Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 6, June 2018, pg.1 – 8

Partial Gray Scale Image Encryption Based on DNA Encoding Technique

Sushma M P[1], Jithendra P R Nayak[2]

[1]M.Tech Student, G. Madegowda Institute of Technology, Karnataka, India
[2]Assistant professor, Dept. of ECE, GMIT Mandya, Karnataka, India
[1] m.p.sushma7@gmail.com; [2] getintojithendra@gmail.com

Abstract*— Increasing need for telemedicine in healthcare industry created a great necessity to secure and transmit the data among medical centres. In this paper, DNA Based Approach for Partial gray scale Image Encryption have been presented. In this algorithm, original gray scale image split into eight binary layers. 4-DNA planes are obtained by applying the DNA encoding process for original gray scale image. Based on the chaotic map sudoku like random image is generated. Random image also undergo DNA encoding process to produce 2 DNA sequence based bit planes. According to random bit plane selection table, select a 2-DNA planes and perform a DNA addition with the chaos based 2-DNA planes. Finally apply the DNA decoding process to get the Partial encrypted gray scale images. Simulation result shows that the proposed algorithm suitable for the medical information security.

***Keywords*— Partial image encryption (PIE), chaotic map, DNA addition**

I. INTRODUCTION

With increasing use of computers leads to an increasing tendency to security and image fidelity verification. Transmitted images may have different applications, such as commercial, military and medical applications. So it is necessary to encrypt image data before transmission over the network to preserve its security and prevent unauthorized access. For example military and law enforcement applications require full encryption. Nevertheless, there is a large spectrum of applications that demands security on a lower level, as for example that ensured by partial encryption (PE) or selective encryption (SE). Such approaches reduce the computational requirements in networks with diverse client device capabilities. In several papers, the distinction between selective encryption (SE), partial encryption (PE) and soft encryption is not very clear. The goal of PE of an image is to encrypt only regions of interest (ROI) which are defined within specific areas of the image. The goal of SE is to encrypt a well-defined range of parameters or coefficients.

yue wu etc.al [10] introduces a novel symmetric image cipher using wave perturbations to permute the original image. using PRNG to perform diffusion operation. Qiang zhang et.al introduced a [13] novel couple images encryption algorithm based on DNA subsequence operation and chaotic systems. This algorithm is not use complex biological operation, but just uses the idea of DNA subsequence operation (such as elongation operation,truncation operation, and deletion operation). And then, do the DNA addition operation under the

Chen's Hyper-chaotic map in this image cipher. sara tedmori etc.al [5] explained a lossless symmetric key encryption based on the harr wavelet transform. image is tranformed into the frequency domain and important subbands are encrypted. this algorithm is designed to shuffle and reverse the sign of each frequency in the transformed image before the image frequencies are transformed back to the pixel domain. qiang zhang etc.al [11] presented a new image encryption based on DNA encoding combined with chaotic system. The algorithm uses chaotic system to disturb the pixel locations and pixel values and then DNA encodings according to quaternary code rules are carried out. At last the image encryption through DNA decoding is achieved. sukalyan som and sayani sen presented [4] a Non-adaptive Partial Encryption of Grayscale Images Based on Chaos. here original grayscale image into its corresponding binary eight bit planes then encrypted using couple tent map based pseudorandom binary number generator (PRBNG). Panuranga H T etc.al [2] all presented a partial image encryption for smart camera to increase the smartness of camera. this algorithm uses hill cipher and control the amount of encryption. Qiang zhang et.al introduced a [12] explained a novel image encryption based on DNA encoding combined with chaotic system is proposed. The algorithm uses chaotic system to disturb the pixel locations and pixel values and then DNA encodings according to quaternary code rules are carried out. The pseudo DNA operations are controlled by the quaternary chaotic sequences. At last the image encryption through DNA decoding is achieved. xingyuan etc.al [6] explained a (6)cryptanalysis on an image encryption based on Chebyshev chaotic map. This algorithm evaluate the following : (1) chosen plaintext attack break the scheme. (2) there exist equivalent keys and wea keys for the encryption scheme . (3) The scheme has low sensitivity to the changes of plain image. Panduranga H T etc.al [3] explains the partial image encryption using block wise shuffling and chaotic map. original image divided into several macro blocks and according chaotic sequence, pixels within the macro blocks are shuffled. The rest of this paper is organized as follows. Section IIexplains the basic theory for DNA encoding and addition. Section III briefly explain the concept of chaotic map. Section III-A describes the proposed partial encryption algorithm. The security of the scheme is evaluated in Section IV. Experimental results described in section V. Section VI concludes the paper.

