Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/090309

Quantum Colour Image Encryption Algorithm Based on DNA and Unified Logistic Tent Map

R. Sridevi and P. Philominathan*

Department of Physics, A.V.V.M. Sri Pushpam College, Thanjavur, Tamil Nadu, India

Received: 7 Feb. 2020, Revised: 18 June 2020, Accepted: 22 June 2020.
Publishedonline:1 Sep 2020.

Abstract: This paper presents a Quantum encryption technique which is built by adopting Haar Integer Wavelet Transform (HIWT), RC6 (Rivest Cipher) block cipher and DNA (deoxyribonucleic acid) sequences. A Unified Chaotic Logistic Tent Map (ULTM) has been employed in the permutation phase to produce the pseudo-random sequence for shuffling the RGB planes of the Quantum represented source image in spatial and transform domains. HIWT is adapted to extract various subband information from the Quantum represented source image. Then RC6 block cipher encryption is used to encrypt LL subband which contains an informative part of an image. Further, it is encoded based on the DNA sequence order and performed DNA-XNOR operation. The proposed encryption algorithm is implemented using Novel Enhanced Quantum Image Representation (NEQR) on various test images with statistical and differential attack analyses. This technique yields average entropy of 7.992, correlations of horizontal -0.000043, vertical 0.00002, diagonal -0.02204 and a larger keyspace of 10^{204} respectively. By various analyses, it has confirmed the significant immune level of the Quantum cryptosystem.

Keywords: NEQR, Haar IWT; RC6; DNA; Combined chaotic maps; Image encryption; FPGA- reconfigurable hardware.

1 Introduction

The public network systems have been rapidly elaborated by increasing the speed of data communication, by processing information which becomes significant attention for cyber-attacks. Quantum image encryption has captivated considerable attention from both scientists and engineers in the last couple of years [1-17]. Quantum computation has become an innovative tool for meeting with real-time computational requirements [18-23]. Quantum image encryption intends to carry out the tasks that are not achieved or intractable with conventional image encryption. Digital data transmission through an open medium attains an enormous demand for security and privacy. Among all other multimedia objects, digital images were used for information sharing due to their bulk data capacity [1]. Encryption is the efficient technique which is adapted for securing the images. Conventional encryption algorithms are not appropriate for digital colour images because of their weak correlation and more rounds of operation. Hence an effective image encryption algorithm is needed to protect it. The approach of chaos theory in image encryption gained a significant role due to its ergodicity, stochasticity and haphazardness properties [2]. Chaotic maps play a curial role in random number generation, which directly influences the encryption process. It can be a multi-dimensional mathematical model which requires an initial condition and seeds to trigger it. The keyspace of the cryptosystem has been improved by cascading more number of 1D chaotic maps [3].

Pak and Huang proposed a combined chaotic scheme for RGB colour image encryption where chaotic logistic, sine and Chebyshev maps are used. The chaoticity of the newly generated chaotic map has been evidenced through the bifurcation diagram and Lyapunov exponent. Further, this is carried out in three states such as permutation, diffusion and linear transformation. This work is evaluated using statistical, differential and error metric analyses where the encryption time has not been discussed [4]. Assad and Farajallah suggested an encryption technique through bit-level permutation followed by pixel level diffusion in which a modified 2D cat map has been used for the permutation process. This method takes 8.38 mS to perform encryption where entropy, correlation and histogram analyses have been conducted to witness it [5]. Zhou et al. experimented image encryption through combined chaotic maps which take logistic, sine and tent chaotic systems merged to form a new map. To perform encryption, the original image is separated for rows, and 1D substitution has been performed using a combined chaotic system who's chaotic behaviour is evaluated through the bifurcation diagram and Lyapunov exponent. This method requires four rounds of operation to achieve proper encryption [6].

Heterogeneous bit permutation technique is introduced by Wang and Zhang, in which the colour image encryption uses the chaotic sequences of correlated chaos. The initial parameters of chaos have been generated through SHA – 256, which enhances security. Further, key sensitivity, differential attack and NIST tests analyses have been

*Corresponding author e-mail: amir@ece.sastra.edu

performed to ensure the strength of encryption [7]. Wang et al. [8] propose a technique where confusion, diffusion, and 2D logistic maps are used to form random sequence matrices. These matrices permutated the pixel values of colour images where XOR operation is employed in each round to produce cipher image. However, the number of rounds of operation for this encryption has not been reported. Liu and Wang proposed RGB image encryption with Piece-Wise Linear Chaotic Map (PWLCM) and Chen chaotic system. A colour image has been decomposed into its gray levels and converted as matrices. The generated random sequences by PWLCM are used for scrambling, whereas diffusion is performed using XOR function with the chaotic sequences produced by Chen chaotic system [9].

Murillo – Escobar *et al*., proposed fast RGB image encryption using the 1D logistic map with optimized distribution to lessen the time complexity. Permutation and substitution processes have been carried out through chaotic sequences which are produced by the logistic map to accomplish the encryption [10]. Patidar *et al*., developed an image scheme which is equivalent to the existing PPS09 cryptosystem through chaotic standards and logistic map. This work mainly focuses on the solutions for chosen plain and known-plaintext attacks analyses [11]. Other than 1D chaotic maps and hyperchaos also introduced in image encryption through which keyspace and randomness of encryption were increased [12-14]. In chaos system attractors are also a classification of three or four-dimensional chaotic maps with more number of control parameters to enhance the security [15-17].

By the advancement of technology, the process of encryption based on DNA computation has drilled into various fields. Chaotic maps are combined with other techniques such as DNA to enhance security. One such work is illustrated by Wu *et al*., in which DNA encoding with chaotic maps plays a crucial role. In these three different chaotic maps are adopted for generating random sequences where DNA addition and XOR operations have been performed to form cipher image [24]. Though this work yields acceptable correlation, the entropy of cipher images needs to be further improved. Jiahui Wu et al. suggested an image encryption technique for a grayscale based on DNA approach by 2D-HSM secrete key and achieve entropy of 7.9976 and keyspace of 10^112. And stated by utilizing DNA technique, the encryption technique improves the computing efficiency [25]. Rasul Enayatifar et al. proposes a permutation and diffusion based on DNA sequence and image indexes by employing DNA sequence provides the algorithm more power to oppose various attacks with entropy 7.999 [26].

