IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Image encryption using dynamic DNA encoding and pixel scrambling using composite chaotic maps

To cite this article: K Aditya *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **872** 012045

View the article online for updates and enhancements.

Recent citations

- Design of multi-parameter composite modulated signal for anti-deceptive jamming
  Xinyu Dao *et al*

Image encryption using dynamic DNA encoding and pixel scrambling using composite chaotic maps

Aditya K[1], Ashish K Mohanty[1], G Aravinth Ragav[1],V Thanikaiselvan[1] and Amirtharajan R[2]

[1] School of Electronics Engineering (SENSE), Vellore Institute of Technology (VIT), Vellore, 632 014, India

[2] School of Electrical & Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

thanikaiselvan@vit.ac.in

Abstract: In this digital world, encryption plays an important role in various domains. Securing the information is the main goal when transfer of information takes place. Image encryption is a very important part of this as it applies to various domains like medical, multimedia, defence etc. A new method for image encryption is proposed here taking into account the "confusion-diffusion" structure. While working with secure data, requirements like fast computation, compression and processing are important issues. Deoxyribonucleic Acid (DNA) encoding has the capability to cope up with this requirement. In this paper a new algorithm is proposed based on composite chaos map for pixel scrambling and hence image encryption. First the algorithm takes the image and XORs with a composite chaotic map which further goes into dynamic DNA encoding followed by pixel scrambling which results in the image being very random thus it becomes less prone to attacks. The method discussed performs efficiently as shown in the experimental results.

Keywords: Composite Chaotic Map, Dynamic DNA encoding, Pixel Scrambling, Image Encryption.

1. INTRODUCTION

As technology is getting advanced day-by-day, an image is vastly used in all the domains. Hence, a powerful and an efficient cryptographic method is required for at ease image transmission and storage. The existing techniques like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) for encryption does not fulfil the requirements of image encryption as they have low performance measures in terms of efficiency and security [1]. To achieve a secure cryptosystem, an image encryption algorithm consists of many phases such as permutation, substitution, diffusion, confusion etc.

Cryptography based on DNA is predicated on the various DNA characteristics in accordance with methods to increase safety and efficiency. The advantages of these methods are the self-assembling standards of the Molecules, capability of computing parallelly and huge storage capabilities [2]. After years of research and study on DNA, researchers have concluded that the DNA sequence has a quaternary combination, which can be compared to the semiconductors on & off system[3]. An equivalent phenomenon which can be seen in a deterministic system is chaos and is a very interesting and important topic in the field of non-linear science. A chaotic system has the ability of generating sequence repetitively, rapidly which makes it perfect for encryption of images. It is because chaos has a natural reference to cryptography so more and more scientists and researchers are focusing on the chaotic image encryption.

Using DNA encoding technique, the data can be stored and calculated using randomness of the nucleotides [4] & [5]. A method was introduced called OTP which was based on DNA. The cryptography had two such kind of schemes [6]. Proposed a cryptography method that made use of deoxyribonucleic acid sequence [7]. Took the help of these sequences to resolve the key distribution issue [8]. Introduced a scheme that used a method of contrast mapping to insert values into any random part of a deoxyribonucleic acid sequence. Also, this didn’t affect the function of the acid [9].

The encryption methods based on DNA, results in high computing power and also in the capabilities of storing the data. In the recent years, many algorithms were introduced which combined the traditional ciphers and the DNA to result in more efficient algorithms. In 2014, an algorithm was proposed which was based on chaos map and encoding [10]. In the year 2015, an algorithm that was based on DNA and logistics mapping (2D) [11]. An encryption algorithm which worked on the combination of DNA and chaos map [12].

This paper has a target of increasing the efficiency and security of the encryption algorithm over the older cryptosystem methods such as Elliptic Curve Cryptography (ECC), *Rivest–Shamir–Adleman* (RSA) etc. The multi-fold security makes this method more efficient. The rest of this paper is presented in the following order – Section 2 has the Related Works presented in it to discuss about the various maps that are used in the paper. The methodology, algorithm and the steps used are explained in section 3 while the next section- Section 4 illustrates the results of encryption of five test images. Section 5 concludes the paper.

