An Efficient Image Encryption using DNA Cryptography and Reversible Cellular Automata

Rajwant Kaur
M-Tech Student
SSIET, Patti, Punjab, India

S. A. Khan. PhD
Head of Department
SSIET, Patti, Punjab, India

Simranjit Kaur
M-Tech Student
SSIET, Patti, Punjab, India

ABSTRACT
The hybridization of DNA with reversible cellular automata techniques is an open area of research. This paper has focused on reversible cellular automata technique and DNA cryptographic operations which are used for compressing and encrypting together for an image. Usually, the image encryption techniques have more focused towards the providing security while there is a still room for an improvement in computational speed. An efficient approach for achieving higher information security at fast speed can be termed as "image encryption using hybridized DNA cryptography and reversible cellular automata". The algorithm mechanism is such that the original image is measured by measurement matrices in two directions to achieve compression and encryption simultaneously. Then DNA sequence operations are performed on the resultant image for further security. These DNA sequence operations include DNA addition and subtraction using DNA coding rules. The sequences worked under the control of 2D logistic map. Hence, the proposed technique is capable of providing security quickly as compared to existing technique.

Keywords
Image encryption, DNA cryptography, Reversible cellular automata, 2D logistic map, Chaos theory

1. INTRODUCTION
With the increase in the development of internet, image encryption-compression techniques have become the thrust areas in the field of computers. Cryptography methodologies are significantly essential for storage of information and transmission over the network, for example, the web. For high security, encryption is one of the strategy to protect the information from being get attacked. To protect confidential information from unauthorized users, image encryption converts the image information to a non-understandable form. On the other side of the coin, compression of data is an active and a big field at large level. The main problem is that data which is not in compressed form requires large amount of bandwidth for transmission or storage. This problem makes the research area of image compression to develop algorithms that compress images to save storage while maintaining the quality of the image. An efficient approach for achieving higher information security at fast speed can be termed as "image encryption using DNA cryptography and reversible cellular automata". Initially traditional algorithms like AES, DES [1] were used for encryption but it is no more suitable for digital image encryption. To improve the encryption of images many new algorithms have been proposed such as chaotic system, reversible cellular automata and DNA cryptosystem etc. Chaotic encryption technology has been used as the mainstream of encryption technology in recent years [2], But the use of chaotic technology only is not safe enough [2–5]. In recent years, image encryption technology based on DNA computing has been extensively used by scholars, but work is still at the initial stages of research.

1.1 Compression and Reversible Cellular Automata
Compression is a technique in which we represent the data in a condensed form. The media which is not compressed demands significant storage capacity, bandwidth and takes more time for transmission. Image compression have its various applications such as transmission for TV, video calling, exact transmission of printed material, images [6]. The main motive is to cut the bit rate for transmission at an extent such that the quality of image is acceptable. Representation of digital image with less number of bits while maintaining the quality of the image and along with take care of the cost related with transmitting less amount of data over the network is process of compression. It also takes care of reducing the probability of transmission errors. The main advantage of compression is that it uses less memory and gives best compression ratio [7].

In proposed work, reversible cellular automata is used for doing compression and encryption at the same time. With the help of measurement matrix the plain image is measured in 2 directions and then dimensions are reduced by partial Hadamard matrix. Now the remaining scrambling operations are applied on small amount of data.

1.2 Chaos Theory
Chaos theory explains the behavior of specific nonlinear dynamic system that shows dynamics under certain conditions which are deterministic and unpredictable. In [8], an iterated function "f" of a situation space "S" determined chaotic system and are extremely responsive to initial condition. The iterated function generates the values which are entirely arbitrary in nature but restricted between bounds. The iterated function changes the present state of the system into the next one, i.e.

$$FSn+1 = (Sn) \quad (1)$$

Where $S_n \in S$ indicates a state of the system at the discrete time. In chaos based cryptography, it is normally a finite binary space.

S= P= C= {0, 1} n, n=1, 2…

Where P=Plain text, C=Cipher text.

In proposed work, 2D logistic map are used to control and generate the pseudo random sequences. The random sequences create the confusion and appears to be random but beneath they are random in nature. This is the specialty of the logistic map. Logistic maps usually helps in decreasing the

adjacent correlation coefficient among pixels. 2D logistic map is more efficient than 1D logistic map.