Xiuli Chai et al. suggested a cryptosystem based on DNA for the colour image by intra-inter permutation. For generating a random key 4D hyperchaotic map is used, which has better performance to resist attacks [27]. Aqueel et al. suggested an inter-intra substitution for the pixels by DNA sequence for reducing the redundancy of the algorithm. To generate the random, secrete key logistic map, PWLC map, are adopted for operating the encryption algorithm and achieved entropy of 7.9973 [28]. A DNA based colour image encryption is suggested by Xiangjun Wu et al. using the NCA map. To enhance security, DNA addition, subtraction, XOR techniques were used in this cryptosystem [29]. Dhivya et al. suggested work on securing medical image by DNA blend chaos, where permutation encoding, and substitution is performed to achieve an encrypted image in the spatial domain [30]. Mengmeng Guan et al. suggested image encryption on frequency domain by DNA and hyperchaos for its unprecedented advantages and achieved entropy of 7.9923 [31].

Likewise, many DNA based cryptosystem has been intended for image encryption for its high performance, extensive parallelism, large storage, etc. and implemented on the spatial domain. Comparing the frequency domain (FD) with the spatial domain (SD), the FD is steadier and high immune to tamper than SD. In time FD, there are several wavelets renders lossless decryption and suppress floating-point values by indicating integer to integer values. To intensify the security level for the encryption algorithm, both the spatial and frequency domains have been adopted [32-41].

Therefore, the outstanding performance of the chaos-DNA approach has influenced to utilize in the proposed encryption method for the dual domain. The proposed method presents a unique duo scrambling on spatial and transforms the domain approach for the image encryption scheme. The digital colour image provides enormous amounts of information and contains integral pixel values, which are directly mapped as integers for HIWT without incorporating any truncation or rounding error. Hence HIWT is chosen in this proposed scheme where two-dimensional HIWT fragments the image into LL, LH, HL, HH subband coefficients.

To randomize the data distribution, chaotic map-based data and pixel selection algorithms have been used before the HIWT. An RC6 block encryption algorithm is employed to encrypt the LL sub-band. Additional, it is encoded by DNA rule 1 and DNA XNOR operation is performed. The other subbands LH, HL, HH, are permutated each by row and column-wise with the developed ULTM key.

Feynman in 90s introduces Quantum principle operating computers, which allow dissimilar likely inputs which obey coherence and superposition principle. Quantum image encryption is consummated through the properties of quantum mechanics such as the quantum no-cloning theorem and the Heisenberg uncertainty principle which can effectively reduce calculation complexity, speed up processing tasks and secure information transmission

[42].

Quantum encryption is well known to the promise of virtually unbreakable encryption. In order to effectively compile quantum image, a variety of illustration models have been springing up to tackle images in equivalent quantum representations [43]. Qubit Lattice Representation which stores the gray information by transforming the frequency of electromagnetic waves to quantum states, Entangled image, Real Ket representation to encode quantum image by using quantum states and coefficients, Flexible Representation of Quantum Image(FRQI) which requires only 2n+1 qubits [44,45]. When encoding an image, Multi-Channel Quantum Image Representation (MCQIR), log-polar and Novel Enhanced Quantum Representation (NEQR) which requires more qubits, grayscale information is stored in a sequence of qubits.

The significant contributions of this work are as follows,

1. Quantum cryptosystem has been implemented using NEQR format with dual confusions in spatial as well as in transform domains
2. A combined chaotic map is developed, and random sequences were generated with different seeds and initial conditions
3. HIWT has been adopted for subbands classification which is free from round-off errors
4. Lightweight block encryption algorithm such as RC6 has been utilized for diffusion which improves the sensitivity of the encryption scheme
5. A DNA encoding along with DNA-XNOR technique has been operated, which requires only one round of operation to yield more reliable security.

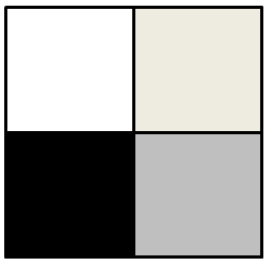
2 Preliminary

2.1 Novel Enhanced Quantum Representation (NEQR)

It is used to symbolize the equivalent quantum image format representation of classical image input. This method utilizes the qubit sequence which is entangled to accumulate the pixel and its position values [46]. The primary benefit of using this representation is that it reveals a sharp quadratic drop. q+2n qubits are required to handle images of size $2^n \times 2^n$ as in Figs 1-3.

$$|\psi\rangle = \frac{1}{2^n}\sum_{M=0}^{2^n-1}\sum_{N=0}^{2^n-1}|g(M,N)\rangle \otimes |MN\rangle$$

Where g(M, N) represents the conventional image pixel values and $g(M, N) \in [0, 2^q-1]$.



$|I\rangle = \frac{1}{2}|255\rangle\otimes|00\rangle+|125\rangle\otimes|01\rangle+|0\rangle\otimes|10\rangle+|200\rangle\otimes|11\rangle$

$|I\rangle = \frac{1}{2}|11111111\rangle\otimes|00\rangle+|01111101\rangle\otimes|01\rangle+|00000000\rangle\otimes|10\rangle+|11001000\rangle\otimes|11\rangle$

Fig. 1.a NEQR representation of a 2 × 2 grayscale image.

2.2 SWAP gate

It swaps the two-qubit states. The swap gate is prepared using three CNOT gates. The sequence is as follows. The inputs are |A⟩, |B⟩. The output of the first CNOT gate is |A, A⊕B⟩. This is given to the second CNOT gate (Fig 2) and the output of the second CNOT gate is |A⊕(A⊕B), A⊕B⟩ = |B, A⊕B⟩. The output of third CNOT gate is |B, B⊕(A⊕B)⟩ = |B, A⟩.

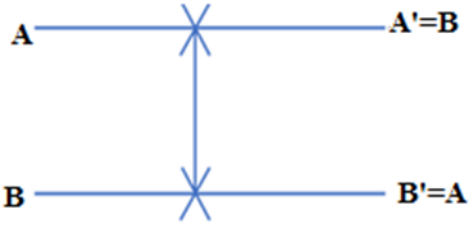


Fig. 2: Representation of SWAP gate.

2.3 CONTROLLED NOT gate

The wire-level representation of Controlled NOT gate is shown in Fig 3. In the diagram, control qubit and target qubit acts as inputs. The circuit representation of the CNOT gate is shown in figure 2. The topmost line represents the control qubit, while the bottom line represents the target qubit. The act of the gate is described as follows. The control bit decides the target output either to flip or to remain in the same state.

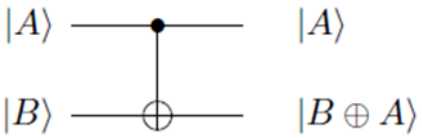


Fig. 3. Wire representation of Controlled NOT gate.