2. RELATED WORKS

2.1. Dynamic DNA Encoding

Every DNA molecule has 4 DNA nucleotides which are cytosine (C), adenine (A), thymine (T), and guanine (G). The stability of a DNA molecule is based on the Hydrogen (H)-bonds formation between the nucleotides of two single-stranded DNA molecules. G and C nucleotides are paired by 3 H-bonds, whereas the A and T nucleotides are paired by 2 H-bonds as per the base pairing principle by Watson-Crick. Naturally they combine quaternary and so, the permutations and combinations of these base nucleotides store the information and also helps in further calculations. The pixel confusion in DNA coding is achieved by the definition of the rules shown in table1.

The paper proposes a dynamic algorithm by using a chaotic map to dynamically index the rule selection in the confusion process for every pixel, making the confusion process even harder for attacks. For example, if the value in sixty-sixth row and sixty-fifth column of the original image is

198, which in binary is [11000110], the encoded DNA pixel sequence is [ATGC] considering the developed dynamic encoding technology to select the encoding rule 8 for that pixel.

Table 1.DNA Rules for Encoding

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

Table 2 containing the base transforming rule is used to induce disturbance in the pixel value.

Table 2.DNA Rules for XOR

XOR	**A**	**C**	**G**	**T**
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

2.2. Composite map pixel scrambling

Image scrambling is a good method for providing security to image data by making it difficult to decrypt it for unauthorized users. Our algorithm divides the image matrix into 16 sub-blocks as shown in the figure 1 and each of these blocks is rotated to a measure of 90^o in the clockwise direction. These rotated blocks undergo pixel scrambling separately using the key generated from 8 different chaotic maps. Every key is indexed to two of these 16 blocks using a separate chaotic sequence of length 16 containing unique indexes. This algorithm not only provides randomness to the chaotic map allotment to these blocks but also provides chaos at the scrambling sequences by the individuality provided by the eight maps used.

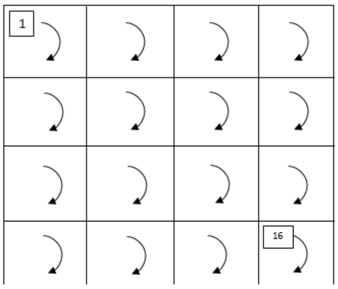


Figure 1. Scrambling Procedure

2.3. XOR function

The bitwise XOR operation is used here as a part of a more complex encryption algorithm. XOR is used as a step after every major encryption process in every iteration of the procedure to increase the complexity of encryption. Two different chaotic sequences are generated. Each of it is circular-shifted with itself to generate a key. The two such keys generated are XOR-ed with the image matrix to result in a resultant image matrix.

2.4. Chaotic mappings

Chaotic maps use the chaos theory on deterministic systems whose behaviour over time can be predicted by theory. The main idea that is used here in these maps is that a minute difference at the beginning of the mapping can result in a huge change in the final result as time increases. In these maps, the uncertainty increases exponentially with time. Several chaotic maps are prepared till date [13] and few of them that are used in proposed algorithm are explained below.

*2.4.1 Quadratic map.*This map is a very primitive chaotic map, and its classical version is,

$$P_{n+1} = a - (P_n)^2 \qquad (1)$$

where a is the parameter for chaos and n being the total iterations. The map's chaos is due to its nonlinearity. When a is in the range of [1.5, 2], the system turns chaotic, which can be seen in figure 2.

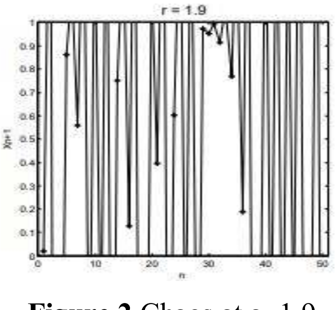


Figure 2. Chaos at a=1.9.

