IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. I (May.-June. 2017), PP 01-05
www.iosrjournals.org

Reversible Datahiding Using Reserved Room Approach with Magic Rectangle Encryption

P.Subashini [1], Jaspal Singh[2], Adipta Biswas[3]
[1.]*Assistant Professor Department Of Computer Science and Engineering, SRM University, Chennai, India,*
[2.]*UG Scholar Department Of Computer Science and Engineering, SRM University, Chennai, India,*
[3.]*UG Scholar Department Of Computer Science and Engineering SRM University, Chennai. India,*

Abstract: *In this project, we are trying to promote security to the data using developed encryption techniques. The image is encrypted using Magic Rectangle (MR) encryption technique, and text using the RSA algorithm with LSB as data concealment technique. The data hiding technique uses LSB replacement algorithm for hiding the secret message bits into encrypted image. By choosing the decryption keys, both the image and encrypted text will be extracted.*
Keywords*: Reversible data hiding, MR encryption, LSB replacement, RSA key encryption.*

I. Existing Method

It is widely used in medical and military purpose for secret data communication. In this system vacating room after encryption(VRAE) is used for allocating the space to hide the data and the pixel difference expansion methods are used. The pixel difference expansion based RDH is the spatial domain process to hide secret text messages within an image. The process involves the adjacent pixel to get subtracted to determine the difference in values. The message bits are affected by the difference produced. This technique produces spatial distortion which reduces the quality of the image produced and it is less compatible. It distorts the image quality wherever the secret message bits are hidden. This will eradicate by the method of least significant bits(LSB).

II. Proposed System

In this system, the Chaos Encryption is being replaced with Magic Rectangle for image encryption, and RSA algorithm is used for text encryption and decryption with LSB as data concealment. MR is used to check the existing problems of public key cryptosystem. MR is helpful in enhancing the security as in terms of its complexity of the encryption process, and it does not change the quality of the image. It also introduces an additional feature of security in the public key algorithm.

III. Methodology

Lifting Wavelet Transform

The lifting wavelet transform is widely used in signal processing in general and in image compression research. In application, such as still image compression, discrete wavelets transform(DWT) based schemes have outperformed other coding schemes like the ones based on DCT. Since there is no need to divide the input image into nonoverlapping 2-D blocks and its basis functions have variable length, wavelet-coding schemes at higher compression ratios avoid blocking articles. Because of their inherent multi-resolution.

Forward transform

Step 1: Column wise processing to get H and L
H= (Co-Ce); L=(Ce+H/2)
Where Co and Ce is the odd column and even column wise pixel values.
Step 2: Row wise processing to get LL, LH, HL and HH, Separate odd and even rows of H and L, Namely, Hodd-odd row of H, Lodd-odd row of L,
Heven-even row of H

Leven-even row of L
LH=Lodd-Leven;
LL=Leven+(LH/2)
HH=Hodd-Heven;
HL=Hodd-Heven;
HL=Heven + (HH/2)

Reverse lifting Scheme

Inverse Integer wavelet transform is formed by the reserve lifting scheme. Procedure is like the forward lifting scheme. Recently the JPEG committee has released its new image coding standard.

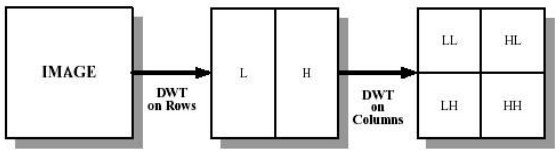


Image Encryption

The plan image is converted into blocks of single bytes and then the block is replaced as the valve of MR. Further, the control parameter of the magic rectangle (MR) selected by the user. The images used will have three bytes extracted, the byte values are transposed as MR values and further encrypted to obtain the cypher text. The numerical process of the MR is displaced from their respective position and encrypted to obtain the cypher text. Therefore, the size of the image is negligible during encryption and decryption.

Fig.1 Cover Image

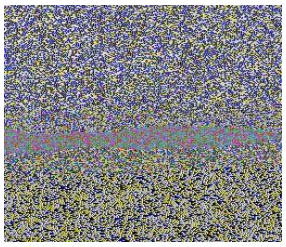


Fig.2 Encrypted Image

Magic Square

The magic square is same as like a magic rectangle. A magic square is defined as an arrangement of integers of the order nxn matrix. The important feature of a magic square is that the sum of all the elements in every column, row and along the two main diagonals are equal. The magic constant of a magic square depends only on n and has the value:

$$M(n) = n(n^2+1) / 2$$

Magic square can be classified into three types: odd, doubly even (n divisible by four), singly even (n is even and not divisible by four).

