Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1265 – 1271

RESEARCH ARTICLE

Utilizations of LSB Matching and Replacement for Efficiency Improvement in Digital Secret Communication

Nisha.M.J[1], G.H.Asha[2], Anandh Kumar.V[3], Mahendar.R[4]

[1]Department of E&C, MCE Hassan, Karnataka

[2]Associate Professor of E&C, MCE Hassan, Karnataka

[3]Assistant Professor, Department of ECE, SECE, Tamilnadu

[4]Department of ECE, Anna University, Tamilnadu

[1] nishamj22@gmail.com; [2] ashaghmce@gmail.com; [3] anand.kkr@gmail.com; [4] rajmahendar09@gmail.com

Abstract— To develop and check the Steganography based information's by using Matlab this proposal investigates the detection of information hidden in digital media by both the least significant bit (LSB) matching and replacement scheme. Which can completely recover the original images without any distortion from the secret images by utilizing the parity features of the original images and defining two embedding pairs are used embeds hidden message via LSB matching and replacing the LSB of the cover image with the MSB of the message image will help us to form a stego image which would contain the message. This message can be retrieved only by that receiver who knows that it is a stego image sent by the sender. The proposed method always has lower distortion for various levels of abstractions. Experimental results disclose that the proposed method not only provides better performance and size reductions than those of OPAP and DE, but also is secure under the detection of some well-known steganalysis techniques tested here.

Keywords— LSB; stego; MSB; Matlab; DE; OPAP

I. INTRODUCTION

digital Data hiding is a method of hiding secret messages into a cover-media such that an not planned observer will not be aware of the fact of the hidden messages. Colour images are used as a medium to hide images are called cover-images. Original images with the hidden messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the secret data and data rate. In the literature, many techniques about data hiding have been proposed. One of the common techniques is based on manipulating the least significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the embedded message bits. LSB methods typically achieve higher capacity and security. The distortion formed by data embedding is called the embedding distortion .A good stegno method should be capable of avoid visual and statistical detection while providing an adjustable equipment. The least significant bit substitution method, referred to as LSB in this paper, is a well-known data-hiding method. This method is easy to implement with low CPU cost, and has become one of the popular embedding techniques [2]. However, in LSB embedding, the pixels with even values will be increased by one or kept unmodified. The pixels with odd values will be decreased by one or kept unmodified. Therefore, the imbalanced embedding distortion emerges and is vulnerable to steganalysis.

The LSB and OPAP methods employ one pixel as an embedding unit, and conceal data into the right-most m LSBs. Another group of data-hiding methods employs two pixels as an embedding unit to conceal a message digit rB in B-ary notation system. We term these data-hiding methods as pixel pair matching (PPM). Proposed an LSB matching method based on PPM. He used two pixels as an embedding unit. The LSB of the first pixel is used for carrying one message bit, while a binary function is employed to carry another bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance a pixel value has to be changed by one yet another 1/4 chance no pixel has to be modified. Accordingly, the MSE is defined as the square of error between cover image and stego-image. The distortion in the image can be measured using MSE.

II. IMAGE STEGANALYSIS

Algorithms for image steganalysis are primarily of two types: Specific and Generic. The clearly defined approach represents a variety of image steganalysis techniques that very much based on the underlying steganographic algorithm used and have a high success rate for detecting the presence of the secret message if the message is hidden with the algorithm for which the techniques are meant for.[1],[2] The Generic approach shows a variety of image stegano techniques that are independent of the understood steganography algorithm used to hide the message and produces good results for detecting the presence of a secrete message hidden using new and/or unconventional steganographic algorithms. The image steganalysis techniques under both the specific and generic categories are often designed to detect the presence of a secret message and the decoding of the same is considered complementary not mandatory[3].

$$\text{Image} = 0.3*R+0.59*G+0.11*B; \quad [1]$$

$$\text{MSE}= ([1/M*N]^2 \sum_{i=1}^{q} \sum_{i=0}^{n} (Ri - R'i))^2 \quad [2]$$

The mean square error is calculated by using 2 equations, where R_i is The intensity value of the pixel in the original image,R'_i is shows the intensity value of the pixel in the stego image and M*N is a Size of an Image.