2.3 DNA

A deoxyribonucleic acid (DNA) sequence has been widely used in numerous fields for its extensive parallelism, unique storage capacity, data processing range, low power dissipation. There is nucleic acid present in DNA they are adenine, cytosine, guanine and thymine. These are

complementary base pairing in which, A bond with *T* and *C* bond with *G* follows the principle of Watson–Crick. Meanwhile, in the binary system 0 and 1; 00 and 11; 01 and 10 are a complement to one another [38].

For illustration, an 8-bit grayscale image can be encoded by DNA base orders. A pixel value is 10000101 is encoded as GACC by rule 1 as per Table 1. A DNA XNOR sequence in Table 2 is performed in this proposed algorithm.

Table 1: DNA sequencing.

1	A – 00	T - 11	C - 01	G – 10
2	A – 00	T - 11	C - 10	G – 01
3	A – 11	T - 00	C - 10	G – 01
4	A – 11	T - 00	C - 01	G – 10
5	A – 10	T - 01	C - 00	G – 11
6	A – 01	T - 10	C - 00	G – 11
7	A – 10	T - 01	C - 11	G – 00
8	A – 01	T - 10	C - 11	G – 00

Table 2: DNA XNOR Rule.

XNOR	**00**	**11**	**01**	**10**
00	11	00	10	00
11	00	11	00	10
01	10	00	11	00
10	00	10	00	11

2.4 Haar Integer Wavelet Transform

HIWT is one of the fascinating transformation methods that transform the data from a spatial to the frequency domain. It possesses an energy compaction property that has been widely applied to resolve the signal and image processing problems [40],[41]. The lifting schemes are employed to perform IWT, which manipulates the matrices using the process of averaging and differencing. The two-dimensional transformation is done by applying the lifting scheme sequentially to the image's rows as well as columns, as shown in Fig. 4.

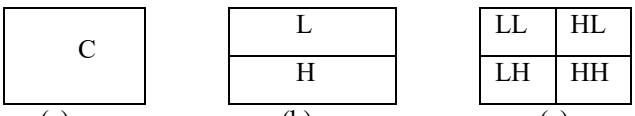


Fig. 4: (a) Input image with size M × N, (b) First level decomposition and (c) Second level decomposition.

Where, HH-vertical and horizontal high pass, HL-vertical low pass and horizontal high pass, LH- vertical high pass and horizontal low pass and LL-vertical and horizontal low pass. Eq. 1 and 2 are used to obtain the 2D integer wavelet transform.

Decomposition in 1D and 2D are given as follows:

$$H_1 = P_o - P_e$$

$$L_1 = P_e + (H/2 \tag{1}$$

Here, P_o = odd column pixels

P_e = even column pixels

H_{odd} = odd row H_1

L_{odd} = odd row of L_1

H_{even} = even row of H_1

L_{odd} = even row of L_1

$$LH_1 = L_{odd} - L_{even}$$

$$LL_1 = L_{even} + [LH / 2] \tag{2}$$

$$HH_1 = H_{odd} - H_{even}$$

$$HL_1 = H_{even} + [HH/ 2]$$

2.5 Unified Chaotic Logistic Tent Map (ULTM)

ULTM is procured from two 1D chaotic maps, i.e. logistic and tent maps. Both the maps are simultaneously driven using the initial values and optimal control parameters to enhance the randomness. The chaotic maps are very sensitive to minimal changes in the control parameter and initial value, which produce an extensive, unpredictable sequence. To further enhance the randomness and to extend the seed length, a combination of both the maps has been proposed. On combining the seed maps, a multistage expansion in the chaotic range of the proposed system is observed when compared to its seed maps by performing bifurcation analysis and its stability was verified through bifurcation and Lyapunov analysis (Figs. 5-7). The mathematical expressions relating to the logistic map, tent map and the proposed ULTM map is expressed below.

Logistic Map: It is a 1-dimensional chaotic map which is defined as eq. 3 [8].

$$P(n+1) = l(P(n), r) = r * P(n) * \big(1 - P(n)\big) \qquad 0 < P_N < 1 \tag{3}$$

Tent Map: The chaotic tent map is defined as eq.4 [24].

$$P(n+1) = t(P(n), u) = \begin{cases} u * \dfrac{P(n)}{2} & 0 < P(n) < 0.5 \\ u * \dfrac{\big(1 - P(n)\big)}{2} & 0.5 \le P(n) < 1 \end{cases} \tag{4}$$

Unified Logistic Tent

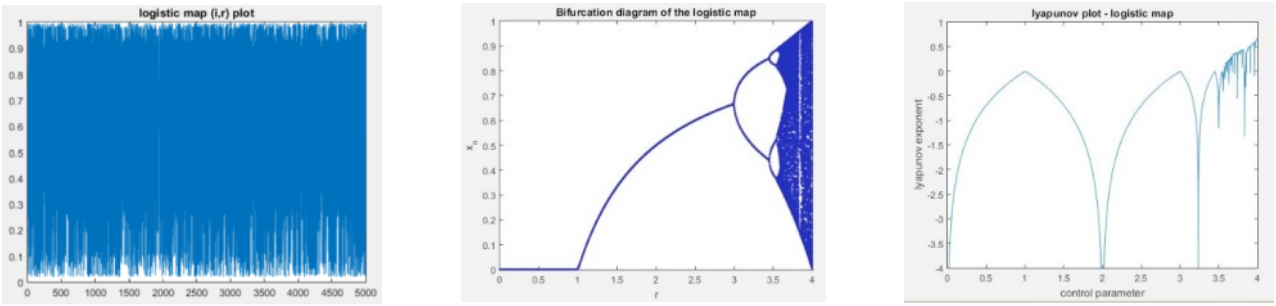
$$P(n+1) = tl(P(n), r, u) = \begin{cases} \mod\left(\left(r * P(n) * (1 - P(n))\right) + \left(u * \frac{P(n)}{2}\right), 1\right) & 0 < P(n) < 0.5 \\ \mod\left(\left(r * P(n) * (1 - P(n))\right) + \left(u * \frac{1 - P(n)}{2}\right), 1\right) & 0.5 \le P(n) < 1 \end{cases}$$

Microsoft word has been used widely in writing scientific Where P(n) denotes the current value, r denotes the logistic map control parameter, and u denotes the control parameter for tent map. The initial condition values are r=3.49, p(n)=0.1 and u=0.585 for logistic and tent map respectively. The control parameters can lie in the range of r(0,4); p(n)=(0,1);u=(0,4).

