Permutation based Image Encryption Technique

Sesha Pallavi Indrakanti
Associate professor
Department of Computer Applications,
GVP Degree College (A),
Visakhapatnam

P.S.Avadhani
Professor
Department of CS and SE,
Andhra University College of Engineering(A),
Andhra University, Visakhapatnam

ABSTRACT

Information security is the key in the era of electronic data exchange. Images constitute a large portion of the electronic data. Confidentiality of color images is a difficult process. Most of the image encryption algorithms are complex and compromise on the quality of the image. This paper proposes a new image encryption based on random pixel permutation with the motivation to maintain the quality of the image. The values used in the encryption process are preserved in the form of a 64 bit key and sent to the receivers. The receivers jointly use the key and the shares to see the secret.

Keywords

Image, Encryption, Decryption, Security, Permutation.

1. INTRODUCTION

Internet has made life easy and at the same time added complexity to the world of security. The change in technology and the internet over the span of 10 years is a huge one. In earlier days the format of data that was used was only textual, but now with the rapid growth of computer networks large files, such as images, audio and video can easily be transmitted over the internet. These advantages come at a cost, in the form of compromise in the privacy of the data that is being sent. Encryption is the process of transforming the information to ensure its security. There are different data encryption techniques widely available, but the crisis is that most of the available encryption algorithms are designed for textual data. Different types of data demand different aspects, and techniques to protect the confidentiality of data from unauthorized access[2]. The large size of image compared to that of the text demands more time for the encryption process. The textual encryption process demands 100% exact results after decryption, where as image decryption is acceptable with trivial distortion

The security of digital images has become more significant with the rapid progress of the Internet. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Numerous image encryption methods have been proposed to improve the security of the images. The lookout of digital images encryption started from the middle of 1990s[3].The process of secret image transmission has been classified into 3 types: position permutation[4][5], value transformation[1][9] and visual transformation[6]. These methods range from light encryption (degradation), to strong encryption algorithms. A classification of the proposed schemes from the open literature is given in [8].Most of these proposed algorithms concentrate on dividing the image into different blocks which result in a stronger encryption algorithm with less correlation between the shares[7]. A work on the application of Salsa20 for image encryption is also being done [11]. There are lots of work done on the quality comparison of the image encryption techniques [10][12]. Most of the techniques involve lots of computations and compromise on the quality of the color image that is recovered.

2. THE PROPOSED SCHEME

This technique makes use of all the 3 types of classifications like position permutation, value and visual transformation. The technique involves three different phases in the encryption process. The first phase is the image encryption where the image is split into blocks and these blocks are permutated. Further permutation is applied based on a random number to strengthen the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The receiver takes the help of the key to construct the secret image in the decryption process. The technique proposed is a unique one from the others in a way that the key is generated with valid information about the values used in the encryption process. Most of the encryption processes first generate the key and then do the encryption process. This technique generates a relation between the encryption process and the key.

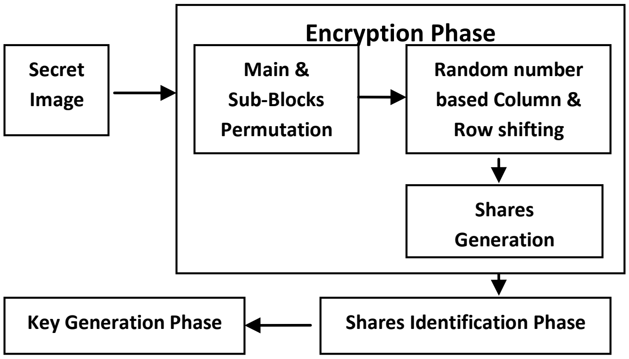
Encryption Phase
Secret Image
Main & Sub-Blocks Permutation
Random number based Column & Row shifting
Shares Generation
Key Generation Phase
Shares Identification Phase

Figure 1.The Proposed Scheme

2.1 Image encryption phase

The image encryption process first selects a random color image of n*n size. This image is split into 4 blocks and numbered. These numbered blocks are shuffled based on the 24 permutations available. Each sub block is further shuffled. A random number is selected which lies in the range of 0 to 255.These rows and columns of the total images are shifted based on the random number that is selected. The algorithms row and column shifting are given below.

Algorithm for row shifting:

```
Incr=0, ranno, temp=0
For i=0 to n
if  temp<n
                  {
              array2[j][i]=array1[j][temp];
              temp=temp+ranno
                  }
          Else
                  {
             Incr++
            Temp=incr
                  }
```

Algorithm for row shifting:

```
Incr=0,ranNo,temp=0
For j=0 to n
if  temp<n        {
              array2[j][i]=array1[temp][i];
              temp=temp+ranNO
                  }
          Else
                  {
             Incr++
            Temp=incr
                  }
```

Where in the above algorithm
array2: RGB values of image after
transformations
array1: RGB values of image before transformations
Temp: Temp value for row or column shifting
ranno: Random number

The above algorithms have to be applied for each row and column. For example if the random number is 23 and image is of size 500*500, row and column co-ordinates of normal image range from 0,1,2,3,…….. 499.
Row and column co-ordinates of image will be shuffled based on random number 23 such as 0,23,46,69…, 1,24,47,70 …, 2,25, 48,71…,499.

2.2 Identification phase

The encryption process gives out 4 shares. Each of these shares has to be numbered distinctly for the identification process. All the 4 shares of the image are numbered uniquely with the same series. These numbers are embedded into the share in the form of a watermark. The same number series is kept in the key. The receiver will compare the number sequence of the shares with that in the key to compute the right secret with the valid shares.

