DNA Computing for RGB image Encryption with Genetic Algorithm

Hany H. Hussien

Lecturer
Department of Information Systems
Higher Institute of Management Science and Advanced Computing, El-Beheira
Alexandria, Egypt
Hany_lotus2003@hotmail.com

***Abstract*—A combination of DNA computing and a genetic algorithm is announced for RGB image encryption. The model is strong based on the scrambling technique of DNA computing operations using the crossover and mutation process and establishing a dynamic key based on a genetic algorithm, including a set of parameters such as population size, number of generation and mutation probability .First, the decoding of the image GA selected DNA sequence encoding process and the random key for the three R G B channels were followed by the DNA addition process. The decoded DNA added to the matrix of the output. Finally, conduct the XOR-mod procedure on the decoded matrix and the random number of the genetic algorithm to obtain the encrypted image. The paper includes countless experimental steps to confirm that the model has a high degree of safety and strength against different types of attacks.**

Keywords—Image Encryption, Image Decryption, Cryptography, DNA Encoding, DNA addition, Security, Genetic algorithms

I. Introduction

Recently data safety has become a major problem for the government, private and defense organizations owing to large information losses from illegal information access. The appreciated data from illegal readers can be protected by using numerous cryptographic techniques. Development increases rapidly in the information security field by using innovative and different techniques, which assurance both of accessibility, completeness, and confidentiality [1] [2].

Cryptography is the practice of hiding and manipulating data to be transmitted over a network by complex or logical mathematics to shield info against opponents and make it visible only to the recipient [3].

All creatures on this planet are made of the same type of genetic blueprint coded inside the cells of the human body containing a whole unit of Deoxyribo Nucleic Acid (DNA) containing dual-stranded nucleotide helix which holding the code of the inherited cell information. DNA is produced by building chemical blocks that are recognized as nucleotides that collect into three parts: phosphate group, sugar group, nitrogen bases. The DNA element is formed by linking nucleotides to a chain using uneven phosphate and sugar, while the Nitrogen bases are Adenine, Thymine, Cytosine, and Guanine [4] [5] [6].

DNA computing begins in 1994 and started a new information epoch based on features found in DNA for huge parallelism, vast storage, and ultra-low consumption of power. DNA cryptography developed by DNA computing in the context of an innovative cryptography technique, where DNA acts as a data carrier that considers modern biological technology [7] [8].

Genetic algorithm is a randomized approach to search and optimization based on the principle of natural selection structures motivated via Darwin's theory of development. There are three primary operators in the genetic algorithms: selection, crossover, and mutation. Depending on some criteria, the operation's that they joined a loop called generation stopped. The strongest search system for genetic algorithms is reproduction coupled with crossover operation [9] [10] [11].

The paper's structure is as follows. Section 2 includes certain similar work in the area of image encryption on DNA computing. Section 3 introduces DNA computing. Section 4 describes the suggested model. The results of security shall be explored in Section 5. Section 6 suggests, at last.

II. Related Work

An additional DNA sequence method for the encryption of pictures was viewed in [12]. Two additional DNA activities scramble each gray picture pixel and complement DNA. The DNA sequence image encoding is then divided into identical blocks which are combined by adding DNA, and as a result of the two logistic maps, the DNA structure is incorporated into the blocks. The model has accomplished excellent outcomes in both encryption and potential attack resistance.

Image encryption dealing with four different types of chaotic maps and additional DNA mixed with noise introduced in [13]. To get the encrypted image, the image first encoded with DNA then applied two chaotic maps, then applied DNA

978-1-7281-5260-8/19/$31.00 ©2019 IEEE

addition together with two other chaotic maps joined with noise effect. Among the other maps, the cross chaotic map gives the best results.

DNA subsequence operations plus chaotic maps are suggested in [14]. DNA processes are used in combination with a logistic map to fumble the picture pixel. The model is capable of resisting high-protection comprehensive and statistical attacks

For the encryption image, a DNA sequence genetic algorithm is introduced in [15]. Using GA, the image pixel is converted to decrease the pixel correlation and then replaced with random DNA substrings that consider the key to XOR activity attaining the substitution stage. The model against attacks of all types is fast and easy and robust.

III. DNA COMPUTING

A. DNA Encoding and Decoding

DNA stores data as a file consisting of four organic seats: adenine (A), guanine (G), cytosine (C), and thymine (T). DNA seats are coupled, A with T and C with G, to process base pairs components that suit one another. There are couples in 0 and 1 of binary arithmetic, so 00 and 11 are couples, 01 and 10 are also couples. [16] [17]. For each pixel, the binary value of the four biological units of DNA is: A is equal to 00, C is equal to 01, G is equal to 10, and T is equal to 11 every 8 bit [18].