*2.4.2 Logistic map.*A straightforward easy map is the logistic map with the polynomial equation:

$$P_{n+1}=b*(P_n)*(1-P_n) \qquad (2)$$

where 'b' is the bifurcation factor and P_n implying n^th generation population and. As the growth rate 'b' is altered, this map shows a range of behaviour the change in initial conditions makes the map very sensitive. When P_n belongs to [0, 1], Parameter 'b' belongs to [3.569946, 4] and also $b \in$ N, the generated sequence illustrates chaos as shown in the bifurcation diagram, figure 3.

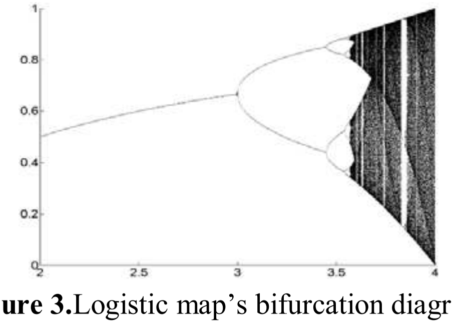


Figure 3. Logistic map's bifurcation diagram

*2.4.3 Singer map.*The Singer map [14] represents the iterated function or otherwise the chaotic map as defined by:

$$P_{n+1}=r* (7.86*P_n-23.31*P_n^2+28.75*P_n^3-13.3*P_n^4) \quad (3)$$

where r, the chaotic parameter lies in [0.9, 1.08]. The chaotic sequence is generated in the intervalP$_n$ ϵ [0, 1].

*2.4.4 Sine map.*This chaotic sequence is generated from an iterative function whichcontains sine itself and is defined as:

$$P_{n+1} = x * \sin(\pi * P_n) \quad (4)$$

where $0 \leq x \leq 1$. The sequence obtained in this map is in the interval Pn ϵ [0, 1].

*2.4.5 Piecewise map (pwlcm).*The pwlcm is an iterative function consisting of four linear parts that are calculated by the function:

$$A_{n+1} = \begin{cases} \frac{A_n}{p}; \mathbf{0} \leq A_n < p \\ \frac{A_n-p}{0.5-p}; p \leq A_n < 0.5 \\ \frac{1-A_n-p}{0.5-p}; \mathbf{0.5} \leq A_n < 1-p \\ \frac{1-A_n}{p}; \mathbf{1} - p \leq A_n < 1 \end{cases} \quad (5)$$

where p ϵ [0, 0.5]. The resultant chaotic sequence A$_n$ is in the interval [0, 1].

*2.4.6 Lorenz map.*Lorenz map is determined by the following iterative method:

$$a' = x(b-a)$$
$$b' = y*a-b-a \quad (6)$$

where x denotes Prandtl number, y denotes Rayleigh number and z being an aspect-ratio. The apostrophe notation is used to denote the derivatives w.r.t. time.Though not all solutions of the Lorenz system are chaotic, when y =28, a=10 and z=8/3, the solutions are chaotic in nature.

*2.4.7 Ikeda map.*A dynamic system over discrete-time given by the complex map:

$$a_{n+1}=1+x(a_n \cos t_n - b_n \sin t_n) \quad (7)$$
$$b_{n+1}=x(a_n \sin t_n + b_n \cos t_n)$$

where x is a chaos parameter and $t_n=0.4-6/(1+a_n^2+b_n^2)$. The map has a chaotic attractor for values of x>*=0.6*.

*2.4.8 Henon map.*Being one of the most used variant of dynamic systems that showschaoticnature, this map is a dynamic system of discrete-time. A new point is mapped to a point (x_n, y_n) in the plane by this map.

$$P_{n+1}=1-x*P_n^2+Q_n (8)$$
$$Q_{n+1}=y*P_n$$

where the 2 parameters of values, x = 1.4 and y = 0.3 makes it a classical versionof the Henon map which always stays chaotic because for few other values of thesetwo parameters, x and y the map might be either chaotic, intermittent, or can evenconverge to a periodic orbit making it non-chaotic.

2.4.9 Coupled Logistic-Sine (CLS) map.

$$P_n=\mathrm{mod}(rP_n-1*(1-P_n-1) + (4-r) *\sin(\pi P_n-1)/4,1) \tag{9}$$

The system is chaotic in [0, 4] interval.

