Volume-4, Issue-12, Dec-2015 • ISSN No 2277 - 8160

Research Paper | Engineering

Introduction to 3D Chaotic Map for Image Encryption

Lokesh Gagnani IT Department, KITRC, Ahmedabad, INDIA

ABSTRACT

Encryption of images is different from that of texts due to some intrinsic features of images such as bulk data capacity and high redundancy, which are generally difficult to handle by traditional encryption methods. Due to the exceptionally desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. In this paper, the two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption. Various parameters for key sensitivity analysis, Statistical analysis and Differential analysis are discussed.

KEYWORDS : Chaotic system, cryptography, arnold cat map, key senstiivty analysis, statistical analysis, differential analysis

Introduction

The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging .Telemedicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information. Encryption will be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text [1]. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read.

Chaotic Image Encryption

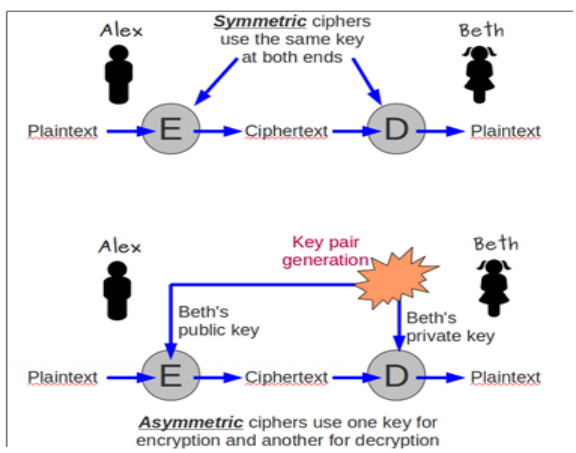
The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics, unpredictable behavior and non linear transform. This concept leads to techniques that can simultaneously provide security functions and an overall visual check, which might be suitable in some applications. Digital images are widely used in various applications, that include military, legal and medical systems and these applications need to control access to images and provide the means to verify integrity of images.

The difference between chaos-based system and traditional cryptography is shown in Table 1.

Chaotic Systems	Cryptographic algorithms
Phase space: set of real numbers	Phase space: finite set of integers
Iterations	Rounds
Parameters	Key
Sensitive to initial conditions and parameters	Diffusion

Table 1: Difference of Chaotic system & Cryptographic system

There are 2 types of methods: Symmetric and Asymmetric. In symmetric same key is used for encryption as well as decryption. In asymmetric different key is used for encryption and decryption. This is shown in Fig 1:



3D Chaotic Image Encryption

The general algorithm or flowchart for chaos-based image cryptosystem is depicted in Fig 2:

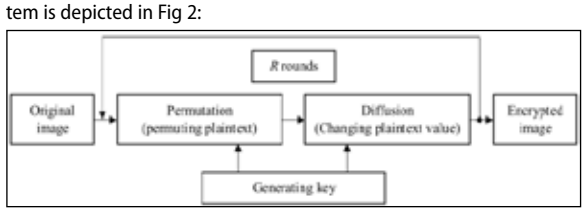


Fig 2: Chaos based Image Cryptosystem

Image Encryption on Lena image (Grayscale) will produce results as shown in Fig 3:

(a) (b)

Fig 3 (a) Plain Image (b) Cipher Image

In 3D chaotic image cryptosystem the 2D image is to be piled up to 3D. Then 3D Arnold Cat Map is applied. After the diffusion process the

Security Analysis
A good encryption scheme should resist all kinds of known attacks, such as known-plain-text attack, cipher-text-only attack, statistical attack, differential attack, and various brute-force attacks.

A. Key Space Analysis
A good image encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible

1. Number of control parameters

2. Key Sensitivity Test: It is tested s per the following steps:

1. First, a 512 X 512 image is encrypted by using the test key "1234567890123456".

2. Then, the least significant bit of the key is changed, so that the original key becomes, say "1234567890123457" in this example, which is used to encrypt the same image.

3. Finally, the above two ciphered images, encrypted by the two slightly different keys, are compared.

Here lena image of 512 X 512 size is considered.

