© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Multiple Image Encryption Using Chaotic Map And DNA Computing

Aarti Patel[1], Dr. Mehul Parikh[2]

[1]M.E(I.T) Student, I.T Department, L.D College Of Engineering, Ahmedabad, Gujarat, India

[2]Associate Prof., I.T Department, L.D College Of Engineering, Ahmedabad, Gujarat, India

ABSTRACT

Security of image and video data has become increasingly important for various applications such as internet-based communications, video conferencing, medical and military application etc. Encryption is usually recommended to solve this issue. Repeatedly, Encrypt the single image is very undesirable. So Multiple image encryption has received attention. Multiple image encryption based on mixed image element and chaos proposed by Zhang,Wang is less secure due to only the order of image blocks scrambled in algorithm and not a content of image.So to resolve that problem novel algorithm proposed in which image content is also scrambled using DNA computing. which will more dependent on plaintext to resist plaintext attack and reduce correlation between pixels to resist stastical attack.DNA technology has been used with chaotic cryptosystem to double assurance the security of image cryptosystem by chaotic system and DNA biological manipulation. So proposed algorithm will be more secure and resisted against recognized attack.

Keywords: : Image Encryption,Algorithm,Chaotic Map,DNA Computing.

I. INTRODUCTION

Algorithms, such as DES,AES and RSA are found unsuitable for multimedia data because these algorithms are designed for accurate data. while digital image has some intrinsic features such as bulk data capacity and high redundancy.Fibonacci, Hash,DNA,Chaos,Transform domain and S-box, have been proposed to be applied to image encryption in the past decade.

A. Requirements Of Image Encryption

- ✓ Ability to get pixel values from image.
- ✓ Create strong encrypted image so that can not easily hacked.
- ✓ Faster encyption time so that can easily transfer to person.
- ✓ Lossless image which can be get after decrypting it.
- ✓ Confusion process in which the pixel positions are permuted to reduce inter-pixel correlation.
- ✓ Diffusion process in which consists of some reversible computations that change the pixel values.

B. Parameters Consider For Security Of Image

a. Key Space Analysis

For an image encryption algorithm to have high security, key space should to at least as large as to resist brute force attack.

b. Key Sensitivity

An encryption algorithm should be very sensitive to any secret key. Any trivial change must lead to a different cipher-image or a wrong decrypted image, from the same cipher-image.

c. Plaintext Sensitivity

It means that any tiny change, even just one bit change, in the plain-image could cause a huge difference in the cipher-image.

d. Information Entropy

The information entropy is defined as the degree of uncertainties in the system. The greater the entropy, the more is the randomness in the image, or the image is more uniform. Thus statistical attacks become difficult.It should be nearer to 8.

$$H(m) = \sum_{i=0}^{2^N-1} p(mi) \times log_2[\frac{1}{p(mi)}]$$

where p(mi) represents the probability of symbol mi , and log2 represents the base 2 logarithm so that the entropy is expressed in bits, N represents the number of bits we use to represent a pixel, and for one colour channel of a pixel, it is clear that N = 8. If an image is ideal random, then for each i, p(mi) = 1/256, and we can easily find that H(m)= 8.

e. NPCR

Number of Pixels Change Rate (NPCR) stands for the number of pixels change rate while one pixel of plain image changed. The NPCR gets closer to 100 to the changing of plain image, and the more effective for the cryptosystem to resist plaintext attack.

$$NPCR = \frac{\Sigma_{i,j} D(i,j)}{M \times N} \times 100\%$$

f. UACI

UACI(Unified Average Changing Intensity) stands for the average intensity of differences between the plain image and ciphered image. The UACI gets closer to 33.333.

$$UACI = (\sum_{i,j} \frac{|C'(i,j) - C(i,j)|}{255})/(M \times N))$$

where M and N are the width and height of the encrypted image, respectively. C and C' are the cipher images, whose corresponding plain images have only one pixel difference. Clearly, in order to with stand the differential attack, the NPCR and UACI values for an ideal cryptosystem should be large enough.

g. Computational Time

It should be less so encryption speed increase.