1.3 DNA Cryptography

DNA cryptography is an evolving technique which perform operations on methods of DNA computing. Biological structure of deoxyribonucleic acid (DNA) contains nucleotides named as Adenine (A), Cytosine(C), Guanine (G) and Thymine (T). DNA cryptography is focused on utilizing DNA sequences to encode binary data in certain sort or another.

Advantages of DNA computing:

- Speed: Combining DNA strands made the computations 100 times quicker compared to the quickest computer.
- Storage requirement: The storage density of DNA memory is approximate 1 bit per cubic nanometer whereas conventional computer requires 1012bit per cubic nanometer.
- Power requirement: DNA computing does not require outside power source.

In the proposed technique DNA sequence operations are used for scrambling the bits. These operations are DNA addition and subtraction which are applied on the remaining left sequence after reducing the dimensions by reversible cellular automata.

The remainder of the paper is organized as follows: Section 2 gives the brief background of 2D logistic map, Reversible cellular automata and DNA Cryptography. Section 3 gives the pseudo code of the proposed scheme then its flowchart and description. Section 4 gives the simulation result and experimental analysis. Section 5 concludes this paper.

2. BRIEF BACKGROUND OF PROPOSED TECHNIQUE

2.1 Mathematical Definition of 2D logistic map

Mathematically, this 2D logistic map can be discretely defined as Eq. (2), where r is the system parameter and (xi, yi) is the pair-wise point at the ith iteration.

2D Logistic map: $$\begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \end{cases} \quad (2)$$

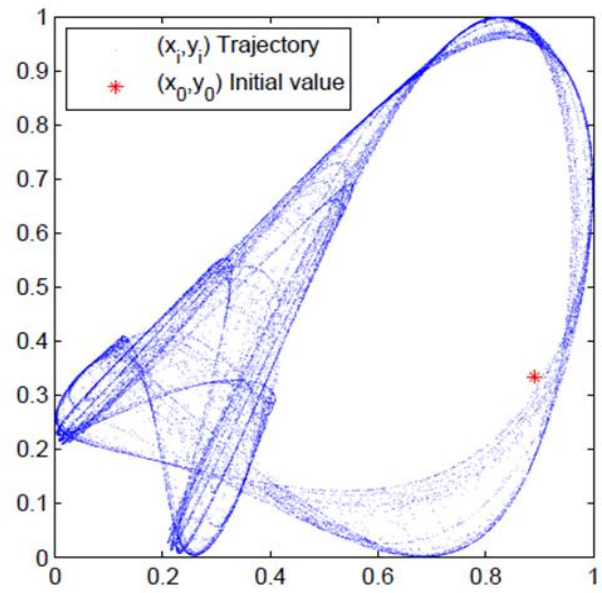

Figure 1. Trajectory of 2D Logistic map [9]

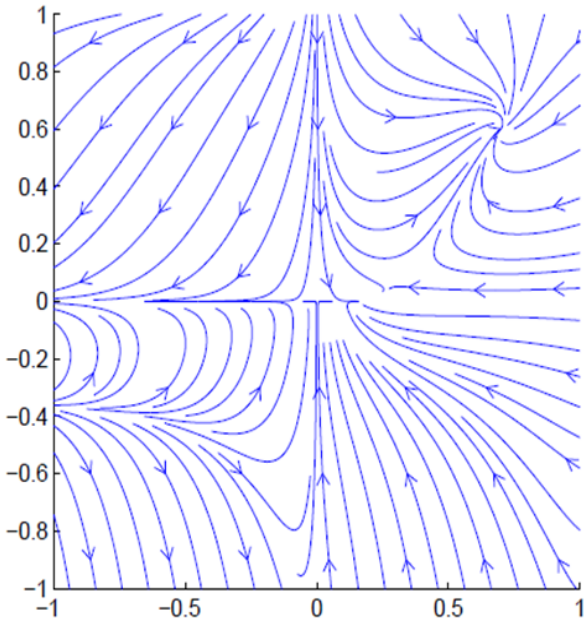

Figure 2. A phase portrait of 2D Logistic map [9]

Figure 1 shows the scatter plot of 30; 000 points from the trajectory [9] of the 2D logistic map using the parameter r = 1:19 and the initial value (x_0, y_0) at (0.8909, 0.3342). Therefore, the ith point on the trajectory can be determined by knowing (x_0, y_0, r, i) as Eq. (3)

$$\begin{cases} x_i = l_x^{2D}(x_0, y_0, r, i) \\ y_i = l_y^{2D}(x_0, y_0, r, i) \end{cases} \quad (3)$$

Figure 2 shows the phase portrait [9] of the 2D logistic map when r = 1:19. It is noticeable that this phase portrait matches the mathematical depiction of the 2D logistic map for r = 1:19. Since a (x, y) trajectory with respect to the chaotic behavior is random-like but is completely predictable when r and (x_0, y_0) are both known, it can be used as a pseudo number generator for cryptography.

