International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 11 | Nov 2019 www.irjet.net p-ISSN: 2395-0072

Analysis of Chaotic, Hyperchaotic and DNA Sequence for Image Encryption

Puja Vyavahare[1], Prof. Harish Barapatre[2], Prof. Nilima Nikam[3]

[1]M.E Student, Computer Department, Y.T.I.E.T Collage Karjat, Maharashtra, India
[2,3]Professor, Computer Department, Y.T.I.E.T Collage Karjat, Maharashtra, India

---***---

Abstract - *The hyperchaotic sequence and the DNA sequence are utilized jointly for image encryption. A four-dimensional hyperchaotic system is used to generate a pseudorandom sequence. The main idea is to apply the hyperchaotic sequence to almost all steps of the encryption. All intensity values of an input image are converted to a serial binary digit stream, and the bitstream is scrambled globally by the hyperchaotic sequence. DNA algebraic operation and complementation are performed between the hyperchaotic sequence and the DNA sequence to obtain a robust encryption performance. The proposed hyperchaotic sequence and DNA sequence based (HC-DNA) method is compared with the chaotic sequence and DNA sequence-based (C-DNA) method, the cipher diffusion in crisscross pattern-based (CDCP) method, a class hyperchaos based (CHC) method. The parameters of CDCP, CHC, and C-DNA are set to the values given by the respective authors. The experiment results will demonstrate that the encryption algorithm achieves the performance of the state-of-the-art methods in term of quality, security, and robustness against noise and cropping attack.*

Key Words: **Hyperchaotic, DNA sequence, CDC, CDCP**

1. INTRODUCTION

In addition to the conventional framework, DNA computing is recently applied to chaos-based image encryption system due to its several good characteristics, such as massive parallelism, huge storage, ultralow power consumption, etc. Zhang [3] et al [2] proposed a DNA-based image encryption algorithm without the pixel position scrambling, but it has no robustness against noise because the input image is divided into blocks for DNA addition. Liu et al [2] transformed each nucleotide into its base pair, and their results showed that the information entropy of the cipher image is a little small. Wei et al [2] proposed a color image encryption algorithm to divide each RGB channel into blocks and to perform DNA addition operation for each block. However, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) of the cipher image are far from the maximum theoretical values, which means that Wei et al.'s[2] algorithm is not sensitive to small changes of the input image. Different from the Wei et al.'s algorithm, Liu et al [2] Proposed an RGB image encryption algorithm to perform DNA computing and pixel scrambling for each RGB channel so that the correlation coefficients of the adjacent pixels in the cipher image is relatively high. Kulsoom et al [2] extracted the most significant bits and the least significant bits for each pixel of an image and performed DNA computing between them. In Kulsoom et al.'s algorithm [2], most digits of each pixel are not changed, which leads to low robustness against noise.

2. BASIC CONCEPT

We jointly use hyperchaotic sequence and DNA sequence for image encryption. The schematic diagram is illustrated in Fig. 1. The hyperchaotic sequence is utilized in each step: GBS, DNA addition, DNA complementation, and the binary XOR. The pixel position scrambling and pixel value substitution are realized by the proposed GBS algorithm simultaneously. With GBS, the correlation of the adjacent pixels is very low. The DNA addition, the DNA complementation, and the binary XOR are used to achieve efficiency. In this way, the sensitivity to the input image of the proposed scheme is greatly increased. The advantage of this scheme is that it is capable of decrypting correctly in spite of crop-ping attacks or the accumulation of noise. The experimental results on six images will show that the proposed method achieves better image encryption performance than state-of-the-art approaches.

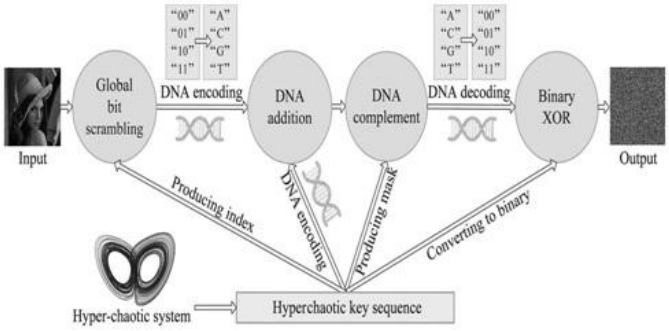

Fig -1: **Schematic diagram of the Hyperchaotic DNA scheme**

2.1 Hyperchaotic System

Hyperchaos is developed from chaos. The essential difference between chaos and hyperchaos is that a hyperchaotic system has two or more positive Lyapunov exponents. The hyperchaos exists in high-dimensional nonlinear systems [at least four-dimensions (4-D)]. Compared with the chaotic system, the hyperchaotic system has more complex dynamical behavior. The randomness and the uncertainty are greatly enhanced in the hyperchaotic system. The chaotic system has a simpler form and a higher efficiency, so its key space is smaller and the system complexity is lower, which results in a lower security protection. Due to more state variables in a hyperchaotic system, a high-dimensional chaotic system has a larger key space and its nonlinear behavior is more complex and unpredictable.

