IMAGE ENCRYPTION USING BINARY BIT PLANE AND ROTATION METHOD FOR AN IMAGE SECURITY

[1]R.Aarthi, [2] Mrs. S.Kavitha

[1]M.Phil Scholar, Department of Computer Science, Sakthi College of arts and science for women, oddanchatram, India.

[2]Head of the Department, Department of Computer Science, Sakthi College of arts and science for women, Oddanchatram, India.

Abstract

Image encryption plays a major role in information security. It is mainly used to convert the original image into another form. In this work, we propose a bit plane slicing of digital image to provide the more security. To enhance security of the bitplane decomposition based image encryption methods, this paper introduces a novel image encryption algorithm using a bitplane of a source image as the security key bitplane to encrypt images. It focuses on three techniques such as image scrambling, bit plane slicing and image rotation for efficient image encryption. Arnold scrambling and bit plane slicing process are performed in the source image. From the decomposed source image, particular bitplane is assigned as the security key bit plane to perform the encryption process in the original image. As an example, this paper also proposes a bit-level scrambling algorithm to change bit positions. Simulations and security analysis are provided to demonstrate an excellent encryption performance of the proposed algorithm.

Index Terms – Image Encryption, Bit Plane Slicing, Rotation, Scrambling.

1. INTRODUCTION

Cryptography is an efficient method of transferring information in a secure way. It scrambles the image before transmitting in order to change the structure of an image. Even the attacker cannot able to hack because it is difficult for him to retrieve the original image. It only provides the modified form of an image but it does not hide the image even though it is better secure method. The main intention is to provide better protection of the original image. Bit plane slicing is mainly used for splitting images into binary planes. Each bit is used to represent the intensity of each pixel of an image. Image scrambling is always based on pixel values of an image. The digital image is divided into 8 bit planes because it is useful for analyzing the importance of each bit in an image. Whereas a small change in color affect bit value of an image. The color image is composed of many pixels is decomposed into 8 bit planes. It is used to represent the highest order and lower order bits to specify the contribution of each bit in an image. It achieves better image encryption than the other least significant bit, perceptual masking technique. This process is done on without changing
the overall image quality.

Image Encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it, however that authorized parties. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. They protect the secret information by

converting the secret information to some unintelligible form using a key. By using a key, we protect the secret information by converting the secret information to some incomprehensible form. We get back information through encrypted information should be converted back to original information. On the Basis of key, the encryption algorithm can be classified into two categories. They are(i) Symmetric key encryption-This algorithm uses same key for both encryption and decryption and (ii) Asymmetric key encryption-This algorithms uses different keys for encryption and decryption. Asymmetric key algorithm has very higher computational costs than Symmetric key encryption algorithms which have comparatively lower cost. Asymmetric key algorithms are most time prohibitive for multimedia data. But the characteristic of multimedia data is totally different from text data. All multimedia data has got a lot of redundancy but text data does not possess any redundancy. The pixel value of a location is highly correlated to values of its neighboring pixels. Like, a sound sample is correlated to its next sample and its previous samples. This correlation proves to be attack points to any standard encryption algorithm. Because they can predict the values of neighboring pixels or next sound sample by finding out pixel value at a location or one sound sample with reasonable accuracy.

Nearly all the available encryption algorithms like .DES, AES, RSA and IDEA are used for text data. Act of them DES, AES, RSA and IDEA can achieve high security, it is not be suitable for images and videos encryption due to the intrinsic characters of images and videos .So we need some other technique for encrypt image and videos. For large data size and high redundancy, encryption special requirements and different encryption algorithms is needed. The image encryption algorithms divided into three major groups: (i) position permutation based algorithm, (ii) value transformation based algorithm (iii) visual transformation based algorithm .Several encryption algorithms are based on chaotic maps. In this project, we propose image encryption using Random Scrambling and XOR operation. Arnold transform that is based on shuffling the image pixels and they encrypting the resulting image using XOR operation. We used 32 bit key that is good for practical purposes.

