DNA Key Based Visual Chaotic Image Encryption

Jan Sher Khan*, Jawad Ahmad †, Saygin Siddiq Ahmed *, Hafza Ayesha Siddiqa‡, Saadullah Farooq Abbasi§ and Sema Koç Kayhan*

* Department of Electrical and Electronics, University of Gaziantep, 27310 Gaziantep, Turkey.

†Glasgow Caledonian University, School of Engineering and Built Environment, Glasgow, United Kingdom.

‡Department of Electrical Engineering, HITEC University Taxila, Pakistan.

§Department of Electrical Engineering, ISRA University Islamabad, Pakistan.

***Abstract*—With the exponential growth of Internet technologies, digital information exchanged over the Internet is also significantly increased. In order to ensure the security of multimedia contents over the open natured Internet, data should be encrypted. In this paper, the quantum chaotic map is utilized for random vectors generation. Initial conditions for the chaos map is computed from a DNA (Deoxyribonucleic acid) sequence along with plaintext image through Secure Hash Algorithm-512 (SHA-512). The first two random vectors break the correlation among pixels of the original plaintext image via row and column permutation, respectively. For the diffusion characteristics, the permuted image is bitwise XORed with a random matrix generated through the third random vectors. The diffused image is divided into Least Significant Bit (LSB) and Most Significant Bits (MSBs) and Discrete Wavelet Transform (DWT) is applied to the carrier image. The HL and HH blocks of the carrier image are replaced with LSBs and MSBs of the diffused image for the generation of a visually encrypted image. The detailed theoretical analysis and experimental simulation of the designed scheme show that the proposed encryption algorithm is highly secured. Efficiency and robustness of the proposed visually image encryption scheme is also verified via a number of attack analyses, i.e., sensitivity attack analysis ($>$ 99%), differential attack analysis (NPCR $>$ 99, UACI $>$ 33), brute force attack (almost 7.9892), statistical attack (correlation coefficient values are almost 0 or less than zero), noise tolerance, and cropping attack. Further security analyses such as encryption quality ($I_D \cong$ 1564, D_H = 3.000), homogeneity (0.3798), contrast (10.4820) and energy (0.0144) of the scheme are also evaluated.**

***Keywords*: Light-weight, secure, visual image encryption, chaos, Deoxyribonucleic acid, permutation, diffusion**

I. Introduction

With the evolution of Internet technologies, multimedia data over the Internet is transmitted and received faster as compared with older technologies. However, along with the evolution of Internet technologies, powerful attacks on multimedia data by intruders is also significantly increased. Such attacks on images seriously compromises individual privacy. Therefore, securing digital image information from illegal interpretation is a hot research area. Out of various security methods, encryption is a technique in which image data is manipulated in such away that an illegal person cannot read the original contents. Over the last two decades, several encryption algorithms have been designed for the security of digital images. These image encryption schemes is categorized into two different types i. full image encryption ii., and partial image encryption. Full image encryption deals with encrypting the entire image data and utilizes many resources and need more time for full encryption. Whereas, the second type of encryption method i.e., partial encryption generally need less computation and time. Moreover, partial encryption requires less resources when encrypting only region of interest in an image. Partial image encryption schemes is highly computational efficient which are then suitable for real time implementations and applications, such as teleconference and camera surveillance etc.

In recent years, chaotic maps were extensively studied in various subjects such as mathematics, physics, computer science and engineering field. Due to sensitivity, blanketing nature and topological transitivity of many chaotic maps, application of chaotic maps were not only restricted to the aforementioned subjects. Many researchers and cryptographers were attracted towards chaos-based image encryption since last two decades. A number of 1-D and higher dimensional chaotic maps i.e., Logistic map, 2-D Logistic map, Intertwining Logistic map, Henon map, Quantum map, Burger map, Skew-tent map, Bernoulli's map, Beta map, and Piecewise Linear Chaotic Map (PWLCM) e.t.c were presented in past [1]–[8]. Generally, chaotic maps are utilized to generate random numbers which are highly sensitive to initial conditions. These random numbers are used in the confusion (pixels positions changing) and diffusion (pixels value changing) process. Due to sensitivity to initials key and light-weight nature of chaotic maps, researchers have found a close relationship between chaos and cryptography [4], [5]. In 1989, Mathew proposed the idea of image encryption via chaos for the first time [1]. Chen et al. [2] proposed 3D cat map and Logistic map based image encryption scheme in 2004. Image pixels were permuted via 3D cat chaotic map in Chen et al scheme. The relationship between plaintext and ciphertext images was confused through the logistic chaotic map. In 2012, the idea of improved hyperchaotic sequences in encryption was proposed by Zhu et al. [3]. Zhu's et al generated chaotic keystream by modifying the hyperchaotic sequences. In 2015, Khan et al. [4] proposed a new idea of image encryption algorithm. Khan's et al shuffled rows and columns and also performed XOR operation using henon and skew tent maps, respectively. Rehman et al. [5] in 2016, encrypted images through dynamic S-Boxes. Images were divided into four random blocks which were shuffled using Burger map. Ahmad et al. improved a chaos-based image encryption algorithm [6] by adding a bitwise XOR operation. Ahmad et al. also improved an orthogonal matrix based image encryption and results were compared with conventional schemes [7] in the year 2017. The authors in [8] find out some weakness in the existing encryption algorithm. A Non-Linear chaotic algorithm and S-boxes were utilized to improve the performance of the scheme.

The ciphertext image of many encryption schemes is a noise/texture-like image and thus resist various attacks i.e., known plaintext attack, chosen ciphertext attack etc. However, the possibility of attacks on noise like the image is high when compared to visual meaningful image [9]. To overcome this issue, Bao et al. transformed a plaintext image into a visually meaningful encrypted (secret) image [9]. In pre-encryption step, a plaintext image was encrypted and then embedded in a carrier image using discrete wavelet-based transform. The authors in [10], present a salient regions visual image encryption scheme. Saliency detection model is used to detect the salient regions. Then chaos is utilized to encrypt the detected salient regions. Finally, the encrypted salient regions are embedded in a carrier image to generate visual encrypted image. To reduce the number of attacks on a ciphertext image, Singh et al. proposed visual multiple image encryption algorithm [11]. The carrier image is embedded with multiple ciphertext data. Chai et al proposed compression sensing-based visual meaningful image encryption [12]. The plaintext image was converted into wavelet coefficients and then pixels were confused via the zigzag motion. Furthermore, the image was compressed using a compressive sensing method and embedded into a carrier image. Li et al. proposed a new visual meaningful image encryption via novel perfect black visual cryptography [13]. Properties like extensive parallelism, ultra-low power utilization and bulky storage make DNA computing extremely useful for cryptographic applications. Recently, cryptographers used DNA computing as a new cryptographic application. The idea of coupling DNA operator and chaotic maps was given by Zhang et al. [14]. Simulation results proved that the presented scheme can withstand exhaust attack, differential and statistical attacks. Liu et al. [15] presented an encryption algorithm which combines chaotic maps and DNA coding. The proposed scheme in [15] can withstand multiple attacks, and therefore provides sufficient security. In order to produce random numbers for bitwise XORing, Wang et al. utilized spatiotemporal chaotic system. A plaintext image was cofused through a DNA matrix which was generated from DNA-based encoding rule [16]. Chai et al. utilized SHA-256 and proposed a new image encryption method using DNA sequences [17]. Encryption algorithms through chaotic dynamic S-boxes and DNA sequence operation was suggested by Tian et al. [18]. The keyspace was large enough due to an external 256-bit in Tian et al scheme. Chen et al. proposed image confusion-diffusion using DNA encoding and secured digital images from eavesdroppers and attackers [19].

