Advanced Hyperchoatic Image Encryption Technic with DNA Sequence

M Karpagam, 1 M Shyam Kumar1, M Sowmiya1, A Monikavishnuvarthini1
1Department of Electronics and communication, Sri Krishna College of Engineering and Technology, Coimbatore, India
karpagam@skcet.ac.in, 19epae002@skcet.ac.in. 19epcm002@skcet.ac.in, 19epcm001@skcet.ac.in

Abstract. As the development of computer usage increases the need for security also increases as it had changed from entertainment based to high confidential files maintaining medium. So, there was a great improvement in the field of cryptography for data transfer and these are basically text and so they are more simple to process when compared to higher level of files like image and vide. This lead to the need for encryption methods for fast and secure techniques to avoid quality and quantity of high speed encrypted data files. There are lots of highly secure cryptographic methods but they need to be compatible with image for processing. So the project goes along with a technic called hyper chaotic encryption technique with DNA sequence for hybrid image cryptography.

1. Introduction
The need for secure medium to transfer a high range of data files from highly classified military files, medical documents and private firms valuable files coins the need for technic to protect the files like hiding inside a casual file to avoid attention or to mask the confidential image with algorithm based key combining with image pixel matrix values in vector form [1-5]. The chaotic method is based on the chaos algorithm which is highly deterministic and highly sensitive to minor changes in the input. The image is representation of pixels with wide range of scale values with grayscale has value of $2^8=256$ i.e the range or the representation of details in image can use $0 – 255$ variety of information. Normal image is 2D with X and Y as column and row but the RGB image will be 3D as there are three images sets like the grayscale set, they are R, G, B, each has its own column and row. Most of the image processing method uses Y Cr Cb as the change in luminance is more visible to human eye but the change in the chrominance is not much noticeable and splitting luminance from chrominance is easier when compared to RGB. Conversion of RGB to is easy and is converted, one of the way of conversion based on International Radi Consultive Committee guidance and this is the method used in JPEG based on the below formula

$$Y = 0.29900R + 0.58700G + 0.11400B$$
$$Cb = -0.1687R -0.33126G +0.50000B$$
$$Cr = 0.50000R - 0.41869G - 0.08131B.$$
The implication of chaos algorithm ensure the security of communication due the function of it being unpredictable which is the key point of secure data transfer as the unpredictable feature ensures the hacker from predicting the information easily. The chaos under symmetric cryptography which is also referred as symmetric encryption which is the method of using single key on both sides of encryption and decryption. In Y Cb Cr, luminance is encoded by Y and the red and blue with Cr and Cb. The chaotic encryption uses the below Equation (1). Figure 1 shows Chaos wheel

\[ X(n+1) = \lambda \times X_n (1 - X_n) \]  

Figure 1. Chaos wheel

There are two different process under chaotic encryption but both are opposite to each other, they are chaotic cryptography which refers to the process of encrypting the image whereas cryptanalysis as in the term used for analyzing is method of decrypting the image for further process like analyzing. Symmetric Chaotic encryption works by the method of discrete chaotic map [6-10]. Normal will be continuous but as we are working on digital image processing we need discrete output to go for further processing. When the talk of image encryption begins will get into a debate of encryption time and complexity involved in encryption which increase the time taken. First most of them move forward towards simple encryption method to get more faster processing but as the computational power of the computers fires the security issue to move forward as we are in time of expecting to bring quantum computing in security as many experiments already started and so we need to have method to have good complexity with moderate time for processing as the computational also boosts the speed of complex computation as the simple map used before. Figure 2 shows Bifurcation for logistic map

Figure 2. Bifurcation for logistic map

2. DNA Encoding

Though we use various methods in encryption to secure the data intruders try to intercept and explore the message by breaking the encryption with help of various techniques called attacks [10-14]. In which some of the attacks like exhaustive, statistical and differential attacks can be defended with help of the
DNA encoding. DNA refers to Deoxyribonucleic acid and it consists of four nucleic acid bases pair ATCG they are adenine (A), cytosine (C), guanine (G) and thymine (T). Figure 3 shows Bits to DNA conversion rules.

| DNA RULE | A   | T   | C   | G   |
|----------|-----|-----|-----|-----|
| Rule 1   | 00  | 11  | 01  | 10  |
| Rule 2   | 00  | 11  | 10  | 01  |
| Rule 3   | 01  | 10  | 00  | 11  |
| Rule 4   | 01  | 10  | 11  | 00  |
| Rule 5   | 10  | 01  | 00  | 11  |
| Rule 6   | 10  | 01  | 00  | 11  |
| Rule 7   | 11  | 00  | 01  | 10  |
| Rule 8   | 11  | 00  | 10  | 01  |

![Figure 3. Bits to DNA conversion rules.](image)

In the paper we have used the rules 1 and we had the bits value which is converted to DNA sequence based on the rules as “00” = ”A”, ”01” = ”C”, ”10” = “G” and “11” = ”T”. The DNA has the ability to store a large amount of data in small amount of DNA to put it in practical perspective a gram DNA can store 455 Exabyte of data.

The first input image is encoded to get the first set of DNA sequence next we will get the matrix and break them into blocks of equal size and some times the last block will be small. Next logistic map is used for complement operation and then will get DNA sequence matrix.

3.  **Runge Kutta Method**

The method had find it's way in major applications, due to the use of ordinary differential equations in many real life scenarios. If we want to calculate value of a long time problem such as population growth or like position of object affected with number of constraints to be integrated to get output then we need runge kutta method. The method will predict the “P” position which is now in ideal point (P0) so if we have a initial point we can use the available values like the velocity to predict the position of the “P” at time Pt.

