International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey of 3D Chaotic Map Techniques for Image Encryption

Lokesh P. Gagnani[1], Dr. Sunita Varjani[2]

[1]Assistant Professor, Information and Technology Department
Kalol Institute of Technology, Kalol, Gujarat, India

[2]M. G. Science Institute, Ahmedabad, Gujarat, 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 Sensitivity analysis, Statistical analysis, Differential analysis

1. 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 [5]. 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.

2. Chaos Theory (Chaotic Maps)

A chaotic map is a map (evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter.

Chaos theory is the field of study in mathematics that studies the behavior of dynamical systems that are highly sensitive to initial conditions—a response popularly referred to as the butterfly effect. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for such dynamical systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. This behavior is known as **deterministic chaos**, or simply **chaos**. The theory was summarized by Edward Lorenz as:

–Chaos: When the present determines the future, but the approximate present does not approximately determine the future."

2.1 Principles of Chaos

- **The Butterfly Effect**: This effect grants the power to cause a hurricane in China to a butterfly flapping its wings in New Mexico. It may take a very long time, but the connection is real. If the butterfly had not flapped its wings at just the right point in space/time, the hurricane would not have happened. A more rigorous way to express this is that small changes in the initial conditions lead to drastic changes in the results.

- **Unpredictability**: Because we can never know all the initial conditions of a complex system in sufficient (i.e. perfect) detail, we cannot hope to predict the ultimate fate of a complex system. Even slight errors in measuring the state of a system will be amplified dramatically, rendering any prediction useless. Since it is impossible to measure the effects of all the butterflies (etc) in the World, accurate long-range weather prediction will always remain impossible.

- **Order / Disorder** Chaos is not simply disorder. Chaos explores the transitions between order and disorder, which often occur in surprising ways.

- **Mixing**: Turbulence ensures that two adjacent points in a complex system will eventually end up in very different positions after some time has elapsed. Examples: Two neighboring water molecules may end up in different parts of the ocean or even in different oceans. A group of helium balloons that launch together will eventually land in drastically different places. Mixing is thorough because turbulence occurs at all scales. It is also nonlinear: fluids cannot be unmixed.

- **Feedback:** Systems often become chaotic when there is feedback present. A good example is the behavior of the stock market. As the value of a stock rises or falls, people are inclined to buy or sell that stock. This in turn further affects the price of the stock, causing it to rise or fall chaotically.

- **Fractals:** A fractal is a never-ending pattern. Fractals are infinitely complex patterns that are self-similar across different scales. They are created by repeating a simple process over and over in an ongoing feedback loop. Driven by recursion, fractals are images of dynamic systems – the pictures of Chaos. Geometrically, they exist in between our familiar dimensions. Fractal patterns are extremely familiar, since nature is full of fractals. For instance: trees, rivers, coastlines, mountains, clouds, seashells, hurricanes, etc.

Various chaotic maps that are commonly used are: Arnold Cat Map, Baker Map, Henon Map, Ikeda Map, Logistic Map, Lorenz attractor, Rossler attractor, Tangent Map, Tent Map, Tinkerbell Map. Further Arnold Cat Map is used mostly.

3. Literature Review

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. Due to strong correlation in image pixels the traditional cryptography methods such as DES, IDEA, etc fail. However the chaos theory is a solution to this due to butterfly effect in initial conditions. The 2D chaotic methods are extended to 3D for resistance against attacks.

Table 1: Difference of Chaotic system & Cryptographic system

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

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 Figure 1:

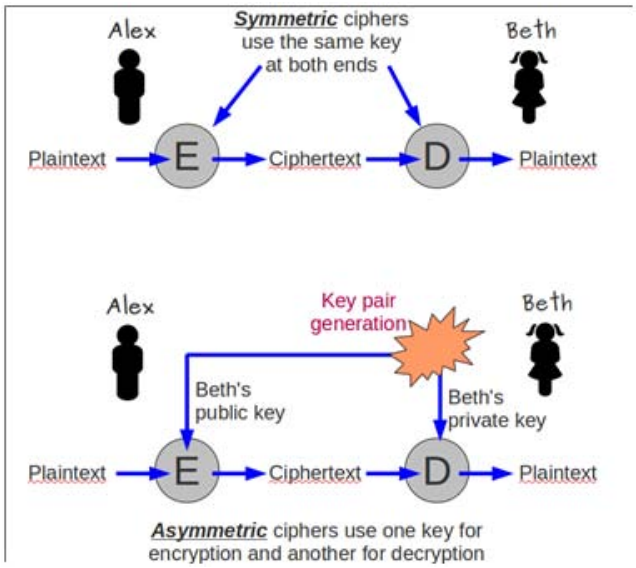

Figure 1: Symmetric and Asymmetric Ciphers

The existing approaches are depicted in Table 2. Comparisons of various block and stream encryption techniques are discussed in Abhishek Misra (2011) [1].

