A REVIEW STUDY ON VARIOUS DIGITAL IMAGE ENCRYPTION TECHNIQUES

Amandeep Kaur [1], Gurjit Singh[2]

[1]M.Tech Scholar Electronics and Communication & Engineering Department
Amritsar College of Engineering and Technology, Amritsar
[2] Asst. Prof. Amritsar College of Engineering and Technology, Amritsar
Amritsar College of Engineering and Technology, Amritsar

ABSTRACT

This paper proposed easy algorithm to encode and decode the grey level image base on the random number generation. The image encode by changing the position of every pixel in the original image without changing the value of grey level. the original image reads row by row pixel by pixel every pixel can take a brand new position in encode image. The new position selected based on random number generation from the random number generators. The key can generate throughout the encoding process. The key which will used to decode image, it'll generate as a matrix. The key saves the position of every pixel in encode image. The encrypted image can decode by using the key. every pixel in encode image return back to its first position in decode image position that saved in key then the decode image builds. The function "Rand" in Matlab is used to generate the random numbers that need to scramble The Image.

Keyword: Decrypt Image, Grey Level Image, Image Scrambling, Image Encryption, Random Number Generation.

I INTRODUCTION

The importance of digital image security enhanced particularly after the networking, internet development and fashionable communication media. Several decoding algorithms studied to develop processes of encoding and decoding [1]. In internet there are a lot of weakness points of attack and the information these transfers throw the network need to be secret and guarded against the attacker [2]. The encoding of {data |of knowledge |of information} is used to transmit data in safety method through the internet and networks [3]. Several research used completely different algorithm have been proposed in image encoding in last 20 years [6]. Encoding of images means that build the image one thing that not understanding or not easy to understand [8]. If the hacker catches the image he/she won't know what this image. The image encoding uses 2 basic methods: replacement methods or scrambling methods. the first one is changing the value of the pixel in the original image. The scrambling is dynamic the position of the pel in original image that build the first image tough to recognize by an attacker. the only user who has the key will access the content of the original image and may reconstruct the first image. Scrambling methods based on permuting coordinates of pixels. this type of methods typically uses the following steps to scramble an image: (1) construct a matrix with a similar size of the image to be scrambled (the matrix size is denoted as s) and each part in it's assigned completely different natural number from 0 to s-1; (2) the generated matrix is mapped to the image matrix row by row and column by column, where each element's value within the generated matrix is as the coordinate of the corresponding pixel in image matrix; (3) move each pixel to the next position, if the mapped pixel coordinate is x, then move the pixel into the position with the mapped coordinate (x+1) mod s. In these methods, the key step is to generate a matrix as Coordinate shifting path. [4].Image is scrambling disarrange pixel position or pixel color order to create it unrecognizable and finding the algorithm to construct the original image. [5] 2 kinds of scrambling one base on 2nd matrix transformation and alternative is based on 2nd Arnold transformation [7].Many researchers are learning the various ways that and techniques that be wont to encode the image [6]. In this paper new technique has been suggested to encode a grey level value image by using transportation technique and scrambling the image pixel.

II CRYPTOGRAPHY

The many schemes used for enciphering constitute the area of study known as cryptography [9].

There are three types of cryptography:

2.1Secret Key Cryptography

This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption

The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption. [9]

2.2 Public Key Cryptography

This type of cryptography technique involves two key crypto system in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption.

In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob's public key and Bob can decrypt the message with its private key[9]

2.3 Hash Functions

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus.

Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information Therefore it's very important to protect our image from unauthorized access.[9]

III AES ALGORITHM

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES simply permits a 128 bit data length which will be divided into four basic operation blocks. These blocks operate array of bytes and organized as a 4×4 matrix that's known as the state. For full encoding, the data is passed through Nr rounds (Nr = 10, 12, 14) [10]. These rounds are governed by the following transformations:

(i) Bytesub transformation: is a non linear byte Substitution, using a substation table (s-box), that is constructed by multiplicative inverse and affine transformation. The Fig.1 shows the step of the Bytesub transformation.[10]

(ii) Shiftrows transformation: could be a easy byte transposition, the bytes within the last 3 rows of the state are cyclically shifted; the offset of the left shift varies from one to 3 bytes.

(iii) Mixcolumns transformation: Is similar to a matrix multiplication of columns of the states. Every column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials instead of numbers.

(iv) Addroundkey transformation: could be a simple XOR between the working state and the roundkey. This transformation is its own inverse.