B. Statistical analysis
1. Histograms of encrypted images
Select several 256 grey-scale images of size 512 X 512 that have different contents, and calculate their histograms. One typical example among them is shown in Fig. 6. From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image.

2. Correlation of two adjacent pixels
To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively, in a ciphered image, the following procedure was carried out. First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate the correlation coefficient of each pair by using the following two formulas:

$$\operatorname{cov}(x,y) = E(x - E(x))(y - E(y)),$$

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

C. Differential Analysis
In general, the opponent may make a slight change (e.g., modify only one pixel) of the encrypted image, and then observes the change of the result. In this way, he may be able to find out a meaningful relationship between the plain- image and the cipher-image. If one minor change in the plain-image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then this differential attack would become very inefficient and practically useless.

There are three common measures were used for differential analysis: MAE, NPCR and UACI. Mean Absolute Error (MAE). The bigger the MAE value, the better the encryption security. NPCR means the Number of Pixels Change Rate of encrypted image while one pixel of plain-image is changed. UACI which is the Unified Average Changing Intensity, measures the average intensity of the differences between the plain-image and Encrypted image.

Let C (i , j) and P (i , j) be the color level of the pixels at the i th row and j th column of a W × H cipher and plain-image, respectively. The MAE between these two images is defined in

$$\mathrm{MAE} = \frac{1}{W \times H} \sum_{j=1}^{W} \sum_{i=1}^{H} \left| c(i,j) - p(i,j) \right|.$$

Consider er two cipher-images, C 1 and C 2, whose corresponding plain-images have only one pixel difference. The NPCR of these two images is defined in

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

where W and H are the width and height of the image & D (i ,j) is defined as

$$D(i,j) = \begin{cases} 0, & \text{if } C1(i,j) = C2(i,j) \\ 1, & \text{if } C1(i,j) \neq C2(i,j) \end{cases}$$

Another measure, UACI, is defined by the following Formula:

$$\mathrm{UACI} = \frac{1}{W \times H} \sum_{i,j} \left[\frac{c1(i,j) - c2(i,j)}{255} \right] \times 100\%$$

CONCLUSION
In this paper, the well-known two-dimensional chaotic cat map has been generalized to three-dimensional, and then used to design a fast and secure symmetric image encryption scheme. This new scheme employs the 3D cat map to shuffle the positions (and, if desired, grey values as well) of image pixels and uses another chaotic map to confuse the relationship between cipher-image and plain-image, thereby significantly increasing its resistance to various attacks such as the statistical and differential attacks. This scheme is particularly suitable for real-time Internet image encryption and transmission applications.

APPLICATIONS
(1) Military Applications
(2) Image Steganography
(3) Image Watermarking
(4) Biometric Applications
(5) Banking
(6) Medical diagnosis
(7) Video Processing
(8) Security Appliances

REFERENCES

[1] Guanrong Chen, Yaobin Mao , Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Elsevier, 2004, pp. 749-761. [2] Ephin M, , Judy Ann Joy, N. A. Vasanthi, "Survey of Chaos based Image Encryption and Decryption Techniques", IJCA, 2013, pp. 1-5. [3] Geeta, "A survey on different chaotic Encryption approaches", IJATER, 2014, pp. 99-104. [4] Ruisong Ye and Wei Zhou, "A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", MECS, 2012, pp. 38-44. [5] Pawan N. Khade and Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", IJCSI, 2012, pp.323-328. [6] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, "A Survey On Different Image Encryption and Decryption Techniques.", IJCSIT, 2013, pp. 113 – 116. [7] Kamlesh Gupta , Sanjay Silakari , "New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, 2011, pp. 139-150. [8] Mintu Philip, Asha Das, "Survey: Image Encryption using Chaotic Cryptography Schemes", IJCA, 2011, pp. 1-4. [9] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", Elsevier, 2012, pp. 2943-2959. [10] Shiguo Lian, Yaobin Mao, Zhiquan Wang, "3D Extensions of some 2D chaotic maps and their usage in data encryption", IEEE, 2003,pp. 819-823. [11] Schneier B. Cryptography: Theory and Practice. Boca Raton: CRC Press; 1995. [12]