IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

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

Digital Object Identifier 10.1109/ACCESS.2017.DOI

DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption

JAN SHER KHAN[1], WADII BOULILA[2,3] (Senior Member, IEEE), JAWAD AHMAD[4] (Senior Member, IEEE), SAEED RUBAIEE[5], ATIQUE UR REHMAN[6], ROOBAEA ALROOBAEA[7] , AND WILLIAM J. BUCHANAN[4]

[1]Department of Electrical and Electronics Engineering, University of Gaziantep, 27310 Gaziantep, Turkey
[2]RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia
[3]College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[4]School of Computing, Edinburgh Napier University, United Kingdom
[5]Department of Industrial and Systems Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia
[6]Department of Electrical Engineering, HITEC University Taxila, Pakistan
[7]College of Computers and Information Technology, Taif University, Saudi Arabia

Corresponding author: Jan Sher Khan (e-mail: J.S.Khan@ieee.org).

ABSTRACT Visual selective image encryption can both improve the efficiency of the image encryption algorithm and reduce the frequency and severity of attacks against data. In this article, a new form of encryption is proposed based on keys derived from Deoxyribonucleic Acid (DNA) and plaintext image. The proposed scheme results in chaotic visual selective encryption of image data. In order to make and ensure that this new scheme is robust and secure against various kinds of attacks, the initial conditions of the chaotic maps utilized are generated from a random DNA sequence as well as plaintext image via an SHA-512 hash function. To increase the key space, three different single dimension chaotic maps are used. In the proposed scheme, these maps introduce diffusion in a plain image by selecting a block that have greater correlation and then it is bitwise XORed with the random matrix. The other two chaotic maps break the correlation among adjacent pixels via confusion (row and column shuffling). Once the ciphertext image has been divided into the respective units of Most Significant Bits (MSBs) and Least Significant Bit (LSBs), the host image is passed through lifting wavelet transformation, which replaces the low-frequency blocks of the host image (i.e., HL and HH) with the aforementioned MSBs and LSBs of ciphertext. This produces a final visual selective encrypted image and all security measures proves the robustness of the proposed scheme.

INDEX TERMS Security, Deoxyribonucleic Acid (DNA), Diffusion, Confusion, Encryption, Chaos.

I. INTRODUCTION

NOWADAYS , digital networking has modified most common means of communication. Any user can send and receive information through the network easily, but this also creates a great threat for eavesdroppers to breach the security of confidential information. One of the most effective means of overcoming this privacy issue is to encrypt confidential data, thus protecting it from eavesdropping users who lack authorized access. The process of converting data into coded forms is known as encryption. With encryption, coded information about any type f data - from plaintext to images - can only be decrypted by the intended receiver, who possesses the key needed to translate, or decrypt the cipher data [1]. However, traditional encryption algorithms developed in last two decades may not be well-suited for certain types of data, such as digital image formats, because of bulk data, real-time constraints and unknown environment.

In 1989, Matthews was the first to design an encryption scheme utilizing chaos [2]. Factors such as pseudo-randomness, unpredictability, sensitivity (both to initial conditions and to added control parameters), and an element of ergodic uncertainty combine to make chaos a more secure and convenient means of encrypting large-scaled data sets. Following Matthews, a number of researcher have also utilized chaos to proposed different secure image encryption schemes. For instance, Xu et al. developed and tested a new cryptosystem derived from Piece Wise Linear Chaotic Maps (PWLCM) [3]. In this system, two different binary sequences of plain image are diffused mutually followed by binary elements swapping. Khan et al. utilized a Henon map and, a Skewtent map combined with S-Box to develop a secure

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

image encryption scheme via confusion-diffusion encryption structure [4]. The authors in [5], designed dynamic S-Boxes based image encryption scheme using multiple chaotic maps. Zhu et al. designed a chaos-based S-boxes to enhance the security of an image encryption scheme [6]. Double S-box concept is utilized to make the scheme secure against four classical attacks. Thus, this scheme has an advantage over other S-box based image encryption scheme. Authors in [7], transform chaotic sequences produced by the quadratic polynomial chaotic map into a new random sequence via an arc sine function. To validate the application of the new generated random numbers, they applied it in a new image encryption scheme. Authors in [8], used a chosen-plaintext attack to break the newly designed colour image encryption scheme and decipher the cipher image. Then logistic tent map is utilized to improve the same algorithm. To resist the chosen-plaintext, the key parameters are computed by the plaintext image through the SHA-3 hash function. Mehmet et al. performed a side-channel analysis of two chaos-based S-boxes and compared the results with AES S-box [9]. The results demonstrate that chaos-based-boxes are highly resistant to side-channel attacks. Firat et al. improved the performance of chaos-based S-boxes via designing a post-processing scheme [10]. The zigzag transformation method is utilized to enhance the performance of the designed S-box. The authors in [11], used Ikeda chaotic map, Henon map an S-box to designed dynamic S-box based image encryption scheme. The image is first shuffled row-and column-wise and then bitwise XORed with a random matrix. Then, through Henon, a random S-Box is selected and the image pixel is substituted randomly. Belazi et al. first transformed the plaintext image into frequency domain via wavelet transform and then just encrypt the critical part of information to design chaos based partial image encryption algorithm [12]. In literature [13]–[19], many schemes convert a plain image to a random like noise. Even such images (random like images), though, can still alert eavesdroppers that the encrypted or ciphertext image may contain important information. To address this issue and divert eavesdropper attention, Long et al. transformed the original plaintext image into an encrypted image with covert visual meanings [20]. Hua et al. later combined chaotic maps and Chinese Remainder Theorem (CRT), to present a secret image sharing scheme [21]. The authors in [22], designed visually secure cryptosystem based on compressive sensing. The authors in [23], use the Least Significant Bits (LSB) embedding and compressive sensing (CS) to designed visually image compression and encryption scheme. Zigzag confusion and CS is applied to the original image followed by dynamic LSB embedding, to hide the encrypted and compressed image in a host image. This final embedded image is the visually meaningful encrypted image. Similarly, the authors in [24], produce visually secure encrypted images using 2-D CS, chaotic systems and multi-embedding strategy. The measurement matrices are computed via compressing the three layers. Then these compressed layers are bit-wise and pixel-wise shuffled and diffused to generated compressed cipher image. Finally, the compressed cipher image is embedded in the carrier image to get visually secured compressed cipher image. The parameters for zigzag confusion were computed by passing the plaintext image through SHA-256 hash function. Ghebleh et al. also enhanced the general security and overall performance of a pre-existing scheme for image encryption by designing a lossy image encryption using large primes [25]. The authors in [26], tried to avoid attackers attention by designing visually-secure images based on an intertwining logistic map.

Due to its intrinsic characteristics, DNA computing has been used extensively in the field of cryptography. These intrinsic characteristics are huge parallelism, elevated level computational ability and capability of storing huge amount of data. To encode the plaintext data in DNA computing scenarios, researchers use existing biological information from DNA public databases. In 1999 [27], Clelland et al. proposed a novel scheme where secret messages are concealed with human genomic DNA. Xiuli et al. utilize DNA sequence operations and chaotic maps to develop what was then a new type of encryption scheme [28]. After encoding the plaintext image into a DNA matrix, row- and column-wise circular permutation was applied to the matrix. Yueping et al. proposed an algorithm that was mainly based on high-dimensional chaotic system for image encryption [29]. The scheme designed by Yueping et al. was found to withstands numerous forms of attack (including chosen-ciphertext and chosen-plaintext attacks) quickly and efficiently. Others [30] have likewise, presented DNA and chaos-based encryption scheme that are secure but lightweight. In one such method, the plaintext image is first confused via random number generated from cross coupled chaotic logistic map and then encrypted via DNA computation. Chen et al. also proposed a secure, and efficient image encryption scheme, this one derived from self-adaptive permutation-diffusion and random DNA encoding. This scheme was found significantly more efficient due to its promotion of re-usable random variables [31].