3 Proposed Methodology

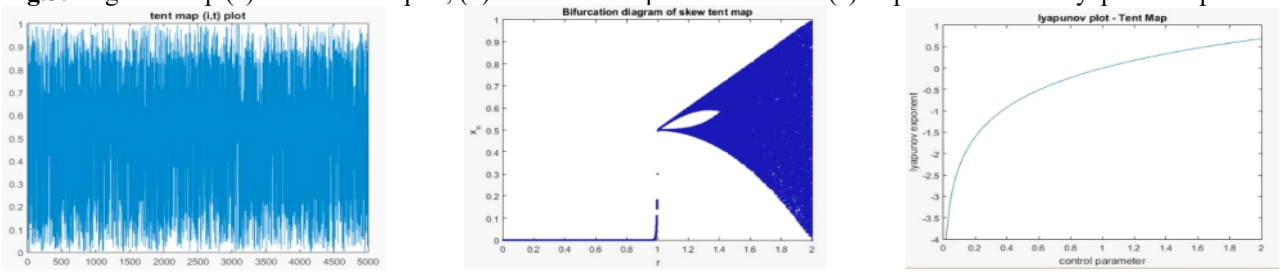
Fig. 8 represents the block illustration of the proposed transformation stage, diffusion stage and inverse encryption scheme. This algorithm comprises of four stages for encrypting the M × N image, i.e. permutation stage, transformation stage. Fig 9 represents an example of DNA encoded based upon rule 1, DNA-XNOR operation, further DNA decoded to achieve a final encrypted LL sub-band.

During the permutation stage, ULTM based pseudo-random sequences are used to permute the depiction according to row, column and block-wise respectively. In the transformation stage, Integer wavelet transform generates the wavelet coefficient from the permutated image. In the diffusion stage, RC6 block cipher encryption algorithm and DNA-XNOR is employed to encrypt the LL coefficient. Moreover, confusion in HH, HL and LH coefficients itself provides diffusion. The encryption algorithm is given below:



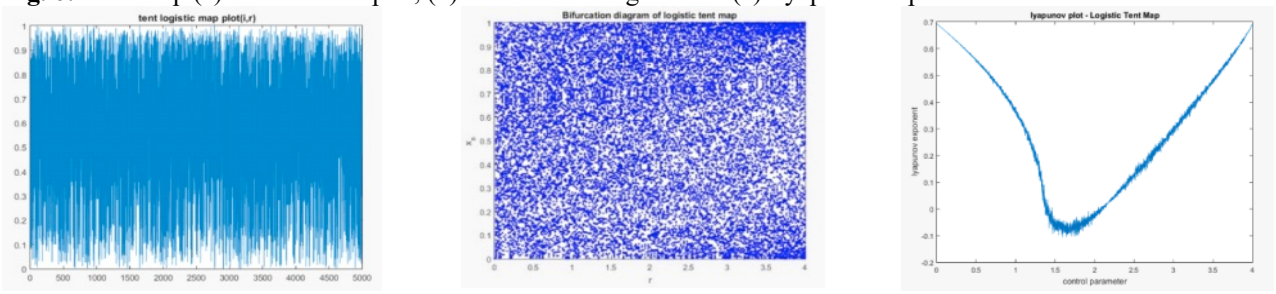
(a) (b) (c)

Fig.5: Logistic Map (a) Randomness plot, (b) Bifurcation representation and (c) Representation of Lyapunov exponent.



(a) (b) (c)

Fig. 6: Tent Map (a) Randomness plot, (b) Bifurcation diagram and (c) Lyapunov exponent.



(a) (b) (c)

Fig. 7: Unified Logistic Tent Map (a) Randomness plot, (b) Bifurcation diagram and (c) Lyapunov exponent.

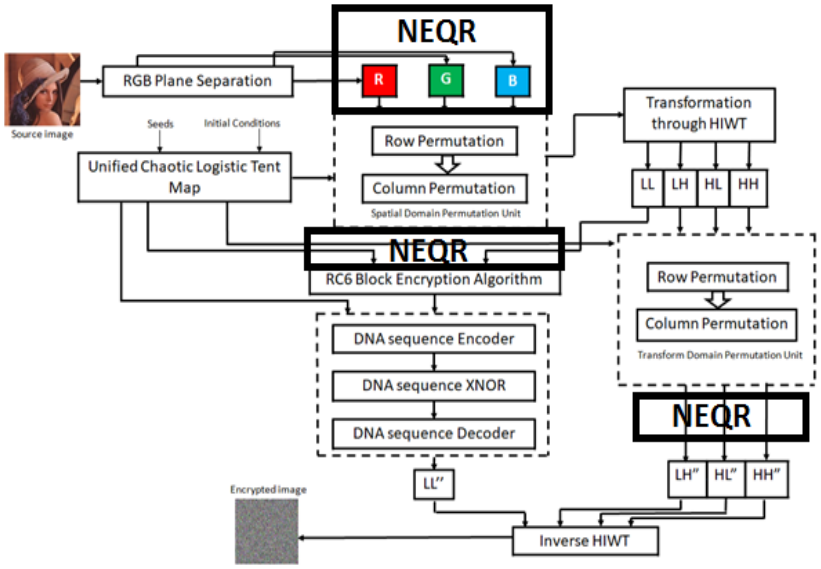


Fig. 8: Representation of the Quantum encryption scheme.

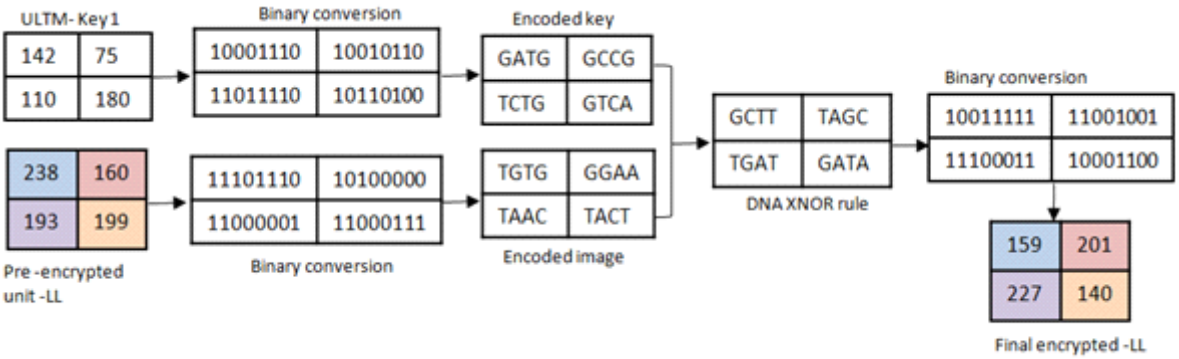


Fig. 9: Block diagram of the DNA encoding and an XNOR operation with ULTM key.

