Image Encryption using Random Permutation by Different Key Size

Ravi Prakash Dewangan
M.E Scholar, Faculty of Shri Shankaracharya Group of Institution, Bhilai, India

Chandrashekhar Kamargaonkar
Associate Professor, Faculty of Engineering Shri Shankaracharya Group of Institution, Bhilai, India

ABSTRACT

Security of information is main aspect in network communication. The information may be in the form of text, voice and multimedia (Image, video). In new generation of technology peoples transmit images over an open network which is need to be secure. There are various encryption methods to secure image from unauthorized parties. In the proposed work, image is encrypted using different combination random permutation techniques. A digital image can be represented by two dimensional arrays which have numeric value called pixel and a pixel is collection of bits. The image is encrypted by various combination of bit, pixel and block permutation. We used 1-D and 2-D key for image encryption and comparing the performance of various combination of permutation on the basis of key size and encryption time. The experimental results demonstrate that large key size makes a brute force attack redundant and faster encryption speed are considered good for practical use.

Keywords:— image encryption, random permutation, Information security, key size, encryption time

INTRODUCTION:

The fastest development of cell phone and their multimedia application enhanced the need of security of multimedia information over network communication. Security of image is an important aspect in network communication. Encryption, steganography and watermarking are the techniques which can be used to provide security. Among them encryption technique gives high level of security. There are various encryption algorithms which are based on either transposition cipher or substitution cipher. Some traditional encryption scheme such as DES, AES, RSA etc. are not appropriate for image encryption. An efficient encryption technique must have certain properties like less encryption time, large no of key space, complexity, high security form different types of attacks.

There are various technique of image encryption have been developed which is based on permutation. Rong-Jian Chen, Wen-Kai Lu, and Jui-Lin Lai [1] presented encryption scheme is based on permutation of the pixels of the image and replacement of the pixel values. The permutation is done by scan patterns generated by the SCAN methodology and the pixel values are replaced using a progressive cellular automata (CA) substitution. Encryption method was loss-less, symmetric private key encryption, very large number of security keys. Li Chuanmu Hong Lianxi [4] presented image encryption scheme based on hyperchaotic map. The ergodic matrix of one hyperchaotic sequence is used to permute the image and the other one is used to confuse the relationship between cipher-image and plain-image. Yong Feng and Xinghuo Yu [6] presented image encryption approach based on the Line maps, which can perform two processes of image encryption simultaneously, permutation and substitution, using the same maps. A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna [2] presents an approach for a random combination of the permutations for image encryption, they observed that the permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation. Pareek, Patidar and Sud [3] proposed image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps. Encryption process used eight different types of operations. The secret key is modified after encrypting a block of sixteen pixels of the image.

The development of image encryption using chaotic random permutation is attracted in recent year. Our proposed work focused on the image encryption using different random permutation techniques. The basic permutation can be performed in three ways such as bit, pixel and block permutation. In this paper presented image encryption by all three basic permutations and various combination of basic permutation using different size of encryption key. A pixel in a digital image is collection of 8 bits therefore maximum available key of bit permutation is equal to 8! (40320) .The pixel permutation can be performed by shuffling the pixel position according to the encryption key and for block permutation image is divided into sub-blocks and these sub-blocks are shuffled according to the encryption key. The encryption key size can be one dimensional (1-D) or two dimensional (2-D) for pixel permutation and block permutation. 2-D key has more number of encryption key as compare to 1-D key. The encrypted image can be decrypted only if attacker has knowledge of key and large numbers of possible key spaces make it infeasible to extract the original information.

PROPOSED WORK

There are three basic permutation is possible in an image [2] which are bit, pixel and block permutation. A digital image is combination of pixels and a pixel in the image is combination of 8-bits. Bit permutation is performed by permuting bit in a pixel using encryption key. The maximum size of encryption key for bit permutation is of 8 bit therefore the maximum number of available key is equal to factorial of 8 which is not very large. The process of permuting pixel in an image according to key is known as pixel permutation. Pixel permutation can be performed in different way depending on size key, if size of key is one dimensional then we can perform row permutation and column permutation according to key and if size of key is two dimensional then pixels are place at the position according to the key. Image can be divided into sub blocks. Sub blocks are permuted in block permutation. The process of block permutation is same as pixel permutation. The size of key for pixel and block permutation is not fixed it can be chosen randomly.

