A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis

Aradhana Soni
School Of Computer Engineering,
KIIT University, Bhubaneswar, India

Anuja Kumar Acharya,
School Of Computer Engineering,
KIIT University, Bhubaneswar, India

ABSTRACT
Chaotic based image permutation and DNA encoding methods are used extensively in the area of the image encryption. This paper presents a hybrid approach of chaos and DNA encoding methods for image encryption. Chaos sequence is used for permutation and DNA Encoding is used for the diffusion process. Index based chaotic sequence is generated using 1D logistic map for permutation; and DNA sequence matrix is obtained by encoding the permuted image and index based chaotic sequence using DNA encoding rule. The DNA matrices are added using DNA addition operation to generate a new matrix. The generated matrix is decoded using DNA decoding rule and encrypted the image is produced. The proposed approach has two unique characteristics: (i) the way integer sequence is generated from the real valued chaotic logistic sequence; and (ii) the formation of the encoded DNA key matrix. The simulation results indicate that the proposed algorithm is highly secure, is resistant to statistical attacks, and has a larger key space.

Keywords

Image encryption; Chaotic map; Logistic Map; Permutation; Diffusion;

1. INTRODUCTION
In order to restrict unintended recipients from viewing confidential and potentially dangerous data, an encryption scheme is a must in modern day electronic communication. Varieties of encryption algorithms have been proposed in the past to maintain the data confidentiality. However, most of the traditional text based encryption algorithms such as AES and IDEA are not suitable for image encryption.
This paper proposes a method for image encryption, where DNA encoding method is used for the diffusion process; which increases the difficulty in cryptanalysis for the intruder. Also, the method generates the correlation factor of adjacent pixels to a low value. The chaotic based systems are highly sensitive to initial condition, i.e.: a small change in the initial condition can drastically change the long-term behavior of the system. Chaotic sequences produced by chaotic maps are pseudo-random sequences; and have very complex structures, which makes it difficult to analyze and predict the data. In other words, chaotic systems can improve the security of encryption systems [1-3]. Matthews work was the first one to report use of discrete chaotic dynamical systems in cryptography [4]. General permutation–diffusion architecture for chaos-based image encryption was employed in Refs [5-9]. In the permutation stage, the image pixels are relocated, but their values remain unchanged; whereas the pixel values are modified in the diffusion stage.
In the proposed approach, an index based integer sequence is used for pixel permutation, and DNA encoding is used for the diffusion process. The integer sequence is created by generating a chaotic series of n real numbers with 1D logistic map and storing the index position of these real numbers in ascending order of their real values. On the basis of this integer sequence, the pixel position of the image is permuted and a key matrix is generated from the sequence. These sequences are converted into DNA encoding, and is added to the image pixel using DNA addition rule.
The rest of the paper is organized as follows: Section 2 gives a brief introduction to chaotic maps, generation of the integer sequence and also brief description of DNA coding. Section 3 describes the proposed approach. Section 4 shows the simulation results and performance analysis. Section 5 concludes the work.

2. RELATED THEORIES AND CONCEPTS

2.1. Chaotic Map

Chaotic sequences are real valued sequences. This paper focuses on 1D logistic map.

$$a_{k+1} = \mu \, . \, a_k \, . \, (1 - a_k) \quad (1)$$

The above equation is chaotic where a_0 is the initial condition and its value varies between 0 and 1; μ is the control parameter, and $3.6 < \mu \leq 4$.

2.2. Index based pseudorandom sequence generation from chaos
Chaotic sequence is a real valued sequence. This real valued sequence can be converted into the integer sequence. In this approach, an index based chaotic sequence is generated. First, a chaotic sequence is generated using 1D logistic map, after which the index values that are stored in a row matrix, are generated according to ascending order of the chaos sequence. Index values represent the position of chaos sequence. The resultant row matrix or the array contains an integer sequence which can be used for permutation.

