INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Secure Cryptosystem For Images Using Chaos Based Confusion And Diffusion Mechanism

Sandeep Kumar S
M.Tech student, Dept. of CSE, CEC Mangalore
Ramesh Nayak
Professor, Dept. of ISE, CEC Mangalore

Abstract:

with the fast development of computer technology and the information processing technology, the problem of information security is becoming more and more important. Information hiding is usually used to protect the important information from disclosing when it is transmitting over an insecure channel. Images are routinely used in diverse areas such as medical, military, science, entertainment, advertising, education as well as training. The typical structure of these schemes has the permutation and the diffusion stages performed alternatively. As a result, more overall rounds than necessary are required to achieve a certain level of security. In this paper, we suggest introducing certain diffusion effect in the confusion stage by cyclic shift and XOR operations. The purpose is to reduce the workload of the time consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed. Apart from this, one more level of security is provided by using the recent AES algorithm for confusion and diffusion permutations.

Key words:*Confusion, Diffusion, Ergodicity, Permutation, XOR.*

1.Introduction

Secure transmission of confidential digital images has become a common interest in both research and applications. Image encryption is different from text encryption due to some intrinsic properties of images such as bulky data capacity and high redundancy [1-8], which are generally difficult to handle by using traditional techniques. The main obstacle in designing effective image encryption algorithms is that it is rather difficult to swiftly shuffle and diffuse [7] such image data by traditional cryptographic means. With the desirable Properties of pseudo-randomness, ergodicity, high sensitivity to initial conditions and parameters, chaotic maps has demonstrated great potential for information especially image encryption. The nature of chaos has initiated a lot of Interests in different engineering disciplines, where Cryptography must be one of the most potential applications. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters [6-8], have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. As the basis for developing cryptosystem, the advantage of chaos lies in its random behavior and sensitive to initial condition and parameter setting to fulfill the classic Shannon requirements of confusion and diffusion.

2.Literature Survey

A block cipher based on a suitable use of the chaotic standard map 29 November 2004.Shiguo Lian, Jinsheng Sun, Zhiquan Wang [1], proposed a block cipher based on the chaotic standard map, which is composed of three parts: a confusion process based on chaotic standard map, a diffusion function, and a key generator. The parameter sensitivity of the standard map is analyzed, and the confusion process based on it is proposed. With the desirable properties of ergodicity and high sensitivity to initial conditions and parameters, chaotic maps are very suitable for various data encryption schemes. In particular, chaotic maps are easy to be implemented by microprocessors and personal computers. Therefore, chaotic cryptosystems generally have high speed with low cost, which makes them better candidates than many traditional ciphers for multimedia data encryption. There are some other types of chaotic cryptosystems, most of which transform plaintext directly. And they are often classified into two types: (1) chaotic stream cryptosystems (2) chaotic block cryptosystems. In chaotic stream cryptosystems, a key stream is produced by a chaotic map, which is used to encrypt a plaintext bit by bit. A chaotic block cryptosystem, on the other hand, transforms a

plaintext block by block with some chaotic maps.

A Fast Image Encryption Scheme based on Chaotic Standard Map 2006.

Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law [3] introduce certain diffusion effect in the confusion stage by simple sequential add-and-shift operations. The purpose is to reduce the workload of the time consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed. There are two iterative stages in the proposed chaos-based image cryptosystem. The confusion stage permutes the pixels in the image, without changing its value. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image.

An Efficient Diffusion Approach for Chaos-based Image Encryption 2009.

Kwok-Wo Wong, Bernie Sin-Hung Kwok[4] propose a more efficient diffusion mechanism using simple table lookup and swapping techniques as a light-weight replacement of the 1D chaotic map. A two dimensional (2D) lookup table is specially designed for pixel value diffusion purpose via dynamic swapping and relative indexing of table entries. As the table lookup and entry swapping operations are much efficient than real valued arithmetic operations, the proposed diffusion mechanism leads to a substantial acceleration of existing chaos-based image cryptosystems.

A Novel Encryption Method for Image Security 2012.

Mohammed Abbas Fadhil Al-Husainy [7] proposed method that provides good confusion and diffusion properties that ensures high security due to mixing the two Boolean operations: XOR and Rotation that are done on the bits of the pixels in the image. This method is implemented by firstly doing a sequential XOR operation on all the bits of pixels in the image, and secondly makes a circular rotate right of these bits. These two operations are repeated many times during the encryption phase. The main idea behind the proposed method to encrypt digital images is trying to create an easiest and high secure encryption and decryption method that is satisfying good confusion and diffusion features in the encrypted image.

An Efficient Approach for Image Cryptosystem based on Chaotic Confusion- Diffusion Mechanisms 2012.