We adopt a hyperchaotic system that is determined by the following nonlinear equations:

$$\begin{cases} \dot{x}_1 = \alpha(x_2 - x_1) + \lambda_1 x_4, \\ \dot{x}_2 = \xi x_1 - x_1 x_3 + \lambda_2 x_4, \\ \dot{x}_3 = -\beta x_3 + x_1 x_2 + \lambda_3 x_4, \\ \dot{x}_4 = -\tau x_1, \end{cases} \tag{1}$$

Where α, β, ξ, τ, λ1, λ2, and λ3 are the control parameters of the system. When α = 35, β = 3, ξ =35, τ = 5, λ1 = 1, λ2 = 0.2, and λ3 = 0.3, the system presents hyperchaotic behavior.

2.2DNA Encoding

DNA sequence contains four nucleic acid bases: "A" (adenine), "C" (cytosine), "G" (guanine), and "T" (thy-mine). "A" and "T" are complementary to each other, and the same as "C" and "G". Because binary digits, "0" and "1," are also complementary, we use two-bit binary digits to denote a DNA base. There are 24 kinds of rules for the representation, and only eight rules satisfy the Watson–Crick complement rule. The eight DNA coding rules are given in Table 1.

2.2.1. DNA Sequence Algebraic Operation

In DNA computing, the DNA addition and subtraction are performed according to the traditional binary addition and subtraction. The DNA addition and subtraction rules are shown in Tables 2 and 3, respectively.

Table-1: DNA coding rules.

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

Table: - 2: DNA sequence addition.

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

Table:-3 DNA sequence subtraction.

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

3. PROPOSED ALGORITHM:

Here we have proposed the basic two techniques

1 **Image Encryption Scheme**
2 **Hyperchaotic Sequence Generation**

As the pseudo randomness of a hyperchaotic system is strong and the hyperchaotic sequence has good statistical properties, we use the hyperchaotic system to generate the pseudorandom sequence. The hyperchaotic sequence generation comprises four steps:

1. The hyperchaotic system is preiterated N0 times to eliminate the adverse effects and to increase the security.

2. After the iteration N0 times, the system is iterated another m × n times. We use j to denote the iteration index. In each iteration j, four state values fxj1; xj2; xj3; xj4g is stored.

3. During iteration, each state value xji is used to generate two different key values $(s_i^a)^j \in [0, 255]$, (i= 1, 2, 3, 4) and $s_i^b \in [0, 255]$, respectively.

   They are calculated by

$$(s_i^a)^j = \mathrm{mod}\{\lfloor[(|x_i^j| - \lfloor|x_i^j|\rfloor) \times 10^{15}]/10^8\rfloor, 256\}, \quad i = 1, 2, 3, 4, \tag{2}$$

$$(s_i^b)^j = \mathrm{mod}(\lfloor\mathrm{mod}\{[(|x_i^j| - \lfloor|x_i^j|\rfloor) \times 10^{15}], 10^8\}\rfloor, 256), \quad i = 1.2.3.4. \tag{3}$$

Where mod (.) denotes the modulo operation and $\lfloor . \rfloor$ denotes flooring operation, i.e., it rounds the element to a nearest integer toward minus infinity.

These key values are concatenated with Eq. (4) to be a vector sj,

$$s^j = [(s_1^a)^j, (s_2^a)^j, (s_3^a)^j, (s_4^a)^j, (s_1^b)^j, (s_2^b)^j, (s_3^b)^j, (s_4^b)^j]. \tag{4}$$

4. After the whole iteration, these sequences are concatenated with Eq. (5) to obtain k,

$$k = [s^1, s^2, \cdots, s^{m\times n}]. \quad (5)$$

One element in k can be denoted by

$$k_i,\ i \in [1, 8mn].$$

- **Global Bit Scrambling**

An input image P with intensity value in the range of [0, 255] has eight bits. The intensity values of the image are globally scrambled bit by bit in order to reduce the correlation between adjacent pixels. The intensity value of each pixel is also changed in the global bit scrambling (GBS), which implies that the pixel substitution is realized by GBS at the same time.