II. Proposed scheme

This section explains a DNA key based chaotic meaningful image encryption scheme. The detailed step of the proposed encryption scheme can be seen in Fig. 1. The scheme consists of (i) DNA based key generation, (ii) chaos based pseudo-random number generation, (iii) image encryption phase, and (iv) an embedding phase to get the final meaningful ciphertext image. The next section provides a detailed description of all the four phases.

```
**Phase 1 Algorithm:** DNA based key generation phase
**Inputs:** DNA sequence, Plaintext image (Cthead image)
**Outputs:** x(1), y(1) and z(1)
$DNA = ADWB00000000$
$I = imread('Cthead.png')$
$Opt.Method =' SHA - 512'$
$hash_1 = DataHash([DNA], Opt)$
$hash_2 = DataHash([I], Opt)$
$x(1) = hex2dec(hash_1(1:64))/2^{255}$
$y(i) = hex2dec(hash_1(65:128))/2^{260}$
$z(i) = hex2dec(hash_2)/2^{514}$
```

A. DNA based key generation phase

Deoxyribonucleic Acid (DNA) is the main constituent of chromosomes. Basically a DNA sequence consist of Adenine (A), Thymine (T), Guanine (G) and Cytosine (C), where Adenine is complementary of Thymine and Guanine is complementary of Cytosine, respectively. All known nucleic acid information sets can be found in nucleic acid database. Each sequence assigned a unique and permanent ID number in the data base which is known as sequence code. For public access, there are more than 163 million DNA sequences in the enormous databases. In image encryption applications, such databases can be treated is a natural password. To increase the security of the proposed scheme, a DNA sequence number "ADWB00000000" is selected randomly from 163 million existing sequences. SHA-512 is a hash function that generates 512 bits (128 characters) hash values. The application of hash function can be found in pseudo-random number generation, fast encryption, computer virus detection, password verification and storage etc [20], [21]. In order to make the proposed scheme dependable on the selected DNA sequence and plaintext image, both the DNA sequence and the plaintext image are passed through SHA-512 hash function. Hash values (4af26d01d41315adf857c91c46e6890539fb2719e8a4d7056469ce62a0d2afd4ebb6e72ad8de70a73b29838349f5f1b4145674eb69fc5e600c2250df72461773) and (36b013fa6af311f6d80f509ddbd8759afe4407036b70bb9f81f1f31592a8a2f52dfbca1410b0c8367028c4b18ea78a87dbf877be51c98bd623c8c6b3474c9d33) are generated, respectively. These hash values are utilised in the computation of initial conditions for the Quantum chaotic map. One can found further details about initial conditions generation in pseudo code phase 1.

B. Pseudo-random number generation

The authors from [22]–[25] analysed and explored the effects of quantum correction and state ($\alpha = < \alpha > + \delta\alpha$) which construct a quantum logistic map with quantum corrections. Where $\delta\alpha$ demonstrates the quantum fluctuation about $< \alpha >$. In [22]–[25], authors proved that for the lowest order

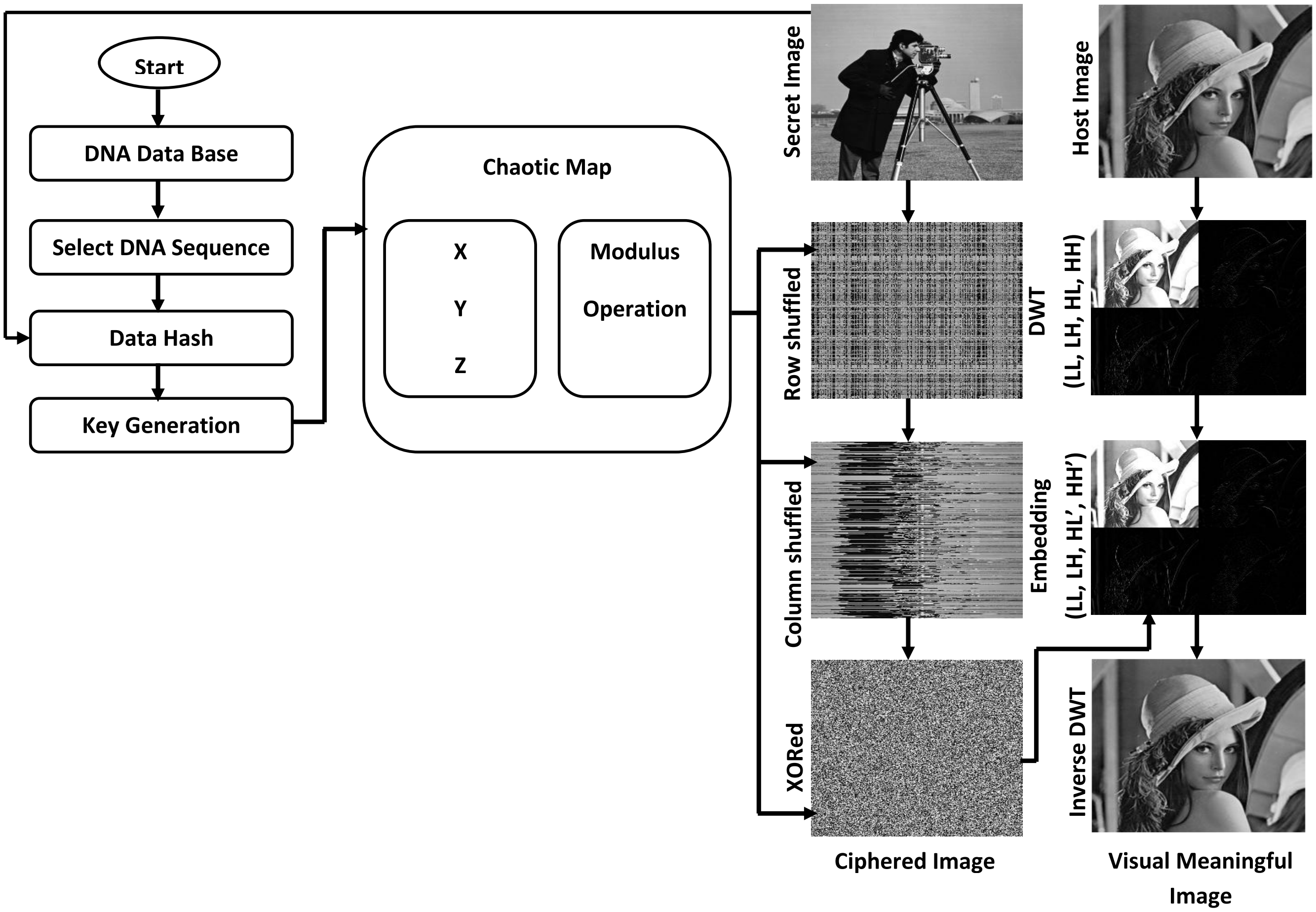


Fig. 1: Flowchart of the proposed scheme

of quantum correction, the following quantum chaotic map can be generated:

$$x_{(n+1)} = \gamma(x_n - |x_n|^2) - \gamma y_n.$$

$$y_{(n+1)} = -y_n e^{-2\beta} + e^{-\beta}.\gamma[(2-x_n-x'_n)*y_n - x_n z'_n - x'_n z_n]$$

$$z_{(n+1)} = -z_n e^{-2\beta} + e^{-\beta}.\gamma[2(1-x'_n)*z_n - 2x_n y_n - x_n] \quad (1)$$

where,
$\beta \in [6, +\infty]$
$\gamma \in [0, 4]$
$0 \leq x_n \leq 1$
$0 \leq y_n \leq 0.1$
$0 \leq z_n \leq 0.2$
$x'_n = x_n$
$z'_n = z_n$
x_n, y_n and z_n are the initial parameters. Generally, the initial parameters x_n, y_n and z_n are complex numbers with x'_0 and z'_0 are complex conjugate of x_n and z_n, respectively. One can confirm randomness and key sensitivity of Quantum chaotic map from Fig. [2]a and [2]b, respectively. From Fig. [2]b, it is confirmed that if the initial conditions are changed slightly, the Quantum chaotic system will generates totally different random number.

The aforementioned map is utilised in our proposed DNA key-based chaotic visual image encryption. The map is iterated for 256 times and the random numbers were generated i.e., $x = \{x_1, x_2, x_3, ...x_{256}\}, y = \{y_1, y_2, y_3, ...y_{256}\}$ and $z = \{z_1, z_2, z_3, ...z_{256}\}$ for initial parameters $x_n = 0.6, y_n = 0.07, z_n = 0.14, x'_n = x_n$ and $z'_n = z_n$ and control parameters $\gamma = 3.99$ and $\beta = 8$.

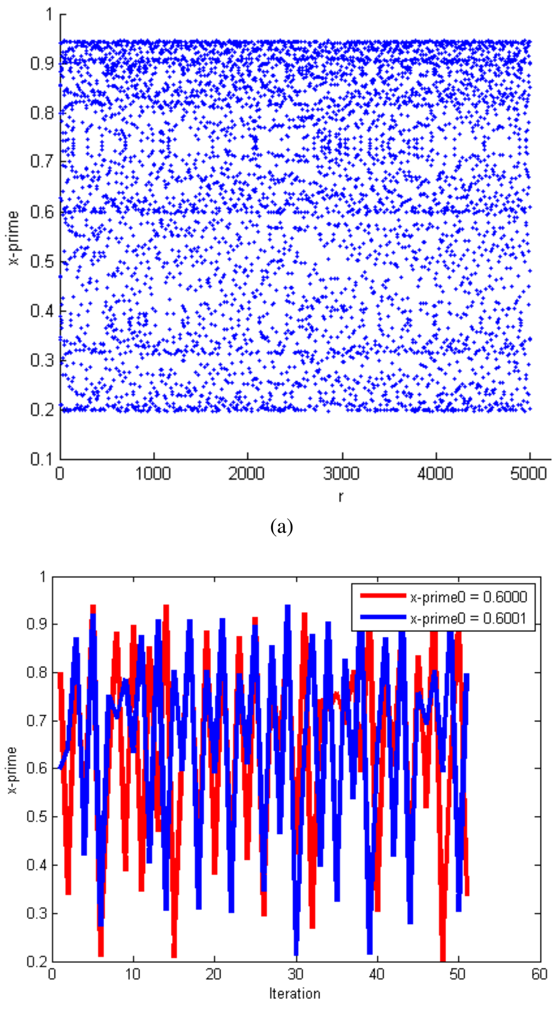
C. Image encryption phase

In this phase, the correlation among plaintext P pixel can be broken through random vectors x and y. The plaintext image pixels are shuffled through row and column permutation, respectively.

$$\begin{cases} Row_{Per}(:, i) = P(:, x(i)) & i = 1, 2, ..., n, \\ Col_{Per}(i, :) = Row_{Per}(y(i), :) & i = 1, 2, ..., n. \end{cases} \quad (2)$$

where Row_{Per} and Col_{Per} are row and column shuffled images, respectively. To get the diffused image or ciphertext image C, random vector z is arranged in matrix form and also bitwise XORed with permuted image as follow:

$$Diffused_{image} = bitxor(Col_{Per}, z). \quad (3)$$



(a)

(b)

Fig. 2: (a) 5000 random numbers computed using Quantum chaotic map. (b) Quantum map plot for a small change in $x - prime_0$.

D. Embedding phase

As compared to the size of plaintext image P, the size of host image CI must be 2 times of the size of P. The pixel values of ciphetext image C are converted to 8 bits binary or ASCII code and then divided into 4 bits i.e., MSBs and LSBs. The 4 bits binary MSBs and LSBs are now converted to decimal values. Discrete Wavelet Transform (DWT) is applied on the carrier image for the generation of four matrices i.e., LL, LH, HL and HH of sizes $(m/2) \times (n/2)$. Where m and n represents the carrier image rows and columns sizes, respectively. To get the visual encrypted image V, HL and HH matrices of carrier image CI are replaced with MSBs and LSBs of ciphertext image C and passed through inverse Discrete Wavelet Transform (IDWT). The pseudo code of the embedding process is shown in phase 4.

Phase 4 Algorithm: Carrier Embedding

Inputs: Ciphertext image C, its row and column numbers row, col, Carrier image CI

Outputs: Visual encrypted image V

```
for $i = 1$ to $row$
    for $j = 1$ to $col$
        $C_{Binary} = dec2bin(C(i,j))$
        $MSBs \leftarrow C_{Binary}(5:8)$
        $LSBs \leftarrow C_{Binary}(1:4)$
        $MSBs_{Matrix}(i,j) = bin2dec(MSBs)$
        $LSBs_{Matrix}(i,j) = bin2dec(LSBs)$
    Endfor
Endfor
$[LL \quad LH \quad HL \quad HH] = dwt2(CI,'db1')$
$V = idwt2(LL, \quad LH, \quad MSBs_{Matrix}, \quad LSBs_{Matrix},'db1')$
```

III. Experimental analysis and discussion

The proposed scheme is tested on grey scale high correlated images that were saved in our database. However, the proposed visual image encryption scheme can be applied to any image; including colour images. In the case of a colour image, the scheme must be applied on all the three layers (green, blue, and red). We have applied the proposed scheme on white, monolithic grey, black and Cthead images, respectively. These image are highly correlated. The reason for selecting a correlated image is that if the proposed scheme performs well for the correlated image it can perform even better on other images. The encryption and decryption results are shown in Fig. 5. The strength and efficiency of the proposed scheme is also verified through security tests as outlined below. Furthermore, the results are also compared with related work [10] and [11].

