ISSN No. 0976-5697

Volume 6, No. 6, July - August 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Image Encryption Technique for Wireless Network

Kakali Chatterjee
Department of Computer Science and Engineering
National Institute of technology Patna

Abstract: Wireless Networks are now extensively used to transmit critical image data relating to area monitoring in defence organizations. Encryption plays an important role in such networks as the image data collected by the devices need to be encrypted before transmitting to neighbouring nodes and base stations for further processing. Image encryption is necessary to protect image data, but very challenging in such networks as the devices have constrained in terms of memory and processing speed. In this paper, an image encryption technique is proposed using threshold technique for sharing the image. The technique is used to produce two or more shares of any image. After that simple block transformation is used for encryption of the shares and then concatenate the encrypted shares to produce a single image. Experimental result shows that, this encrypted image has high entropy and low correlation coefficient, so from this encrypted image it is more difficult to understand the original image.

Keywords :Image Encryption, Correlation, Threshold Cryptography, Information Entropy

I. INTRODUCTION

A major issue in wireless networks is tomaintain confidentialityof important information.Internet is widely used in such networks and the information transmitted over internet is not only text, but also contains multimedia like image, audio, etc. The more extensively the image is used, the more important their security will be. For example, it is important to protect military image database, ensure confidential video conferencing and protect personal online photograph albums. Encryption is the most easy and efficient way to achieve data security by hiding the contents of a message in anintelligent way. The purpose of encryption is to prevent unauthorized useof data. Simple conventional encryption process use some substitution technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data, but cryptanalysis shows that can be easily breakable.Hence modern days two different encryption techniques are used: Symmetric Encryption which uses a single key to encrypt and decrypt the message and Asymmetric Encryption which uses two different keys – a public key to encrypt the message, and a private key to decrypt it. Currently, there are several types of symmetric key based encryption algorithms such as: DES, AES, Blowfish are used for image encryption and others but all of these algorithms depend on high mathematical manipulations. Hence performance efficiency reduces in some devices. In wireless networks, many small devices such as cell phones, PDAs etcused for communication which are constrained in terms of memory, computing power and energy supply. Due to the device constraint, it is very difficult to perform complex operation on an image file. Hence one simple and efficient way to encrypt image data is through block transformation by rotation of bits. In rotation of bits operation, the bits are moved, or shifted, to the left or to the right which reduces computational cost.

In this paper a block based transformation is proposed for high level security of image. In this technique, first the image is divided into two shares and segmented into blocks. Then a new key generation technique is used for symmetric key generation and bit shifting method for encryption. After producing the two encrypted transformed image, concatenation of these two images is performed to produce a single image which will sent through wireless media. In receiver side the reverse process is applied two get the original image. As entropy and correlation coefficient are two critical parameters to measure the security level and capability of a technique, it is also checked. The result shows that this encryption process decreases the mutual information among the encrypted image variables and thus increasing the entropy value.

The rest of the paper is organized as follows:

Section 2 presents related work, Section 3 provides proposedimage encryption technique, Section 4 presents Implementation and Performance Analysis,and finally, we conclude the paper in Section 5.

II. RELATED WORK

Wireless networks are the essential part of today's communication purpose. Different types of data (image, text) are transmitted through these networks. Many times critical digital images relating to area monitoring, environment are transmitted for further processing. Hence security of digital images has attracted more attention and many different image encryption methods have been proposed for image security.Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are encryption of binary and gray-scale images [1, 2, 3, 4, 15, 16, 17].In 2004, Maniccam *et al.* [9] proposed image encryption technique which is performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher. But Shujun Li *et al.* [13] states that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. Ozturk *et al.* [14] compared all image encryption algorithms and proposed new schemes which add compression capability. In 2005, Zhi-Hong Guan *et al.* [11] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image. To provide high security, Sinha *et al.* [12] also proposed an image encryption by using Fractional Fourier Transform (FRFT) in image bit planes. In 2006, Mitra *et al.* [10] have proposed a random combinational image encryption approach with block permutations to design highly secured images.