The remainder of our paper is presented as follows. The concept of chaotic maps is defined and analyzed in section II, while proposed DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption scheme is demonstrated in section III. The attributes and strengths of the proposed scheme form the focus of section IV, and finally, section V illustrates the conclusion of the proposed work.

II. PRELIMINARIES

Three different chaotic maps are utilized in the proposed encryption scheme. These three maps are explained in detail below, and Fig. 1, demonstrates their sensitivity to a slight change in initial conditions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

A. LOGISTIC CHAOTIC MAP

Due to sample nature and easy implementation, the logistic chaotic map is the non-linear system most often studied and applied in literature when researchers design new algorithms for secure image encryption. Mathematically, a logistic chaotic map may be computed as follows [32]:

$$X(i+1) = \gamma \times X(i) \times (1 - X(i)) \tag{1}$$

the variable $Xi \in (0, 1)$ denotes the system. The control parameters γ value must be in the range $3.57 < \gamma \leq 4$ to generate either random numbers or completely chaotic behaviors [32]. In addition, the initial condition X_0 and the control parameter γ can be regarded as cipher keys in the case of image encryption schemes.

B. GAUSSIAN MAP

A Gaussian map is a non linear chaotic map based on Gaussian functions. This type of map may also be called a "mouse map," due to the mouse-like shape of bifurcation diagram. Mathematically, a Gaussian map can be computed as follows [33]–[35]:

$$Y(n+1) = e^{-aY_n^2} + b \tag{2}$$

here a and b denote different control parameters. To generate random numbers, we set the value of $a = 4.93$ and the value of $b = -0.58$. Similar to the logistic chaotic map, the control parameters and initial condition here will act as cipher keys in case of image encryption schemes.

C. CHEBYSHEV CHAOTIC MAP

Let $z \in R$ and n be an integer, then a Chebyshev polynomial A_n of degree n can be defined as [36]:

$$A_n(z) = 2zA_{n-1}(z) - A_{n-2}(z) \tag{3}$$

when $n > 1$, the above polynomial will behave as a chaotic map. With $A_0 = 1$ and $A_1 = z$, the first few Chebyshev polynomials are:

$$A_2(z) = 2z^2 - 1 \tag{4}$$

$$A_3(z) = 4z^3 - 3z \tag{5}$$

$$A_4(z) = 8z^4 - 8z^2 + 1 \tag{6}$$

One property of Chebyshev polynomials is that they act as semi-group, which makes this particular type of chaotic map even more secure. The Chebyshev map behaves like a logistic map in case of n=2.

III. OUR PROPOSED SCHEME

Figure 2 illustrates the block diagram of the scheme that we are proposing, a visually-selective image encryption scheme. We begin with a plaintext image of an adult woman (hereafter, "Lena") measuring 128 pixels $\times$128 pixels and a host image of a baboon (hereafter, "Baboon" or "H") measuring 256 pixels $\times$256 pixels. In dimensional terms, the plaintext image "Lena" is four time smaller than the host image "Baboon". A more detailed description of tour proposed image encryption scheme will be presented below:

Step 1: Initial conditions i.e., X_0 and Y_0 regarding logistic and Gaussian maps have been generated by passing a random DNA sequence through SHA-512. The initial condition Z_0 for Chebyshev map is computed via passing plaintext image through SHA-512. The SHA-512 will produce 512 distinct bits (128 characters) hash value.

$$\begin{aligned} &Hash\_value_1 = SHA\_512(DNA\_sequence),\\ &Hash\_value_2 = SHA\_512(Plaintext\_image),\\ &X_0 = \frac{Hash\_value_1(1:64)}{2^{255}},\\ &Y_0 = \frac{Hash\_value_1(65:128)}{2^{257}},\\ &Z_0 = \frac{Hash\_value_2(1:128)}{2^{513}}. \end{aligned} \tag{7}$$

Step 2: Random indices X_i, Y_i and Z_i are acquired by reiterating each of these chaotic maps $M \times N$ times using the initial conditions X_0, Y_0 and Z_0, respectively. Mod 255 is then applied to store all random numbers between 0 and 255.

$$X, Y, Z = mod(floor((X, Y, Z) * 10^{14}), 255) \tag{8}$$

Step 3: The original plaintext image (hereafter P) is then altered and permuted in rows utilizing random numbers vector X_i. The row-permuted image is then stored in R_P.

Step 4: To acquire the final permuted image, the row-permuted image R_P is shuffled column-wise using random numbers vector Y_i. The column-permuted image is stored in C_P.

Step 5: 256 random numbers are selected from Z_i and arranged in 16 pixels $\times$16 pixels random matrix R_{Matrix}.

Step 6: The permuted image C_P is breakdown into n blocks of 16 pixels $\times$16 pixels. The correlation coefficient of each block is computed. The bitwise XORed operation is carried out between a random matrix R_{Matrix} and blocks whose correlation coefficient values are greater than 0.3. All the blocks are combined together to obtain the final diffused image D_P.

Step 7: The decimal pixel values of diffused image D_P are converted into binary values. Most Significant Bits (MSBs) and Least Significant Bits (LSBs) matrices i.e., $MSBs_{Matrix}$ and $LSBs_{Matrix}$ are generated after separating the binary values.

Step 8: A lifting wavelet transformation is then applied to the host image ("H") to obtain LL, LH, HL and HH blocks.

$$[LL \quad LH \quad HL \quad HH] = lwt2(H,' db1'). \tag{9}$$

Step 9: The HL and HH blocks from H are next replaced with $MSBs_{Matrix}$ and $LSBs_{Matrix}$, respectively. To obtain the final visual selective encrypted image V_{Enc}, an inverse lifting wavelet transform is applied on

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

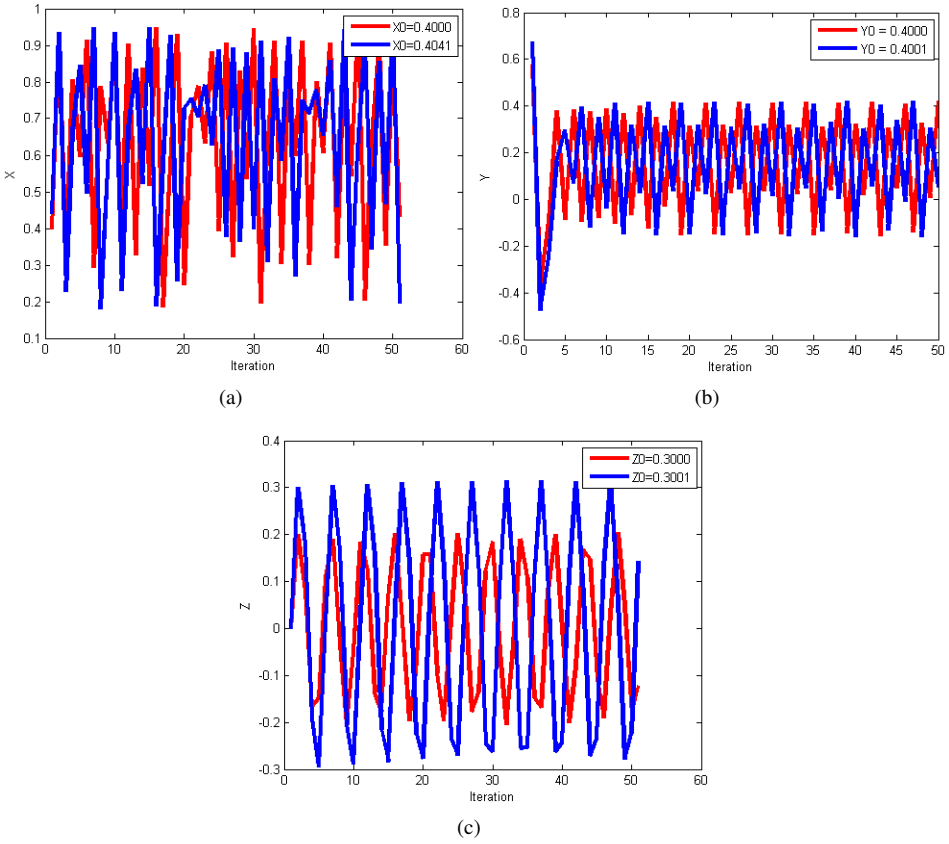

FIGURE 1. Different random number generation plots for a slight change in initial conditions: (a) a logistic map, (b) a Gaussian map, and (c) a Chebyshev map.

