IMAGE ENCRYPTION USING PERMUTATION AND ROTATIONAL XOR TECHNIQUE

Avi Dixit, Pratik Dhruve and Dahale Bhagwan

Department of Electronics and Telecommunication, Thakur College of Engineering and Technology, Mumbai University, Mumbai, India
avi.dixit25@gmail.com, dhruve.91@gmail.com, swami.dahale@gmail.com

ABSTRACT

Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images.

In this paper, we introduce an algorithm. The binary code of the pixel values of a colour image is extracted and permuted according to the entered 8 bit key which is followed by the permutation of every 8 consecutive pixels [4]. The image is further divided into blocks which are shifted accordingly. The above mentioned technique has a few drawbacks, like the small key size. To further enforce the encryption another method is appended to it which requires a 43 digit key. The encryption takes a total of 10 rounds in which two keys are use, both of which are derived from the 43 digit entered key. The results showed that the correlation between image elements was significantly decreased by using the proposed technique.

KEYWORDS

Image, Encryption and Permutation.

1. INTRODUCTION

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data.

In most of the natural images, the values of the neighbouring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbours). Encryption is the process of transforming the information to insure its security. 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 become more and more important due to the rapid evolution of the Internet in the digital world today. 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.

Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012.
 DOI : 10.5121/csit.2012.2301

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.

In order to dissipate the high correlation among pixels and increase the entropy value, we propose a transformation algorithm that divides the image into blocks and then shuffles their positions. The process continues in this way and three sets of keys are calculated. The three sets are then used to calculate the final 40 digit encryption key. To bring about confusion and diffusion in the encryption process each pixel element influences the next row of pixels. Due to this even a slight change in the pixel value results large changes in the cipher image. The encryption takes place in a total of 10 rounds and in each alternating round a different key is used which is obtained from the encryption key by rotating it periodically. Moreover, after every round the image is divided into four planes and the four planes are cyclically rotated.

2. THE PROPOSED ENCRYPTION TECHNIQUE

2.1. Bit permutation

The image can be seen as an array of pixels, each with eight bits for 256 gray levels. In the bit permutation technique the bits in each pixel taken from the image are permuted with the key chosen from the set of keys by using the pseudo random index generator. The entire array of these permuted pixels forms the encrypted image. The encrypted image obtained from the bit permutation technique is transmitted to the receiver through the insecure channel. At the receiver the encrypted image is decrypted using the same set of keys. As the number of bits in each pixel is eight, we also take the key length equal to eight. The number of permutations obtained with eight elements is 8! (=40320).

2.2. Pixel permutation

In this scheme each group of pixels is taken from the image. The pixels in the group are permuted using the key selected from the set of keys. The encryption and decryption procedure is same as the bit permutation technique. The size of the pixel group is same as the length of the keys, and all the keys are of same length. If the length of the keys is more than the size of pixel group, the perceptual information reduces. In this work the group of pixels is taken along the row without the loss of generality, i.e., the column wise procedure would yield same kind of results.

2.3. Block permutation

In this technique the image can be decomposed into blocks. A group of blocks is taken from the image and these blocks are permuted same as bit and pixel permutations. For better encryption the block size should be lower. If the blocks are very small then the objects and its edges don't appear clearly. In this block permutation the blocks are permuted horizontally in the image. The permutation of blocks along vertical side is also similar to horizontal side block permutation. At the receiver the original image can be obtained by the inverse permutation of the blocks. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbour's. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbour's. At the receiver side, the original image can be obtained by the inverse transformation of the blocks.

2.4. Algorithm Steps

1. Load image.

2. Input the 8 bit key.
3. Convert each decimal pixel value into binary.
4. Repeat step for pixel in all three planes.
5. Rearrange the bits according to the key entered.
6. Convert the permuted value back to decimal.
7. Transfer a row of pixels to a temporary matrix.
8. Permute the pixels according to the key entered.
9. Divide the image into 8 blocks, vertically and horizontally.
10. Rearrange the blocks according to the key entered.

3. RESULTS OF IMAGE ENCRYPTION

Figure 1. Original image (Waterlillies.jpg)

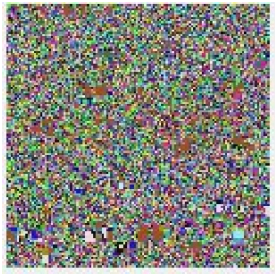

Figure 2. Encrypted image using permutation technique

4. STATISTICAL ANALYSIS

4.1 Histogram of encrypted image

We have selected the 25level bit map image Waterlillies.jpg and its encrypted image and obtained their histograms. Figure 3 shows histograms for this image and corresponding encrypted image. From the figure, one can see that the histogram of the encrypted image (cipherimage) is fairly uniform and is significantly different from that of the original image (plainimage).