Table 2: Existing Approaches in 3D Image Encryption

Author	*Approach*	*Merit*	*Research Gap*
Guanrong Chena[5]	3D cat map with diffusion by XOR and mod operation	Fast and secure	Confusion by other methods.
Ruisong Ye[13]	3D Skew Tent Map and Coupled Map Lattice	Resistance to cipher-image attacks	Not compared with chaos method
Pawan N. Khade[10]	3D logistic map, 3D Chebyshev map, and 3D, 2D Arnolds cat map	Higher key sensitivity	Not compared with chaos method
A. Kanso[2]	3D Arnold cat map	Better statistical properties	Not compared with chaos method
Juan Li[6]	3D Logistic map	Resistance to statistical attack	Not compared with chaos method
Neethu Subash[9]	2D Arnold cat map, 3D Chebyshev map, 3D logistic & double layer NN	Better NPCR and UACI values	more time when it comes to large size data
Pragati Thapliyal[11]	Arnold cat map and hash function	Diffusion through Arnold Cat map and hash functions are for authenticity.	Video data
Chinchu Thampi	3D chebyshev map and 3D logistic map	Resistance against plaintext attack is obtained using masking process.	Not compared with chaos method

4.3D Chaotic Image Encryption

The general algorithm or flowchart for chaos-based image cryptosystem is depicted in Figure 2. The chaos based encryption architecture consists of 2 stages: confusion and diffusion. In the confusion stage, permutations of image pixels are done in a secret order, without changing their values. The purpose of the diffusion stage is to change the pixel values sequentially so that a small change in one pixel is spread out to many pixels, with anticipation to the whole image. To decor relate the affiliation between adjacent pixels, the confusion stage is performed n times, where n is usually larger than 1, followed by the diffusion stage. The complete n-round confusion and single round diffusion repeat for m times, with m usually larger than 1, so as to get an acceptable level of security.

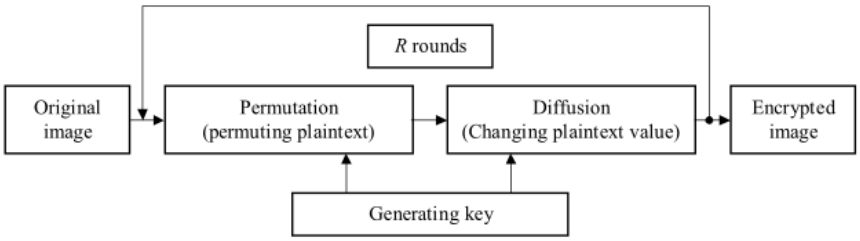

Figure 2: Chaos based Image Cryptosystem

Image Encryption on lena image (Grayscale) will produce results as shown in Figure 3. For color image the result of image encryption is shown in Figure 4.

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

Figure 4 (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 3D image is transformed back to 2D image.

5. 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.

5.1 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 as 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.

5.2 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:

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

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

5.3 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 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:

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

6. 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] Abhishek Misra, Ashutosh Gupta and Damodar Rai, ―Analysing the parameters of chaos based image encryption schemes", World Applied Programming, 2011, pp. 294-299.
[2] A. Kanso, M. Ghebleh, ―Anovel image encryption algorithm based on a 3D chaotic map", Elsevier, 2012, pp. 2943-2959.
[3] Ephin M, Judy Ann Joy, N. A. Vasanthi, ―Survey of Chaos based Image Encryption and Decryption Techniques", IJCA, 2013, pp. 1-5.
[4] Geeta, ―A survey on different chaotic Encryption approaches", IJATER, 2014, pp. 99-104.
[5] Guanrong Chen, Yaobin Mao, Charles K. Chui, ―A symmetric image encryption scheme based on 3D chaotic cat maps", Elsevier, 2004, pp. 749-761.
[6] Juan Li, Yong Feng, Xuqiang Yang, ―Discrete Chaotic based 3D Image encryption Scheme", IEEE, 2009.
[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] Neethu Subash, Meera Vijayan, Dr. Varghese Paul, ―A Triple Key 3-d Chaotic Image Encryption Method using Double Chaotic Neural Networks", IJARCCE, Vol. 3, Issue 1, January 2014, pp. 5015-5020.
[10] Pawan N. Khade and Prof. Manish Narnaware, ―3D Chaotic Functions for Image Encryption", IJCSI, 2012, pp.323-328.
[11] Pragati Thapliyal, Madhu Sharma, ―Image Encryption and Authentication scheme using 3D Chaotic Map", IJCA, Volume 117, No. 17, May 2015, pp. 15-18.

[12] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, ―ASurvey on Different Image Encryption and Decryption Techniques.” IJCSIT, 2013, pp. 113 – 116.
[13] Ruisong Ye and Wei Zhou, ―AChaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice”, MECS, 2012, pp. 38-44.
[14] Schneier B. Cryptography: Theory and Practice. Boca Raton: CRC Press; 1995.
[15] Shiguo Lian, Yaobin Mao, Zhiquan Wang, ―3D Extensions of some 2D chaotic maps and their usage in data encryption”, IEEE, 2003, pp. 819-823