*2.4.10 Coupled Logistic-Tent (CLT) map.*The representation of the map is as follows-

$$A_n=\begin{cases} \mathbf{mod}(\boldsymbol{\beta A_{n-1}} * (\mathbf{1}-\boldsymbol{A_{n-1}}) + \frac{(\mathbf{4}-\boldsymbol{\beta})*\boldsymbol{A_{n-1}}}{\mathbf{2}}, \mathbf{1}); \\ \quad \boldsymbol{for\ A_n} < 1/2 \\ \mathbf{mod}(\boldsymbol{\beta A_{n-1}} * (\mathbf{1}-\boldsymbol{A_{n-1}}) + \frac{(\mathbf{4}-\boldsymbol{\beta})*(\mathbf{1}-\boldsymbol{A_{n-1}})}{\mathbf{2}}, \mathbf{1}); \\ \quad \boldsymbol{for\ A_n \geq 1/2} \end{cases} \tag{10}$$

where$\boldsymbol{\beta}$ is the control parameter and makes the system chaotic in the interval [0,4].

*2.4.11 Circle map.*This 1-D map, maps itself to a circle. The equation is

$$\beta_{n+1}=\beta_n+ \theta-(K/2\pi) * \sin(2\pi\beta_n) \tag{11}$$

where β_{n+1} is calculated to mod 1. This map has 2 parameters, namely, θ which is the term for externally applied frequency, and K being a term for strength of nonlinearity.

Table 3 presents the chaotic maps used in this algorithm and their chaotic ranges with the remarks of at what step is the chaotic map being used.

Table 3. Parameters Used and Its Chaos Ranges

S. No.	Chaotic Map	Parameters/Chaos Range	Remarks
1.	Quadratic	a = {1.5,2}, n	Used in pixel scrambling
2.	Logistic	b = {3.56, 4}, n	Used in DNA encoding, pixel scrambling
3.	Singer	r= {0.9,1.08}, n	Used for chaotic map selection in pixel scrambling
4.	Sine	x= {0,1}, n	Used in DNA encoding, pixel scrambling
5.	Pwlcm	A_n = {0,1} p= {0,0,5}	Used in pixel scrambling
6.	Lorenz	y =28, a=10 and z=8/3	Used in pixel scrambling
7.	Ikeda	x> = {0.6}	Used in pixel scrambling
8.	Henon	x= {1.4};y= {0.3}	Used in pixel scrambling
9.	Tent	b=2	Used in pixel scrambling

3. PROPOSED METHODOLOGY

3.1. Encryption

The flow chart proposed algorithm is shown in figure 4. This encryption process hasseveral steps that are described below:

*Step 1.*Grayscale input image *im*is taken as a 2-D matrix I1of size *m* x *n*.

*Step 2.*The XOR function generates two keys k1 & k2 from two chaotic maps. Key k1 is XORed with I1and the resultant is XORed with key k2 to obtain image matrixI2.

*Step 3.*A chaotic logistic map is used for the rule selection during the dynamic DNA encoding process. The DNA encoded Matrix is later DNA-XORed*(table 2)* with a DNA Encoded chaotic SINE map. The DNA-XORed Matrix is then encoded with Codebook rule 3 *(table 1)* and then converted into an image matrix I3.

Step 4. Step 2 is repeated with image matrix I3 to produce image matrix I4.

Step 5. The image Matrix I4 is divided into 16 sub-blocks. A total of 8 chaotic maps are used inthe pixel scrambling process to permute the pixel position of the image matrix I4. A Singer map is used to randomize the use of these 8 chaotic maps on the 16 sub-blocks. Finally, these 16 sub-blocks are merged into image matrix I5.

Step 6. Step 2 is repeated with image matrix I5 to produce image matrix I6.

*Step 7.*A second iteration of encoding and scrambling process takes place by performing the *steps- 3 to 6* on Image matrix I6 generating the final transmitted encrypted image.

