An Asymmetric Image Encryption Based on Matrix Transformation

Han Shuihua* and **Yang Shuangyuan****, Non-members

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 using private key in its transformation domain; Finally the receiver uses the public key to decrypt the encrypted messages. This scheme satisfies the characters of convenient realization, less computation complexity and good security.

Keywords: Image encryption, Matrix transformation, Asymmetric block encryption

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. Besides 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.

Most traditional or modern cryptosystems have been designed to protect textual data. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. Once the cipertext has been produced, it is saved in storage or transmitted over the network. Upon reception, the ciphertext can be transformed back into the original plaintext by using a decryption algorithm.

However, images are different from text. Although we may use the traditional cryptosystems(such as RSA and DES-like cryptosystems) to encrypt images directly, it is not a good idea for two reasons. One is that the image size is much greater than that of text, so the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image, a decrypted image containing small distortion is acceptable due to human perception.

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. In order to farther add security of matrix transformation, the second encryption schema is used to produce transformation matrix by pseudo-random gauss white noise.

The remaining of this paper is as follows. Section 2 surveys some related image cryptosystems. Section 3 gives some characteristics of an image cryptosystem. Section 4 describes a five-step process of encrypting every block of the original image in DCT transformation and then decrypting them. Then, we discuss the relationship between public key and private key and analyze how to ensure their security in section 5. Computing complexity is discussed in section 6. Experimental results and conclusions are given in section 7 and section 8, respectively.

2. RELATED IMAGE CRYPTOSY STEMS

According to the differences between image and text, recently there have been several innovative encryption techniques(Schwartz, 1991; Bourbakis and Alexopoulos,1992; Kuo, 1993; Chang and liou, 1994; Yi Kai-Xiang, 2000; C-C Chang, 2001)

Schwartz (1991) proposed a scrambling method to encrypt image. Its first step is to generate a sequence of random points on the original image. These random points are notably determined by the seed of the random number generator, the seed is the private key of this method. Next, this method draws some graphical lines between each two consecutive points of this sequence. Moreover, its drawing pen is in the inverted mode, which changes each white pixel to black and vice versa. After drawing many inverse lines on the original image, the plain image is thus encrypted.

Manuscript received on May 21, 2005 ; revised on February 12, 2006.

*The author is with Department of Information System, School of Management, Xiamen University, P.R.CHINA, 361005. e-mail: Hansh@xmu.edu.cn

**The author is with Postdoctoral Station of Business Administrator, Xiamen University, P.R.CHINA, 361005. e-mail: yangshuangyuan@yahoo.com.cn

This method is simple and fast, however, its security degree is not high enough to protect images.

Bourbakis and Alexopoulos (1992) developed another image encryption method. It converts a 2D image into 1D list, and employs a SCAN language to describe the converted result. In this language, there are several SCAN letters. Each SCAN letter represents one kind of scan order. Different kinds of combination of SCAN letter may generate different kinds of secret image. After determining the combination of SCAN letters, the schema then generates a SCAN string. This string defines the scan order of the original image. Next, this method scans the original image in the determined order and , moreover, encrypts the SCAN strings by using commercial cryptosystems. Since the illegal users cannot obtain the correct SCAN string, the original image is therefore secure. There is no image compression in this method, thus it is inefficient to encrypt or decrypt the image directly.

Kuo (1993) proposed an encryption method that referred to the image distortion. This method obtains the encrypted image by adding the phase spectra of the plain image with those of another key image. Since the phase spectra of the encrypted image are randomly changed, the cipher image is unrecognizable. Thus this method is safe, but no image compression is considered.

Chang and liou (1994) proposed an encryption method for images. This method employs two technologies to achieve the compression and encryption purposes. They are quad tree data structure and the SCAN language, respectively. This method first compresses the original image by using a quad tree, and then encrypts the compressed data by SCAN. So, this method can compress and encrypt images concurrently. Quadtree is notably a lossless data compression technology, therefore this method is also lossless, it may not be secure enough to resist some illegal attacks such as jigsaw puzzle attack and neighbor attack etc.