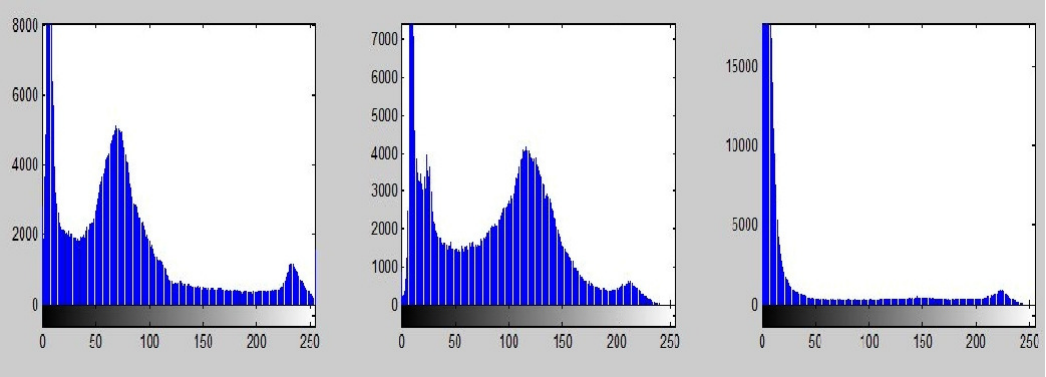

Figure 3. Histogram of plainimage

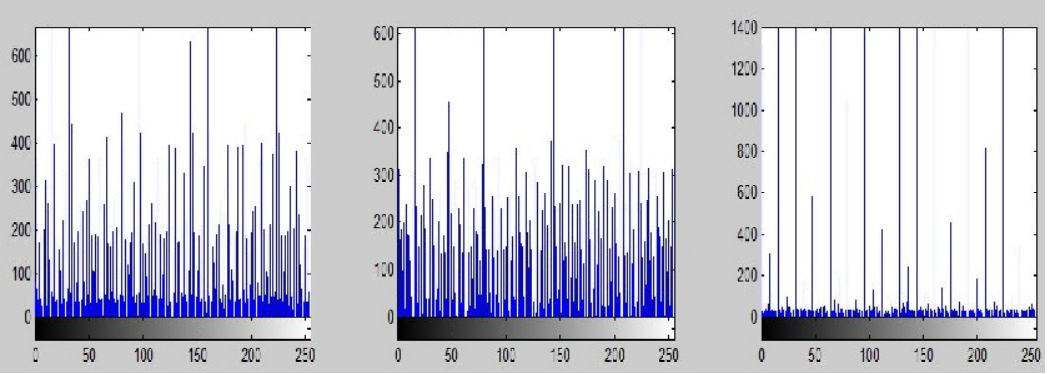

Figure 4. Histogram of encrypted image

4.2 Correlation of two adjacent pixels

Further, we also obtain the correlation graph of the plain and encrypted image. The correlation graph is obtained by taking a pair of consecutive pixels and plotting them on a x-y graph. Due to high level of correlation present in the pl ain image the points are focused very near to the x=y line. From the figure, one can see that the graph of the encrypted image (cipherimage) is fairly uniform and is significantly different from that of the original image (plainimage).