2.3. DNA Encoding and decoding technique
DNA sequencing is a process used to map out the sequence of the nucleotides that comprise a strand of DNA. The bases, adenine (A), thymine (T), guanine (G), and cytosine(C)

represent the genetic code. A bonds with T; and G bonds with C. These base pairs are complement with each other just like binary values 0 and 1. In this approach, we consider binary values of A, C, G and T as 00, 01, 10 and 11 respectively. A and T indicates 00 and 11, which are complement to each other; similarly, C and G indicates 01 and 10, which are complement to each other. In the 8 bit grey images, each pixel is denoted by a DNA sequence of length 4.

2.3.1. Rules for DNA Addition and Subtraction

With the rapid development of DNA computing, various biology operations and algebraic operations based on DNA sequence have been presented by researchers [9-12] (for example: addition operation). Addition and subtraction operations for DNA sequences are performed according to traditional addition and subtraction operation. For example: addition of $10 + 11 = 01$ indicates $G + T = C$ and subtraction of $10 - 11 = 11$ indicates $G - T = T$. The addition and subtraction rule are shown below in Table 1 and Table 2 respectively.

Table 1. DNA Addition Table 2. DNA Subtraction

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

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

3. PROPOSED ALGORITHM

The proposed approach consists of two step process. In the first part, the image is permuted in which each of the pixels is shuffled on the basis of the generated integer sequence. In the diffusion part, the generated sequence and permuted image are converted into the encoded DNA form. These two converted DNA matrix is then added to get the final encrypted image. Entire process of encryption is described below.

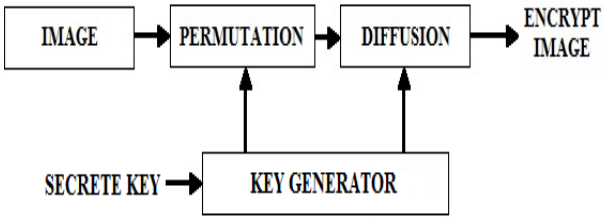


Fig 1: Block Diagram of the Proposed Model

3.1 Permutation

The rearrangement of the pixel is carried out by generating an integer sequence. Index based chaotic is used for pixel permutation. Algorithm 1 for pseudorandom sequence using logistic map:

Step1. Generate the chaotic sequence of length n by using the formula (1) and store it in an one dimensional matrix {a1, a2, a3, a4, ... , an}.

Step2. Find the index of the smallest number from the sequence of n number and then store it in b(1). Next find the index of the 2nd smallest number and store it in b(2). Repeat This process until nth smallest number is stored in b(n).

Step3. The array b contains sequence of n random number generated from the chaos sequence.

3.2 Diffusion

Diffusion is the process where actual pixel value is modified. To make this encryption method more secure and difficult to analyze, the permuted pixels are again fed to diffusion process. Here each pixel value of the permuted image is modified by a key value using DNA addition.

3.3 Key matrix

A key matrix is created for the pixel modification, which is generated from the integer sequence a[ ]. TheThe size of the a[ ] is first reshaped from$(1, m \times n)$, and then each of the value in the integer sequence can be mapped into the key matrix as follows:

$$k(i,j) = \mathrm{mod}(a(i,j), 256) \quad (2)$$

where $0 \leq k(i,j) \leq 255$.

The size of the key matrix is (m, n) and this matrix is converted into binary matrix, and then into a DNA sequence of size $(m, n \times 4)$.

Algorithm 2 for Image Encryption:
Steps of the algorithm are:

Step1. Take the original gray image matrix I of size (m, n), where m and n are the number of rows and columns of the image matrix.

Step2. Generate chaotic sequence by using 1D logistic map and call algorithm (1) to generate integer sequence and store into a 1-D array a[ ] of size $(1, m \times n)$.

Step3. Convert image matrix into row matrix of size $I(1, m \times n)$. Shuffle the pixel position of the image matrix I on the basis of integer sequence a[ ]. The image matrix now is permuted.

