Digital image based cryptography scheme for hybrid model of DNA computing for chaotic systems.

[1]Swetha T.N., [2]Dr.Sreerama Reddy GM
[1]Research Scholar, (Visvesvaraya Technological University, belagavi), Department of Electronics and Communication Engineering,CBIT, Kolar .Mail: swethareddy.t.n@gmail.com
[2]Professor & Research Supervisor(Visvesvaraya Technological University, belagavi), Department of Electronics and Communication Engineering,CBIT, Kolar

DOI: 10.48047/ecb/2023.12.si4.1696

Abstract

In this research article, we propose an encryption and decryption scheme for the standard image database available online and in extended to an hybrid model of DNA computing and chaotic system. The significant distinctive of the proposed cryptographic methodology is secure and efficient. In the DNA level of permutation, mapping function orientation with the logistic mapping is applied to DNA image with random position of element in DNA image In a DNA level of basic operation of cryptography with addition of two level of additional bits For the basic image of consideration. The experimental results are carried out in MATLAB environment for a secure analysis The image encryption technique is basically an improvisation of the different levels of application of digital image processing with consideration of fixed resolution as 512 x 512. The entire process of DNA based chaotic cryptography intended with encryption process of generation of cypher text with symmetric key. The encryption and the decryption time is calculated and estimated. The recovery of the image is also analysed with the histogram braced analysis, The parameters that reflect the quality of encryption are calculated like NPCR and UACI.

Keywords: Cryptography, Cypher, Decryption, Digital Image Processing, DNA, Encryption, Histogram, NPCR, Pixel, UACI

1. Introduction

The digital image processing have become one of the growing research area as the technology, science, and Computer industry is developing day by day. Developed The digital image processing is occupying a greater domain all over the world The digital images are now very popular, and are used for different fields, like defense, economics, politics, education and so on [1]. There are equally potential threat to the image transmission network and the nature of operation of images. The level of confidentiality required for certain images from a military affairs, commerce and the medical treatment are very high [2]. Hence, images should be encrypted with an effective technology, and so that the transmission of the data is secured.

There are different encryption algorithm available for common image encryption. They also include the text encryption technologies. The SCAN language based encryption technology, Quality image encryption technology, pseudo random sequence encryption technology, And many other image based encryption technologies are used to encrypt the images. All these encryption technologies are mainly based on the “key image”. These encryption technologies also use the DNA computing for encrypting the images [3-10]. In recent days. It is seen that chaotic encryption technology is seeking lot of attention from worldwide of the researchers. The initial values are left very sensitive in the chaos of inner class random process in a non linear system performance. This results in an result, which is merely unpredictable The implementation of chaotic encryption technology is a simple it is faster encryption technology, giving high security and also the robustness [11]. This encryption technology has many advantage, At the same time, it has different disadvantages also. For consideration at the current scenario, most of the chaotic encryption algorithm have a kind of confusion between the single pixel value or the location. At the same time, it is true that it utilizes anyone of the two strategies and will not ensure any sort of high security for the images. This making the attackers can crack the image very easily by simple pixel comparison method [12].

The DNA computing was first introduced in the year 1994 by Adleman, This was firstly introduced into encryption field. A new stage of information is created by processing the obtained data. In current scenario the DNA encryption method is in the frontier of international cryptographic research [13-14]. The low energy consumption and the capacity to store high density of images have made DNA molecular harness massive parallelism Very attractive scenario to use the methodology [15-16]. And hence, there is a unique advantages for every DNA computing process which are better than the traditional cryptographic encrypting techniques and the algorithms that exist currently. But still, the DNA encoding and encrypting of images is not so secure. The current researchers have made a combination of chaos encryption technology and the DNA computing to solve the insecurity problem that exists in the current technology. The chaotic encryption technology uses the technique of confusion to mix up the digital image pixels These pixels are diffused into confused pixels using the encoding methodology of DNA. The chaotic encryption technology is now used to obtain the encrypted result.

As a summary of the study, a successful combination of chaotic encryption technology and the DNA coding method will result in a very large number of experiment and security analysis. This helps to rationalize the algorithm and to create a new algorithm that can improve the security of image encryption.

2. Literature Survey

The authors in [17], Proposes DNE for the purpose of information security. The authors use a pseudo-DNA method to decentralise the molecular biology and to encrypt the images. The DNA based grip proof of it. Method is proposed, which helps in symmetric algorithm that generates a pseudo-DNA cryptography. The proposed algorithm has certain rules that makes it more secure with additional layers of security. That helps in conventional cryptographic technique. In this paper, the author proposes how the encryption decryption methods are carried out. The results are showing a better encryption methodology than the existing state of art methods.

