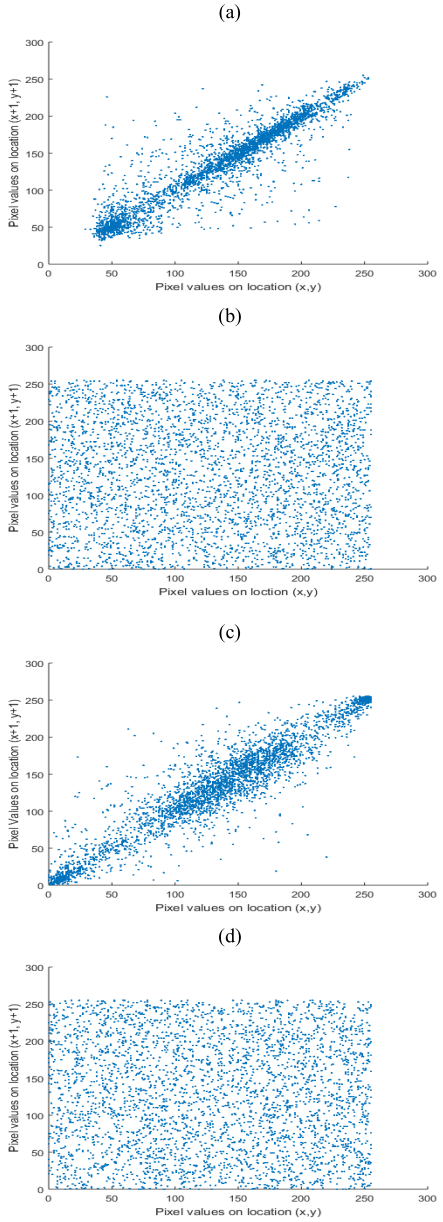


FIGURE 6. The diagonal correlation plots of the images: (a) the plain Lena image (256×256), (b) the encrypted Lena image (256×256), (c) the plain Panda image (256×256), (d) the encrypted Panda image (256×256).

6) KNOWN/CHOSEN-PLAINTEXT ATTACKS (KCPA)

In the known plaintext attack, the attacker uses some pre designed images for encryption and tries to extract some useful information about the plain image. Our proposed algorithm resists this attack as our encrypted image is related to the chosen plain color image. Also the key stream is not directly related to image rather it is indirectly related to it, i.e., through hash algorithm SHA-256/512. For simulation of this attack, we have used all black or white pixel images. The encrypted output in Fig. 7 shows that it will be very difficult for the intruder to extract some useful information about the plain color image.

TABLE 10. The Information Entropy comparison of SDC-Encryption with the existing works, whenever data is available. All images are (512×512).

Image	Entropy Plain (RGB)	Entropy Encrypted (RGB)
Panda	7.8028	7.9989
Lena	**7.7363** (7.4288 [12])	**7.9984** (7.9964 [14], 7.9973 [42], 7.9976 [12])
Peppers	7.7150	7.9984 (7.9992 [14], 7.9974 [42])
Baboon	7.6429	**7.9985** (7.9978 [16])
Splash	7.2428 (7.2428 [60])	7.9997 (7.9998 [60])
Tiffany	**6.7926** (6.4165 [60])	7.9988 (7.9998 [60])

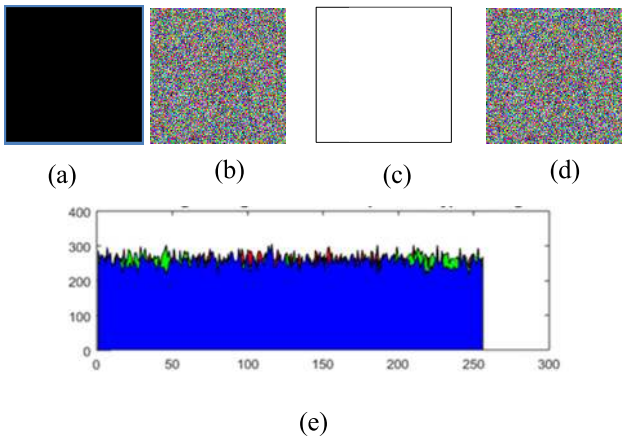


FIGURE 7. Simulation results of the chosen plaintext attacks: (a) all black pixel image (256×256), (b) encrypted of (a), (c) all white pixel image (256×256), (d) encrypted of (c), (e) RGB histogram of (b).

