Permutation of Image Encryption System Based block cipher and stream cipher encryptioin Algorithm

Huang Chunguang, Cheng Hai, Song yu, Ding qun
Key Laboratory of Electronic Engineering
University of Heilongjiang
Harbin, China
dahuangr@163.com

***Abstract*— In recent years, a variety of encryption algorithms have been investigated to image cryptosystems. Most of them are based on permutation and diffusion architecture. These two procedures are independent according to the encryption algorithm. Block cipher and stream cipher can also be used to encrypt the image, the permutation can be different. This paper proposed the corresponding permutations based on block cipher and stream cipher.**

Keywords-permutation ; block cipher; stream cipher

I. INTRODUCTION

With the development of the internet and personal computers, the digital photo and video have become popular. Image encryption has been one of the most widely used techniques in the past decade for securing the confidentiality, integrity, availability while spreading through a network. Furthermore, special and reliable security in storage and transmission of digital image is needed in many applications, such as medical imaging systems, military image communications and personal information.

In this case, encryption algorithm is needed to protect the uses sensitive digital data from stolen. In computer or communication system, encryption and decryption is most important scheme for digital data.

In recent years, several image encryption schemes have been proposed in the literature based on different approaches for design [1-5]and implementation [6-9]. In cryptography, permutation and substitution are two properties of the operation which were identified by Shannon [10]. Substitution refers the replacement of image with other component, permutation refers to manipulation of the order of image according to some algorithm.

A lots of image encryption method have been proposed. Image can be encrypted in spatial domain, frequency domain or both. [11] proposes a novel permutation and substitution scheme based on chaotic standard map. Each encryption round comprised of three stages: permutation round, substitution round and again permutation rounds. Row-by-row and column and column instead of pixel-by-pixel is used to increase the speed of encryption. [12] presents an image encryption algorithm in frequency domain using a chaotic permutation. The plain image are encrypted in block 8 x 8 because of the image represented in JPEG format. [13] proposes a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. The random-like nature of chaos is effectively spread in the encrypted image through permutation and transformation of pixels in the plain image.

This paper will present the permutation of image when encrypting the plain image based on block cipher and stream cipher. In section 2, we discuss the image permutation based on block cipher. In section 3, we discuss the image permutation based on stream cipher. In section 4, we evaluate the performance of different scheme. In section 5, we give a conclusion.

II. PERMUTATION BASED ON BLOCK CIPHER

A block cipher is a function $E:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. This equation means that E takes two inputs, one being a k-bit string and the other an n-bit string, and returns an n-bit string shown in Fig. 1. The first input is the key. The second might be called the plaintext and the output might be called a cipher text. k is the length of the key and n is the length of the block. These two are the parameters associated to the block cipher.

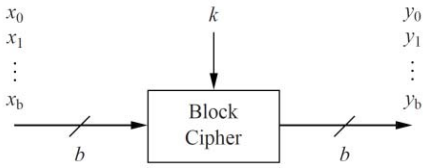

Figure 1. Block cipher encryption

For each cipher key $k \in \{0,1\}^k$, we let $E_k:\{0,1\}^n \to \{0,1\}^n$ be the function which is defined by $E_k(M) = E(K,M)$。 For any block cipher and the key, the function E_k should be a permutation on $\{0,1\}^n$. This mean that it is a bijection $\{0,1\}^n \leftrightarrow \{0,1\}^n$. Accordingly E_K^{-1} is the reverse of E_K. This function also maps $\{0,1\}^n \leftrightarrow \{0,1\}^n$, and we get $E_K^{-1}(E_K(M)) = M$ for all $M \in \{0,1\}^k$.

978-1-4673-9647-9/15 $31.00 © 2015 IEEE
DOI 10.1109/RVSP.2015.46

Some block ciphers such as DES, AES and SMS4 can be used to encrypt the image. And image should be separated to block which has the same bits number with block of cipher.

It is well know that a strong cryptosystem must include two phases: permutation and diffusion. A permutation-only encryption scheme is vulnerable to plaintext attacks. A diffusion-only encryption scheme is vulnerable to differential attacks. The encryption process should be performed several rounds to achieve a good encryption effect.

Serious of block cipher outputs 128bit in one iteration such as AES and SMS4. And each pixel of gray image is composed by 8 bit. Every iteration of block cipher, 16 pixels can be encrypted.

1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1

Figure 2. Block of Image.