II. DNA THEORY

A. DNA encoding

DNA computing is a form of computing which uses DNA, biochemistry and molecular biology, instead of the traditional silicon-based computer technologies. DNA computing, or more generally, bimolecular computing, is a fast developing interdisciplinary area. With the rapid development of DNA computing, the researchers presented many biological operations and algebra operations based on DNA sequence. Single-strand DNA sequence is composed by four bases, they are A, C, G and T, where A and T are complement to each other, so are C and G. In the modern theory of electronic computer, all information is expressed by binary system. But in DNA coding theory, information is represented by DNA sequences. So we use binary numbers to express the four bases in DNA sequence and two bits binary number to represent a base. In the theory of binary system, 0 and 1 are complementary, so we can obtain that 00 and 11, 01 and 10 are also complementary. We can use 00, 01, 10 and 11 to express four bases and the number of coding combination kinds is 4! = 24. Due to the complementary relation between DNA bases, there are only eight kinds of coding combinations that satisfy the principle of complementary base pairing in 24 kinds of coding combinations. Table 1 gives eight encoding rules: Example: The binary pixel value of an image is [00111010], so the corresponding DNA sequence is [ATGG] according to the first encoding rule, similarly according to the seventh decoding rule, the decoding sequence is [11001010]. In the proposed algorithm, we put the eight encoding and decoding rules mapped to the eight sub-region of (0,1), and using the seed generated by random number to choose different rules

B. The addition and subtraction operation of DNA sequence

Since the development of DNA computing, scholars have proposed using algebraic operation of DNA sequence to replace the traditional computer algebraic operation. Based on this, we use DNA addition operation to realize DNA sequence matrix computing for R, G, B components. The algorithm of this paper finds out DNA addition and subtraction rules by using mod 2 operations of binary figure when 01 A, 10 T, 00 C, 11 G, and you can find the rules in Table 2.

TABLE I
EIGHT KINDS OF DNA PATTERNS.

0-A	0-A	0-C	0-C	0-G	0-G	0-T	0-T
1-C	1-G	1-A	1-T	1-T	1-A	1-C	1-G
2-G	2-C	2-T	2-A	2-A	2-T	2-G	2-C
3-T	3-T	3-G	3-G	3-C	3-C	3-A	3-A

TABLE II
ADDITION AND SUBTRACTION OPERATION OF DNA SEQUENCE

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

III.CHAOTIC MAP

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behavior regarding complexity, chaotic properties cycle length, chaotic interval, periodic windows, etc., sensitivity to initial conditions and reaction to trajectory perturbations, etc., that influence the structure or behavior of the chaotic encryption system. In fact, some systems have been broken for not considering the weaknesses of the chosen chaotic map and efficiency, it is desirable to provide some independency between the cryptosystem and the chaotic map under consideration. This independency means that, a full knowledge of the selected chaotic map is not needed to fulfill the security and efficiency requirements of a good cryptosystem.
For their mathematical simplicity there are two options: logistic map and tent map. The logistic map is represented by

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

The logistic map chaotic signal used has primary values of X0 2 [0; 1] and r€[3:57; 4].

IV.PROPOSED METHODOLOGY

Block diagram for DNA Based Approach for Partial gray scale Image Encryption as shown in figure 1. This algorithm uses a gray scale image of size mxn. Original gray scale image is split into eight binary plane. 4-DNA planes are obtained by applying the DNA encoding process for gray scale image. Similarly by using chaotic map, a sudoku like random image is generated. This random image also undergo DNA encoding to produce 2-DNA planes. According to random bit plane selection table 3, select a 2-DNA planes and perform a DNA addition with the chaos based 2-DNA planes. Resultant encrypted DNA bit planes are place into the corresponding plane of original gray scale planes. Finally apply the DNA decoding for encrypted original gray scale DNA planes to get partially encrypted gray scale images.

