Image encryption using chaotic maps

Article · February 2015

CITATION
1

READS
3,014

2 authors:

Ashutosh Gupta
M.J.P. Rohilkhand University
47 PUBLICATIONS **141** CITATIONS
SEE PROFILE

Ashwani Gupta
M.J.P. Rohilkhand University
4 PUBLICATIONS **128** CITATIONS
SEE PROFILE

IMAGE ENCRYPTION USING CHAOTIC MAPS

Ashwani Gupta[1], Ashutosh Gupta[1]

[1,2]CS IT Department, Faculty of Engineering & Technology, MJP Rohilkhand University,(India)

ABSTRACT

The cryptographic techniques based on chaos theory reveal some new and effective directions to develop secure image encryption schemes. In this paper, we present an image encryption using 1 D logistic map. The proposed scheme is based on key stream generator for confusion process. The confusion process is initiated by a secret key of 256 bits which is itself generated by a logistic map. To make the cipher more dynamic against any attack, the secret key is modified after encrypting each block of the image. The experimental results show that the proposed method provides an efficient and secure way for real-time image encryption and transmission.

Keywords: Chaotic Maps, Image Cryptography, Key Generation.

I. INTRODUCTION

Development of society leads towards the importance of data used, so huge amounts of digital visual data is stored on various media and exchange over various sorts of networks now a day .Image have enough importance in our life, so it used in digital form and increasing importance due to improvements of performance in computer speed, media storage and network bandwidth. So the vulnerability of this form of information to be attacked such as modification and fabrication is higher as compared to paper based image.

Some sorts of techniques are required to maintain privacy, integrity and authenticity. Encryption [1] is a good way to ensure about security features. It is used to protect data in transit, for transfer via networks (i.e. the Internet, Palmtops, Cellular devices). Encryption algorithm such as DES, IDEA and RC5 that are computationally complex and has a low level efficiency with the large volume image data [2, 3]. The most common primitives for image encryption are classified into three major types: Positive permutation [4, 5], value transformation [6, 7] and combined form [8]. Chaos encryption is majorly employed to achieve the first two primitives for a long time.

Chaotic maps often occur in the study of dynamic nonlinear systems. Mathematical equations rules its behavior and slight change in initial position leads to a significant different outcome, and appears in random and disorderly, but actually they follows some of the patterns[9]. Chaotic output signals, which presents random statistical properties are used for both confusion and diffusion operation in a cryptosystem.

In this paper, we propose a chaotic image encryption scheme and a key generator. The generated key can be used as an initial condition for 1D logistic map. The plain image is divided into fixed size block and each block is encrypted with the different key obtained through 1D logistic map. The size of block is considered as 8 bits.

The experimental results using the image database shows the effectiveness and strength of the proposed chaotic image encryption for various images. At last, security analysis shows that the proposed scheme is able to generate statistically random encrypted images.

The reminder of the paper is organized as follows: In section 2, the review on existing encryption schemes are briefly explained followed by proposed design of the encryption and decryption system in section 3. Section 4

illustrates the simulation results and security analysis of the encrypted images and finally section 5 concludes the work.

The introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

II. RELATED WORK

The In [10, 11] Fridrich pointed out that a chaos based encryption scheme should be built up of stages mainly: chaotic confusion and pixel diffusion. Confusion permutes the pixels of a plain image with a 2D chaotic map followed by diffusion, alternates the intensity of each pixel. Indeed it was the first approach for image encryption based on addition and subtraction performed on square images.

In [12], Mazleena et al presented a cryptosystem for variable sized images based on Baker's map. The proposed algorithm also supports two modes of operation namely EBC and CBC and performed XOR operation with a password, and stretching and stacking of the square images is performed. A nonlinear and pixel shifting performed to get encrypted image.

Aloka Sinha and Kehar Singh [13] have proposed a technique to encrypt an image for transmission. The digital signature of original image is processed with its encoded form. The encoding of the image is done using Bose-Chaudhuri Hochquenghem (BCH) code [14]. At the receiver end, after the decryption of the image, the digital signature is used to verify the authenticity of the image.

Yu Li et al [15] pointed a new approach based on one dimensional cellular automata. Original image and secret key is divided into two parts, obtained subsections of encrypted image are assembled again to find final encrypted image. Key space is based on secret image generated by key stream generator and inverse rules of toggle cellular automata.

Gao H et al [16] presented a nonlinear chaotic algorithm which used power functions and tangent functions. It used one-time-one password system. This nonlinear chaotic algorithm map behaves as chaotic maps on certain control parameters [17].

Abid Awad and Abdelhakim Saadane[18] presented an encryption scheme based on piece wise linear chaotic map (PWLCM) and perturbed PWLCM with good inherent properties.