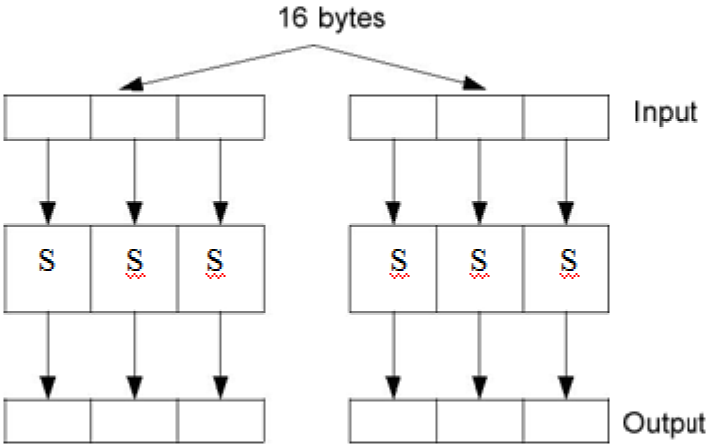


Fig. 1 Block diagrams for Substitution

The encoding procedure consists of many steps as shown by Fig. 2. After an initial add round key, a round function is applied to the data block (consisting of byte sub, shift rows, mix columns and add round key transformation, respectively). It's performed iteratively (Nr times) looking on the key length. The decoding structure has exactly the same sequence of transformations because the one within the encoding structure. The transformations Inv-Byte sub, the Inv-Shift rows, the Inv-Mix columns, and the Add round key allow the form of the key schedules to be identical for encoding and decoding.[10]

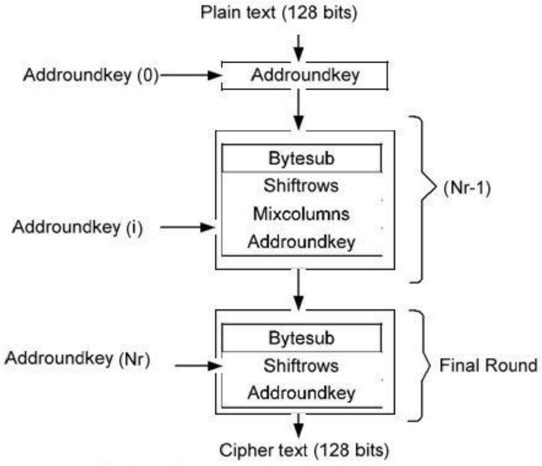


Fig. 2 AES algorithm- Encryption Structure

IV SECURITY ANALYSIS BY STATISTICAL APPROACH

A good encoding scheme should resist all types of known attacks, such as known-plain-text attack, cipher-text attack, statistical attack, differential attack, and various brute-force attacks. Some security analysis techniques perform on the AES image encoding scheme, as well as the statistical analysis and key space analysis.

4.1 Statistical Analysis

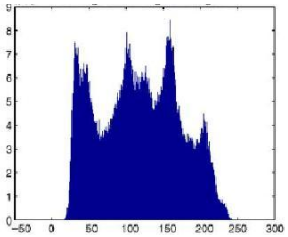
Shannon suggested 2 ways of diffusion and confusion in order to frustrate the powerful attacks based on statistical analysis [12]. statistical analysis has been performed on the AES, demonstrating its superior confusion and diffusion properties that strongly defend against statistical attacks. this can be shown by a test on the histograms of the enciphered image and on the correlation of adjacent pixels in the ciphered image.

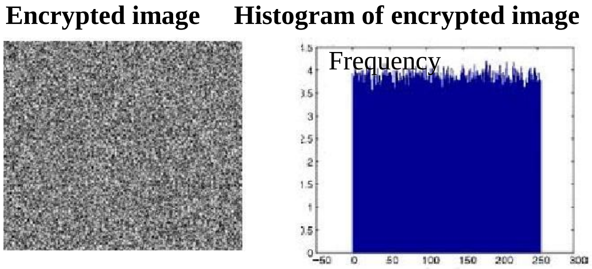
4.1.1 Histograms of Encrypted pictures

We choose many grey- scale pictures (256×256) having completely different contents, and that we calculate their histograms. One typical example among them is shown in Fig. 3. we can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Therefore, it doesn't give any indication to employ any statistical attack on the image under consideration. Moreover, there's no loss of image quality after performing the encryption/decryption steps [11].