$LL, LH, MSBs_{Matrix}$ and $LSBs_{Matrix}$.

$$V_{Enc} = ilwt2(LL, LH, MSBs_{Matrix}, LSBs_{Matrix}, 'db1'). \quad (10)$$

We can retrieve the original plaintext image by starting from step 9 and going toward step 1 in reverse order.

IV. SECURITY ANALYSIS

In this section, the security-focused analysis of proposed new scheme and our results are all detailed. Results are analyzed using plaintext images ("Lena" and "Cameraman") measuring 128 pixels $\times$128 pixels. The encryption results are demonstrated in Fig. 3 (b,n), in which it is demonstrated that all ciphertext images run through the proposed cryptosystem conceal all information from the original plaintext images. Any random/noise-like ciphertext image alerts eavesdropper that the encrypted/ciphertext images may contain important information, even if they cannot extract that information yet. To address this issue and divert eavesdropper attention, the ciphertext images we work with are further embedded in host images to produce a visual encrypted image. From Fig. 3 (c,o) and (d,p), it is clear that after embedding the ciphertext images in host images, the changes in host images are not noticeable. Once these images have been generated, we subjected them to various attacks commonly utilized against encrypted data, including statistical attack, brute force attack, noise attacks, and data loss attacks. We also performed key sensitivity analysis and analyzed the results generated by all of these items. The checklist provided in [37] has been kept in mind while analysing the security of the proposed scheme. The results we obtained confirmed the security, robustness, and efficiency of this encryption scheme, as detailed below.

A. ANALYSIS OF STATISTICAL ATTACK

Statistical attack analysis can be done via histogram and correlation coefficient tests. The histogram test demonstrates the distribution of pixels at various intensity levels. Therefore, as Fig. 3 (h,t) demonstrates the histograms generated by ciphertext images tend to be distributed uniformly. Figure 3 (i,u) and (j,v) also reveals how the histogram of visually encrypted images are very similar to their corresponding host images. Similarly, one can also quantitatively confirms the distribution characteristics of a histogram via computing variance of the histogram. Mathematically, it can be computed as [38]:

$$Var(X) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{1}{2} \times (x_i - x_j)^2 \quad (11)$$

where $X = \{x_0, x_1, x_2, \ldots, x_{N-1}\}$ is a vector and x_i and x_j are gray values pixels numbers. For an 8-bit gray level image, $N = 256$, which basically represents the numbers of gray levels in an image. The variance of histogram is computed for

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

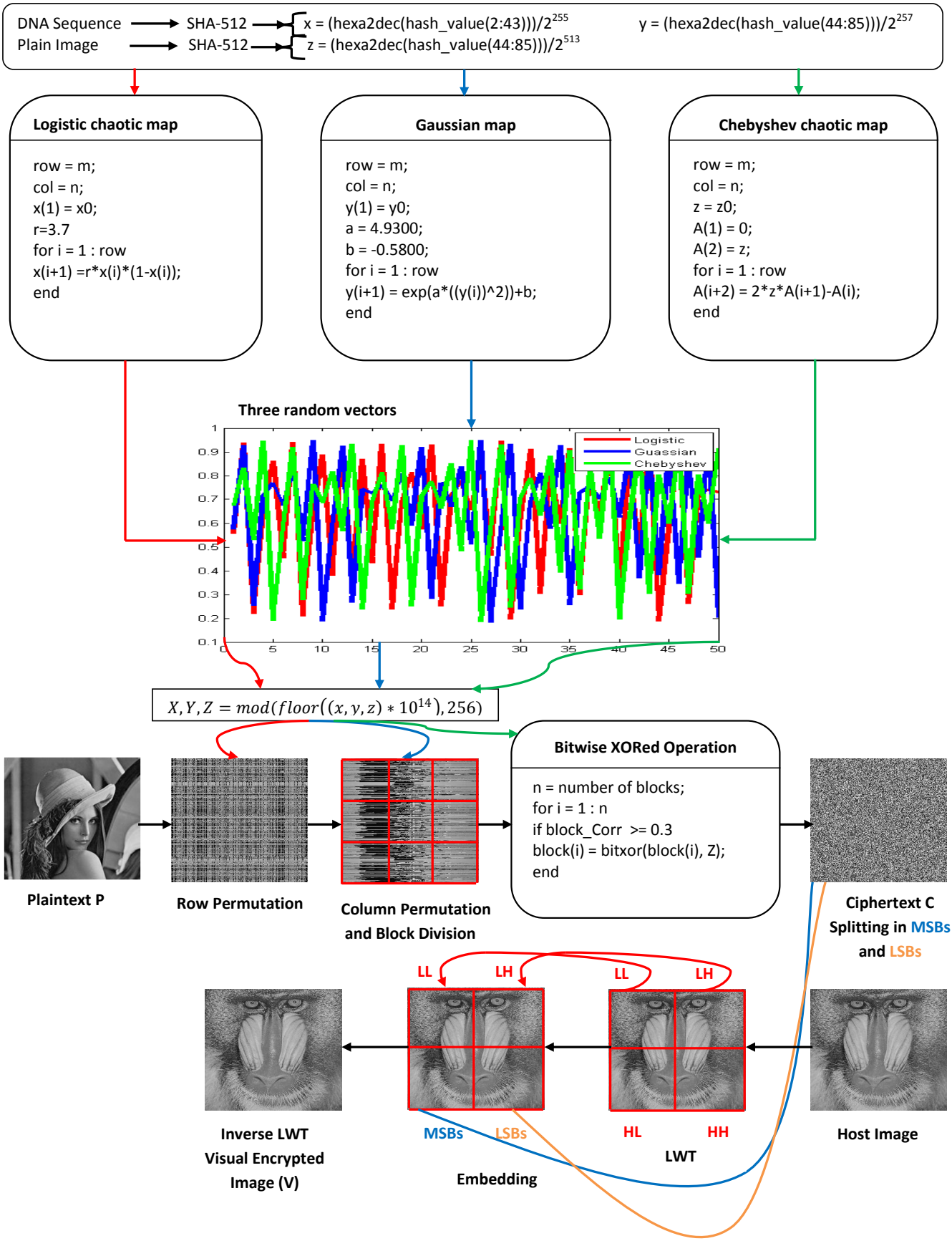

FIGURE 2. Block diagram demonstrating the proposed encryption scheme and its basis in visually selective images.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