In this paper we presented encryption of image using all three basic permutation technique and different combination of basic permutation technique using different key size. The block diagram of one of the combination of basic permutation using pixel and block permutation encryption is shown in Fig.1

The proposed method is shown above. First figure shows the plain image that we read. In the proposed method we first encrypt the image using pixel permutation then after we applied block permutation. The process of proposed method is explained by following steps:

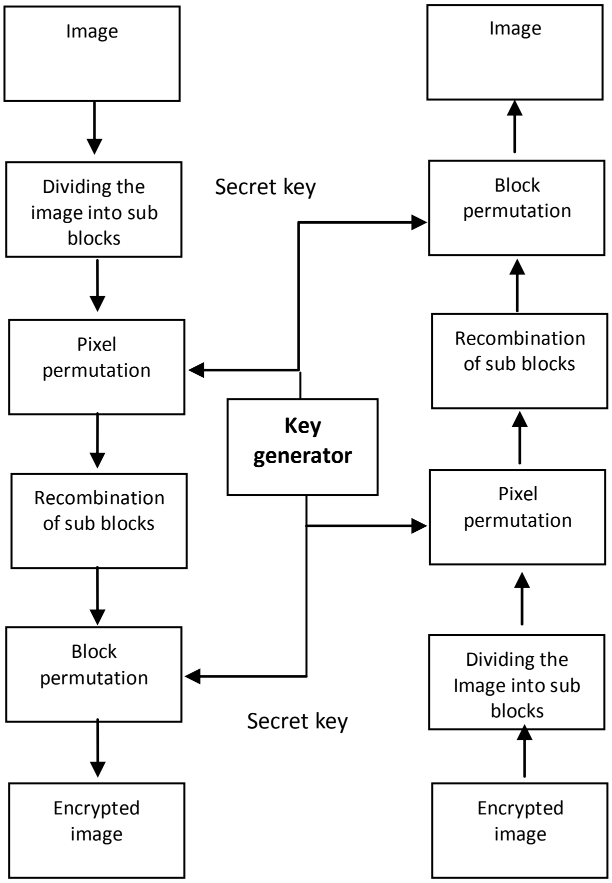


Fig.1. The general block diagram of combination of pixel and block permutation schemes

1) A 256 gray level plain image of size (M, M) is taken and decomposed it into X number of sub-blocks in a row and same number of sub-block in a column. The size of each sub-block is of (N, N) and the position number is assign to each pixel of sub-block from (1,1) to (N, N)
2) Pixel permutation is applied to the each sub-block using generated two dimensional encryption key of size (N, N). The encryption key is arrangement of random number at different position.
3) Pixel of sub-block is mapped at different position of row and column according to the key. The position of pixel can be determined by

$$r = \frac{floor\ (K_{n,n})}{N} + 1 \qquad 1$$

$$c = mod\big((K_{n,n}), N\big) \qquad 2$$

Where 'r' and 'c are row and column position at which pixel to be placed and $K_{n,n}$ is a random number at different position of key. Both above equations are only valid in the condition whenc $\neq 0$. If $c = 0$ the row position should be equal to 'r-1' and column position should be equal to 'N'. Pixel of each sub-block is placed at the position of calculated row and column position.

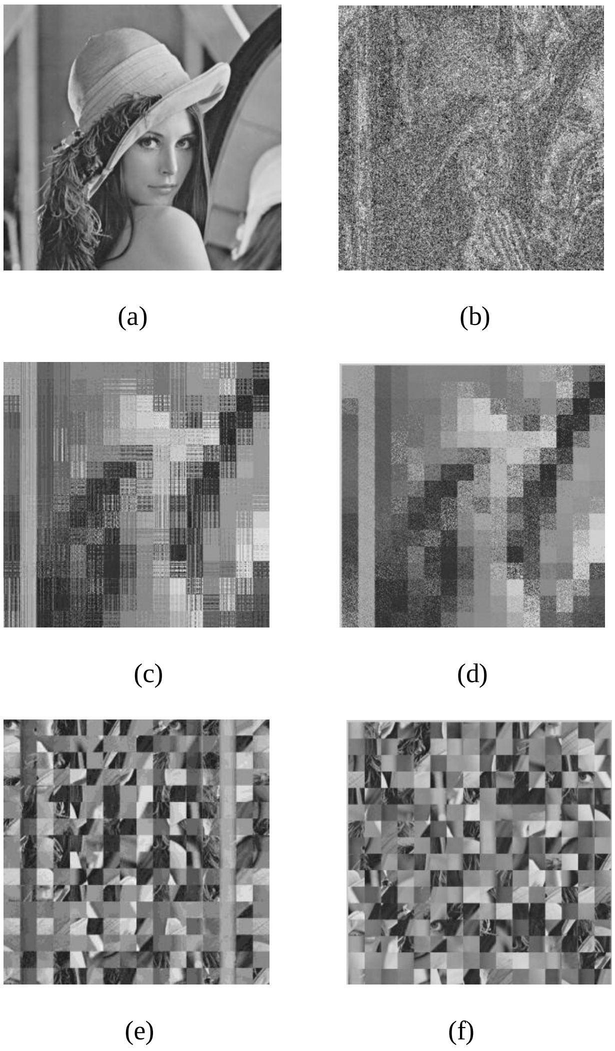
4) After pixel permutation, sub-blocks are combined and assign position number to each sub-block from row to column which starting from (1, 1) to *(X, X)*.
5) Block permutation is applied after pixel permutation using generated two dimensional key of size *(X, X)*. The process of block permutation is same as pixel permutation except the key size and block is permutated instead of pixel. Similarity we can calculate row and column position as we have done for pixel permutation and place the block at the position of calculated row and column position.

