Encrypting and Decrypting Photos Using Cat Chaotic Map

Thal Ei Khaing, May Phyo Oo
Computer University, Pathein
thaleikhing@gmail.com, mayphyooo@gmail.com

Abstract

Digital image encryption/decryption is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. This paper presents a new scheme of digital image encryption based on the cat chaotic mapping. In this system, a cat chaotic mapping is used to disorder the pixel coordinates of the digital image and then perform exclusive OR operation between certain pixel value of the digital image and a chaotic value that is dependent on the encryption parameters, the iterative time and the coordinates. In addition, the statistical characteristics of the encrypted digital image can be uniformed by diffusion technique of Cat Chaotic Map. Hence this system is easy to realize, has satisfied scrambling effect, and can be used as pretreatment for digital image hiding and disguising.

1. Introduction

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. There are two algorithms in cryptography. They are symmetric and asymmetric algorithm. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Asymmetric algorithm is a public-key cryptosystems; the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption [5].

The main aim of digital image scrambling, which is used as the preprocessing or post-processing in image information hiding, is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. The encryption permutation of the digital image requires applying “permutation” and “diffusion” mechanism alternately. Permutation is used to transform the pixel coordinate of the graph, while diffusion is used to iterative the pixel value of the graph, in order to uniform the statistical characteristics of the encrypted graph, and complicate the relationship between the plaintext graph and cipher text graph [3].

The chaos system is an outer complex behavior produced by the internal random property of the nonlinear definite system, which is a pseudo-random movement while it looks like a random process. Today, chaos-based techniques have been involved in data securities and confidential communication system. Recently, many methods concerning chaotic carrier modulation in digital communication that can overcome the multipath-related problems are to present certain securities[7].

This system can be used in the secure transmission of images, such as maps, photos, building image used in military area. With the rapid development of Internet technology, communication using multimedia technique has become one main approach of communication. Image information has become important because of its vitality and visualization. Image data transferred in the network must not be public and both sides of communication must implement secure communication, such as photographs from military satellite, drawings of military establishment.

The organization of this paper is as follows. In section 2, we review related work and problem domain. In section 3, we introduce about Chaotic System, Encryption Process and Decryption Process of Cat Chaotic Map. Section 4 explains Proposed System in detail. Implementation of this system is described in section 5. We conclude in section 6 with a brief discussion of conclusion and future work.

2. Related Work

Image data transmitted are characterized in term of privacy, integrity and authenticity thought public network. Thus keeping secret of image data is getting more and more attention. Conventional cryptosystem, such as DES, is not suitable for image encryption because of the special storage characteristics of an image. Most of the conventional image encryption algorithms are based on position permutation [2].

The development of chaotic dynamics makes people realize that chaos can be novel nature cryptosystem because chaotic systems have their corresponding counterparts in cryptosystems, such as ergodicity, confusion, exponentially growth, and sensitivity to the initialize conditions. There are several algorithms in chaotic map image encryption system such as Standard Map, Cross Map, Cat Map, Baker Map etc. In this system, Cap Map algorithm is used. With the simplicity and dependence on the initial values, its security nature is unbreakable.

Chaos encryption has been researched since the last decade. Several papers regarding this have been published, most of which discussed about application of chaos encryption in secure communication as well as in optical data [4–5]. However, for the past five years there are several chaotic image encryption algorithms that have been proposed. These algorithms manipulate the pixels by scattering them according to some chaotic function. Yen, and Guo [8-9] proposed two chaotic image encryption algorithms whereby the image’s pixels are rearranged based on a random binary sequence generated by a chaotic system. Li et al., [6] and Cai, Y. improved the chaotic encryption scheme of Alvarez et al., [6] because the original scheme is so vulnerable to attacks. Conversely, Fridrich [2-3] proposed another chaotic image encryption algorithm that does not require a chaotic generator.

This system firstly uses a cat chaotic mapping to disorder the pixel coordinates of the digital image. Based on the cat chaotic mapping, we use a new diffusion technique to uniform the statistical characteristics of the encrypted digital image. A chaotic value, which is dependent upon the encryption parameters, the iterative time and the coordinates, would be performed exclusive OR operation with certain pixel value of the digital image. Thereby we obtain the encrypted message. In order to restore the information, the disordered digital image should be performed inverse exclusive OR operation and inverse cat mapping.