Step4. Again reshape the permuted image row matrix in to a two dimensional matrix of size $I(m, n)$. Convert this two dimensional matrix into a binary matrix and then from binary matrix to DNA encoded matrix using encoding rule. The matrix I is now of m rows and $n * 8/2$ columns.

Step5. Reshape integer sequence stored in array a[ ] (step 2) into a two dimensional matrix $a(m, n)$.

Step6. Construct a key matrix k of size (m, n) using equation (2). Covert the key matrix k into binary matrix and then convert the binary matrix to DNA encoded matrix using encoding rule of size $\left(m, n * \frac{8}{2}\right)$.

Step7. Finally, each pixel of I[ ] is added with each pixel of k[ ] using DNA addition rule; and a new matrix A[ ] of size $(m, nx4)$ is created.

Step8. Then decode the DNA matrix A[ ] to binary matrix by using reverse of encoding rule, and reconstruct it to an image matrix. This image matrix is the encrypted image.

The algorithm operation starts with taking initial key value for μ. Step1 to step2 is used for the generating the integer sequence. Step3 is used for rearranging the pixel and followed to this permutation process for the image pixel is carried out. Step4 generates the DNA sequence of the corresponding permuted image. Step5 and step6 are used for the generation of the key matrix and finally, step7 is used for DNA encoding.

The decryption process is just the replication of the encryption process. With the initial key value, an integer sequence is created and the encrypted pixel is brought back to its correct position. After permutation, same key matrix is generated and DNA subtraction operation is carried out to get the original image.

4. PERFORMANCE ANALYSIS

4.1. Key space analysis

Key space analysis is one of the important criteria of the performance analysis of image encryption algorithm. A good encryption algorithm should have a large key space, and also should be sensitive to the key value. In this paper we have considered the initial value of μ as the key of the encryption algorithm. As the chaotic system are dynamic systems, which are very much sensitive to the initial key value; thus, a small variation to the initial seed or the key value creates a major impact on the encrypted image. This effect can be viewed in the simulation result in figure 2(g), by changing the μ value from 3.61 to 3.62. The Figure2 (f) shows the histogram of wrongly decrypted image. From above results, we can conclude that the encryption algorithm is very sensitive to the key value.

4.2. Histogram

The operations have been performed on the standard image "leena.jpg", and the histograms of original image and encrypted image are plotted. Figure 2(a) shows the original image and 2 (b) its histogram and figure 2(c) and 2(d) shows encrypted image and its histogram. Histogram of encrypted image is uniform in nature and it is completely different from original image histogram. Hence, any statistical attack is unlikely in the proposed encryption technique.

4.3. Correlation coefficient analysis

Correlation is a statistical measurement of the relationship between two variables. Possible correlations range from +1 to –1. A zero correlation indicates that there is no relationship between the variables. A correlation of –1 indicates a perfect negative correlation, indicating that as one variable increases, the other decreases. A correlation of +1 indicates a perfect positive correlation, indicating that both variables move in the same direction together. As it is well known that in any image, the correlation of adjacent pixels is very high. A good encryption algorithm should lower the correlation between adjacent pixels.

In order to test the correlation of two adjacent pixels, we randomly select 2000 pairs (horizontal and vertical) of adjacent pixels from the original and encrypted images and by using the following formulas the correlation coefficient of the adjacent pixel is calculated.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (3)$$

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - E_x)(y_i - E_y)}{\sqrt{\sum_{i=1}^{n}(x_i - E_x)^2 (y_i - E_y)^2}} \quad (4)$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (5)$$

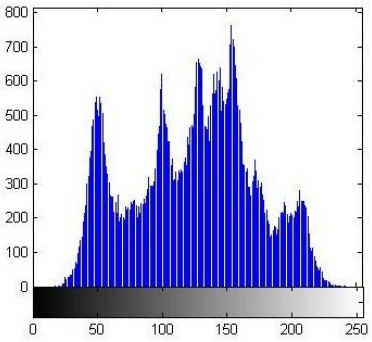
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (6)$$

Figure 3(a) and (b), show the correlation of two horizontally adjacent pixels in the original image and its encrypted image, where the correlation coefficients are 0.9468 and 0.0261 respectively. Similarly, figure 3 (c) and (d), show the correlation between two vertically adjacent pixels in the original and encrypted image. Table 3 shows that the correlations of adjacent pixels in the original and encrypted image have been sufficiently reduced.