3.1 Encryption Procedure

BMP colour image named P of dimension 256 × 256 × 3 is taken as input and produces a cipher image named C by performing the following steps.

Step 1: Image is separated into R, G & B planes and NEQR format is applied to each plane in-order to attain the

Quantum representation of the classical image.

Step 2: Pseudo-random numbers are generated by the combined chaotic scheme, i.e. ULTM

Step 3: Row and column permutation have been performed individually using values generate in step 2

Step 4: Permuted RGB planes are divided into 8 × 8 blocks.

Step 5: HIWT is applied to each 8 × 8 blocks to generate LL, LH, HL and HH subbands.

Step 6: Row permutation is performed on LH, HL & HH to generate HL*, LH* & HH*.

Step 7: Column permutation is performed on LH*, HL*, HH* to generate HL", LH" & HH"

Step 8: Key sequence K of 128 bit is generated using combined chaotic scheme – ULTM.

Step 9: Pre-encryption is carried over the LL band using the generated key sequence K to drive the RC6 block cipher

Step 10: Then it is encoded based on DNA rule 1 and performed a DNA-XNOR operation to enhance LL-encrypted image. DNA – XNOR is performed using CNOT and Cswap gates, respectively.

Step 11: Apply inverse HIWT on the subband coefficients

to obtain final cipher image C.

Step 12: To perform decryption, the reverse process of encryption has been carried out.

Fig 10 and 11 provide the wire diagram illustration of the encryption and decryption algorithms, respectively.

4 Experimental Results

HIWT image encryption technique is implemented using MATLAB R2016b. The feasibility and effectiveness of the projected encryption algorithm is assessed by different security metrics such as correlation, information entropy and key sensitivity analysis. The original and cipher images are depicted in Fig. 12 (a, c) and 13 (a, c).

4.1 Uniform Histogram Analysis Estimation

The histogram representation of the original image and its corresponding cipher image are depicted in Fig. 12 (b, d) and Fig. 13 (b, d). By the results, it proves that unlike the original image, encrypted image possesses uniform sharing attribute, which is robust towards various attacks.

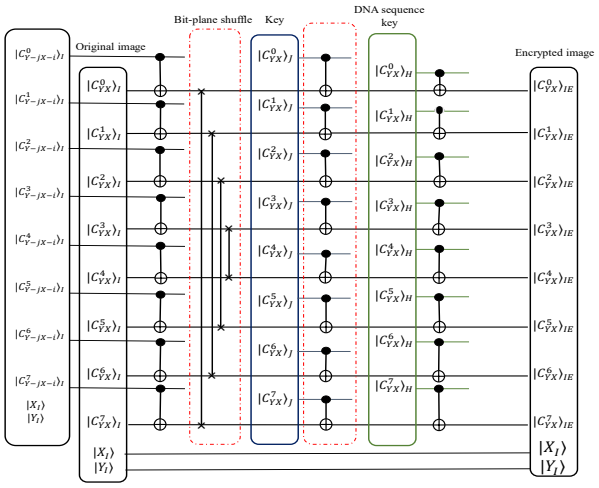


Fig. 10: Wire diagram of the sub section of the proposed encryption architecture.

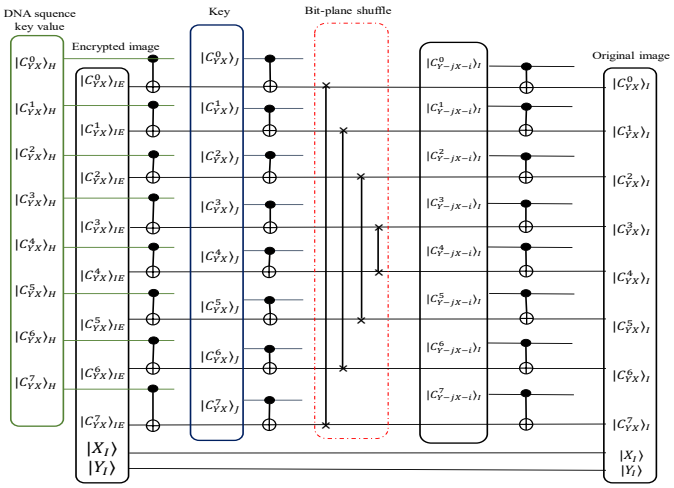


Fig. 11: Wire diagram of the subsection of proposed decryption architecture.

4.2 Estimation of Correlation Analysis

To evaluate the correlation among neighbouring pixels, the subsequent performance tests are initiated. In the first level, 10000 adjacent pixel pairs of X, Y and Z axis pixels are selected arbitrarily from both original and cipher images. The analysis for the selected pairs is calculated as given in Eq. 6 to 9.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{6}$$

$$D(x) = \frac{1}{N} \sum_{i=0}^{N} [x_i - E(x)]^2 \tag{7}$$

$$Conv\,(x,y) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)] \tag{8}$$

$$r_{xy} = \frac{conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

x and y describe the neighbouring pixel values in the selected image and N represents the total pixel count that are arbitrarily selected. Estimated values are given in Table 3.

Table 3 confirms that derived coefficient values for these standard test images are insignificant and confirms non-correlation between the original image and its equivalent encrypted image. Therefore, this algorithm is robust against various statistical attacks.

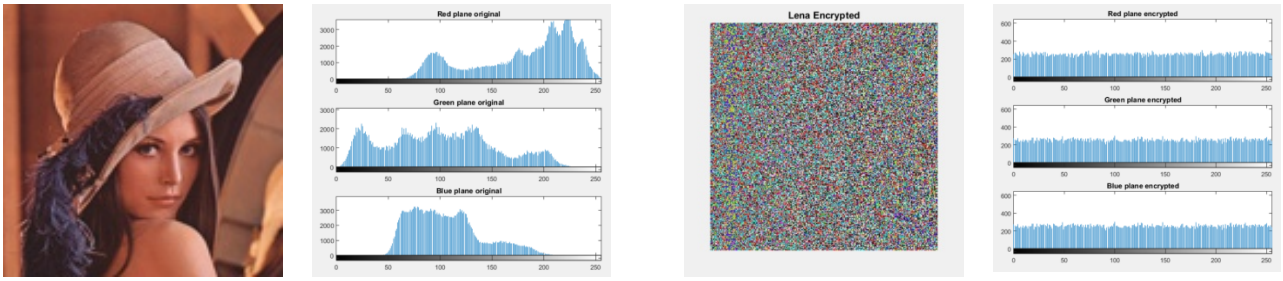
4.3 Estimation of Entropies

It is a standard metric to calculate the unpredictability of data [39]. In the case of images, the encryption algorithm decreases mutual data amidst pixels, increasing the entropy rate. A covert system must satisfy the information entropy test to establish that the encrypted value is uncorrelated to the original.

