An Image Encryption using Block based Transformation and Bit Rotation Technique

Ankit Gupta
Dept. of CSE
MANIT
Bhopal

Namita Tiwari
Dept. of CSE
MANIT
Bhopal

Meenu Chawla,
Ph.D
Dept. of CSE
MANIT
Bhopal

Madhu Shandilya,
Ph.D
Dept. of EC
MANIT
Bhopal

ABSTRACT
Along with the rapid increasing growth of computer and network technologies, images are being transmitted more and more frequently. Security of image is a big issue. Image information is lively and visual, and has been an important means of expressing information of person. There are many encryption algorithm had been available each one having some strength and weakness. In this paper we present an image encryption technique that combines the concept of block based transformation and pixel manipulation. The proposed method consist of two stages 1) In first step we apply block based matrix transformation for pixel position manipulation; 2) In second stage, apply bit rotation technique that change the value of each pixel.

Keywords
Image encryption, block based matrix transformation, bit rotation.

1. INTRODUCTION
With the rapid development of communication and internet technology, there is always a growing concern about the security of multi-media information such as image. A major challenge is to protect the confidentiality of such images so that the visual data cannot be misused. Applications like information storage, information management, patient information security, satellite image security, telemedicine, military information security etc which require information security. Different cryptographic methods are [1] used by different organization for protecting their confidential data. But cryptography hackers are always trying to break the cryptographic method. For this reason cryptographers are trying to develop new cryptographic method to keep the data safe as far as possible. For this reason, cryptographers are always trying to propose new methods and techniques to keep data/information secure. Until now, several data encryption algorithms had been presented such as DES, AES, IDEA, RSA, etc. [2, 3] most of which are used for encrypting text data. It is not suitable to use them for multimedia data because multimedia data is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels.

Image Encryption can be divided into two ways [4] as Image Encryption using pixel manipulation and Image Encryption using pixel position manipulation. In pixel manipulation technique, weight of a pixel is changed as we know that weight is responsible for its colour. Since the change in weight leads to encryption. In pixel position manipulation change the position of each pixel by apply some rearrangement or transformation that leads to encryption.

2. BLOCK BASED TRANSFORMATION & BIT ROTATION TECHNIQUE
The original square image is divided into blocks of fixed size. After that square image is seen as two matrix above the diagonal and below the diagonal i.e. lower and upper triangular matrix. Shuffle these blocks of lower and upper triangular matrix as per the matrix transformation given below.

Table 1. Image Divided in to block and their corresponding block shuffled image

1,1	1,2	1,3	1,4
2,1	2,2	2,3	2,4
3,1	3,2	3,3	3,4
4,1	4,2	4,3	4,4

→

1,1	2,1	3,1	4,1
1,2	2,2	3,2	4,2
1,3	2,3	3,3	4,3
1,4	2,4	3,4	4,4

After that apply Bit rotation technique over the shuffled image that changes the value of each pixel of image. In this method, a password is taken with input image.

Let's take a password "ax" .Password length is considered for bit rotation. First we convert the decimal value of pixel in 8 bit binary number

P(x) is the value of pixel at position (i,j)

Convert p(x) in binary $[a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8]$ After that apply the left rotation on $[a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8]$ by the key L_R. Number of bits to be rotated to left decided by the length of password. Let L be the length of the password and L_R be the effective length i.e. number of bits to be rotated to left. The relation between L and L_R is represented by equation (1)

$$L_R = L \bmod 8 \qquad \text{eq.(1)}$$

Lets the effective length of the password be L_R =2.

Then $[a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_1\ a_2\ ]$ be the rotated binary by using the L_R, let this is p(y) be the value of pixel at position (i,j).

In this technique pixel at odd position is rotated to left by using the shift of L_R and pixel at even position is rotated to left by using the shift of L_{R1}

$$L_{R1} = (L_R + k) \bmod 8 \qquad \text{eq.(2)}$$

Where the value of k is an integer.

3. LITERATURE SURVEY

3.1 An image encryption approach using pixel and position manipulation technique

Panduranga H T, Naveen Kumar S K [4] presented a new image encryption technique using pixel and position manipulation technique. Experimental result shows that we can predict the original image if we use only position manipulation or pixel value manipulation but if we combine it is very difficult to predict.

3.2 SD-EI:A cryptographic technique to encrypt images

Somdip Dey [5] presented SD-EI image encryption, which basically has two steps. In First step apply the *bits rotation and reversal* method based on password after that Extended Hill Cipher technique for image encryption. Experimental results shown that the presented approach is implemented for different image and results are satisfactory.