GBS is realized by two steps:

1 The intensity value of each pixel is expressed as binary digits one-by-one to obtain a one-dimensional (1-D) binary sequence b0. The hyperchaotic sequence k is arranged in ascending order to attain the index sequence kx.

2. According to the index sequence kx, b0 is globally scrambled to the index sequence.

$$b_i^1 = b_{k_i^x}^0, \qquad i \in [1, 8mn]. \quad (6)$$

3.1 ALGORITHUM FOR IMAGE ENCRYPTION

GBS results in a complex nonlinear relationship between the input image and the cipher image, which increases the security.

The image encryption scheme is cast into a seven-step procedure:

Step 1. Let m × n denote the size of the input image P. GBS is performed on an image P to obtain the binary sequence b1.

Step 2. b1 is encoded to a DNA sequence d1 by the first DNA coding rule (see Table 1). The DNA addition (see Table 2) on each element of d1 is performed to obtain d2 by

$$\begin{cases} d_1^2 = d_0 + +d_1^1, \\ d_i^2 = d_{i-1}^2 + +d_i^1, \ i \in [2, 4mn], \end{cases} \quad (7)$$

Where ++ denotes the DNA addition operation and d0 is a specified initial value.

Step 3. A sequence

$$k^s = [k_1, k_2, \cdots, k_{mn}]$$

is extracted from k, and the decimal sequence ks is converted to binary digits bk. bk is encoded to dk by the third DNA encoding rule. The DNA addition between d2 and dk is performed to obtain a sequence d3.

Step 4. A threshold function f(z) is defined by

$$f(z) = \begin{cases} 0, & 0 \le \frac{z}{255} \le 0.5, \\ 1, & 0.5 < \frac{z}{255} \le 1. \end{cases} \quad (8)$$

A cut sequence of k, $k, [k_1, k_2, \cdots, k_{4mn}]$, is transformed to a mask sequence w by Eq. (8). The mask sequence w and d3 are used to construct d4, i.e., if wi = 1, the corresponding d3i is complemented to obtain d4i, otherwise it is not changed. In this way, we obtain a DNA sequence d4.

Step 5. The first DNA coding rule is used to decode d4 to obtain a binary sequence b2.

Step 6. Bitwise XOR is performed between b2 and bk to obtain the cipher binary sequence b3.

Step 7. The binary sequence b3 is converted to a cipher image Q.

The decryption process is similar to encryption in a reverse order.

5. ANALYSIS OF EXPERIMENTAL RESULT:

For this experiment the Matlab 11 has been used. The proposed algorithm has implemented on some 24-bit colour images. One such image is 225*225 Lena image which can be shown in Fig-2. Here size of the secret scrambling pattern matrix is 256*256. So need to pad the Aerial image. The histogram of the three different channels (Red, Green, and Blue) of original Aerial image and the final encrypted image (Fig-3) are shown below.