h. Image Restoration

The cipher-image can be fully recovered by the receiver without loss of data.

i. Robustness

To evaluate robustness of algorithm, attack the encrypted image by salt and pepper noise and block removal. algorithm should robust enough to moderate noise contamination and block missing.

j. Correlation Of Two Adjacent Pixel

It tells us how much there is relation between the same pixels of the original and the encrypted image. The adjacent pixels in plain image are usually highly correlated, which is a weakness to statistical attack. An image encryption should decrease the correlation of two adjacent pixels in the ciphered image. To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, The result indicates that the correlation coeffcients of the plain image are always nearly equals 1, while that of the ciphered image are greatly reduced to close 0.

$$r_{xy} = \frac{E[(x-\gamma_x)(y-\gamma_y)]}{\eta_x \eta_y}$$

where x and y are the gray values of two adjacent image pixels, and E[.] represents the expectation value, denotes the mean value, and η indicates the standard deviation.

II. PRELIMINARIES

A. Chaos Theory

Chaos is supposed to be that the smallest of changes in a system can result in very large differences in that systems behavior.Chaos is a deterministic, random like process found in nonlinear, dynamical system, which is non-period, nonconverging and bounded.Moreover, it has a very sensitive dependence upon its initial condition and parameter.The chaotic sequences are uncorrelated when their initial values are different and spread over the entire space.A chaotic map is a discrete-time dynamical system, defined as the following Eq. 1:

$$x_{k+1} = f(x_k), x \in (0,1), k = 0,1,2,3..$$

B. DNA Computing

A DNA sequence contains four nucleic acid bases A(adenine),C(cytosine),G(guanine),T(thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary.By using four bases A, C,G and T to encode 00; 01; 10 and 11, there are 24 kinds of coding schemes.But there are only 8 kinds of coding schemes that used, which are shown in Table 1 DNA sequence encoding table.

Table 1. The Encoding And Decoding Rules For DNA Sequences.

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

C. Benefits Of DNA Computing

- ✓ Extraordinary information density,
- ✓ Massive parallelism and
- ✓ Ultra low energy consumption.

III. LITERATURE REVIEW

A. Multiple-Image Encryption With Bit Plane Decomposition And ChaoticMaps[1]

Tang proposed algorithm that decomposes input images into bit planes, randomly swaps bit blocks among different bit planes, and conducts XOR operation between the scrambled images and secret matrix controlled by chaotic map. Finally, an encrypted PNG image is obtained by viewing four scrambled grayscale images as its red, green, blue and alpha components. These techniques ensure that it is difficult to observe useful trace between secret keys and plaintext/ciphertext.But this algorithm encrypt only 4 grayscale images.

B.Multiple Image Encryption Algorithm Based On Mixed Image Element And Chaos[2]

Zhang,Wang proposed algorithm based on the mixed image element and piecewise linear chaotic maps (PWLCM).This novel algorithm is for k grayscale images without compression technology. The effciency and the security are contradictory in an encryption algorithm. In Tangs algorithm[1],both the order of image blocks and the content of image blocks are processed. However, only the order of image blocks is scrambled in the new algorithm.Therefore,the security of this algorithm may be a little weaker than Tangs algorithm[1] in theory.

C.Lossless Chaotic Color Image Cryptosystem Based On Dna Encryption And Entropy[3]

The proposed algorithm consists of four processes: key streams generation process, DNA sequences confusion process, DNA sequences diffusion process and pixel level diffusion. .In this algorithm, the final secret key streams are related to both the chaotic system and the original plain-image, which increases the security level and resistance against known/chosen plaintext attacks of the cryptosystem.

D. A Chaotic Color Image Encryption Using Integrated Bit-Level Permutation[4]

Author has proposed algorithm which convert the color image into three bit-level images (R, G, B components) and combine them to one bit-level image.Then, only use bit-level permutation architecture based on chaotic system to encrypt the integrated image. The encryption and decryption speed of our proposed method is 16.97 MB/s while the speed of AES with 128 bit key, AES with 192 bit key, AES with 256 bit key are 11.23 MB/s, 9.25 MB/s, 9.19 MB/s.