In this paper [18], The authors use DNA based computing to blend the colours in the grey images, The author proposes this as an advanced encryption scheme that helps the image to be encrypted and to be decrypted. The grey and colour images have different rules of authentication in an individual identity image, and they exhibit the authentication and have different mattresses. The key generation the author proposes the process of key generation as two-level mathematical operation. This can be having an encrypted key to improve the security in the images. The DNA computing can also be added. The algorithm has good resistance against the differential attacks and the statistical attacks, as per the authors and the results obtained in the paper.

In the paper [19], The researchers mentioned the DNA encoding and decoding algorithm using chaotic maps The author describes how the chaotic maps can be adopted for DNA encoding and decoding methods. The authors show how the proposed hybrid algorithm behaves for different types of attacks and proposes that the proposed algorithm have better results when compared to the state of art techniques.

3. DNA encoding and chaotic maps

3.1 The Encoding using DNA and the complementary rule.

A DNA strand is a sequence mapped with the nucleotide. The unique combination of the nucleotide forms a strand of DNA. The four bases of DNA are adenine, thiamine, guanine and cytosine (A,T,G,C). These are the basic building blocks of a genetic code that forms a structure of DNA. The binding is always a unique combination, Addy 9 always binds with the thiamine and guanine always binds with the cytosine [20]. Coming to the digital images, each pixel can be expressed by 8 bit binary number [21]. The binary numbers are always represented using zeros and ones, Hence, the complimentary can also be used for representation 00,01,10,11. So the deoxynucleotides can also be represented using the complementary binary codes as A as 00, T as 11, G as 01 and C as 10. This enables to encrypt each of the image pixel into a special combination of nucleotide. This makes the digital image pixel as 228 binary corresponding values as “11100100”. Hence, making the strings of nucleotide corresponding to TCGA, Having 24 different combinations using four nucleotides. Because there are only eight combinations in the coding, they are suitable for the complementary in principle rule. The complete technique can be summarised as mentioned in table 1.

Currently, let us assume there is an original image which is of grayscale represented as I, Let the dimension of the image be M X N. Let us transform the binary image into binary matrix as I'. One of the eight combinations of DNA code is now selected to encode the obtained binary matrix I'. In the next step, The coded matrix is called as I''. The coded matrix is now converted into unidirectional sequence called as X. This can be expressed as the following equation (1).

$$X = \{x_1, x_2, x_3, x_4 \ldots\ldots x_{4MN}\}, x_i \in \{A, T, G, C\} \qquad (1)$$

By using the complementary base principle, the nucleotide string x_i can be encoded as nucleotides as follows:

$$x_i \neq P(x_i) \neq P\big(P(x_i)\big) \neq P\Big(P\big(P(x_i)\big)\Big),$$

$$x_i = P(P(P(P(x_i)))) \qquad (2)$$

In the above equations $P(x_i)$ and x_i remains complementary always. In other words, this can be expressed as the base pairs. The conditions of injective mapping are represented using base pairs. From the equation (2), It can be formed as six rational complementary combination using the base pairs:

Table 1: DNA Pairs

{AC)(CG)(GT)(TA), (AT)(TG)(GC)(CA), (AC)(CT)(TG)(GA), (AG)(GT)(TC)(CA), (AT)(TC)(CG)(GA), (AG)(GC)(CT)(TA).

Using the DNA complementary rule, each pixel is diffused into a new nucleotide. Anyone from the 6th rule can be selected to achieve the complementary substitution. This helps in achieving the objective of pixel diffusion.

3.2 Logistic map.

In the current paper, there are two types of chaotic maps. This helps in Chebyshev's chaotic map and logistic chaotic map. The polynomial for these chaotic maps have the depth of two [22]. This makes the mathematical definition of the maps as follows [23-24].

$$X_{n+1} = \mu X_n(1 - X_n) \qquad (3)$$

The logistic map uses the algorithm for confused pixels. This making the size of original image as M X N. This gives the main idea to summarise the things as follows:

Step 1: Let us consider two arrays as C_l and R, These are used to record the rows and columns of the images. And let it be represented by the equation (4).

$$R = \{1,2,3, \ldots\ldots. M\}$$

$C_l \; = \; \{1{,}2{,}3, \ldots \ldots . N\}$ (4)

Step 2: Pseudo random sequence are generated as two arrays, Each of them having the size of m and n, This is developed using logistic map. The arrays are represented in equation (5)