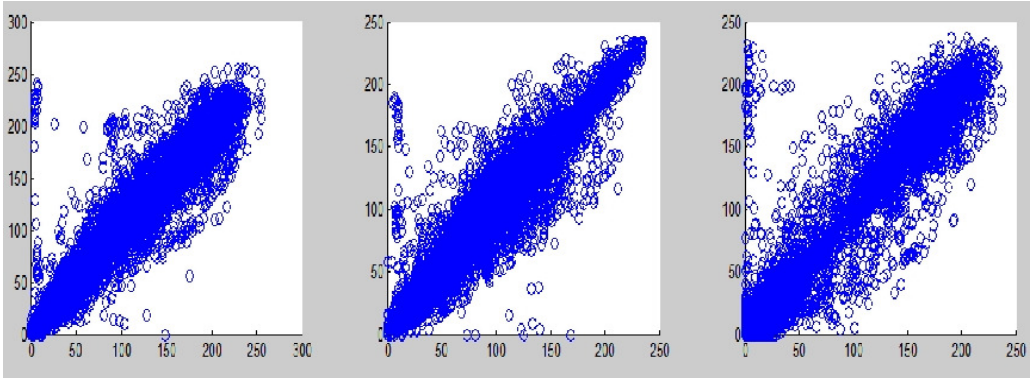

Figure 5. Correlation graph of plainimage

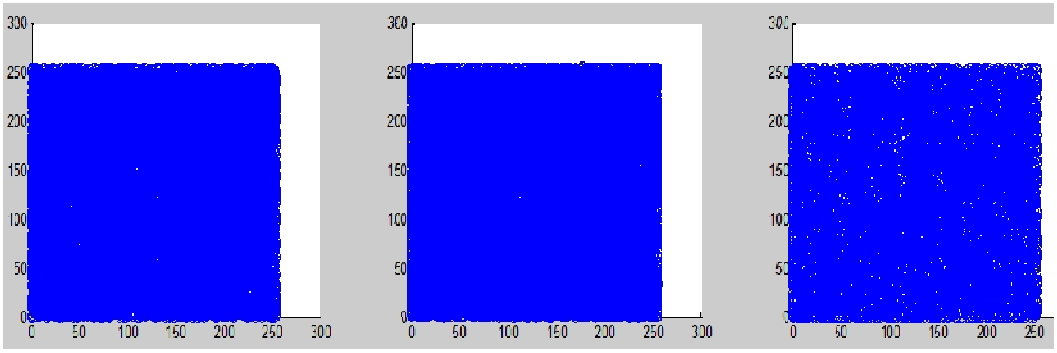

Figure 6. Correlation graph of encrypted image

5. SHORTCOMINGS OF ENCRYPTION

One of the main flaws in the previous permutation encryption technique was the small key size involved which resulted in only 40320 combinations of the key which is very small when compared to the speed of present day computers. Further, there is another problem associated ith this encryption. As the colours depend mainly on the value of the MSB's, any key that does not shuffle the MSB's will not result in an efficient encryption. Encryption techniques need to have two very important qualities which are:

5.1 Confusion

Confusion refers to making the relationship between the plaintext and the ciphertext as complex and involved as possible. In other words, he non-uniformity in the distribution of the individual letters (and pairs of neighbouring letters) in the plaintext should be redistributed into the non-uniformity in the distribution of much larger structures of the ciphertext, which is much harder to detect

5.2 Diffusion

Diffusion means that the output bits should depend on the input bits in a very complex way. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner. In particular, for a randomly chosen input, if one flips the i-th bit, then the probability that the j-th output bit will change should be one half, for any i and j — this is termed the strict avalanche criterion. More generally, one may require that flipping a fixed set of bits should change each output bit with probability one half.

6. IMPROVEMENT IN ENCRYPTION TECHNIQUE

To bring about the above mentioned qualities into the encryption we propose another step in the already performed 8 bit encryption technique. This requires a 43 digit key and takes a total o f ten rounds. The 43 digit key entered is used to calculate the key required for encryption in such a way that a change in one digit of the key would bring about a large change in the encryption process. The figure below shows how the key is calculated.

The 43-digit key entered is used to calculate three set of keys. The 43-digt key is first divided into three parts(1-17,14-30,27-43). What happens here from the process is that it infuses a certain amount of diffusion in the key that makes the encryption technique is even more robust.

