© 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
National Conference on Advanced Research Trends in Information and Computing Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering, Ahmedabad, Gujarat, India In association with
International Journal of Scientific Research in Science, Engineering and Technology

A Survey on Multiple Image Encryption Using Chaos Based algorithms 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

Due to the development in the field of network technology and multimedia applications, every minute thousands of messages which can be text, images, audios, videos are created and transmitted over wireless network.So encryption is used to provide security. To ensure the security of image transmission,people have proposed many single-image encryption(SIE) algorithms. In the age of big data,although multiple images can be repeatedly encrypted by the SIE algorithm in theory,the encryption effciency is always ineffcient.The encryption algorithm should plaintext sensitive,key sensitive,and lossless.DNA technology has been used with chaotic cryptosystem to double assurance the security of image cryptosystem by chaotic system and DNA biological manipulation.In this paper different multiple image encryption technique based on chaotic map and DNA computing have been studied.

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

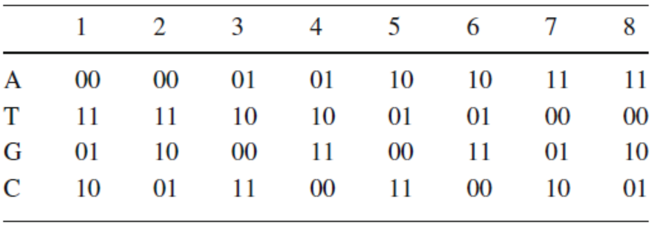
Chaos is supposed to be that the smallest of changes in a system can result in very large differences in that systems behavior.Chaos is a deterministic, random like process found in nonlinear, dynamical system, which is non-period, nonconverging and bounded.Moreover, it has a very sensitive dependence 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 Figure 1 DNA sequence encoding table.



	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

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

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 Chaotic Maps

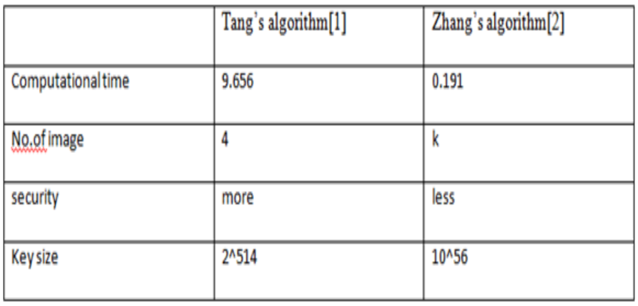
Tang proposed algorithm that decomposes input images into bit planes, randomly swaps bit blocks among different bit planes, and conducts XOR operation between the scrambled images and secret matrix controlled by chaotic map. Finally, an encrypted PNG image is obtained by viewing four scrambled grayscale images as its red, green, blue and alpha components.
Some techniques [7,8] can encrypt multiple images, but their decrypted images are not completely the same with the original images. This means that they are lossy algorithms and thus are not suitable for those applications requiring images with good visual quality, such as medical images.The proposed algorithm reaches good performances in security, robustness, and computational time. It can losslessly retrieve original images from the encrypted images.

This algorithm is robust against salt and pepper noise attack and block removal. 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

Zhang,Wang proposed algorithm based on the mixed image element and piecewise linear chaotic maps (PWLCM).Firstly,The sender combines original images into a big image, and divides it into many pure image elements; secondly, she scrambles these pure image elements with the chaotic sequence generated by the PWLCM system to get mixed image elements; thirdly, she combines these mixed image elements into a big scrambled image,and segments it into small images with the equal size of original images; finally, these small images, i.e.encrypted images, are named with the filenames generated by another PWLCM system.

This novel algorithm is for k grayscale images without compression technology.Li et al. proposed a MIE algorithm based on the cascaded fractional Fourier transform [7] . most of these algorithms encrypt images in the transform domain and usually combine with the image compression technology,So the decryption images are always with some obvious distortion. Meanwhile, these algorithms require the data conversion between the spatial domain and the transform domain.
Therefore, their encryption effciency is always undesirable. 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 in theory.