A = $\{a_1, a_2, \ldots \ldots . a_m\}$, B = $\{a_1, a_2, \ldots \ldots . a_n\}$, (5)

Step 3: The sequence in the arrays A and B are arranged in a descending order. This helps in recording the location of the data and hence the descending indexes are obtained as Index 1 and Index 2, These indexes are obtained from Pseudo random sequence, And is represented using equations (6)

Index 1 = $\{i_1, i_2, \ldots \ldots . i_m\}$, Index 2 = $\{j_1, j_2, \ldots \ldots . j_n\}$ (6)

The main goal of these indices is to find the index of the largest number within the sequence. The sequence size shall be M and they are stored in i_1. The second largest number indices is noted and is stored in i_2. The process is repeated until the descending sequence is stored in index array 1 with all sequence indices The same technique can be used to obtain the index 2 by rearranging the sequence in B. The sequence is arranged in descending order.

Step 4: The rows and columns are now exchanged in between index 1 and index 2. The new exchange row and the column can be used to confuse the image pixels.

3.3 Chebyshev's map.

The mathematical model of Chebyshev map is expressed as equation (7)

$Z_{i+1} \; = \; \cos(\omega \; x \; arccos \; (Z_i)),$ (7)

In the above map, it is seen that $-1 \; \leq \; Z_i \; \leq \; 1, 2 \; \leq \; \omega \; \leq \; 6$. In the above equation, where the $\omega \; \in$ [2,6]. The Chebyshev map is a chaotic map [24]. In this condition, the infinite computational accuracy can be obtained using infinite length, chaotic real valued sequence and a non periodic sequence [25]. In the encryption system, it is seen that the Chebyshev map have the most useful applications.

To diffuse the pixels in the given image. The Chebyshev map is used to replace the iterations of complementary DNA encoding methodology. The major steps are described as follows

The Chebyshev map has two initial values, which are represented as z_0 and q_0 . It has two parameters that are represented as $\omega_z \; and \; \omega_q$. The pixels of confused grayscale image are having the dimension of M X N. Every pixel can be represented by 4 2-bit nucleotide. Therefore, one dimensional image of DNA encoding method will be having dimension as M x N x 4.

Step 1: Two one dimensional sequences are generated using the equation (8) And are represented as Z and Q. The initial values are z_0 and q_0. respectively with the two parameter values ω_z and ω_q.

$$Z = \{z_1, z_2, \ldots\ldots, z_{4MN}\},\ Q = \{q_1, q_2, \ldots\ldots, q_{4MN}\} \qquad (8)$$

Step 2: A new one-dimensional sequence is generated using the equation (10), Which is represented as P. This one-dimensional sequence is used to find the location that helps in obtaining its digital form as Z. The key space has to be enlarged So a random selection from digit of 15 decimal is taken and is located on the sequence P as in equations (9) and (10) [26].

$$P = \{p_1, p_2, \ldots\ldots, p_{4MN}\}, \qquad (9)$$

$$p_i \ = \ (q_i\ x\ 10)\ mod\ 15 + 1 \qquad (10)$$

Step 3: Another sequence C is obtained using the equation (12), This sequence is used to understand the number of iterations done. This sequence also has a 1 to 1 correspondence with the nucleotide sequence. Which is expressed in the equation (11).

$$C = \{c_1, c_2, \ldots\ldots, c_{4MN}\}, \qquad (11)$$

$$c_1 \ = \ int\ (extract(z_i, p_i))\ mod\ 4 \qquad (12)$$

In the above equation (12), The extract function is used to extract the number of p_i using digital form of z_i [27].

4. Image encryption and decryption algorithm.

4.1. Encryption algorithm

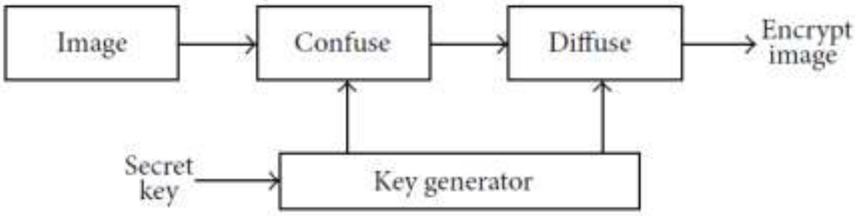


Figure 1: The image encryption algorithm.

The clear vision of encryption algorithm is shown in figure 1. If the grayscale image I has a size of M x N. The encryption step for the above-mentioned block diagram is as follows:

The standard set for the encryption is Image I, From the logistic map, The initial values are set a_0 and b_0. And the parameters are μ_a and μ_b. From Chebyshev maps the initial values and the parameters are z_0 and q_0 and ω_z and ω_q respectively.