2.2 Reversible cellular automata

In [10] Reversible cellular automata theory, sampling of signal and compressing could be done at the same time. The 1 dimensional signal x in R^N with length N can be represented as:

$$X = \sum_{i=1}^{N} a_i \Psi_i = \Psi a \text{ or } c = \Psi^T x \quad (4)$$

Where Ψ is an N×N matrix and a = [a_1, a_2…a_n] are the sequence of coefficients of the one dimensional signal x. If A where (A<N) coefficient nonzero in the coefficient vector c, the signal can be sparse and compressible. Then, a compressed depiction between S and a group of test functions $\{\Phi_i\}_{i=1}^{M}$ could be directly captured in $y_i = (x,\Phi_i^T)$ by an M (M<N) dimension linear measurement. The compressed signal could be acquired by stacking x_i into an M×1 vector and an M×N matrix Φ could be composed by gathering the rows Φ_i i.e.,

$$y = \Phi x = \Phi\Psi a = \theta a \quad (5)$$

2.3 DNA Coding

DNA (Deoxyribonucleic Acid) is a source plasma in all living life, and it is a form of biological super molecule formed by nucleotides. Monomer unit of DNA is called deoxyribonucleotides. There are four types of bases or nucleotides found in DNA or DNA consists of four bases [11]. These bases or nucleotides are given below:

Adenine(A)

Cytosine(C)

Thymine(T)

Guanine(G)

In [13], there are four nucleotides, namely A, T, C, and G, whereby pairing is allowed only between A and T & C and G. Moreover, the binary value pair for each pixel in grayscale image constitutes a complementary relationship pair. By using the digit pairs 00, 01, 10, and 11, DNA bases four nucleotides (A, C, G, and T) can be encoded. Some operations like addition, subtraction, xor can be performed.

Table 1: 8 Rules for DNA

	I	***II***	***III***	***IV***	***V***	***VI***	***VII***	***VIII***
T	11	11	10	10	01	01	00	00
A	00	00	01	01	10	10	11	11
G	10	01	11	00	11	00	10	01
C	01	10	00	11	00	11	01	10

Table 2:. Addition using rule 5 [12]

Rule 5	***A***	***G***	***C***	***T***
A	C	T	A	G
G	T	A	G	C
C	A	G	C	T
T	G	C	T	A

Table 3. Subtraction using rule 3 [12]

Rule 3	***A***	***G***	***C***	***T***
A	C	T	A	G
G	T	C	G	A
C	A	G	C	T
T	G	C	T	A

3. PROPOSED ALGORITHM AND METHODOLOGY

The plain image is measured with the help of measurement matrices in 2 direction to achieve compression & encryption simultaneously. Then, encryption process is employed again on produced image. This encryption have been done with the help of Bitwise XOR operation and DNA sequence operation. Random sequences are controlled by 2D Logistic chaotic map. Partial matrices i.e. Hadamard matrices are generated with the help of circular shift matrices which are the under control of the chaotic 2D logistic map.

Proposed Image Encryption-Compression Algorithm

Step 1: The plain image X is stretched out in the Ψ domain and then get the projection measurement in Ψ_1 to obtain $B_1 = \Phi_1 \Psi^T X$, where Ψ_1 is the M × N measurement matrix and Ψ is the N × N orthogonal basis.

Step 2: Then B_1 is extended in the Ψ domain to obtain $B_2 = \Psi^T X^T \Psi \Phi_1^T$, where measurement result $B = \Psi^T X^T \Psi$, and it is the transform in the 2D Ψ domain.

Step 3: The partial Hadamard matrices help in building up the measurement matrices Φ_1 and Φ_2, which works under the control of two different logistic maps.

For the construction of the measurement matrix Φ_1 below are the steps:

(1) First initial condition x_{01}, which is produced by logistic map, is utilized to create a sequence $\lambda = [\lambda_1\ \lambda_2 \ldots\ldots\ \lambda_{2N}]$ which is 2N long. To get the index sequence $s = [s_1, s_2 \ldots\ s_N]$, the previous N elements of λ are dropped.