V. FUNDAMENTAL PERFORMANCE ANALYSIS

A. MEAN ABSOLUTE ERROR (MAE)

MAE determines the difference between the plain image ($m \times n$) and the encrypted image ($m \times n$) and computed as

$$mae(pI, eI) = \frac{\sum_{1 \le i \le m,\ 1 \le j \le n} |eI(i,j) - pI(i,j)|}{m \times n}. \quad (17)$$

Larger values of MAE imply more secure and robust cryptosystems. Table 11 lists the MAE values for our proposed algorithm and its comparison with the existing works.

TABLE 11. The Mean Absolute Error (MAE) comparison of SDC-Encryption with the existing works, whenever data is available. All images are (256×256).

Image	MAE		
	R	G	B
Lena	76.8790 (84.2492 [23])	**79.2186** (78.5999 [23])	**82.6461** (70.7826 [23])
All white	127.29997 (127.7523 [23])	**127.64708** (127.2898 [23])	127.62926 (127.7881 [23])
All black	128.1602	127.7749	127.13945
Female4.1.03	**68.87440** (69.1804 [23])	**68.21820** (68.1057 [23])	**68.34314** (68.1736 [23])

It is noted that our results are almost equal to the results of the existing works.

B. ROBUSTNESS AGAINST NOISE AND OCCLUSION ATTACK

Inherently, encryption induces noise. Noise may be defined as an unwanted, random and an undesirable form of energy or signal that pollutes the data. Image noise concerns the variation of color information in the images. We consider three types of noises to check resistivity of SDC-Encryption against them: Salt & Pepper Noise (SPN), Speckle Noise (SN) and Gaussian Noise (GN). SPN is an impulse or spike noise that pollutes image by adding dark pixels in bright regions and vice versa. SN is a commonly detected noise that arises due to the effects of environment on the imaging sensor during acquisition of ultrasound images [61].

Other than quality, resistivity of an encryption algorithm against noise can also be measured by PSNR [46]. Our PSNR (refers (6)) results for all three noise types for the Panda image (256×256) are compared with the existing works in Table 12. In general, high PSNR values imply the reconstructed images contain less noise. Robustness of SDC-Encryption against all three noise types is demonstrated well by high PSNR values.

Two noise cases are selected from Table 12 (SPN (5%) and SN (1%)) to visually highlight the robustness of the proposed algorithm (please see Fig. 8).

An occlusion attack covers an encrypted image partially or completely with some fixed value pixels. Performance against occlusion attack on the encrypted image is tested in three scenarios and shown in Fig. 9. Our results indicate recognizable recovery (decryption) from occlusion attacks of up to 60%.

TABLE 12. The robustness against three noise types comparison of SDC-Encryption with the existing works using PSNR of the Panda image (256×256).

Noise & parameter	PSNR
SPN (0.2%)	**78.0834** (34.4133 [23])
SPN (0.5%)	**69.2037** (29.03 [29])
SPN (5%)	23.7173
SN (1%)	19.4837
GN (0, 0.0001)	22.2021
GN (0, 0.0003)	20.97
GN (0, 0.000001)	**51.4473** (28 [23])

FIGURE 8. Resistivity against noises added to the encrypted Panda image (256×256), (a) SPN density 5%, (b) decrypted image of (a), PSNR=69.2037, (c) SN density 1%, (d) decrypted image of (c), PSNR=19.4837.

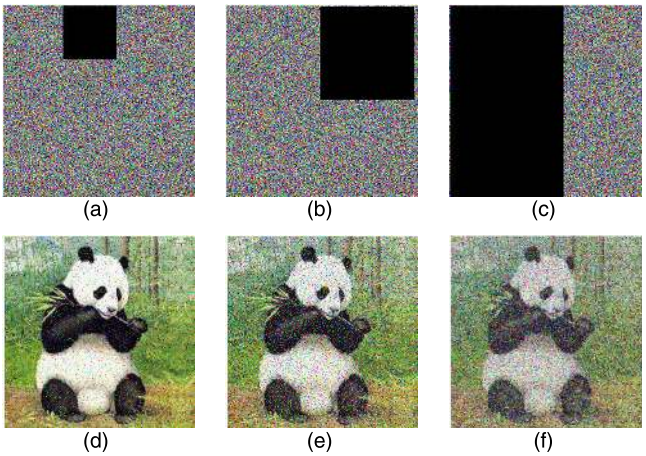


FIGURE 9. Simulation results of occlusion attacks on the Panda image (256×256): (a)-(c) different occlusion attacks, (d)-(f) corresponding recovered images.