SCOPE OF THE STUDY

The need for image processing has increased sharply. Encryption and gloves are both dirt-cheap and widely available. Image processing has applications in many fields. Improvement of secured pictorial representation for human interpretation and processing security image information were the two main reasons behind the need for image processing.

OBJECTIVE OF THE STUDY

The main objective of the system is

- To enhance the security of the image.
- To enhance the performance of the image encryption and decryption.

2. LITERATURE SURVEY

Image encryption technique plays a vital role in image processing. Lot of image encryption technique has been developed so far. In this literature review some encryption techniques are discussed. The techniques such as Arnolds algorithm, Bit plane algorithm, Scrambling algorithm by means of block analysis, enhance the security and bit plane generation are discussed.

R.Gopinath et al., Image encryption is used to protect the images and transform into different format. In this paper, lossless encryption for color images using binary key images has been proposed. In proposed method, the key image size is same as the original image. The key image is either a bit plane or an edge map generated from another image. The method is discussed against common attacks such as the plaintext attacks, brute force attack and cipher text attacks. The experimental results shows that the lossless encryption of all type of images.

Rinkipakshwar et al., This paper aims at improving the level of security and secrecy provided by the digital gray scale image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. Since the pixel of the image is highly correlated to their neighboring pixels. Due to this strong correlation any pixel can be practically predicted from a value of its neighbors. So there is a need of a technique that can shuffle the pixels to reduce the correlation between the neighbor pixels. Hence we use scrambling technique that shuffles the pixels of image. This scrambling image is called 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 size of key in our algorithm is 32 bit long which proves to be strong enough. The proposed encryption algorithm in this study has been tested on some Gray scale images and showed good results.

Li W and Yuan Y proposing two attacks to sketch the outline of the original image directly from the scrambled JPEG compressed image. In particular, Li and Yan proposed nonzero count attack to sketch the outline of the original image. However, their method requires the tuning of threshold values.

3. METHODOLOGY

3.1. ARCHITECTURE DIAGRAM

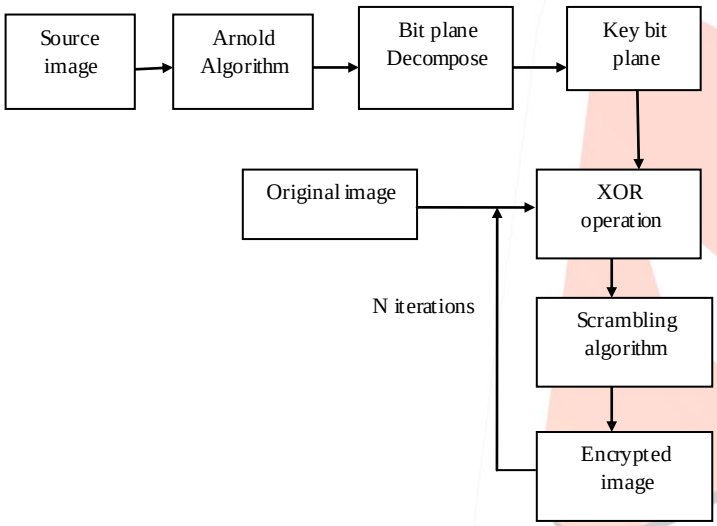

Figure 3.1. Architecture diagram

3.2. FUNCTIONAL COMPONENETS

The modules of the image encryption using Arnolds transform algorithm has briefly described as below:

- Image Scrambling Using Arnold Transformation
- Binary Bitplane Decomposition
- Transformation of Bitplane into Vector
- Scrambling with XOR operation

Image Scrambling using Arnold Algorithm

Arnold scrambling algorithm is base on square digital image and these images are mostly $N \times N$ pixels of the digital image. However, most of the digital images are non-square in the real world, so that this system cannot use Arnold scrambling algorithm widely. To improve the Arnold scrambling algorithm, this system the original Arnold scrambling algorithm, so that this system applies Arnold scrambling algorithm to $M \times N$ non-square pixel digital image, it means the length and width of the image is not equal .