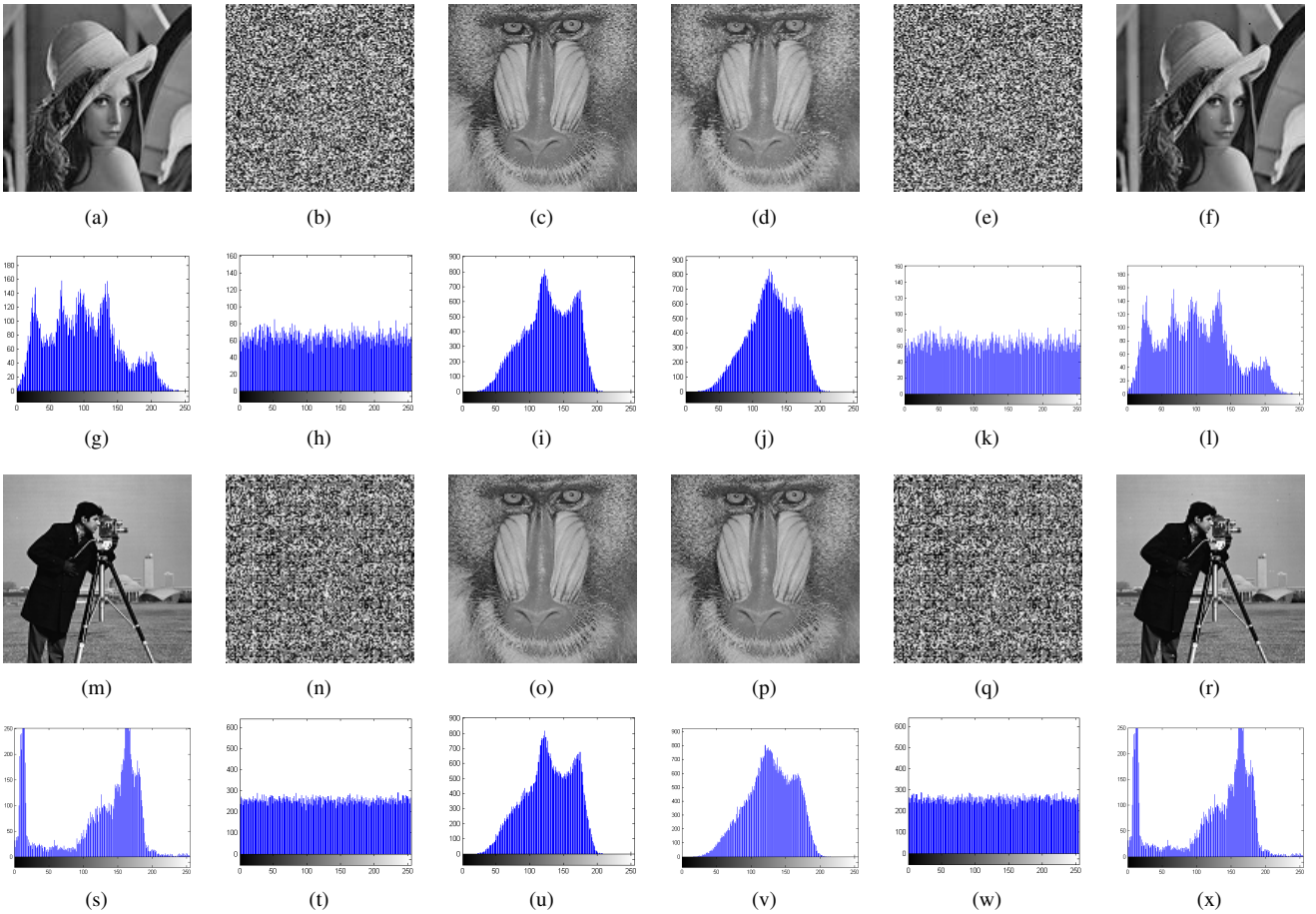

FIGURE 3. Encryption and decryption results of the proposed scheme. Column (1)[a,g,m,s] includes the plaintext Lena image, the plaintext Cameraman image and their corresponding histograms, respectively. Column (2)[b,h,n,t] includes corresponding ciphertext images and their corresponding histograms. Column (3)[c,i,o,u] includes plaintext carrier images and their corresponding histograms. Column (4)[d,j,p,v] includes visually encrypted images and their corresponding histograms. Column (5)[e,k,q,w] includes extracted ciphertext images and their corresponding histograms. Column (6)[f,l,r,x] includes decrypted images and their corresponding histograms.

TABLE 1. Statistical attack analysis: Variance of histogram.

Image	Lena	Cameraman
Plaintext	30578.00	113650.00
Ciphertext	310.44	845.16
Carrier	14972000.00	14972000.00
Visually Encrypted	47497.00	475950.00
Ref [38]	262.50	201.79

cipher images of size 256256 pixels and visually encrypted images of size 512×512 pixels. The calculated values are demonstrated in Table 1.

Pearson's correlation, developed by mathematician Karl Pearson and made public knowledge in 1884 can be used in correlation coefficient tests that will measure or compute the degree of similarity between two variables. It has a value between -1 and 1. To check the similarity between adjacent pixels values, we carried out this test in various directions: vertical, horizontal and diagonal. Mathematically, the correlation coefficient is given by [25]:

$$C_{xy} = \frac{\frac{1}{N}\sum_{n=1}^{N}(x_n - \bar{x})(y_n - \bar{y}))}{\sigma_x \sigma_y} \tag{12}$$

$$\sigma_x = \frac{1}{N}\sum_{n=1}^{N}(x_n - \bar{x})^2 \tag{13}$$

$$\sigma_y = \frac{1}{N}\sum_{n=1}^{N}(y_n - \bar{y})^2 \tag{14}$$

where N represents the aggregate number of pixels within in an $M \times N$ matrix. Here, σ_x and σ_y denote standard deviations while $\bar{x}$ and $\bar{y}$ compute mean values, respectively. From Tables 2 and 3, it is clear that ciphertext images have correlation coefficient values that are lower than zero. Meanwhile, the correlation coefficient values for visually encrypted images remain very similar to those of the plaintext host images, demonstrating that the visually encrypted images are not overly changed. However, the relatively low values of correlation coefficients and the uniformly distributed histogram of ciphertexts both confirm that the image encrypted using our

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

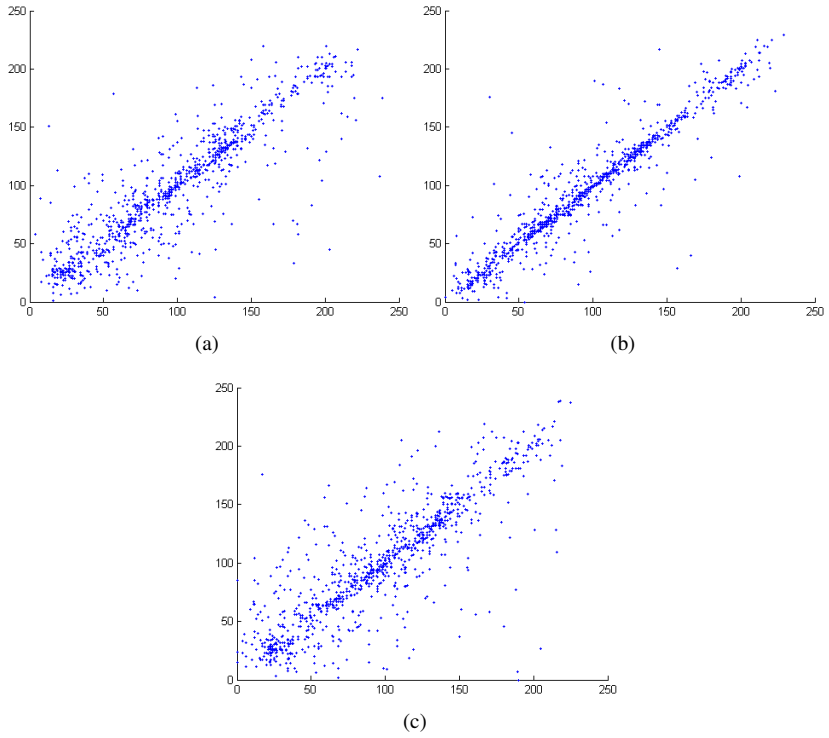

FIGURE 4. Plots depicting correlation analysis for plaintext image "Lena" in various directions: (a) horizontal, (b) vertical, and (c) diagonal.