In 2007, Zeghid*et al.* [18] add a key stream generator (W7,A5/1) to AES for increasing the encryption performance.In 2008, Younes *et al.* [19] introduce a new permutation technique based on RijnDael. In 2010, Mohammed Amin*et al.* [20] proposed chaos-based stream cipher, composing two chaotic logistic maps and external secret key for encryption of image. In 2011, Alsafasfeh *et al.* [21] proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rossler chaotic system. In 2012, Sun*et al.* [22] designed general random scrambling method which has more stable scrambling degree than the classical method.All these techniques are useful for real-time encryption in different applications.

III. PROPOSED IMAGE ENCRYPTION TECHNIQUE

Proposed image encryption technique is shown in Fig-1. At first divide an image in two Share S1 and S2 than encrypt both E1 and E2 with proposed encryption algorithm individually. Than concatenate both encrypted imageE1||E2. This encrypted image send to receiver side and receiver side again separate it in two parts just as the sender side, and decrypt by decryption algorithm. After decryption two shares S1 and S2 will generate which will overlap to generate the original image.

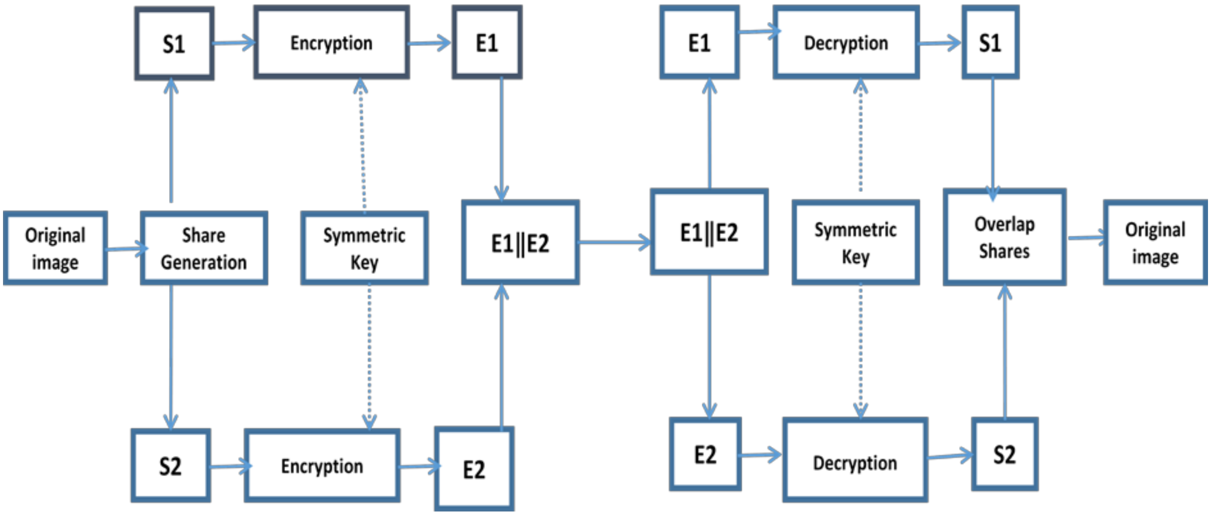

Figure 1:- The proposed technique for Image encryption

The proposed technique has three main phase as described below:

a. *Share Generation Phase:*

Breaking an image into n shares is popular in image encryption so that only receiving all n shares one can decrypt the image by overlaying each of the shares over each other[23].In this phase, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of four sub-pixels. Each pixel in the secret image is broken into four sub pixels in such that white pixel is shared into two identical blocks of four sub-pixels and black pixel is shared into two complementary blocks of four sub-pixels. Fig-2, shows the share generation process.