C. COMPUTATION COMPLEXITY ANALYSIS

The primary concern of an encryption algorithm is the security it provides; next important performance measure is the computation complexity. We evaluate the computation complexity of SDC-Encryption and compare it with other works (please see Table 13). Our evaluation considers all operations such as XOR, DNA XOR, permutation, generating chaotic sequences (using three chaotic maps), DNA encoding, DNA decoding, decimal binary conversion, creating post processing key. The overall computational complexity

TABLE 13. The computation complexity comparison of SDC-Encryption with the existing works.

Algorithm	Image	Complexity Order (high order terms only)
[52]	Gray	$O(124 \times m \times n)$
[62]	Gray	$O(579 \times m \times n)$
[63]	Gray	$O(108 \times m \times n + 72L^4)$
[64]	Color	$O(9 \times m \times n)$
[47]	Color	$O(69 \times m \times n)$
SDC-Encryption	Color	$O(168 \times m \times n)$

is $O(168 \times m \times n)$. We comment that the chaotic sequences generated in SDC-Encryption (using three chaotic maps, permutations of Step 2 and Step 5, and the generation of the post processing key of Step 12) improves the security but leads to an increased computation complexity.

SDC-Encryption and the selected existing works are implemented on a Laptop (core i3, 4GB RAM, MatlabR2015a installed on Windows 7). SDC-Encryption time performance of our tests is given in Table 14.

TABLE 14. The average encryption time (eT) and the decryption time (dT) comparison of SDC-Encryption. The color images Lena, Baboon, Peppers and Panda each of size (512 × 512) are tested on existing algorithms as well as on SDC-Encryption.

Algorithm	Average ET (sec.)	Average DT (sec.)
[64]	7.2	6.94
[65]	1300.51	1300.69
[66]	85.1965	85.12
[67]	407.9352	408.19
[68]	149.7175	144.5
[69]	43	41.32
[70]	9.41	10.14
SDC-Encryption	22.43	23.12

VI. CONCLUSION

With the advancement of DNA/quantum computing, the existing security mechanisms might not provide the required levels of barriers. There is a dire need to reinforce security mechanisms by introducing newer methods. Our experimental results are promising. We present analysis for key irreproducibility to evaluate the chances of duplicating the secret key as generated by our algorithm, key sensitivity, entropy, histogram, maximum deviation, irregular deviation, GLCM based analysis, variance and correlation, number of pixel change rate and unified average cipher intensity, known/chosen-plaintext attacks, mean absolute error, robustness against noises of various types using PSNR and occlusion attacks. Better results of security analysis, resistance against multiple attacks, larger key space and sensitivity to chaotic secret keys reflect the importance and advantages of proposed scheme. It is demonstrated that mostly our proposed encryption algorithm has enhanced performance as compared to contemporary works in information security, while comparable in other cases. The computation complexity of our algorithm is determined to evaluate its feasibility in various use cases especially that require run time encryption. The proposed algorithm time increases logarithmically for images up to (512×512) and exponentially beyond.

In future we intend to study vulnerability, weaknesses and optimization of computation complexity intensive operations to further improve the proposed approach and to accommodate larger color images greater than or equal to (1024×1024). We also intend to introduce S-box and single or two chaotic maps instead of multiple chaotic maps in the future version of this paper.

REFERENCES

[1] I. Peterson, "Computing with DNA," *Sci. News*, vol. 150, no. 2, p. 26, 2007.

[2] T. Anwar, S. Paul, and S. K. Singh, "Message transmission based on DNA cryptography: Review," *Int. J. Bio-Sci. Bio-Technol.*, vol. 6, no. 5, pp. 215–222, Oct. 2014.

[3] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, Jun. 1999.

[4] M. Rusia and R. H. Makwana, "Review on DNA based encryption algorithm for text and image data," *Int. J. Eng. Res. Technol.*, vol. 3, no. 1, pp. 3182–3186, 2014.

[5] Q. Yin and C. Wang, "Using breadth-first search and dynamic diffusion," *Int. J. Bifurcation Chaos*, vol. 28, no. 4, pp. 1–13, 2018.

[6] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on the 3D permutation model and chaotic system," *Symmetry*, vol. 10, no. 11, p. 660, Nov. 2018.