A) Peak Signal Noise Ratio (PSNR)

It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. it measures the statistical difference between the cover and stego-image, is calculated using Equation 3.

$$PSNR=10\log_{10} (2\text{^}8)^2/MSE \text{ db} \quad [3]$$

B) Histograms

Histogram is a find of the number of occurrence of pixels with respect to particular pixel value [4]. During embedding pixel value changes hence number of pixel having a particular pixel value changes. These changes can be used to detect steganography. Hence lesser the difference of histograms of cover and stego-image indicates more resistivity to detect.

In this project LSB with pseudo random generator is implemented. Matlab in built pseudo-random number generator is used for this purpose and seed to this is taken as key of steganography. First of all an array of random numbers, with the length equal to secret bit stream, is generated using key. Then with the help of this array, different pixel positions are calculated. Now secret bits are embedded to LSB of these pixels. The algorithm for embedding process is as below [4],[5].

III. EMBEDDED ALGORITHM FOR ENCRYPTION/DECRIPTION

The embedded algorithm can be shows that many methods have been proposed to improve LSB embedding schemes. On the one hand, it has been proposed to improve embedding efficiency by using coding theory. Roughly speaking, the idea is to gather several samples and, using coding theory, to embed more than one bit of hidden data for each modification of cover medium samples [5], On the other hand, focusing on image steganography, it has been proposed to choose the pixels in textured areas on the assumption that those areas are difficult to model and, hence, hidden bits should be more difficult to detect [6], the recently proposed HUGO algorithm [7] selects pixels location by minimizing a distortion function. However, those steganographic methods rely on LSB embedding and the detection of simple LSB matching is a first step to addressing the detection of improved algorithms.

Input: original image, secret key, secret message (text, image)

A) Procedure:

Step1: Convert the secret message into bit stream (Length L)

```
msg_type = input('Enter 1 for TEXT Message, 2 for IMAGE Message:\n');
                    if msg_type == 1
[FileName,PathName] = uigetfile('*.txt','Select TEXT MESSAGE.');
          testmsg = fopen( strcat(PathName,FileName) );
[msg] = fscanf(testmsg,'%c');
                   elseif msg_type == 2
[FileName,PathName] = uigetfile({'*.jpg';'*.png';'*.gif';'*.bmp'},'Select IMAGE MESSAGE.');
 msg = imread( strcat(PathName,FileName) );
```



```
                                    else
        error('Invalid Message Type Selection');
                                      end
```

Step2: Generate L number of pseudo random number using enc-key key

```
      enc_key = input('Please Enter an Encryption Key Between 0 - 255:\n');
      if enc_key < 0 || enc_key > 255
      error('Invalid Key Selection');
              end
      enc_key = uint8(enc_key);
```

Step3: Calculate the OPAP pixel positions in the cover image

```
  for i = 1 : height
     for j = 1 : width
        LSB = mod(double(c(i,j)), 2);
       if (k>m || LSB == b(k))
          s(i,j) = c(i,j);
       else
          if(LSB == 1)
             s(i,j) = c(i,j) - 1;
          else
             s(i,j) = c(i,j) + 1;
          end
       k = k + 1;
     end
     end
  end
```

Step4: Choose the seed pixel positions in the cover image

```
   encode = input('Enter 1 for Sequential Encoding, 2 for Random Encoding:\n');
     if encode == 1
     % SEQUENTIAL ENCODING: This only needs an Encryption Key Input.
     output = stegancoder(img,msg,enc_key);
   elseif encode == 2
     % RANDOM ENCODING: This needs the Encryption Key AND Random Seed
     %   Value.
     % Random Seed Value
     randSeed = input('Please Enter Random Seed Value Between 1 - 100:\n');
```



```
    if randSeed < 1 || randSeed > 100
       error('Invalid Random Seed Value')
    end
     randSeed = uint8(randSeed);
    % Final Output
    output = stegancoder_Rand(img,msg,enc_key,randSeed);
  else
    error('Invalid Encoding Selection');
  end
```

Step5: while complete bit stream not embedded

{Replace LSB of pixel denoted by ith pixel position, with secret bit
Insert pixel into cover image
}

End

Output: Stego-image

From this algorithm we have to analysis various hidden and retrieve methods and utilize the cover image with stego data without any distortion almost.