B. DNA Sequences Regulations for Addition and Subtraction

DNA sequences have several functions, including insertion, transformation, addition, and subtraction. Table 1 and Table 2 show the guidelines for addition and subtraction [19] [20].

TABLE I. : DNA ADDITION PROCESS

+	A	T	C	G
G	C	A	G	T
C	A	T	C	G
T	G	C	T	A
A	T	G	A	C

TABLE II. :DNA SUBTRACTION PROCESS

-	A	T	C	G
G	T	A	G	C
C	G	T	C	A
T	A	C	T	G
A	C	G	A	T

IV. THE PROPOSED MODEL

There are the following steps in the model:

1. Read the RGB image and resize it to 128 *128 blocks
2. Divide the image into channels R G B
3. Randomly initialize Key1 (from 1 to 8)
4. Get the random Key1 DNA Coding as shown in Table 3.

TABLE III. : DNA CODING TABLE

Key number	DNA Coding
1	ACGT
2	AGCT
3	CATG
4	CTAG
5	GACT
6	TCGA
7	GATC
8	TGCA

5. Convert the image for each R G B channel into a binary matrix
6. DNA encoding for the based binary matrix image
7. Apply DNA Addition to matrix blocks
8. Apply DNA Decoding and GA Crossover and mutation process to the DNA matrix blocks.
9. Generate key 2 on genetic algorithm basis
10. Initialize key generation as the algorithm's basis

a. Initialize the population size to 128

b. Set the number of generation to 500

c. Initialize the probability of mutation to 0.18

d. Initialize random matrix fitness

e. Loop until the generation number is stopped (population crossover and mutation process)

f. Get the final population that is considered to be pseudo-random

11. Use the decoded matrix and key2 with the XOR-plus-mod operation
12. Recover the cipher image

The method of decryption is the opposite of the technique of encryption. Receivers get two secret keys from the transmitter. In step 7, while the other steps are set, the subtraction is alternated with the addition. The model procedure proposed is shown in Fig. 1.

V. RESULTS AND ANALYSIS SIMULATION

The core I5 -1.7 GHz CPU was evaluated for simulation with 4 GB of RAM operating on Windows 10 pro and using MATLAB 2018a. Results are tested on two standard 128 X 128 images, Lena, and Baboon as the original image based on different quality measurements. Fig.2 The original, encrypted, wrongly decrypted and decrypted images with the correct and the wrong secret key.