The proposed encryption is described below.

Step 1: in Fig x, 4×4 pixels are grouped which is shown. Each group has 16 pixel shown in Fig.2 . Let the image size $L=N\times N$ ($N=4^n$). N is the width and length of the image. The plain image should be structured when the size of image is not $L=N\times N$ ($N=4^n$). Then we can get $(N/4)^2$ groups. XOR operation is used to encrypt the groups by the block cipher. The pixel values will be modified sequentially by mixing with the block cipher so as to confuse the relationship between cipher image and plain image.

Step 2: Permutation is used to resist the differential attacks.

The image group are composed of $4^2\times4^2$ pixels shown in Fig. 3. Permutation is used to regroup the image and such diffusion approach can spread a slight change of plain image to a large scale in the ciphered image and thus differential attack may be practically useless. The pixel values will be modified sequentially by mixing with the block cipher.

Step 3: The image group are composed of $4^i\times4^i\,(1<i\le n)$. Permutation and confusion are also done as step 1 and step 2 until i equals n .

The decryption is the complete reverse of the encryption and the plain image can be obtain after the same operation.

Simulation is carried out using MATLAB, the 256*256 Lena image is used to encrypt. The block cipher *SM4* is used to encrypt the image which is shown in Fig. 4.

Table 1 is the numbers of permutation and confusion according to the size of image.

Table 1. Comparison Table between the Size of Image and Counts of Confusion and Diffusion

Size of image	permutation	confusion
4*4	0	1
16*16	1	2
64*64	2	3
256*256	3	4
1024*1024	4	5
4096*4096	5	6

1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
5	5	5	5	6	6	6	6	7	7	7	7	8	8	8	8
5	5	5	5	6	6	6	6	7	7	7	7	8	8	8	8
5	5	5	5	6	6	6	6	7	7	7	7	8	8	8	8
5	5	5	5	6	6	6	6	7	7	7	7	8	8	8	8
9	9	9	9	10	10	10	10	11	11	11	11	12	12	12	12
9	9	9	9	10	10	10	10	11	11	11	11	12	12	12	12
9	9	9	9	10	10	10	10	11	11	11	11	12	12	12	12
9	9	9	9	10	10	10	10	11	11	11	11	12	12	12	12
13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16
13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16
13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16
13	13	13	13	14	14	14	14	15	15	15	15	16	16	16	16

Figure 3. Image block

(a)Original Image Lena (b)Image Encrypted

Figure 4. Application of block cipher on digital image lena

One of the security requirements for an effective image encryption scheme is its ability to resist differential attack. An effective image cryptosystem should spread out a slight modification in plain image to a larger scale in the cipher text, so as to resist differential attack. Two performance indices, NPCR (number of pixels change rate) and UACI (unified average changing intensity) are generally utilized to numerically evaluate the effectiveness of an image cryptosystem. Suppose that I_1 and I_2 are two images, and $D(i,j)$ is

$$D(i,j)=\begin{cases}D(i,j)=0, I_1(i,j)=I_2(i,j)\\ D(i,j)=1, I_1(i,j)\neq I_2(i,j)\end{cases}$$

NPCR is defined as

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M*N} *100\%$$

UACI is defined as

$$UACI = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} |I_1(i,j) - I_2(i,j)|}{255 \times M \times N} *100\%$$

Table 2. Analysis of Image Diffusion

Iteration	NPCR	UACI
1	4.8828e-4	1.8298e-4
2	3.8859e-3	1.2528e-3
3	6.1991e-2	2.0668e-2
4	0.9881	0.3323

From the Table 2 we can see the NPCR and UACI scores can approach the expected values after the iteration when size of plain image is 256*256.

III. PERMUTATION BASED ON STREAM CIPHER

Stream ciphers encrypt bits individually. This is achieved by adding a bit from a key stream to plaintext bit. Binary stream ciphers using linear feedback shift registers (LFSRs) because they be easily implemented in hardware and can be readily analyzed mathematically. The use of LFSRs on their own, however is insufficient to provide good security. Various schemes have proposed to increase the security of LFSRs [14].

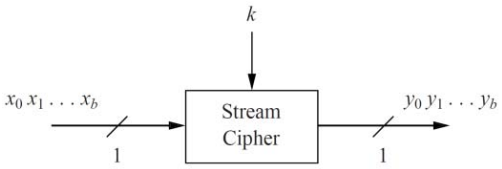

Figure 5. Stream Cipher

The image encryption algorithm based on the stream cipher should undergoes several stages of diffusion using feedback, pixel confusion and bit permutation.