The digital image can be seen as a two-dimensional matrix. When the size of the image is N, then I have $N \times N$ elements, the subscript x, y stand for the position of pixel, x, $y \in \{0, 1, 2..., N\text{-}1\}$. Let x, y corresponds to the x, y of Arnold scrambling, for each pair x, y, after all do Arnold scrambling, become x' and y', which equivalent to the original image of the point from (x, y) move to the = (x', y'), so realized the movement of pixels in the image, the image with Arnold scrambling traverse all the points to complete a picture of Arnold scrambling.

The cycle of Arnold scrambling is relate to the size of the image, but not directly proportional. If size is 128 × 128 pixel image of Arnold scrambling cycle is 96, size 240 × 240 pixel image of Arnold scrambling for 60 cycles.

Binary Bit Plane Decomposition

A non-negative decimal number N can be represented by a binary sequence (b_{n_1};…; b_1; b_0) based on the following equation:

$$N = \sum_{i=0}^{n-1} b_i 2^i = b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}$$

Because pixel values in a gray scale image are decimal numbers between 0 and 255,each pixel can be represented by an 8-bit binary sequence. Thus, BBD can decompose a gray scale image into 8 binary bit planes (BBs). The i^{th} bit plane consists of all the i^{th} bits of the binary representation of each pixel within the gray- scale image. Among these bit planes, higher bit planes contain more significantly visual information of the original image while lower bit planes show more details

Transformation of Bit Plane into Vector

In Bit-Plane Slicing image is sliced into eight binary planes. The bits which are presents in the bit plane 0 is the least significant bit and the bits which are present in the bit plane 7 are the most significant bits. All pixel values of the image is converted into binary vector space based on the bit plane slicing.

In terms of 8-bits bytes, plane 0 contains all lowest order bits in the bytes comprising the pixels in the image and plane 7 contains all high order bits.

Separating a digital image into its bit planes is useful for analyzing the relative importance played by each bit of the image, implying, it determines the adequacy of numbers of bits used to quantize each pixel , useful for image compression.

In terms of bit-plane extraction for a 8-bit image, it is seen that binary image for bit plane 7 is obtained by proceeding the input image with a thresholding gray-level transformation function that maps all levels between 0 and 127 to one level (e.g 0)and maps all levels from 129 to 253 to another (eg. 255).

Scrambling With XOR Operation

The algorithm first decomposes the original image (the image to be encrypted) into eight binary bit planes using binary bit plane decomposition. To change bit values, each bitplane is then performed the XOR operation with a security key bitplane, individually. A scrambling algorithm is used to change all bit locations. After n iterations of the XOR and scrambling processes combines all bit- planes to obtain the encrypted image.

The security keys of DecomCrypt consist of the iterations n, source image or its location (the location of an image database or a link of webpage), decomposition method and its parameters, location of the security key bitplane, as well as the scrambling algorithm and its security keys. These security keys are encoded as messages or emails and then transmitted over separated security channels. This ensures that they are safely and correctly delivered to the authorized users for image decryption

3.4. IMAGE SCRAMBLING

Image Scrambling (IS) is a process of scrambling the positions of pixels in an image using permutations. There are several image scrambling techniques like Arnold-Cat map, Standard map, row-column shuffling, SCAN Pattern, Index bit-reversal order and Matrix transformation. In Image Encryption (IE), the value of the pixel is get altered by using some mathematical operations like bitwise xor, bit shuffling, bitwise rotation, matrix addition, matrix multiplication and manipulation in transform domain.

Image scrambling is a process of rearranging the pixels position of an input image using permutations. Correlation between adjacent pixels is more important in an image. Using scrambling process this correlation between adjacent pixels are reduced and hence scrambled image reduces the intelligible property of an image.

4. RESULTS AND DISCUSSION CONCLUSION

Image encryption and decryption using Arnold scrambling and bits scrambling process are written in MATLAB. Simulations have been performed on a Matlab R 2008 platform to verify the validity of the proposed encryption technique.