Yi Kai-Xiang (2000) gives an image encryption algorithm based on chaotic sequence. First, the real number value chaotic sequences using the key value is generated. Then it is dispersed in to symbol matrix and transformation matrix. Finally the image is encrypted using them in DCT domain. DCT is a lossy data compression technique, image may occur some distortions caused by lossy data compression and noise, but this method can still correctly decrypt and restore original image, and can achieve a high security degree.

C-C Chang (2001) proposed a fast image encryption algorithm based on vector quantization (VQ), cryptography and number theorems. In VQ, the image was first decomposed into vectors and the sequentially encoded vector by vector. Then traditional cryptosystem from commercial applications was used, for enhancing security and reducing the computational complexity of encryption/decryption, some number theorems were applied. VQ is an efficient approach to low bit-rate image compression, therefore speeds up the encryption process and achieve high security.

All these proposed methods belong to symmetric key cryptosystem, they are vulnerable in case they employ the unique key in their proposed system(Jinn-Ke Jan, 1996). To avoid the known plaintext attack in a symmetric key cryptosystem, the expression defining the encryption and decryption key should be different in every encryption process of the image, and the expression can by sent after encryption by using asymmetric cryptosystem, which makes the encrypted data more secure. Here, we propose a novel asymmetric image encryption scheme. Using certain matrix transformation to create a novel asymmetric block encryption scheme, all the pixels and frequencies in each block of the original image are scrambled. Our method can achieve the following two goals. One is that it is easily implemented and highly efficient to quickly encrypt and decrypt image messages based on matrix transformation. The other is that asymmetric encryption mechanism makes the encrypted data more secure.

3. CHARACTERISTICS OF AN IMAGE CRYPTOSYSTEM

For studying image encryption, we must first analyze the implementing differences between image and text data:

1. when cipher text is produced, the decrypted text must be equal to the original text in a full lossless manner. However, this requirement is not necessary for image, the cipher image can be decrypted to a original image in some lossy manner.
2. Text data is a sequence of words, it can be encrypted directly by using block or stream ciphers. However, digital image data are represented as 2D array.
3. Since the storage space of a picture is very large, it is inefficient to encrypt or decrypt image directly. One of the best methods is to only encrypt/decrypt information that is used by image compression for reducing both its storage space and transmission time.

In general, there are three basic characteristics in the information field: privacy, integrity and availability. For privacy, an unauthorized user can not disclose a message. For integrity, an unauthorized user can not modify or corrupt a message. For availability, message is made available to authorized users faithfully.

A perfect image cryptosystem is not only flexible in the security mechanism, but also has high overall secure performance, the image security requires following characteristics:

1. The encryption system should be computationally secure. It requires a extremely long time to attack, unauthorized user should not be able to read privileged image.
2. Encryption and decryption should be fast enough not to degrade system performance. The algorithm for encryption and decryption must be simple enough to be done by user in personal computer.
3. The security mechanism must be as widespread as possible.
4. The security mechanism should be flexible.
5. There should not be a large expansion of encrypted image data.

4. 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 $K\times K$ coefficients of $P_{\times}P$ every 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.

First, we create a set of orthonormal bases $\{u_i, i=1,2,\dots K\}$ of length P and an invertible matrix A of size $P\times P$ by using the method of [7]. $\{u_i\}$ forms the column vector of U, defined as:

$$[A]=\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1P} \\ a_{21} & K_{22} & \dots & a_{2P} \\ \vdots & \vdots & \vdots & \vdots \\ a_{P1} & a_{P2} & \dots & a_{PP} \end{bmatrix}$$

$$[U]=\{u_i\}=\begin{bmatrix} u_{11} & a_{12} & \dots & a_{1K} \\ u_{21} & K_{22} & \dots & a_{2K} \\ \vdots & \vdots & \vdots & \vdots \\ u_{P1} & a_{P2} & \dots & a_{PK} \end{bmatrix} \quad (1)$$

The private key and public key are AU and $A^{-t}U$, respectively, where A^{-t} denotes the inverse transpose of A. The details of encryption and decryption are as following:

1) Encryption

Step 1: Dividing original image into distinct $P\times P$ blocks and transforming them into DCT domain, the corresponding DCT coefficients are named as $X_{M\times N}$.

