Performance Comparison of Chaotic Cat Map and Modified Chaotic Cat Map Encryption

Moe Moe Myint, Khin Kyu Kyu
Computer University, Pathein
m.moe90@gmail.com, khinkyu28@gmail.com

Abstract

Nowadays, Image information is routinely used in many applications. When those images are transmitted over the communication channel, it needs the privacy. Therefore, Image encryption plays an important role in protecting images. This paper presents an image encryption based on chaotic algorithm for securing images. In this system, chaotic maps are 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 chaotic value. The implementations of Cat chaotic map and Modified Cat Chaotic map encryption algorithm are presented for different types of image files such as jpeg, bmp, gif and so on. Finally, the computational running times to analyze the encryption time and decryption time of the two algorithms are compared.

1. Introduction

Nowadays, Electronic communication is being widely used all over the world. With the proliferation of the Internet and maturation of the digital signal processing technology, applications of digital imaging are prevalent and rapidly increased. Many digital devices, such as medical imaging systems, military image database and communications as well as confidential video conferencing require special and reliable security in storage and transmission of digital images/videos.

In this regard, strong security technology is required to protect users' sensitive digital data. Encryption is the most trusted practical security technique for digital data in computer and communication systems. Conventional cryptosystem, such as DES, is not suitable for image encryption because of the special storage characteristics of an image. Due to the tight relationship between chaos and cryptography, chaotic systems have been widely used in image encryption to realize diffusion and confusion in a good cipher.

The main aim of digital image scrambling 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.

This paper proposed an alternative to the symmetric key encryption algorithm for securing images based on chaos. Cat map and modified cat map algorithm are used to encrypt and decrypt the digital images. Then, the system compares and analyzes the processing time of these algorithms.

This paper is organized as follows: The first section is the introduction of the system. Section 2 explains related work for the system. Section 3 explains chaotic maps used in this paper. Section 4 and 5 describe the implementation and design of the system. Experimental result of the system is explained in section 6 and the paper is concluded in section 7.

2. Related work

Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data. However, Conventional cryptosystem is not suitable for image encryption because of the special storage characteristics of an image.

The idea of using of chaos for encryption can be traced to the classical Shannon's paper [1]. Chaos has many characteristics such as sensitive dependence on initial conditions and parameters, mixing, randomness in the time domain, broadband power spectrum and ergodicity.

So, chaotic systems are widely used in communications, optimization, control and image processing etc. In 1989, Matthews used discrete chaotic dynamical system in cryptography firstly [6]. He derived a one-dimension chaotic map. Jiri Fridrich presented an encryption algorithm that adapted certain invertible chaotic two dimensional maps to create new symmetric block encryption schemes at [2]. Jui-Cheng Yen et al. [3] proposed a new chaotic key-based design for image encryption and its VLSI architecture. Sobhy [4] presented an algorithm for encrypting texts and images. Mazleena Salleh et al [5] give an alternative chaotic image encryption based on Baker's map.

3. Chaotic system

Chaos is a dynamical system that is extremely sensitive to its initial conditions. It is a deterministic nonlinear system that has random-like behaviors. The property that stability may depend on initial conditions is characteristic only for nonlinear systems. Discrete chaotic dynamic systems (i.e., maps) are used in cryptography. This sensitivity property is commonly applied to cryptosystems. If a parameter that describes a linear is changed, then the quantitative behavior of the system will change, but the quantitative nature of the behavior remains the same.

3.1. Characteristics of chaotic system

Chaotic systems are very suitable for data message encryption because they have several good properties, for example

- Chaotic motion is neither periodic nor convergent, and the domain is limited.
- The outputs of chaotic systems are very irregular, similar to the random noise.
- Chaotic systems are extremely sensitive to their conditions.
- The long term movement trace of systems cannot be forecasted.

3.2. Logistic chaotic map

The logistic map is very simple mathematical system and a sort of dynamical system which involves no derivatives and no integrals. But this function exhibits the universal features of the behavior, such as the period-doubling leading to chaos. It is defined as follows.

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

where μ and x_0 are initial conditions and secret keys. The value of μ is greater than 3.5699456 and is less than and equal to 4. The value of X_0 is between 0 and 1. This map is used to generate diffusion key.

3.3. Cat chaotic map

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

$$x_{n+1} = (x_n + a y_n) \bmod N$$
$$y_{n+1} = (b x_n + y_n (ab + 1)) \bmod N \quad (2)$$

where (x_n, y_n) are pixels position in an N x N image; (x_{n+1}, y_{n+1}) is the transformed position after cat map; both "a" and "b" are the system parameters and must be the plus integers. 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). Image position can be scrambled by using cat map.