3. Chaotic System

The chaos is an outer complex behavior produced by the internal random property of the nonlinear definite system, which is a pseudo-random movement while it looks like a random process. Today, chaos-based techniques have been involved in data securities and confidential communication system. Recently, many methods concerning chaotic carrier modulation in digital communication that can overcome the multipath-related problems are to present certain securities.

The two basic properties of chaotic systems are the sensitivity to initial conditions and mixing. Sensitivity to initially close points, iterates quickly diverged, and bear no correlation after a few iterations. Sensitivity to parameters causes the properties of the map to change quickly when the parameters on which the map depends on mildly disturbed. Mixing is the tendency of the system to quickly confuse small portions of the state space into an intricate network so that two nearby points in the system totally lose the correlation they once shared and get scattered all over the state space. These properties are the key aspects of chaotic maps that have allowed them to be used to generate complicated patterns of pixels and the gray levels in an image.

Traditionally, there are two ways in which chaos is used an image encryption schemes: (1) 1-D chaotic maps like logistic map and generalizations of logistic map to generate pseudo-random bits with desired statistical properties to realize secret encryption operations. and (2) 2-D chaotic maps like Arnold's cat map, Baker map or fractal-like curves to realize secret permutations of digital images. The first approach has been widely used to design chaotic stream chipers, while the second is specially employed by chaos-based block encryption schemes.

3.1. Properties of Chaotic Map

The characteristics of the chaotic maps have attracted the attention of cryptographers since it has many fundamental properties such as ergodicity, sensitivity to initial condition and system parameter, and mixing property, etc. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

3.2. Cat Chaotic Map

The cat chaotic mapping is a discrete chaotic modal proposed by Arnold and Avez. The image can be permutated and the mapping is defined as below:

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \text{ (mod 1)}, A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

Where (xn, yn) is pixels position in an N x N image; (xn+1, yn+1) is the transformed position after cat map; both “a” and “b” are the system parameters and must be the plus integers. The determinant value is 1, so cat map is a map which keeping area (no attractor). At the same time, the cat map is one-to-one mapping; each point in matrix can be transformed to another point uniquely. Cat map has two typical factors, which bring chaotic movement: tension (multiply matrix in order to enlarge x, y) and fold (taking mod in order to bring x, y in unit matrix). In fact, cat map is a chaotic map.

Image position can be scrambled via the iteration of cat map, consequently realizing the image encryption. With the difference of the iteration times, the relevant result of scrambling is also different. For a 256 x 256 gray image, it is hard to find out the trace of original image after iterating 30 times, reaching the effect of scrambling; the image after iterating 64 times is the same as the original image, so cat map has the periodicity. With the differences of the parameter and the image's size, the periodicity is different. Image can be scrambled via keeping the value of a, b secret, but the periodicity will bring some insecure factors, so applying cat map solely can not meet the demands of encryption; and cat map only transforms the original image's position, however the pixels' values have not been changed. The original image can be recovered via the method of exhaustion, so on the base of scrambling, it is necessary to modify the pixels' values to realize double encryption.

3.2.1 Encryption Process

The cat chaotic mapping to transform the pixel coordinate of the digital image using, to translate the original coordinates (x, y) of the image information into the new coordinate (x ', y ') .it can get that:

$$x' = (x + ay) \pmod N \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$y' = (bx + (ab + 1)\, y) \pmod N \ldots\ldots\ldots\ldots (2)$$

Firstly with the cat chaotic mapping, need to translate(x,y)into ((x+ay) (modN), (bx+(ab+1)y) (modN)) and disorder the coordinates of the image information. Secondly in order to diffuse the pixel value, it should calculate f (x,y,a,b,k) which performed exclusive OR operation with certain pixel value P of the coordinates p(x,y) to get a new pixel value P' .k is the iterative time.

$$P' = P \wedge f(x, y, a, b,k) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Where,

$$f(x, y, a, b, k) \quad = (x' * y' + k) \pmod N = ((x + ay) * (bx + (ab + 1)\, y) + k) \pmod N \ldots\ldots\ldots\ldots\ldots (4)$$

k = iteration times to induce security of encrypted image

The chaotic mapping is sensitive to the initial value, which guarantees the uniqueness and unbreakable of the disordering process.