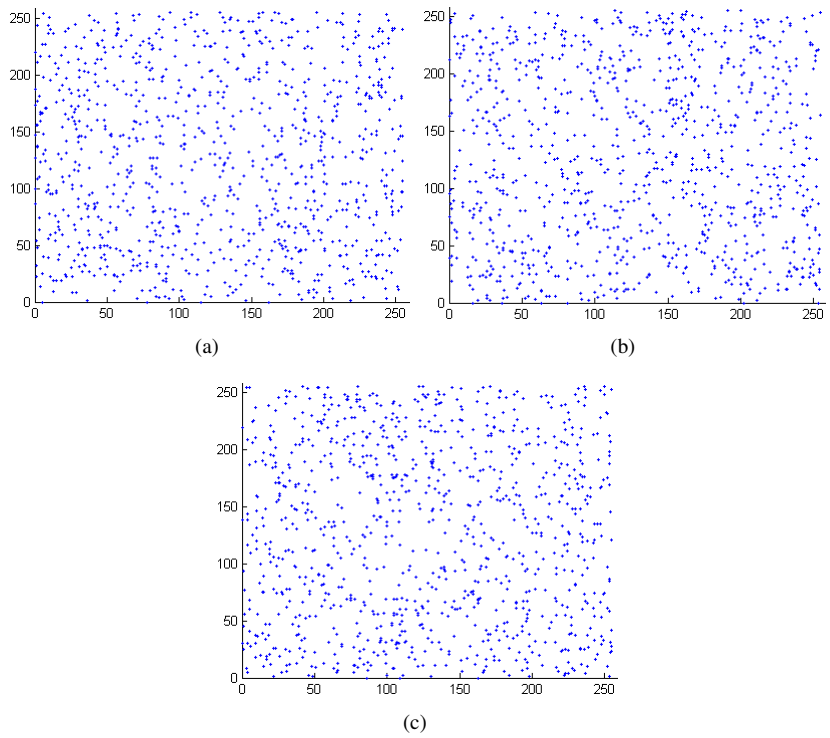

FIGURE 5. Plots depicting correlation analysis for the ciphertext image "Lena" in various directions: (a) horizontal, (b) vertical, and (c) diagonal.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

TABLE 2. Statistical attack analysis: Correlation coefficient values of the Lena image.

Direction	Plaintext	Ciphertext	Carrier	Visually Encrypted
Horizontal	0.8841	-0.0041	0.7042	0.5901
Vertical	0.9463	-0.0037	0.6547	0.4487
Diagonal	0.8430	-0.0065	0.6280	0.3021

TABLE 3. Statistical attack analysis: Correlation coefficient values of the Cameraman image.

Direction	Plaintext	Ciphertext	Carrier	Visually Encrypted
Horizontal	0.8563	-0.0015	0.7042	0.8182
Vertical	0.8970	-0.0143	0.6547	0.7387
Diagonal	0.8090	-0.0236	0.6280	0.6925

proposed scheme can withstand statistical attacks. Similarly, from the small values of variance of histograms for cipher images, it is confirmed that the histogram are flat and the proposed scheme can resist statistical attack.

B. ANALYSIS OF BRUTE FORCE ATTACK

In the next step, entropy and key space tests are conducted to assess whether images encrypted using our proposed cryptosystem can resist brute force attack. Entropy is a statistical test of randomness, normally used to characterize the image in textural terms, while the key space test determines the number of possible secret keys. For a cryptosystem to withstand a brute force attack, its key space must accommodate enough value and the entropy values must be close to the ideal value of 8. Numerically one can compute entropy as follows [39]:

$$H = \sum_{i=0}^{N-1} p(a_i) \times \log_2(\frac{1}{p(a_i)}) \tag{15}$$

where $p(a_i)$ computes the probability of occurrence for the variable a. Table 4 demonstrates, that the entropy values computed for ciphertext images are almost equal to the ideal value 8, while entropy values of visually encrypted images are nearly the same. Here, X_0, γ, Y_0, a, b and z serve as secret keys for the proposed encrypted scheme. Keeping the precision of 10^{-15} in mind, the key space can be computed as follows [40]:

$$\begin{aligned} \text{KS} &= \left(10^{15}.10^{15}.10^{15}.10^{15}.10^{15}.10^{15}\right) \\ &= 10^{90} \\ &= 2^{299} \end{aligned} \tag{16}$$

The computed values of key space are shown in Table. 5. Thus, the higher value of entropy and key space confirms that our proposed encryption scheme can defy brute force attacks.

C. ANALYSIS OF DIFFERENTIAL ATTACK

Differential attack analysis basically computes the occurrence of change or alteration in the encrypted image following a small change being made to the original plaintext image. An encryption algorithm must be very sensitive to very small change in the plaintext image, down to the value of a single bit or pixel. The Number of Pixels Change Rate (NPCR) test and the Unified Average Changing Intensity (UACI) test can each be used to conduct and evaluate differential attack analysis. Let C_1, and C_2 denote two encrypted images, each of which is only one different pixel value different from their corresponding plaintext images. The two testing measures introduced above, the NPCR and the UACI, can be computed as follows [4], [41]:

$$NPCR = (\frac{\sum_{k,l} T(k,l)}{M \times N}) \times 100\% \tag{17}$$

where

$$T(k,l) = \begin{cases} 0 & \text{if } C_1(k,l) = C_2(k,l) \\ 1 & \text{otherwise.} \end{cases} \tag{18}$$

$$UACI = (\sum_{k,l} \frac{C_1(k,l) - C_2(k,l)}{255}) \times \frac{1}{M \times N} \times 100. \tag{19}$$

In the above equations, M and N denote the height and the width of the plaintext image, respectively. The values computed by the NPCR and UACI tests, respectively (Table 6) confirm our proposed scheme's security against differential attack, since the change that occurred after embedding the ciphertext image into the carrier image is very small.

D. ANALYSIS OF KEY SENSITIVITY

A secure and efficient cryptosystem will be responsive to even very tiny changes in secret keys. To inspect the key sensitivity performance of the designed cryptosystem, a ciphertext image is generated using $X_0 = 0.4756, \gamma = 3.8000, Y_0 = 0.4008, a = 4.9300, b = -0.5800$ and $z = 0.3074$. We decrypt the same ciphertext image with a small change in of the keys i.e., $X_0 = 0.4757, \gamma = 3.8000, Y_0 = 0.4008, a = 4.9300, b = -0.5800$ and $z = 0.3074$. The resulting images, both ciphertext and decrypted are include in Fig. 6. Figure 6(b), shows the decrypted image with a minute modification in one of its secret keys while Fig. 6(c) demonstrates difference between the ciphertext image and its corresponding decryption. The computed percentage difference between Fig. 6(a) and Fig. 6(b) is also greater than 99%. These results confirm that the cryptosystem we propose is highly sensitive to even minute changes in the relevant keys. Both the schemes in [23] and [24], have also greater than 99% percentage difference.

E. ANALYSIS OF NOISE AND OCCLUSION ATTACK

Because the transmission of images take place via networks, there is always the possibility of noise attacks or data loss,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

TABLE 4. Brute force attack analysis: Entropy values.