Step 1: The original grayscale image is now converted into two dimensional matrix, which is also called as I. The two array named as R and C are now used to represent the rows and columns.

Step 2: A descending index, a sequence is generated, which is having two, 1 dimensional arrays as in (3). And it has the logistic mapping, which is used to exchange the columns and rows in the matrix I. This helps in creating the confused image matrix I'.

Step 3: The image I' is now converted into two dimensional matrix, which is represented as I''. The newly obtained matrix has the dimension of M x N Number of rows and 8 columns. This is completely based on the DNA encoding rule that is mentioned in table 1. DNA encoding matrix will be having M x N rows with 4 columns. And finally, this is converted into one dimensional DNA coding sequence that represented as M x N x 4.

Step 4: A sorting unit is generated, which is represented as P. This can have a Chebyshev mapping in the given scenario. This can have an iteration with the C and P. The random integers are generated from one to six as r2. This will help in deciding which rule should be applied among six types of complementary base pair rules. From every value of CI, it is seen that the output of nucleotide Xi is fixed in the sequence. The DNA sequence is mentioned in the X. The different iteratives that can be substituted in the above are as follows.

switch c_i;

Case 0, let the x_i remain the same;
Case 1, x_i = L (x_i);
Case 2, x_i = L(L(x_i));
Case 3, x_i = L(L(L(x_i)))

The complemtary DNA sequence is X'.

Step 5: The Random integer r3, Is generated from one to 8 that is decided by DNA encoding rule. As per the table 1. Which helps in converting the sequence from one dimension to binary sequence II'.

Step 6: Now the newly obtained binary sequence is converted into decimal dimensional matrix III. The new matrix consists of N columns and M rows. The encryption image III' is now developed using the dimensional matrix. The output is the encryption image.

4.2 Image decryption algorithm

The process of decryption is completely opposite to the process of encryption. And it operates as follows:

The input of the decryption algorithm is an encrypted image III'. At the initial conditions, the logistic maps have as $a_0\ and\ b_0$, the parameters are $\mu_a\ and\ \mu_b$. The initial values of Chebyshev map are and the variables are as follows $z_0\ and\ q_0$ and $\omega_z\ and\ \omega_q$ r1, r2, r3.

The output obtained will be an original grayscale image.

Step 1: The encryption image is converted into binary sequence image. III' → II'.

Step 2: The binary sequence image is now converted into one dimensional DNA coding sequence image. At this stage, it uses DNA encoding rule r3. II'→X'

Step 3: The sorting unit is generated using P of equation 7 and the Chebyshev mapping. The sequence is obtained using the iterations C with P the complementary pair is calculated with each of the nucleotide. The DNA coding sequence is used for complementary base payer rules in r2.

Step 4: The sequence X is now converted into 2-dimensional matrix, The Encoding of DNA using rule one. Then it is transformed into sequence with the 2-dimensional matrix I'.

Step 5: The rows and the columns of the image are recovered as I'. It has a descending index generated by equation (3). The decrypted image is obtained after the logistic mapping.

5. Comparative Parameters

5.1 Differential attack.

The encrypted image is always significantly different from the original image. This is one of the general requirements of image encryption algorithm. There are two criteria that has to be measured to understand the efficiency of the algorithm. The Number of Pixel Change (NPCR) Rate and Unified Average Changing Intensity (UACI) are the two criteria that has to be measured.

For a plain text attack. Whenever the NPCR value is larger, it is said to have a greater resistance to it. The change rate is nothing but the average strength of original image and the encrypted image The value of UACI should be as strong as enough to resist different other attacks.

The mathematical models to calculate the values of UACI and NPCR are as mentioned in the equation (13).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W\ x\ H}\ x\ 100\%\ ,\ UACI = \frac{1}{W\ x\ H}\left[\sum_{i,j} \frac{|C(i,j) - C'\ (i,j)|}{255}\right] \text{x } 100\% \qquad (13)$$

In the above image, the H and W represents the height and width of the image. C and C dash are the encryptions of the images before and after pixel of the plain image changed. The correlation of coefficients are also calculated from the algorithm Proposed.

5.2 Robustness Noise

The most important problem in the current communication technology is to have a cryptosystem that is robust against the noise. As an application parameter, the power signal to noise ratio is calculated, For the proposed hybrid algorithm. The PSNR is calculated in two scenarios, The first is when the crop attack is made And the second is when salt and pepper noise are added.