[7] A. Fatahbeygi and F. A. Tab, "A highly robust and secure image watermarking based on classification and visual cryptography," *J. Inf. Secur. Appl.*, vol. 45, pp. 71–78, Apr. 2019.

[8] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual Meaningful Encryption Scheme Using Intertwinning Logistic Map," in *Intelligent Computing* (Advances in Intelligent Systems and Computing), vol 857, K. Arai, S. Kapoor, and R. Bhatia, Eds. Cham, Switzerland: Springer, 2019.

[9] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[10] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[11] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[12] T. Gopalakrishnan and S. Ramakrishnan, "Chaotic image encryption with hash keying as key generator," *IETE J. Res.*, vol. 63, no. 2, pp. 172–187, Mar. 2017.

[13] P. Zhen, G. Zhao, and L. Min, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, Jun. 2016.

[14] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *J. Electron. Imag.*, vol. 26, no. 1, Feb. 2017, Art. no. 013021.

[15] K. A. K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-D chaotic maps," *J. Inf. Secur. Appl.*, vol. 46, pp. 23–41, Jun. 2019.

[16] M. Annaby, M. Rushdi, and E. Nehary, "Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion," *Opt. Lasers Eng.*, vol. 103, pp. 9–23, Apr. 2018.

[17] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–15, Jun. 2018.

[18] Y. Chen, "The existence of homoclinic orbits in a 4D Lorenz-type hyperchaotic system," *Nonlinear Dyn.*, vol. 87, no. 3, pp. 1445–1452, Feb. 2017.