Amany Sarhan, Fatma Elgendy, Tarek Eltobely, Osama S. Faragallahs [8] proposed approach for chaos-based image cryptosystems which composed of alternative confusion and diffusion stages. A multi-dimensional chaotic map is usually employed in the confusion stage for image pixel permutation while a one-dimensional (1D) chaotic map

is used for diffusion purpose. The encryption scheme is composed of two steps: chaotic confusion and pixel diffusion, where the former process permutes a plain-image with a 2D chaotic map, and the latter process changes the value of each pixel one by one. In the confusion process, the parameters of the chaotic map serve as the confusion key; in the diffusion process, such parameters as the initial value or control parameter of the diffusion function serve as the diffusion key.

3.Existing And Proposed Methods

3.1.Existing System

The typical structure of these schemes has the permutation and the diffusion stages performed alternatively. The confusion and diffusion effect is solely contributed by the permutation and the diffusion stage, respectively. As a result, more overall rounds than necessary are required to achieve a certain level of security.

3.2.Problem Definition

Image encryption is different from text encryption due to some intrinsic properties of images such as bulky data capacity and high redundancy, which are generally difficult to handle by using traditional techniques. The main obstacle in designing effective image encryption algorithms is that it is rather difficult to swiftly shuffle and diffuse such image data by traditional cryptographic means. Image data have strong correlations among adjacent pixels, which makes fast data-shuffling quite difficult. Statistical analysis on large numbers of images shows that averagely adjacent 8 to 16 pixels are correlative in the horizontal, vertical, and also diagonal directions for both natural and computer-graphical images.

3.3proposed Solution

Here in the confusion stage, both the cyclic permutation on pixel position and the change of pixel value by using xor operation are carried out at the same time while the diffusion process we perform sequential pixel modification. As a result, the pixel value mixing effect of the whole cryptosystem is contributed by two levels of diffusing operations: the modified confusion process and the original diffusion function. As the diffusion effect is not solely contributed by the diffusion function, the same level of security is achieved in fewer cipher rounds. The encryption speed is thus accelerated. Apart from this, one more

level of security is provided by encryption, by the recent AES algorithm for confusion and diffusion permutations.

4.Architecture

The confusion stage permutes the pixels in the image without changing its value. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image. To de correlate the relationship between adjacent pixels, there are m, *n* permutation rounds in the confusion and Diffusion stage with m, *n* larger than 1. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The parameters of the chaotic maps governing the permutation and the diffusion should better be different in different rounds. This is achieved by a round key generator with a seed secret key as input. The chaotic function is sensitive to initial condition, is unpredictable, indecomposable and yet contains regularity. This algorithm uses Henon map for image encryption. Henon map is discrete time dynamic system, which is a mathematical concept where a fixed rule describes the time dependence of a point in a geometrical space. Henon map is defined by the function:

$Xn+1 = Yn+1-aX^2n$ (1)

$Yn+1=bX^2n$ (2)

$Zn+1=1-cY^2n+1+Xn$ (3)

Where a, b and c are constant. This function generates the random value and these random values are bitXORed with the original value of the image, i.e. X value will be bitXORed with the red channel pixel, Y with the green channel and Z with the blue channel.

Image encryption using chaos map include the input image, secret key for encrypting the plain image. The first step will be to generate the keys, which will consist of four variable K1, K2, K3, K4.The value of Xn, Yn and Zn will be generated using the Henon function, which will be used to generate the key. The K1 key will be generated by multiplying the value of Xn, Yn and dividing it by 256. The K2 key will be generated by multiplying the value of Yn, Zn and dividing it by 256. The K3 key will be generated by multiplying the value of Zn, Xn and dividing it by 256. The K1 key will be generated by taking mod of Xn and 255.The keys will be generated by the following rules:

K1= (Xn*Yn)/256 (4)

K2= (Yn*Zn)/256 (5)

K3= (Zn*Xn)/256 (6)

K4=mod (Xn, 255) (7)

5.Confusion

Fridrich suggested that a chaos-based image encryption scheme should compose of two processes: chaotic confusion and pixel diffusion. Confusion and diffusion were first proposed by Shannon .Confusion is the process of hiding the plain image. In this algorithm Confusion is performed by bitXORing first pixel of red channel of the image with key K1, first pixel of green channel with K2, first pixel of blue channel of the image with key K3 and the other pixels will be XORed respectively.

R (1, 1) = R (1, 1) XOR k1 (8)

G (1, 1) = G (1, 1) XOR K2

B (1, 1) =B (1, 1) XOR k3

R (1, 2) = R (1, 2) XOR k4

The process will continue till all the pixels of R, G, and B channel are xored. After confusion, diffusion process is used. In diffusion process the output bits should depend on the input bits in a very complex way. To achieve this, in this algorithm diffusion process is carried out in two steps i.e. horizontal diffusion and vertical diffusion.