3.4. Modified cat chaotic map

In chaotic Cat map, pixel of position (0, 0) keeps unchanged after any number of iterations. If $(x_0, y_0) = (0, 0)$, then $(x_0^n, y_0^n) = (0,0)$ after n numbers of chaotic iterations. (0, 0) is the first pixel' position in normal scan mode, which cannot be permuted by Cat map. It is a threat to the whole cryptosystem. In order to avoid it, modified cat map can be used. After the iteration of chaotic map, a random-couple (k_x, k_y) is generated, which represents the position of a randomly selected pixel in the square image. Then whole image shifts in horizontal and vertical directions by k_x and k_y, respectively. That is the left-top pixel shifts from (0, 0) to (k_x, k_y). The random shift process changes the normal scan mode into a random one. The map is defined as follow:

$$x_{n+1} = (x_n + k_x + (a(y_n + k_y))) \bmod M$$
$$y_{n+1} = (b(x_n + k_x) + (y_n + k_y)(ab + 1)) \bmod N \quad (3)$$

where (x_n, y_n) are pixels position in an M x N image; (x_{n+1}, y_{n+1}) is the transformed position after cat map; k_x *and* k_y are the random scan couple keys to change the pixel position (0, 0); both "a" and "b" are the system parameters and must be the plus integers. Image position can be scrambled by using modified cat map.

4. Chaos-based image cryptosystem

The structure of chaos-based image encryption system is shown in figure 1. There are two iterative stages in this cryptosystem: confusion and diffusion. Confusion permutes the pixels in the image, without

changing its value. Confusion process is called permutation. To confuse the pixels, new positions must be calculated by using chaotic maps. Diffusion is modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image. Diffusion process is called substitution.

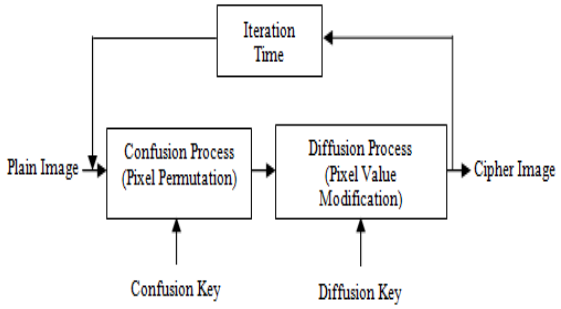

Figure 1. Chaos-based image encryption scheme

In this paper, there are used two image encryption algorithms. They are image encryption based on cat map and image encryption based on modified cat map.

4.1. Image encryption based on chaotic cat map

This image encryption consists of two parts: confusion and diffusion.

4.1.1. Confusion process. The original coordinates (x_n, y_n) can be translated into the new coordinate (x_{n+1}, y_{n+1}) by using the following formulas.

$$x_{n+1} = (x_n + a y_n) \bmod N$$
$$y_{n+1} = (b x_n + y_n (ab + 1)) \bmod N \quad (4)$$

where, *a* and *b* are control parameters and secret keys. Confusion process for decryption is as follows:

$$y_{n+1} = (y_n - b x_n) \bmod N$$
$$x_{n+1} = (x_n - a y_n) \bmod N \quad (5)$$

4.1.2. Diffusion process. The diffusion process is encrypting pixels values with XOR function. In order to diffuse the pixel value P of the coordinates P(x, y) to get a new pixel value P', the following formulas can be used.

$$P' = P \wedge f(x_{n+1}, y_{n+1}, k) \quad (6)$$

where, k is the iteration time and secret key and

$$f(x_{n+1}, y_{n+1}, k) = (x_{n+1} * y_{n+1} + k) \bmod N \quad (7)$$

This diffusion formula used in both encryption and decryption process.

4.2. Image encryption based on modified chaotic cat map

This image encryption consists of three parts: key generation, confusion and diffusion.