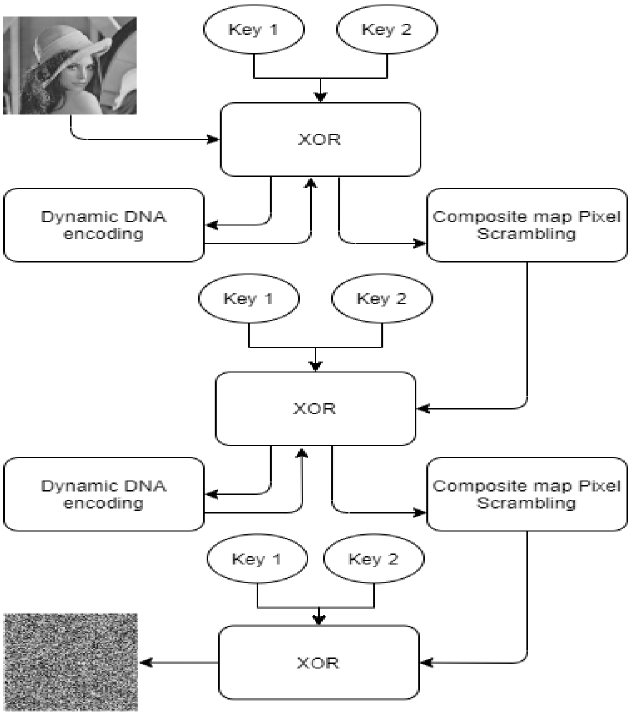


Figure 4. Encryption Algorithm

3.2. Decryption

The decryption process has several steps that are described below:

*Step 1.*The initial conditions and control parameters for every chaotic map and the encrypted matrix are obtained. Decryption process works in the opposite order of the encryption.

*Step2.*The Reverse XOR works in the opposite way of XOR. The encrypted image is XORed with key k_2& the result is then XORed with key k_1.

Step 3. For pixel unscrambling, the 8 maps used for pixel scrambling should be regenerated and singer map with same initial conditions would give the indexes of the 8 chaotic maps to be used for unscrambling. The result from *step 2* is be divided into 16 sub blocks and 8 maps are used to unscramble the image matrix.

Step 4. Step 2 is repeated on the result obtained from *step 3.*

*Step 5.*Chaotic SINE map is generated to create a chaotic sequence which is used to create theDNA decodedsequence. The same DNA-XOR truth table is used to decrypt the image matrix obtained from *step 4* and the dynamic DNA decoding process takes place followed by Reverse XOR.

*Step 6.*A second iteration of the decoding and unscrambling process happens performing the *steps- 2 to 5* generating the original image.

4. RESULTS

4.1. Performance Analysis

*4.1.1 Histogram Analysis.*Input and encrypted image histograms are plotted. Originalimage's histogram shows a non-uniform form whereas the histogram of encrypted image shows uniform nature, proving that the working of DNA encoding & pixel scrambling by chaotic maps.

*4.1.2 NPCR and UACI.*Number of Pixel Change Rate (NPCR) and Unified Average Changed Intensity (UACI) [15] are metrics used to assess the robustness of theencryption process for protection against attacks mainly spatial attacks. Let P^1(j, k) is pixel value at point (j, k) before encryption and P^2 (j, k) is pixel value at point (j, k) after encryption and F be the largest pixel to fit.

$$D\,(\mathrm{j,\,k}) = \begin{cases} \boldsymbol{0, if\ P^1(j,k) = P^2(j,k)} \\ \boldsymbol{1, if\ P^1(j,k) \neq P^2(j,k)} \end{cases}$$

$$\boldsymbol{NPCR = \sum \frac{D(j,k)}{N} * 100\%} \qquad (12)$$

$$\boldsymbol{UACI = \sum \frac{|P^1(j,k) - P^2(j,k)|}{(F.N)} * 100\%}$$

*4.1.3 Correlation Coefficient.*A statistical metric used to evaluate the similarity between variables and gives information about the relationship between two adjacent pixels in diagonal, horizontal and vertical, directions. Lower the value of correlation coefficient between two pixels, better will be the confusion in the image. A negative correlation coefficient between 2 adjacent pixels shows an inverse relationship between them.