Figure 7. First step in key generation

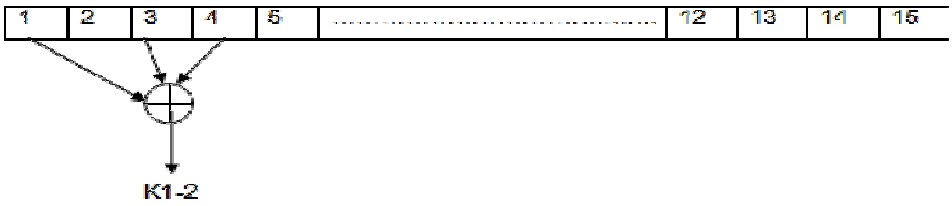

Figure 8. Second step in key generation

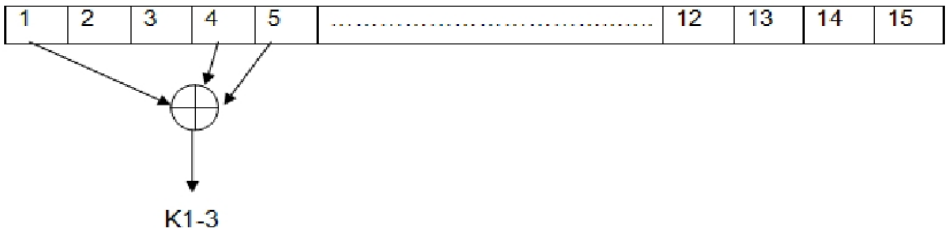

Figure 9. Third step in key generation

The process continues in this way and three sets of keys are calculated. The three sets are then used to calculate the final 40 digit encryption key. To bring about confusion and diffusion in the encryption process each pixel element influences the next row of pixels. Due to this even a slight change in the pixel value results large changes in the cipher image. The encryption takes place in a total of 10 rounds and in each alternating round a different key is used which i s obtained from the encryption key by rotating it periodically. Moreover, after every round the image is divided into four planes and the four planes are cyclically rotated.

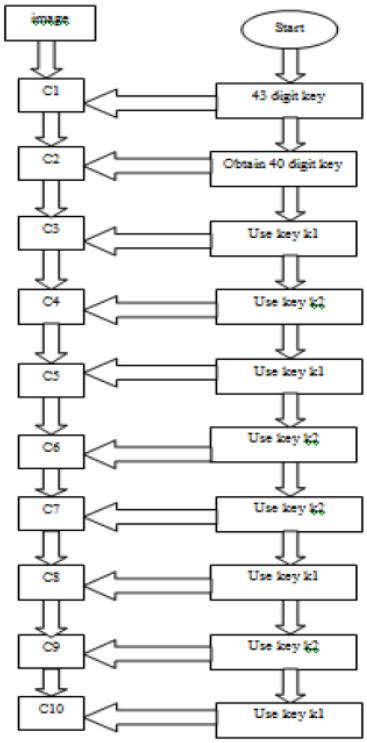

Figure 10. Ten rounds of encryption

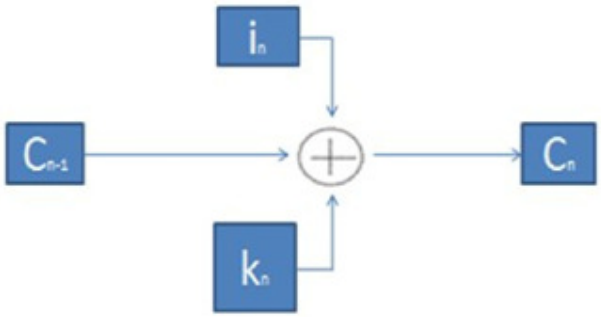

Figure 11. Individual pixel being encrypted

The above figure shows the individual step in each round. These ten steps are appended to initial permutation process which makes it more robust with an initial key size of 8 bits and a secondary key of 43 digits. In this way each pixel value affects each following cipher value as the new cipher value is calculated using the calculations from all the preceding pixels.

7. RESULTS

Figure 12. Original image (Waterlillies.jpg)