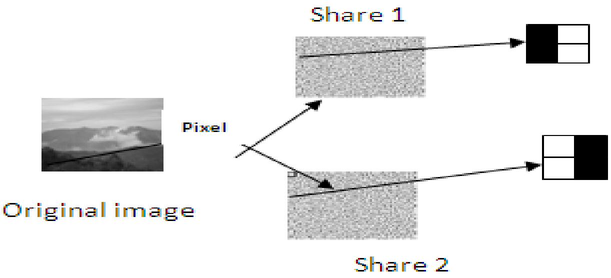

Figure 2:- Share generationProcess

HereShamir's [24] (k, n) threshold secret sharing technique is used for share generation where n is the no of shares and k is a threshold value (k≤n). The polynomial equation used to express it mathematically as follows.

$$\mathrm{F(X)} = \sum_{i=0}^{k-1} \mathrm{a_i} x^i$$

Using this technique all pixels in the original image are convertedin shares. Eachshare havingtwo black and two white sub pixels from the original image such that when two shares are joined together, the result is either medium grey (which represents white) or completely black (which represents black).

b. *Key GenerationPhase-*

The main feature of the encryption/decryption process is the generation of the encryption key. A symmetric encryption key is used for the encryption which means the same key is shared for both encryption and decryption. But here only three random no will transmit. Sender and receiver separately will follow the same process given in Fig 3. for symmetric key generation.

The technique of generating the key uses three methods: random number generation, swapping and combination. First, a long number (10 decimals) called A is generated. Consider another long number (20 characters) called B andgenerated so that the size of B is twice the size of A. Another number (30 decimals) called C is also randomly generated and these three values (A, B, C) is transmitted from sender to receiver. The both sender and receiver will follow the steps of key generation phase given below.

Step I: First an insertion operation is performed such that each digit of A is inserted after two characters of B. The result of the insertion is called key K1 having 30 values

Step II: Now it divided into two halves. Swapping operation is performed so that the left half is become right half and right one will become left half.

Step III: Then two halves will rejoined to form new K1.

Step IV: After that C is combined with K1 by replacing alternately one character or digit from K1 with a digit from C. The result of the combination is a relatively strong key K2.

Step V: Now an odd and even partitioning is performed on the resultant key K2. The position of each character/no in the key decides it to be an even or an odd. For example, the character at position 0 is an even one while the character at position 1 is an odd character. In this way all 30 values are separated.

Step VI: The even part of the key is combined together and the odd part of the key is combined together.

Step VII: Finally, the two parts of the key are joined. Since the final key is a key that consists of all characters and integers, so another key with binary ASCII values is obtained. The result is a very long key of size 30 bytes.

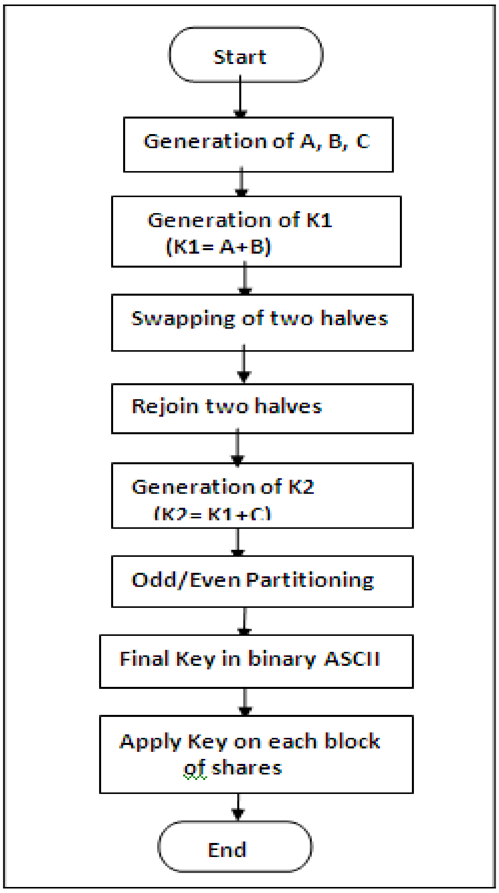

Figure 3: Flow Chart of key Generation

c. *Encryption Phase-*

For the Encryption/decryption each share image is decomposed into 30×30 blocks. Actually increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. Each block size is (10×10) pixel.Each block has a position. The blocks are transformed into new locations applying the encryption rule. We will shift the blocks using three steps:

Step I- If the first bit in the key stream is0 that means a circular rotation of block to the left is performed and it will move to the left.