We get an encrypted image after performing pixel and block permutation using two dimensional key. The main advantage of permutation based encryption is the size of encrypted image is same as plain image. The decryption process is similar to the encryption process but key for decryption is different. In cryptography, key is an important parameter without it algorithm will not produce appropriate result. The total number of available key for pixel permutation and block permutation is equal to $N^2!$ and $X^2!$ respectively. In this paper we compare the encryption technique of image using basic permutation and combination of basic permutation. Image is encrypted using bit permutation using 8 bit key therefore maximum number of available key is equal to 8!. Image is also encrypted by pixel permutation and block permutation using 1-D and 2-D key. We also performed encryption of image using bit, pixel and block permutation. The advantage of using 2-D key over 1-D key is available number of key, total number of available key using 2-D key is equal factorial of multiplication of length of row and column and of available key using 1-D key is equal factorial of twice of length of the key.

RESULT AND ANALYSIS

Encryption performed on lena.bmp image of size 512x512 with 256 gray levels shown in Fig.2(a). Here we encrypt the image using basic permutation technique and combination of them. Image is encrypted using bit permutation using key of size 8 bit shown in Fig.2 (b).

For pixel and block permutation, image is divided it into sub-block of size 32x32 and we get 16x16 numbers of sub-locks. 1-D of length 32 and 2-D key of size 32x32 have been used for pixel permutation, the encrypted image using 1-D key and 2-D key is shown in Fig.2 (c) and Fig.2 (d) respectively. The plain image is also encrypted using block permutation using 1-D key of length 16 and 2-D key of size 16x16 individually shown in Fig.2 (e) and Fig.2 (f) respectively.


(a) (b)

(c) (d)

(e) (f)

Fig. 2. (a) Original image.
(b) Bit permutation Encrypted image.
(c) Pixel permutated image using 1-D key.
(d) Pixel permutated encrypted image using 2-D key.
(e) Block permutated encrypted image using 1-D key..
(f) Block permutation encrypted image using 2-D key

We also have encrypted the image using different combination of bit, pixel and block permutation

1) **Combination of pixel and block permutation using 1-D key**: In this combination, image is first decomposed into sub-blocks of size 32x32.pixel permutation is performed using two 1-D key of length 32, one key is used for row permutation and second key is used for column permutation of pixel. Block permutation is applied using two 1-D key of length 16.

2) **Combination of pixel and block permutation using 2-D key**: The image decomposed into sub-block similarly as we have perform in previous combination but here we used one 2-D key instead of two 1-d key for both pixel and block permutation.

3) **Combination of bit, pixel and block permutation**: In this combination, Bit permutation is first applied to the image using 8 bit key. After bit permutation, image is encrypted using pixel and block permutation using 1-D key.

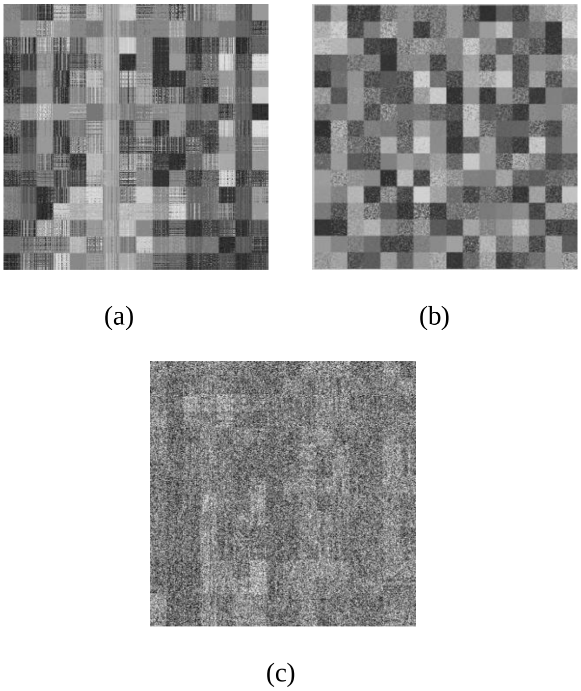


Fig.3. (a) Combination of pixel and block permutated image using 1-D key.
(b) Combination of pixel and block permutated image using 2-D key
(c) Combination of bit, pixel and block permutated image

