Edge Adaptive Image Steganography using LSB Matching Revisited

Miss. Vaishali V. Jadhav [1], Mrs. P.P.Belagali,[2] Ms.Sapana Kishor Soudagar [3] , Ms.Pooja Adgonda Patil [4]

[1]*(Dr.J.J.Magdum College Of Enggineering, Jaysingpur / Shivaji University,Maharashtra)*
[2]*((Dr.J.J.Magdum College Of Enggineering, Jaysingpur / / Shivaji University,Maharashtra)*
[3]*Asst.prof., Electronics dept., Dr. J.J.M.C.O.E., Jaysingpur, Dist -Kolhapur,Maharashtra* [4]*Asst.prof.,*
[4]*Electronics dept., Dr. J.J.M.C.O.E., Jaysingpur, Dist -Kolhapur,Maharashtra*

ABSTRACT : *The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. The LSB matching revisited image steganography with an edge adaptive scheme can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quailty of stego images at the same time.*

Keywords *- steganography ,*

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet.

II.Different kinds of steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement. The four main categories of file formats that can be used for steganography.1 Text 2 Images 3 Audio/video 4 Protocol

2.1 Image steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

2.2 Image and Transform Domain

Image steganography techniques can be divided into two groups:

2.2.1. Image Domain (also known as spatial domain) **-** Embed messages in the intensity of the pixels directly.

2.2.2. Transform Domain (also known as frequency domain)-Images are first transformed and then the message is embedded in the image.

In Image Domain Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover image.

The best known steganographic method that works in the spatial domain is the LSB steganography

2.3. LSB Steganography In this method the lowest bit plane of a bitmap image is used to convey the secret data. It is extremely simple to implement. The eye cannot detect the very small perturbations introduced into an image. LSB methods are commonly used among the many free steganography tools available on the internet.

Two types of LSB steganography are listed below:

2.3.1. **LSB replacement** is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms, such as the Chi-squared attack [9], regular/singular groups (RS) analysis [10], and sample pair analysis [11].

2.3.2. LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then +1or -1 is randomly added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM.

III. LSB matching revisited (LSBMR)

IT uses a pair of pixels as an embedding unit, in which the LSB of the first pixel carries one bit of secret message, and the relationship (odd–even combination) of the two pixel values carries another bit of secret message. In such a way, the modification rate of pixels can decrease from 0.5 to 0.375 bits/pixel (bpp) in the case of a maximum embedding rate, meaning fewer changes to the cover image at the same payload compared to LSB replacement and LSBM. It is also shown that such a new scheme can avoid the LSB replacement style asymmetry, and thus it should make the detection slightly more difficult than the LSBM approach based on our experiments. The typical LSB-based approaches, including LSB replacement, LSBM, and LSBMR, deal with each given pixel/pixel pair without considering the difference between the pixel and its neighbors.