(2) Arrange the nature sequence n = [1, 2...N] according to the index sequence s and this sorted sequence is identified as $l = [l_1, l_2, .l_i \ldots l_N]$, where $l_i \in \{1, 2 \ldots N\}$.

(3) The M row vectors H (l_1, :), H (l_2, :)… H (l_i, :), H (l_M, :) of the Hadamard matrix H of order N are used to classify into the following measurement matrix Φ_1.

$$\Phi_1 = [H(l_1, :), H(l_2, :) \ldots H(l_i, :), H(l_M, :)\ ]^T \quad (6)$$

Where H (l_i, :) denotes the l_i –the row vector of H. With another initial condition x_{02}, the measurement matrix Φ_2 could be composed in a same way.

Step 4: By considering $Y = \Phi_2 B \Phi_1^T$, the intermediate values of Y could be retrieved by measuring B.

Step 5: Confirm the values of the initial condition {Y} and applied DNA sequence operations. DNA sequence {Y} is generated.

Step 6: The DNA sequences {Y} is transformed into integer sequences $\{t_i^*\}$, t can be replaced by Y.

$$t_i^* = |\lfloor (t_i - \lfloor t_i \rfloor) \times 10^{14} \rfloor| \bmod 224 \quad (7)$$

Where ⌊x⌋ round off x to the nearest value towards zero.

Step 7: Construct DNA sequence $K = \{k_1, k_2 \ldots\ldots\ldots k_{2^{2n}}\}$. If the result of h_i^* mod 3 equals to 0, 1,and 2, then one takes k_i as Yi^* correspondingly to apply DNA addition operation. The integer Y_i can be interpreted as a binary number

$Yk_i = h_i^7, h_i^6, \ldots . h_i^0, h_i^j \in \{0,1\}, i = 1,2, \ldots ., 2^{2n}$, j=0, 1… 7.

Step 8: The pseudo random sequence created by the DNA Cryptosystem is transformed as:

$$R_2 = \{R_2 | R_{2i} = \text{round}[\bmod(1000_{y_i}, 8)]\}, i = 1,2, \ldots . \quad (8)$$

Step 9: All pixels of Y are mapped into an integer range from 0 to255.

$$C = \text{round}[255 \times \frac{y}{\max y}] \quad (9)$$

Now, the decomposition of each pixel into an 8 bit binary number is stored in C.

$$a^t(i,j) = \begin{cases} 1. \; {}^{a(i,j)}/_{2^t \bmod 2} = 1; \\ 0, \text{others} \end{cases} \quad (10)$$

In Eq. (10), the results are arranged in a row in turn, and the size of the transformed matrix $D_{8\times M^2}$ is $8M^2$.

Step 10 Apply Bitwise XOR on pixel values to scramble the values.

$$R_2 : C' = T(D_{8\times M^2}, R_2. \quad (11)$$

Step 11: Deduce an M × M binary matrix from C' and obtain the encrypted image G.