[19] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102361.
[20] M. Sabry, M. Hashem, and T. Nazmy, "Three reversible data encoding algorithms based on dna and amino acids' structure," *Int. J. Comput. Appl.*, vol. 54, no. 8, pp. 24–30, Sep. 2012.
[21] S. Hamad, A. Elhadad, and A. Khalifa, "DNA watermarking using codon postfix technique," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 15, no. 5, pp. 1605–1610, Sep./Oct. 2018.
[22] A. Anees, "An image encryption scheme based on lorenz system for low profile applications," *3D Res.*, vol. 6, no. 3, p. 24, 2015.
[23] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.
[24] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26191–26217, Oct. 2018.
[25] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, "Image encryption using sequence generated by cyclic group," *J. Inf. Secur. Appl.*, vol. 44, pp. 117–129, Feb. 2019.
[26] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 235–246, Feb. 2016.
[27] J. A. Alzubi, O. A. Alzubi, G. Suseendran, and D. Akila, "+ A novel chaotic map encryption methodology for image cryptography and secret communication with steganography," *Int. J. Recent Technol. Eng.*, vol. 8, no. 1C2, May, pp. 1122–1128, 2019.
[28] M. Sokouti and B. Sokouti, "A PRISMA-compliant systematic review and analysis on color image encryption using DNA properties," *Comput. Sci. Rev.*, vol. 29, pp. 14–20, Aug. 2018.
[29] F. Peng, X.-w. Zhu, and M. Long, "An ROI privacy protection scheme for H.264 video based on FMO and chaos," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 10, pp. 1688–1699, Oct. 2013.
[30] L. Sharp, "DNA sequencing and sorting: Identifying genetic variations," COMAP, Bedford, MA, USA, Tech. Rep., 2015.
[31] S. Hamad, "A novel implementation of an extended 8×8 playfair cipher using interweaving on DNA-encoded data," *Int. J. Elect. Comput. Eng.*, vol. 4, no. 1, pp. 93–100, 2014.
[32] J. A. Alzubi, "Diversity-based boosting algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 5, pp. 524–529, 2016.
[33] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019.
[34] O. A. Alzubi, T. M. Chen, J. A. Alzubi, H. Rashaideh, and N. Al-Najdawi, "Secure channel coding schemes based on algebraic-geometric codes over hermitian curves," *J. Univ. Comput. Sci.*, vol. 22, no. 4, pp. 552–566, 2016.
[35] C. Thomas, B. Jorge, A. Jafar, and A. Omar, "Intrusion detection," *IET Publishibg*, vol. 1, no. 1, pp. 1–9, 2014.
[36] M. Suryadi, Y. Satria, and M. Fauzi, "Implementation of digital image encryption algorithm using logistic function and DNA encoding," *J. Phys., Conf. Ser.*, vol. 974, Mar. 2018, Art. no. 012028.
[37] T. T. Zhang, S. J. Yan, C. Y. Gu, L. Ren, and K. X. Liao, "Research on image encryption based on dna sequence and chaos theory," in *Proc. 2nd Int. Conf. Mach. Vis. Inf. Technol. (CMVIT)*, vol. 1004, 2018, pp. 149–154.
[38] A. Tsuneda and K. Morikawa, "A study on random bit sequences with prescribed auto-correlations by post-processing using linear feedback shift registers," in *Proc. Eur. Conf. Circuit Theory Design (ECCTD)*, Sep. 2013, pp. 1–4.
[39] M. Bucci and R. Luzzi, "A fully-digital chaos-based random bit generator," in *The New Codebreakers* (Lecture Notes in Computer Science), vol. 9100. Berlin, Germany: Springer, 2016, pp. 396–414.
[40] C. Li, D. Lin, B. Feng, J. Lu, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.
[41] S. R. Maniyath and T. Kaiselvan, "A novel DNA based encryption algorithm for multimedia information," *Compusoft*, vol. 5, no. 1, p. 2036, 2016.
[42] X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," *Optik-Int. J. Light Electron Opt.*, vol. 153, pp. 117–134, Jan. 2018.
[43] *Human Genome Resources at NCBI*. Accessed: Mar. 12, 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/projects/genome/guide/human/index.shtml
[44] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22 Rev 1a, 2010.
[45] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.
[46] S. N. Lagmiri, J. Elalami, N. Sbiti, and M. Amghar, "Hyperchaos for improving the security of medical data," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 1049–1055, Jul. 2018.
[47] X. Wu, J. Kurths, and H. Kan, "A robust and lossless DNA encryption scheme for color images," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 12349–12376, May 2018.
[48] P. Malathi, M. Manoaj, R. Manoj, V. Raghavan, and R. E. Vinodhini, "Highly improved DNA based steganography," *Procedia Comput. Sci.*, vol. 115, pp. 651–659, Jun. 2017.
[49] S. Babbage *et al.*, "ECRYPT II yearly report on algorithms and keysizes," Eur. Netw. Excellence Cryptol. II, Katholieke Univ. Leuven, Leuven, Belgium, Tech. Rep. ICT-2007-216676, Sep. 2012. [Online]. Available: http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[50] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Process.*, vol. 11, no. 5, pp. 324–332, Apr. 2017.
[51] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," in *LATIN'98: Theoretical Informatics* (Lecture Notes in Computer Science), vol. 1380, C. L. Lucchesi and A. V. Moura, Eds. Berlin, Germany: Springer, 1998, pp. 163–169.
[52] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.
[53] N. Ahmed, H. Muhammad, S. Asif, and G. Saleem, "A benchmark for performance evaluation and security assessment of image encryption schemes," *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, pp. 18–29, Dec. 2016.
[54] J. S. Khan, J. Ahmad, and M. A. Khan, "TD-ERCS map-based confusion and diffusion of autocorrelated data," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 93–107, Jan. 2017.
[55] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, Nov. 2017.
[56] P. Mohanaiah, P. Sathyanarayana, and L. Gurukumar, "Approach," *Int. J. Sci. Res. Publications*, vol. 3, no. 5, pp. 1–5, 2013.
[57] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.
[58] 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.
[59] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[60] K. A. K. Patro and B. Acharya, "Secure multi–level permutation operation based multiple colour image encryption," *J. Inf. Secur. Appl.*, vol. 40, pp. 111–133, Jun. 2018.
[61] R. Dass, "Speckle noise reduction of ultrasound images using BFO cascaded with wiener filter and discrete wavelet transform in homomorphic region," *Procedia Comput. Sci.*, vol. 132, pp. 1543–1551, Jan. 2018.
[62] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201714.
[63] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.
[64] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *Int. J. Bifurcation Chaos*, vol. 29, no. 09, Aug. 2019, Art. no. 1950115.
[65] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.
[66] X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme," *Opt. Lasers Eng.*, vol. 102, pp. 106–111, Mar. 2018.