In the encryption process, first the source image is read from the file. Then perform the Arnold scrambling process for the source image. After completion of Arnold scrambling process, scrambled image's 8 bit planes are extracted individually. From the extracted 8 bit plane, particular key bit plane is selected and passed to the XOR operation and scrambling process with the original image. After completion of this process, original image is selected and read from the image file and histogram is generated for the original image. Generated key from Arnold scrambled image and the original image is passed into the image encryption process. Original image's bit positions are encrypted using key data with XOR and bits scrambling process. Thus the image is encrypted. Encrypted output for the image is obtained. Image decryption is performed in the reverse order of encryption. Thus the original image is obtained.

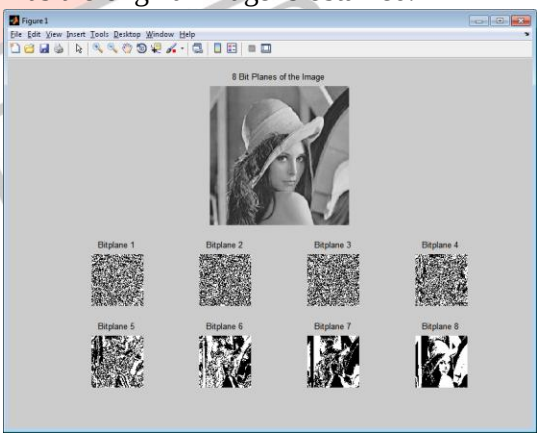

Figure 4.1. 8 bit planes of the image

A bit plane of a digital discrete signal (such as image or sound) is a set of bits corresponding to a given bit position in each of the binary numbers representing the signal.

The above figure 4.1 shows the source image with its bit slicing images.

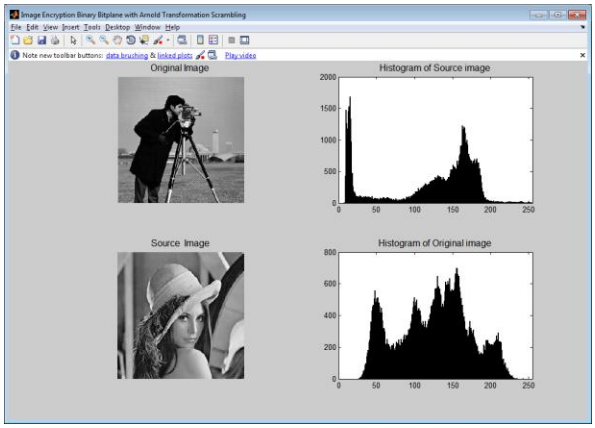

Figure 4.2. original image and source image with histogram

Histogram of the image data calculates the histogram for the intensity image and displays a plot of the histogram. The number of bins in the histogram is determined by the image type. The above figure shows the histogram for the original image and also source image.

Source image is used to perform the Arnold scrambling and select the particular key bit plane. Key bit plane is used to encrypt the original image.

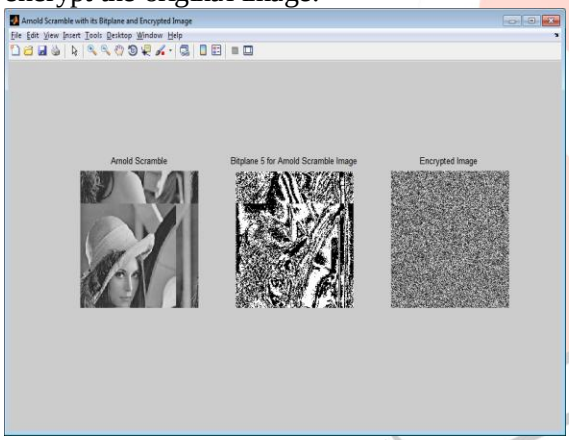

Figure 4.3. Arnold scramble for the source image with selected key bit plane and encrypted original image

The above figure 4.3 shows the Arnold scramble of the given original image and selected key bit plane from the 8 bit planes of the scrambled image. Selected key bit plane is used to perform the encryption process with the selected original image.