$$a(i,j) = \sum_{t=0}^{7} 2^t \times a^t(i,j) \quad (12)$$

$$G = \frac{C'}{255} \times \max Y \quad (13)$$

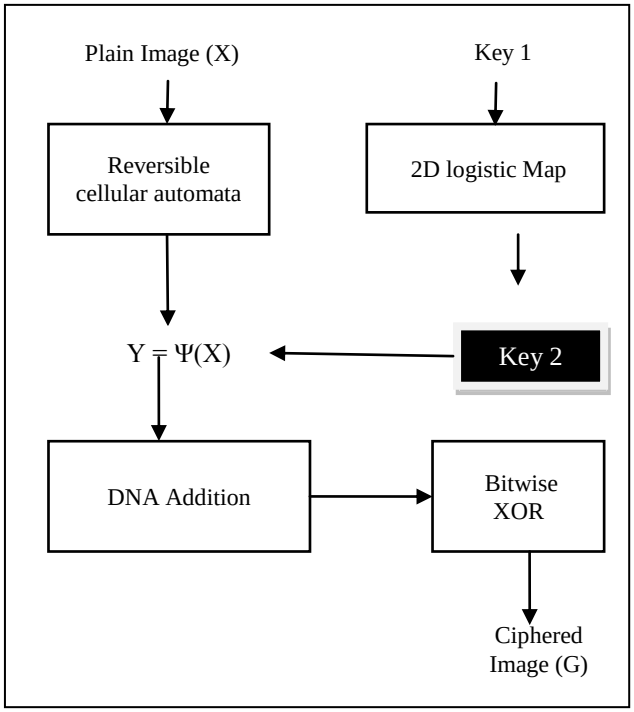

Figure 3. Flowchart of image DNA cryptography and Reversible cellular automata

4. PERFORMANCE ANALYSIS

This paper has designed and implemented the proposed technique in MATLAB tool R2013a. The evaluation of proposed technique is done on the basis of following metrics i.e. SDR, Peak Signal to Noise Ratio, Computational Speed, Execution Time, and Execution Time (speed).

1) Signal to distortion ratio(SDR)

It determines the SDR between the recovered and plain image.

$$SNR = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} \hat{f}\,(x,y)^2}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x,y) - \hat{f}\,(x,y)^2]}$$

Where m, n is the size of the image and I_1 is decrypted image, I_2 is original image.

Table 4. SDR

Images	***SDR (Existing)***	***SDR (Proposed)***
Flower	0.1971	0.0920
Cloud	0.1983	0.0912
Triangle	0.1945	0.0892
Hill Station	0.2005	0.0945
Boats	0.1902	0.0858
Car	0.1974	0.0897
Ground	0.1971	0.0808
Oranges	0.1983	0.0813
Women	0.1920	0.0820
Airplane	0.1945	0.0801

The recorded values in table-4 has been interpreted by bar graph. In the figure 4 blue color depicts the SDR value of the existing technique while the red color depicts the SDR values of proposed technique for all the ten images Serial Number 1 to 10 (s.no) in table 4. The improvement can be notice clearly as the value of the SDR of Proposed technique is decreasing as compare to the SDR value of the Existing technique.

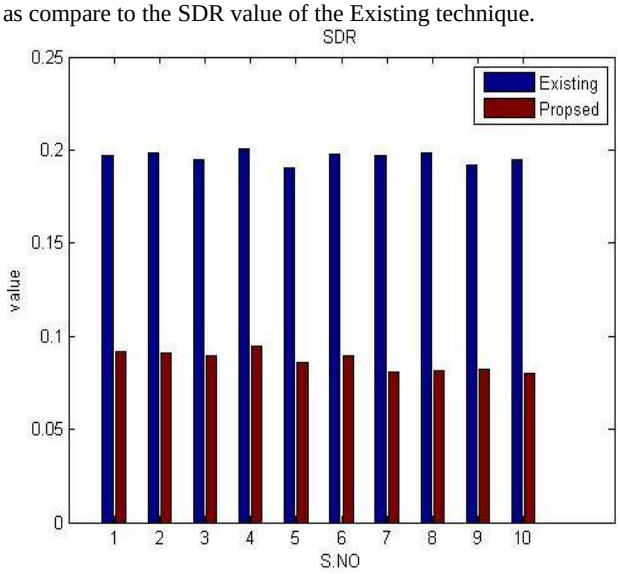

Figure 4: Bar Graph for SDR

2) Peak Signal to Noise Ratio(PSNR)

During transmission channels may lose some data which result into decrypting the image harder. It is used to test the capacity of recovering the plain images from ciphered images. PSNR is used to evaluate the occlusion performance. It computes the quality of the recovered image.

$$10 \times \log_{10} \frac{255 \times 255}{\text{MSE}} (\text{db}) \qquad (15)$$

Table 5. Peak Signal to Noise Ratio

Images	***PSNR(Existing)***	***PSNR(Proposed)***
Flower	62.2371	68.8517
Cloud	62.1830	68.9333
Triangle	62.3541	69.1209
Hill Station	62.0895	68.6200
Boats	62.5472	69.4573
Car	62.2233	69.0757
Ground	62.2371	69.9809
Oranges	62.1830	69.9339
Women	62.4649	69.8498
Airplane	62.3541	70.0565