A. Brute force attack analysis

Resistance against Brute force attack is verified through Key space and entropy analyses. The total number of keys utilized in the encryption/decryption algorithm is known as the key space size. Crypto-systems must be completely sensitive towards secret keys. For a secure and good cryptosystem, the key-space must be at least 2^{100} [26], [27]. Entropy is known as the statistical measurement of randomness. For a true random source that emits 2^8, i.e. $a = [a_1, a_2, ..., a_{2^8}]$, its entropy should be 8 bits. Mathematically, the key space K and entropy H can be defined as:

$$\begin{aligned} \mathrm{K} &= \left(10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15}\right) \\ &= 10^{75} \\ &= 2^{249.165} \end{aligned} \tag{4}$$

$$H = \Sigma_{i=0}^{N-1} p(a_i) \times \log_2(\frac{1}{p(a_i)}) \tag{5}$$

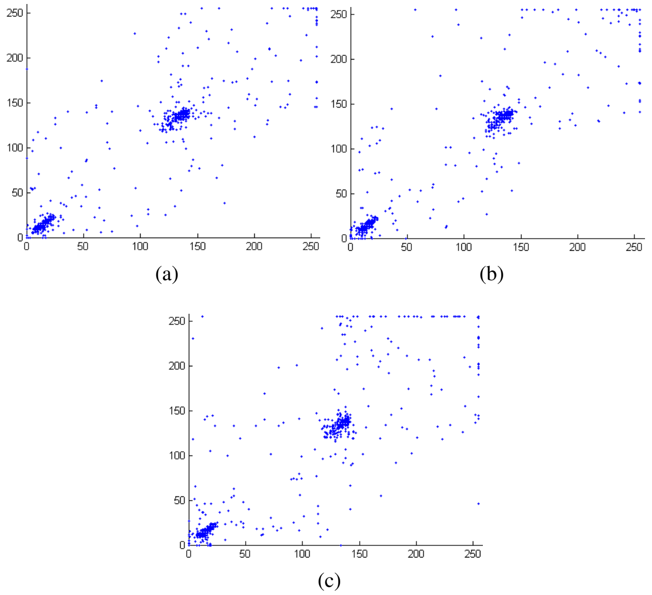
where $p(a_i)$ is the symbol a_i occurrence probability and and N is the total number of gray values. One can see from equation 4 and Table I that the values of key space and entropy of the proposed image encryption scheme are large enough and hence can resist brute force attack.

TABLE I: Entropy analysis.

Image Type	Plaintext Image	Ciphertext Image	Carrier Image	Visual Encrypted Image	Ref. [10]	Ref. [11]
White	0.2354	7.9892	7.1273	7.0850	7.9745	7.9801
Monolithic Gray	0.0000	7.9870	7.1273	7.0837	7.9670	7.9550
Black	0.2214	7.9884	7.1273	7.0843	7.9701	7.9561
Cthead	5.6763	7.9886	7.1273	7.0839	7.9685	7.9743

TABLE II: Horizontal correlation coefficient analysis.

Image Type	Plaintext Image	Ciphertext Image	Carrier Image	Visual Encrypted Image	Ref. [10]	Ref. [11]
White	0.5723	0.0272	0.7288	0.7866	0.0322	0.0423
Monolithic Gray	1.0000	0.0191	0.7288	0.8183	0.0236	0.0223
Black	0.6042	0.0458	0.7288	0.8107	0.1035	0.1745
Cthead	0.9426	0.0356	0.7288	0.8255	0.1188	0.0654



(a)

(b)

(c)

Fig. 3: Correlation analysis plots for Cthead plaintext image (a) horizontal (b) vertical (c) diagonal directions.

TABLE III: Vertical correlation coefficient analysis.

Image Type	Plaintext Image	Ciphertext Image	Carrier Image	Visual Encrypted Image	Ref. [10]	Ref. [11]
White	0.5781	-0.0111	0.6248	0.7092	0.2048	0.1002
Monolithic Gray	1.0000	0.0467	0.6248	0.6875	0.1893	0.0674
Black	0.6623	-0.0045	0.6248	0.7391	0.0367	0.0465
Cthead	0.9501	-0.0071	0.6248	0.6948	0.0387	0.0274

B. Statistical attack analysis

The histogram plots of a good encrypted ciphertext image must be uniform and the values of correlation coefficient must be close to zero. Histogram can be define as the pictorial pixel value distribution of an image. Correlation of an image is the statistical measurement of relationship between two adjacent pixels. A good cryptosystem must break the strong correlations in the plaintext image and then transform them into noise-like images with ideally zero correlations. Mathematically, correlation values can be computed as:

$$Corr_{xy} = \frac{Cov(x,y)}{\sigma_x \sigma_y} \tag{6}$$

$$Covar(x,y) = \frac{1}{L}\sum_{i=1}^{L}(x_i-\bar{x})(y_i-\bar{y}) \tag{7}$$

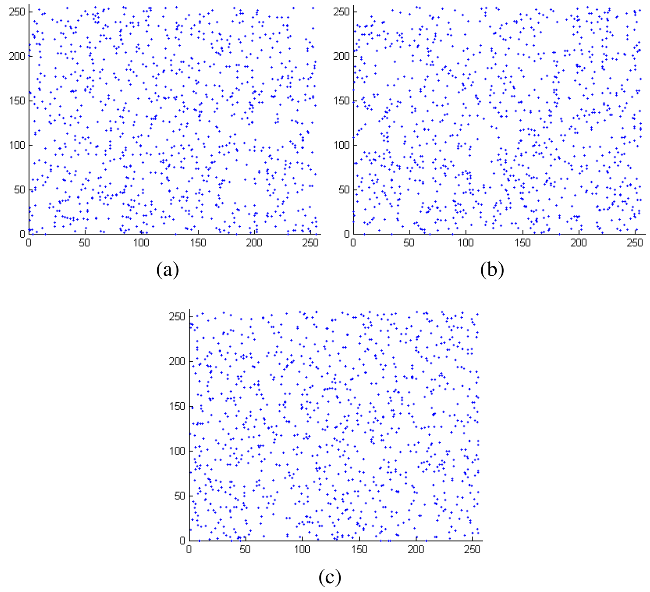
$$\sigma_x = \frac{1}{L}\sum_{i=1}^{L}(x_i-\bar{x})^2 \tag{8}$$