*4.1.4 Structural Similarity Index (SSIM).*A perceptual metric which evaluates the degradation of image quality due to external factors. It includes luminance masking and contrast masking terms. In case of spatial damages to the image SSIM can be a reliable metric for quantifies perceived change in structural information.

4.2. Simulation Results

MATLAB R2019a software was used to develop and testthis algorithm. Lena.jpg, Cameraman.tif, peppers.png, canoe.tif and tape.png are the testimages used. All the images are demo MATLAB images preloaded in the software built.

As per table 4(b) Entropy for every image tested lies in range >7.99 which is ideal for an encrypted image. The correlation between pixels is very less (ideal) in all the imagestested.

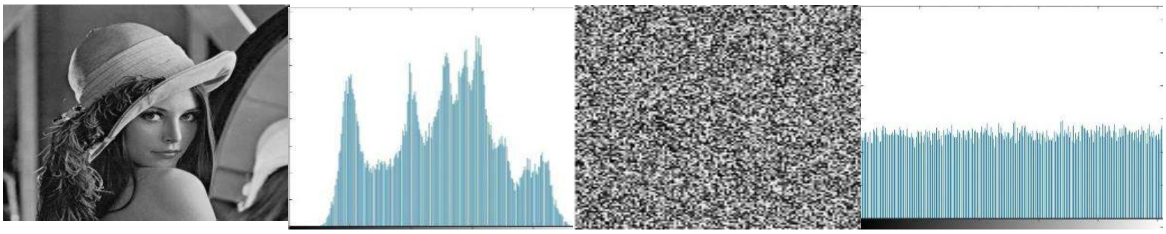
NPCR & UACI quantities were also taken into account for testing of strength of the algorithm. NPCR lies in between 99.36-99.56 whereas UACI is 33% ideal for anencryptedimage. SSIM was also considered between the original and the encryptedimage.Forall test images SSIM was less than 1%. Correlation coefficient between the original and encrypted images were taken which was well under 10% in all the cases. The SSIM and correlation coefficient values can be seen in table 4(a).

Plots of Horizontal, Vertical, and Diagonal Correlation are also shown in figure 7. These images show that the correlation of original image pixel intensifies in a particular rangewhereas the encrypted image's horizontal, vertical, diagonal correlation of pixels remainuniform. Figure 5 shows the original and the encrypted images and their respective histograms. It can be observed that the encrypted image histogram displayed is evenly spreadout as per requirements.

These results imply that this algorithm has a high key sensitivity, *strong key space* which is *not crack-able by brute force*, performance parameters which are ideal as per standards.

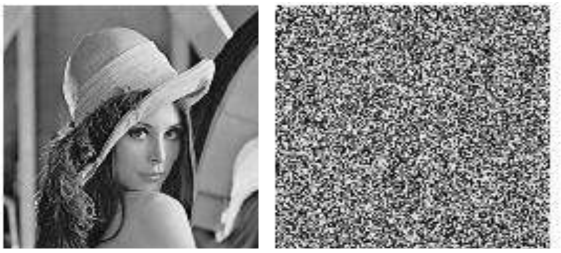
Table 4 (a).*SSIM & Correlation Coefficient*

Test Images	SSIM	Correlation Coefficient
Lena	0.0102	0.0031
Cameraman	0.0069	-0.0072
Peppers	0.0090	0.0022
Canoe	0.0086	-0.0029
Tape	0.0071	-0.0020



(5.1) (5.2) (5.3) (5.4)

Figure 5. Experimental results: (5.1) Original image; (5.2) Histogram of original image; (5.3) Encrypted image; (5.4) Histogram of encrypted image



(a) (b)

Figure 6. Decrypted Images: (a) Decrypted through Key Set – 1 from table 5; (b) Decrypted through Key Set – 2 from table 5