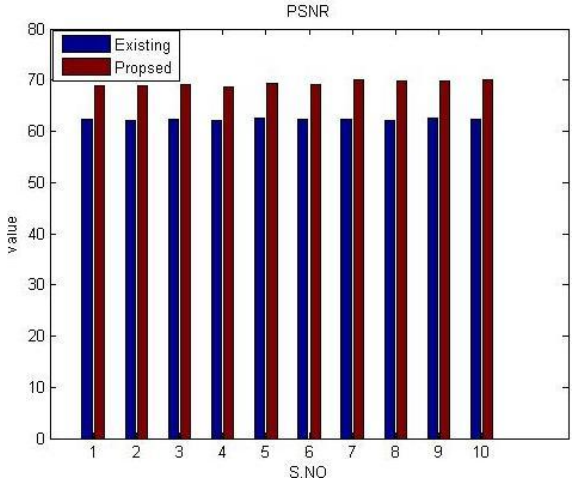

Figure 5. Bar Graph for PSNR

The recorded values in table-5 has been interpreted by bar graph. In the figure 5 blue color depicts the PSNR value of the existing technique while the red color depicts the PSNR values of proposed technique for all the ten images Serial Number 1 to 10 (s.no) in table 5. The improvement can be notice clearly as the value of the PSNR of Proposed technique is increasing clearly as compare to the PSNR value of the Existing technique.

3) Computational Speed

The adjacent pixels of the original image have a high correlation in the horizontal, vertical and diagonal directions. An ideal encryption algorithm should make the Computational speed of the pixels in the encrypted image have a sufficiently low Computational speed to resist statistical attacks. Encrypted image must have low correlation with adjacent (horizontal, vertical, diagonally) pixels.

Table 6. Computational Speed

Images	Computational Speed ***(Existing)***	Computational Speed ***(Proposed)***
Flower	4.3031	3.2029
Cloud	4.2905	3.2989
Triangle	4.2664	3.2155
Hill Station	4.2215	3.1007
Boats	4.2721	3.1989
Car	4.2478	3.1501
Ground	4.3128	3.2205
Oranges	4.2932	3.2426
Women	4.2585	3.1810
Airplane	4.2598	3.1140

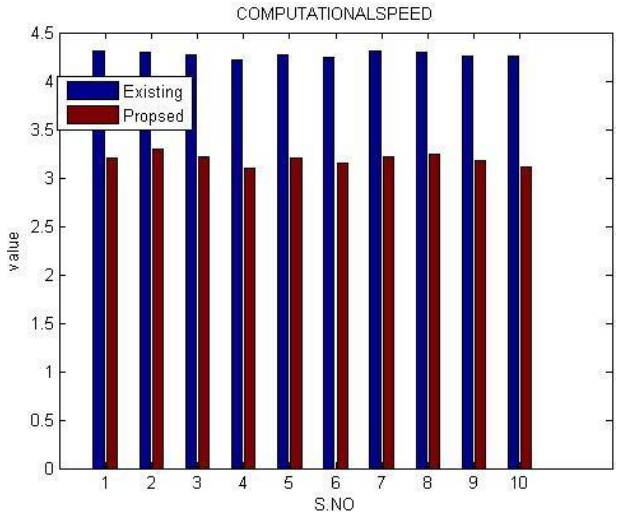

Figure 6. Bar Graph for Computational speed

The recorded values in table-6 has been interpreted by bar graph. In the figure 6 blue color depicts the computational speed value of the existing technique while the red color depicts the computational speed values of proposed technique for all the ten images Serial Number 1 to 10 (s.no) in table 6. The improvement can be notice clearly as the value of the correlation coefficient value of proposed technique is increasing clearly as compare to the correlation coefficient value of the Existing technique. It means that the recovered decrypted image from ciphered image has greater correlation as compare to the image recovered by using existing technique.

4) Execution Time

The Execution Time of an algorithm is calculated by two main factors known as computational cost and complexity of algorithm used. Computational cost checks the number of rounds during encryption and also considers how many permutation and diffusion operations occurred within a round.

Table 7. Execution Time

Images	***Bit Error Rate (Existing)***	***Bit Error Rate(Proposed)***
Flower	7.8410	4.8386
Cloud	6.9983	4.8064
Triangle	7.0351	4.8233
Hill Station	6.9110	4.6490
Boats	6.9529	4.7970
Car	6.9851	4.7406
Ground	7.5856	4.7253
Oranges	6.9895	4.7815
Women	6.9556	4.7611
Airplane	6.9496	4.7364