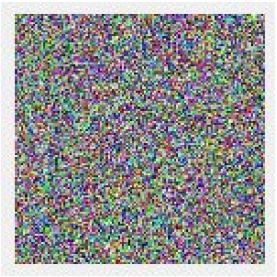

Figure 13. Encrypted image

8. STATISTICAL ANALYSIS

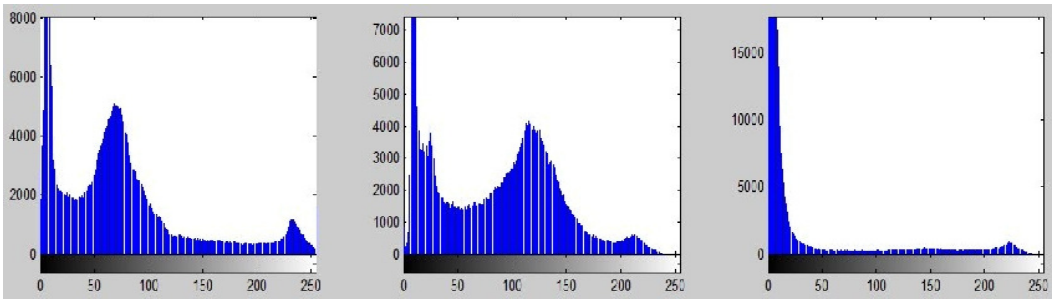

Figure 14. Histogram of plainimage

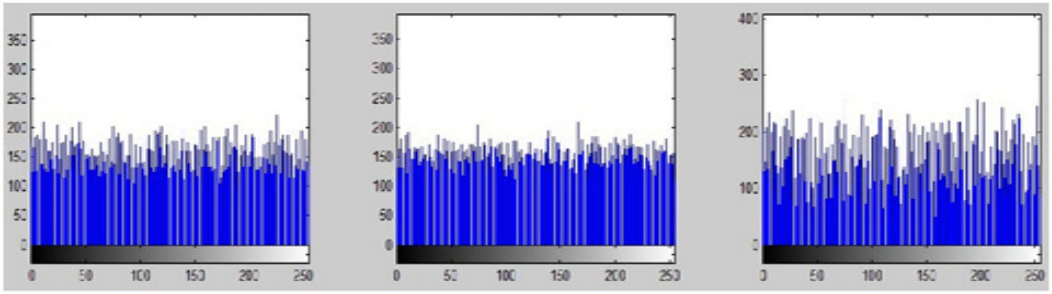

Figure 15. Histogram of encrypted image

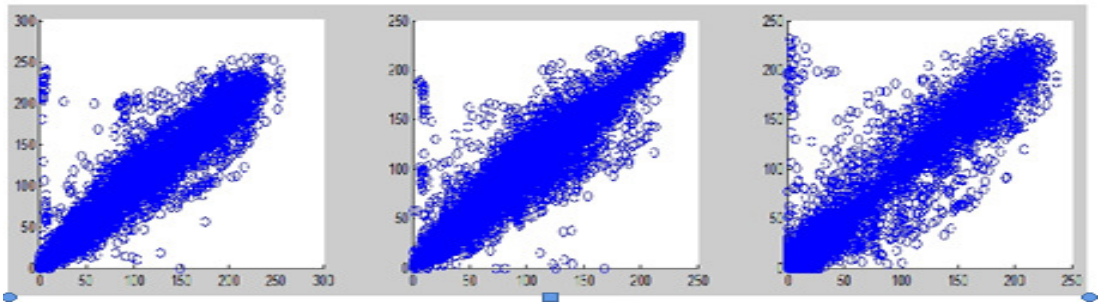

Figure 16. Correlation graph of plainimage

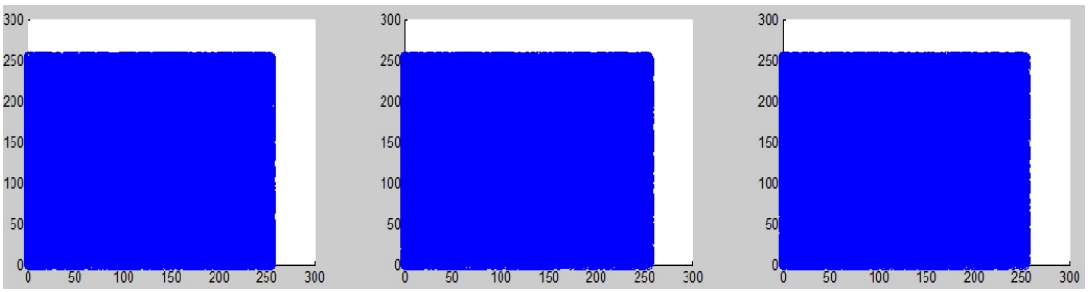

Figure 17. Correlation graph of encrypted image

9. CONCLUSIONS

The proposed encryption process occurs in two steps and utilises two keys: which result in a total of (8!*256^43) combinations. This large key size makes a brute force attack redundant as it is expected that half the keys are tried before a person can crack the key. Further the confusion and diffusion properties used in the second step of encryption make cryptanalysis very difficult.

REFERENCES

[1] [Bor1 02] J.C.Borie, W.Puech, M.Dumas, Encrypted Medical Images for Secure Transfer,

[2] [Bor2 02] J.C.Borie, W.Puech, M.Dumas, Encrypted images for Secure transfer with RSA algorithm

[3] Cryptography and Network Security Principles and Practices 4th Ed - William Stallings

[4] Maps Ismail Amr Ismail1, Mohammed Amin2, and Hossam Diab2 A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic

[5] Chung- Ping Wu, Member, IEEE, and C.-C. Jay Kuo, Fellow, IEEE Design of Integrated Multimedia Compression and Encryption Systems

[6] Goldburg, S. Sridharan, and E. Dawson, “Design and crypt-analysis of transform-based analog speech scramblers,” IEEE J. Select. Areas Commun., vol. 11, no. 5, p. 735, Jun. 1993.