3.1 Data embedding & Data extraction using LSBMR

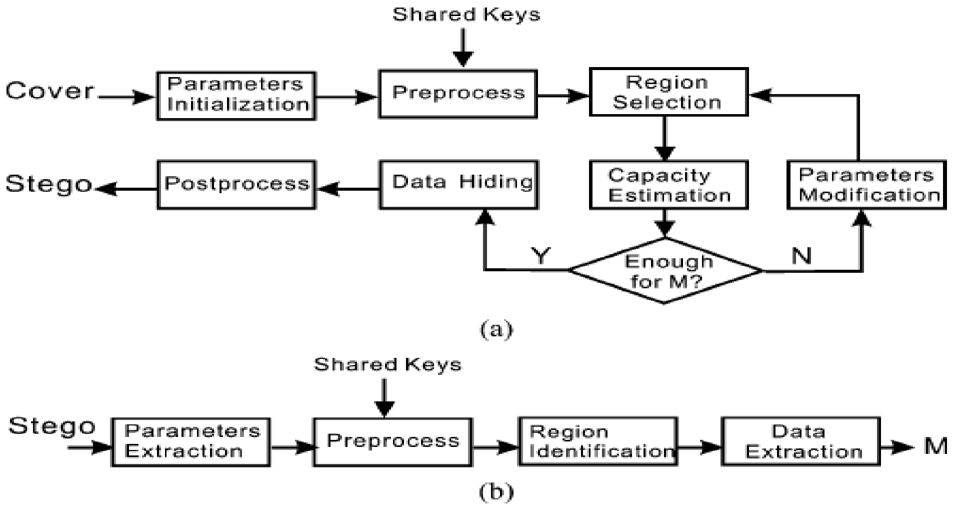

Fig: 3.1Data embedding & Data extraction

3.1.1 Data embedding

The flow diagram of LSBMR scheme is illustrated in Fig a,b. In the data embedding stage(Fig a.), the scheme first initializes some parameters, which are used for subsequent data preprocessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message M, then data hiding is performed on the selected regions. Finally, it does some post processing to obtain the stego image. Otherwise the scheme needs to revise the parameters, and then repeats region selection and capacity estimation until M can be embedded completely. Please note that the parameters may be different for different image content and secret message M. We need them as side information to guarantee the validity of data extraction. In practice, such side information (7 bits in our work) can be embedded into a predetermined region of the image.

3.1.2 Data extraction

The data extraction scheme is illustrated in Fig b. In data extraction, the scheme first extracts the side information from the stego image. Based on the side information, it then does some preprocessing and identifies the regions that have been used for data hiding. Finally, it obtains the secret message M according to the corresponding extraction algorithm.

IV. Data embedding & Data extraction algorithms

In this LSBMR, a region adaptive scheme to the spatial LSB domain is applied. The absolute difference between two adjacent pixels is the criterion for region selection, and use LSBMR as the data hiding algorithm. The details of the data embedding and data extraction algorithms are as follows.

Step1

The size of cover image is m x n. Divide it into non overlapping blocks Bz X Bz.
Rotate the each block by random degree in the range of {0,90,180,270}.
This is determined by secret key K1.
The resulting image is rearranged as row vector V.
The row vector is divided into non overlapping embedding units with every consecutive pixels (Xi,Xi+1),Where i=1, 3… (mn-1).

Benefits obtained by the random rotation.

- It can prevent the detector from getting the correct embedding units without the rotation key, (k1) and thus security is improved.
- Both horizontal and vertical edges (pixel pairs) within the cover image can be used for data hiding.

Step2

According to the scheme of LSBMR, 2 secret bits can be embedded into each embedding unit. For the given message M , the threshold T for region selection is determined as

T= {2 x |EU (t)|>= |M|}

Where

EU (t) = set of pixel pairs whose absolute differences are greater than or equal to parameter t

$$EU(t) = \{(x_i, x_{i+1}) \| x_i - x_{i+1}| \geq t, \forall (x_i, x_{i+1}) \in V\}.$$

|EU (t)|= total no of elements in set of EU (t)
t Є {0,1,…..31}
|M|= size of secret message M

Step3

We deal with following embedding units in a pseudorandom order determined by secret keyK2

$$EU(t) = \{(x_i, x_{i+1}) \| x_i - x_{i+1}| \geq t, \forall (x_i, x_{i+1}) \in V\}.$$

4.1 Data Embedding

For each unit (Xi, Xi+1) the data hiding according following four cases

a. **LSB (x_i) = m_i & f (x_i, x_{i+1}) = m_{i+i}**
(x_i’,xi_{+1}’)= (x_i, x_{i+1})

b. **LSB (x_i) = m_i & f (x_i, xi_{+1}) ≠ m_{i+i}**
(x_i’,xi_{+1}’)= ($x_{i,}$,x_{i+1}+r)

c. **LSB (x_i) $\square$ m_i & f (x_i-1, x_{i+1}) = m_{i+i}**
(x_i’,xi_{+1}’)= (x_i-1,x_{i+1})

d. **LSB (x_i) $\square$ m_i & f (x_i-1, x_{i+1}) ≠ m_{i+i}**

$$(x_i',xi_{+1}')=(x_i+1,x_{i+1})$$

Where m_i and m_{i+1} denotes two secret bits to be embedded.
(x_i',x'_{i+1}) denotes pixel pair after data hiding

