Image Encryption using Block Shuffling and Affine Transform: A Review

Harshit Somani
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
The rapid development of communication technology due to the global spread of the internet and the digital information revolution has given rise to a huge increase in the use and transmission of multimedia information. Encryption technology is studied in this paper, and a new image encryption algorithm based on correlation of pixels is proposed. The main goal of this paper is security management. Researchers have proposed incompatible methods to encrypt images. So, here we go through a new way of image encryption and decryption using block based image encryption using affine transform. First of all the plain image is divided into fixed size blocks. All these blocks then shuffled according to the proposed algorithm and we get a block shuffled image. At last the encrypted algorithm of affine is used iteratively for each of the pixels. It uses the keys for the purpose of encryption.

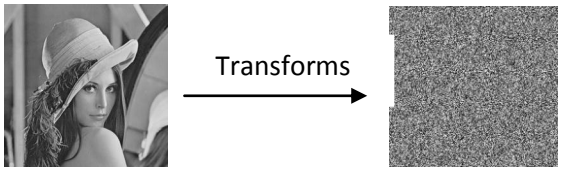
Keywords
Image encryption; Shuffling; Affine transformation; Block shuffled image; Security (key words)

1. INTRODUCTION
In recent years with the growth of internet and the digital technology, it broadens the scope of right and wrong, as there are privacy violations, information theft and so on [1]. Digital images are widely used now a day so its security is very vital. Now digital security is a major theme in computer security. As the number of users increases exponentially, the need to protect data and the multimedia on the Internet has become a high priority. To prevent the data from unauthorized access, encryption technique is widely used. Encrypting the data in the form of images is new interest of researchers.

Most of the encryption algorithms are based on textual data. These algorithms may not be suitable for encrypting image data types. Due to large data size, algorithms that are good for textual data may not be suitable for image data [2]-[4]. The encryption algorithm can be divided into 2 parts: (i) Symmetric key encryption and (ii) Asymmetric key encryption. Symmetric key encryption algorithm uses same key for both encryption and decryption while asymmetric key encryption algorithms uses different keys for encryption and decryption.

Asymmetric key algorithm has very higher computational costs which are most of the time prohibitive for multimedia data. Symmetric key encryption algorithms are comparatively lower cost and may be used for multimedia data. But the characteristic of multimedia data is different from text data. Text data does not have any redundancy where as all multimedia data has a lot of redundancy. The pixel value of a pixel is highly correlated to its neighbor pixels.

There are various algorithms available such as DES [5], AES [5], RSA [5] and IDEA [5] provides very high security but they are used only for text data. They are not suitable for image encryption because of intrinsic characteristics behavior of images, such as high redundancy and large data size. Due to which image encryption is divided into three major groups: (i) Position permutation based algorithm, (ii) value based transformation algorithm, (iii) visual transformation based algorithm. In this paper we have proposed a two-phase encryption and decryption algorithms that are divide the image into blocks, then shuffling the blocks and then apply affine transformation.



(a) Plain Image (b) Encrypted Image

2. RELATED WORK
2.1 Image Encryption Using Block-Based Transformation Algorithm
In 2008 Mohammad Ali Bani Younes and Aman Jantan [6] gave an idea that there is a vital difference between text based encryption and image based encryption. They proposed that the original image was divided into fixed number of blocks, which were reshuffled into a transformed image by the help of a transformation algorithm.

The results had proved that the correlation between image elements was decreased significantly by using the proposed technique.

2.2 Image Encryption Using Affine Transform and XOR Operation

In 2011 Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar [7] proposed a new location transformation based encryption technique. They redistributed the pixel values to different location using affine transform technique with four 8-bit keys. The resulted image then divided into 2 x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total key size used in our algorithm is 64 bit which proves to be strong enough.

Affine transform is defined as:

$$X' = (K0 + K1 * x) \bmod N$$

$$Y' = (K2 + K3 * y) \bmod N$$

Where (x, y) is an old point of pixel

(X', Y') is a new point of pixel

And K0, K1, K2, K3 are keys.

The old point pixel and the new point pixel are swapped.

