International Symposium on Communications
and Information Technologies 2004 (ISCIT 2004)
Sapporo, Japan, October 26- 29, 2004

AN ASYMMETRIC IMAGE ENCRYPATION BASED ON MATRIX TRANSFORMATION

Yang Shuangyuan Lu Zhengding Han Shuihua

(School of Computer Science, Huazhong University of Science&Technology, Wuhan, China 430074)

Email:ysydragon@sina.com.cn

ABSTRACT

In this paper, it is shown how to adapt certain matrix transformation to create a novel asymmetric block encryption scheme. The proposed scheme is especially useful for encryption of large amounts of data, such as digital images. First, a pair of keys are given by using matrix transformation; Second, the image is encrypted in its transformation domain. This scheme can satisfy the characters of convenient realization and locate the possible changed region.

1. INTRODUCTION

With the rapid progress of Internet, in recent years, to establish the transmission of images, highly reliable and high-speed digital transmission is required. Beside this, Internet applications have to deal with security issue. Internet users exasperate potential security threats such as eavesdropping and illegal access. They want to be protected and to ensure their privacy.

Network security and image encryption has become important and high profile issues. Innovative encryption techniques have been developed for effective data encryption[1-7]. Few of these algorithms can satisfy efficient and secure encryption.

In this paper, a novel asymmetric image encryption scheme is proposed. Based on certain matrix transformation, all the pixels and frequencies in each block of the original image are scrambled. To implement this algorithm, first, a pair of keys are created based on matrix transformation; Second, the image is encrypted by using private key in its transformation domain; Finally the receiver uses the public key to decrypt the encrypted messages. Because of the proposed scheme based on matrix transformation, it is easily implemented and highly efficient to quickly encrypt and decrypt image messages. The asymmetric encryption mechanism makes the encrypted data more secure.

The remaining of this paper is as follows. Section 2 describes a five-step process of encrypting every block of the original image in DCT transformation and then decrypting them. In Section 3, we discuss the relationship between public key and private key and analyze how to ensure their security. Experimental results and conclusion are given in Section 4 and Section 5 respectively.

2. ENCRYPTING AND DECRYPTING

Without loss of generality, we consider encrypting the grayscale image, named as $I_{M\times N}$ (To RGB image, using its luminance space). The whole encryption process is described as follows:

Step 1: Creating the key pairs: private key for encryption, public key for decryption;

Step 2: Dividing original image into distinct $P\times P$ blocks and transforming them into DCT domain;

Step 3: Using the private key to encrypt the frontal $K\times P$ coefficients of every $P\times P$ block;

Step 4: Making the inverse DCT transformation and uniting all $P\times P$ blocks;

Step 5: Deal with the transformed coefficients and keep them between 0 and 1.

Corresponding decryption process is:

Step 1: Dividing un-decrypted image into distinct $P\times P$ blocks and transforming them into DCT domain;

Step 2: Recovering the DCT coefficients;

Step 3: Using the public key to decrypt the $P\times P$ coefficients of every $P\times P$ block;

Step 4: Making the inverse DCT transformation and uniting all $P\times P$ blocks;

For creating the pair of private key and public key, first, with Gaussian white noise , we create two matrices:

$U \in R^{K \times P}$ and $V \in R^{P \times K}$ whose ranks are equal to K; and then make the matrix multiplication between U and V into an invertible matrix A of size $K \times K$, defined as:

$$A = UV = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1K} \\ a_{21} & a_{22} & \cdots & a_{2K} \\ \vdots & \vdots & \vdots & \vdots \\ a_{K1} & a_{K2} & \cdots & a_{KK} \end{bmatrix} \tag{1}$$

Assume $S \in R^{K \times K}$ is the principal square root of the invertible matrix A, it is easy to say that S is also invertible. In the proposed scheme, the private key and public key are VS^{-1} and $S^{-1}U$ respectively where S^{-1} denotes the inverse of A. The details of encryption and decryption are as following:

1) Encryption

Step1: Dividing original image into distinct $P \times P$ blocks and transforming them into DCT domain, the corresponding DCT coefficients are named as $X_{M \times N}$.

$$X_{M \times N} = DCT(I, [P \quad P]) \tag{2}$$

Step2: Encrypting the frontal $K \times P$ coefficients of every $P \times P$ block respectively. Let X_1 denotes the matrix composed by the frontal $K \times P$ coefficients of certain $P \times P$ block X_0, the corresponding encryption formula by using the private key VS^{-1} can be described as:

$$X_2 = VS^{-1} X_1 \tag{3}$$

Step3: Replacing the frontal $P \times P$ coefficients of X_0 with $X_2 \in R^{P \times P}$

If K is close to P, according to the characteristic of DCT coefficients, the rest $(P-K) \times P$ coefficients are all close to 0. So we can directly replace them and the decrypted image is almost not influenced.

$$X_0(i,j) = X_2 \{1 \le i \le P, 1 \le j \le P\} \tag{4}$$

Step4: Making the inverse DCT transformation and uniting all $P \times P$ blocks, the final result is defined as $X2_{M \times N}$.