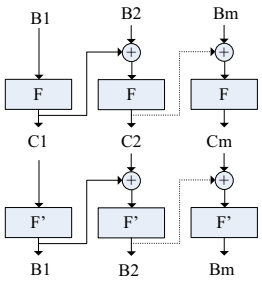

Figure 6. Cipher block chaining

Permutation of image encryption based on stream cipher is CBC (cipher block chaining) mode. These method can resist the differential attack and improve the security of image.

The proposed algorithm is implemented in MATLAB, the Lena picture is used, and size of Lena is 256*256. XOR operation is used for substitution, and CBC mode is used for permutation.

The proposed encryption is described as follow.

Step 1: Encrypt the image using the stream cipher from the beginning to the end.

Step 2: Encrypt the image using the same stream cipher from the end to the beginning.

Step 3: Repeat the encryption until the NPCR and UACI reach the ideal state.

Form the Table 3 we can see the relationship between number of iteration and NPCR, UACI.

Table 3. Analysis of image permutation base on stream cipher

Iteration	NPCR	UACI
1	0.0313	0.0105
2	0.9941	0.3340
3	0.9960	0.3346

IV. CONCLUSION

In this paper, permutations based on block cipher and stream cipher are discussed. Permutation based on block cipher is proposed by grouping the image and diffusing to the other group to increase the spread rate. Permutation based on stream cipher is proposed by cipher block chaining mode to increase the diffusion rate. The results show that iteration times have the exponential relationship with the size of image when block cipher is used to encrypt the image and iteration times are limited no matter the size of image.

ACKNOWLEDGMENT

This work was supported by the Heilongjiang University Youth Fund (QL200611).

REFERENCES

[1] Zhang, Guoji, and Qing Liu. "A novel image encryption method based on total shuffling scheme." Optics Communications 284.12 (2011): 2775-2780.

[2] Fu, Chong, et al. "A chaos-based digital image encryption scheme with an improved diffusion strategy." Optics Express 20.3 (2012): 2363-2378.

[3] Jin, Jun. "An image encryption based on elementary cellular automata."Optics and Lasers in Engineering 50.12 (2012): 1836-1843.

[4] Zhang, Yushu, et al. "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations." Signal Processing: Image Communication 28.3 (2013): 292-300.

[5] Brown, Robert, Donald Felton, and James Ian McNiven. "Display of a verification image to confirm security." U.S. Patent No. 8,621,242. 31 Dec. 2013.

[6] Rajagopalan, Sundararaman, et al. "Dual cellular automata on FPGA: An image encryptors chip." Res. J. Inform. Technol 6 (2014): 223-236.

[7] Bhatnagar, Gaurav, and QM Jonathan Wu. "Selective image encryption based on pixels of interest and singular value decomposition." Digital Signal Processing 22.4 (2012): 648-663.

[8] Gore, M., and V. Deotare. "FPGA Implementation of Area Optimized AES for Image Encryption/Decryption Process." Design and reuse online journal(2013): 1.

[9] Upadhyay, Har Narayan, and John Bosco Balaguru Rayappan. "Survey and analysis of hardware cryptographic and steganographic systems on FPGA."Journal of Applied Sciences 12.3 (2012): 201-210.

[10] Shannon, Claude E. "Communication theory of secrecy systems*." Bell system technical journal 28.4 (1949): 656-715.

[11] Patidar, Vinod, et al. "Image encryption through a novel permutation-substitution scheme based on chaotic standard map." Chaos-Fractals Theories and Applications (IWCFTA), 2010 International Workshop on. IEEE, 2010.

[12] Munir, Rinaldi. "A block-based image encryption algorithm in frequency domain using chaotic permutation." Telecommunication Systems Services and Applications (TSSA), 2014 8th International Conference on. IEEE, 2014.

[13] Sathishkumar, G. A., Siddharth Ramachandran, and K. Bhoopathy Bagan. "Image encryption using random pixel permutation by chaotic mapping."Computers & Informatics (ISCI), 2012 IEEE Symposium on. IEEE, 2012.

[14] Alghamdi, Abdullah Sharaf, et al. "Bio-chaotic stream cipher-based iris image encryption." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 2. IEEE, 2009.