$$H(m) = \sum_{i=0}^{M-1} A(m_i) log_2 \frac{1}{A(m_i)} \tag{10}$$

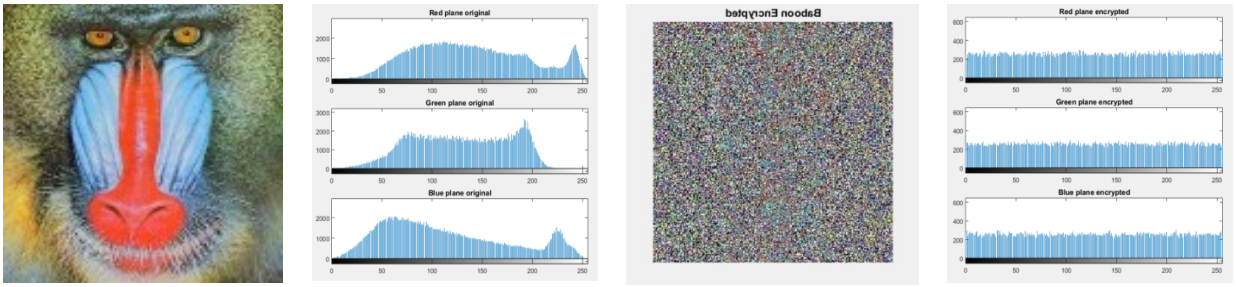
A (m_i) represents the possible symbol occurrence.

Global entropy alone cannot represent the randomness of the original images under study. In order to estimate complete randomness of the entire image, local entropy was introduced which divides the images into non-intersecting blocks and estimates entropy. For the significance level of 0.05, the accepted local entropy should lie in the range (7.901, 7.903). It can be estimated using the following formula



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

Fig. 12: (a) Original Lena, **(b)** histogram (RGB) of (a), **(c) e**ncrypted image (a), **(d) histogram (**RGB) of (C).



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

Fig. 13: (a) Original baboon, **(b)** histogram (RGB) of (a), **(c) e**ncrypted image (a), **(d) histogram** (RGB) of (c).

Table 3: Analysis of correlation coefficients

Colour_Images	Hor_dir			Ver_dir			Diag_dir		
	R_H	G_H	B_H	R_V	G_V	B_V	R_D	G_D	B_D
Lena_ori	0.9300	0.9163	0.8935	0.9606	0.9503	0.9313	0.8947	0.8817	0.8575
Enc_ Lena	-0.0009	0.0197	-0.0228	0.0009	0.0430	-0.0212	-0.0112	-0.0746	-0.0495
Baboon_ori	0.8990	0.8317	0.8981	0.8965	0.8326	0.9064	0.8711	0.7857	0.8699
Enc_ Baboon	0.0059	-0.0032	-0.0194	0.0205	-0.0149	0.0078	0.0192	0.0015	0.0086
Pepper_ori	0.9096	0.9455	0.8983	0.9214	0.9572	0.9155	0.8679	0.9203	0.8507
Enc_ Pepper	0.0047	0.0364	-0.0244	0.0029	0.0108	-0.0213	-0.0025	-0.0212	-0.0423
Airplane_original	0.9055	0.8923	0.9088	0.8869	0.8961	0.8574	0.8252	0.8309	0.8215
Enc_ Airplane	0.0051	0.0093	0.0111	0.0051	0.0034	0.0104	-0.0008	0.0034	0.0093
House_ori	0.9671	0.9805	0.9820	0.9353	0.9474	0.9749	0.9126	0.9320	0.9625
Enc_ House	0.0034	0.0047	0.0089	0.0118	0.0035	-0.0045	0.0098	0.0035	0.0007
Jelly Beans_ori	0.9745	0.9757	0.9890	0.9763	0.9801	0.9880	0.9537	0.9603	0.9799
Enc_ Jelly Beans	0.0143	0.0031	0.0110	0.0105	0.0070	0.0036	0.0003	-0.0022	0.0050
Splash_ori	0.9824	0.9550	0.9572	0.9931	0.9681	0.9525	0.9775	0.9350	0.9224
Enc_ Splash	0.0026	0.0054	0.0105	-0.0014	0.0032	0.0077	-0.0034	0.0035	0.0116

$$\overline{H_{k,T_B}} = \sum_{i=1}^{k} \frac{H(P_i)}{k}$$

$$\overline{E_{l,t_b}} = \sum_{j=1}^{l} \frac{E(P_j)}{l}$$

where P_1, P_2, ….P_l represents the non-intersecting blocks and $E(P_j)$ is the global entropy of P_j μ represents the significance level of 0.05, l be the count of the non-intersecting blocks considered from the test image is 30 and the total number pixel count t_b is 1936.

The estimation of global and local Entropies for various images is depicted in Table 4 and 5. From table 5, the estimated local entropy values lies in the acceptable range.

4.4 Chi-Square Test

This test is used to find out the histogram uniformity which can be calculated using the formula below:

$$\chi^2 = \sum_{j=1}^{U} \frac{[(Actual\ value(j) - predicted(j))^2]}{predicted}$$

where predicted is equal to the histogram value and U represents the pixel intensity level. The optimal degree of freedom (255) values are 310.457 and 293.2478 by considering the significant levels for 1% and 5%. The

Table 4: Global entropy analysis.

Colour_Images	R_E	G_E	B_E
Lena_Enc	7.9989	7.9991	7.9994
Baboon_Enc	7.9965	7.9904	7.9856
Pepper_Enc	7.9792	7.9810	7.9982
Airplane_Enc	7.9915	7.9916	7.9913
House_Enc	7.9913	7.9913	7.9916
JellyBeans_Enc	7.9914	7.9915	7.9919
Splash-Enc	7.9921	7.9920	7.9913

estimated values are shown in table 5. The tabulated values confirm the uniform distribution of pixels in the encrypted image histogram.