$$X2_{M \times N} = IDCT(X_{M \times N}) \tag{5}$$

Step5: Keeping all the transformed coefficients between 0 and 1

Step6: Saving the encrypted image as bmp file

2) Decryption

The decryption operation is a usual correlation process with three elements: (1) block length P; (2) encryption matrix dimension K; (3) public key $S^{-1}U$. Suppose $X3_{M \times N}$ denotes the encrypted image, the details of decryption are following:

Step1: Recovering all coefficients of $X3_{M \times N}$

Step2: Applying DCT transformation to each distinct $P \times P$ block of $X3_{M \times N}$

$$X4_{M \times N} = DCT(X3_{M \times N}, [P \quad P]) \tag{6}$$

Step3: Decrypting the frontal $P \times P$ coefficients of every $P \times P$ block respectively.

Let D_1 denotes the matrix composed by $P \times P$ coefficients of certain $P \times P$ block D_0, the corresponding decryption data $D_2 \in R^{K \times P}$ by using the public key $S^{-1}U$ can be given as following:

$$\begin{aligned} &\Rightarrow D_2 = (S^{-1}U) D_1 \\ &\Rightarrow D_2 = (S^{-1}U)(VS^{-1}) X_0 \\ &\Rightarrow D_2 = (S^{-1}(UV) S^{-1}) X_0 \end{aligned} \tag{7}$$

Because $UV = A = S^2$, we can draw the conclusion:

$$\Rightarrow D_2 = X_0 \tag{8}$$

Step4: Replacing the frontal $P \times P$ coefficients of D_0 with D_2 and 0.

$$D_0(i,j) = \begin{Bmatrix} D_2 & \{1 \le i \le K, 1 \le j \le P\} \\ 0 & \{K < i \le P, 1 \le j \le P\} \end{Bmatrix} \tag{9}$$

Step5: Making the inverse DCT transformation, uniting all $P \times P$ blocks and saving the decrypted image as bmp file.

3. ATTACK ANALYSIS

Since the encrypted image and the public key are open to the public, the attackers may attempt to compute the private key from the public key in order to decrypt the encrypted image. The security of the proposed scheme therefore relies on whether VS^{-1} can be computed from the knowledge of $S^{-1}U$. If P is equal to K, it is easily proved that $S^{-1}U$ and VS^{-1} become a square matrix. As using the following matrix transformation:

$$\begin{aligned} &\Rightarrow (S^{-1}U)(VS^{-1}) \\ &\Rightarrow S^{-1}(UV)S^{-1} \\ &\Rightarrow S^{-1}S^2S^{-1} \\ &\Rightarrow E \end{aligned} \tag{10}$$

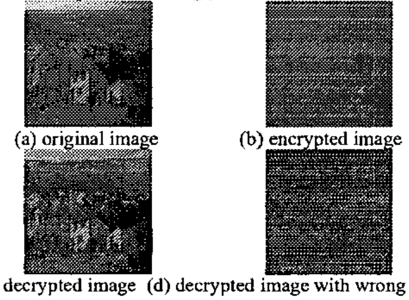
VS^{-1} can be directly computed from the knowledge of $S^{-1}U$. It is evidently very dangerous. So, K is usually made less than P. That is to say, $S^{-1}U$ is not a square matrix, Thereby, from the view of matrix theory, it is evidently not possible to obtain the private key VS^{-1} from the public key $S^{-1}U$ only through the formula (10) directly. So when U and V are created, we ensure they are not the square matrices. When P is more bigger than K, the proposed scheme is more robust against this attack.

For more security against this direct attack, we apply different A and U to every $P\times P$ block. The only possibility of computing VS^{-1} arises when the attacker has the knowledge of the whole public key $S^{-1}U$, and at the same time, U and V must be the square matrices.

After analyzing the relation between K and P, now we discuss their suitable values. If P is too big, the block DCT transformation loses its actual effect. However, if P is too small, it makes the encryption and decryption process very slow. In general, the size of many images keep between 256×256 and 512×512. So, to keep the generality and the encryption and decryption efficiency of the proposed scheme, P is given to 32 in this paper. For K, to obtain enough coefficients, K should be ensured around $P/2$. In this paper, it is 18.

4. EXPERIMENTAL RESULTS

In this paper, we test many images for better validating the effect of the proposed scheme. As a representative, only the results of "goldhill" of size 512×512 are shown. The original image is presented in fig.1 (a). The encrypted image and decrypted image are shown in fig.1 (b) and (c), separately. In fig.1 (d), the decrypted image with wrong public key is shown.

