Hybrid Encryption algorithm using Scan plans, 1D logistic sequences and DNA encoding

[1]Pragya Tiwari, [2]Pradeep Tripathi

Department of Computer Science and Engineering,
Vindhya Institute of Technology & Science, Satna (M.P)

***Abstract*: Secure transmission of digital images or information is a highly essential for today networking technology. Image encryption schemes is demanding field for this application. Presently many image encryption method s available, many of them have areas that are not resilient to chosen plain-text attacks, mainly the mask method. The proposed hybrid encryption algorithm is combination of scan plan and chaotic system based permutation and DNA based diffusion. In proposed algorithm it is found that due to random sequence and DNA encoding the data difficult to analyze for the intruder. And also found that algorithm is also more effective for various types of attacks.**

***Keywords*: image encryption, DNA encoding, Scan plans, chaotic system**

I. INTRODUCTION

In development of information technology and the rapid growth of computer networks us e transmission of large files, such as digital images. In order to restrict unwanted recipients from viewing private and unsafe data, Encryption is used. Encryption is the process of transforming the information to ensure its security. The encryption process requires an encryption algorithm and a key. The process of recovering plaintext from cipher text is called decryption. The accepted view amongst cryptographers is that the encryption algorithm should be published, whereas the key must be kept secret [1]. Various types of algorithm are developed for encryption. However, most of the traditional text based encryption algorithms such as AES and IDEA are not suitable for image encryption.

For image encryption various researcher has studied and developed a new and hybrid technique. Maniccam et al. have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves. [2]. Kehar et al. proposed a new technique in which the digital signature of the original image is added to the encoded version of the original image. A best suitable error code is followed to do encoding of the image, ex: Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after decryption of that image, the digital signature verifies the authenticity of the image [3]. Chang et al. proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures is regenerate to binary phase encoding and then these images are encrypt with binary random phase images by binary phase XOR operation [4].

Fethi et al. used the method that can be used for binary images encryption with the possibility of using several keys ex: initial state, the external parameters and iterations' number [5]. Qais proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rossler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and highlevel security, high obscure level and high speed [6]. Aradhana et al. developed a hybrid algorithm are image encryption which used 1D logistic map for permutation and DNA encoding is used for diffusion. They found that the hybrid approach is more attractive as compare to the single images [7].

This paper proposes a hybrid method for image encryption, where various scan patterns are used for generation of scan co-ordinates which is used for permutation of images. Afterword 1D logistic map based chaotic sequences are used. 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 [7]. 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 [5-7].

II. THEORIES AND CONCEPTS

A. Scan Plans

The encryption using scan is applied on binary images and the bit sequence along the scan path and the bit sequence to represent the scan path together represents encrypted image. Key factors which is important when using scanning paths for encryption:
(a) The scan path should be compact enough so that the bits needed to represent them can be less.
(b) Images are non-homogeneous and scanning this images are possible using non-homogeneous scan paths, due to this the bit sequence will have large number of segments of 0s and 1s.

B. Chaotic Map

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

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

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 $3.6 < \mu \leq 4$.

C. 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 [7]. Rules for DNA Addition and Subtraction are shown in below table.

Table 1
DNA Addition

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

Table 2
DNA Subtraction

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

With the rapid development of DNA computing, various biology operations and algebraic operations based on DNA sequence have been presented by researchers [7-9] (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 [7-9].

III. PROPOSED METHODOLOGY

The proposed methodology has two major steps and shown in figure 1. First is, image permutation, in this stage input images is first permuted using scan plans co-ordinates, in which each of the pixels is shuffled on the basis of the generated scan sequences this permuted image is further used in second stage. In this image are diffused and for diffusion 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.

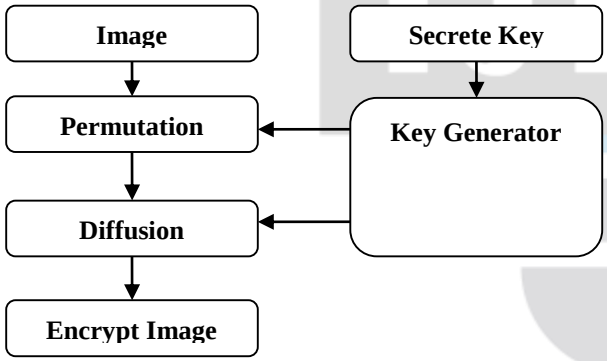

Figure 1 Block Diagram of the Proposed Model

IV. PERFORMANCE ANALYSIS

A. Histogram Analysis

Histogram of the images is a graphical representation of tonal distribution of a digital image. For histogram analysis standard images such as leena.jpg, Cam.tif, barbara.jpeg, Peppers.png, saras.jpeg are used and after words the histogram of original image as well as encrypted image are plotted. Histogram of original images is different for different images while the histogram of encrypted image is uniform in nature and it is completely different from original image histogram so any statistical attack must be impossible in this encryption technique.

B. 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, meaning that as one variable goes up, the other goes down. A correlation of +1 indicates a perfect positive correlation, meaning that both variables move in the same direction together. As we know that in any image correlation of adjacent pixel is very high. A good encryption algorithm should bring the correlation between adjacent pixels to low. In order to test the correlation between the original and encrypted images the following formulas is used and table 3 shows the correlation of the adjacent pixels in the original and encrypted image.