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

Step 2: Encrypting the frontal $K\times K$ coefficients of every $P\times P$ block, respectively. Let X_1 denotes the matrix composed by the frontal $K\times K$ coefficients of certain $P\times P$ block X_0, the corresponding encryption formula by using the private key AU can be described as:

$$X_2=AUX_1 \quad (3)$$

Step 3: Replacing the frontal $P\times K$ coefficients of X_0 with $X_2\in R^{P\times K}$

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

$$X_0\left(i,j\right)=X_2\left\{1\le i\le P, 1\le j\le K\right\} \quad (4)$$

Step 4: Making the inverse DCT transformation and uniting all $P\times P$ blocks, the final result is defined as $X2_{M\times N}$.

$$X2_{M\times N}=IDCT\left(X_{M\times N}\right) \quad (5)$$

Step 5: Keeping all the transformed coefficients between 0 and 1.

```
% Get the minimum of X2_{M×N}, named as Min
Min = max((-1) × X2_{M×N})
% Ensure all the coefficients of X2_{M×N} more than 0
X2_{M×N} = X2_{M×N} + Min
% Get the maximum of updated X2_{M×N}, named as Max
Min = max(X2_{M×N})
% Ensure all the coefficients of X2_{M×N} less than 1
X2_{M×N} = X2_{M×N} / Max
```

(6)

Step 6: Saving the encrypted image as bmp file.

2) Decryption

The decryption operation is a usual correlation process with five elements: (1) block length P; (2) encryption matrix dimension K ; (3) public key $A^{-t}U$; (4) the coefficient minimum Min; (5) the coefficient maximum Max. Suppose $X3_{M\times N}$ denotes the encrypted image, the details of decryption are following:

Step 1: Recovering all coefficients of $X3_{M\times N}$

$$X3_{M\times N}=X3_{M\times N}\times Max-Min \quad (7)$$

Step 2: Applying DCT transformation to each distinct $P\times P$ block of $X3_{M\times N}$

$$X4_{M\times N}=DCT\left(X3_{M\times N},[P\ \ P]\right) \quad (8)$$

Step 3: Decrypting the frontal $P \times K$ coefficients of every $P \times P$ block, respectively.

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

$$\begin{aligned} &\Rightarrow D_2 = \left(A^{-t}U\right)^t D_1 \\ &\Rightarrow D_2 = \left(U^t A^{-1}\right)(AU)X_0 \\ &\Rightarrow D_2 = \left(U^t U\right) X_0 \end{aligned} \tag{9}$$

Because the column vector of U is a set of orthonormal bases, it is easily proved: $U^t U = E$. So, we can draw the conclusion:

$$\Rightarrow D_2 = X_0 \tag{10}$$

Step 4: Replacing the frontal $P \times K$ coefficients of D_0 with D_2 and 0.

$$D_0(i,j) = \begin{cases} D_2 & \{1 \le i,\, j \le K\} \\ 0 & \{K \le i \le P,\ 1 \le j \le K\} \end{cases} \tag{11}$$

Step 5: Making the inverse DCT transformation and uniting all $P \times P$ blocks, the final result is defined as $X5_{M \times N}$.

$$X5_{M \times N} = IDCT\left(X4_{M \times N}\right) \tag{12}$$

Step 6: Saving the decrypted image as bmp file.

5. SECURITY 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 AU can be computed from the knowledge of $A^{-1}U$. When we apply different A and U to every $P \times P$ block, the only possibility of computing AU arises when the attacker has the knowledge of the whole public key $A^{-1}U$.