3.2.2 Decryption Process

The procedure for the decryption is similar with encryption, except that the inverse permutation transformation formula can be changed as:

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = A^{-1} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} (\mathrm{mod}\, N),\ A^{-1} = \begin{bmatrix} ab+1 & -a \\ -b & 1 \end{bmatrix}$$

Before every inverse permutation transformation, exclusive OR operation with the pixel value for each pixel coordinates should be performed. When compiling the simulation program, this algorithm will induce error in the course of inverse transformation.

4. Proposed System

This system presents the photo image encryption and decryption by CAT Map Chaotic System. This system can be used in the secure transmission of images, such as maps, photos, building image used in military area. Image file is encrypted using CAT chaotic map algorightm. Chaotic map encryotoin consists of two process – confusion and diffusion. Confusion process is shift pixels according to CAT Map algorithm and diffusion process is encrypting pixels values (color values) with XOR function. Both process needs input parameters (keys). The structure of CAT map encryption used in this system is shown in Figure 1. Confusion and diffusion processed is looped according to iteration time which is user input parameter.

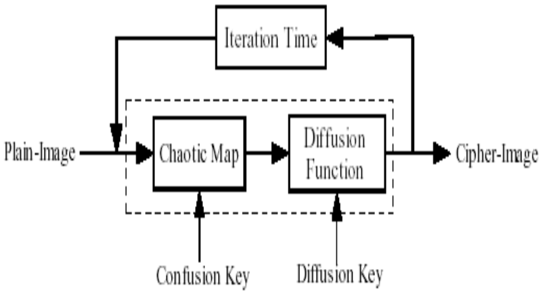


Figure 1 Chaotic Map Structure

Confusion Key = key used in confusion process, in this system they are a and b.

Diffusion Key = key used in diffusion process, in this system diffusion key is a, b and k.

4.1 Process Flow of the System

The process flow of the system is as follows:

The system reads the pixels of input image. If the image has different width and height, it is padded to form the squared image (same width and height) as in the Figure 2. Then coordinates of the image pixels are shuffled according to equation 1. This step is the confusion process of CAT Map algorithm. The pixel value of the confusion image is decrypted by diffusion process. Then we got the encrypted image. In the decryption phase, pixel values are XOR to get the original pixel value. Then inversed process of confusion phase is performed to get the right coordinate.

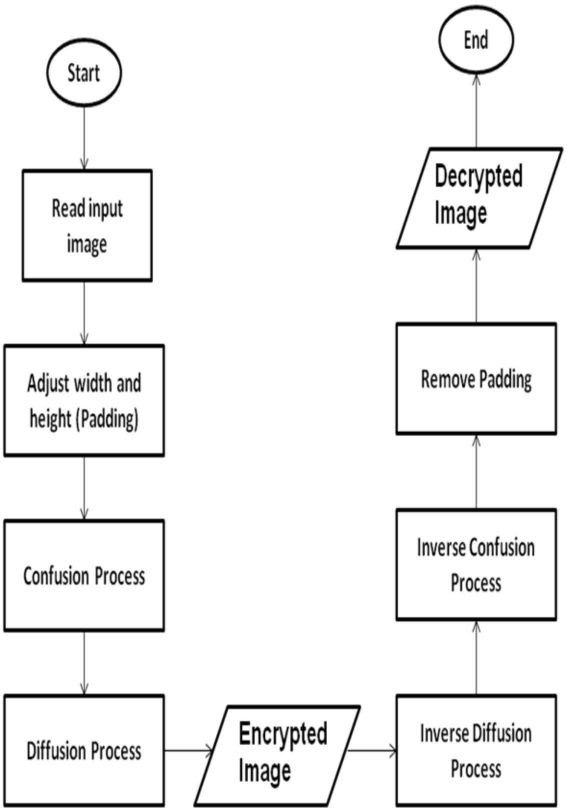


Figure 2: Process Flow of the System

Image reading process of this system is shown in the following algorithm:

```
Algorithm ReadingImage
Input Image inputimg
Output int [] colors
Begin
        width = inputimg.getWidth ( );
        height = inputimg.getHeight ( );
        int [] colors = new int [width * height];
        int c = 0;
        for (int x = 0; x < width; x++)
        for (int y = 0; y < height; y++)
        colors[c++] = inputimg.getRGB(x, y);
        end for
        return colors
End
```

