Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 8, August -2017

Image Encryption by Taking Block of Pixels

Pothipoka Ramesh[1], T. Sreenivasulu Reddy[2],

[1]Department of Electronics and Communication Engineering, SVU College of Engineering, Tirupati
[2]Professor, Department of Electronics and Communication Engineering, SVU College of Engineering, Tirupati

Abstract— *The process of securing the data in communication from source to receiver is called cryptography. In the process of cryptography, we use a key and an algorithm. The key influences the security of the data partially. Also, the algorithm influences the security partially. In cryptography, the size of the key is limited due to human memorability. It is impossible to design the key by knowing its dimensions. A modified and advanced approach is proposed in this paper for increasing the security of the data. We are concentrating the key part of the cryptography as well as the input image for increasing the security of the data. We use the 2Dimensional graphic image designed by the user which composed of pixels in which every pixel have same or different ASCII value. In the proposed algorithm, we will generate a key of any size which is used in encryption as well as in decryption.*

Keywords- *Cryptography, Encrypting, Key, Decrypting,Human-Memorability, Confidentiality, Integrity, Array, Noise, Image, Pixel, Randomization, Cyber security, Hacking, Steganography, Digital Image Processing*

I. INTRODUCTION

Now a days, each and every sector is using online services in the part of their work. These sectors include public sectors and private sector such as education sector, medical sector, and service sector. The government is also using the online services for the better delivery of the services. Cyber threat is a major problem in the present days. Recent attack of ransom ware is also an example for this. Many unauthenticated users are using the hacking techniques to access the highly confidential of many sectors. It has becomemajor concern. So, there is a need to improve the security of the data by using highly secured methods. For improving the security, there are many ways of which steganography and cryptography which are well known.

Steganography is the process of hiding the data in a covering media to provide security.in this process, a covering media is taken (i.e., plain text, images, audio, video and so on) and the secret message is imbibed into the covering media. This function is done by the covering function. In this, the key is optional. At the receiver, the inverse covering function will do the inverse process of steganography. In this way, the data is secured.Security became a big challenge in today's world. Cyber security standards are decreasing and the hacking techniques developing rapidly. The sensitive data of many countries is under the threat of the hackers. Many terrorists are using these sensitive data to promote their anti-social activities. So, we have to secure the data so as to curb the anti-social elements.

To improve the security of the data, the process of cryptography is also is used. Cryptography consists of two processes. They are encryption and decryption. The process of encryption converts the plain text (understandable format) into the cypher text(non-understandable format). The encryption process requires a key as well as an algorithm. At the transmitter side, the plain text is converted into the cypher text by using the key and the algorithm. This process is called encryption. In this process, the algorithm performs two functions. They are substitution and transposition. Substitution is the process of replacing one value with other value. Transposition is the process of shuffling the positions of the values. At the receiver side, all these processes are done in the reverse manner i.e, the cypher text is converted into the plain text. The conversion is done by using the algorithm and the key. It is done by reshuffling positions of the characters into their original positions. After this, reverse substitution is done to get the original values. These two processes complete the decryption process. The encryption and decryption processes will complete the cryptography. The process of cryptography is used in many fields such as to encrypt audio,video,image and so on.

In cryptography, we can modify the algorithm to enhance the security of the data. We can also modify the key generation technique to improve the security. In this paper, we are concentrating on key generation and key manipulation techniques using 2Dimensional graphics image. The property of the 2Dimensional graphics image is that it is not possible to design the exact image by knowing the dimensions of the image. Even a small value of mismatch will create a large amount of distortion, thus enhancing the security. Digital images are the representation of intensity or gray level values in a matrix form i.e., rows or columns. Each value is called a pixel. The intensity or gray level of a pixel determines its brightness. A

digital image is also called a bitmap. The size of the image is represented as mXn, where m is the number of rows and n is the number of columns. So, in an image, each pixel is shown as a tiny dot which has its own gray level.

Digital images can be classified into two types. They are black and white images and colour images. In black and white images, the pixels are made of its gray level values. These gray level values will range from pure black to pure white. In colour images, the images are made up of colouredpixels. In black and white images, each pixel has only one value which corresponds to its gray level. Normally, a pixel of black and white image consists of eight bits. Therefore a pixel can have 256 different types of gray levels. The gray level 0 represents black and the gray level 255 represents white. In black and white digital images, a pixel can be stored in a single byte i.e., eight bits of memory.

Colour images are made up of the pixels consisting of three values which corresponds to three colours i.e., red, blue and green. Each value consists of eight bits. So, the three values together consist of twenty four bits. Each value will have 256 possible values. In the same manner, all the three values will have 256 possible values each. Therefore, a pixel of a colour image consists of total twenty four bits. So, a pixel can have approximately 16.7 million different possible colours. The red, blue and green (RGB)are called primary colours for mixing light. Therefore red,blue and green are called the primary colours.