$$\sigma_y = \frac{1}{L}\sum_{i=1}^{L}(y_i-\bar{y})^2 \tag{9}$$

Where σ_x and σ_y are the standard deviations, $Corr_{xy}$ represent correlation coefficient and its value must be between -1 and 1. $Covar(x,y)$ computes the covariance at pixel locations x and y, $\bar{x}$ and $\bar{y}$ computes the mean value. L is the total number of pixels in a $M \times N$ matrix. From Figs. 6(b,h,n,t), one can confirm that the histograms of ciphertext images are uniformly distributed and thus can resist statistical attacks. Additionally, from Figs. 6(c,i,o,u) and 6(d,j,p,v), one can see that the histogram plots of visual encrypted image is almost similar to the histogram plots of carrier image. Therefore, it will be hard for an attacker to statistically decrypt the visual encrypted image. The horizontal, vertical and diagonal correlation coefficient values for the proposed scheme are given in Tables II, III, and IV, respectively. One can see that the correlation coefficient values for the ciphertext are less than zero or almost near to zero and for visual encrypted image the correlation coefficient values are almost near to the carrier image correlation coefficient values. Therefore, it is evident that the proposed encryption method can resist statistical attack. Figures 3 and 4 highlights the correlation plots for both plaintext original and ciphertext encrypted Cthead images, respectively. These plots also confirms that the correlation are reduced among ciphertext image pixel values.

C. Sensitivity attack analysis

Sensitivity attack analysis is generally used to confirm the sensitivity against single bit change in key. Lets generate two ciphertext images C_1 and C_2 with parameters $(x_0 = 0.6, y_0 = 0.07, z_0 = 0.14, x_0' = x_0, z_0' = z_0, \gamma = 3.78, \beta = 8)$ and $(x_0 = 0.6 + 10^{-15}, y_0 = 0.07, z_0 = 0.14, x_0' = x_0, z_0' = z_0, \gamma = 3.78, \beta = 8)$, respectively. One can confirm from Fig. 7(a,b), that the two ciphertext images are completely different from each other. Figure 7(c) show that the subtraction of C_1



(a)

(b)

(c)

Fig. 4: Correlation analysis plots for Cthead ciphertext image (a) horizontal (b) vertical (c) diagonal directions.

TABLE IV: Diagonal correlation coefficient analysis.

Image Type	Plaintext Image	Ciphertext Image	Carrier Image	Visual Encrypted Image	Ref. [10]	Ref. [11]
White	0.2751	-0.0014	0.6365	0.6566	-0.0228	0.0765
Monolithic Gray	1.0000	-0.0239	0.6365	0.7137	0.0375	-0.1087
Black	0.6481	-0.0388	0.6365	0.6638	0.0067	0.0890
Cthead	0.9220	0.0030	0.6365	0.6849	0.0298	0.0176

and C_2 also generate a complete different ciphertext image. The percentage difference are shown in Table V which is higher than 99% for the proposed image encryption scheme. Thus the proposed visual image encryption scheme can resist sensitivity attack effectively.

TABLE V: Key sensitivity analysis of the proposed scheme (%).

Image Type	Proposed	Ref. [10]	Ref. [11]
White	99.6399	99.0645	98.8965
Monolithic Gray	99.6457	98.7865	98.8744
Black	99.5850	98.0987	99.0034
Cthead	99.6277	98.0127	98.2986

TABLE VI: Differential attack analysis of the proposed scheme (NPCR).

Image Type	Ciphertext Images	Visual Encrypted Images	Ref. [10]	Ref. [11]
White	99.6094	91.7587	99.0067	98.7898
Monolithic Gray	99.5911	91.7374	98.0956	98.0867
Black	99.5605	91.5695	99.2189	99.3244
Cthead	99.6338	91.7923	98.6598	97.9870

TABLE VII: Differential attack analysis of the proposed scheme (UACI).

Image Type	Ciphertext Images	Visual Encrypted Images	Ref. [10]	Ref. [11]
White	33.1699	1.4400	32.6690	32.7612
Monolithic Gray	33.3000	1.4520	32.2098	32.4309
Black	33.1588	1.4528	32.6754	32.8844
Cthead	33.4451	1.4554	32.7899	32.2065

D. Differential attack analysis

Resistance against differential attacks can be verified via two important paremetrs i.e., i. Number of Pixel Change Rate (NPCR), and ii. Unified Average Change Intensity (UACI). NPCR analysis is generally used to test the number of changed pixels whereas UACI is used to calculate the ciphertext differences. Both NPCR and UACI score are directly proportional to the resistance against differential attacks. Mathematically, NPCR and UACI are given as [28]–[31]:

$$NPCR = \frac{\sum_{a=0}^{M-1} \sum_{b=0}^{N-1} D(a,b)}{M \times N} \times 100 \tag{10}$$

$$UACI = \frac{\sum_{a=0}^{M-1} \sum_{b=0}^{N-1} |C_1(a,b) - C_2(a,b)|}{256 \times M \times N} \times 100 \tag{11}$$

where $D(a,b) = 1$ when $C_1(a,b) \neq C_2(a,b)$; otherwise $D(a,b) = 0$. $C_1(a,b)$ and $C_2(a,b)$ are the encrypted images (size $M \times N$) before and after a single bit change in plaintext image, respectively. The results of NPCR and UACI tests are shown in Tables VI and VII, respectively. The higher value of NPCR and UACI for ciphertext images reveals higher security of the proposed visual encryption scheme against differential attacks. The value of NPCR and UACI are smaller for visual encrypted images. This is due to the fact that just higher frequency elements of the carrier image were changed. Most of the original information of carrier image remains the same.

E. Noise tolerant resistant analysis

The unwanted signals might be added and degradation of signals might occurred during transmission. Such unwanted signal addition in original signal is known as noise. Generally, in image applications, salt and pepper noise is common in wireless channels. Therefore the ciphertext image is exposed to salt and pepper noise of density 0.2. The resultant noisy visual ciphertext is shown in Fig. 8(a). Figure 8(b) shows