5.1.Horizontal Diffusion

This is one of the techniques used in this algorithm. In horizontal diffusion each pixel is bitXORed with the next pixel row wise. Starting from the second pixel of red channel, the first pixel of the red channel is XORed with the second pixel and in the same way all the three channels are horizontally diffused

R(i,j+1)=bitxor(R(i,j+1,1),R(i,j,1)); (9)

G(i,j+1,2)=bitxor(G(i,j+1,2),G(i,j,2));

B(i,j+1,3)= bitxor (B(i,j+1,3),B(i,j,3));

5.2.Vertical Diffusion

Vertical diffusion starts with the last pixel. In Vertical diffusion the second last pixel of the R channel is bit XORed with the last pixel of G channel and B channel respectively whole channel is XORed. The second last pixel of the G channel is bit XORed with the last pixel of R channel and B channel respectively whole channel is XORed and the second last pixel of the B channel is bit XORed with the last pixel of R channel and G

channel respectively whole channel is XORed.

R(i-1,j)=bitxor(R(i-1,j),G(i,j),B(i,j)); (10)

G(i-1,j)=bitxor(G(i-1,j),R(i,j),B(i,j));

B(i-1,j)=bitxor (B(i-1,j),R(i,j),G(i,j))

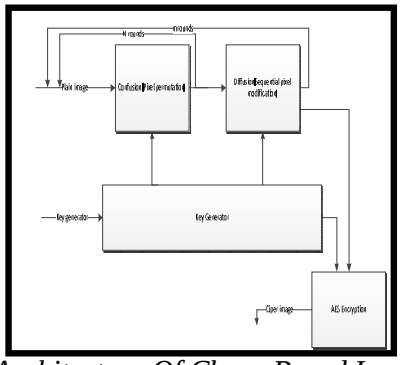

Figure 1: Architecture Of Chaos Based Image Encryption

- Algorithm

Start

Step 1: Input an colored image (which contains R, G, B pattern).

Step 2: R, G, B pattern will be in the form of matrix.

Step 3: Each pixel of the input image is replaced by another value and that value will be generated by random number generator ex. Henon function.

Step 4: After generating the random numbers, that random numbers will be XORed with the original pixel.

Step 5: The output will be an encrypted image.

End

6.Security Analysis

The crucial measure for the quality of a cryptosystem is its capability to withstand the attempts of an unauthorized participant, or an opponent, to gain knowledge about the unencrypted information. A good cryptosystem should resist all kinds of known attacks, such as statistical attack, differential attack, and various brute-force attacks.

Authors	Parameters				
	Key Space	Correlation Coefficients		Differential Attack	
		Plain Image	Cipher Image	NPCR	UACI
Lian-1	H (N, L, n, m) = $(N^2!, N^2.L)^n$.	Not mentioned	Not mentioned	99.26% (m=n=4)	31.70%
Kwok-Wo Wong-3	Not mentioned	-	0.002637	99.62% (m=n=4)	33.47%
Kwok-Wo Wong-4	$2^1.2^2.2^3.N.N.256!$ when N is larger than 256	0.975103	0.003828	99.61% (m=n=4)	33.43%
Mohammed Abbas-7	$(8*P)$ bits, where $P \geq 1$ i.e $2^{(8*P)}$	0.59971	0.00412	Not mentioned	Not mentioned
Amany Sarhan-8	$S = S1.S2$	0.9954	-0.0209	99.61 %	28.61 %.
Proposed system	-	0.9960*	0.00238*	99.62%*	33.52%*

Table 1: Show The Security Analysis Of Various Methods.
*Note * Indicates The Accepted Results Of Proposed System*

7.Conclusion

This paper proposes an improved permutation for Confusion and diffusion Mechanism. To improve the security of the confusion module, a significant diffusion effect is introduced in confusion stage through a cyclic shift and XOR operation.The pixel value mixing effect is then contributed by the diffusion module as well as the improved confusion process. As a result, the number of overall rounds and hence the number of time-consuming diffusion processes is reduced without downgrade the security level. The efficiency of the cryptosystem is thus improved. Theoretical analysis indicates that the proposed chaos-based image encryption scheme can achieve a high performance and is secure against Statistical and Differential attacks and all kinds of brute-force attacks.

8.Reference

1. Lian SG, Sun J, Wang Z. "A block cipher based on a suitable use of chaotic standard map". Chaos, Solitons and Fractals 2005.
2. Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "Security Analysis of A Chaos-based Image Encryption Algorithm" Elsevier Science, 2005.
3. Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map" 2006.
4. Kwok-Wo Wong, Bernie Sin-Hung Kwok, "An Efficient Diffusion Approach for Chaos-based Image Encryption" 2009.
5. Chen Wei-bin, Zhang Xin, "Image Encryption Algorithm Based on Henon Chaotic System"2009.
6. Qiu Run-he cao Yun," Integrated Confusion-Diffusion Mechanism for Chaos Based Image Encryption"2011.
7. Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", Vol. 6, No. 1, January, 2012.
8. Amany Sarhan, Fatma Elgendy, Tarek Eltobely, Osama S. Faragallah, "An Efficient Approach for Image Cryptosystem based on Chaotic Confusion-Diffusion Mechanisms" 2012.
9. Yaobin Mao and Guanrong Chen,"Chaos Based Image Encryption".
10. url: https:// www.wikipedia.com.