All colours can be created by using the red, blue and green colours. These are called additive primary colours. We also have subtractive primary colours. They are cyan, magenta and yellow. All colours can be created by using cyan, magenta and yellow colours in certain proportions.In some images, each pixel is represented by only one bit. These type of images are called binary images. So, there is only two possible values i.e., 0 and 1. 0 represents the black colour and 1 represents the white colour. Therefore we cannot represent the intermediate gray levels. In photography, we can use the black and white images as well as the colour images. But, we cannot use the binary images in the photography because it cannot represent the gray level values between black and white.

We can create some images by using a limited number palette of colours typically 256 different colours. These types of images are called indexed colour images because, for each pixel, there will be corresponding palette of colours. We cannot use the indexed colour images in photography. Because, if the image contains more than the palette of colours, to decrease the number of colours, we have to use some techniques. These techniques will degrade the quality of the images. If the image has lesser number of colours than the given palette of colours, it will also create some problems. We cannot combine two or more indexed colour images which consisting of different palettes of colours. So, we cannot use the use the indexed colour images in the photography.

II. RELATED WORK

Xiukum Li, Xiangqian Wu, Ning Qi, Kuanquan Wang have created a cryptographic algorithm in 2008. That algorithm uses the iris features, add/subtract operator, and Reed-Saloman error correcting algorithms. This algorithm will directly encrypt and decrypt the data. They defined a region of interest from an iris textural image. This region of interest is passed through a Gabor filter to get the filtered image. The filtered image is divided into sub parts and their mean value is calculated. The mean values of same images will be different because of the noise. Then, they has taken the normalized iris feature vector. On this normalized iris feature vector, encryption and decryption operations were performed.

B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani proposed a cryptographic algorithm to generate a key using the image features in 2012. They performed encryption as well as decryption processes by using the image features. They created the Gray Level Cooccurance Matrix (GLCM) from the image. Among all the properties of the matrix, the features are extracted from the matrix on the basis of high rank. They generated the key using these features and used thekey for the encryption and decryption processes.

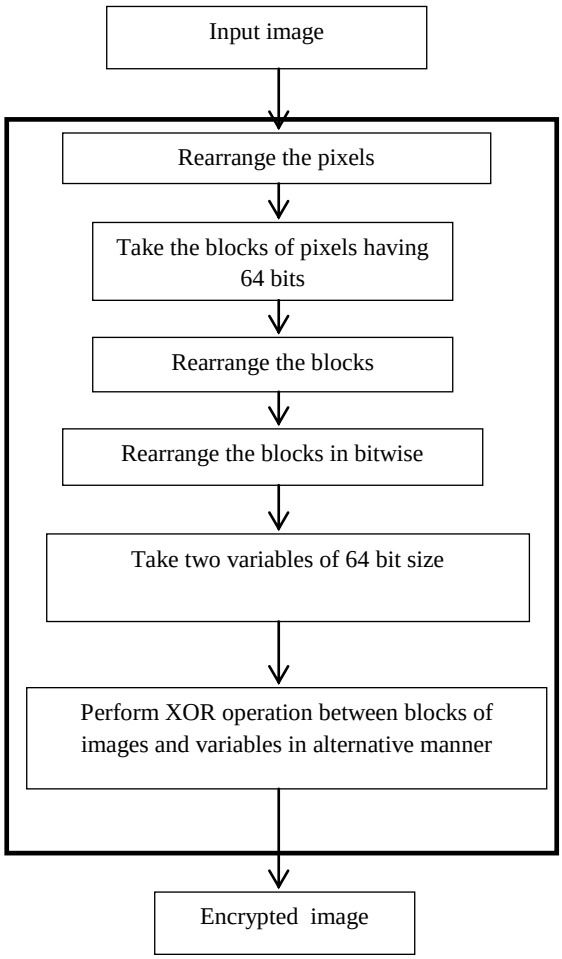
Pratik Shrivastava, Rajesh Jain, K.S. Raghuwanshi also proposed a novel cryptographic algorithm in 2014 in which they have used the key manipulation. They modified the key by shuffling the positions of the bits of the key. The same process is used in encryption as well as decryption.

III. PROPOSED METHODOLOGY

In the proposed method, we are giving more importance to the key part of the cryptography as well as the input image. In this method, we are free in taking the key of any size, shape, pattern, signature, etc. the only thing is that, the key can be easily remembered by the user. This key pattern has also the pixels having different colours or gray levels. These values are also represented in the binary format.

In the encryption process, if the image is directly taken, then there will be possibility of insecurity. To overcome it, we will first take the zigzag scan of the image. Similarly, we will use any different type of scan. This scanned image is then encrypted to improve the security. At the decryption process, the inverse of the zigzag scan is performed.

In the proposed algorithm, we are we are manipulating the image as well as the key part. Manipulation of image as well as the key part gives more security to the image. The following steps are used in the proposed algorithm.



Algorithm

1. Read the input image which has to be encrypted.

2. Read the pixels of the image and shuffle the positions of the pixels. That is exchange the first pixel with the last pixel and second pixel with the second last pixel and so on.
3. Take a group of pixels having 64 bits. i.e., eight pixels.
4. Reverse the 64 bit block i.e., exchanges the most significant bit with the least significant bit and so on.