IV. ANALYSIS OF SECURITY AND EFFICIENCY

We have to analysis both security and efficiency of the proposed method, since we have to use both LSB replacement and LSB matching. The goal of steganography is to evade statistical detection. It is shows that MSE is not a good measure of security against the detection of steganalysis. For example, low-MSE embedding such as LSB replacement is known to be highly detectable but provide good resolutions rather than LSB matching. In this proposal, we analyse the security of APPM under two statistical steganalysis schemes, including Subtractive Pixel Adjacency Matrix (SPAM) steganalyzer proposed by[7] and the HVDH scheme proposed .[1],[8]. SPAM steganalyzer is a novel Steganographic method for detecting stego images with low-amplitude independent stego signal, while the HVDH scheme is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms.

A. Security Analysis by using SPAM

SPAM is a most powerful technique for detecting stego images with independent random stego signal for which typically not found in natural digital images [9]. SPAM obtains the features of images by calculating the transition probabilities along eight directions, and the number of features is determined by the SPAM order and the range of difference N. A soft-margin support vector machine (SVM) with Gaussian kernel is employed to implement the steganalyzer.

The error rate is calculated by equations 4

$$Q_{err} = \tfrac{1}{2}(Q_{fp} + Q_{fn}) \qquad [4]$$

In equation 4 we evaluate the security of a data-hiding method against the detection of SPAM, where Qfb and Qfm is the probability of false positive and false negative, respectively. The higher the error rate, the lower the detectability.To evaluate the detectability of APPM using SPAM, we trained the SPAM steganalyzer on images obtained from UCID and RSP image databases, respectively. the below table shows the calculations of our proposal

Table 1

MSE COMPARISON

image	**8bit LSB**	**8bit OPAP**	**APPM(Efficiency)**
Eman.jpg	8.32	4.27	32.16
SMOKES.BMP	8.42	4.335	32.09
6.jpg	8.71	4.35	32.71

V. **SIMULATIONS AND RESULT**

The simulations result is done by MATLAB Version10.1 and above (R2011b) is used to implement and simulate 4 steganography techniques: LSB matching and replacement Distortion of spatial domain steganography is checked by seed value herewith sequential and random seeding value has to be used. MATLAB is used because of large number of advanced inbuilt functions and image processing toolbox. We take results for various colour cover image for different secret files. We saw that visual quality of spatial domain steganography is better than transform domain techniques.

Table 2

Work done conclusions

Cover image pixel size (N*N*3)	N=128,256,512,1024
Secret text file size	Possible to hide 1kb to 128kb
Secret image file size	Embedded rate whatever may be (30kb to few mb)
Image type	Jpeg,tiff,bmp

VI. **CONCLUSIONS**

From our analysis we have to concluded the utilizations of both LSB matching and replacement for steganography system for both security and efficiency purpose. The effectiveness of the proposed methods has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).furthermore for seed value we have to test both sequential and random value. The spatial domain techniques provide high PSNR, high ability of quality and high embedding capacity but these not provide robustness. On the other side transform domain provide robustness while providing very less embedding capacity, low PSNR and low perceptual quality. At final stage we have to combine matching and replacement method provides robustness even though the embedded rate whatever maybe. The paper also presents cast the detection of data hidden with the LSB matching scheme

within the framework of hypothesis testing theory. Asymptotically maximizes the detection power whatever the hidden data embedding rate might be, is presented. Second, the detection power of the proposed AUMP test is analytically calculated.

REFERENCES

[1] Wien Hong et.al "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching" ieee transactions on information forensics and security, february 2012.

[2] Rémi Cogranne, Member, IEEE, and Florent Retraint "An Asymptotically Uniformly Most Powerful Test for LSB Matching Detection", IEEE transactions on information forensics and security, march 2013.

[3] J. Fridrich and J. Kodovský, "Steganalysis of LSB replacement using parity-aware features," in Information Hiding.NewYork,NY,USA: Springer, 2012, LNCS.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. San Mateo, CA, USA: Morgan Kaufmann, 2007.

[5] J. Harmsen and W. Pearlman, "Higher-order statistical steganalysis of palette images," inProc. Security, Steganography, and Watermarking of Multimedia Contents V, 2005, vol. 5020, Proc.

[6] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp.868–882, Jun. 2012

[7] O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran, and B. Manjunath, "Detection of hiding in the least significant bit,"IEEE Trans.Signal Process., vol. 52, no. 10, pt. 2, pp. 3046–3058, Oct. 2004

[8] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," Pattern Recognit.