Sayadzade SM [19] presented an algorithm based on SHA-512[1]. The idea of the algorithm is to use one half of image data for encryption, other half of image reciprocally. The first does preprocessing operation to shuffle one half of the image, second uses hash functions to generate a random number mask. The mask is than XORed with another part of image which is to be encrypted.

III. PROPOSED DESIGN

In this section, we discuss the operation of our algorithm in detail. Let $I(x, y)$ represents the gray scale value of a pixel at position x and y respectively where $0 <= x <= M-1$, $0 <= y <= N-1$ and M x N refers to height and width of an image. The image is partitioned into 8 bit block i.e. each pixel is processed independently. The description of encryption and decryption process is explained in the next section. Like encryption, the decryption process is just a reverse of encryption using the decryption key. In brief, the encryption process can be written as C = E(P, K), and the decryption process as P = D(C, K).

3.1 Key Generation

The proposed algorithm uses an external secret key of 256-bit long. The seed secret key is consist of eight fields: K_1 K_2 K_3 K_4 K_5 K_6 K_7 K_8. The sub keys K_1 and K_8 are derived through 1 D logistic map. Each sub key is 32 bits long thus forming a seed secret key of 256 bits long.

Logistic map is considered as a simplest chaos functions that have been studied recently for cryptography. The logistic chaotic map is expressed as:

$$X_{n+1} = rX_n (1 - X_n) \quad (1)$$

Where X_n takes values in the interval (0,1). It is one of the simplest models that present chaotic behavior [10]. When parameter $r \in [3.57, 4]$, it becomes a chaotic system and can be used for image encryption. The logistic map is iterated 1000 times for each sub key K_i and each X_{n+1} is mapped to domain $(0, 2^{32} - 1)$. The eight different values of X_{n+1} are assigned to each sub key K_i, $1 <= i <= 8$.

3.2 Pixel Modification

The confusion process sequentially reads a gray scale value p_i from the plain image and each pixel undergoes into encryption to produce its corresponding cipher c_i according to the expression.

$$c_i = [p_i + c_{k-1}] \bmod 256 \quad (2)$$

where c_{k-1} is computed as:

$$c_{k-1} = \left(\left(\left(\sum_{i=1}^{K_8} K_i \oplus K1 \right) \oplus K3 \right) \oplus K5 \right) \quad (3)$$

Each pixel is then encrypted to produce corresponding cipher image pixel c_i using the 1D logistic map.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

Simulation results and performance analyses of the proposed image encryption scheme are provided in this section. Some security analysis has been done on the proposed scheme, including the most important ones like key space analysis, key sensitivity test and statistical analysis. The results show the efficiency of the proposed scheme. .

4.1.Key Space Analysis

The encryption key of the proposed scheme is composed of eight parts which includes K_1 K_2 K_3 K_4 K_5 K_6 K_7 K_8 where all sub keys consist of 32 bits each. The generated encryption key used in the proposed scheme is consisting of 32*8 = 256 bit length. This makes the cipher key space comparable to or better than existing encryption schemes and standards.

4.2.Key Sensitivity Test

In the proposed scheme, a 1D logistic map is used which is sensitive on the initial condition and thus makes it more immune to key sensitivity.

Assume that a 32 character (256 bits long) cipher key is used. The image of cameraman of size 512 x 512, gray-scale (0-255) as the original image (plain image) and the secret key of "12345678901234567890123456789012" is used for encryption. For key sensitivity tests, following steps are performed:

4.2.1. An original image in Figure 1(a) is encrypted by using the secret key K^1 = "12345678901234567890123456789012" and the encrypted image **A** is shown in Figure 1(b).

4.2.2. The same original image is encrypted by making the slight modification in the secret key i.e. K^2 = "32345678901234567890123456789012" (the MSB is changed in the secret key) and the resultant encrypted image **B** is shown in Figure 1(c).

4.2.3. The difference image **C** between encrypted images **A** and **B** is shown in Figure 1(d). The Figure 1 shows the key sensitivity of the proposed algorithm with respect to encryption, where K^1 and K^2 differ in one bit. The image A encrypted by the key K^1 = "12345678901234567890123456789012" has 99% of difference from the image encrypted by the key K^2 = "32345678901234567890123456789012" in terms of intensity values, even though there is only one bit difference in K^1 and K^2.

4.3. Statistical Analysis

The statistical analysis is performed by calculating the histograms and the correlations of two adjacent pixels in the plaintext image and ciphertext image.

4.3.1. Histograms Analysis

The histograms of the several encrypted images as well as its original images are analyzed. Figure 2 shows some ciphertext histograms from the encrypted images. From these results, it is clear that although some plaintext images contains large spikes, the ciphertext image histograms is more uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image.