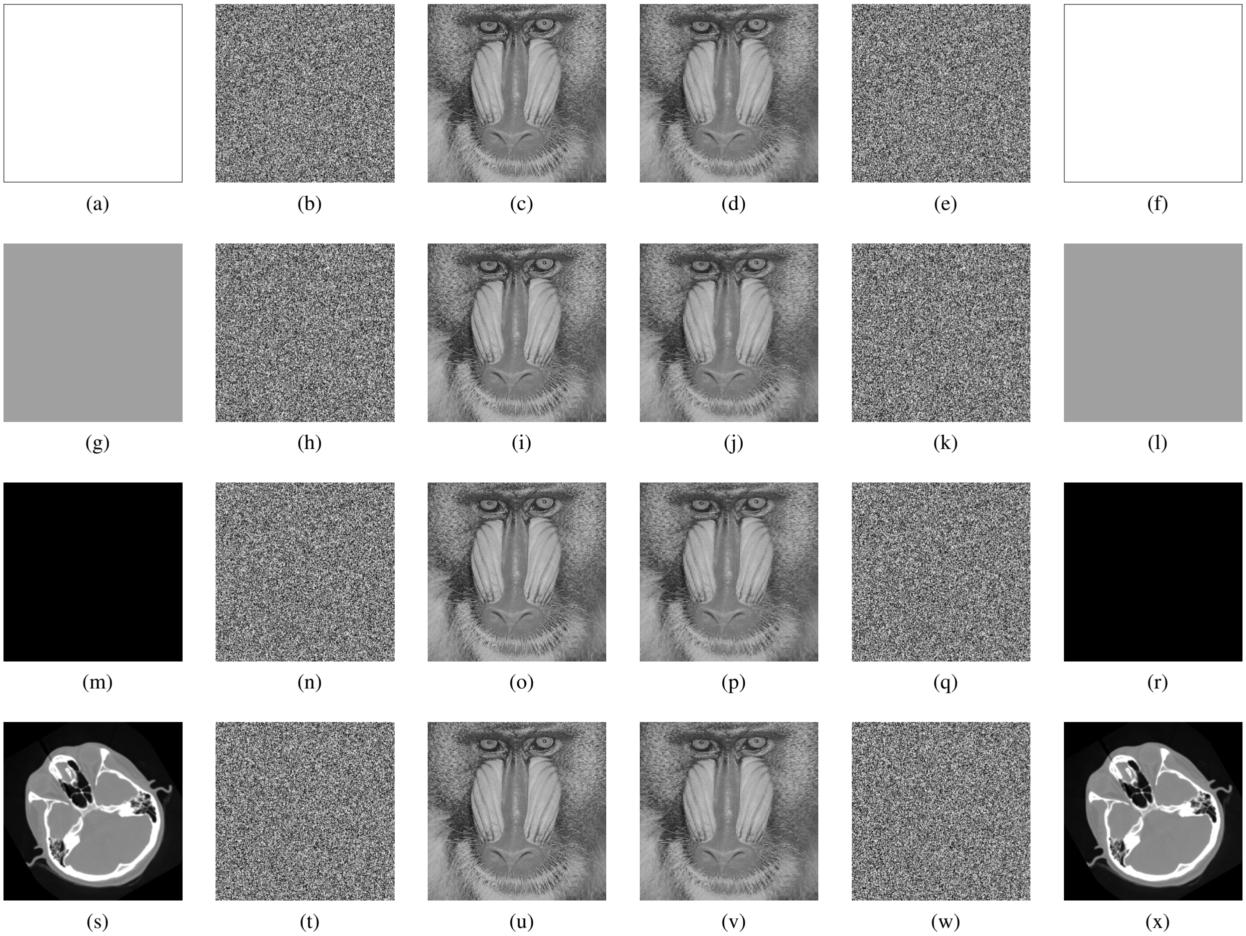


Fig. 5: Encryption and decryption result of the proposed scheme. Column (1)[a,g,m,s] are plaintext white, monolithic gray, black and Cthead images, respectively. Column (2)[b,h,n,t] are corresponding ciphertext images. Column (3)[c,i,o,u] are plaintext carrier images. Column (4)[d,j,p,v] are their corresponding visual encrypted images. Column (5)[e,k,q,w] are corresponding extracted ciphertext images. Column (6)[f,l,r,x] are corresponding decrypted images.

the decrypted image after noise addition. From Fig. 8(b) it is confirmed that decryption can be successfully performed even with noise addition. Thus, the proposed image encryption scheme can withstand noise attack as well.

F. Cropping attack analysis

In data loss attack, a part of ciphertext image data disappear. An efficient and a good encryption scheme should also resist data loss attack. In order to test this attack on the proposed scheme, first 50×50 pixels of visual encrypted image are corrupted with cropping effect. The resultant corrupted image is shown in Fig. 9(a). Figure 9(b) shows the decrypted Cthead image after cropping attack. Thus Figs. 9(a) and 9(b) confirms that the proposed encryption scheme is resistant against data loss attack.

G. Encryption quality analysis

Irregular deviation (I_D) and deviation from uniform histogram (D_H) tests are used for checking the quality of encryption. I_D measures the closeness of uniform statistical distribution. Irregular deviation is inversely proportional to the quality of an encrypted image. Ideally, the encrypted image should have a uniform histogram. A Lower value of D_H is the indication of high encryption quality. Mathematically, I_D and D_H are given by [8]:

$$I_D = \sum_{a=0}^{N-1} H_{D_a} \tag{12}$$

where,

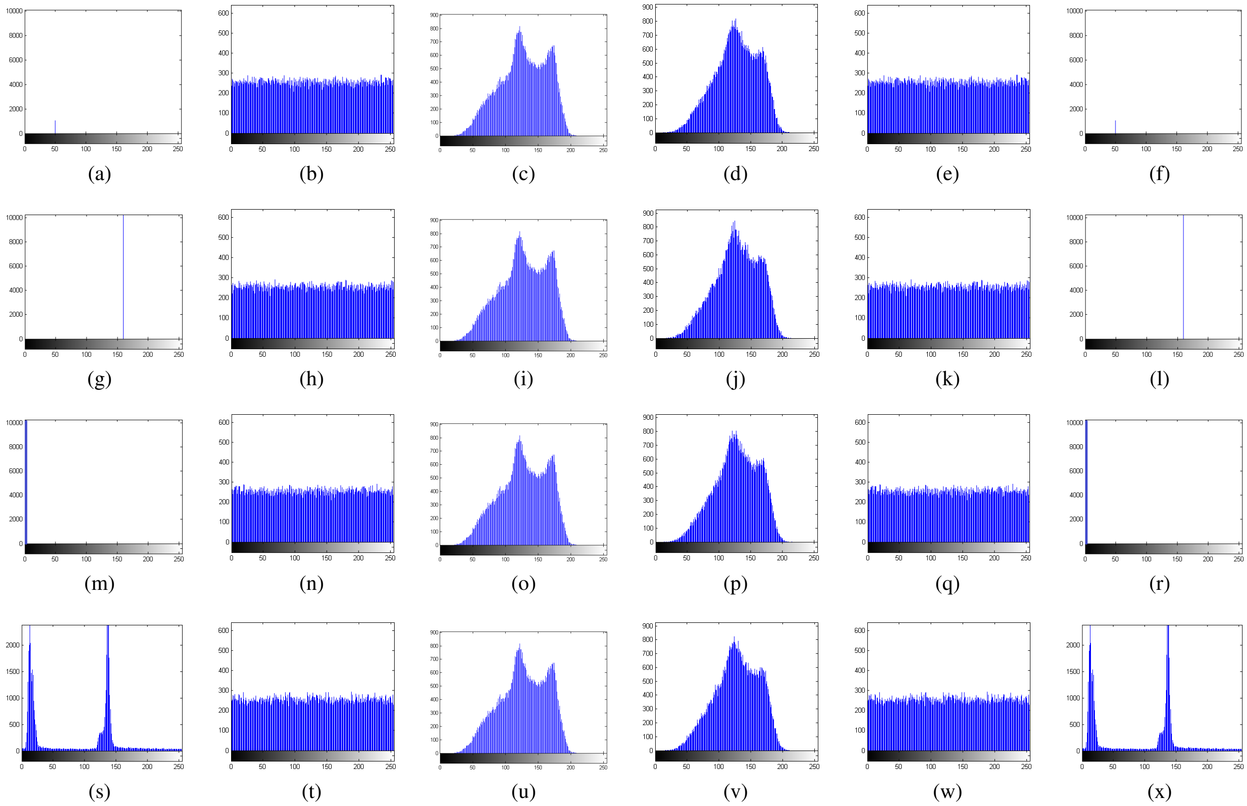
$$H_{D_a} = |H_a - M_H| \tag{13}$$

$$H_a = Histogram(D) \tag{14}$$

$$M_H = \frac{1}{N}\sum_{a=0}^{255} h_a \tag{15}$$

$$D_H = \frac{\sum_{C_a=0}^{255} |H_{C_a} - H_C|}{M \times N} \tag{16}$$

where h_a is the a_{th} index value of histogram. D is the absolute difference. H_{C_a} is the i_{th} index value of an ideal histogram. H_C is the original histogram. The computed values of I_D and D_H for different images are shown in Tables VIII and IX, respectively. Smaller values of I_D and D_H confirms

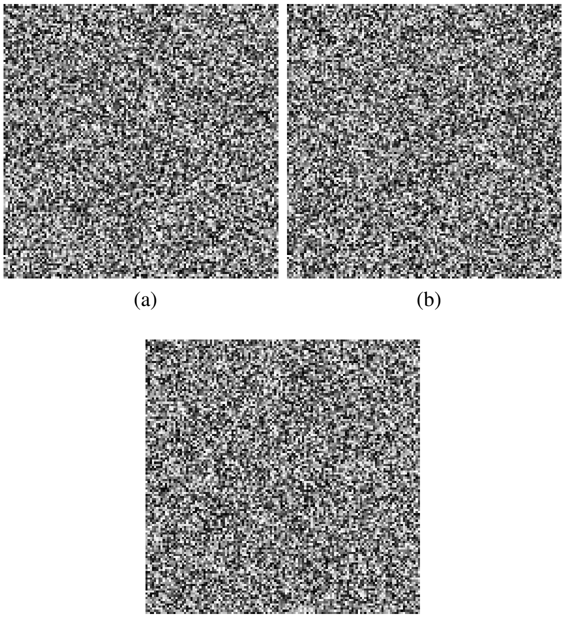

(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

(m) (n) (o) (p) (q) (r)

(s) (t) (u) (v) (w) (x)

Fig. 6: Histogram plots of the proposed scheme. Column (1)[a,g,m,s] are plaintext white, monolithic gray, black and Cthead histograms, respectively. Column (2)[b,h,n,t] are their corresponding ciphertext histograms. Column (3)[c,i,o,u] are plaintext carrier image histograms. Column (4)[d,j,p,v] are their corresponding visual encrypted histograms. Column (5)[e,k,q,w] are corresponding extracted ciphertext histograms. Column (6)[[f,l,r,x] are corresponding decrypted images histograms.


(a) (b)

(c)

Fig. 7: Key sensitivity plots (a) $C_1(x_0 = 0.6, y_0 = 0.07, z_0 = 0.14, x'_0 = x_0, z'_0 = z_0, \gamma = 3.78, \beta = 8)$ (b) $C_2(x_0 = 0.6 + 10^{-15}, y_0 = 0.07, z_0 = 0.14, x'_0 = x_0, z'_0 = z_0, \gamma = 3.78, \beta = 8)$ (c) difference of C_1 and C_2.

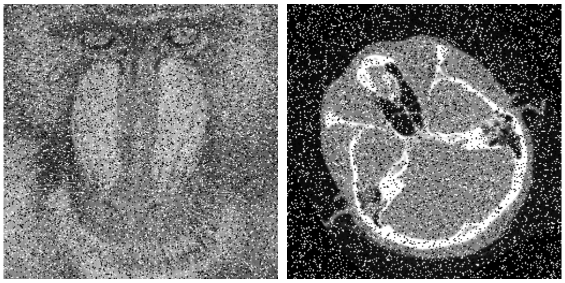
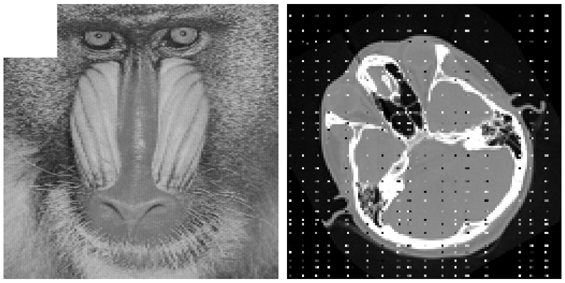

(a) (b)

Fig. 8: Noise tolerant plots (a) Visual encrypted image with salt and pepper noise of density level 0.2 (b) Decrypted Cthead image with some noise distortion.

the good quality of the proposed visual image encryption scheme is achieved. As we have changed only the higher frequency components in carrier image, therefore the values of I_D and D_H for visual encrypted image is higher. This further confirms that the visual encrypted image is less deviated from the carrier image.

H. Homogeneity

Homogeneity determines, how closely the elements in the Gray-Level Co-occurance Matrices (GLCM) are distributed to



(a)

(b)

Fig. 9: Cropping analysis plots (a) Visual encrypted image cropped with first 50×50 pixels(b) Decrypted Cthead image with some noise distortion.

TABLE VIII: Encryption quality analysis of the proposed scheme (I_D).

Image Type	Plaintext and ciphertext image	Carrier and visual encrypted image
White	1538	108384
Monolithic Gray	12558	108404
Black	1564	108312
Cthead	6420	108364

the GLCM diagonal. GLCM shows the statistical combinations of pixel grey levels in tabular form. The GLCM table also determines the frequency of the patterns of different pixel gray levels. Mathematically, Homogeneity is defined as:

$$Homogeneity = \sum_{a,b} \frac{P(a,b)}{1+|a-b|} \tag{17}$$

where the gray-level co-occurrence matrices in GLCM is represented by $P(a,b)$. From Table X, one can see the smaller values of homogeneity for the proposed visual image encryption scheme. These smaller values of homogeneity reflects a higher secure nature of the proposed image encryption.

I. Contrast

For an image, contrast analysis calculates the intensity differences between two neighbouring pixels. Through contrast analysis, the viewer clearly identifies the object in texture of an image. For a strong image encryption scheme, higher contrast is required as it verifies that the texture is non-homogeneous. Mathematically, contrast is given by:

$$Contrast = \sum_{a,b}^{N} |a-b|^2 P(a,b) \tag{18}$$

where $P(a,b)$ computes the number of GLCM matrices and N demonstrates the grand total of rows and columns. Values of contrast for the proposed scheme is shown in Table X. Higher contrast values in Table X reveals the higher security of the proposed scheme.