2.3 Key generation phase

All the information about encryption is kept in the key. Most of the encryption processes happens based on the key. Here as stated the key is built after the encryption process. The information used in the encryption process is embedded in the key. The key is 64 bits in size. Each byte is divided into a segment. The key is composed of 8 segments. The classification of key is listed in the table below.

Table 1. Table captions should be placed above the table

Segment	No of bits	Description
1	8	Main block permutation order
2	8	First sub block permutation order
3	8	Second sub block permutation order
4	8	Third sub block permutation order
5	8	Fourth sub block permutation order
6	8	Random number for row and column shifting
7	8	Image co-ordinates (Horizontal & Vertical)
8	8	Share Identification Information

The block permutation which is identified with a number is represented as a binary number in the key. For example if the block combination is 1234 it is represented as 00011011 which is 8 bits in size, same way 2341combination is represented as 01101100. The random number that ranges from 0 to 255 is represented as an 8 bit binary number. As the image is made into 4 shares the share identification information is also embedded into the key for decryption process. The total key is composed of 8 segments each of 1 byte. The key concept that is employed here is unique and provides more security to the image.

2.4 Decryption phase

The process of decryption involves obtaining the key that is generated and the shares. These shares are identified by comparing the information in the key with the watermark. Once the identification process is done the permutation information and the random number from the key is obtained to implement the inverse of the permutations to reveal the secret.

3. RESULTS

The algorithm was applied on a JPEG image of size 500* 500 pixels with 256 colors.

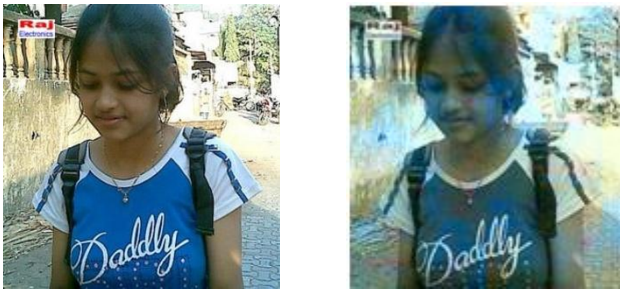

Figure.2 (a) the original image (b) The recovered image

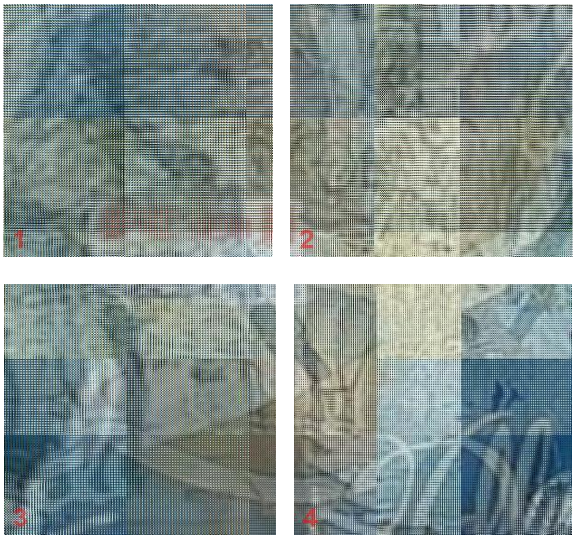

Figure .3 Four watermarked shares

Fig.2 shows the original image before encryption and the recovered image after decryption. Fig.3 shows the four watermarks shares obtained from the encryption process

4. CONCLUSION

The disturbance of the strong correlation among the adjacent pixels assures high security of the images. This can be obtained with the help of permutation process. The proposed technique provides confidentiality to color image with less computations Permutation process is much quick and effective. The key generation process is unique and is a different process. This method can be extended in trying to handle multiple images instead of single image.

5. REFERENCES

[1] Chin-Chen Chang, Min-Shian Hwang, Tung-ShouChen, “A new encryption algorithm for image cryptosystems”, The Journal of Systems and Software, 2001, 83-91

[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] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm", Journal of transactions on engineering computing and technology, December, vol. 3, 2004, p.38.

[4] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, p.127, 2006.

[5] Li. Shujun, Li. Chengqing, C. Guanrong, Dan Zhang., and ikolaos,G., Bourbakis, "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004, http://eprint.iacr. Org/2004/374.pdf

[6] Mohammad Ali Bani Younes and Aman Jantan, “Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, Feb 2008.

[7] Mohammad Ali Bani Younes and Aman Jantan “An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption”, IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.4, April 2008 191.

[8] M. Sharma and M. K. Kowar, “Image Encryption Techniques Using Chaotic Schemes: a Review,” International Journal of Engineering Science and Technology, vol. 2, no. 6, pp. 2359–2363, 2010

[9] Z. H. Guan, F. Huang, and W. Guan, “Chaos-Based Image Encryption Algorithm,” Physics Letter A, vol. 346, pp. 153-157, 2005.

[10] Ismail Amr Ismail, Mohammed Amin, and Hossam Diab, “A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps,” International Journal of Network Security, Vol.11, No.1, PP.1{10, July 2010

[11] Alireza Jolfaei and Abdolrasoul Mirghadri,” Survey: Image Encryption Using Salsa20,” IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010 pg 213-220

[12] A. Jolfaei and A. Mirghadri, “A New Approach to Measure Quality of Image Encryption,” International Journal of Computer and Network Security, vol. 2, no. 8, pp. 38–44, 2010