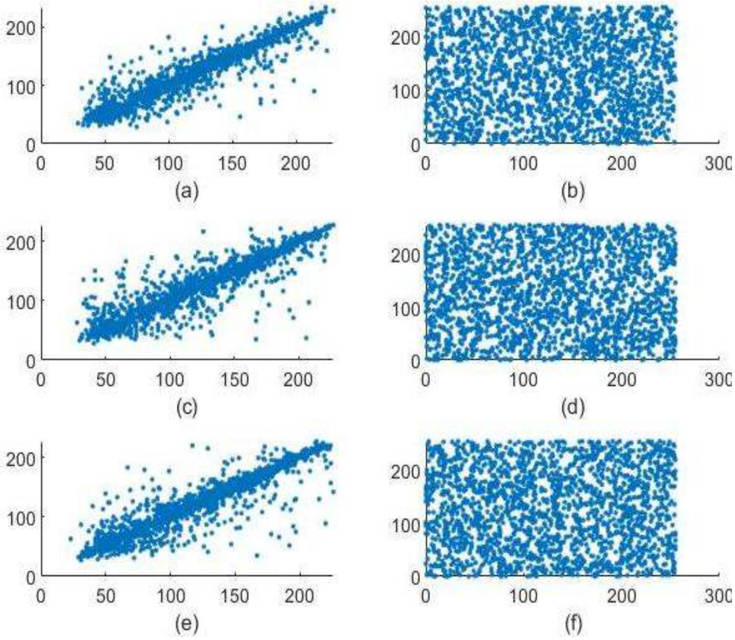


Figure 7. Experimental results for; (a) Horizontal Correlation-Original Image; (b) Horizontal Correlation-Encrypted Image; (c) Vertical Correlation-Original Image; (d) Vertical Correlation-Encrypted Image; (e) Diagonal Correlation-Original Image; (f) Diagonal Correlation-Encrypted Image.

Table 5 shows different key sets for the proposed algorithm. Key Set-1 is the original set used at encryption side. Key Set-2 is the changed set at the underlined position. Figure 6 shows that Key-set 1 can decrypt the encrypted image correctly, Key Set-2 with changed value couldn't decrypt. Key Space for this algorithm is $10^{(\text{No of parameters})*(\text{No of decimals in each})} = 10^{180}$.

Table 4(b). Performance analysis Original and Encrypted Image

TEST IMAGES	ENTROPY		CORRELATION COEFFICIENTS						NPCR (%)	UACI (%)
	ORIGINAL	ENCRYPTED	ORIGINAL			ENCRYPTED				
			HORIZONTAL	VERTICAL	DIAGONAL	HORIZONTAL	VERTICAL	DIAGONAL		
Lena	7.4331	7.9974	0.9455	0.9726	0.9211	-0.0007	0.0028	-0.0019	99.60	33.46
Cameraman	7.0097	7.9977	0.9334	0.9592	0.9086	0.0045	-0.0019	00015	99.60	33.46
Peppers	6.9836	7.990	0.9809	0.9783	0.9630	-0.0022	0.0019	-0.0019	99.60	33.46
Canoe	7.4132	7.994	0.7810	0.8130	0.7301	0.0025	00015	-0.0016	99.60	33.46
Tape	6.7254	7.9973	0.9915	0.9736	0.9697	-0.0041	0.0009	-0.0058	99.6	33.46

Table 5. Key Sensitivity Analysis

Functions with Chaotic Map Initial Parameters	Key Set-1 (Original Set)	Key Set-2 (Underlined Value Changed)
XOR Function Parameters - K_1	Y1=1.9506457812	Y1=1.9506457812
	Y2=0.2004547845	Y2=0.2004547845
	Y3=0.1003695214	Y3=0.1003605214
Dynamic DNA Encoding Parameters - K_2	Y1=0.9999994587	Y1=0.9999994581
	Y2=3.9999993698	Y2=3.9999993698
Composite Chaotic Maps - K_3	Y1=16.1547852365	Y1=16.1547852365
	Y2=45.9214146983	Y2=45.9214146983
	Y3=3.9999987412	Y3=3.9999987412
	Y4=0.0100054756	Y4=0.0100054756
	Y5=0.9452147836	Y5=0.9452147836
	Y6=1.4000000001	Y6=1.4000000001
	Y7=0.3000000001	Y7=0.3000000001
	Y8=0.4000002111	Y8=0.4000002111
	Y9=3.9999998634	Y9=3.9999998634
	Y10=0.9999944552	Y10=0.9999944552
	Y11=3.9998989899	Y11=3.9998989899
	Y12=0.5036000102	Y12=0.5036000102
	Y13=0.2030049872	Y13=0.2030049872