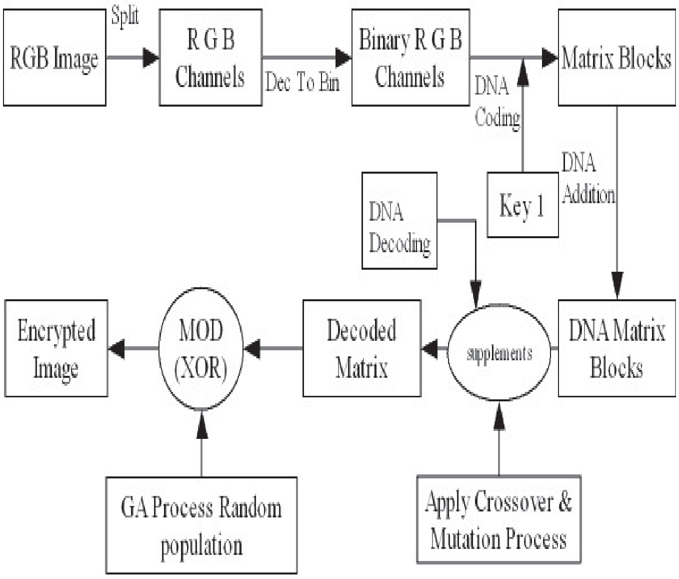

Fig. 1. The Model Block Diagram

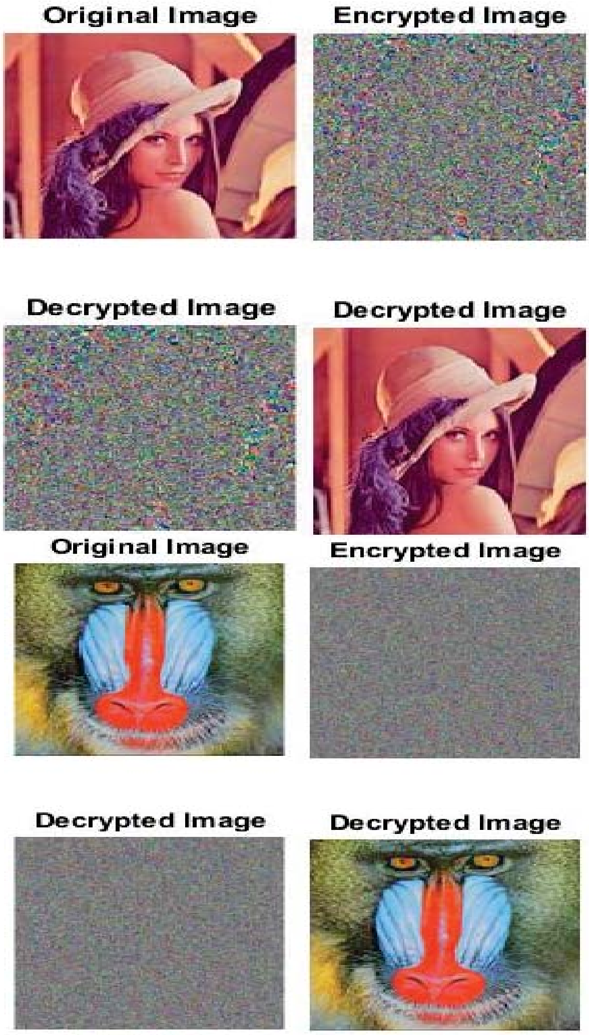

Fig. 2. Original & decrypted with incorrect key & image decrypted with right key

A. Statistical attack resistance

1) Analysis of the histogram

Fig. 3 displays the histograms for the novel and encrypted picture, that shows that the encrypted image's R, G and B channels are exactly the same, while the novel picture has different values with clear densities, so that statistical attacks are difficult to achieve [21].

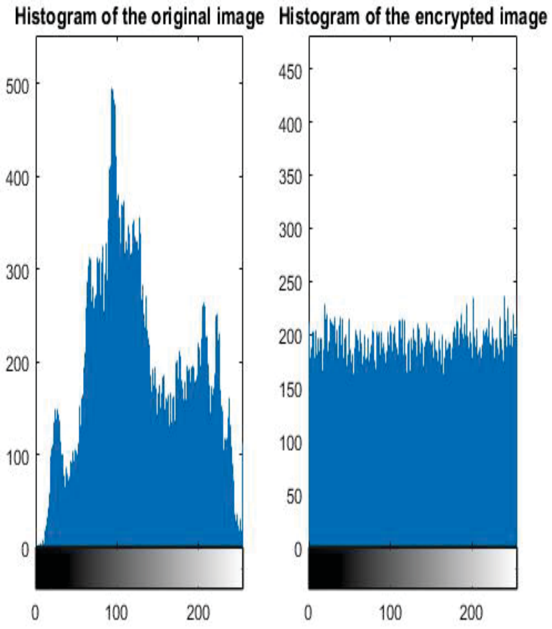

Fig. 3. Original & Encrypted Histogram Image

2) Coefficient of correlation analysis

The relationship of the original picture adjacent pixels is very high, while it must be very low at the encrypted image to resist statistical attacks. A random selection of 2500 sets (horizontal, vertical, as well as diagonal) of corresponding pixels from the novel and the encrypted image are formed based on the relevant equations to examine the contiguous pixel association [22] [23].

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(X_i - E(x))^2 \qquad (2)$$

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \qquad (3)$$

$$r_{xy} = \frac{COV(x,y)}{\sqrt{D(x)}x.\sqrt{D(y)}} \qquad (4)$$

In which x and y are pixel standards, whereas Cov (x, y) is covariance, D(x) is a distinction, E(x) is mean. Fig. 4 indicates the corresponding pixel association. The assessed value of the correlation coefficients plus additional algorithm is described in Table 4. The system can effectively extinguish any nearby pixel relativity.