Image Type	Plaintext	Ciphertext	Carrier	Visually Encrypted	Ref. [24]
Lena	7.5892	7.9897	7.1273	7.0849	7.2718
Cameraman	7.1096	7.9890	7.1273	7.0836	7.4387

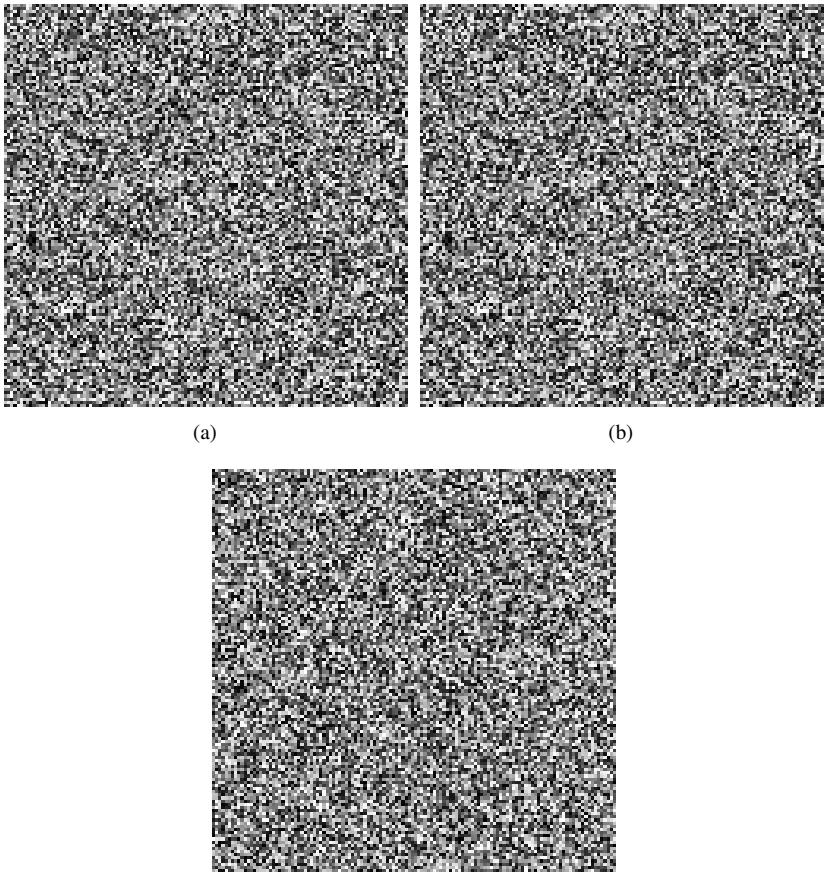

FIGURE 6. Sensitivity plots: (a) $Cipher_{image}$ with parameters $X_0 = 0.4756, \gamma = 3.8000, Y_0 = 0.4008, a = 4.9300, b = -0.5800$ and $z = 0.3074$, (b) $Decrypted_{image}$ with parameters $X_0 = 0.4757, \gamma = 3.8000, Y_0 = 0.4008, a = 4.9300, b = -0.5800$ and $z = 0.3074$, and (c) difference of $Cipher_{image}$ and $Decrypted_{image}$.

TABLE 5. Key space comparison.

Algorithm	Ours	Ref. [23]	Ref. [24]
Key space	2^{299}	$10^{56} = 2^{186}$	$>2^{215}$

TABLE 6. Differential attack analysis.

Test Type	Ciphertext Lena	Visually Encrypted Lena	Ciphertext Cameraman	Visually Encrypted Cameraman
NPCR	90.1978	82.9285	91.7114	84.3140
UACI	30.0263	1.3088	30.8406	1.3489

when an attackers crops or replaces portions of the image data. Noise and data loss can each create problems during the decryption process later, and therefore, a secure image encryption scheme must withstand these two types of attacks. To test our proposed encryption scheme, we added salt and pepper noise of 20% density to the image being visually encrypted (results depicted in Fig. 7(b)). we also replaced the initial 50×50 pixels with a white box and then decrypted the modified image, as demonstrated in Fig. 7(d). The results demonstrates that our proposed scheme is resistant to noise and cropping attack.

F. ANALYSIS OF ENCRYPTION QUALITY

Tests such as irregular deviation (ID) and Uniform Histogram deviation (HD) are often used to analyze the quality of encryption. ID measures, how much deviation caused by encryption is irregular while HD maximize the deviation between the original image and its encrypted counterpart. To calculate ID, the following steps are required. First,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

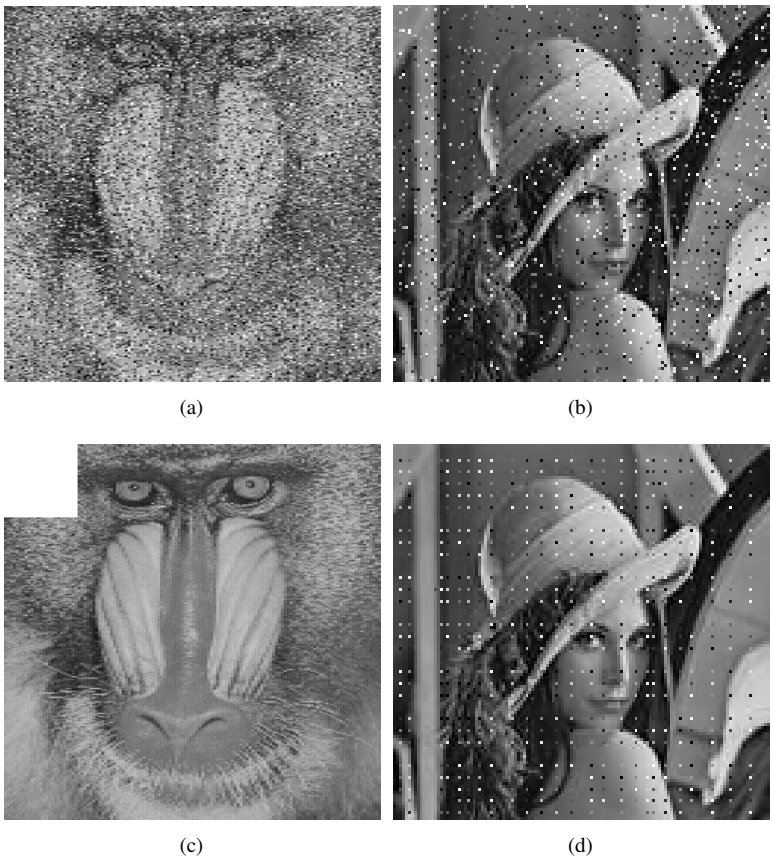

FIGURE 7. Noise and cropping attack plots: (a) Visual ciphertext image complete with salt and pepper noise [density level 0.2], (b) decrypted original Lena image with some noise distortion, (c) visual ciphertext image with 50×50 cropped pixels, and (d) decrypted original Lena image with some noise distortion

the absolute difference between plaintext and cipher images must be calculated and then estimated to compute estimated histogram E_H. In the next step, the mean value M_{EH} of the histogram is estimated or computed. Finally, from these results, it is possible to calculate the absolute value of the histogram's deviation from the mean, which can be done as follows [40]:

$$H_D(n) = |E_{H(n)} - M_{EH}| \tag{20}$$

Now ID can be computed as:

$$ID = \frac{\sum_{n=0}^{255} H_D(n)}{M \times N} \tag{21}$$

Similarly, HD can be calculated as:

$$HD = \frac{\sum_{n=0}^{255} H_{E(n)} - H_E}{M \times N} \tag{22}$$

$$H_{E(n)} = \begin{cases} \frac{M \times N}{256} & \text{if } 0 \leq E(n) \leq 255 \\ 0 & \text{otherwise.} \end{cases} \tag{23}$$

where H_E demonstrates the histogram of ciphertext image while $H_{E(n)}$ computes the number of occurrence at position n. Table 7 demonstrates the computed values of ID and HD. The lower values of both ID and HD for ciphertext images, confirms that there is considerable irregularity and less divergence of histogram from uniform histogram. While the greater values of ID and HD for visually encrypted images shows that there is less irregularity and more divergence of histogram from uniform histogram. Thus, one can conclude that the encryption is of good quality.

TABLE 7. Encryption quality analysis.

Test Type	Ciphertext Lena	Visually Encrypted Lena	Ciphertext Cameraman	Visually Encrypted Cameraman
ID	10468	108376	10020	108306
HD	0.7500	0.9445	0.7203	0.9423

G. ANALYSIS OF ENERGY

Energy computes the aggregate of all elements squared in the "Grey Level Co-occurrence Matrix" (GLCM), which is generally utilized to quantify the information in an image. In an effective encryption scheme or algorithm, the energy level should be quite low. Mathematically, energy can be computed as [42]:

$$Energy = \sum P(k,l)^2 \tag{24}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3020917, IEEE Access

TABLE 8. Energy analysis

Image Type	Plaintext	Ciphertext	Carrier	Visually Encrypted
Lena	0.0645	0.0162	0.0898	0.1062
Cameraman	0.1618	0.0168	0.0898	0.1052

TABLE 9. Contrast analysis

Image Type	Plaintext	Ciphertext	Carrier	Visually Encrypted
Lena	1.1303	10.3737	0.8582	0.5946
Cameraman	1.2015	9.6847	0.8582	0.6017

where $P(k,l)$ represents the pixel value at index k, and l. The energy values computed for our proposed encryption scheme are presented in Table 8, where low values of energy confirm that there is maximum disorder in the encrypted image and so the encryption is of high quality.