4.5 Differential Attack Analysis

The two metrics used to compute the performance of resisting differential attack sensitivity of encryption algorithm, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) as per eq. 11 and 12, respectively [39].

$$NPCR = \frac{\sum_{p,q} R(p,q)}{M \times N} \times 100\% \quad (11)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{p,q}\frac{|L_1(p,q) - L_2\ (p,q)|}{255}\right] \times 100\% \qquad (12)$$

Where, L1 and L2 are two cipher images that are associated with the two original images, in which one image is altered with a single bit, and M and N describe the length and width of the image, R (p, q) is a binary array of identical dimension as images L_1 and L_2. R (p, q) values are determined using Eq.13.

$$R(p,q) = \begin{cases} 0 & if\ L_1(p,q) = L_2(p,q) \\ 1 & if L_1(p,q) \neq L_2(p,q) \end{cases} \qquad (13)$$

NPCR and UACI results of both cipher images L_1 and L_2 for a standard digital image are given in Table 6.

Table 5: Chi-square and local entropy analysis.

Images	Chi-square	Local Entropy
Cameraman	282.5	7.9011
Girl	246.6172	7.9014
House	230.9219	7.9025
Lena	241.4413	7.9024
Pepper	243.3438	7.9030
Splash	249.875	7.9029

The results show that the proposed work has been achieved optimal values for NPCR and UACI, which have been compared with the critical values depicted in [39]. Hence, this work is susceptible even for small alterations in the input image, which results in the method are resistant in opposition to differential attacks.

4.5 4.6 Key Space Analysis

For any encryption algorithm, the primary concern is its security which reckons on its keyspace. The range of the key should be more significant than 2^128 to strengthen the durability inaccessible. The keyspace used for the proposed technique is $2^{680} \approx 10^{204}$, which is vast enough to withstand all sorts of attacks.

5 Discussions

The efficiency of this proposed algorithm technique is evaluated by comparing the results with other earlier works. Fig. 10 (a) has been taken as a reference image for comparison. Correlation, entropy and time taken for encryption have been considered as critical parameters to evaluate the proposed work. Table 7 portrays the analyses of the correlation coefficients and uniformity of the cipher image through entropy against other literature methods [4, 5, 7, 9, 13, 14, 15, 27, 29, 30, 32, 33, 34] where the proposed method attained a near-zero correlation and better entropy.

Table 6: Differential attack analyses.

Colour_Images	**NPCR_values**			**UACI_values**		
	R_N	**G_N**	**B_N**	**R_U**	**G_U**	**B_U**
Lena_Enc	99.6723	99.9732	99.7755	33.5752	33.8775	33.4638
Baboon_Enc	99.5056	99.2432	99.6782	33.6436	33.1111	33.5422
Pepper_Enc	99.5911	99.6242	99.6707	33.2498	33.4415	33.5434
Airplane_Enc	99.5636	99.5987	99.5575	33.3105	33.3972	33.1323
House_Enc	99.6109	99.6017	99.6063	33.2353	33.2536	33.3023
Jelly Beans_Enc	99.5728	99.6414	99.6170	33.2538	33.3293	33.3743
Splash_Enc	99.5367	99.5636	99.6155	33.2887	33.2264	33.3696

Table 7: Comparison: Correlation and entropy analysis of the RGB image.

Colour Images	**Horizontal**	**Vertical**	**Diagonal**	**R**	**G**	**B**
Ref. [4]	-0.0038	-0.0026	0.0017	NA	NA	NA
Ref. [5]	0.00312	-0.00317	-0.00310	NA	NA	NA
Ref. [7]	-0.0098	-0.0050	-0.0013	7.9974	7.9970	7.991
Ref. [9]	-0.0035	-0.0574	0.0578	7.9791	7.9802	7.9827
Ref. [13]	0.0011	-0.0018	0.0007	NA	NA	NA
Ref. [14]	0.0022	0.0001	-0.0017	7.9971	7.9975	7.9974
Ref. [15]	0.0002	-0.0001	0.0007	7.9973	7.9973	7.9975
Ref. [21]	-0.0004	0.0032	-0.0063	7.9973	7.9969	7.9971
Ref. [23]	-0.0082	-0.0128	-0.0012	7.9892	7.9898	7.9899
Ref. [24]	-0.0025	-0.0016	0.0116	7.9970	7.9970	7.9973
Ref. [26]	-0.01616	-0.0143	-0.0175	7.9993	7.9949	7.9918
Ref. [27]	0.0032	0.00004	-0.0039	7.9975	7.9973	7.9974
Ref. [28]	-0.0031	0.0010	-0.0008	7.9993	7.9992	7.9992
Proposed Work	**-0.00013**	**0.00075**	**-0.04510**	**7.9989**	**7.9991**	**7.9994**

Table 8: Encryption time of the proposed algorithm at various level.

Image	1St level of row column permutation (sec)	DNA decoding (sec)	2nd level of row column permutation (sec)	complete encryption (sec)
Cameraman	0.336739 sec	0.366370 sec	12.286355 sec	12.902445 sec
Girl	0.329240	0.375753	12.699364	13.060341
House	0.340660	0.369280	12.721590	13.369479
Lena	0.339363	0.367769	12.684791	13.898037 sec
Pepper	0.329694	0.365034	12.760663	12.974514
Splash	0.338686	0.372626	12.757800	13.053205

Table 8 provides the encryption time taken by the proposed algorithm at various stages of encryption.

6 Conclusion

This work has presented a Quantum novel encryption algorithm intended for the colour image by utilizing in the duo domain by HIWT, UTLM, RC6 block cipher, and DNA-XNOR techniques. The UTLM is developed to enhance the keyspace and to enlarge the range of unpredictable secret key. The sturdiness of the algorithm is validated by analyzing various security metrics with the existing encryption schemes and proved that the proposed system is more prominent and secure with less computation time. Future work will be on developing chaos influenced DNA based image encryption scheme in transform domain for medical data security.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," Optics and Laser Technology., **121**,105777(2020).

[2] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," IEEE Photonics Journal., **10(2)**, 1–14(2018).

[3] D. Ravichandran, S. Rajagopalan, H. N. Upadhyay, J. B. B. Rayappan, and R. Amirtharajan, "Encrypted Biography of Biomedical Image - a Pentalayer Cryptosystem on FPGA," Journal of Signal Processing Systems.,**91(5)**, 475–501(2019).

[4] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Processing., **138**,129–137(2017).

[5] S. El and M. Farajallah, "Signal Processing: Image Communication A new chaos-based image encryption system," Signal Process. Image Commun., **41(2016)**, 144–157(2017).

[6] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," Signal Processing., **97**, 172–182(2014).

[7] X. Wang and H. L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," Opt. Commun., **342**, 51–60(2015).

[8] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," Opt. Lasers Eng., **82**, 79–86(2016).

[9] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Opt. Commun., **284(16–17)**, 3895–3903(2011).

[10] M. A. Murillo-Escobar, C. Cruz-hernández, and F. Abundiz-pérez, "A RGB image encryption algorithm based on total plain image characteristics and chaos," Signal Processing., **109**, 119–13(2015).