Table (I) shows test of encryption speed of various permutation based image encryption scheme and total number of available key. A good encryption scheme should have large number of key space and fast encryption speed. We can see that bit permutation based encryption has maximum 8! (40320) of key space which is not very large and encryption process is very slow therefore bit permutation based encryption is not suitable and any of the combination using bit permutation (e.g. combination of bit, pixel and block permutation) is also not suitable for image encryption. Encryption using each pixel and block permutation using 1-D and 2-D key has large number of key space and fast encryption speed but image may be decrypted by visual intelligence attack. Image encryption using combination of Pixel and Block permutation by 1-D and 2-D key has large number of encryption key, fast encryption speed and more secure from cryptanalytic attacks but encryption using 2-D key is more secure and has fast encryption speed.

TABLE I. List of key space and encryption time of different permutation techniques

Combination	Key space	Encryption Time (In sec.)
bit	8!	212.716
Pixel (1-D)	32!	0.2201
Pixel (2-D)	1024!	0.1148
Block (1-D)	16!	0.0301
Block (2-D)	256!	0.0088
Bit, Pixel and Block (1-D)	8! x 32! x 16!	212.968
Pixel and Block(1-D)	32! x 16!	0.2504
Pixel and Block(2-D)	1024! x 256!	0.1127

CONCLUSION

In this paper we proposed image encryption base on permutation. The different combination of the permutations for image encryption has been performed using different size of key. It is observed that image encryption using individual basic permutation is not suitable but different combination of basic permutation is effective against malicious attacks. It is also observed that bit permutation based image encryption takes long time to encrypt so any of the combination of bit permutation will take long time to encrypt an image and it will be not suitable for image encryption. It is found that image encryption by combination of pixel and block permutation using 2-D encryption key has large key space and very short encryption time which makes a brute force attack redundant and faster encryption speed are considered good for practical use.

BIBLIOGRAPHY

[1] Rong-Jian Chen, Wen-Kai Lu, and Jui-Lin Lai. “Image Encryption Using Progressive Cellular Automata Substitution and SCAN.” IEEE International Symposium on Circuits and Systems, 2005 .

[2] A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna. “A New Image Encryption Approach using Combinational Permutation Techniques.”International Journal of Electrical and Computer Engineering 1:2 2006.

[3] N.K. Pareek, Vinod Patidar and K.K .Sud. “Image encryption using chaotic logistic map” Elsevier Image and Vision Computing 24 (2006) 926–934.

[4] Li Chuanmu and Hong Lianxi. “A New Image Encryption Scheme based on Hyperchaotic Sequences.” IEEE International Workshop on Anti-counterfeiting, Security, Identification. April 2007.

[5] Xiaojun Tong and Minggen Cui. “A Novel Image Encryption Scheme Based On Feedback and 3D Baker.” IEEE International Conference on Wireless Communications, Networking and Mobile Computing, 2008.

[6] Yong Feng and Xinghuo Yu. “A Novel Symmetric Image Encryption Approach based on an Invertible Two-dimensional Map.”IEEE Conference on Industrial Electronics 2009.

[7] Sesha Pallavi Indrakanti and P.S.Avadhani. “Permutation based Image Encryption Technique.” International Journal of Computer Applications (0975 – 8887) Volume 28 – No.8, August 2011

[8] G.A.Sathishkumar, Srinivas Ramachandran and K.Bhoopathy Bagan.“ Image Encryption Using Random Pixel Permutation by Chaotic Mapping” IEEE Symposium on Computers & Informatics 2012.

[9] Ameena Marshnil N and Binish M C. “Image Encryption Based On Diffusion Process and Multiple Chaotic Map.”IEEE International Conference on Power, Signals, Controls and Computation (EPSCICON) January 2014

[10] Avi Dixit, Pratik Dhruve and Dahale Bhagwan. “Image Encryption Using Permutation and Rotational Xor Technique” Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012.