Secure Image Encryption based on Baker Chaos Function

Saw Mya Nandar, Soe Soe Aye
University of Computer Studies, Kyainge Tong
madar008@gmail.com; soesoeaye74@gmail.com

Abstract

Image information is important, especially in the field of military. When those images are transmitted over the communication channel, it needs the privacy. There are a lot of image encryption algorithms. Because of storing large size of pixels, most of the functions are not appropriate for the image encryption.

This paper presents an alternative symmetric-key encryption algorithm for securing images, namely Secure Image Encryption based on chaos. Generally, it comprises of three main components: (1) horizontal-vertical transformation function (HVT); (2) shift function (S), and (3) gray scale function (GS). HVT function is based on a two-dimensional chaotic map that utilized Baker's map algorithm. GS function extends the algorithm to three-dimension, whereby, the third dimension refers to the level of the grayscale of a pixel. This secure image encryption applies to encrypt military images, such as Maps, Buildings, Army forces, etc.

1. Introduction

Image information has become important because of its vitality and visualization. Some image data transmitted are characterized in term of privacy, integrity and authenticity through the public network. Images transferring 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.

Conventional cryptosystem, such as DES, is not suitable for image encryption because of the special storage characteristics of an image. The common method of protecting the digital documents is to scramble the content so that true message of the documents is unknown. 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. This paper is based on the characteristics of chaos, which are sensitivity of parameters, sensitivity of initial points, and randomness of sequences obtained by iterating a chaotic map. It presents an image encryption algorithm using chaos mapping through simple permutation of the pixels location as well as the transformation of the gray scale value through boolean XOR operation.

This paper is organized as follows. Section 1 is the introduction, section 2 is related work. Cryptology is described in section 3. In section 4, digital image encryption and chaos based encryption are presented. Section 5 illustrates Baker map encryption. Section 6 is the proposed system design and section 7 is the system implementation and sample case study for Baker map algorithm. Section 8 is the conclusion and future work of the system.

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.

The idea of using chaos in data encryption has been introduced and discussed in, for instance, [Fridrich, 1997, 1998; Li et al., 2002; Mao & Chen, 2004, Chen et al., 2004; Scharinger, 1998]. It has been shown that chaos-based algorithms have advantages in applications of bulk data encryption, which make use of two special features of chaotic maps - the sensitivity to initial conditions and parameters and the mixing property (topological transitivity or ergodicity), [Fridrich, 1998; Kocarev, 2001; Kocarev & Jakimovski, 2001; Masuda & Aihara, 2002]. Sensitivity to initial conditions means that when a chaotic map is iteratively applied to two extremely close initial points, the iterates quickly diverge, and become uncorrelated in the long term. This in image encryption, since two adjacent pixels in an image are highly correlated but while using a chaotic map, they will be uncorrelated after several rounds of iteration. Sensitivity to parameters causes

the properties of the map to change quickly when slightly perturbing the parameters on which the map depends. This property of the parameters is just like that of a cipher key, therefore, in a chaotic based encryption scheme, those parameters are often used as keys. Mixing is the tendency of the system to quickly blend small portions of the state space into an intricate network of filaments. This character can also make correlated information become scattered all over the phase space. These characteristics form a basis of chaotic data encryption. Two-dimensional baker map is used to compose a fast and secure image encryption scheme.

3. Cryptography

Cryptography can be defined as the practice and study of hiding information. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. 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.

Encryptin is the process of converting ordinary information (plaintext) into unintelligible gibberish. Decryption is the reverse, moving from unintelligible ciphertext to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and a key. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

There are several ways of classifying cryptographic algorithms. They will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms are shown in Figure 1.

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information [2].

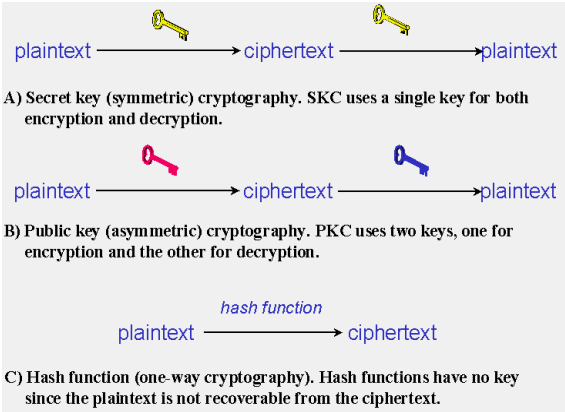

Figure 1. Three Types of Cryptography

Figure 1 presents three types of cryptography; symmetric cryptography (secret key cryptography, where encryption and decryption use same key), asymmetric cryptography (public key cryptography, uses two keys) and hash function.