4.2.1. Key generation. The proposed scheme, variable key size can be used depending on the security requirements of the applications. Logistic map is used to generate the diffusion key as follow:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (8)$$

4.2.2. Confusion process. To confuse the key stream and pixels for a 24-bit color $M \times N$ image, the following formula is used.

$$x_{n+1} = (x_n + k_x + (a(y_n + k_y))) \bmod (M \times 3)$$
$$y_{n+1} = (b(x_n + k_x) + (y_n + k_y)(ab + 1)) \bmod N \quad (9)$$

where, *a* and *b* are control parameters and secret keys respectively. Decryption procedure for confusion is as follows:

$$y_{n+1} = (y_n - b x_n - k_y) \bmod N$$
$$x_{n+1} = (x_n - k_x - a k_y - a y_n) \bmod (M \times 3) \quad (10)$$

4.2.3. Diffusion process. To diffuse the pixels, the following formula is used.

$$C_i = P_i \oplus C_{-1} \oplus K_i \quad (11)$$

where, C_i is i^{th} cipher pixel, P_i is i^{th} plain pixel, C_{-1} is the seed value of the diffusion function, and K_i is i^{th} diffusion key generated from Logistic map.

Decryption procedure for diffusion is as follow:

$$P_i = C_i \oplus C_{-1} \oplus K_i \quad (12)$$

5. Propose system

In this system, the user opens input image file to encrypt or decrypt. Then, the user chooses Cat map or Modified Cat Map algorithm for encryption and decryption process and also enters the input key. The system displays the output of the plaintext and ciphertext and then shows the comparison of the encryption and decryption time output. The overall design of the system is shown in figure 2.

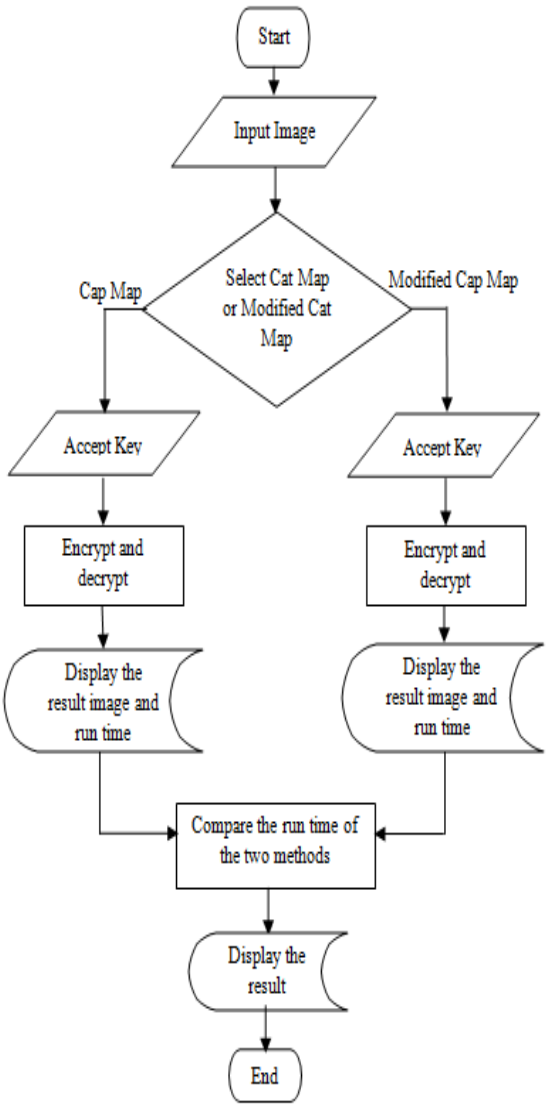

Figure 2. System design

6. Experimental results

The file type of the following flower image is jpeg image and 223×167 dimension with true color. Image size is 6.46 KB and image resolution is 96×96 dpi. This original image is encrypted and decrypted with cat map and modified cat map algorithm. The experimental results of this image after encryption and decryption are shown in figure 4.

Figure 3. Original image

(a) Encrypted image (b) Decrypted image

Figure 4. Encryptede and decrypted images using cat map and modified cat map

The histograms of plain image and cipher images are shown in Figure 5 and 6. Histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histogram of the original image in figure 5. We have calculated and analyzed the histograms of the encrypted image as well as its original image that have widely different content.