For discussing the relationship between A and U, we let $A \in R^{P \times P}$, and $U \in R^{P \times K}$. Because the rank of U is equal to K, P is not less than K. If P is equal to K, it is easily proved that U becomes a square orthogonal matrix because $UU^t = U^t U = E$. As using the following matrix transformation:

$$\begin{aligned} &\Rightarrow \left(A^{-t}U\right)\left(A^{-t}U\right)^t = \left(A^{-t}U\right)\left(U^t A^{-1}\right) \\ &\Rightarrow \left(A^{-t}U\right)\left(A^{-t}U\right)^t = A^{-t}\left(UU^t\right)A^{-1} \\ &\Rightarrow \left(A^{-t}U\right)\left(A^{-t}U\right)^t = A^{-t}A^{-1} \\ &\Rightarrow \left(A^{-t}U\right)\left(A^{-t}U\right)^t = \left(AA^t\right)^{-1} \end{aligned} \tag{13}$$

AU can be directly computed from the knowledge of $A^{-t}U$ because

$$AU = AA^t\left(A^{-t}U\right) \tag{14}$$

It is evidently very dangerous. So, K is usually made less than P. That is to say, U is not a square matrix, and $UU^t = Q \in R^{P \times P}$. Because the rank of U is K less than P, not all the row vectors of U is kept orthodoxy between each other. Thereby,

$$\Rightarrow \left(A^{-t}U\right)\left(A^{-t}U\right)^t = A^{-t}QA^{-1} \tag{15}$$

From the view of matrix theory, it is evidently not possible to obtain the private key AU from the public key $A^{-t}U$ only through the formula (15) directly. So when U is created, we ensure it is not a square matrix. When P is more bigger than K, the proposed scheme is more robust against this attack.

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 keeps 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 between $P/2$ and P. In this paper, it is 28.

6. COMPUTING COMPLEXITY

(1) Encryption Image encryption includes three steps: first makes 32×32 block DCT transformation to original image, then creates a pair of private key and public key for each 32×32 block, and then makes matrix multiplication operation to the block using private key, finally makes reverse block DCT transformation.

Assume image size is $N \times N$ then image can be split into $\left[\frac{N}{32} \times \frac{N}{32}\right] = \left[\frac{N^2}{1024}\right]$ blocks, each block computing complexity is $O\left(32^2\ log_2^{32}\right)$, total computing complexity of block DCT transformation is $O\left(32^2\ log_2^{32}\right) * \left[\frac{N^2}{1024}\right] = O\left(5N^2\right)$. Private key computing complexity for each 32×32 block is $O\left(32^2\right)$, public key computing complexity for each 32×32 block is $O\left(32^3\right) * O\left(32^2\right) = O\left(32^5\right)$. So sum complexity for a pair of keys is $\left(O\left(32^5\right) + O\left(32^2\right) * \left[\frac{N^2}{1024}\right] = O\left(\left(32^3+1\right)N^2\right)\right)$; matrix multiplication for each 32×32 blocks is $O\left(32^2\right) * \left[\frac{N^2}{1024}\right] = O\left(N^2\right)$. In the same way, reverse block DCT transformation is $O\left(5N^2\right)$. The computing complexity for all image encryption is: $O\left(5N^2\right) + O\left(\left(32^3+1\right)N^2\right) + O\left(N^2\right) + O\left(5N^2\right) = O\left(\left(32^3+12\right)N^2\right)$.