Then the image is decomposed into n/2 * n/2 blocks.

For each block xor is performed with four more keys K4, K5, K6 and K7.

2.3 A New Scrambling Method Based on Arnold and Fermat Number Transformation

In 2009 Zhang Yanqun and Wang Qianping [8] proposed that the statistical character of the whole image is unchanged although the partial relativity of pixels are destroyed. That is the histogram of originally image and the histogram of scrambled image are the same. The statistical character of secret images pre-processed with Arnold can be attacked easily, so it is necessary to study a new information hiding method that can change the texture information of image and also change the statistical character of image. Arnold transform is simply known as cat map transformation. Suppose the coordinate (x, y) in 2-D plain. The Arnold transformation that change the coordinate (x, y) to the (x', y') by using formula:

$$X' = X + Y \bmod N$$

$$Y' = X + 2Y \bmod N$$

This should transform the image iteratively.

2.4 Image Encryption Using Random Pixel Permutation by Chaotic Mapping

In 2012 G.A.Sathishkumar, Srinivas Ramachandran and Dr.K.Bhoopathy Bagan [9] proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps. The random-like nature of chaos is effectively spread into the encrypted image through permutation and transformation of pixels in the plain image. This results in the encryption scheme being resistive to cryptanalytic.

2.5 An Image Encryption Algorithm Based on Knight's Tour and Slip Encryption-filter

In 2008 Jiang Delei , Bai Sen and Dong Wenming [10] proposed a knight's tour matrix emended as slip encryption-filter template matrix and then they produce a knight's tour matrix again with the same size of the image waiting for encryption as a knight's tour slip matrix. Finally, the center of the slip encryption-filter template move along with the knight's tour slip matrix to do convolution operation, and achieve the cipher image.

3. PROPOSED WORK

The encryption algorithm is divided into two phases i.e. block dividing of fixed size then shuffling the blocks and at last applying Affine transformation algorithm. The working of the encryption algorithm is explained in the following steps:

Step 1: Input Image

Step 2: Block Based Transformation:

i) Divide the input image into equal size blocks,

ii) Shuffle the blocks according to a transformation so the correlation between the neighbor pixel decreases,

Step 3: Apply affine transformation iteratively.

Step 4: Output encrypted image.

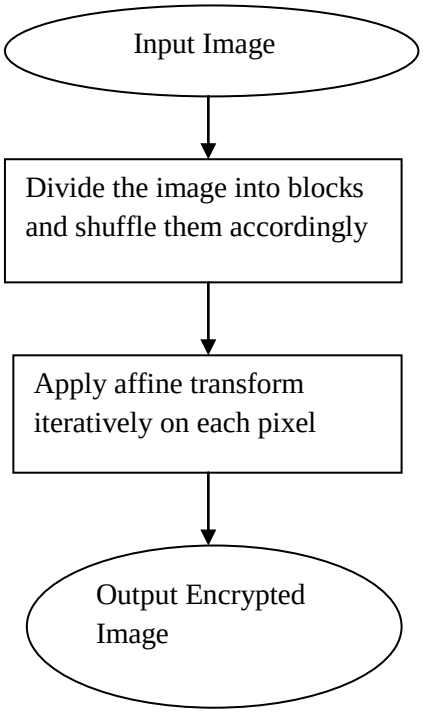


Fig 1: Flow diagram of the above method

3.1 Block Based Technique:

Block encryption methods are based on the encryption of image block by block. Image is first divided into pre-calculated size of blocks and then theses blocks are encrypted within its boundaries one at a time. By the help of block rearrangement, we define a transformation by which the blocks of the image get shuffled such that the correlation of the pixels with the neighbor pixel decreases.

3.2 Affine Transformation:

x'= (K0+K1*x)mod N

y'= (K2+K3*y)mod N

Where (x, y) is an old point of pixel

(x', y') is a new point of pixel

And K0, K1, K2, K3 are keys.

N is used as the length and width of the image.

The old point pixel and the new point pixel are swapped.