3.3 SD-IES:An advanced image encryption standard

Somdip Dey et al. [6] presented SD-IES image encryption which encrypts the image in an effective way to maintain its security and authentication. As compared with SD-EI, there are more bit wise manipulations in SD-IES method. SD-IES method consists of four stages in first step apply Modified Bits Rotation and Reversal technique after that Extended Hill Cipher technique after that Modified Cyclic Bit Manipulation And Bit Reversal Technique. Because of more bitwise manipulation involved in SD-IES it is more secure.

3.4 An image encryption algorithm based on Knight's tour and slip encryption filter

Jiang Delei et al. [7] presented a new image encryption algorithm based on knight's tour and slip encryption-filter is discussed. The number of key space is sufficiently huge using Knight's Tour matrix. Experimental results show that the encryption algorithm has perfect effects, better efficiency and higher security.

3.5 Image encryption based on zigzag transformation and inner product polarization vector.

Xu xioalin [8] proposed a Image Encryption based on the combination of Improved Zigzag scrambling algorithm and Inner product polarization vector. Zigzag transformation is a kind of scrambling algorithm with low time complexity and good scrambling effect and inner product polarization vector algorithm is a new encryption algorithm deduced from Attribute Theory.

3.6 Image Encryption Using Affine Transform and XOR Operation

Amitava Nag et al. [9] presented a new location transformation base encryptions technique. It redistribute the pixel values to different location using affine transform with four 8-bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total key size used in this algorithm is 64 bit which proves to be strong enough.

3.7 Encryption approach for images using bits rotation reversal and extended hill cipher techniques

Naveen Kumar S K et al. [10] presented a new image encryption technique based on bit rotation reversal and extended hill cipher technique. The proposed algorithm is implemented for different images using MATLAB. Experimental results shows that the original image is predicted if only bit rotation reversal technique is used but it is very difficult to predict if extended hill cipher is used.

4. PROPOSED WORK

The encryption algorithm is divided into two stages i.e. Divide the image into block of fixed size then shuffling these blocks by applying the matrix transformation and at last applying bit rotation algorithm. The working of the encryption algorithm is explained in the following steps:

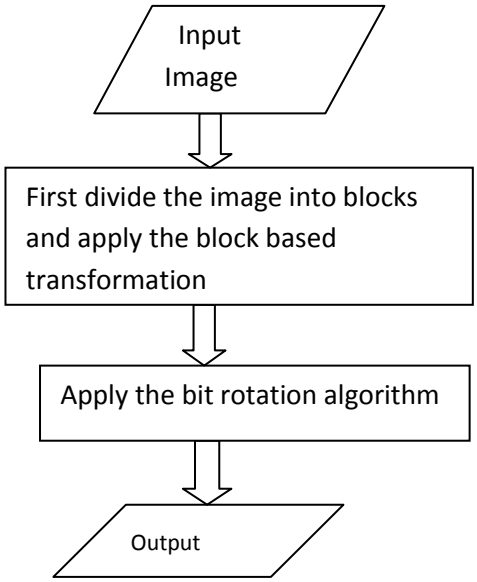


Fig 1: Diagram of proposed technique

1) Step 1: Input Image.

2) Step 2: Divide the input image into equal size blocks, after that Shuffle these blocks by matrix transformation.

3) Step 3: Apply bit rotation algorithm.

4) Step 4: Output encrypted image.

5. RESERCH PARAMETER

To determine whether the proposed encryption algorithm is safe enough to be implemented, performed analysis and testing of the encryption algorithm uses several parameters, namely

5.1 Entropy

Information entropy means randomness of the data, i.e. more entropy shows data will be effectively disordered and hence, prediction of information becomes difficult. So the value entropy should not be more than 8. If entropy is less than 8, there is possibility certain degree of predictability. The basic formula of information entropy is defines as

$$H(S) = \sum_{i=0}^{2N-1} P(S_i) log\left(\frac{1}{P(S_i)}\right) \quad \text{eq.(3)}$$

Here P(s_i) is the probability of the ith gray level and n is the number of gray level in the image (256 for 8 bit images).