Fig.1: *Results of encryption and decryption*

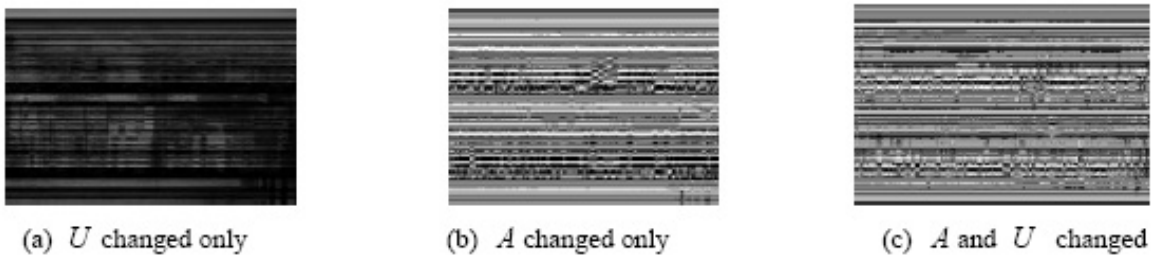

Fig.2: *Decryption results with different wrong key*

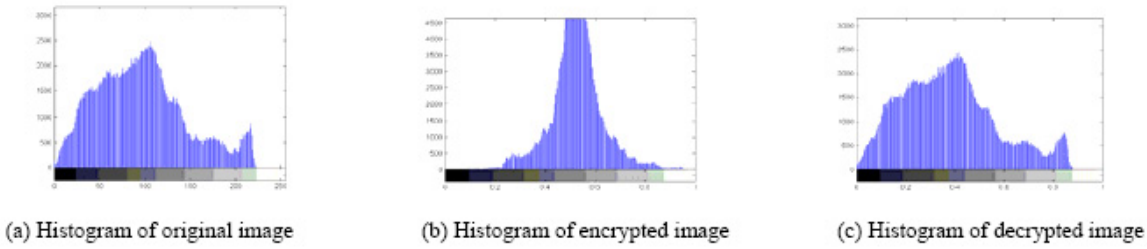

Fig.3: *Histograms of original, encrypted and decrypted image*

Fig.4: *Decrypted results under JPEG compression*

We can make out that, when DCT block is more bigger, computing complexity is more higher, cost time is more long. On the contrary, block is more smaller computing complexity is more lower, cost time is more shorter. From view of pure computing efficiency of encryption, DCT block is better to be smaller. But for security, if block is too small ,it may be easily broken by enemy. So, 32×32 block is chosen, if more security is needed, block can be 64×64.

(2) Decryption

Decryption includes three steps: first makes 32×32 block DCT transformation for data encryption, then makes matrix multiplication operation to the block using public key, finally makes reverse block DCT transformation. Total computing complexity is