H. ANALYSIS OF CONTRAST

Contrast generally identifies the objects in the image's texture. The ciphertext images generated via an effective image encryption algorithm will exhibit high contrast due to high randomness. Mathematically, the contrast can be illustrated as follows [42]:

$$Contrast = \sum_{k,l} |k-l|^2 P(k,l) \tag{25}$$

where $P(k,l)$ represent $GLCM$. The contrast values computed following our proposed scheme is collected in Table 9, where demonstrate that this cryptosystem is efficient and offer higher security. Lower values of contrast for visually encrypted image would have demonstrated that the embedding didn't generate much randomness.

I. ANALYSIS OF HOMOGENEITY

The proximity quantification of the elements distributed in the GLCM is managed through homogeneity. The GLCM or alternately the Grey Tone Spatial Dependency Matrix (GTSDM), can illustrate the values of pixel brightness or greyness statistically. Mathematically, homogeneity can be computed as follows [42]:

$$Homogeneity = \sum \frac{P(k,l)}{1+|k-l|} \tag{26}$$

The computed homogeneity values for our scheme is demonstrated in Table 10, where lower homogeneity values for ciphertext images and higher values for visually encrypted images confirms this scheme's security, quality, and efficiency.

J. ANALYSIS OF KNOWN-PLAINTEXT AND CHOSEN-PLAINTEXT ATTACKS

Initial values for all three chaotic maps: logistic (x_0), Gaussian (y_0) and Chebyshev (z_0) are generated via SHA-512.

TABLE 10. Homogeneity analysis

Image Type	Plaintext	Ciphertext	Carrier	Visually Encrypted
Lena	0.7634	0.3946	0.7502	0.7840
Cameraman	0.8563	0.4069	0.7502	0.7807

These values are totally dependent on a random DNA sequence and plaintext image. As the confusion and diffusion parameters are correlated to these initial conditions, thus a small change in the DNA sequence or plaintext image will generate a totally different initial condition and so different chaotic vectors. As a result, the algorithm will produce totally different cipher images and an eavesdropper will be unable to decrypt a specific image using the computed initial conditions. Thus, this encryption scheme will be able to withstand both chosen-plaintext attacks and known-plaintext attacks.

K. COMPUTATIONAL TIME COMPLEXITY

The proposed scheme is tested in Matlab 2013a, Intel 391 Core i5-380M (2.53 GHz) Central Processing Unit 392 (CPU) with 4 GB RAM. The tested images, plaintext original image and carrier or host image are of size 128×128 pixels and 256×256 pixels, respectively. The proposed scheme consists of three main parts: (a) Random sequence generation, (b) Encryption and (c) Embedding. For Lena plaintext image and Baboon carrier images, the random sequence generation phase takes 0.0775 seconds, encryption phase takes 4.4282 seconds and the embedding phase completed in 0.0905 seconds. Thus, to generate the final visual cipher image, the proposed scheme takes 4.5962 seconds. The scheme in [6] takes 0.4640 seconds and the scheme in [7] takes 0.093 seconds as per their defined specification of the systems, respectively.

V. CONCLUSION

An efficient DNA and plaintext dependent chaotic visual selective image encryption is designed, examined, and recommended. All initial values and controlled parameters of relevant chaotic systems are computed by passing DNA sequence and plaintext image through SHA-12 hash function. The original plaintext image to be encrypted is shuffled via row and column of pixels using two random sequences to introduce confusion. The confused or shuffled image is divided into blocks, with blocks of correlation coefficients valued more than a certain defined threshold are bitwise XORed with a random matrix to introduce diffusion. The diffused blocks are recombined, the ciphertext image is embedded in a host image to achieve the final visually selective encrypted image that will withstand cryptographics attacks. Statistical attack analysis, brute force attack analysis, noise attack analysis, key sensitivity analysis and data loss attack analysis are all conducted on the final image in order to confirm the security, robustness, and efficiency of the new encryption scheme. The main advantage of the proposed scheme is that encrypted

image is not random like noise and hence attacker may not know that image contain confidential information. The disadvantage of the proposed scheme is that it takes more time than a traditional scheme. Future works will investigate the problem of encrypting remote sensing big data [43]–[46].

REFERENCES

[1] V. Divya, S. Sudha, and V. Resmy, "Simple and secure image encryption," IJCSI International Journal of Computer Science Issues, vol. 9, no. 6, pp. 286–289, 2012.

[2] R. Matthews, "On the derivation of a chaotic encryption algorithm," Cryptologia, vol. 8, no. 1, pp. 29–41, 1984.

[3] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Optics and Lasers in Engineering, vol. 78, pp. 17–25, 2016.

[4] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and s-box," in Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on, pp. 1–6, IEEE, 2015.

[5] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, "A new image encryption scheme based on dynamic s-boxes and chaotic maps," 3D Research, vol. 7, no. 1, p. 7, 2016.

[6] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic s-boxes," Entropy, vol. 21, no. 8, p. 790, 2019.

[7] S. Zhu, C. Zhu, H. Cui, and W. Wang, "A class of quadratic polynomial chaotic maps and its application in cryptography," IEEE Access, vol. 7, pp. 34141–34152, 2019.

[8] 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.

[9] M. Ş. Açikkapi, F. Özkaynak, and A. B. Özer, "Side-channel analysis of chaos-based substitution box structures," IEEE Access, vol. 7, pp. 79030–79043, 2019.

[10] F. Artuğer and F. Özkaynak, "A novel method for performance improvement of chaos-based substitution boxes," Symmetry, vol. 12, no. 4, p. 571, 2020.

[11] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, W. J. Buchanan, et al., "Chaos-based confusion and diffusion of image pixels using dynamic substitution," IEEE Access, 2020.

[12] A. Belazi, A. A. A. El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," Optics and Lasers in Engineering, vol. 88, pp. 37–50, 2017.

[13] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," Information Sciences, vol. 396, pp. 97–113, 2017.

[14] 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 s 8 permutation," Journal of Intelligent & Fuzzy Systems, no. Preprint, pp. 1–13, 2017.

[15] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel substitution box for encryption based on lorenz equations," in Circuits, System and Simulation (ICCSS), 2017 International Conference on, pp. 32–36, IEEE, 2017.

[16] S. Farwa, N. Muhammad, N. Bibi, S. A. Haider, S. R. Naqvi, and S. Anjum, "Fresnelet approach for image encryption in the algebraic frame," Applied Mathematics and Computation, vol. 334, pp. 343–355, 2018.

[17] Y. Luo, R. Zhou, J. Liu, Y. Cao, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," Nonlinear Dynamics, pp. 1–17, 2018.

[18] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," Multidimensional Systems and Signal Processing, pp. 1–19, 2018.

[19] F. Masood, W. Boulila, J. Ahmad, S. Sankar, S. Rubaiee, W. J. Buchanan, et al., "A novel privacy approach of digital aerial images based on mersenne twister method with dna genetic encoding and chaos," Remote Sensing, vol. 12, no. 11, p. 1893, 2020.

[20] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," Information Sciences, vol. 324, pp. 197–207, 2015.

[21] W. Hua and X. Liao, "A secret image sharing scheme based on piecewise linear chaotic map and chinese remainder theorem," Multimedia Tools and Applications, vol. 76, no. 5, pp. 7087–7103, 2017.

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

[23] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic lsb embedding," Optics and Lasers in Engineering, vol. 124, p. 105837, 2020.