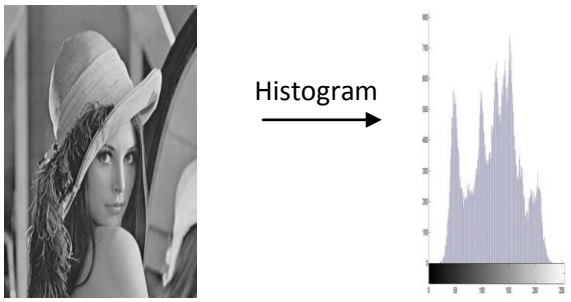
The formula is used iteratively for all the pixels.

4. RESULT ANALYSIS

Result parameters are:

4.1 Histogram Analysis

A histogram is a graphical representation of the distributed data. It is an estimation of the probability distribution of a continuous variable. Histogram is used to plot the density of data. It looks like



(a) Plain Image (b) Histogram

4.2 Mean Square Error

The Mean Squared Error (MSE) of an estimator is a ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.

$$MSE = \frac{1}{n2}\sum_{i,j=0}^{N-1} \| C(i,j) - \hat{C}(i,j) \|^2$$

The Mean Square Error should be less then we will get a more secure image.

4.3 Normalized Cross Correlation

It is used to evaluate the degree of similarity or dissimilarity between two compared images. The advantage of the normalized cross correlation over the cross correlation is that it is less sensitive to linear changes in the amplitude of illumination in the two compared images.

$$C_{AB} = \frac{\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(A_{ij} - \overline{A})(B_{ij} - \overline{B})}{\sqrt{\left(\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(A_{ij} - \overline{A})^2 \frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(B_{ij} - \overline{B})^2\right)}}$$

$A_{i,j}$ and $B_{i,j}$ are the pixels in the i^{th} row and j^{th} column of A and B respectively and r, c represent the no. of rows and columns in the image.

4.4 PSNR (Peak Signal to Noise Ratio)

PSNR is defined as ratio of amount of significant signal information to noise. It shows quality measure of an encryption technique. If the value of PSNR is low that means the encryption is stronger. It is defined as:

$$PSNR = 10\log\frac{(2^N - 1)^2}{MSE}$$

4.5 Entropy

Entropy quantifies the expected value of the information contained within a message. The formula for entropy is:

$$h = -(p_i \log_2 p_i)$$

Where p_i is the frequency of intensity level i in the image. The maximum h can attain in an 8–bit image is 8. In our method the entropy will not changed because the pixels and transforming their value is not changing.

5. CONCLUSION

The above mentioned encryption techniques have advantages such as security, performance, less noise, etc. But in block based transformation if the criterion is identified then the hacker can decrypt the image, so in our proposed work we will use two-level encryption which is highly secure. In terms of performance and noise the method is less noisy then other methods and has a good performance. It uses key, hence key should be protected.

High key sensitivity is required by secure image cryptosystems means that the cipher image cannot be decrypted accurately. This guarantees the security of the proposed technique against brute-force attacks.

6. REFERENCES

[1] Tian-jian Chen Shan-xue Summarization of digital watermarking and image authentication. Communication Technology, vol(12), pp. 253-255, 2007.

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

[3] S. Changgui, B. Bharat, "An efficent MPEG vedio encripted 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," proceeding of iasted international conference, single processing, pattern recognition and application, 2002, pp.25-28.

[5] W. Stalling, Cryptography and Network Security principles and practices, 3rd ed. , Pearson Education, 2003.

[6] Mohammad Ali BaniYounes and ArnanJantan, " Image Encryption Using Block-Based Transformation Algorithm*", IAENG* International Journal of computer science , *35:1 , IJCS_35_1_03.*

[7] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar, " Image Encryption Using Affine Transform and XOR Operation", Sarkar, *P.P*. in International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN),2011 International.

[8] Zhang Yanqun and Wang Qianping , " Digital Image Scrambling Technology Based On Two Dimension Fibonacci Transformation And Its Periodicity", Third International Symposium on Information Science and Engineering

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

[10] Jiang Delei , Bai Sen and Dong Wenming, "An Image Encryption Algorithm Based on Knight's Tour and Slip Encryption-filter", International Conference on Computer Science and Software Engineering, 2008.