5. CONCLUSION

An Encryption algorithm using Dynamic DNA Encoding and Pixel Scrambling using Composite Chaotic Maps is proposed. Scrambling was done by 8 different chaotic maps where selection of these maps was done by another chaotic map. The diffusion of the pixel values was done dynamic DNA encoding. The DNA encoding was done through XOR of an encoded chaotic map and encoded image pixel values. A separate XOR function with 2 different maps was also embedded after every step. The result analysis showed that two iterations of DNA encoding and pixel scrambling, effectively resists attacks like plaintext, differential, spatial and statistical, making it a secure and capable encryption application.

REFERENCES

[1] L. Y. Zhang *et al*. 2017, On the security of a class of diffusion mechanisms for image encryption, *IEEE Transactions Cybern*., vol. **48**, no. 4, pp. 1–13.

[2] O. Tornea. 2013, Contributions to DNA cryptography: applications to text and image secure transmission,*Université Nice Sophia Antipolis; Technical University of Cluj-Napoca* (Roumanie).

[3] X. Zhang *et al*2017, Fluorescence resonance energy transfer-based photonic circuits using single stranded tile self-assembly and DNA strand displacement, *Journal of Nanoscience and Nanotechnology*, vol. **17**, no. 2, pp. 1053–60

[4] Jonathan P. L Cox 2001, Long-term data storage in DNA, *Trends in Biotechnology*, Volume **19**, Issue 7, Pages 247-50

[5] X. Zhang, Jin X. et al 2009, Application of a novel IWO to the design of encoding sequences for DNA computing*,Computers & Mathematics with Applications*Volume **57**, Issues 11–12, Pages 2001-08

[6] Gahlaut A., Bharti A., Dogra Y., Singh P. 2017, DNA Based Cryptography, *International Conference on Information, Communication and Computing Technology*, pp 205-15

[7] Jie Chen 2003, A DNA-based, biomolecular cryptography design, *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS '03.*, Bangkok, pp. III-III.

[8] K. Tanaka, A. Okamoto, et al 2005, Public-key system using DNA as a one-way function for key distribution*,Biosystems*Volume **81**, Issue 1, Pages 25-29

[9] H. Mousa, K. Moustafa, W. Abdel-Wahed, and M. Hadhoud 2011,Data hiding based on contrast mapping using DNA medium," *International Arab Journal of Information Technology*, Vol. **8**, No. 2.

[10] Y. Liu, Q. Zang, and X. Wie 2012, A RGB image encryption algorithm based on DNA encoding and chaos map*,Computers & Electrical Engineering*Volume **38**, Issue 5, Pages 1240-1248.

[11] Wang, X., Zhang, Y. & Zhao, Y. 2015 A novel image encryption scheme based on 2-D logistic map and DNA sequence operations, *Nonlinear Dyn***82**, 1269–80

[12] X. Chai, *et al*2017, A novel chaos-based image encryption algorithm using DNA sequence operations, *Optical Lasers Engineering*, vol. **88**, pp. 197–213, 2017.

[13] L. Chunli and L. DongHui 2012, Computer network security issues and countermeasures, 2012 *IEEE Symposium on Robotics and Applications (ISRA)*, Kuala Lumpur, pp. 328-31.

[14] A. G. Tomida 2008, Matlab Toolbox and GUI for Analyzing One-Dimensional Chaotic Maps, *2008 International Conference on Computational Sciences and Its Applications*, Perugia, pp. 321-30.

[15] Y. Wu, J. P. Noonan, S. Agaian 2011, NPCR and UACI randomness tests for image encryption, *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 31-3.