4.3.2. Correlation Coefficient Analysis

The procedure to evaluate the correlation coefficients is determined as: First, randomly select 1024 pairs of vertically, horizontally and diagonally adjacent pixels from an image. Then, calculate their correlation coefficient using the following equation:

$$\rho(x,y)= \sum_{j=1}^{N}[(x_i - E(x))(y_i - E(y))] \Big/ \sqrt{\sum_{j=1}^{N}[(x_i - E(x))]^2}\sqrt{\sum_{j=1}^{N}[(y_i - E(y))]^2} \quad (4)$$

Where E(x) =mean (x_i) and x, y are gray values of two adjacent pixels in the image.

The correlation coefficients in plaintext images and ciphertext images in all three directions are listed in TABLE 1 and TABLE 2 respectively. The correlation coefficient value shows that the two adjacent pixels in the plaintext images are highly correlated to each other, whereas the values obtained for ciphertext images are closer to 0. This shows that the proposed scheme highly de-correlate the adjacent pixels in ciphertext images.

Table 1: Correlation coefficient of Two Adjacent Pixels in Plain-Images

Test Images	Correlation Coefficient		
	Vertical	Horizontal	Diagonal
Lena	0.9806	0.9762	0.9611
Cameraman	0.9841	0.9632	0.9710

Table 2: Correlation Coefficient of Two Adjacent Pixels in Cipher-Images

Test Images	Correlation Coefficient		
	Vertical	Horizontal	Diagonal
Lena	-0.0261	0.00671	0.00412
Cameraman	-0.2223	0.00411	0.0332

V. CONCLUSION

In this paper, an image encryption using chaotic map is presented which is based on 1D logistic maps. The system is based on key generator with 256 bit secret key and an encryption process. The initial condition for 1D logistic map is derived using the external secret key by performing some external operation. It is establish that such a design of encryption can improve the randomness. A detailed key analysis and statistical analysis is given. From the experimental results, it is established that it maintains satisfactory security measures in terms of security.

REFERENCES

[1] Stallings W, Cryptography and Network Security: Principles and Practices (London,Pearson Education; 2004)

[2] G Chen, Y Mao and C K Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitions & Fractals,21(3),749-761, 2004.

[3] chiaraluce F, Ciecarelli L, et al, A new chaotic algorithm for video encryption, IEEE Trans Consum Electron, 48, 838-843, 2002.

[4] DingWei, QiDongxu, "Digital image transform, information hiding and camouflage technique", Journal of Computers, 21, 838-843, 1998.

[5] A Shamir, How to share a secret, Communications of ACM, Vol. 22,612-613, 1979.

[6] M Noar, Visual cryptography, proceeding of Eurocrypt, 441-449, 1994.

[7] C Zhenfu, A threshold key escrow based on public key cryptosystem, Science in China (Series A),44, 441-448, 2001.

[8] C E Shannon, Communication theory of secrecy systems, Bell System Technical Journal, 28,656-715,1994.

[9] Chaos Mathematics, December 2001, Citing Internet sources URL http://library.thinkquest.org/3120/text/math.htm.

[10] J Fridrich, Symmetric Ciphers Based on Two-Dimensional Chaotic Maps, International J. Bifurcation and Chaos, 8(6), 1998.

[11] J Fridrich, Image Encryption Based on Chaotic Maps, Proceeding IEEE Conference on Systems, Man, and Cybernetics,1105-1110, 1997.

[12] M Salleh, S Ibrahim, I F Isnin, Enhanced Chaotic Image Encryption Algorithm Based on Baker's Map, IEEE Conference, 508-511, 2003.

[13] A Sinha and Kehar Singh, A technique for image encryption using digital signature, Optical Communications,229-234, 2003.

[14] R Blahut, Theory and Practice of Error Control Codes, Addison Wisley, Reading, MA, 1983.

[15] Y Li, L Yuanxiang, X Xuewen, Image Encryption Algorithm Based on Self-Adaptive Symmetrical-coupled Toggle Cellular Automata, Congress on Image and Signal processing, 32-36, 2008.

[16] H Gao, Y Zhang, S Liang and D Li, A new chaotic algorithm for image encryption, Chaos, solitions and Fractals, 29,393-399,2006.

[17] MI Sobhy, AR Shehata, methods of attacking chaotic encryption and countermeasures, IEEE Acoust Speech Signal Process, 1001-1004, 2001.

[18] Abir Awad and A Saadane, Efficient Chaotic Permutation for image encryption algorithm, Proceeding of the World Congress on Engineering,10, 2010.

[19] S M Sayedzade, R E Atani, S Mirzakuchaki, A novel image encryption algorithm based on hash function, IEEE, 2010.