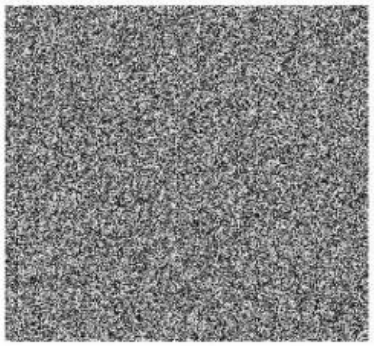
Table 3. Correlation of adjacent pixels in the original and encrypted image

Model	Original image	Encrypted image
Horizontal	0.9991	-0.0261
Vertical	0.9952	0.0682

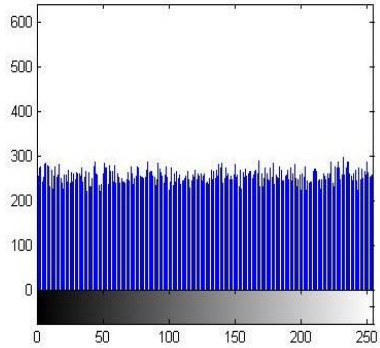
(a)



(b)

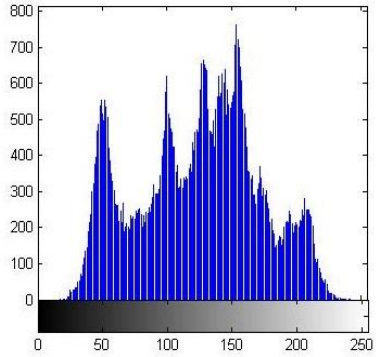


(c)

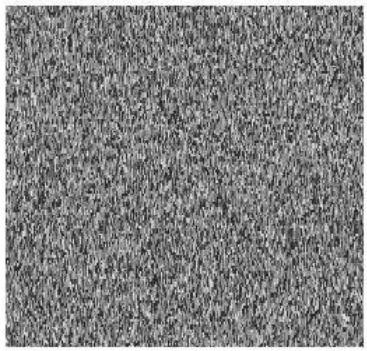


(d)

(e)

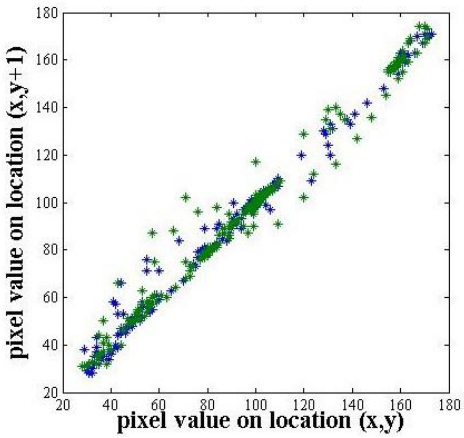


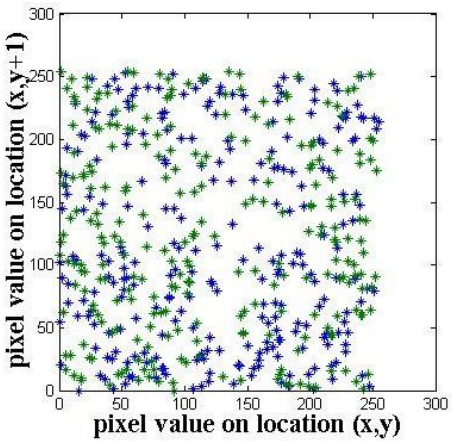
(f)