Original image

Histogram of original image





Encrypted image   Histogram of encrypted image

Fig. 3 Histograms of the plain image and ciphered image

4.1.2 Correlation of Two Adjacent Pixels

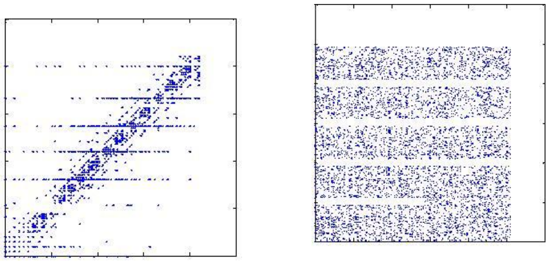
We test the correlation between 2 vertically adjacent pixels, and two horizontally adjacent pixels respectively, in a ciphered image. First, we randomly choose n pairs of 2 adjacent pixels from a picture. Then, we calculate the correlation coefficient of every pair by using the following formula.

$$\mathrm{cov}(x,y) = E(x – E(x))(y – E(y)) \qquad (1)$$

Where x and y are grey-scale values of 2 adjacent pixels within the image. Figs. 4(a)-(b) show the correlation distribution of 2 horizontally adjacent pixels within the plain-image and within the ciphered image, respectively.

4.2 Key space Analysis

A good encoding scheme should be sensitive to the secret keys, and the key space should be large enough to create brute-force attacks infeasible [13]. In our case, the key space size is 10128. it is large enough to resist at all kind of brute-force attacks. The experimental results additionally demonstrate that AES is extremely sensitive to the secret key. Table I illustrates the sensitivity of AES to the secret key. Fig. 4(a) shows Lena-image encrypted using totally different. As may be seen once the key is modified slightly the encrypted image becomes absolutely different.



4(a)   4(b)

Fig.4 Correlation of two horizontally adjacent pixels; 4(a) in the plain-image, and 4(b) in the ciphered-image

V CONCLUSION

This algorithm is used to encode and decode the grey level image. It reads the initial image, then scrambling the pixel position the scrambling methods base on random number generation. . The key's represented in a one dimensional array for row and one dimensional array of columns. The decode image is clear without any noise. The algorithm is implemented with success for various image size and types.

REFERENCES

[1] Li. Shujun, X. Zheng, "Cryptanalysis of a chaotic imageencryption method," Circuits and Systems, IEEE International Symposium on ,Vol.2) , pp.708-711, may. 2002.

[2] V.V.Divya, S.K.Sudha and V.R.Resmy ,” Simple and Secure Image Encryption” International Journal of Computer Science Issues, Vol. 9, pp. 186-289, November .2012.

[3] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya” A Survey On Different Image Encryption and Decryption Techniques.” International Journal of Computer Science and Information Technologies, Vol. 4, pp.113-116 , February. 2013.

[4] S.Liping,Qin, Z. Liu Bo, Q. Jun, L.Huan,” Image Scrambling Algorithm Based on Random Shuffling Strategy”3rd IEEE Conference on Industrial Electronics and Applications, 2008,pp. 2278 – 2283.

[5] ZHAO Xue-feng, Digital image scrambling based on the baker’s transformation. Journal of Northwest Normal.

[6] R. Rhine, N.Bhuvan, “Image Scrambling Methods for Image Hiding: A Survey”, International Journal of Computer Science and Network Security, vol.15, pp.86-91, February .2015.

[7] D.X. Qi, “Matrix Transformation and Its Applications to Image Hiding,” Journal of North China University of technology, Vol. 11, pp. 24-28, 1999.

[8] M. Al-Husainy, “A Novel Encryption Method for Image Security” International Journal of Security and Its Applications,vol. 6 ,January. 2012.

[9] Rajinder Kaur, Er.Kanwalprit Singh, Image Encryption Techniques:A Selected Review,” IOSR Journal of Computer Engineering, ISSN: 2278-8727, Vol. 9, pp. 80-83, 2013.

[10] J. Daemen, V. Rijmen, "The block cipher Rijindael", Proceedings of the Third International Conference on smart card Research and Applications, CARDIS’98, Lecture Notes in computer Science, vol.1820, Springer, Berlin, 2000, pp.277_284.

[11] J.J. Amador, R. W.Green “Symmetric-Key Block Cipher for Image and Text Cryptography”: International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.

[12] C.E. Shannon, “Communication theory of secrecy system", Bell syst Tech,, 1949; 28; 656-715.

[13] H. Gilbert, M. Minier, “A collision attack on 7 rounds of Rijndael”, In The third Advanced Encryption Standard Candidate Conference, pages 230– 241, NIST, April 2000.