1. Input image: Aerial

Fig-: 2.Input Image

2 Encryption of Image using Different Method

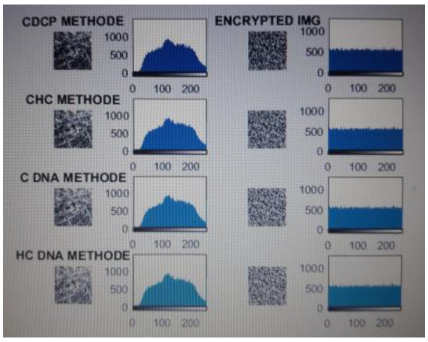

Fig-: 3.Histogram and Encryption

3. Correlation of images

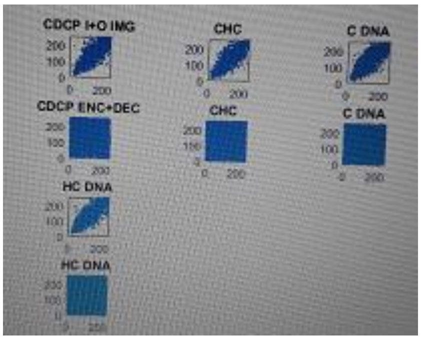

Fig 4. Image Correlation

4. Decryption of image using diff method

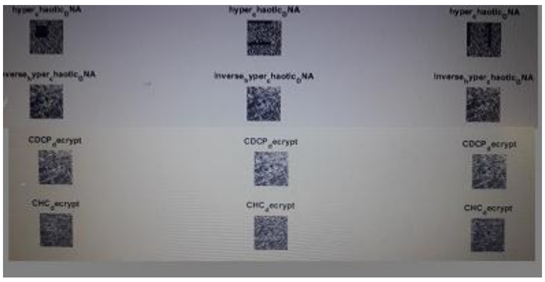

Fig 5.Output

3. CONCLUSION

The hyperchaotic sequence and the DNA sequence are utilized jointly for image encryption. A four-dimensional hyperchaotic system is used to generate a pseudorandom sequence. The main idea is to apply the hyperchaotic sequence to almost all steps of the encryption. All intensity values of an input image are converted to a serial binary digit stream, and the bitstream is scrambled globally by the hyperchaotic sequence. DNA algebraic operation and complementation are performed between the hyperchaotic sequence and the DNA sequence to obtain a robust encryption performance. The experiment results demonstrate that the encryption algorithm achieves the performance of the state-of-the-art methods in term of quality, security, and robustness against noise and cropping attack.

REFERENCES

[1] **Chong Fu, Zhou-feng Chen [2017],** “A New Fast Color Image Encryption Scheme Using Chen Chaotic System” , 978-1-5090-5504-3/17/©2017 IEEE SNPD 2017, June 26-28, 2017, Kanazawa, Japan.

[2] Xu, Lu, et al. [2016] "A novel bit-level image encryption algorithm based on chaotic maps." *Optics and Lasers in Engineering* 78 (2016): 17-25.

[3] **Wang XY, Zhang HL.[2015],** “A color image encryption with heterogeneous bit- permutation and correlated chaos”. IEEE, Opt Commun2015; 342:51–60.

[4] Wang **XY, Liu LT, Zhang YQ [2015].** “A novel chaotic block image encryption algorithm based on dynamic random growth technique”. IEEE Opt Lasers Eng 2015; 66:10–8.

[5] **Abuturab MR.[2015]**, “an asymmetric single-channel color image encryption based on Hartley transform and gyrator transform”. IEEE Opt Lasers Eng 2015; 69:49–57.

[6] **Zhou YC, Cao WJ, Chen CLP.[2014]** “Image encryption using binary bit plane”. Signal Process 2014; 100:197–207.

[7] **Tong XJ.[2013]**,”Design of an image encryption scheme based on a multiple chaotic map”. Commun Nonlinear Sci Numer Simul2013; 18(7):1725–33.

[8] **Sethi, Nidhi, and Deepika Sharma[2012].** "A novel method of image encryption using logistic mapping." *Int. J. Comput. Sci. Eng* 1.2 (2012): 115-119.

[9] **Wang XY, Teng L, Qin X. [2012],**”A novel color image encryption algorithm based on chaos”. Signal Process 2012; 92(4):1101–8.

[10] **Ye GD, Wong KW [2012].** “An efficient chaotic image encryption algorithm based on a generalized Arnold map”. Nonlinear Dyn2012 IEEE 69(4):2079–87.

[11] **Teng, Lin, and Xingyuan Wang.[2012]** "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive." *Optics Communications* 285.20 (2012): 4048-4054.

[12] **Zhu ZL, Zhang W, Wong KW, Yu H.[2011]** A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci2011; 181(6):1171–86.

[13] **Liu HJ, Wang XY[2011].,** “Color image encryption using spatial bit-level permutation and high-dimension chaotic system.” Opt Commun2011; 284(16):3895–903.

[14] **Wang XY, Yang L, Liu R, Kadir A [2010].** "A chaotic image encryption algorithm based on perceptron model". Nonlinear Dyn 2010; 62(3):615–21.

[15] **Liu HJ, Wang XY [2010].** "Color image encryption based on one-time keys and robust chaotic maps". Computer Math Appl 2010; 59 IEEE (10):3320–7.

[16] Li S, Chen G, Cheung A, Bhargava B, Lo K-T [2007]."On the design of perceptual MPEG- Video encryption algorithms". IEEE Trans Circuits Syst Video Technol 2007; 17 (2):214–23.

[17] **Xiao GZ, Lu MX, Qin L, Lai XJ [2006],** "New field of cryptography: DNA cryptography". Chin Sci Bull 2006; 51(12):1413