TABLE IV. VALUE OF ADJACENT PIXELS FOR CORRELATION COEFFICIENTS WITH OTHER ALGORITHM

	original image		encrypted image		[12]
	Lena	**Baboon**	**Lena**	**Baboon**	**Lena**
Horizontal	0.9543	0.9453	0.0018	0.0020	0.0036
Vertical	0.9507	0.9422	0.0194	0.0240	0.0023
Diagonal	0.8698	0.5789	0.0234	0.0333	0.0039

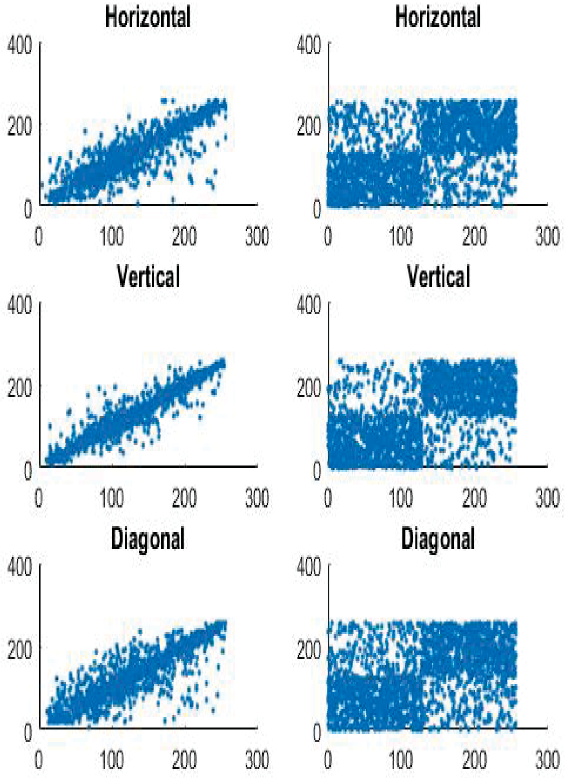

Fig. 4. Original & Encrypted correlation

B. Resistance to differential attack

The attacker's try to compare the indicated initial image with the changeable initial image after several modifications to determine any link between images [24] [25].

Measures are NPCR (pixel change rate number) and UACI (unified average change intensity) which can be used to study differential attack resistance performance [26] [27] [28]. By using the equations below.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \tag{5}$$

In which M as well as N are the image's height and width.

$$D(i,j) = \begin{Bmatrix} 0, if\ C_1(i,j) = C_2(i,j) \\ 1, if\ C_1(i,j) \neq TC_2(i,j) \end{Bmatrix} \tag{6}$$

In which D (i,j) is the matrix for the two C1 as well as C2 encrypted images.

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |c_1(i,j) - c_2(i,j)|}{255 \times M \times N} \times 100\% \tag{7}$$

The two encrypted pictures are C1 and C2 where M and N are the height and width of the picture. Table 5. show the NPCR and UACI Values

TABLE V. VALUES OF NPCR & UACI

	NPCR	**UACI**
Lena	99.69%	33.44%
Baboon	99.44%	33.34%

from the apparent outcomes it appears that any change even a slight change to the main picture would result in a greater chance of the encoded image which makes the suggested model is competent and strongly resisting the differential attack.

VI. CONCLUSION

The suggested model is very quick and meets the cryptography principles criteria. The system utilizes the addition of the DNA sequence to scramble the image's three RGB channels pixels based on a random key and utilizes XOR-plus-mod as a confusing procedure by using the genetic algorithm process as a pseudo-random number generation, besides using the crossover and mutation process with DNA decoding for more security, resistance to various attacks, such as differential and statistical attacks, is strongly increased. The scheme is easy, robust and appropriate for image encryption, plus has no problems in mathematics.

REFERENCES

[1] Stallings, W., Network security essentials, Prentice Hall, Fourth edition, 2011.

[2] William Stallings, Lawrie Brown, Computer Security Principles and Practic, Pearson, Third Edition, 2015.

[3] Stallings, W., Cryptography and network security principles and practice (5th ed.), Boston: Pearson, 2014.

[4] Grasha Jacob, A. Murugan, "DNA based cryptography an overview & analysis", International Journal of emerging science 3(1), 2013, pp. 36-42.

[5] Hariram S, Dhamodharan R, "A Survey on DNA Based Cryptography using Differential Encryption and Decryption Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 10, Issue 5, Ver. II, 2015, PP 14-18.

[6] K. Li, S. Zou, J. Xv, "Fast parallel molecular algorithms for DNA based computation: Solving the elliptic curve discrete logarithm problem over gf (2 n)", Journal of Biomedicine and Biotechnology, Hindawi., Vol. 2008, pp. 1–10.

[7] Adleman, "Molecular computation of solutions of combinatorial problems", Science 266, 1994, pp. 1021_1024.