[24] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, "Hiding cipher-images generated by 2-d compressive sensing with a multi-embedding strategy," Signal Processing, vol. 171, p. 107525, 2020.

[25] M. Ghebleh and A. Kanso, "A novel secret image sharing scheme using large primes," Multimedia Tools and Applications, vol. 77, no. 10, pp. 11903–11923, 2018.

[26] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual meaningful encryption scheme using intertwinning logistic map," in Science and Information Conference, pp. 764–773, Springer, 2018.

[27] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in dna microdots," Nature, vol. 399, no. 6736, p. 533, 1999.

[28] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," Optics and Lasers in engineering, vol. 88, pp. 197–213, 2017.

[29] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Optics and Lasers in Engineering, vol. 90, pp. 238–246, 2017.

[30] B. Mondal and T. Mandal, "A light weight secure image encryption scheme based on chaos & dna computing," Journal of King Saud University-Computer and Information Sciences, vol. 29, no. 4, pp. 499–504, 2017.

[31] J. Chen, Z.-l. Zhu, L.-b. Zhang, Y. Zhang, and B.-q. Yang, "Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption," Signal Processing, vol. 142, pp. 340–353, 2018.

[32] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," Chaos, Solitons & Fractals, vol. 40, no. 5, pp. 2557–2568, 2009.

[33] R. C. Hilborn et al., Chaos and nonlinear dynamics: an introduction for scientists and engineers. Oxford University Press on Demand, 2000.

[34] A. Sahay and C. Pradhan, "Gauss iterated map based rgb image encryption approach," in Communication and Signal Processing (ICCSP), 2017 International Conference on, pp. 0015–0018, IEEE, 2017.

[35] I. Bashir, F. Ahmed, J. Ahmad, W. Boulila, and N. Alharbi, "A secure and robust image hashing scheme using gaussian pyramids," Entropy, vol. 21, no. 11, p. 1132, 2019.

[36] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on chebyshev chaotic maps," Nonlinear Dynamics, vol. 77, no. 1-2, pp. 399–411, 2014.

[37] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," Nonlinear Dynamics, vol. 92, no. 2, pp. 305–313, 2018.

[38] 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.

[39] C. E. Shannon, "Prediction and entropy of printed english," Bell system technical journal, vol. 30, no. 1, pp. 50–64, 1951.

[40] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," IEEE Access, vol. 7, pp. 147106–147118, 2019.

[41] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," Nonlinear Dynamics, vol. 82, no. 4, pp. 1839–1850, 2015.

[42] J. S. Khan, J. Ahmad, S. S. Ahmed, H. A. Siddiqa, S. F. Abbasi, and S. K. Kayhan, "Dna key based visual chaotic image encryption," Journal of Intelligent & Fuzzy Systems, vol. 37, no. 2, pp. 2549–2561, 2019.

[43] I. Chebbi, W. Boulila, and I. R. Farah, "Big data: Concepts, challenges and applications," in Computational collective intelligence, pp. 638–647, Springer, 2015.

[44] I. Chebbi, W. Boulila, and I. R. Farah, "Improvement of satellite image classification: Approach based on hadoop/mapreduce," in 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), pp. 31–34, IEEE, 2016.

[45] W. Boulila, I. R. Farah, and A. Hussain, "A novel decision support system for the interpretation of remote sensing big data," Earth Science Informatics, vol. 11, no. 1, pp. 31–45, 2018.

[46] W. Boulila, "A top-down approach for semantic segmentation of big remote sensing images," Earth Science Informatics, vol. 12, no. 3, pp. 295–306, 2019.

JAN SHER KHAN has recently completed his master in Electrical Engineering (with highest distinction) from the Department of Electrical and Electronics Engineering, University of Gaziantep, Gaziantep, Turkey. He obtained his bachelor of science degree in Electrical Engineering, from HITEC University Taxila, Pakistan with highest distinction. As an exchange student, he completed his fourth year of undergraduate studies in the Department of Electrical and Electronics Engineering at Istanbul Technical University (ITU), Turkey. His research interest includes chaos based encryption, cryptography, compressive sensing, machine learning and medical imaging.

WADII BOULILA (SENIOR MEMBER, IEEE) received the Eng. degree in computer science from the Aviation School of Borj El Amri in 2005, the MSc degree from the National School of Computer Science (ENSI), University of Manouba, Tunisia in 2007, and the Ph.D. degree conjointly from ENSI and Telecom-Bretagne, University of Rennes 1, France in 2012. He is currently an associate professor of computer science with IS Department, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia. His primary research interests include big data analytics, deep learning, cybersecurity, data mining, artificial intelligence, uncertainty modeling, and remote sensing images. He is a senior researcher with the RIADI laboratory (University of Manouba, Tunisia) and an associate researcher with the ITI department (University of Rennes 1, France). Dr. Boulila served as chair, reviewer and TPC member for many leading international conferences and journals. He is a Senior IEEE Member and a Senior Fellow of the Higher Education Academy (SFHEA), UK.

JAWAD AHMAD is an experienced researcher with more than 10 years of cutting-edge research and teaching experience in prestigious institutes including Edinburgh Napier University (UK), Glasgow Caledonian University (UK), Hongik University (South Korea) and HITEC University Taxila (Pakistan). He has co-authored more than 50 research papers, in international journals and peer-reviewed international conference proceedings. He has taught various courses both at Undergraduate (UG) and Postgraduate (PG) levels during his career. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. He is an invited reviewer for numerous world-leading high-impact journals (reviewed 50+ journal papers to date). His research area is cybersecurity, multimedia encryption, machine learning, and application of chaos theory in cybersecurity.

SAEED RUBAIEE received the B.S. degree in chemical engineering from Tennessee Tech University, Cookeville, TN, USA, in 2009, the M.Sc. degree in industrial engineering/management from the University of South Florida, Tampa, FL, USA, in 2010, and the Ph.D. degree in industrial engineering from the Department of Industrial Systems and Manufacturing, Wichita State University, Wichita, KS, USA, in 2015. He is currently an Associate Professor with the Department of the Industrial and Systems Engineering, University of Jeddah, Jeddah, Saudi Arabia. His research interests include engineering systems, sustainability and green manufacturing, production equipment operation, renewable energy, energy-efficient production planning, manufacturing engineering, materials engineering, advanced materials, mathematical/statistical optimization and applied optimization.

ATIQUE UR REHMAN completed his Bachelor of Computer Engineering from Comsats univeristy, Lahore, Pakistan in 2011, and the Master of Science in Electrical Engineering from HITEC University Taxila, Pakistan in 2016. He has published many articles in the field of secure communication. His research interests include cryptography, digital image processing, secure Communication, computer and machine vision.

ROOBAEA ALROOBAEA received bachelor's degree (Hons.) in computer science from King Abdulaziz University (KAU), Saudi Arabia, in 2008, and the master's degree in information system and the Ph.D. degree in computer science from the University of East Anglia, U.K., in 2012 and 2016, respectively. He is currently an Associate Professor at the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include human–computer interaction, software engineering, cloud computing, the Internet of Thing, artificial intelligent, and machine learning.

WILLIAM J. BUCHANAN is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS and the IET. He was awarded an OBE in the Queen's Birthday awards in June 2017. Bill currently leads the Centre for Distributed Computing, Networks, and Security and The Cyber Academy, and works in the areas of security, Cloud Security, Web-based infrastructures, e-Crime, cryptography, triage, intrusion detection systems, digital forensics, mobile computing, agent-based systems, and security risk. Bill has one of the most extensive academic sites in the World and is involved in many areas of novel research and teaching in computing. He has published over 27 academic books, and over 250 academic research papers, along with several awards for excellence in knowledge transfer, and for teaching. He was named as one of the Top 100 people for Technology in Scotland from 2012 to 2017. Recently he was included in the FutureScot "Top 50 Scottish Tech People Who Are Changing The World".