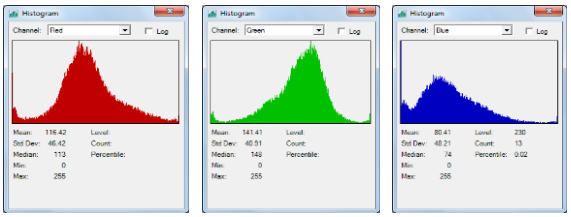

Figure 5. Histogram of original image

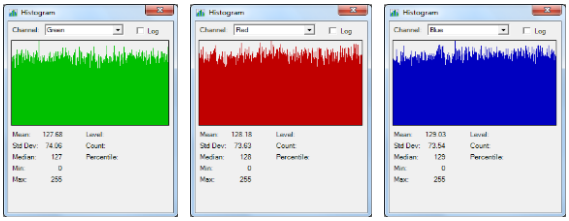

Figure 6. Histogram of encrypted image

In addition, the various file type and file size of images are encrypted and decrypted with Cat map and Modified Cat map algorithms. The experimental results of encryption and decryption time between two algorithms are shown in Table 1, 2 and figure 5 and 6. The encryption and decryption time of Cat Map algorithm is faster than Modified Cat map algorithm. Table 1 shows the results of comparing encryption time on various file types and sizes using two algorithms. Table 2 shows the decryption time. Figure 5 and figure 6 show the results by charts.

Table 1. Comparison of encryption time between different file size and file type

File Type	File Size	Cat Map (milisec)	Modified Cat Map (milisec)
JPEG	89*95	51.031	748.134
PNG	167*167	79.025	995.465
TIFF	239*155	97.542	1173.565
GIF	256*256	126.003	1430.422
BMP	300*295	196.402	1688.533

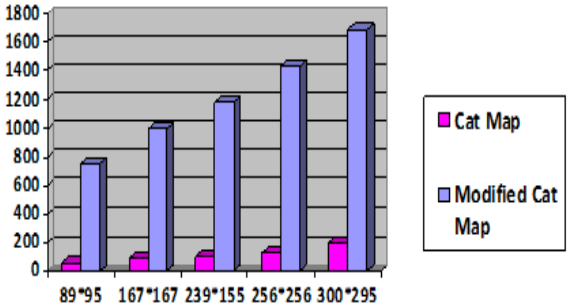

Figure 7. Comparison of encryption time with chart

Table 2. Comparison of decryption time between different file size and file type

File Type	File Size	Cat Map (milisec)	Modified Cat Map (milisec)
JPEG	89*95	49.501	727.509
PNG	167*167	76.812	967.431
TIFF	239*155	94.445	1140.359
GIF	256*256	122.507	1390.401
BMP	300*29	190.076	1641.875

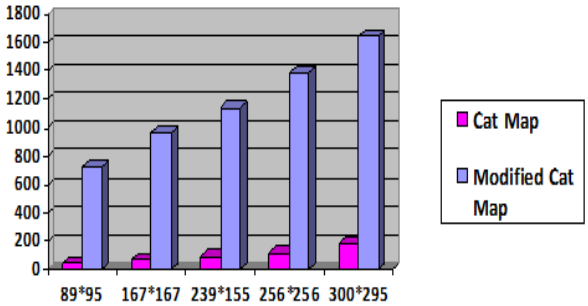

Figure 8. Comparison of decryption time with chart

7. Conclusion

In this paper, we present the two encryption algorithms: Cat map and Modified Cat map encryption algorithm. This system can encrypt any type of image file formats such as jpg, gif, bmp, tiff, png and etc. This system can encrypt the gray images and color images. When the performance of the two algorithms is compared, the encryption and decryption time of Cat map is faster than the encryption and decryption time of Modified Cat map. This paper are compared the runtime of the Cat map and Modified Cat map algorithm. So, this system can be extended to test the security analysis which algorithm is more secure.

8. References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems", *The Bell System Technical Journa*l, 1949, vol. 28, no. 4, pp.656-715.

[2] Jiri Fridrish, "Image Encryption Based on Chaotic Maps", *Processing of IEEE Conference On Systems, Man, and Cybernetics*, pp.1105-1110, 1997

[3] Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp.IV-49-IV-52, May. 2000.

[4] M.I.Sobhy, and A.R.Shehata, "Chaotic Algorithms for Data Encryption", IEEE Proceeding of ICASSP 2001, Vol 2, pp.997-1000, May. 2001.

[5] Mazleena Sallen, Subariah Ibrahim, and Ismail Fauzi Isnin, "Enhanced Chaotic Image Encryption Algorithm Based on Vaker's Map", IEEE Proceeding of ISCAS 2003, Vol 2, pp. II-508-II511, May. 2003.

[6] Zhang Han, Wang Xiufeng, et al, "A new image encryption algorithm based on chaos system [A]". *International conference on robotic, intelligent systems and signals processing*, Changsha, *China*, 2003:778-782.