5. System Implementation

This system is implemented using Java Programming language with jdk 1.5. Image types that have been supported by Microsoft Windows, such as jpeg, gif, png, bmp, etc., are supported in this system. Images with larger size are processed with slower performance. It has been tested on the computer with Intel (R) Oentium(R) Dual CPU E2200 @ 2.20 GHz 2.22 GHz, 1.99 GB of RAM. It performs well for the image with wallpaper size until 1280 x 1280 pixels.

Step by Step running example of encryption process and decryption process is simulated in the following blocks. The example scenario is based on 10 x 7 images.

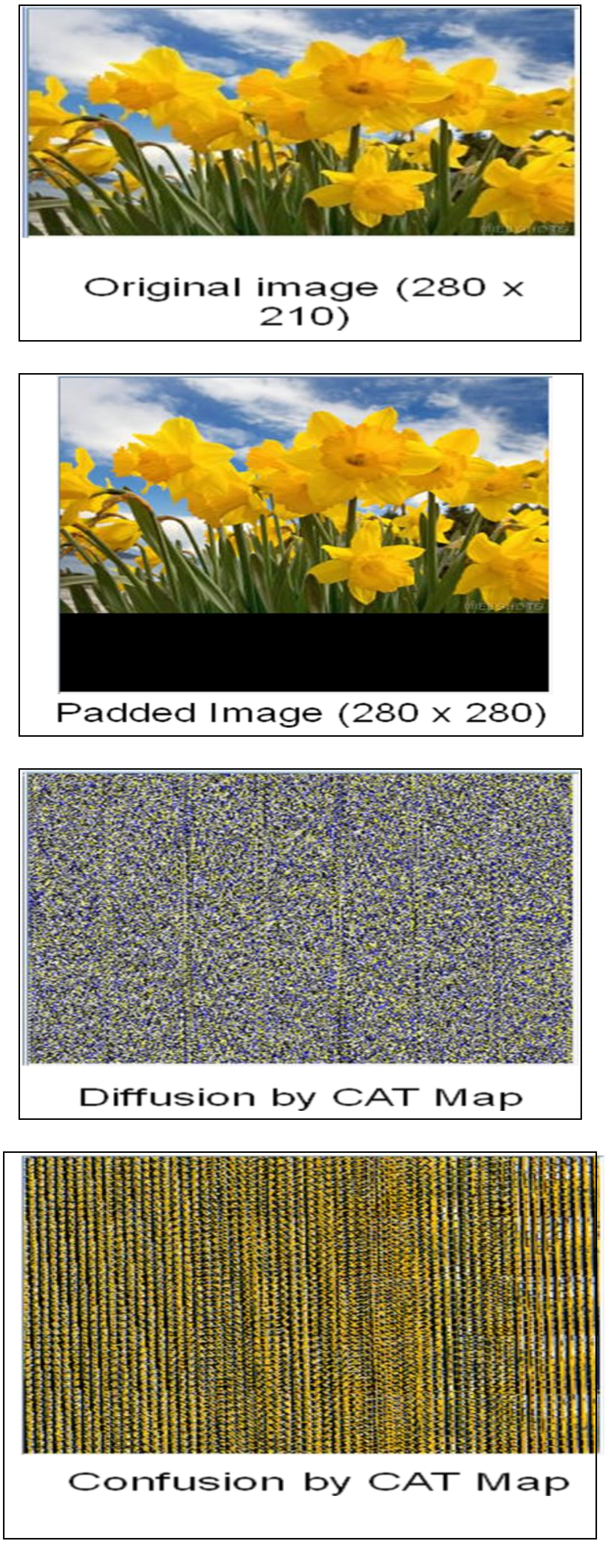
The input pixel values:

[221, 121, 43, 0, 234, 101, 0, 4, 5, 6
7, 0, 34, 65, 78, 192, 99, 19, 25, 25
1, 1, 4, 89, 89, 100, 100, 78, 188, 200
95, 29, 29, 37, 76, 98, 98, 17, 17, 100
123, 123, 78, 90, 26, 39, 45, 4, 90, 18
90, 12, 16, 18, 34, 87, 95, 90, 90, 30
30, 56, 78, 39, 49, 50, 34, 87, 75, 75]

When it is padded to 10 x 10 image, the pixel values will be:
[221, 121, 43, 0, 234, 101, 0, 4, 5, 6
7, 0, 34, 65, 78, 192, 99, 19, 25, 25
1, 1, 4, 89, 89, 100, 100, 78, 188, 200
95, 29, 29, 37, 76, 98, 98, 17, 17, 100
123, 123, 78, 90, 26, 39, 45, 4, 90, 18
90, 12, 16, 18, 34, 87, 95, 90, 90, 30
30, 56, 78, 39, 49, 50, 34, 87, 75, 75
0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

6. Experimental Result

This system is tested with different types of images with different image sizes. We tested images obtained from the internet and from the wall papers in computer. Following images show the step by step process of encryption. The topmost image is the orginal image provided by user. The width of input image is larger than the height, so 0 value (black color) is padded at the lower portion of the input image, so that the width and height become the same. Then pixels of padded image are shift according to CAT map algorithm.



Original image (280 x 210)

Padded Image (280 x 280)

Diffusion by CAT Map

Confusion by CAT Map

Figure 3: Running process by CAT map encryption

7. Conclusion

This paper presents image encryption/decryption scheme which utilizes a cat chaotic map system. It is a feedback mechanism, which leads the cipher to a cyclic behavior so that the encryption of each plain pixel depends on the key (K), the value of the previous cipher pixel (Ci) and the output of the cat chaotic map (Xi). This system is useful for real-time image encryption, decryption and transmission applications because cat chaotic map is fast and secure algorithm. It can be applied to Encryption of Military map, building photos, construction plan (sketch). The chaotic cat mapping is sensitive to the initial value, which guarantees the uniqueness and unbreakable of the disordering process. In addition, the experimental results of the chaotic mapping show that this diffusion technique can solve the problems. Hence, this system is very effective to uniform the statistical characteristics of the encrypted graph, and the efficiency is very high.

8. REFERENCES

[1] Bruce Schneider. John Wiley & Sons, Inc. New York, second edition. 1996. Applied Cryptography Protocols, Algorithms, and Source Code in C.

[2] G. C. Kessler. Published by Auerbach, 1998' (22 December 2007). An Overview of Cryptography. http://www.garykessler.net/

[3] H J Gao, Y S Zhang, S Y Liang, et al. Chaos, Solitons and Fractals, 2006, vol.29, pp.393-399 26. A New Chaotic Algorithm for Image Encryption.

[4] K. Wang , Pei , Z. Liuhua ,S. Aiguo Song, H. Zhenya. Elsevier, Physics Letters A, Vol. 343, Issue 6, 2005, pp. 432–439. On the Security of 3D Cat Map based Symmetric Image Encryption Scheme.

[5] Neal Koblitz. Springer-Verlag. ISBN: 0-387-94293-9. A Course in Number Theory and Cryptography.

[6] P. P. Dang, P M. Chau. IEEE Trans. Consumer Electronics, vol. 46, no.3, 2000, pp. 395-403. Image Encryption for Secure Internet Multimedia Applications.

[7] Philip R.Zimmermann. Scientific American. October 1998. Cryptography for the Internet.

[8] W. Stallings. Prentice Hall, New Jersey. 1999. Cryptography and Network Security: Principles and Practice.

[9] Z H Guan, F J Huang, W J Guan. Physics Letters A, 2005, vol. 34, pp.153-157. Chaos based Image Encryption Algorithm.