TABLE IX: Encryption quality analysis of the proposed scheme (D_H).

Image Type	Plaintext and ciphertext image	Carrier and visual encrypted image
White	3.0000	3.7656
Monolithic Gray	3.0000	3.7683
Black	3.0000	3.7703
Cthead	3.0000	3.7690

J. Energy

Energy is the statistical measurement of texture that considers the spatial relationship of pixels in the GLCM. Mathematically, energy of a ciphertext image is given by:

$$Energy = \sum_{a,b} P(a,b)^2 \tag{19}$$

where $P(a,b)$ is the number of GLCM matrices. Energy values obtained for the proposed visual image encryption scheme are given in Table X. The lower values of energy confirms a higher degree of disorderedness in the ciphertext image.

K. Computation analysis

The computation speed basically tells about the time required to generate a ciphertext image and then to embed that cipher data into the carrier image. The simulations are performed on Matlab 2013a, Intel Core i3-380M (2.53 GHz) Central Processing Unit (CPU) with 4 GB RAM. For 256×256 image, the scheme in [10] takes around 2.85 seconds while the scheme in [11] takes 2.71 seconds. The proposed visual image encryption scheme executes in around 2.94 seconds. The proposed algorithm executes in a little higher times than the related algorithms, this is because of the extra key computation using DNA and SHA-512 in the proposed visual encryption scheme.

IV. Conclusion

A DNA key-based visual image encryption scheme using quantum chaotic map is suggested in this article. Initial conditions of the map are computed from a DNA (Deoxyribonucleic acid) sequence, plaintext image, and SHA-512 hash function. Three random vectors are generated through DNA, plaintext, and SHA-512 based initial conditions. Out of three random vectors, first two random vectors are used for correlation breaking through row and column permutation. The third random matrix is arranged in a matrix form which is used in XORed operation. In order to resist the proposed scheme against well-known cryptographic attacks, the ciphertext is transformed from noise-like texture to visually encrypted image. The diffused image is divided into Least Significant Bit (LSBs) and Most Significant Bits (MSBs). Furthermore DWT is applied on the carrier image. The HL and HH blocks or the higher frequency blocks of the carrier image are replaced with LSBs and MSBs of the diffused image. On the basis of

TABLE X: Homogeneity, contrast and energy tests values for the proposed scheme.

Image Type	Homogeneity	Ref. [10]	Ref. [11]	Contrast	Ref. [10]	Ref. [11]	Energy	Ref. [10]	Ref. [11]
White	0.3798	0.4588	0.5521	10.4780	10.1892	10.0094	0.0151	0.0228	0.0276
Monolithic Gray	0.5438	0.5599	0.3897	10.4083	9.7643	10.1009	0.0157	0.0189	0.2009
Black	0.3894	0.4759	0.5109	10.4398	10.0572	9.6500	0.0144	0.0243	0.0199
Cthead	0.3924	0.6443	0.5288	10.4820	9.5509	9.0012	0.0161	0.0257	0.0231

TABLE XI: Notations and abbreviations.

Acronyms	Abbreviations	Acronyms	Abbreviation
bin2dec	Binary to Decimal	imread	Reading in Image
C	Cipher Image	IDWT	Inverse Discrete Wavelet Transform
CI	Carrier Image	K	Key
C_1	Cipher Image 1	LL	Low-Low
C_2	Cipher Image 2	LH	Low-High
Corr	Correlation Coefficient Value	LSBs	Least Significant Bits
Covar	Covariance	$LSBs_{Matrix}$	Least Significant Bits Matrix
Col_{Per}	Column Permutation	MSBs	Most Significant Bits
DataHash	Hash Function	$MSBs_{Matrix}$	Most Significant Bits Matrix
D_H	Uniform Histogram	NPCR	Number of Pixel Change Rate
DNA	Deoxyribonucleic acid	P	Plaintext image
DWT	Discrete Wavelet Transform	PWLCM	Piecewise Linear Chaotic Map
$Diffused_{image}$	Diffused Image	Row_{Per}	Row Permutation
GLCM	Gray-Level Co-occurance Matrices	S-Box	Substitution Box
H	Entropy	SHA-512	Secure Hash Algorithm 512
HL	High-Low	UACI	Uniform Average Change Intensity
HH	High-High	λx	Standard Deviation of x
hex2dec	Hexadecimal to Decimal	λy	Standard Deviation of y
I_D	Irregular Deviation		

the experimental analyses i.e., sensitivity attack, brute force attack, statistical attack, noise tolerant resistant, cropping attack, encryption quality, homogeneity, contrast and energy, we confirmed that the proposed visual image encryption scheme can withstand attacks. Additionally, the proposed visual image encryption algorithm is also noise resistant.

References

[1] R. Matthews, "On the derivation of a cchaotic encryption algorithm," *Cryptologia*, vol. 8, no. 1, pp. 29–41, 1989.

[2] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[3] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.

[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*. IEEE, 2015, pp. 1–6.

[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] 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.

[7] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and xor operation," *Neural Computing and Applications*, pp. 1–11, 2017.

[8] J. S. Khan, M. A. Khan, J. Ahmad, S. O. Hwang, and W. Ahmed, "An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes," *Informatica*, vol. 28, no. 4, pp. 629–649, 2017.

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

[10] W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "Image salient regions encryption for generating visually meaningful ciphertext image," *Neural Computing and Applications*, vol. 29, no. 3, pp. 653–663, 2018.

[11] L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryp-

tion scheme," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7397–7407, 2018.

[12] 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.

[13] P. Li, C.-N. Yang, and Q. Kong, "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 41–50, 2018.

[14] Q. Zhang, L. Guo, and X. Wei, "Image encryption using dna addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[15] L. Liu, Q. Zhang, and X. Wei, "A rgb image encryption algorithm based on dna encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[16] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[17] 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.

[18] Y. Tian and Z. Lu, "Novel permutation-diffusion image encryption algorithm with chaotic dynamic s-box and dna sequence operation," *AIP Advances*, vol. 7, no. 8, p. 085008, 2017.

[19] 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.

[20] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[21] W. Stallings, "Cryptography and network security, 1999 prentice-hall," *Inc., Upper Saddle River, New Jersey*.

[22] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 4653–4661, 2012.

[23] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dynamics*, vol. 81, no. 1-2, pp. 511–529, 2015.

[24] A. A. A. El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[25] H. Liu and C. Jin, "A novel color image encryption algorithm based on quantum chaos sequence," *3D Research*, vol. 8, no. 1, p. 4, 2017.

[26] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[27] 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.

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

[29] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[30] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices," *Neural Computing and Applications*, vol. 28, no. 1, pp. 953–967, 2017.

[31] X.-y. Wang, F. Chen, and T. Wang, "A new compound mode of confusion and diffusion for block encryption of image based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2479–2485, 2010.