5.2 PSNR (Peak Signal to Noise Ratio)

Peak signal to noise ratio is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is used to measure the quality of encryption. Lower the value of PSNR, more the encryption is stronger because it shows resultant cipher image is noise like and it contains very less amount of significant information. It is defined as:

$$PSNR = 10log\frac{(2^N-1)^2}{MSE} \quad \text{eq.(4)}$$

5.3 Correlation

Correlation coefficient measures the strength and direction of a linear relationship between two variables either horizontally, vertically or diagonally. Correlation coefficient must be low, or close to zero. If the correlation between pixels is low then the encryption system can be said to be safe. To calculate the correlations used the formula:

$$r = \frac{a\sum(xy)-\sum x\sum y}{\sqrt{[a\sum(x^2)-(\sum(x^2)][a\sum(y^2)-(\sum(y^2)]}} \quad \text{eq.(5)}$$

Where

r = correlation coefficient

a = no of pairs of data

$\sum x$ = the number of data x

$\sum y$ = the number of data y

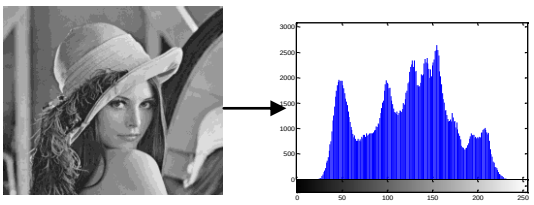
$\sum xy$ = the number of multiplication of x and y

$\sum x^2$ = the number of x squared

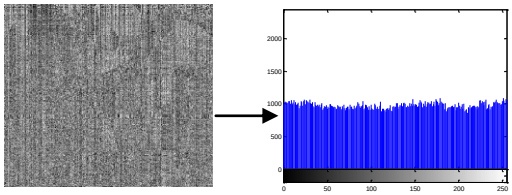
$\sum y^2$ = the number of y squared

5.4 Histogram Analysis

Histogram is a graphical view of the distributed data in digital image. Figure shows the histogram of plain image. If the histogram value has a significant distribution of diversity of encrypted image and also have perfect differences with plain image histogram, it can be said that encrypted image does not give any clues to perform any type of statistical attack on the encryption algorithm



(b) Plain Image (c) Histogram of plain image



(d) Encrypted Image (e) Histogram of encrypted image

6. CONCLUSION

Now a day's images play an important role in our lives, it is used in many applications. Therefore it is essential to protect the integrity and confidentiality of images. In this paper we presented survey of various image encryption techniques. Each technique having some advantages and disadvantages, so there is a need to design algorithm that reduce the correlation between the image pixels and increase the entropy so it is very difficult to decrypt by hacker. The proposed technique shuffles the image pixel position perfectly and changes the value of each pixel

7. REFERENCES

[1] Cryptography & Network Security, Behrouz A. Forouzan, Tata Mcgraw Hill Company.

[2] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems Shiguo Lian, Multimedia Content Encryption: Techniques and Applications. Taylor & Francis Group, LLC, 2009.

[3] R. A. Mollin," An introduction to cryptography", CRC Press Boca Raton FL USA. 2006.

[4] Panduranga H T, Naveen Kumar S K, "An image encryption approach using pixel and position manipulation technique". Proceedings published in internation journal of computer applications (IJCA) (0975-8887)

[5] Somdip Dey, "SD-EI: A Cryptographic Technique To Encrypt Images", Proceedings of "The International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec 2012)", held at Kuala Lumpur, Malaysia, 2012, pp. 28-32

[6] S. Dey, S. A. Sriam, S. B. Subin, and P. K. A. Asis. SD-IES: An Advanced Image Encryption Standard Application of Different Cryptographic Modules in a New Image Encryption System. In 2013 7th International Conference on Intelligent Systems and Control (ISCO), pages 0–4, 2012.

[7] Jiang Delei, Bai Sen, Dong Wenming. An Image Encryption Algorithm Based on Knight's Tour and Slip Encryption-filter [C]//2008 International Conference on Computer Science and Software Engineering. Hubei, China, 2008: 251-255

[8] X. Xu, J. Feng, Research and implementation of image encryption algorithm based on zigzag transformation and inner product polarization vector, in: Proc. of IEEE Int. Conf. on Granular Computing, ACM Digital Library, 2010, pp. 556–561.

[9] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar. Image Encryption Using Affine Transform and XOR Operation "Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011),pp 309 – 312, 21-22 July 2011

[10] Naveen Kumar S K, Sharath Kumar H S, Panduranga H T, " Encryption approach for images using bits rotation reversal and extended hill cipher techniques." International journal of computer applications 2012.