E. A Light Weight Secure Image Encryption Scheme Based On Chaos And DNA Computing[5]

In the proposed scheme chaotic logistic map is used which will generate a highly randomized number sequence.The chaotic logistic map runs on low com putational overhead, so it becomes an light weight PRNG.

IV. PROPOSED ALGORITHM

Methodology

STEP 1: First combine k images into one big image.

STEP 2: Convert it in DNA.

STEP 3: Scrambling using chaotic sequence of henon map.

STEP 4: Divide it in small DNA segments.

STEP 5: Perform XOR of DNA segments with previous segment.

STEP 6: Perform DNA addition with previous DNA segment.

STEP 7: Combine DNA segment..

STEP 8: Perform DNA decoding.

STEP 10: Segment it in original image matrices size.

Here random sequence generated for permutation is based on plaintext entropy. So it will increase plaintext sensitivity and can resist against chosen plaintext attack. For decrease correlation between pixels DNA level permutation and diffusion used.

Flowchart Of proposed Algorithm is given below.

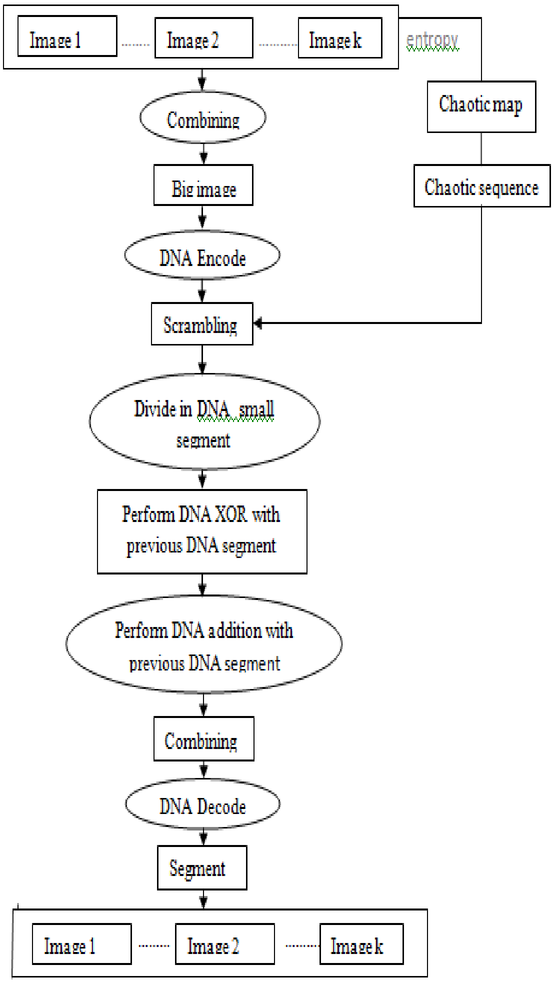

Figure 1. Flowchart For Proposed Model

V. IMPLEMENTATION AND RESULT ANALYSIS

To verify the proposed algorithm, $k = 9$ original gray images whose sizes are equal 512 ×512 taken.

Alice combines these 9 original images into a big image, which is as shown in Fig. 2. Let the initial values and the control parameters of henon systems are,

x(1)=1.234567892456784+en;
y(1)=2.234567892456784+en;
a=1.234567892782301+en;
b=0.123456789987654+en;
where, en=entropy(BigImage);

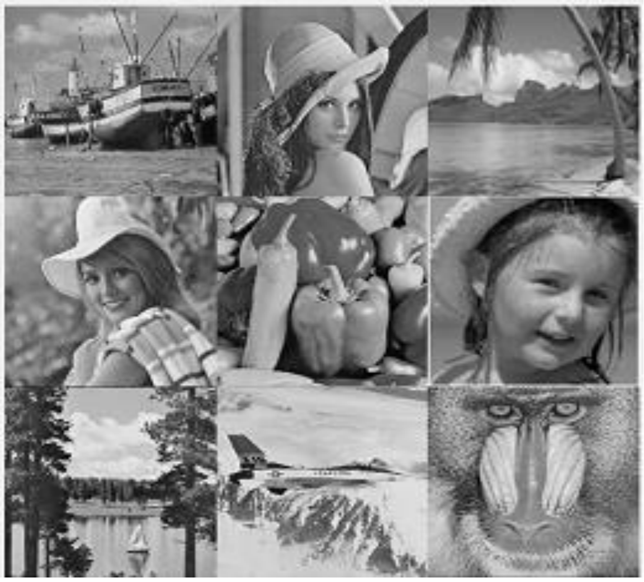

Figure 2. Big Image

The encrypted image is shown in Fig 3.