[67] S. Suri and R. Vijay, "An AES–CHAOS-based hybrid approach to encrypt multiple images," in *Recent Developments in Intelligent Computing, Communication and Devices* (Advances in Intelligent Systems and Computing), vol. 555, S. Patnaik and F. Popentiu-Vladicescu, Eds. Singapore: Springer, 2017.
[68] S. Das, S. Mandal, and N. Ghoshal, "Multiple-image encryption using genetic algorithm," in *Intelligent Computing and Applications* (Advances in Intelligent Systems and Computing), vol 343, D. Mandal, R. Kar, S. Das, and B. Panigrahi, Eds. New Delhi, India: Springer, 2015.
[69] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, Mar. 2019.
[70] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

MUHAMMAD SAMIULLAH received the B.S., M.B.A., and M.S. degrees in computer science from The Islamia University of Bahawalpur, Pakistan, where he is currently pursuing the Ph.D. degree in computer science. He is also an Instructor with the Govt. Sadiq College of Commerce, Bahawalpur, Pakistan. His research interests include wireless network virtualization, radio resource allocation, interference management for cellular systems, and applications of DNA computing in information security.

WAQAR ASLAM received the M.Sc. degree in computer science from Quaid-i-Azam University, Islamabad, Pakistan, and the Ph.D. degree in computer science from the Eindhoven University of Technology, The Netherlands. During his Ph.D. degree, he received the Overseas Scholarship, HEC, Pakistan. He is currently an Assistant Professor with the Computer Science & IT, The Islamia University of Bahawalpur, Pakistan. His research interests include performance modeling & QoS of wireless/computer networks, performance modeling of (distributed) software architectures, radio resource allocation, the Internet of Things, effort/time/cost estimation of software development in (distributed) Agile setups, social network data analysis, and DNA/Chaos-based information security.

HIRA NAZIR received the B.S. degree in information technology and the M.S. degree in software engineering from The Islamia University of Bahawalpur, Pakistan, where she is currently pursuing the Ph.D. degree in computer science. She is also an Assistant Professor with the University of Central Punjab–Bahawalpur, Pakistan. Her research interests include wireless networks, interference management for cellular systems, and applications of DNA computing in information security.

M. IKRAMULLAH LALI received the master's degree in software engineering and the Ph.D. degree in computer science from COMSATS University, Islamabad, Pakistan. He was a Research Fellow with the University of Groningen, The Netherlands, for two years during his Ph.D. degree under the RuG Fellowship. He was with the Ministry of Information Technology, the University of Education, and the University of Sargodha, Pakistan, for several years. He is currently a Professor with the Department of Information Technology, University of Education, Lahore, Pakistan. He is collaborating with different research groups at national and international levels. He has authored more than 60 research articles, which have been published in conferences and reputed journals. His current research interests include machine learning, social network data analysis, formal methods, and computer vision. He is a reviewer of many high-impact-factor journals and reputed conferences.

BASIT SHAHZAD received the Ph.D. degree from University Technology Petronas, Malaysia. He was with King Saud University, Riyadh. He was an Assistant Professor with the COMSATS Institute of Information Technology, Islamabad. He is currently an Assistant Professor with the Faculty of Engineering and Computer Science, National University of Modern Languages, Islamabad. He has numerous publications in journals and conferences of international repute and has a very active research profile. He has an Editorial Role in several conferences and journals of high repute and has edited a number of special issues in significant journals in the areas of software engineering, social networks, and mobile healthcare. His current research interests include information systems (enterprise architecture, software cost, and risk modeling) and advancements in research methodologies (quantitative, qualitative, and mixed method), mobile healthcare, and social networks.

MUHAMMAD RAFIQ MUFTI received the M.Sc. degree in computer science from Bahauddin Zakariya University, Multan, Pakistan, in 1994, the M.Sc. degree in computer engineering from the Centre for Advanced Studies in Engineering (CASE), Islamabad, in 2007, and the Ph.D. degree in electronic engineering from Mohammad Ali Jinnah University (MAJU), Islamabad, in 2012. He is currently a Faculty Member of COMSATS University Islamabad–Vehari, Pakistan. His research interests include sliding mode control, fractional control, neural networks, cognitive radio networks, and network security.

HUMAIRA AFZAL received the M.Sc. degree in computer science from Bahauddin Zakariya University, Multan, Pakistan, in 1997, the M.Sc. degree in computer engineering from the Centre for Advanced Studies in Engineering (CASE) Islamabad, in 2010, and the PhD. degree in computer science from the School of Electrical Engineering and Computer Science, University of Bradford, U.K., in August 2014. She is currently an Assistant Professor of computer science with Bahauddin Zakariya University, Multan, Pakistan. Her research interests include MAC protocol design for cognitive radio networks, performance modeling, queuing theory, network security, and sliding mode control.