Magic Rectangle

A magic rectangle of order (mxn) is an arrangement of integers such that the sums of all the elements in every row as well as every column are equal.The magic rectangle is in the category of singly even.ie, the order of the matrix is even but not divisible by the numeral 4 such as 4x6, 8x12, 16x24, 32x48 and so on. Any order with even number can be used in this work. It can be followed only the order 4x6, 8x12, 16x24, 32x48 etc. The size of the rectangle is purely based on the rules of perfect rectangle or golden rectangle and the singly even magic rectangle. It also follows the methodology of divide and conquer strategy. In magic rectangle, column sum is fixed as 32x48. The existing column sum is divided by two and then apply in 16x24, again further the column sum is divided by two and apply in 8x12 matrix etc. This approach is adopted from divide and conquer strategy. The column sum is taken as even value, then it matches exactly in magic rectangle. In case if the column sum is taken as odd value, then the column sum is reduced by one because of fractional values. This paper focuses only a singly even magic rectangle implementation and their usefulness for public key cryptosystem for image encryption and decryption process i.e. the order of magic rectangle must be even.

Creation of singly even magic rectangle

In this work, the singly even magic rectangle is generated by using any seed number, starting number and magic sum. The numbers are generated in consecutive order.

The proposed work uses the notations as listed below:

- MR: Magic Rectangle
- Nxm: Order of MR where n=4a and m=6a where a=1, 2, 4, 8 etc.
- MR_{nxm} :MR of order nxm
- MRB_{4x6} :Base MR of order 4x6
- $MRnxm_{rsum}$:Row sum of MR of order nxm
- $MRnxm_{csum}$:Column sum of MR of order nxm

The values in the MRB_{4x6} are filled as shown in Table 1. The function is called MR4x6 fill order (Min_{start}, Max_{start}).

Table : Magic Rectangle Filling Order

Max_{start}	*(+2)	*(+4)	-6	-16	*(+16)
*(+8)	-10	-12	*(+14)	*(+24)	-24
-14	*(+12)	*(+10)	-8	-30	*(+30)
*(+6)	-4	-2	*Min_{start}	*(+22)	-22

In above table, '*' represents the places in magic rectangle to be filled having its starting point from Min_{start} and incremented by 2 each time to get the next number. The places without '*' in magic rectangle to be filled having its starting point from Max_{start} and decremented by 2 to get the next number.

//Encryption algorithm

Input: Image file (gif/bmp/jpg)

Output: Cipher text(Numeric Value)

Method:

Step1: Read Image File

Step2: Covert Image file into Sequence of bytes Array

Step3: For i= 0 to Barray.length

```
//Bytearray
Begin
    Flag=0;
    If Barray[i] <0 then
        Begin
            pos=-Barray[i];
            Flag=1;          end          else
        pos= Barray[i];
  Rarray[i]=MRarray[pos];  /*MagicRectagle array and  Result   array*/
```

Step 4: Encrypt using Algorithm

```
If Flag=1 then
   Cipher[i]=-Cipher[i];
    //Cipher array
End
```

Step 5: Produce Cipher Text

ASSYMETRIC KEY CRYPTOGRAPHY

Cryptography allows secure transmission of data over insecure passage. Cryptography also allows safe storage of sensitive data on any computer.

RSA- *Public Key Cryptography*

Public key (E) and modulus N are known to all user's private key(D) (Secret key) provides Authentication / Encryption signing / Decryption operation Verifying/ Encryption operation will be done by:

Where,

C-each character of input text message. **N=p*q**

where,

Cyphertext = C^E mod N

N-modulus-parameter

p & q- two largest prime number obtained from user given 8-bit key.

DATA CONCEALMENT

Steganography is a method of embedding addition information into the digital content that is undetectable to listeners. The idea behind the LSB algorithm is to insert the bits of text into the least significant bits of pixels. The most frequently used steganography method is the technique of the LSB substitution. Altering the LSB will only cause minor change in colour, and this is usually not noticeable to the human eye. This technique works well for 24-bit colour image file.

Advantage-The advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of the cover image. Modulating the LSB does not result in human perceptible difference because the amplitude of change is small. Therefore, to the human eye the resulting stego image will look identical to the cover image.

Least Significant Bit(LSB)

In LSB, the RGB values of color image are taken and the color image is converted into grey image. The 256 * 256 intensities values are obtained. Then, the next step is to embed a message into an image. The message is embedded in the intensity values of image obtained during image to matrix conversion. The intensity values are converted to image back. Both the images are identical.