[11] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "Modified substitution – diffusion image cipher using chaotic standard and logistic maps," Commun. Nonlinear Sci. Numer. Simul., **15(10),** 2755–2765(2010).

[12] A. Kadir, M. Aili, and M. Sattar, "Optik Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections," Opt. - Int. J. Light Electron Opt., **129**, 231–238(2017).

[13] H. Xue, J. Du, S. Li, and W. Ma, "Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets," Opt. Laser Technol., **106**, 506–516(2018).

[14] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," Opt. Lasers Eng., **90(October 2016)**, 225–237(2017).

[15] S. Rajagopalan, R. Sivaraman, H. N. Upadhyay, J. B. B. Rayappan, and R. Amirtharajan, "ON–Chip peripherals are ON for chaos – an image fused encryption," Microprocessors and Microsystems., **61**, 257-278(2018).

[16] P. Daltzis, S. Vaidyanathan, V.--T. Pham, C. Volos, E. Nistazakis, and G. Tombras, "Hyperchaotic Attractor in a Novel Hyperjerk System with Two Nonlinearities," Circuits, Syst. Signal Process., **37(2)**, 613–635(2018).

[17] V.-T. Pham, C. Volos, S. T. Kingni, T. Kapitaniak, and S. Jafari, "Bistable Hidden Attractors in a Novel Chaotic System with Hyperbolic Sine Equilibrium," Circuits, Syst. Signal Process., **37(3)**,1028–1043(2018).

[18] M. Y. Abubakar, L.T. Jung, N. Zakaria, A. Younes, A.-H. Abdel-Aty, Reversible circuit synthesis by genetic programming using dynamic gate libraries, Quantum Information Processing., **16**, 160(2017).

[19] M. Zidan, A.-H. Abdel-Aty, A. Younes, I. Elkhayat, M. Abdel-Aty, A novel algorithm based on entanglement measurement for improving speed of quantum algorithms, Applied Mathematics and Information Sciences.,**12**, 265(2018).

[20] A.-H. Abdel-Aty, N. Zakaria, L. Y. Cheong, N. Metwally, Entanglement and teleportation via partial entangled-state quantum network, Journal of Computational and Theoretical Nanoscience., **12**, 2213(2015).

[21] A.-H. Abdel-Aty, N. Zakaria, L. Y. Cheong, N. Metwally, Quantum network via partial entangled state, Journal of Communications., **9**,379(2014).

[22] A. H. M. Ahmed, M.N. Zakaria, N. Metwally, Teleportation in the presence of technical defects in transmission stations, Appl. Math & Info. Sci., **6**, 781(2012).

[23]A. H. M. Ahmed, L.Y. Cheong, N. Zakaria, N. Metwally, Dynamics of Information Coded in a Single Cooper Pair Box, International Journal of Theoretical Physics., **52**, 1979(2012).

[24] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," Appl. Soft Comput., **37**, 24–39(2015).

[25] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," Signal Processing., **153**, 11–23(2018).

[26] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," Optics and Lasers in Engineering., **115(November 2018)**, 131–140(2019).

[27] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," Signal Processing., **155**, 44–62(2019).

[28] Aqeel-ur-Rehman, X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," Optik., **153**, 117–134(2018).

[29] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," Signal Processing., **148**, 272–287(2018).

[30] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA Chaos Blend to Secure Medical Privacy," IEEE Transactions on Nanobioscience., **16(8)**, 850–858(2017).

[31] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," IET image processing.,**13(9)**,1535–1539(2019).

[32] B. Ramalingam, D. Ravichandran, A. A. Annadurai, A. Rengarajan, and J. B. B. Rayappan, "Chaos triggered image encryption - a reconfigurable security solution," Multimedia Tools and Applications., **77(10)**, 11669–11692(2018).

[33] S. Rajagopalan, S. Rethinam, S. Arumugham, H. N. Upadhyay, J. B. B. Rayappan, and R. Amirtharajan, "Networked hardware assisted key image and chaotic attractors for secure RGB image communication," Multimedia Tools and Applications., 77(18). 2018.

[34] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," Optics and Lasers in Engineering., **115(November 2018),** 7–20(2019).

[35] S.C. Ou, H.Y. Chung, W.T. Sung, "Improving the compression and encryption of images using FPGA-based cryptosystems," Multimed. Tools Appl., **28**, 5–22(2006). doi:10.1007/s11042-006-5117-6.

[36] B. Ramalingam, A. Rengarajan, J. Bosco, and B. Rayappan, "Microprocessors and Microsystems Hybrid image crypto system for secure image communication – A VLSI approach," Microprocess. Microsyst., **50**, 1–13(2017).

[37] C. H. Yang and S. J. Huang, "Secure color image encryption algorithm based on chaotic signals and its FPGA realization," International Journal of Circuit Theory and Applications., **46(12)**, 2444–2461(2018).

[38] J. C. Dagadu and J. L. P. C. Addo, "An image cryptosystem based on pseudorandomly enhanced chaotic DNA and random permutation," Multimedia Tools and Applications., 24979–25000(2019).

[39] S. A. Yue Wu, Joseph P. Noonan, "NPCR and UACI randomness tests for image encryption," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 31–38(2011).

[40] B. Bolourian Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, "TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA," Information Sciences., **486**, 204–230(2019).

[41] A. Belazi, A. A. Abd 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., **88**, 37–50(2017).

[42] Abd El-Latif, A.A., Abd-El-Atty, B., Talha, M.: Robust Encryption of Quantum Medical Images. IEEE Access, . doi:10.1109/ACCESS.2017.2777869., **6**, 1073–1081 (2018)

[43] Li, H.-S., Li, C., Chen, X., Xia, H.: Quantum Image Encryption Algorithm Based on NASS. Int. J. Theor. Phys. , doi:10.1007/s10773-018-3887-z., **57**, 3745–3760 (2018).

[44] Zhou, N., Yan, X., Liang, H., Tao, X., Li, G.: Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. Quantum Inf. Process, doi:10.1007/s11128-018-2104-6, **17**, 338 (2018).

[45] Wang, J., Geng, Y.-C., Han, L., Liu, J.-Q.: Quantum Image Encryption Algorithm Based on Quantum Key Image. Int. J.

Theor. Phys. doi:10.1007/s10773-018-3932-y1–15 (2018).

[46] Zhang Y, Lu K, Gao Y, Wang M (2013) NEQR: A novel enhanced quantum representation of digital images. Quantum Inf Process, doi: 10.1007/s11128-013-0567-z., **12**, 2833–2860(2013).