5. Results and Discussion

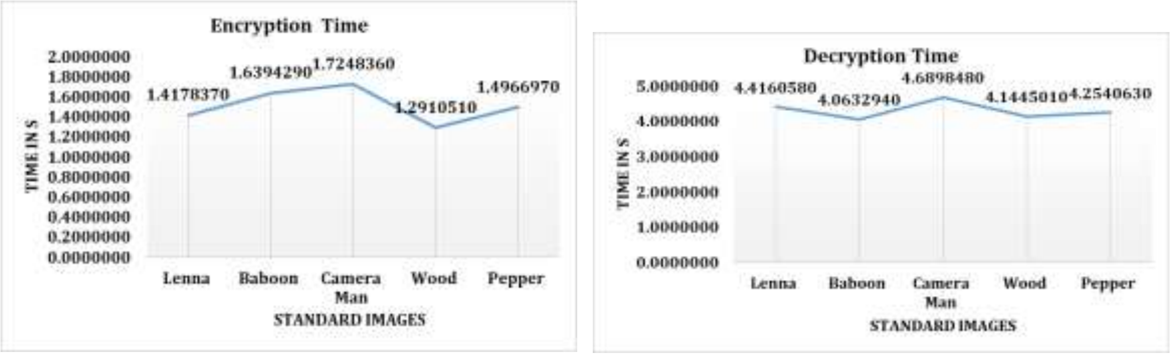
The proposed methodology is implemented using MATLAB code. To implement a personalized computer is used of Intel i5, 9th Generation, With the 2GB Nvidia graphic card, 1 terabyte SSD and 8GB of memory. To analyse the algorithm, the database used is a standard database, The images of Lena, cameraman, baboon, wood and bell peppers are used. The resolution of images that are considered are 512 x 512. All these images are used in ".bmp" format. To analyse the Encryption technique The number of Crop can also be varied, for this paper, the number of Crop is considered as 1, For this exercise, the number of additions are varied are 1 and 2.

5.1 Encryption and Decryption Details

The above mentioned five standard images are encrypted and decrypted using the proposed methodology. The encryption time and decryption time are tabulated as below in table 2. It is seen that, on an average, all the images take approximately same time to encrypt and also to decrypt. Figure 2 represents the graphical representation of encryption time and decryption time variation for different images in the proposed hybrid DNA algorithm.

Table 2: Encryption and Decryption time of hybrid DNA algorithm

	Encryption Time	Decryption Time
Lenna	1.4178370	4.4160580
Baboon	1.6394290	4.0632940
Camera Man	1.7248360	4.6898480
Wood	1.2910510	4.1445010
Pepper	1.4966970	4.2540630



(a) (b)

Figure 2: The encryption and the decryption times of standard images using the Hybrid DNA algorithm.

Table 3: 1-bit addition and 2-bit addition of Crop attack with the corresponding values of NPCR and UACI

	1-bit addition		2-bit Addition	
	NPCR	UACI	NPCR	UACI
Lenna	0.9962960	0.3348370	0.9960560	0.3350540
Baboon	0.9960210	0.3349630	0.9962270	0.3343190
Camera Man	0.9959910	0.3342390	0.9958880	0.3341940
Wood	0.9963110	0.3348780	0.9961890	0.3341740
Pepper	0.9958650	0.3341100	0.9961050	0.3350170

The value of NPCR for all the images is obtained as 0.99 (An approximate value). The value got the highest as possible for all the images that are encrypted using the proposed hybrid algorithm (shown in Table 3). Whereas UACI is 33%, For all the cases for the proposed algorithm. It clearly shows that the proposed algorithm, Is a sustainable for plain text attack, but not so efficiently dependable for a differential attack.

Table 4: PSNR for CROP attack and Salt and Pepper Noise

	PSNR for Crop attack	PSNR for Salt and Pepper Noise
Lenna	11.3754100	31.0872530
Baboon	12.2989630	32.6244260
Camera Man	11.5913810	31.4931770
Wood	11.7731060	31.4248340
Pepper	11.2998410	31.0926370

The above table gives the PSNR values for all the five standard images. The PSNR value is calculated for both the types of attacks. The first is crop attack, and the second is salt and pepper noise attack. From the table 4, It is clear that the PSNR for salt and pepper noise is better when compared to crop attack. This shows the proposed algorithm is resistant to salt and pepper noise, rather than the crop attack.