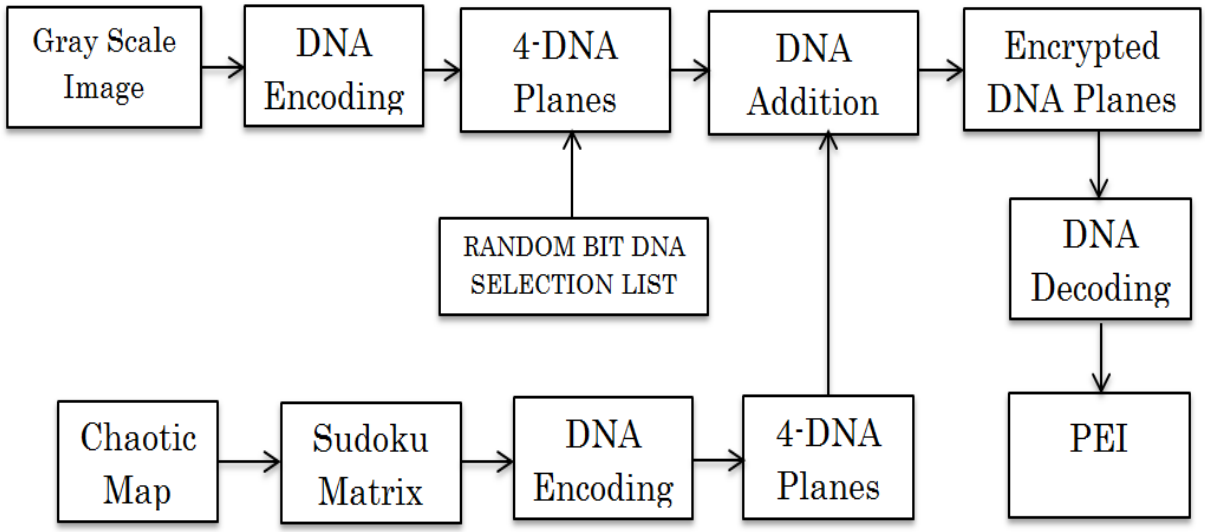


Fig. 1. Block diagram of Proposed DNA Based Approach for Partial Color Image Encryption

TABLE III
RANDOM BIT PLANES SELECTION LIST

Sl.No	Bit Plane changing Number	
1	1	2
2	1	3
3	1	4
4	2	3
5	2	4
6	3	4

Algorithm DNA Encoding process:
1: Consider Gray image I of any size mxn.
2: Pick up each input image pixel and converted into 8-bit binary values.
3: Divide 8-bit binary values into four bit-pairs.
4: Assign a DNA pattern for each two bits pairs.
5: Resultant sequence is DNA sequence.

Algorithm 2 DNA Decoding process:
1: Consider DNA sequence based matrix.
2: Pick each character and converted into 2-bit binary values to obtain a binary sequence.
3: Take 8-bit binary values at a time in binary sequence and convert it into a decimal value to obtain 1D array.
4: Convert 1D array into 2D matrix to get resultant encrypted image.

V. RESULT

Information entropy analysis:

In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(X) of a source x, we have:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \qquad \text{.....2}$$

where X denotes the test image, xi denotes the ith possible value in X, and Pr(xi) is the probability of X =xi, that is, the probability of pulling a random pixel in X and its value is xi. For a truly random source emitting 2N symbols, the entropy is H(X)=N. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be H(X)=8. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Mean Square Error:

Mean squared error (MSE) is defined as an average of the square of the difference between actual image and encrypted image. The MSE is given by the equation

$$\mathrm{MSE} = \frac{1}{\mathrm{MxN}} \sum_{i=1}^{n} \sum_{j=1}^{n} (x(i,j) - y(i,j))^2 \qquad \text{.....3}$$

Where x (i, j) represents the original image and y (i, j) represents the encrypted image and i and j are the pixel position of M x N image.