4. Digital Image Encryption

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. This paper presents a scheme of digital image scrambling based on the baker chaotic mapping. Firstly we use a cat chaotic mapping 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. This is a new diffusion technique to uniform the statistical characteristics of the encrypted digital image. This method is easy to realize, has satisfied scrambling effect, and can be used as pretreatment for digital image hiding and disguising.

The approach adopts a divide-and-conquer, pattern-growth principle as follows: Sequence databases are recursively projected into a set of smaller projected databases based on the current sequential pattern(s), and sequential patterns are grown in each projected databases by exploring only locally frequent fragments.

4.1 Chaotic Map

Chaotic maps present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security. 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.

The Chaotic presented Confusion and diffusion in the sense of cryptography. Confusion stage permutes the pixels in the image, without changing its value[1]. In Diffusion stage, pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels. Chaotic mapping can be applied to image encryption, because it has the sensitivity of initial value and the randomness. With the properties of sensitivity to initial conditions and control parameters, pseudo-randomness and ergodicity, chaotic maps have been widely used in data encryption.

5. Baker Map

In dynamical systems theory, the baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one-another, and compressed.

The baker's map can be understood as the bilateral shift operator of a bi-infinite two-state lattice model. The baker's map is topologically conjugate to the horseshoe map. In physics, a chain of coupled baker's maps can be used to model deterministic diffusion. There are two alternative definitions of the baker's map which are in common use. One definition folds over or rotates one of the sliced halves before joining it (similar to the horseshoe map) and the other does not. Note that baker does not refer to a person so baker should not be capitalized.

Figure 2 is the stretch and slack of generalized baker map with k blocks. Baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one-another, and compressed. The Baker map, B, is described with the following formulas

$$B(x, y) = (2x, y/2) \text{ when } 0 \leq x \leq ½$$

$$B(x, y) = (2x – 1, y/2 + 1/2) \text{ when } 1/2 \leq 1$$

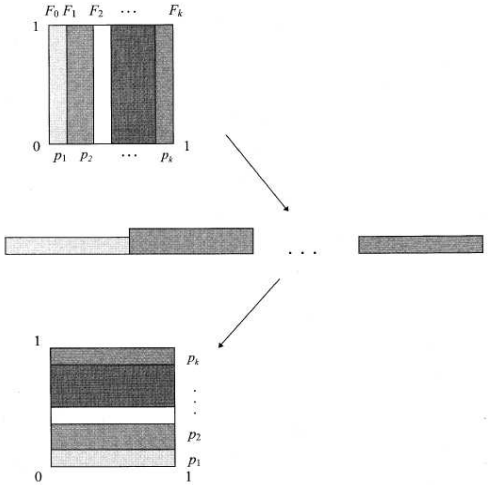

Figure 2: Strech and Slack of generalized baker map

5.1. Key Generation of Baker Map

Since an image is defined on a lattice of finitely many points (pixels), a correspondingly discretized form of the basic map needs to be derived. In particular, the discretized map is required to assign a pixel to another pixel in a bijective manner. Baker map will be denoted B(n1, ..., nk), where the sequence of k integers, n1, ..., nk, is chosen such that each integer ni divides N, and n1 + ... + nk = N.
Denoting Ni = n1 + ...+ ni, the pixel (r, s), with Ni ≤ r < Ni + ni, and 0 ≤ s < N.

6. Proposed System

In this paper, a baker chaotic mapping is to disorder the pixel coordinates of the digital image. This paper presents two dimensional chaotic maps on a square to create a new symmetric block encryption process. A chaotic map is first generalized by introducing parameters and then discretized to a finite square lattice of points which represent pixels or some other data items. Although the discretized map is a permutation and thus cannot be chaotic, it shares certain properties with its continuous counterpart as long as the number of iterations remains small. The discretized map is further extended to three dimensions and composed with a simple diffusion mechanism. As a result, a symmetric block product encryption scheme is obtained. To encrypt an N x N image, the ciphering map is iteratively applied to the image. The construction of the cipher and its security is explained with the two-dimensional Baker map.