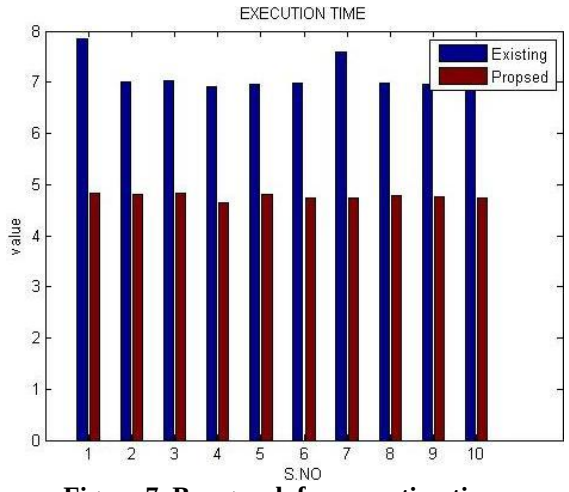

Figure 7. Bar graph for execution time

The recorded values in table-7 has been interpreted by bar graph in fig-7. In the figure 7 blue color depicts the execution time value of the existing technique while the red color depicts the execution time values of proposed technique for all the ten images Serial Number 1 to 10 (s.no) in table 7. The improvement can be notice clearly as the value of the execution time of proposed technique is decreasing clearly as compare to the execution time value of the Existing technique. It shows that the proposed technique is taking less time to complete the execution as compare to the existing one.

5. CONCLUSION

This paper presents an image encryption technique that are based on DNA cryptography and reversible cellular automata. By hybridizing these two techniques, the best qualities of both techniques give rise to the best results. As, DNA cryptography has the outstanding feature of working at high speed, and reversible cellular automata has feature of providing the security along with doing compression of the image. 2D logistic maps are used to control the random sequence. For scrambling the bits, Bitwise XOR operation, DNA addition and subtraction operation has been applied. The proposed technique, when applied on plain image produced the encrypted and compressed image. The Matlab simulation results and performance analysis is done using various parameters like MSE, PSNR, Correlation coefficient, Entropy, BER, and Execution time. All these results have shown that proposed technique not only achieved the better security level but also outperformed as compare to the existing technique. It is observed that the execution time has improved by 26%. In this way, the proposed combination of techniques has provided good security with good performance.

The Meta heuristic techniques such as ant colony optimization, particle swarm optimization can be considered in near future to enhance the results further.

6. REFERENCES

[1] Li S, Chen G, Cheung A, Bhargava B, Lo K-T. On the design of perceptual MPEG-Video Encryption algorithms. IEEE Trans Circuits Syst Video Technol 2007; 17 (2):214–23.

[2] W. Chen, C. Quan, and C. J. Tay, "Optical color image encryption based on Arnold transform and interference method,"Optics Communications, vol. 282, no. 18, pp. 3680–3685, 2009.

[3] R. Enayatifar, A. H. Abdullah, and M. Lee, "A weighted discrete imperialist competitive algorithm(WDICA) combined with chaotic map for image encryption," Optics and Lasers in Engineering, vol. 51, no. 9, pp. 1066–1077, 2013.

[4] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6thorder CNN," Optik—International Journal for Light and Electron Optics, vol. 125, no. 5, pp. 1671–1675, 2014.

[5] S. Lian, "A block cipher based on chaotic neural networks," Neurocomputing, vol. 72, no. 4–6, pp. 1296–1301, 2009.

[6] Nasrabadi, Nasser M., and Robert A. King. "Image coding using vector quantization: A review." IEEE Transactions on communications 36.8 (1988): 957-971.

[7] Al-allaf, Omaima NA. "Improving the performance of backpropagation neural network algorithm for image compression/decompression system." Journal of Computer Science 6.11 (2010): 1347-1354.

[8] Wang XY, Teng L, Qin X. A novel color image encryption algorithm based on chaos. Signal Process2012; 92(4):1101–8.

[9] S. Strogatz, Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering, Westview Press (1994).

[10] Zhou, Nanrun, et al. "Image compression–encryption scheme based on hyper-chaotic system and 2D reversible cellular automata." Optics & Laser Technology 82 (2016): 121-133

[11] M.Babaei," A novel text and image encryption method based on chaos theory and DNA computing," natural computing,12(1),101-107,2013

[12] Jaryal, Shikha, and Chetan Marwaha. "Comparative Analysis of Various İmage Encryption Techniques." International Journal of Computational Intelligence Research 13.2 (2017): 273-284.

[13] Lai, XueJia, et al. "Asymmetric encryption and signature method with DNA technology." Science China Information Sciences 53.3 (2010): 506-514.