MSE is zero when x (i, j) =y (i, j).

Number of Pixel Change Rate (NPCR)"

If C1 and C2 are original image and encrypted image respectively. C_1 (i, j) and C_2 (i, j) are original image pixel and encrypted image pixel respectively. The NPCR is then defined as,

$$NPCR = \frac{\sum i,j\ D(i,j)}{MxN} \text{ X } 100\% \quad \text{.....4}$$

Where, D is bipolar array.

$$D(i,j) = \begin{cases} 1, & C1(i,j) \neq C2(i,j) \\ 0, & \text{otherwise} \end{cases}$$

Peak Signal to Noise Ratio (PSNR):

The peak signal to noise ratio is evaluated in decibels and is inversely proportional to MSE. It is given by the equation

$$PSNR = 10 \log_{10}\left(\frac{255}{MSE}\right) \quad \text{.....5}$$

Unified average changed intensity (UACI):

It is used measure the intensity rate difference between the original image and encrypted image.

$$UACI = \frac{1}{N}\left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255}\right] \quad \text{.....6}$$

If C_1 and C_2 are original image and encrypted image respectively. C_1 (i, j) and C (i , j) are original image pixel and encrypted image pixel respectively.

Universal Image Quality Index (UIQ):

The UIQ indicates the structural similarity between two images. The UIQ lies between [-1, 1] and the value closer to 1, the greater similarity in the images. Mathematically, UIQ is defined as in [7].

$$UQI(x,y) = \frac{\sigma_{xy}}{\sigma_x \sigma_y} * \frac{2\mu_x \mu_y}{\mu_x^2 + \mu_y^2} * \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \qquad (7)$$

Structural Similarity Index Measure (SSIM):

The SSIM is the extended version of the UIQ index. The SSIM lies between [-1, 1]and the value closer to 1, the greater similarity in the images. Mathematically, SSIM is defined as in [9].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C1)(2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C2)} \quad (8)$$

$$MSSIM = \frac{1}{M}\sum_{j=1}^{M} SSIM(x_j, y_j) \quad (9)$$

where C1, C2 are two constants and are used to stabilize the division with weak denominator.

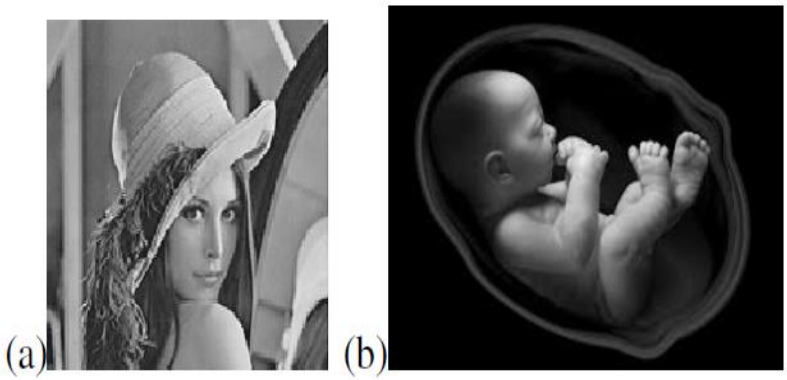


Fig. 2. Test Images (a)Lena (b)Baby in womb

TABLE IV
RESULTS FOR BABY IN WOMB IMAGE

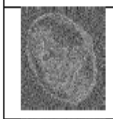
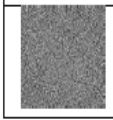
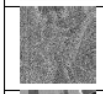
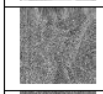
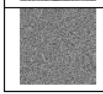
PIE	Ent_in	Ent_enc	MSE	PSNR	NPCR	UACI	SSIM	UQI
	5.09233	6.39102	10.62282	37.86841	94.14063	2.46770	0.53644	0.73267
	5.09233	6.43219	43.13684	31.78232	94.14063	8.92809	0.16663	0.49658
	5.09233	6.89672	17.58415	35.67959	94.14063	36.17313	0.00755	0.25066
	5.09233	6.54968	41.13158	31.98905	94.14063	9.97367	0.15692	0.49257
	5.09233	7.06471	19.76694	35.17141	94.14063	37.23681	0.00726	0.24997
	5.09233	7.11555	28.57933	33.57028	94.14063	41.49031	0.00368	0.25002