DECRYPTION PROCESS

Decryption of Image:

//Decryption Algorithm:

Input: Cipher Text (Numeric Value)

Output: Image file (gif/bmp/jpg) Method:

Step1: Read Cipher text

Step2: For i= 0 to Cipher.length

```
//cipher array
        Begin
          Flag=0;
          If Cipher[i] <0 then
          Begin
            Cipher[i]=-Cipher[i];
             Flag=1;
          End
```

Step 3: Decrypt using Algorithm

```
        Pos =Marray[i];

  //MagicRectaglearray

          If   Flag=1 then
              Barray[i]=-Pos
```

Step 4: Convert Byte Array into Image

Step 5: Produce Original Image

***Decryption of text*:**

Data decryption will be done by:

Plaintext= Cypher^ D mod N.

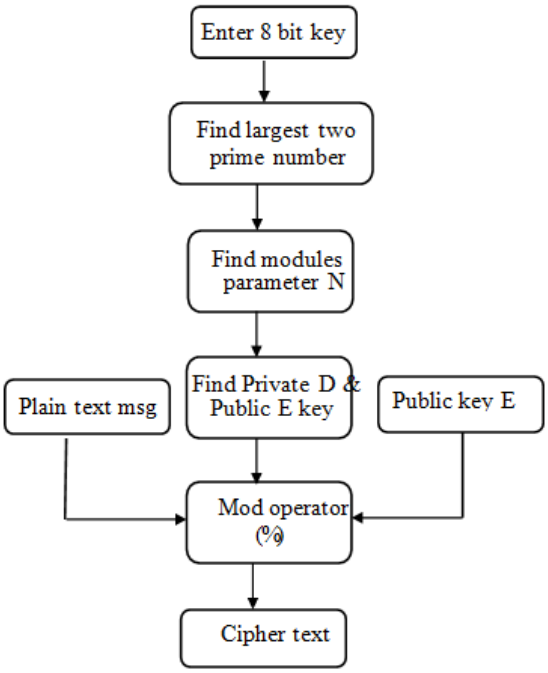
Extracting the message:

(i) Declare the message byte.

(ii) Here, the size of the message is 8-bits.

(iii) Read each pixel, starting address=0.

(iv) Extract LSB & replace ith bit in the message byte where i=1 to 8, when i=8 a byte is extracted.



i=8 a byte is extracted.

IV. Conclusion

The project presented that protection of image quality and hidden data during transmission, based on the approach of reserve room technique and MR encryption with LSB based data concealment.

References

[1]. Champakamala B.S Padmini.K, Radhika D.K Asst Professor "Least Significant Bit algorithm for Image Steganography",International Journal of Advance Computer Technology,volume 3,Number 4.
[2]. KedaMa,Weiming Zhang, Xianfeng Reserving room before Encryption".IEEETrans.Information Forensics and Security, vol 8 No.3 March 2013.
[3]. M. Johnson, P. Ishwar, +V.M.Prabhakaran,D.Schonberg, and K.Ramchandran,"On compressing encrypted data,"IEEE Trans. Signal Process.,vol.52,no. 10,pp.2992-3006,Oct. 2004.
[4]. W. Liu, W.Zeng, L.Dong, and Q.yao,"Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol 19,no.4,pp.107-1102, Apr.2010
[5]. X. Zhang," Lossy compression and iterave reconstruction for encrypted image,"IEEE Trans. Inform. Forensics Sceurity, vol.6,no. 1,pp. 53-58,Feb.2011.
[6]. T.Bianchi, A.Piva, and M.Barni,"On the implementation of discrete Fourier transform in tge encrypted domain," IEEE Trans. Inform. Forensics Security, vol.4, no.1,pp.86-97,Feb.2009.
[7]. KedaMa,Weiming Zhang, Xianfeng Zhao"Reversible Data Hiding in Encrypted images by Reserving Roomm Before Encryption",IEEETrans .Information Forensics and Security.,vol 8 No.3 March 2013.
[8]. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data,"IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[9]. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images,"IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010
[10]. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image,"IEEE Trans. Inform. Forensics Security,vol. 6, no. 1, pp. 53–58, Feb. 2011.
[11]. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.
[12]. A.J.Menezes ,P.C.Van Oorschot, and S.Vanstone , "Handbook of Applied cryptography", CRC Press, Boca Ration,Florida, USA,1997.
[13]. Gopinath Ganapathy, and K.Mani , " Add-On Security Model for publickey Cryptosystem Based on Magic Square Implementation", ISBN 978-988-17012-6-8, Proceedings of the world congress on Engineering and Computer Science 2009 Vol I, San Fransisco, USA.