Complexity Analysis of Image Encryption Technique

***Anil Kumar Yadav and Ravinder Kumar Purwar*[1]**

Department of Computer Application University, Institute of Engineering & Technology,
Chhatrapati Shahu Ji Maharaj University, Kanpur
[1]School of Information Technology, Guru Gobind Singh Indraprastha University, Delhi
E-mail : yadanil@gmail.com, kpravi24@rediffmaill.com

ABSTRACT

In the digital world, security is an important issue, and encryption is one of the ways to ensure security. There are many image encryption schemes have been proposed, each one of them has its strength and weakness. This paper presents complexity analysis of image encryption/decryption scheme.[1]. The proposed scheme is especially useful for encryption of large amounts of data, such as digital images. First, a pair of keys is 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. The salient features of the proposed image encryption method are loss-less, symmetric private key encryption, a very large number of secret keys, and key-dependent pixel value replacement.[2]

Keywords: *Image processing, Matrix transformation, image encryption and decryption.*

1. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, and military communication. However, Images are different from text. Although we may use the traditional cryptosystems (such as RSA and DES) to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always greater than that of text[8]. Therefore, traditional cryptosystems need much time to 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 data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable. The main idea behind the present work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement[8]-[9].

In order to transmit secret images to other people, a variety of encryption schemes have been proposed. Schemes that we analyze here can be classified into three major types: position permutation [4]-[5], value transformation [1]-[2]-[3]-[6] and visual transformation [4].A study of image compression is becoming more important since an uncompressed image requires a large amount of storage space and high transmission bandwidth noise. 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 rest of the paper is as follows. Section 2 surveys some related image cryptosystems. Section 3 gives 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. Section 5, we discuss the relationship between public key and private key and analyze how to ensure their security. Section 6 describes Computing complexity. Experimental results and conclusions are given in section 7 and section 8, respectively.

2. RELATED IMAGE CRYPTOSYSTEMS

According to the differences between image and text, recently there have been several innovative encryption techniques

2.1 A Technique for Image Encryption using Digital Signatures

Aloka Sinha and Kehar Singh [1] have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

2.2 Lossless Image Compression and Encryption Using SCAN

S.S. Maniccam and N.G. Bourbakis [2] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves.

2.3 A new Image encryption algorithm based on vector quantization

C-C Chang (2001) [3] 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

2.4 A New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture

Jiun-In Guo and Jui-Cheng Yen [4] have presented an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm consists of 7 steps. Step-1 determines a 1-D chaotic system and its sequence from chaotic system. Steps-4,5,6, and 7 rearrange image pixels using swap function according to the binary sequence.

2.5 A New Chaotic Image Encryption Algorithm

Jui-Cheng Yen and Jiun-In Guo [5] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point *x(0)*, row size *M* and column size *N* of the image *f*, iteration number *no*, and constants *Á*, *?*, and µ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels.

2.6 Color Image Encryption Using Double Random Phase Encoding

Shuqun Zhang and Mohammad A. Karim [6] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green- Blue) formats.

2.7 Visual Cryptography for Color Images

Visual cryptography uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Young-Chang Hou [7] have proposed three methods for visual cryptography.

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). 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[8]:

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 grade 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 & DECRYPTING

We consider encrypting the grayscale image, named as $I_{M\times N}$ (To RGB image, using its luminance space). The complete 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×P blocks and transforming them into DCT domain.

Step3: Using the private key to encrypt the frontal K × K coefficients of P×P every block.

Step 4: Making the inverse DCT transformation and uniting all P × 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, . ..K$\}$ of length P and an invertible matrix A of size P ×P by using the method of [7]. $\{u_i\}$ forms the column vector of U, defined as:

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

$$[U]=\{u_i\}=\begin{bmatrix} u_{11} & a_{12} & ..... & a_{1K} \\ u_{21} & K_{22} & ..... & a_{2K} \\ . & . & . & . \\ . & . & . & . \\ u_{P1} & a_{P2} & ...... & a_{PP} \end{bmatrix}$$

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:

4.1 Encryption

Step 1: Dividing original image into distinct P × 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 P]) ...(2)

Step 2: Encrypting the frontal K×K coefficients of every P×P block, respectively. Let X1 denotes the matrix composed by the frontal K ×K coefficients of certain P ×P block X0, the corresponding encryption formula by using the private key AU can be described as:

X_2 = AUX1 ...(3)

Step 3: Replacing the frontal P × K coefficients of X_0 with X_2 € $R^{P\times K}$. If K is close to P, according to the characteristic of DCT coefficients, the rest (P - K) × (P - K) 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= i = P, 1 = j= K} ...(4)

Step 4: Making the inverse DCT transformation and uniting all P ×P blocks, the final result is defined as

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

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

% Get the minimum of $X2_{M\times N}$ named as Min

i.e Min = max((-1) x $X2_{M\times N}$

% Ensure all the coefficient of $X2_{M\times N}$ more than 0

i.e $X2_{M\times N} = X2_{M\times N +Min}$

% Get the maximum of updated $X2_{M\times N}$ named as Max

i.e Max =max($X2_{M\times N}$)

% Ensure all the coefficient of $X2_{M\times N}$ less than 1

i.e $X2_{M\times N} = X2_{M\times N / Max}$ ... (6)

Step 6: Saving the encrypted image as bmp file.