Step II- Now the each block will get new position and then apply the key on the next block.\

Step III- If the next bit in the key stream is 1 that means a rotation of block to the right is performed and the block will be moved to the right.

Due to this process, the correlation between the blocks will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbours. Furthermore, this process of dividing and shuffling the positions of image blocks will increase the confusion between the original image and the generated one. Now the output images (encrypted share) are compressed and concatenated to produce a single image of same size.

```
ALGORITHM FOR ENCRYPTION
INPUT: Share Image (BMP image file)
OUTPUT: Encrypted Images
1.   Load the share image
2: Input secret key
3: Get the Width and Height of the image
4: Decompose the input image into Blocks
4.1: Lower Horizontal Number of Blocks =Image Width / 10
4.2: Lower Vertical Number of Blocks =Image Height /10
5: Total Number of Blocks = Total Horizontal Blocks × Total Vertical Blocks
6: Initialize variable
7. Randomize ()
8: For I = 0 to Number of Blocks -1
8.1: Do the rotation of block I from the
   Ist bit value of the Key
8.2: Set block I in its new location
END
```

IV. IMPLEMENTATION AND PERFORMANCE ANALYSIS

In this section, the proposed technique is implemented using MATLAB in a laptop with Intel Core 2DUO CPU T6400@2.00GHz and 32 bit operating system.A gray-scale image of size (300 ×300) pixels is taken for experimental purposes. The results obtained are presented in Fig4.

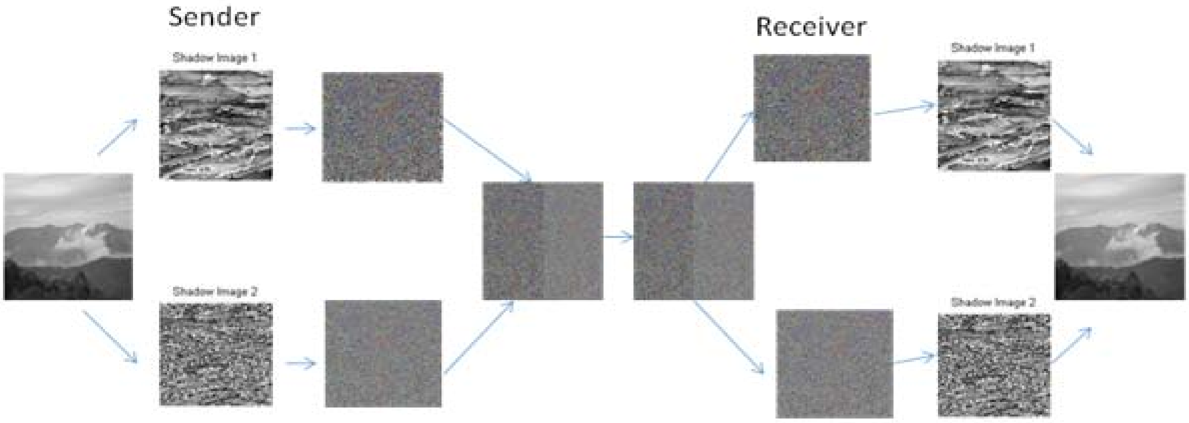

Figure 4: Implementation results of Image Encryption

The results are obtained from all three phases of proposed technique. Now for finding out the entropy and correlation thefollowing equations [18] are used

$\mathrm{H(m)} = \sum_{k=0}^{N-1} \mathrm{P(k)} \log\log_2(\mathrm{P(k)})$……………………….(1)

Where H(m): entropy

N: gray value of input image (0….255)

P(k): is the probability of occurrence of symbol *k*.