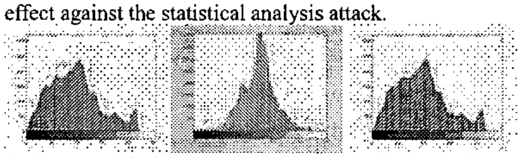


(a) original image (b) encrypted image

(c) decrypted image (d) decrypted image with wrong key

Fig. 1 Results of encryption and decryption

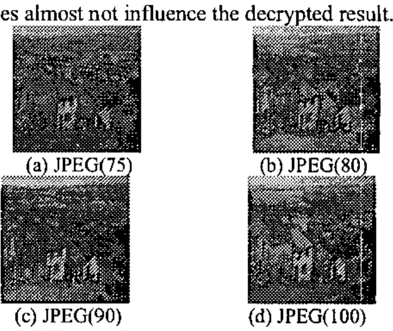
Fig.2 shows the histograms of the original image, encrypted image and decrypted image. Because the proposed scheme uses block matrix transformation to encrypt images, it can scramble the grayscales and frequency domain. So the histogram of the encrypted image are completely changed and keep better secrete effect against the statistical analysis attack.



(a)histogram of original image (b)histogram of encrypted image (c)histogram of decrypted image

Fig.2 histograms of original , encrypted and decrypted image

In fact, the proposed scheme is very robust against JPEG lossy compression. The decrypted results under different JPEG compression quality are shown in Fig.3. Fig.3 (d) shows that only format conversion from bmp to JPG does almost not influence the decrypted result.

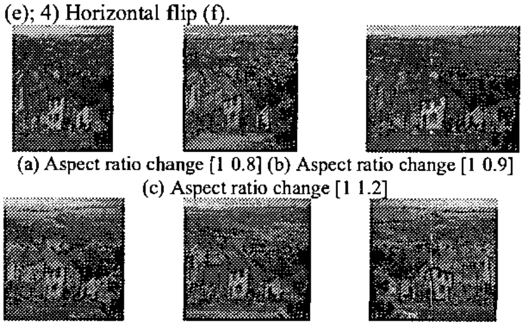


(a) JPEG(75) (b) JPEG(80)

(c) JPEG(90) (d) JPEG(100)

Fig.3 decrypted results under JPEG compression

In fig.4, we show some decrypted results under other attacks. 1) Aspect ratio change: (1,0.8), (1,0.9), (1,1.2), and the first component is the scaling in X direction, and the second is the scaling in Y direction. ((a), (b), (c)); 2) Shearing 5% in y direction (d); 3) Gaussian noise by %2 (e); 4) Horizontal flip (f).

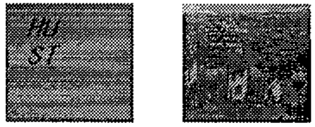


(a) Aspect ratio change [1 0.8] (b) Aspect ratio change [1 0.9] (c) Aspect ratio change [1 1.2]

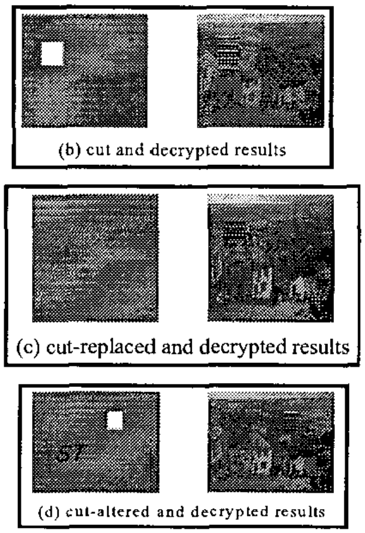
(d)Shearing [5 0] (e) Gaussian noise(2%) (f) Horizontal flip

Fig.4 decrypted results under other attacks

It is another advantage for the propose scheme with good property of localization for the possible changed region. The locations of modified region are shown in Fig.5.



(a) altered and decrypted results



(b) cut and decrypted results

(c) cut-replaced and decrypted results

(d) cut-altered and decrypted results

Fig.5 altered, cut and decrypted results

5. CONCLUSION

Based on matrix transformation, a novel asymmetric scheme is proposed for image encryption in this paper. This scheme satisfies the characters of convenient realization, less computation complexity and better security. The experimental results demonstrate its effectiveness to allow the acceptable JPEG lossy compression and good property of localization for the possible changed region.

6. REFERENCE

[1] Yi Kai-Xiang Sun Xing etc, "An image encryption algrithm based on chaotic sequences", *Journal of Computer Aided Design and Computer Graphics*, 2000, (6): 672-676

[2] Zhang X.H. Liu F. Jiao L.C., "An encryption arithmetic based on chaotic sequence", *Image and Graphics*, 2003,8(4): 374-378

[3] Li C.G Han Z.Z. Zhang H.R. "An image encryption algorithm based on random key and quasi-standard map", *Chinese Journal of Computers*, 2003, 26(4):465-470

[4] Chang H.K. Liou J.L., "An image encryption scheme based on quadtree compression scheme", *Proceedings of the International Computer Symposium*, Taiwan:2001: 230-237

[5] Chang H.K. Liou J.L., "An image encryption scheme based on quadtree compression scheme", *Proceedings of the International Computer Symposium*, Taiwan: 2001,230-237

[6] Chang C.C. etc, "A new encryption algorithm for image cryptosystems", *The Journal of Systems and Software*, 2001,5(7): 83-91

[7] Kou C.J., "Novel image encryption technique and its application in progressive transmission", *J.Electron. Imaging*, 1994,2(4):345-351