A Survey On Multiple Image Encryption Using Chaos Based algorithms And DNA Computing

AARTI PATEL

M.E(I.T) Student,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 efficiency is always undesirable . In this paper different multiple image encryption technique based on chaotic map and DNA computing have been studied.

Keyword-*image encryption, algorithm, chotic map, dna computing.*

1. NTRODUCTION

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. To achieve the security requirement, a variety of methods, such as Fibonacci, Hash, DNA, Chaos, Transform domain and S-box, have been proposed to be applied to image encryption in the past decade.

2. 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 in which the pixel positions are permuted to reduce inter-pixel correlation.
- Diffusion in which consists of some reversible computations that change the pixel values.

3.Parameters consider for security of image.

1 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**.**

2.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.

3.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

4. Information entropy

The randomness of a message measured by information entropy, it should be nearer to 8.

5.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%, the more sensitive the cryptosystem to the changing of plain image, and the more effective for the cryptosystem to resist plaintext attack.

6.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…%, the more effective for the cryptosystem to resist differential attack.

7.Computational time

It should be less so encryption speed increase.

8.Image restoration

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

9.Robustness

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

10.Correlation of two adjacent pixel

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 coefficients of the plain image are always nearly equals 1, while that of the ciphered image are greatly reduced to close 0.

4. Preliminaries

4.1 Chos theory

- Chaos is supposed to be that the smallest of changes in a system can result in very large differences in that system's 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
- A chaotic map is a discrete-time dynamical system, defined as the following Eq. 1:

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

.1

- The chaotic sequences are uncorrelated when their initial values are different and spread over the entire space.

4.2 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.

	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

Benifits of DNA computing

- Extraordinary information density,
- massive parallelism and
- ultra-low energy consumption,

Comparison Analysis

	Paper 1	Paper 2
Computational time	9.656	0.191
No.of image	4	k
security	more	less
Key size	2^514	10^56

	Paper 3	Paper 4	Paper 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 COFFICIENT	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

Conclusion

In this literature Survey ,It is concluded that image encryption is more secure if confusion and diffusion process is more complex .Also diffusion and confusion at pixel level is more secure .It will reduce correlation between pixels. Also dependency on plain message will make algorithm more resist to plaintext attack. So algorithm proposed in Multiple-image encryption based on mixed image element and chaos is less secure.

Future Work

So algorithm for multiple image encryption that will more secure ,lossless, sensitive to plaintext, less correlation coefficient can be propose in future.

References

- Xiaoqiang Zhang , Xuesong Wang . Multiple-image encryption algorithm based on mixed image element and chaos, Computers and Electrical Engineering (2017).
- 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)
- Zhenjun Tang, Juan Song, Xianquan Zhang, Ronghai Sun .Multiple-image encryption with bit-plane decomposition and chaotic maps. Optics and Lasers in Engineering(2016)
- 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
- Lin Teng,& Xingyuan Wang & Juan Meng. A chaotic color image encryption using integrated bit-level permutation. Springer Science+Business Media New York 2017