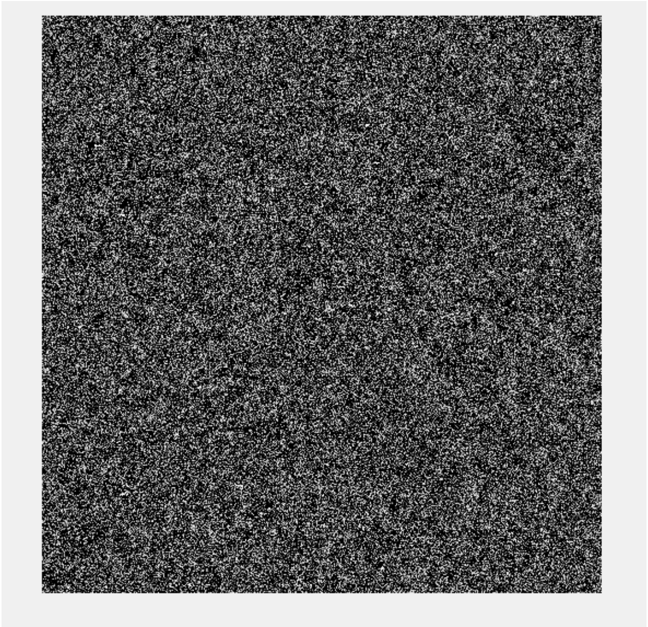

Figure 3. Encrypted Image

1>KeySpace Analysis

The size of the key space is the total number of different keys that can be used in an encryption algorithm. An excellent encryption algorithm should contain large key space to make the brute-force attack infeasible. The proposed algorithm actually does have keys, i.e., the initial values *x*, *y* and the control parameters *a*, *b* of henon systems and entropy of plain image. Supposing that the computer precision is 10^{-15} , so the size of key space is 10^75. Therefore, this key space is large enough to resist the brute-force attack.

2>key sensitivity analysis

The system is very sensitive to the initial conditions which forms the cipher key for the encryption and decryption process. If we taken value of x0 =3.234567892456784 in the encryption process, we get the encrypted image shown in Fig. 4, which clearly shows the dependence of the images on the initial conditions.

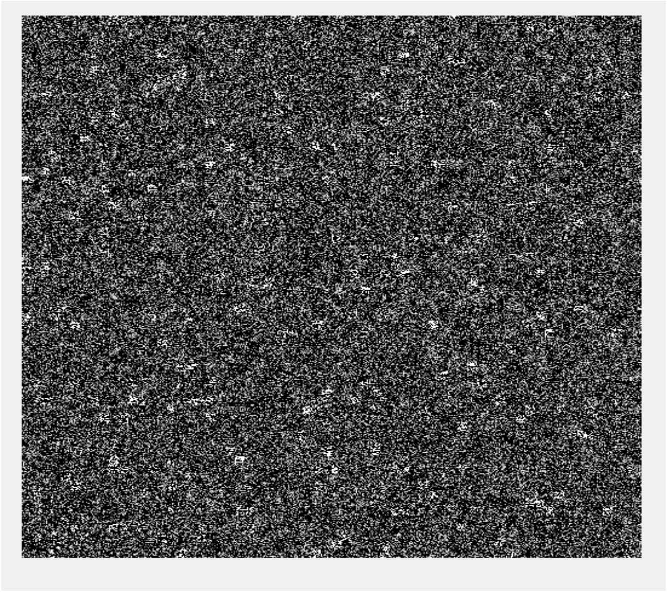

Figure 4. Encrypted Image (key=3.234567892456784)

3>Histogram Analysis

Figs. 5 and 6 show the gray histograms of original images and encrypted images, respectively. It shows that the histogram of the encrypted image is uniform which makes statistical attacks difficult.