4.2 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[6]:

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

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

Step 2: Applying DCT transformation to each distinct P × P block of X3 $_{M\times N}$

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

Step 3: Decrypting the frontal P ×K coefficients of every P × P block, respectively.

Let D1 denotes the matrix composed by P ×K coefficients of certain P×P block D0, the corresponding decryption data D2 2 RK×K by using the public key A^{-t} U can be given as following:

$$\Rightarrow \ D_2 = (A^{-t}U)^t D_1$$

$$\Rightarrow \ D_2 = (U^t A^{-1})\,(AU)\,X_0 \quad ...(9)$$

$$\Rightarrow \ D_2 = (U^t U)\,X_0$$

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

$$\Rightarrow \ D_2 = X_0 \quad ...(10)$$

Step 4: Replacing the frontal P × K coefficients of D0 with D2 and 0.

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

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

$$X5_{M\times N} = I\ DCT\,(X4_{M\times N}) \quad ...(12)$$

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 × 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 € R $^{P\times P}$, and U € 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 $UU^t = U^tU = E$ As using the following matrix transformation [7]:

$$\Rightarrow \ (A^{-t}\,U)\ \ (A^{-t}\,U)^{\,t} = (A^{-t}U)\ \ (U^t\ A^{-1})$$

$$\Rightarrow \ = A^{-t}\,(UU^t)\,A^{-1}$$

$$\Rightarrow \ = A^{-t}\,A^{-1}$$

$$\Rightarrow \ = (AA^{\,t})^{\,-1} \quad ...(13)$$

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

$$AU = A\,A^t\,(A^{-t}\,U) \quad ...(14)$$

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

$$(A^{-t}U)\ \ (A^{-t}\,U)^{\,t} = A^{-t}\,Q\,A^{-1} \quad ...(15)$$

From the view of matrix theory, it is 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 64 in this paper. For K, to obtain enough coefficients, K should be ensured between P/2 and P. In this paper, it is 56.

6. COMPUTING COMPLEXITY

6.1 Encryption

Image encryption includes three steps: first makes 64×64 block DCT transformation to original image, then creates a pair of private key and public key for each 64×64 block, and then makes matrix multiplication operation to the block using private key, finally makes reverse block DCT transformation.

Let us consider I mage size is N×N then image can be split into [N/64× N /64] = [N^2/4096] blocks, each block computing complexity is O (64^2 $\log_2 64$), total computing complexity of block DCT transformation is O($64^2 \log_2 64$)*[N^2/4096] = O(5N^2). Private key computing complexity for each 64×64 block is O(64^2). Public key computing complexity for each 64×64 block is (O(64^3) * O(64^2) = O(64^5). So sum complexity for a pair of keys is O(64^5)+ O(64^2) *[N^2/4096] = O(64^3 + 1)N^2)). Matrix multiplication for each 64×64 blocks is O(64^2)*[N^2/4096] = O(N^2). In the same way, reverse block DCT transformation is O (5N^2). The computing complexity for all image encryption is:

$$O(5 N^2)+ O(643 + 1) N^2)+ O (N^2)+ O(5 N^2)$$

$$= O(643 + 12) N^2.$$

We can make out that, when DCT block is 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, 64×64 block is chosen, if more security is needed, block can be 128 × 128.

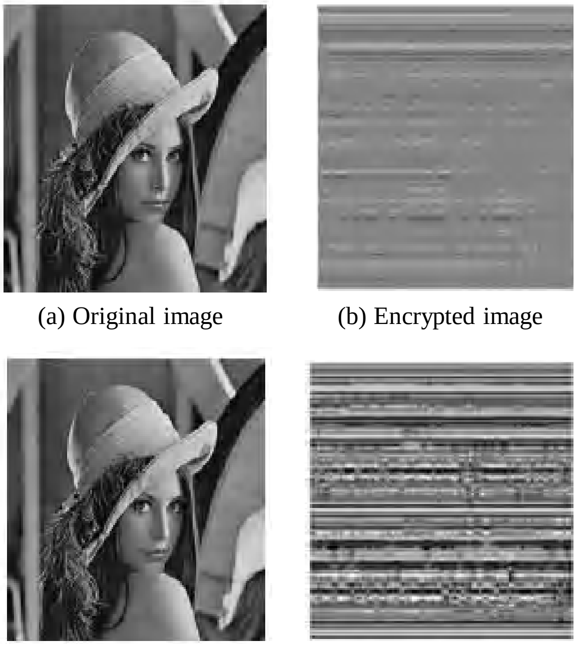
6.2 Decryption

Decryption includes three steps: first makes 64 × 64 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:

O (5 N^2)+ O(64^2) * [N^2/4096] + O (5 N^2) = O(11 N^2). As public key has been created during encryption, public key computing complexity is excluded from decryption.