	Tang's algorithm[1]	Zhang's algorithm[2]
Computational time	9.656	0.191
No.of image	4	k
security	more	less
Key size	2^514	10^56

Figure 2. Comparison between Tang's algorithm[1] & Zhang's algorithm[2]

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

The proposed algorithm consists of four processes:
key streams generation process, DNA sequences confusion process, DNA sequences diffusion process and pixel level diffusion.Many DNA-based image encryption algorithms used the DNA sequence

operations such as addition, subtraction and XOR to diffuse the DNA-encoded image with absence of DNA-level confusion, which makes the security of the cryptosystems not high enough.This proposed scheme involves not only DNA-level confusion and diffusion but pixel-level diffusion, which will enhance the security, complexity and sensitivity of the cryptosystem.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. In order to reach higher security and sensitivity,ciphertext diffusion method employed in crisscross pattern which encrypts two equal sub-images in parallel.

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

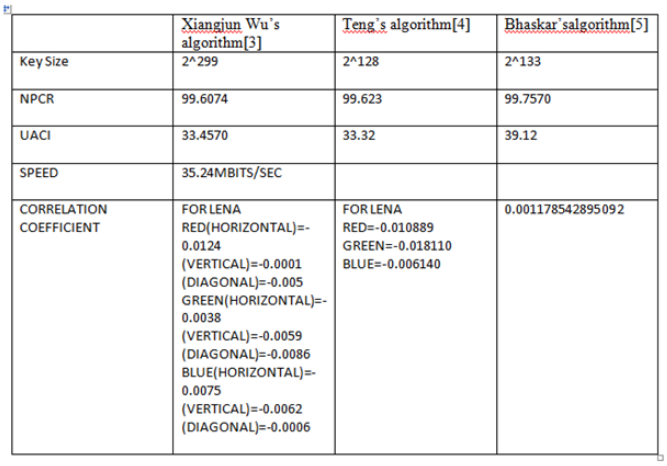
Author has proposed algorithm which convert the color image into three bit-level images (R, G, B components) and combine them to one bit-level image.Then, only use bit-level permutation architecture based on chaotic system to encrypt the integrated image.When diffuse the position of the integrated binary image, the value of the gray pixel is changed as well, so this architecture can achieve similar security to permutation diffusion architecture.

For color image encryption, most of the previous algorithms used multi-round permutation diffusion architecture and encrypt their three color component respectively which is time consuming. 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

In most of the schemes the authors considered the statistical tests like key-space analysis, histogram analysis, correlation of two adjacent pixels, differential attack analysis, information entropy analysis, known plain-text and cipher-text only attack etc. and over all complexity but they have not given enough emphasis on memory uses and energy consumption, throughput of the algorithms.

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. The permuted data are converted to DNA sequence.Same PRNG is again used to generate a random bit sequence. For this purpose, this binary sequence is also converted to its DNA sequence .The DNA sequences C and D are adde together which results in a new DNA sequence E. Eis again converted back to sequence of 8 bit (integer) F form. XORing of each element of the sequence is done with the elements previous to that index on F which gives the final encrypted image.



	Xiangjun Wu's algorithm[3]	Teng's algorithm[4]	Bhaskar'salgorithm[5]
Key Size	2^299	2^128	2^133
NPCR	99.6074	99.623	99.7570
UACI	33.4570	33.32	39.12
SPEED	35.24MBITS/SEC		

CORRELATION COEFFICIENT	FOR LENA
	RED(HORIZONTAL)=-0.0124
	(VERTICAL)=-0.0001
	(DIAGONAL)=-0.005
	GREEN(HORIZONTAL)=-0.0038
	(VERTICAL)=-0.0059
	(DIAGONAL)=-0.0086
	BLUE(HORIZONTAL)=-0.0075
	(VERTICAL)=-0.0062
	(DIAGONAL)=-0.0006
		FOR LENA
		RED=-0.010889
		GREEN=-0.018110
		BLUE=-0.006140
			0.001178542895092

Figure 3. Comparison between Xiangjun Wu's algorithm[3], Teng's algorithm[4] & Bhaskar's algorithm[5]

IV. CONCLUSION

In this literature Survey ,It is concluded that image encryption is more secure if confusion and diffusion process is more complex.An encryption method should more dependent on plain image to resist against plaintext attack and reduce correlation between adjacent pixels to enhace resistance against stastical attack.So algorithm proposed in Multiple image encryption based on mixed image element and chaos is less secure.

V. REFERENCES

[1] Zhenjun Tang, Juan Song, Xianquan Zhang, Ronghai Sun.Multiple-image encryption with bit plane decomposition and chaotic maps.Optics and Lasers in Engineering(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 shuffling 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).