4.  **Chaotic Encryption**

The chaotic encryption works on chaotic maps and there are list of chaotic maps like Arnold’s cat map, Baker’s map, Gauss map. The function of chaotic map is of two types confusion and diffusion, If a intruder has the statistical details about the prior messages and tries to the knowledge to decode the cipher with frequency of symbol usage in cypher text. Shannon proposed a way out of this with two methods which are the confusion also referred as permutation and diffusion. The diffusion is a method which focus on hiding the relationship between plain and cipher. The method should ensure modification of one bit in cipher should change half of the plain information and vice versa. The confusion technic whereas focus on the correlation between the cipher and the key and the method will
ensure a bit modification in cipher modifies all bits in key and vice versa. The confusion technic uses substitution in the process and diffusion uses transposition in the process. Figures 4-9 shows Hena image with histogram graph representation.

**Figure 4.** Hena image with histogram graph representation

**Figure 5.** Encrypted Hena image with histogram graph representation

5. **Hyperchaotic Encryption With Dna Sequence**

Hyperchaotic method is used in the paper due to the increase in number of lyapunov exponents. The security of encryption is directly related to the complexity so the hyperchoatic image encryption is more complex and dynamic than chaotic image encryption system. This increase the rate of unpredictability with random and uncertainty principle. Key space present in the chaotic system is also small and is simpler method with lower level of security. The hyperchaotic system has more key space due to the large number of state variable

The process involves the following steps

1. Iteration takes place in the hyperchaotic system to avoid any attack
2. Iteration of m×n for N times occurs next
3. The x1,x2,x3,x4 gives two different key during the process
4. After the whole process of iteration all these above sequence are concatenated finally
Figure 6. Hena image with correlation and histogram graph representation

![Image of Hena image with correlation and histogram graph representation]

Figure 7. Encrypted Hena image with correlation and histogram graph representation. The hyperchaotic system is determined by

\[ \begin{align*}
    x_1 &= a(x_2 - x_1) + b_1 x_4 \\
    x_2 &= c x_1 - x_1 x_3 + b_2 x_4 \\
    x_3 &= -d x_3 + x_1 x_2 + b_3 x_4 \\
    x_4 &= -e x_1
\end{align*} \]

![Image of Encrypted Hena image with correlation and histogram graph representation]

Figure 8. Anticropping effect on Hyperchaotic encrypted image with decrypted result

![Image of Anticropping effect on Hyperchaotic encrypted image with decrypted result]

6. Conclusion
The hyperchaotic system is commonly used with the data sequence in the image encryption process. The 4 D system is obtained with pseudorandom sequence. The hyperchaotic method is utilized in all part of the process. The pixel value of image input is converted into binary stream sequence and is
changed into hyperchaotic sequence. The DNA method of complementation and algebraic operation is used along with the hyperchaotic method. The statistical information is avoided when we process the input image to encryption this will be visually analysed when compared to encrypted image. The correlation analysis helps in analysing the adjacent pixels in a image so when we measure the correlation of normal image we can find the correlation information but after the encryption the correlation of pixel will be lower down to zero.

References

[1] Vaishali D. Kamble, Prof. Kanchan Doke, A NOVEL SURVEY ON IMAGE ENCRYPTION, International Research Journal of Engineering and Technology (IRJET), 05(09) | Sep 2018.

[2] M. Karpagam, Underwater Wireless Sensor Network Based Marine Environment Monitoring System, International Journal of Oceans and Oceanography, 13, Number 2, 2019.

[3] Zia Bashir a, Tabasam Rashid b, Sohail Zafar, Hyperchaotic dynamical system based image encryption scheme with Q12 time-varying delays, Pacific Science Review A: Natural Science and Engineering, 24 December 2016

[4] M. Karpagam, ACO enhanced RILoD-IN scheme for WSN, 2020 International Conference on Smart Electronics and Communication, pp 744 – 749

[5] Tariq Shah; Tanveer Ul Haq; Ghazanfar Farooq. Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation, 03 March 2020.

[6] M. Karpagam, Analysis of EMCA, EFNR and HEFRN Algorithms in wireless sensor Networks, Applied Mechanics and Materials 550 May 2014,pp 102 - 109.

[7] Hwai-TsuHua, Ling-Yuan Hsu Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression, Elsevier-Computers & Electrical Engineering, Volume 41, January 2015.

[8] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio networks, Computers & Electrical Engineering, vol. 87, p.106784, Oct. 2020. doi: 10.1016/j.compeleceng.2020.106784

[9] A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability, Neural Processing Letters, Aug. 2020. doi:10.1007/s11063-020-10327-3P. O. Izevbizua, Data security in the cloud using serpent encryption and distributed steganography, Int. J. Appl. Sci. Math., 1, 2015.

[10] M. Karpagam A Relay Node Routing Technique to HEF Clustering Algorithm for Time Critical Wireless Sensor Networks, in International Journal of Pure and Applied Mathematics May 29th 2018.

[11] Xiao Chen, Chun Jie Hu Medical image encryption based on multiple chaotic mapping and wavelength transform, 2017.

[12] Arunkumar S, Subramaniyaswamy V, Devika R, Logesh R Generating visually meaningful encrypted image using image splitting technique, 8 August 2017.

[13] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communication ACM 21, 1978