7. SIMULATION RESULTS

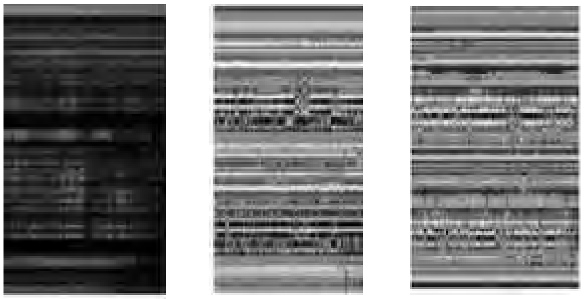
Several simulations were conducted to illustrate various properties of the proposed matrix transformation based image encryption/decryption system that includes pixel rearrangement, confusion, and diffusion properties, in experiment all images are of 512 X 512. The original image is presented in Fig.1 (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. 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. 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,



(a) Original image (b) Encrypted image

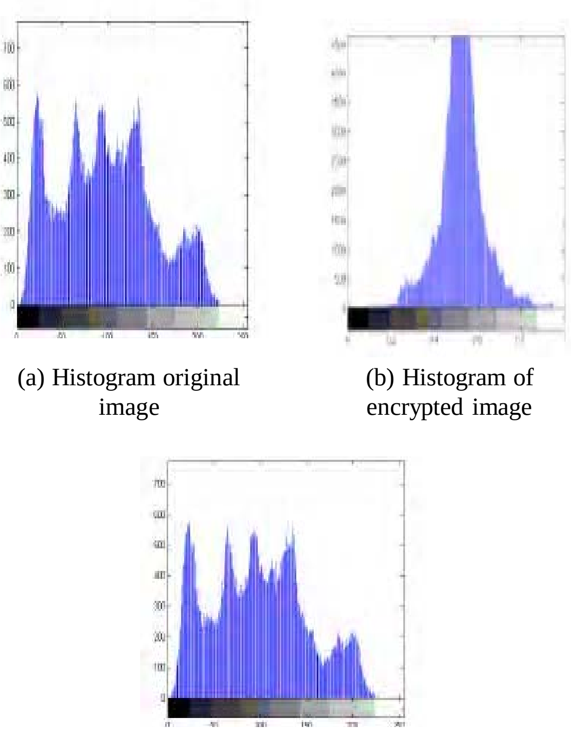
(c) Decrypted image key (d) Decrypted image with wrong

Fig. 1: Results of encryption and decryption



(a) U changed only changed (b) A changed only (c) A & U

Fig 2. Decryption with different key(s)



(a) Histogram original image

(b) Histogram of encrypted image

(c) Histogram of decrypted image

Fig. 3: Histogram original, encrypted and decrypted image

it can scramble the greyscales and frequency domain[10].Another advantage of the proposed schema is good property of localization for the possible changed region.

8. CONCLUSION

We presented a new image encryption/decryption scheme based on matrix transformation in this paper. The salient features of the proposed asymmetric image encryption scheme can be summarized as: (a) Loss-less encryption of image. (b) Less computational complexity.(c) Convenient realization.(d) Choosing a suitable size of matrix according to the size of image.(e) Encryption/decryption scheme uses integer arithmetic and logic operations. It requires minimized computational resources.

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.

REFERENCES

1. Aloha Sinha, Kehar Singh, “A technique for image encryption using digital signature”, Optics Communications, 2003, 1-6. www.elsevier.com/locate/optcom
2. S.S.Maniccam, N.G. Bourbakis, “Lossless image compression and encryption using SCAN”, Pattern Recognition 34 (2001), 1229-1245
3. Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, “A new encription algorithm for image cryptosystems”, The Journal of Systems and Software 58 (2001), 83-91
4. Jiun-In Guo, Jui-Cheng Yen, “A new mirror-like image encryption algorithm and its VLSI architecture”, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China
5. Jui-Cheng Yen, Jiun-In Guo, “A new chaotic image encryption algorithm“,Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.
6. Shuqun Zhang and Mohammed A. Karim, “Color image encryption using double random phase encoding”, MICROWAVE AND OPTICAL TECHNOLOGY LETTERS / Vol. 21, No. 5, June 5 1999, 318-322
7. Young-Chang Hou, “Visual cryptography for color images”.
8. Mitra, Rao and Prasanna, “A new image encryption approach using combinational permutation techniques” International Journal of Computer Science,vol.I,725-727.
9. Maniccam and Bourbakis, “Image and video encryption using SCAN patterns” Pattern Recoginition,725-737.
10. Yas A. Alsultanny, “Image encryption by cipher feedback mode”,ICIC International journal vol 3,589-596.