TABLE V
RESULTS FOR LENA IMAGE

PIE	Ent_in	Ent_enc	MSE	PSNR	NPCR	UACI	SSIM	UQI
	7.43112	7.48439	21.58443	34.78940	94.14063	2.11488	0.82055	0.99980
	7.43112	7.78056	93.66573	28.41500	94.14063	8.01530	0.37613	0.98186
	7.43112	7.99435	92.32877	28.47743	94.14063	28.51369	0.00197	0.85722
	7.43112	7.78730	90.45192	28.56663	94.14063	8.36608	0.36942	0.98197
	7.43112	7.99721	97.10056	28.25859	94.14063	28.83081	0.00214	0.85720
	7.43112	7.99611	116.20056	27.47872	94.14063	28.64220	0.00835	0.87739

From the Table-IV to Table-VI, we can observed that, amount of encryption varies as the changing of a bit planes varies. By changing the bit plane, we can control the amount of encryption as per our requirements and also for a lower bit plane changes, amount of encryption is very less and for a higher bit planes changes, amount of encryption is more.

VI. CONCLUSIONS

In this paper, DNA Based Approach for Partial Gray scale Image Encryption have been presented. In this algorithm, original Gray scale image split into eight binary layers. 4-DNA planes are obtained by applying the DNA encoding process for original Gray scale image. From the experimental results, we conclude that amount of encryption varies as the changing of the bit plane varies. This type of method useful in the medical information security, because small amount of encryption enough to secure the medical data and also reduces the computational cost. FPGA architecture of proposed algorithm can be used in the smart cameras.

REFERENCES

[1] Jawad Ahmad and Fawad Ahmed. Efficiency analysis and security evaluation of image encryption schemes. computing, 23:25, 2012.
[2] SK Naveenkumar, HT Panduranga, and Kiran. Partial image encryption for smart camera. In Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, pages 126–132. IEEE, 2013.
[3] HT Panduranga, SK Naveenkumar, and Kiran. Partial image encryption using block wise shuffling and chaotic map. In Optical Imaging Sensor and Security (ICOSS), 2013 International Conference on, pages 1–5. IEEE, 2013.
[4] Sukalyan Som and Sayani Sen. A non-adaptive partial encryption of grayscale images based on chaos. Procedia Technology, 10:663–671, 2013.
[5] Sara Tedmori and Nijad Al-Najdawi. Image cryptographic algorithm based on the haar wavelet transform. Information Sciences, 269:21–34, 2014.
[6] Xingyuan Wang, Dapeng Luan, and Xuemei Bao. Cryptanalysis of an image encryption algorithm using chebyshev generator. Digital Signal Processing, 25:244–247, 2014.
[7] Zhou Wang and Alan C Bovik. A universal image quality index. Signal Processing Letters, IEEE, 9(3):81–84, 2002.
[8] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: from error visibility to structural similarity. Image Processing, IEEE Transactions on, 13(4):600–612, 2004.

[9] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: From error visibility to structural similarity. Image Processing, IEEE Transactions on, 13(4):600–612, 2004.
[10] Yue Wu, Yicong Zhou, Sos Agaian, and Joseph P Noonan. A symmetric image cipher using wave perturbations. Signal Processing, 102:122–131, 2014.
[11] Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using dna addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11):2028–2035, 2010.
[12] Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using dna addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11):2028–2035, 2010.
[13] Qiang Zhang and Xiaopeng Wei. A novel couple images encryption algorithm based on dna subsequence operation and chaotic system. Optik-International Journal for Light and Electron Optics, 124(23):6276–6281, 2013.