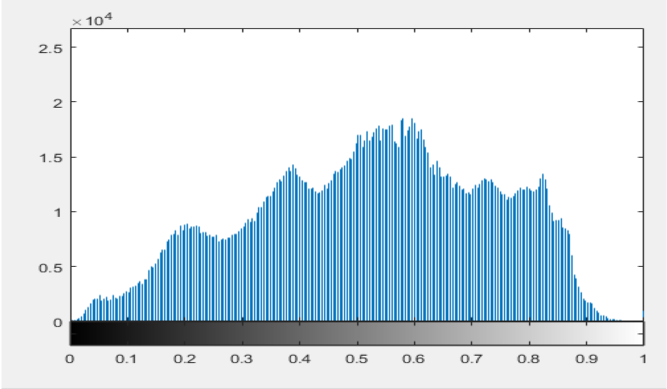

Figure 5. Big Image histogram

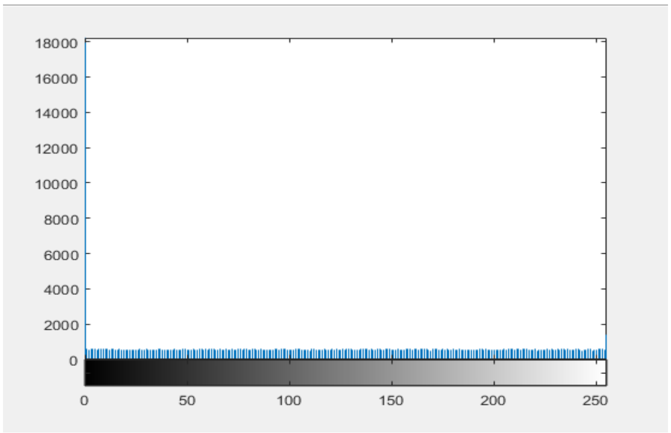

Figure 6. Encrypted Image histogram

4> Differential analysis

The data related to the experimental results are given in Table 2. As can be seen, the proposed method has high *NPCR* and *UACI* values. It means that the proposed algorithm is very sensitive to small changes in the plaintext and can well resist the differential attack.

Table 1

Image	**Correlation between horizontal pixels**	**Correlation between vertical pixels**	**NPCR**	**UACI**
Encrypted image	**0.0612**	**-0.0235**	**99.61**	**33.46**

VI. CONCLUSION

To encrypt multiple image simultaneously and securely, a novel algorithm proposed for multiple image encryption based on DNA computing and chaotic map.Algorithm has benefits of both DNA and chaotic map.which will give more security then Zhang's algorithm in terms of plaintext attack ,statistical attack.

VII. REFERENCES

[1]. Tang Z,Song J,Zhang X,Sun R . Multiple-image encryption with bit-plane decomposition and chaotic maps. Opt Lasers Eng (2016)

[2]. Xiaoqiang Zhang,Xuesong Wang . Multiple image encryption algorithm based on mixed image element and chaos, Computers and Electrical Engineering (2017).

[3]. Xiangjun Wu ,Kunshu Wang ,Xingyuan Wang ,Haibin Kan. Lossless chaotic color image cryptosystem based on DNA encryption and entropy. Springer Science+Business Media B.V. (2017).

[4]. Lin Teng,& Xingyuan Wang & Juan Meng.A chaotic color image encryption using integrated bit-level permutation. Springer Science+Business Media New York (2017).

[5]. Bhaskar Mondal ,Tarni Mandal .A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University Computer and Information Sciences(2016).

[6]. Li Y,Zhang F,Li Y,Tao R . Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform. Opt Lasers Eng (2015).

[7]. Zhang G, Liu Q. A novel image encryption method based on total shuffing scheme. Opt Commun (2011).

[8]. Liu H,Wang X. Color image encryption using spatial bit-level permutation and high dimension chaotic system. Opt Commun(2011).