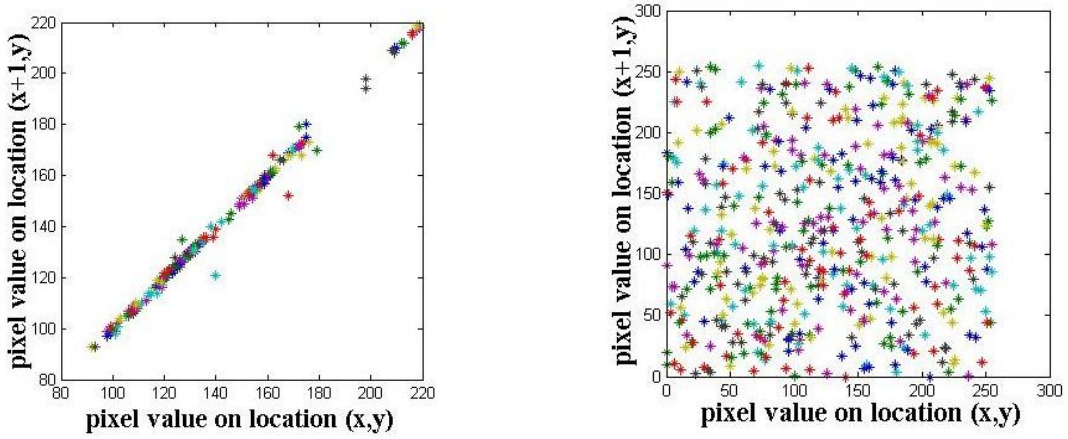
(g)

Fig 2: Experimental Result (a) Original Image (b)Histogram of the Original Image (c) Encrypted Image with μ=3.61 (d) Histogram of the Encrypted Image (e) Decrypted Image (f) Histogram Of the Decrypted Image (g) Decryption of the original by taking different initial value of μ=3.62.





(a) (b)



(c) (d)

Fig 3: figure (a) and (b) shows the correlation between two horizontally adjacent pixels in the plain and encrypted image. Figure (c) and (d) shows the correlation between two vertically adjacent pixel in the plain and encrypted image.

4.4. Speed analysis

When the security requirement is fulfilled, the running speed becomes an important factor for practical application. Speed analysis is the strong point of the proposed algorithm. Mainly the processor time is reduced in generating the integer pseudorandom sequence from the chaotic sequence. In [5, 6] the traditional chaos process of image encryption uses the binary sequences for the image permutation. Chaos sequence are the real valued sequence and to convert it into its corresponding binary sequence, followed by more than one logic operation to generate the integer pseudo random number for image permutation, is a time consuming process. Unlike the above approach, the proposed approach directly generates the integer pseudo random number from the real valued chaotic sequence. This property makes the proposed method more effective and less time consuming for image encryption.

4.5.Differential attacks

Attackers often make a slight change for the original image, use the proposed algorithm to encrypt the original image before and after changing, and through comparing two encrypted images to find out the relationship between the original image and encrypted image. This is known as differential attack.

To test the influence of one pixel change on the whole ciphered image, researchers usually use two measures: the number of pixels change rate (NPCR), which measures the percentage of different pixel numbers between two images; and the unified average changing intensity (UACI), which measures the average intensity of difference between two images. Here the encrypted image of leena is called "leena-test1" and the encrypted image after changing the first pixel gray value from leena is called leena-test2.

$$C(i,j) = \begin{cases} 0, & if\ T_1(i,j) = T_2(i,j) \\ 1, & if\ T_1(i,j) \neq T_2(i,j) \end{cases} \quad (7)$$

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\% \quad (8)$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |T_1(i,j) - T_2(i,j)|}{(255 \times M \times N)} \times 100\% \quad (9)$$

Where M and N are the height and width of the image, $T_1(i, j)$ and $T_2(i, j)$ denote the pixel grey value of an image. We have obtained the result of image which is shown by Table 4.