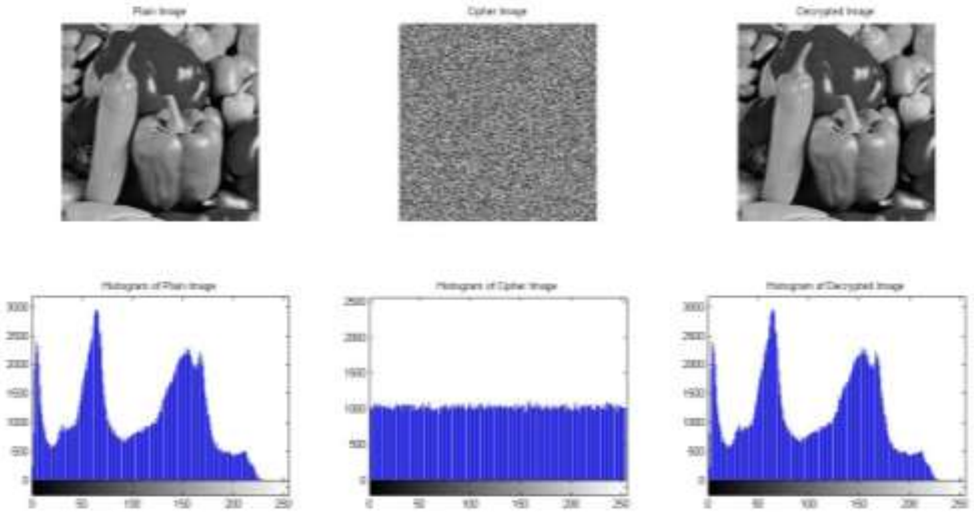


Figure 3: The plain image, the cypher image and the decrypted image with the Histograms respectively.

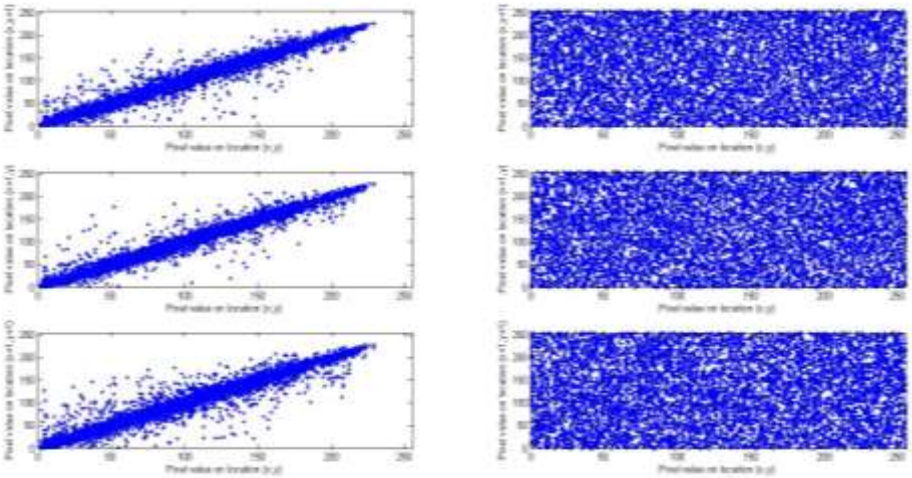


Figure 4: The pixel location on the images at different stages

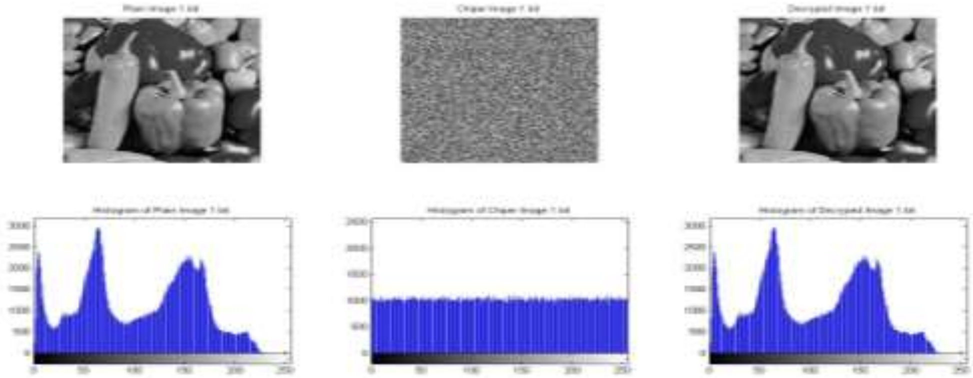


Figure 5: 1-bit addition of Plaintext attack, the original image, cypher image and the decryption images are represented with its histograms, respectively.