This paper presents secured image encryption, based on a two-dimensional chaotic Baker’s mapping.Secure Image Encryption consists of three main components:

- horizontal-vertical transformation function - based on two-dimensional chaotic map using Baker's map algorithm
- shift function
- gray scale function - extends the algorithm to three dimension

6.1. Process Flow of the System

Process flow of the system is as follows. Chaos Map algorithms depends on the initial values or system input. 256 bit key is separated into key segments for the encryption process. Encryption process is performed based on Kr times. Image is partitioned into square blocks, and padded to cover the entire image. It consists of three steps as explained above in the proposed system. Each block is encrypted according to those steps, and cipher blocks then combined to get the cipher image.

The inputs to the system are the image to be encrypted and the key value. Image of size m x n, where m and n represents row and column of the image respectively. f(x, y) = gray scale value of a pixel at position x and y where $0 < x \leq m - 1$ and $0 < y \leq n - 1$. Before proceeding to the encryption process, the image will undergo an initial setup. Padding pixels are appended to the image so that the image can be partitioned into square blocks of size, b × b. The encryption key K (Kseg , Kr) comprises of two parameters and they are:
Size of segments in the block denoted by Kseg = {s1, s2, … , sm} where s1 + s2 + … + sm = b. Number of iterations denoted by Kr. The number of iterations basically determines the level of security. Obviously a higher number of iterations increase the computational time but it enhances the security of the cipher image.

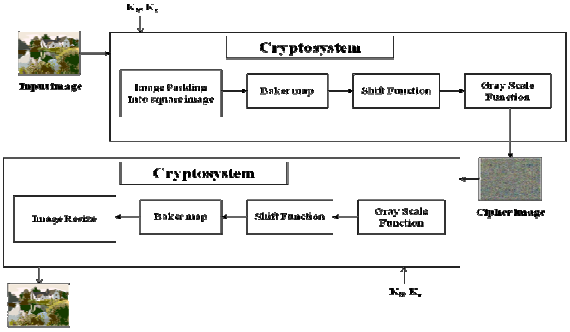

Figure 3: Overview Process flow of the System

Overview process flow of the system is shown in Figure 3. There is input image with segmentation key and looping key. First input image is padded to get the square block. Then baker map function and shift function are applied to permute the pixels and Gray-scale function is applied to encrypt the pixels. Reversed processes are performed to decrypt the image. Kseg is used in every step of Baker map function and Kr is used to iterate the Baker map process.

7. System Implementation

This paper presents an implementation of image encryption process by Java programming language. Jdk 1.5 is used to develop the system. Unlike other encryption algorithms, key is generated based on the dimensions of the image rather than user provides the key. Summation of keys generated by the baker map is the length of the image. Each key is the divisor of the length.

7.1. Encryption Process

The encryption process comprises of three main functions:
Function 1: Baker's transformation

$$B_{(n_1,\ldots,n_k)}(r,\, s) = \left(\frac{N}{n_i}(r - N_i) + s \mod \frac{N}{n_i},\right.$$
$$\left.\frac{n_i}{N}\left(s - s \mod \frac{N}{n_i}\right) + N_i\right)$$

(xj, yj) and (xj+1, yj+1) are the j-th and the j+1-th states, respectively. The key is K = [k1, k2, ..., kt] that satisfies the condition proposed in above equation.
Function 2: Nonlinear feedback substitution
This function changes the gray scale level of the pixels by performing a simple bitwise nonlinear feedback operation, that is f' (xl +1, yk) = f(xl, yk) XOR f(xl +1, yk) for k = 0 – (b-1) and l = 0 - (b-1).
Function 3: Shifting pixels in the rows
To further randomize the transposition of the pixels, pixels in each row will be rotated to the left with 0, 1, 2, 3 or 5 shifts depending on the value of modulus (row number).