[8] G.Z. Xiao, M.X. Lu, L. Qin, X.J. Lai," New field of cryptography: DNA cryptography", Chinese Science Bulletin 51 ,12, 2006, pp. 1413_1420.

[9] V.Srikanth, Udit Asati, Viswajit Natarajan, T.Pavan Kumar, Teja Mullapudi, N.Ch.S.N.Iyengar, "Bit-Level Encryption of Images using Genetic Algorithm", TECHNIA International Journal of Computing Science and Communication Technologies, VOL. 3, NO.1, July 2010, pp. 546-550.

[10] K. F. Man, Member, K. S. Tang, S. Kwong. "Genetic Algorithms: Concepts and Applications", In: IEEE Transaction On Industrial Electronics, Vol. 43, No.5; October 1996, pp. 519 – 534.

[11] D. E. Goldberg, Genetic algorithms in search, optimization, and machine learning, Reading, MA: Addison-Wesley, 1989.

[12] Qiang Zhang, Ling Guo, Xiaopeng Wei, "Image encryption using DNA addition combining with chaotic maps", Mathematical and Computer Modelling 52, 2010, pp. 2028-2035.

[13] Kuldeep Singh, Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications (0975 – 8887), Vol. 23, No.6, June 2011, pp. 17-24.

[14] Qiang Zhang, Xianglian Xue, XiaopengWei, "A Novel Image Encryption Algorithm Based on DNA Subsequence Operation", The Scientific World Journal ,Vol. 2012, pp. 1- 10.

[15] Saswat K Pujari Gargi Bhattacharjee Soumyakanta Bhoi, "A Hybridized Model for Image Encryption through Genetic Algorithm and DNA Sequence", Procedia Computer Science, Vol. 125, 2018, pp. 165-171.

[16] Adleman. M. L ," Molecular Computation of Solutions to Combinatorial Problems, Science", Vol. 266,1994, pp. 1021- 1024.

[17] Tausif Anwar, Sanchita Paul, Shailendra Kumar Singh "Message Transmission Based on DNA Cryptography: Review" in International Journal of Bio-Science and Bio-Technology. Vol 6, No.5, Issue 30, 2014, pp. 215-222.

[18] Morteza SaberiKamarposhti, Ibrahim AlBedawi, Dzulkifli Mohamad, "A New Hybrid Method for Image Encryption using DNA Sequence and Chaotic Logistic Map,"Australian Journal of Basic and Applied Sciences, Vol. 6, No.3 , 2012, pp. 371-380.

[19] W. C. Chen, Z. Y. Chen, Z. H. Chen et al., "Operational rules of the digital coding of DNA sequences in high dimension space," Acta Biophysica Sinica, Vol. 17, No. 3, 2001, pp. 542–549.

[20] W. Piotr, J.M. Jan, R.R. Witold, L. Bogdan, "Adding numbers with DNA", in: International Conference on Systems, Man and Cybernetics, 2000, pp. 265-270.

[21] Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien, "Public key Cryptography Based on Chaotic Neural Network ", International Journal of Computer Application (IJCA), RS publication, Issue 4, Vol. 4, 2014, pp. 200-218.

[22] Li, T.Y.; Yang, M.G.; Wu, J.; Jing, X. "A novel image encryption algorithm based on a fractional-order hyper chaotic system and DNA computing", Complexity 2017, pp. 1-13.

[23] M. I. YOUSSEF, A. E. EMAM, S. M. SAAFAN and M. ABD ELGHANY, " Secured Image Encryption Scheme Using both Residue Number System and DNA Sequence", The Online Journal on Electronics and Electrical Engineering (OJEEE), Vol. (6) – No. (3), 2012, pp. 656-664.

[24] Narendra K Pareek,"Design and analysis of a novel Digital Image Encryption Scheme", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012, pp. 95-108.

[25] Zhenjun Tang , Ye Yang, Shijie Xu, Chunqiang Yu , Xianquan Zhang, " Image Encryption with Double Spiral Scans and Chaotic Maps", Hindawi Security and Communication Networks, Volume 2019, 2019 , pp. 1-15.

[26] M. Amr Mokhtar, Sameh N. Gobran, El-Sayed A-M. El-Badawy, "Colored Image Encryption Algorithm Using DNA Code and Chaos Theory", International Conference on Computer and Communication Engineering, 2014.

[27] Yue Wu, Joseph P. Noonan, Sos Agaian," NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April 2011, pp. 31

[28] Y. Wang, C. Quan, C. J. Tay, "Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain," Optics Communications, Vol. 330, 2014, pp. 91–98.