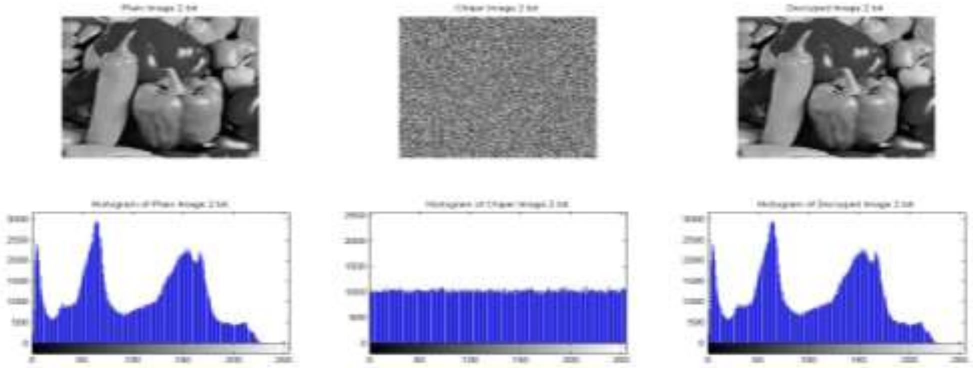


Figure 6: 2-bit addition of a plaintext attack, the original image cypher image and the decryption image are represented with its histogram respectively.

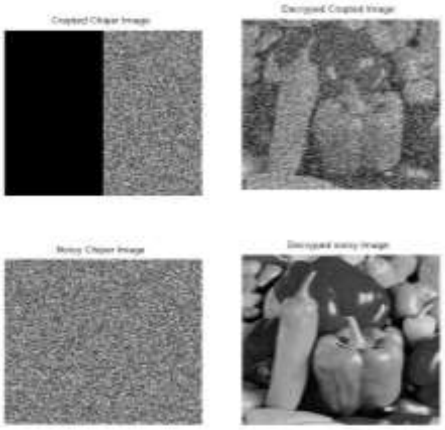


Figure 7: The crop is cypher image decrypted cropped image noisy image. And the final decrypted image.

In the figure 3, the plain image is the cypher image and the decrypted image with the histograms are represented. The standard image of bell peppers are considered in its grayscale and with a resolution of a 512 x 512. The Cypher image is considered, Which is a random data written as a part of code in the DNA algorithm, The image is encrypted using the cypher image. Using the proposed algorithm, it is also decrypted. The histograms of the above are shown to make a comparison. The figure 4 represent different pixel locations that can be placed in the given image.

The figure 5 and figure 6, represents the 1-bit addition of plain text attack and a 2-bit addition of plain text attack, respectively. the images are encrypted with the addition of plain text attacks and is decrypted using the proposed algorithm. In both the conditions, the histogram is represented for the comparison and verification. Figure 7 represents the crop attack on the standard image. From the decrypted noisy image, it is clear that the proposed algorithm is stable and can resist the attacks of plain text, but at the same time, the immunity of the proposed algorithm weakens whenever the crop attacks are made.

6. Conclusion

In the present context of research, an efficient DNA based image encryption and decryption model has been proposed for chaotic system and DNA computing. In the proposed technique of cryptographic secrete, symmetric key is used for ensuring different computing technique with a standard image database available as per the open sources. The DNA computing is followed by two additional steps, such as addition of single bit and 2-bit for histogram analysis for the decryption process by considering NPCR and UACI parameters by fixing the standard image size to 512 x 512, for the five different images of same resolution. The five standard images considered are Lena Pepper Baboon Wood and cameraman The detailed analysis of one bit addition and 2-bit addition for cryptographic analysis is carried out. The proposed system has resulted in almost similar values for NPCR and UACI As the proposed system is efficient in calculation and comparative analysis, is carried out with suitable comparative graph as well. It is also noted that generation of ciphertext has been carried out with time and decryption time is observed. The encryption and decryption times are compared for different images, using the comparative graphs. For the proposed hybrid DNA algorithm, the crop tag and the plaintext attack are induced to verify the results. From the figures and the tabulation, it is clear that the DNA Algorithm is resistant to the plain text attack At the same time the algorithm is weakened when the crop attacks are made, resulting in the noisy decrypted images. The PSNR values are also calculated for crop attack and salt and pepper noise attack, It is clear that the PSNR for salt and pepper noise is better when compared to crop attack. This shows the proposed algorithm is resistant to salt and pepper noise, rather than the crop attack.