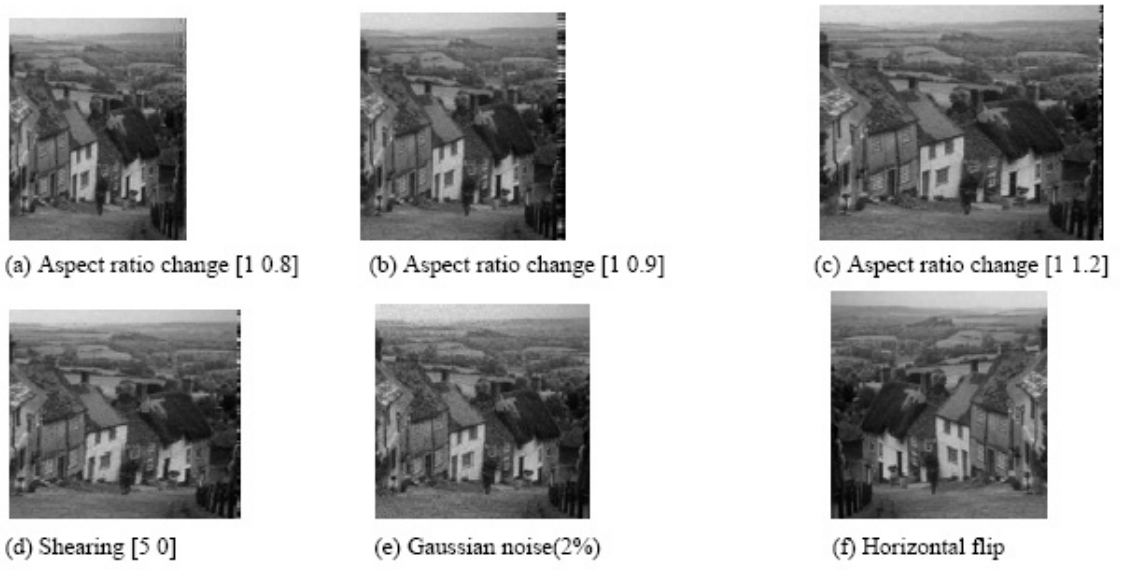

Fig.5: *Decrypted results under other attacks*

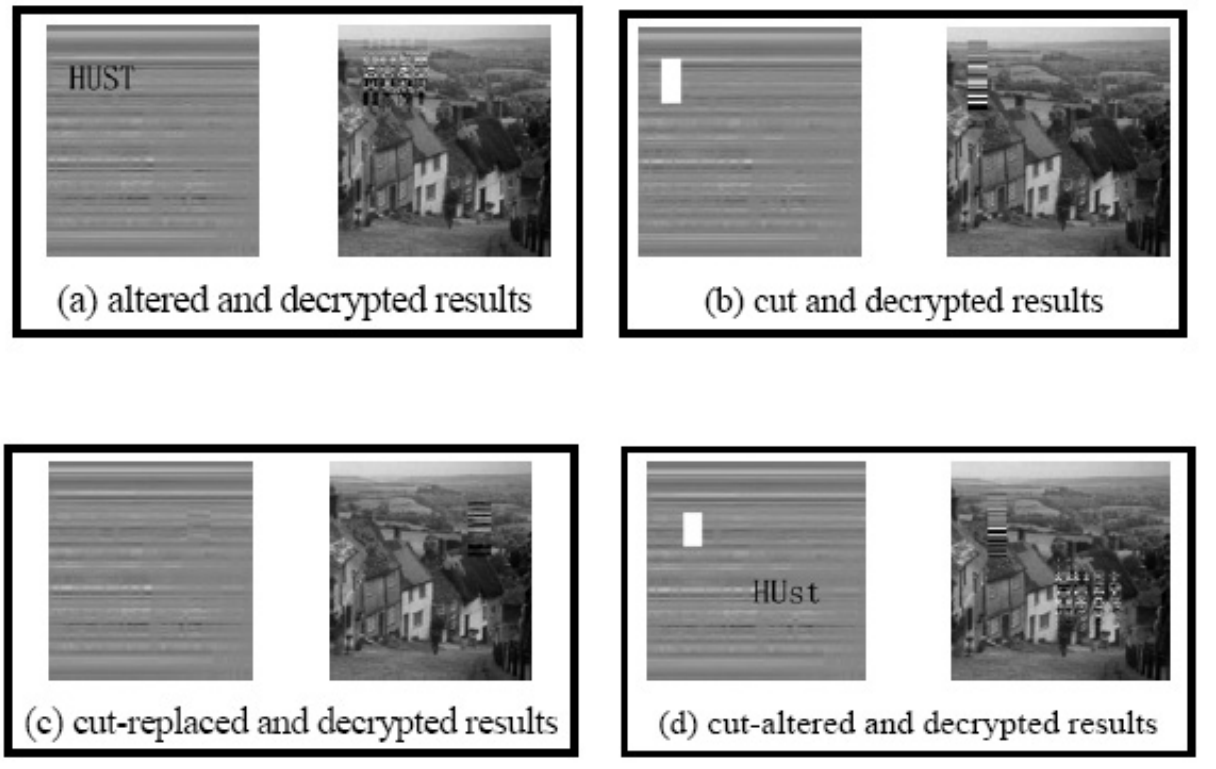

Fig.6: *Altered, cut and decrypted results*

$O\left(5N^2\right) + O\left(32^2\right) * \left[\frac{N^2}{1024}\right] + O\left(5N^2\right) = O\left(11N^2\right)$. As public key has been created during encryption, public key computing complexity is excluded from decryption.