5. Initialize i=1
6. Declare an array to store the image.
7. Declare two different variables variable1 and variable2.

8. While i < size of array
   a. Perform the XOR operation between first block of the shuffled image and variable1.

   b. Perform the XOR operation between the
   c. Second block of the shuffled image and variable2
   d. Repeat the process alternatively up to the last group of pixels of the image.

The resultant image is the encrypted image. Here, we can see a lot of difference between the input image and the encrypted image.so, it will become impossible to decrypt the encrypted image by the unauthenticated person.at the receiver side, the same process is repeated in the reverse manner. By merely knowing the dimensions of the image and without knowing the encryption process, it is not possible to get the original image. The encryption process is shown in the adjacent block diagram

Figure1. Block diagram of encryption

The encryption process is done in many stages to improve the security. If the number of stages is increasing, the extent of security will be increased. At the receiver side, by performing the reverse process of the above process, we can get the original image as the decrypted image. When we are doing this process for any image, the mean square error is zero and the peak signal to noise ratio will be infinite. But, in the process of transmission of the images, there is a possibility that noise may be added to the image. If the salt and pepper noise is used, the mean square error is 18.6918 and the peak signal to noise ratio is 52.2636.

IV. RESULTS

By using the above algorithm for the image encryption, we get the secured image which is not understandable by the unauthenticated person. If the noise is added to the image, the peak signal to output ratio is decreasing and the mean square error is decreasing. To overcome this drawback, we are using the filters of appropriate properties for different types of noises

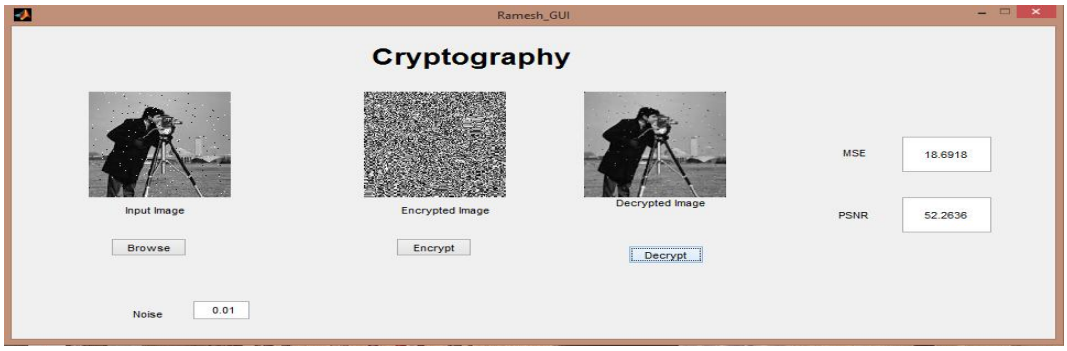


Figure2. Results obtained from MATLAB

The above figure shows the original image, encrypted image and the decrypted image.

The following table shows the mean square error and the peak signal to noise ratio values for different types of noises.

Table1.Results for different types of noises

S.No	Type of noise	MSE	PSNR
1	No noise	0	Infinity
2	Salt and pepper noise	15.0345	53.6181
3	Gaussian noise	45.1329	34.6331
4	Poisson noise	23.4884	47.6951
5	Speckle noise	45.1329	32.8167

V. CONCLUSION AND FUTURE WORK

This paper proposed a modified process in the image encryption process by manipulating both the input image as well as the key. In this paper, we have created a block the blocks of 64 bits of memory and the user is free to take any block at any stage. This work can be done by taking the blocks of 128 bits size, 256 bits size and so on. This process will also be used for the encryption of colour images.

REFERENCES

[1] Soumyendu Das, Subhendu Das, BijoyBandyopadhyay, and SugataSanyal, L. L. 1993. Steganography and Steganalysis: Different Approaches.
[2] AtulKahate, Cryptography and Network Security, 2nd edition,TataMcgraw Hill Education Private Limited, 2011
[3] Xiukun Li, Xiangqian Wu*, Ning Qi, Kuanquan Wang, A Novel Cryptographic Algorithm based on Iris Feature, 2008.
[4] B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani, A Novel Cryptographic Key Generation Method Using Image Features, 2012.
[5] B.Acharya, SK Panigrahy, SkPatra, Image Encryption Using Advanced Hill Cypher Algorithm, 2009.
[6] A.Jolfari, XW Wu, V Muthukkumarasamy, Commenta on the Security of "Diffusion-Substistution Based Gray Image Encryption" Scheme, 2014.
[7] Q Wang, Q Ding, Z Zhang, L Ding, Digital Image Encryption Research Based on dwt and chaos,2008.
[8] Z Lin, H Wang, Efficient Image Encryption Using Chaos-based PWL Memrister, 2010.
[9] PP Dang, PM Chau, Image Encryption for Secure Internet Multimedia Applications, 2000.
[10]Pratik Srivastava, Ratesh Jain, K.S. Raghuwanshi, A Modified Approach of Key Manipulation in Cryptography using 2D Graphics Image, 2014