$$C(x, y) = n\sum(xy) - \sum x \sum y$$

$D(x) = n\sum(x^2)$ - $(\sum x)^2$

$D(y) = n\sum(y^2)$ - $(\sum y)^2$

For Correlation value we use the following equation

$E = \frac{\mathrm{C(x,y)}}{\sqrt{\mathrm{D(x)}}\sqrt{\mathrm{D(y)}}}$…………………(2)

and

$\sqrt{\mathrm{D(x)}} \neq 0$, $\sqrt{\mathrm{D(y)}} \neq 0$

Where x and y are gray level value of two adjacent pixels

E= The correlation value

N= the no of pairs of (x,y)

n$\sum xy$= sum of product of paired xy

$\sum x$ = sum of x data

$\sum y$= sum of y data

$\sum(x^2)$= sum of squared x data

$\sum(y^2)$ = sum of squared y data

Result of encryption of each share by using 10 pixels × 10 pixels blocks shown in Fig 5. Now correlation value and entropy is calculated for each case (A,B,C,D) using the above equations. The result of correlation value and entropy is shown in Table 1.

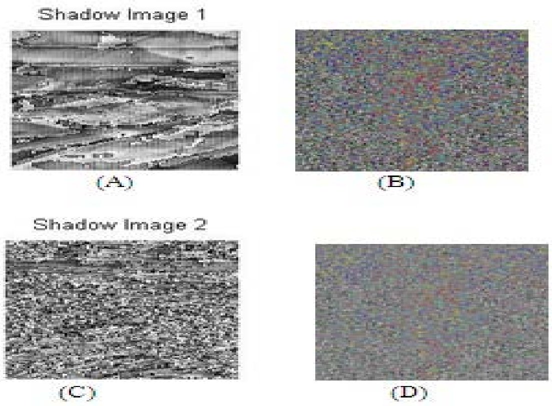

Figure-5: encrypted Images in sender side

Table 1: Results of Correlation value and Entropy

Image	Entropy	Correlation Coefficient
Plain image	7.388	0.953
Share 1(A)	2.341	0.748
Encrypted Share 1(B)	7.354	0.045
Share 2(C)	2.451	0.793
Encrypted Share 2(D)	7.243	0.034
Concatenated Image	7.297	0.039

Correlationcoefficient determines the correlation between two adjoining pixels in an image. The values of correlation coefficients in Table1, shows that the two adjacent pixels in the plain-image are highly correlated to each other and correlation coefficient (0.953) nearly 1.The values of correlation coefficients in the encrypted share images are nearly 0. This shows that the adjacent pixels in the encrypted images are highly uncorrelated to each other.

Information entropy of an encrypted image shows the distribution of gray value. If the distribution of gray value is uniform, then information entropy is very high. As we know that for a gray level image, each pixel has 8 bits, hence entropy of a gray image is equal to 8. If the information entropy of an encrypted image is significantly less than the ideal value 8, there would be a high chance of predictability which threatens the image security. The value of information entropy for the plain-image is comes out to be H(S) = 7.388. However, the values of information entropy obtained for the case of images encrypted by the proposed algorithm is H(S) = 7.297, also very close to the ideal value 8. This means that the information leakage in the proposed encryption process is negligible and the image encryption system is secure against the security attack. Also the encryption/decryption time is measured for the above image and the total process takes 590 ms for file size 17.6 KB (18,123 bytes). It shows that it can be easily implemented in handheld devices which are used in wireless networks.

V. CONCLUSION

In this paper, an image encryption technique is proposed, implemented and analyzed. This technique resists most of the network attacks such as Known key attack; Chosen cipher text only attack as the key is not transmitted. Both sides will generate key independently and at the same time strong key is generated due to confusion and diffusion.

The resultshows that the adjacent pixels in the encrypted images are highly uncorrelated to each other. Also the information entropy obtained for the case of encrypted images by the proposed algorithm is very high which implies of less chance of information leakage. This two results shows that the proposed techniques is providing high level security in wireless networks. Also this image encryption technique uses simple operations to reduce the computational load and less encryption time shows it’s performance efficiency.