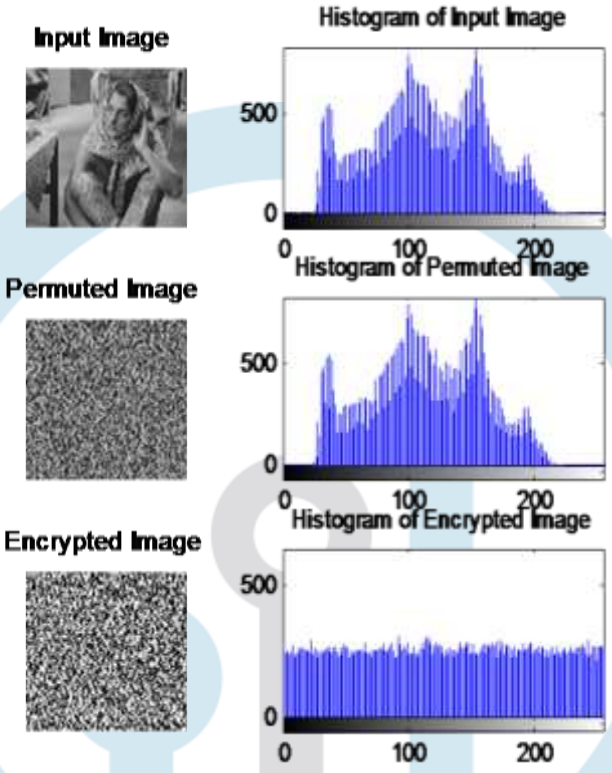

Figure 2 Original Barbara.jpg image, Permuted Image and Encrypted image with histogram

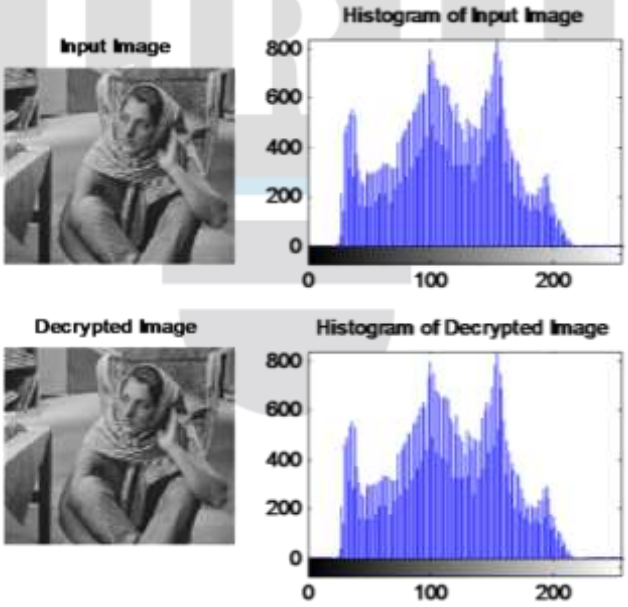

Figure 3 Original Barbara.jpg image, Decrypted image with histogram

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

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - E_x)(y_i - E_y)}{\sqrt{\sum_{i=1}^{n}(x_i - E_x)^2 (y_i - E_y)^2}} \quad (3)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (4)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (5)$$

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

S. No.	*Images*	*Encrypted image*
1	*Leena.jpg*	*-4.10×10^{-4}*
2	*Cam.tif*	*-4.76×10^{-4}*
3	*barbara.jpeg*	*0.0001*
4	*Peppers.png*	*0.0008*
5	*saras.jpeg*	*-0.0015*

C. Information 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:

$$H(m) = -\sum_{i=0}^{L} P(m_i)\, log_2 P(m_i) \quad (6)$$

Where m_i is the i^{th} 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 images are shown in Table 4 all of which are very close to 8. It can be seen that proposed algorithm is very effective.

Table 4 The information entropy of encrypted image

S. No.	*Images*	*Original Image*	*Encrypted*
1	*Leena.jpg*	*7.4490*	7.9965
2	*Cam.tif*	*7.0097*	7.9974
3	*barbara.jpeg*	*7.3625*	7.9964
4	*Peppers.png*	*7.5327*	7.9968
5	*saras.jpeg*	*3.7754*	7.9997

CONCLUSION

This paper has demonstrated a hybrid approach of permutation using scan plans sequence as well as 1D logistic map sequence and diffusion using DNA 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. The correlation factor of the adjacent pixel is found very low. This algorithm is also more effective for various types of attacks.

REFERENCES

[1] William Stallings. Cryptography and network security: principles and practice. Prentice Hall, 1999.
[2] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34, 1229-1245, 2001.
[3]] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229-234.
[4] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003.
[5] Fethi Belkhouche and Uvais Qidwai , "Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.
[6] Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

[7] Aradhana Soni & Anuja Kumar Acharya; A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis; International Journal of Computer Applications (IJCA); Volume 47 - Number 23; 2012.
[8] Qiang Zhang, Ling Guo, Xianglian Xue, Xiaopeng Wei, "Algorithm Based on DNA Sequence Addition Operation", *Bio-Inspired Computing fourth IEEE International Conference*, pp. 1-5, October 2009.
[9] Piotr Wasiewicz,lan J. Mulawka, Witold R. Rudnicki and Bogdan Lesyng, "Adding Numbers with DNA", *InternationaI Conference on Systems,Man and Cybernetics*, pp. 265-270, 2000.