Table 4. Result of NPCR and UACI

Image	NPCR	UACI
Leena.jpg	99.5682	33.6562

4.6.Entropy

The information entropy is defined to express the degree of uncertainties in the system. We can also use it to express uncertainties of the image information. The information entropy can measure the distribution of grey value in the image, the distribution of grey value is more uniform, and the information entropy is greater, whereas it is smaller. The information entropy is defined as follows:

$$H(m) = -\sum_{i=0}^{L} P(m_i) \log_2 P(m_i) \quad (10)$$

Where mi is the ith grey value for L level grey image, $P(m_i)$ is the emergence probability of m_i, so $\sum_{i=0}^{L} P(m_i) = 1$. For an ideally random image, the value of the information entropy is 8. An effective encryption algorithm should make the information entropy tend to 8. The information entropies of encrypted image is H=7.9889 that is close to 8.

5. CONCLUSION

This paper has demonstrated a hybrid approach of permutation and diffusion method for image encryption. This proposed approach has been found to be effective, as it uses a randomized integer sequence for permutation. Also, the randomization of the sequence varies drastically by slightly changing the value of the initial condition. The diffusion part of the algorithm uses DNA encoding method which makes the data difficult to analyze for the intruder. Also, the algorithm

changes the correlation factor of the adjacent pixel to a low value. This algorithm is also more resistant to various types of attacks.

6. REFERENCES

[1] Chong Fu and Zhiliang Zhu., 2008. A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method. The 9th International Conference for Young Computer Scientists. 3057-306l.

[2] Yunpeng Zhang, Fei Zuo, Zhengjun Zhai and Cai Xiaobin. 2008. A New Image Encryption Algorithm Based on Multiple Chaos System. International Symposium on Electronic Commerce and Security. 347-350.

[3] Liu Jin-mei, Qiu Shui-sheng, Xiang Fei and Xiao Hui-juan. 2008. A Cryptosystem Based on Multi-Chaotic Maps. International Symposiums on Information Processing. 740-743.

[4] R. Matthews, 1984. On the derivation of a chaotic encryption algorithm. Cryptologia, 8, 29–41, (January 1984).

[5] F. Sun, S. Liu, Z. Li and Z. Lü., 2008. A novel image encryption scheme based on spatial chaos map. Chaos, Solitons and Fractals, 38 (3), 631 – 640.

[6] L. Wang and K. Smith., 1998. On chaotic simulated annealing. Neural Networks, IEEE Transactions on. 9(4), 716 –718, (July 1998).

[7] Y. Wang, K. W. Wong, X. Liao and G. Chen, 2011. A new chaos-based fast image encryption algorithm. Appl. Soft Comput. 11, 514–522, (January 2011).

[8] K.W. Wong, B. S. H. Kwok and W. S. Law., 2008. A fast image encryption scheme based on chaotic standard map. Physics Letters A. 372(15), 2645-2652 .

[9] Qiang Zhang, Ling Guo, Xianglian Xue, Xiaopeng Wei, 2009. Algorithm Based on DNA Sequence Addition Operation. Bio-Inspired Computing fourth IEEE International Conference. 1-5, (October 2009).

[10] Allen P. Mills Jr., Bernard Yurke and Philip M. Platzman. Article for analog vector algebra computation. BioSystems. 52, 175-180.

[11] Piotr Wasiewicz,lan J. Mulawka, Witold R. Rudnicki and Bogdan Lesyng, 2000. Adding Numbers with DNA. InternationaI Conference on Systems,Man and Cybernetics, 265-270.

[12] Qian Wang, Qiang Zhang and Changjun Zhou, 2009. A Multilevel Image Encryption Algorithm Based on Chaos and DNA Coding. Bio-Inspired Computing fourth IEEE International Conference. (October 2009).

[13] Mintu Philip and Asha Das, 2011. Survey: Image Encryption using Chaotic Cryptography Schemes. IJCA-Computational Science NCCSE' 11.

[14] Anuja Kumar Acharya, 2011. Image encryption using a new chaos based encryption algorithm. In International Conference on Communication, Computing & Security (ICCCS).