In the encryption process, XOR operation is performed in the selected key bit plane and original image's bit data and perform the scramble process. Finally encrypted image is obtained.

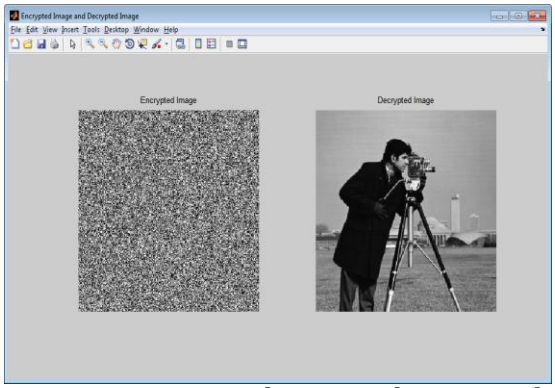

Figure 4.4 Encrypted image with Decrypted image

The above figure 4.4 shows the encrypted image and output of the decryption process. Image decryption is performed in the reverse order of encryption. Thus the original image (decrypted) is obtained.

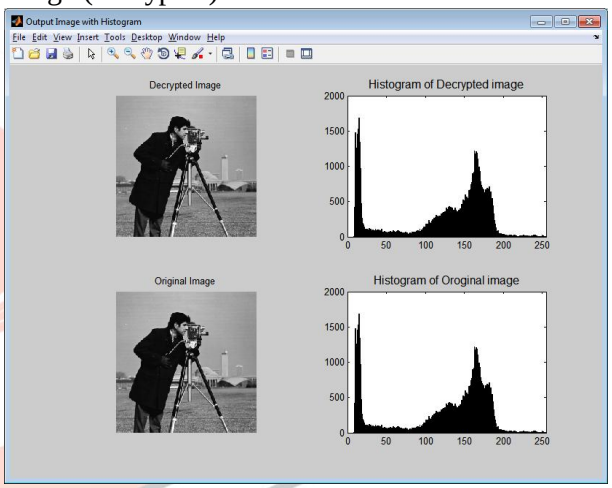

Figure 4.6 Encrypted image and Decrypted image with Histograms

The `psnr` function implements the following equation to calculate the Peak Signal-to-Noise Ratio (PSNR):

$$PSNR = 10\log_{10}(peakval^2/MSE)$$

where *peakval* is either specified by the user or taken from the range of the image data type (e.g. for `uint8` image it is `255`). *MSE* is the mean square error,

i.e. *MSE* between `A` and `ref`.

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to comparing the squared error between the original image and the reconstructed image. There is an inverse relationship between PSNR and MSE. So a higher PSNR value indicates the higher quality of the image (better). PSNR value of the original and decrypted image is 99.00

REFERENCES

1. R.Gopinath, M.Sowjanya"Image encryption for Color images using bitplane and Edge map Cryptography algorithm

2. Somdip Dey, "SD-AEI: An Advanced Encryption Technique For Images", Proc. Of IEEE 2012 Second International Conference on Digital Information Processing and Communications (ICDIPC2012), Lithuania, pp. 68-73.

3. Shujun Li , Xuan Zheng, ―On the Security of an Image Encryption Method―in Proc. IEEE Int. Conference on Image Processing (ICIP'2002 ppII-925 - II-928 vol.2

4. Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, ―A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption‖, in Proc *International Conference on Electronics and Information Engineering (ICEIE 2010), Volume1, pp* V1-141-145.

5. Zhenjun Tang and Xianquan Zhang, Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies, Journal of Multimedia, VOL. 6, NO. 2, APRIL 2011, 202-206.

6. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", *IEEE Proceeding in the year 2003*.

7. 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*.

8. Hui Liu, Cong Jin," A Color Image Encryption Scheme Based on Arnold Scrambling and Quantum Chaotic" International Journal of Network Security, Vol.19, No.3, PP.347-357, May 2017