VI. REFERENCES

[1]. W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," PakistanJournal of Information and Technology. Vol. 2, no. 2, 2003, pp. 191-200. http://www.ansinet.org/

[2]. M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption ofuncompressed and compressed images," In ACIVS’02, Ghent, Belgium.Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[3]. S. Changgui, B. Bharat, "An efficient MPEG video encryption algorithm, " Proceedings of the symposium on reliable distributed systems, IEEE computer society Press, 1998, pp. 381-386.

[4]. S. Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," proceedingof international conference, single processing, pattern recognition and application, 2002, pp. 25-28.

[5]. S. P. Nana'vati., P. K. panigrahi. "Wavelets:applications to image compression- I,". joined of the scientific and engineering computing, Vol. 9, no. 3, 2004, pp. 4- 10.

[6]. AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo, "Video over IP using standard-compatible multipledescription coding, " Journal of Zhejiang University- Science A, Vol. 7, no. 5 ,2006, pp. 668-676.

[7]. H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 blockcipher algorithm for digital images," Menoufia University, Department of Computer Science andEngineering, Faculty of Electronic Engineering, Menouf-32952, Egypt, 2006.

[8]. Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method,"ISCAS 2002. IEEE InternationalSymposium on Publication Date: 2002, Vol. 2, 2002, pp. 708,711.

[9]. S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," Journal ofPattern Recognition Society, Vol. 37, no. 4, pp.725– 737, 2004.

[10]. A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, pp.127-131, 2006, Available:http://www.enformatika.org

[11]. G. Zhi-Hong, H. Fangjun, and G.Wejie, "Chaos - based image encryption algorithm,"Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada.Published by: Elsevier, 2005, pp. 153-157.

[12]. A. Sinha, K. Singh, "Image encryption by using fractional Fourier transform andJigsaw transform in image bit planes," optical engineering, spie-int society opticalengineering, vol. 44, no. 5 , 2005, pp.15-18.

[13]. Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., BourbakisFellow., IEEE. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004,http://eprint.iacr. Org/2004/374.pdf

[14]. I. Ozturk, I.Sogukpinar, "Analysis andcomparison of image encryption algorithm,"Journal of transactions on engineering, computingand technology December, Vol. 3, 2004, p.38.http: //www.enformatika.org/

[15]. A. Sinha , K. Singh, "A technique for imageencryption using digital signature," Source:Opt ics Communications, Vol.218, no. 4, 2003,pp.229-234.http://www.elsevier.com/

[16]. S. S. Maniccam. , G.Nikolaos , andBourbakis, "Lossless image compression andencryption using SCAN," Journal of: Pattern Recognition,Vol. 34, no. 6: , 2001, pp.1229– 1245.

[17]. M. Sonka, V. Hlavac. and R. Boyle, "Digital imageprocessing," in: image Processing, Analysis, andMachine Vision, 1998, 2nd ed. http://www.pws.com

[18]. M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, “A Modified AES Based Algorithm for Image Encryption”, World Academy of Science, Engineering and Technology 27, 2007.

[19]. Mohammad Ali Bani Younes, Aman Jantan, “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption”, International Journal of Computer Science and Network Security, Vol.8 , April 2008.

[20]. Ismail Amr Ismail, Mohammed Amin, Hossam Diab ,”A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps”, International Journal of Network Security, Vol.11, No.1, pp.1 -10, July 2010

[21]. Qais H. Alsafasfeh , Aouda A. Arfoa, “Image Encryption Based on the General Approach for Multiple Chaotic Systems”, Journal of Signal and Information Processing, 2011.

[22]. Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, “Image Encryption Based on Bit-plane Decomposition and Random Scrambling”, Journal of Shanghai Second Polytechnic University , Vol. 09, IEEE, 2012

[23]. D.Jena and S.Jena, “A Novel Visual Cryptography Scheme”,Proceedings of International Conference on Advanced Computer Control, (ICACC’2009), pp.207-211

[24]. A Samir, “How To Share A Secret”, Communications of ACM, Vol.22, 11 (1979), pp. 612–613.