As a future scope, the proposed system can be extended to raw images as well. And analysis can also be carried out by various varying the different combinations of resolutions, number of bits, amount of noise and others. The application of the proposed system can be dealt with different other various biometric systems data communication and other robust systems

7. References

[1] Y. Liu, X. Tong, and S. Hu, "A family of new complex number chaotic maps based image encryption algorithm," Signal Pro- cessing: Image Communication, vol. 28, no. 10, pp. 1548–1559, 2013.

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

[3] Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," Optics and Lasers in Engineering, vol. 51, no. 6, pp. 665–673, 2013.

[4] H. Liu and X. Wang, "Color image encryption based on one- time keys and robust chaotic maps," Computers & Mathematics with Applications, vol. 59, no. 10, pp. 3320–3327, 2010.

[5] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," Applied Soft Computing Journal, vol. 12, no. 5, pp. 1457–1466, 2012.

[6] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," Optics and Laser Technology, vol. 60, pp. 111–115, 2014.

[7] Hussain, T. Shah, and M. A. Gondal, "Application of S-box and chaotic map for image encryption," Mathematical and Com- puter Modelling, vol. 57, no. 9-10, pp. 2576–2579, 2013.

[8] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," Signal Processing, vol. 92, no. 4, pp.1101–1108, 2012.

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

[10] 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 Engi- neering, vol. 51, no. 9, pp. 1066–1077, 2013.

[11] Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryp- tion using skew tent map and hyper chaotic system of 6th-order CNN," Optik, vol. 125, no. 5, pp. 1671–1675, 2014.

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

[13] N. Pisarchik and M. Zanin, "Image encryption with chaoti- cally coupled chaotic maps," Physica D: Nonlinear Phenomena, vol. 237, no. 20, pp. 2638–2648, 2008.

[14] W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Commu- nications in Nonlinear Science and Numerical Simulation, vol. 15, no. 12, pp. 3998–4006, 2010.

[15] F. Zheng, X. J. Tian, J. Y. Song, and X. Y. Li, "Pseudo-random sequence generator

based on the generalized Henon map," The Journal of China Universities of Posts and Telecommunications, vol. 15, no. 3, pp. 64–68, 2008.

[16] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos, Solitons and Fractals, vol. 42, no. 3, pp. 1745–1754, 2009.

[17] C. S. Sreeja, M. Misbahuddin and N. P. Mohammed Hashim, "DNA for information security: A Survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology," International Conference on Computing and Communication Technologies, Hyderabad, India, 2014, pp. 1-6, doi: 10.1109/ICCCT2.2014.7066757.

[18] S. Arunpandian and S. S. Dhenakaran, "DNA based Computing Encryption Scheme Blending Color and Gray Images," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0966-0970, doi: 10.1109/ICCSP48568.2020.9182195.

[19] J Zhang, D Fang, "Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2014, Article ID 917147, 10 pages, http://dx.doi.org/10.1155/2014/917147.

[20] H. Li and Y. Wang, "Double-image encryption based on discrete fractional random transform and chaotic maps," Optics and Lasers in Engineering, vol. 49, no. 7, pp. 753–757, 2011.

[21] Anil Kumar C., Pradeep Kumar B.P, Venu K N, Lavanya Vaishnavi D.A., "Intra Prediction Algorithm for Video Frames of H.264", 2021, Natural Volatiles and essential oils journal, Page 51-58, Volume: 8 Issue: 5.

[22] Q. Zhang, Q. Wang, and X. Wei, "A novel image encryp- tion scheme based on DNA coding and multi-chaotic maps," Advanced Science Letters, vol. 3, no. 4, pp. 447–451, 2010.

[23] S. H. Jiao and R. Goutte, "Code for encryption hiding data into genomic DNA of living organisms," in Proceedings of the 9th International Conference on Signal Processing (ICSP '08), pp. 2166–2169, Beijing, China, October 2008.

[24] Anil Kumar C, Chethan Venkatesh, Lavanya Vaishnavi D A, Harish S, "Computer vision based Hand gesture recognition system", Neuro Quantology, Jul 2022, Volume 20, Issue 7, Page 2859-2866, DOI: 10.14704/nq.2022.20.7.NQ33365

[25] Q. Zhang and X. Wei, "A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system," Optik, vol. 124, no. 23, pp. 6276–6281, 2013.

[26] M. Shan, J. Chang, Z. Zhong, and B. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," Optics Communications, vol. 285, no. 21-22, pp. 4227–4234, 2012.

[27] Liu, Q. Zhang, and X. Wei, "A RGB image encryption algo- rithm based on DNA encoding and chaos map," Computers and Electrical Engineering, vol. 38, no. 5, pp. 1240–1248, 2012.