- Where mi & mi+1= two secret bits to be embedded
- Function f is, f(a,b)= LSB ([a/2]+b)
- r= random value in {-1,+1}
- Xi’,X’i+1= pixel pair after data hiding

Step 4

- After data hiding divide the resulting image is divided into non overlapping blocks (Bz x Bz). Bz={1,4,8,12}
- Rotate the blocks by a random number of degrees based on key K1
- Process is very similar to **Step 1** except that the random degrees are opposite.
- Then embed the two parameters(T,Bz) into a preset region which has not been used for data hiding.

4.2 Data Extraction

- First extract the side information,i.e., the block size Bz and the threshold T from the stego image
- The stego image is divided into blocks Bz X Bz
- The blocks are then rotated by random degrees based on the secret key K1
- The resulting image is rearranged as a row vector V’.Finally, we get the embedding units by dividing V’ into non overlapping blocks with two consecutive pixels
- We travel the embedding units whose absolute differences are greater than or equal to the threshold T according to a pseudorandom order based on the secret key K2, until all the hidden bits are extracted completely.

V. Properties of LSBMR method

- It can first choose the sharper edge regions for data hiding according to the size of the secret message by adjusting a threshold.
- The larger the number of secret bits to be embedded, the smaller the threshold T .Which means that more embedding units with lower gradients in the cover image can be released.
- When T is 0, all the embedding units within the cover become available.In such a case, this method can achieve the maximum embedding capacity of 100% For the PSNR, the LSBMR method performs best.
- The object qualities including PSNR and wPSNR of LSBMR stegos are nearly the best among the seven steganographic methods

VI. Advantages

- It can avoid the LSB replacement style asymmetry & make the detection slightly more difficult than LSBM approach.
- Security performance of LSBMR is better.
- LSBMR is having Maximum embedding capacity.
- With the help of LSBMR method modification rate decreases from .5 to .375 bits/pixel in case of max embedding rate .So fewer changes in cover image Assuming that cover image is made up of many non overlapping small images (regions)and different regions have different capacities for data hiding ,we can choose the sub image with good hiding characteristics while leaving others unchanged .
- Generally the regions located at the shaper edges present more complicated statistical features and are highly dependent on image contents .So it is more difficult to observe changes at sharper edges than those in smooth regions.

VII.Conclusion

There usually exist some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the LSB of stego images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a

PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. To preserve the statistical and visual features in cover images, the LSBMR scheme is used which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. Furthermore, it is expected that our adaptive idea can be extended to other steganographic methods such as audio/video steganography in the spatial or frequency domains when the embedding rate is less than the maximal amount.

Referances

[1]A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[2]F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 16–19, 2007, vol. 1, pp. 401–404

[3]C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008. [5]J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[4]J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[6] A. Ker, "Improved detection of LSB steganography in grayscale images," in *Proc. Inf. Hiding Workshop, Springer LNCS*, vol. 3200, 2004, pp. 97–115.

[7] , "Quantitive evaluation of pairs and RS steganalysis," in *Proc. SPIE Security, Steganography,Watermarking Multimedia Contents*, vol. 5306, E. J. Delp III and P. W. Wong, Eds., 2004, pp. 83–97.

[8] A. Westfeld, "Detecting low embedding rates," in *Proc. Inf. Hiding Workshop, Springer LNCS*, vol. 2578, 2002, pp. 324–339.

[9] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proc. 3rd Int. Workshop on Information Hiding*, 1999, vol. 1768, pp. 61–76.

[10] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001.

[11] S. Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7, pp. 1995–2007, Jul. 2003.

[12]"Edge Adaptive Image Steganography Based on LSB Matching Revisited "Weiqi Luo, *Member, IEEE*, Fangjun Huang, *Member, IEEE*, and Jiwu Huang, *Senior Member, IEEE*