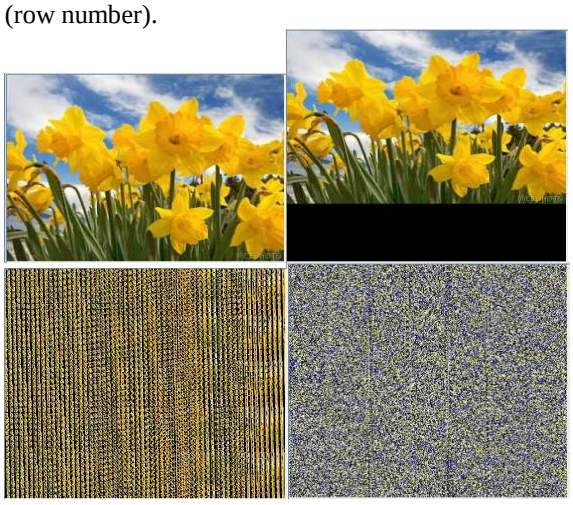

Figure 4: Encryption Process Flow of System; original input image, Padding Image, processing of function-1 and function-2, processing of function-3

Figure 4 presents the encryption process flow of the system, where the first one is the original image, the second one is the image after padding to get the square block, the next one is the image after baker map is applied and the final one is the encrypted image.

7.2. Results and Discussions

This paper presents image encryption with Baker Chaotic Map algorithm. The characteristics of the chaotic maps have attracted the attention of cryptographers to develop new encryption algorithms. As these chaotic maps have many fundamental properties such as ergodicity, mixing property and sensitivity to initial condition, system parameter and which can be considered analogous to some cryptographic properties of ideal ciphers such as confusion, diffusion, balance and avalanche property etc. With Chaotic based system, the following advantages can be obtained:

- The encryption system is computationally secure. It requires an extremely long computation time to break. Unauthorized users should not be able to read privileged images.
- Encryption and decryption process is fast enough not to degrade system performance. The algorithms for encryption and decryption must be simple enough to be done by users with a personal computer.
- The security mechanism is flexible.

This system is tested with P IV computer with Intel (R) Pentium (R) Dual CPU 2.20 GHz and 1.99 GB of RAM. According to the experimental results, this system is very effective to uniform the statistical characteristics of the encrypted graph, and the efficiency of this method is very high. The key is main the controlling parameter and encryption parameter for the cat map. Obviously, the more times we encrypt, the larger the key space can be. For example, if we do the encryption only once, for a graph of 64 × 64, the key space can only be 212. However, if we do the encryption 4 times, the key space for the system can be 216×4 . Furthermore, the key space is also dependent on the size of the graph, i.e. the larger the graph is, the larger the key space is.

8. Conclusion

This paper presents an image encryption scheme for image based on Baker chaotic map, which can overcome the problem of high security. This algorithm highly depends on the initial parameters and there are a lot of initial parameters. Therefore unauthorized users can not decrypt correctly using cipher text-only attack even if they gain the secret image illegally; using known plain-text attack, they still can not decrypt correctly without key even if they know the algorithm. The image can be decrypted only when they know both the key and the algorithm. This paper can be further extended into the encryption of image streams.

9. References

[1] Alvarez, Gonzalo and Li Shujun, "Breaking an encryption scheme based on chaotic Baker map", submitted to Elsevier Science, 21 February 2006

[2] Fridrich, J. 1998. “Symmetric Ciphers Based on Two-Dimensional Chaotic Maps”. Int. J. Bifurcation and Chaos. 8(6).

[3] Fridrich, J. 1997. “Image Encryption Based on Chaotic Maps”. Proc. IEEE Conf. on Systems, Man, and Cybernetics. 1105-1110.

[4] Habutsu, T., et al. 1991. “A Secret Key Cryptosystem by Iterating a Chaotic Map”. Proceedings of Eurocrypt ‘9: 127-140.

[5] Li, S. et. al. 2002. “Chaotic encryption scheme for real-time digital video”. Proc.of SPI,E Vol. 4666: 149-160, Real-Time Imaging VI, Nasser Kehtarnavaz; Ed.

[6] Li, S., X. Mou, and Y. Cai. 2001. “Improving Security of a Chaotic Encryption, Approach”. Physics Letters A. 290(3-4): 127-133.

[7] Wong, Kwok-Wo; Kwok, Bernie Sin-Hung and Law, Wing-Shing, "A Fast Image Encryption Scheme based on Chaotic Standard Map", Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, HONG KONG, 2007

[8] Yen, J.C and J. I. Guo. 1998. “A New Chaotic Image Encryption Algorithm’’. Proceedings of National Symposium on Telecommunications. 358-362.

[9] Yen, J. C. and J. I. Guo. 2000. “Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realization”. IEEE Proceeding Vis. Image Signal Process. 147(2).