7. EXPERIMENTAL RESULTS

Several experiments were conducted to test various properties of the proposed image encryption method which include pixel rearrangement, confusion, and diffusion properties, robustness against JPEG lossy compression and under attacks. In this paper, we test many images for validating the secure 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 de-

crypted image with wrong public key is shown.

For testing the effect of different A and U to the decryption result, we make three types of treatments: (1) U changed only; (2) A changed only; (3) A and U changed. The results are shown in Fig.2.

From Fig.2, we can find that A affects the decryption result more heavily than U, so we should apply different A to every $P \times P$ block, not U, which may be correlative that A is not orthonormal.

Fig.3 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 accords for Gaussian distribution, which is similar to noise and keeps better secrete effect against the statistical attack.

In fact, the proposed scheme is very robust against JPEG lossy compression. The decrypted results under different JPEG compression quality are shown in Fig.4. Fig.4 (d) shows that only format conversion from bmp to JPG does almost not influence the decrypted result.

In Fig.5, 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).

Another advantage of the proposed schema is good property of localization for the possible changed region. The locations of modified region are shown in Fig.6.

8. 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 resist from various image processing and vicious attacks, allows the acceptable JPEG lossy compression and good property oflocal ization for the possible changed region.

As an initial asymmetric scheme for image encryption, there are certainly some limitations. For example, the error result of image decryption in Fig 1 still leaves behind a little of original contour, but this may be solved by a kind of self-definition scrambling method. Meanwhile, the security degree of encryption method has room to improve.

Acknowledgment

This paper is granted by National High Technology Project (2004AA050) and Key Science and Technology Project, Fujian Province (2004HZ02).

References

[1] Yi Kai-Xiang and Sun Xing et al.,"An image encryption algrithm based on chaotic sequences," *Journal of Computer Aided Design and Computer Graphics*, Vol. 12, No. 9, pp. 672-676, 2000.

[2] Schwartz C.,"A new graphical method for encryption of computer data," *Cryptologia*, Vol. 15, No. 1, pp. 43-46, 1991.

[3] Bourbakis N. and Alexopoulos C.,"A Picture data encryption using SCAN patterns," *Pattern Recognition*, Vol. 25, No. 6, pp. 567-581, 1992.

[4] Kou C. J.,"Novel image encryption technique and its application in progressive transmission," *J.Electron. Imaging*, Vol. 2, No. 4, pp. 345-351, 1993.

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

[6] Chang C. C., Hwang M. S., and Chen T. S.,"A new encryption algorithm for image cryptosystems," *The Journal of Systems and Software*, Vol. 5, No. 7, pp. 83-91, 2001.

[7] T. Chuang and J. Lin,"A new multiresolution approach to still image encryption," *Pattern Recognition Image Anal.*, Vol. 9, No. 3, pp. 431-436, 1999.

[8] Jinn-Ke Jan and Yuh-Min Tseng,"On the security of image encryption," *Information Processing Letter*, Vol. 60, No. 5, pp. 261-265, 1996.

[9] B. Schneier, Applied Cryptography, Wiley, New York, 1993.

[10] G. Brassard, Modern Cryptology, Springer, New York, 1988.

[11] S. Landau, Standing the test of time: the data encryption standard, Notices of American Mathematical Society, pp. 341-349, 2000.

[12] S. S. Maniccama and N. G. Bourbakis,"Image and video encryption using SCAN patterns," *Pattern Recognition*, Vol. 37, No. 4, pp. 725-737, 2004.

Shui-hua Han received his M.S. and Ph.D. in Computer Software from Huazhong University of Sci & Tech. Currently, he is a associate professor of Information Systems, Department of Management Science, at Xiamen University Business School. His research interest focus in the area of e-commerce, information/image retrieval, and information security.

Shuang-Yuan Yang received his M.S. and Ph.D. in Computer Software from Huazhong University of Sci & Tech. Currently, he is a postdoctor of Xiamen University Business School. His main research interests are in the area of multimedia information security and watermark technology.