IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

An effective Image steganography using LSB Matching Revisited

Miss. Vaishali V. Jadhav [1], Mrs. P.P. Belagali[2]

Dr.J.J. Magdum College Of Engineering, Jaysingpur, Shivaji University, Maharashtra, India[1,2]

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, LSBM, LSBMR, edge adaptive LSBMR.

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. 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

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

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 Steganography Using LSBM

If secret bit does not match with LSB of cover image then +1 or -1 is randomly added to corresponding pixel value. Asymmetry effect is avoided because probability of increasing or decreasing for each modified pixel value is same. LSBM works as low pass filters on the histogram of image. This means the histogram of stego image contains fewer high frequency components compared with histogram of its cover.

Using this property a detector method is introduced which uses Centre of Mass (COM) of Histogram Characteristic Function (HCF). But original HCFCOM method does not work on gray scale images. So the new method is introduced which is effective for gray scale as well as for JPEG. In this the down sampled image & adjusting histogram is used.

2.3.3 Steganography Using LSBMR

This uses pair of pixels as an embedding unit. LSBMR, deal with each given pixel/pixel pair without considering the difference between the pixel and its neighbours. First pixel carries one bit of information & relationship of two pixel values carries another bit of secret message.

III. EDGE ADAPTIVE LSBMR

Most existing steganographic approaches usually assume that the LSB of natural covers is insignificant and random enough, and thus those pixels/pixel pairs for data hiding can be selected freely using a PRNG. However, such an assumption is not always true, especially for images with many smooth regions. The uncompressed natural images usually contain some flat regions (it may be as small as 5x 5 and it is hard to notice), and the LSB in those regions have the same values (1 or 0).

Therefore, if we embed the secret message into these regions, the LSB of stego images would become more and more random, which may lead to visual and statistical differences between cover and stego images (appearing as a noise-like distribution). Our human vision is sensitive to slight changes in the smooth regions, while it can tolerate more severe changes in the edge regions.

Compared with smooth regions, the LSB of pixels located in edge regions usually present more random characteristics, and they are statistically similar to the distribution of the secret message bits (assuming a 1/0 uniform distribution).

Therefore, it is expected that fewer detectable artifacts and visual artifacts would be left in the edge regions after data hiding. Furthermore, the edge information is highly dependent on image content, which may make detection even more difficult. So this scheme will first embed the secret bits into edge regions as far as possible while keeping other smooth regions as they are.

3.1 Data embedding & Data extraction using LSBMR

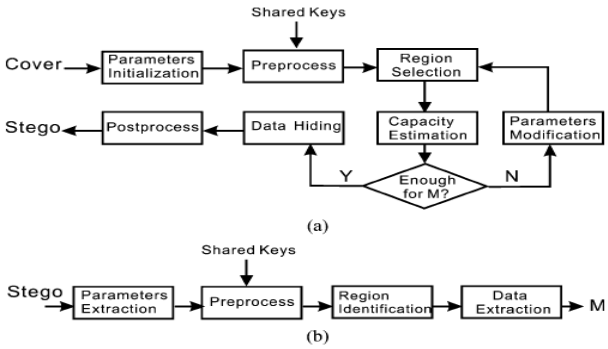

Fig: 3.1Data embedding & Data extraction

3.1.1 Data embedding

The flow diagram of LSBMR scheme is illustrated in Fig 3.1 In the data embedding stage(Fig 3.1), 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. RESULTS OF ALGORITHM

4.1 Image Acquisition

The cover image is shown in Fig. 4.1.

Fig. 4.1 Cover image(1)

Cover image is selected and converted to gray scale image. Converted image shown in Fig. 4.2. Secret image is selected and preprocessed it. Secret image is as shown in Fig. 4.3. and 4.4.

DOI 10.17148/IJARCCE.2016.5304

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Fig. 4.2 Cover image – Gray scale

Fig. 4.3 Secret image - Original

Fig. 4.4 Secret image – Gray scale

Consider the threshold value equal to 80 then region selection is as shown in Fig 4.5

Fig. 4.5 Region selection for T=80

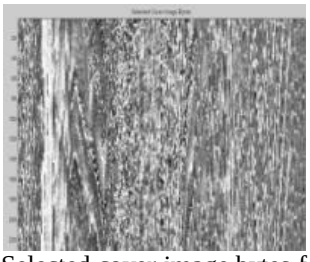

Fig. 4.6 Selected cover image bytes for T=80

Cover image is converted into non overlapping blocks and is as shown in Fig. 4.7 The blocks are rotated 180^0 and as shown in Fig. 4.7 The cover image is arranged as row vector 'V'. This vector is divided into non-overlapping embedding units as shown in Fig. 4.8.

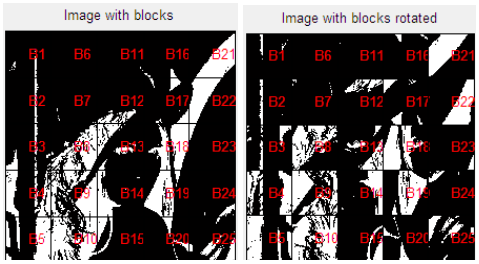

Fig. 4.7 Image with blocks & Image with Blocks rotated with angle 180^0

Cover image bit mask is generated as shown in Fig. 4.8 Secret image is converted into bit streams. Here all the bytes in the secret image (data) are converted in the binary.

Fig. 4.8 Cover image bit mask

4.2 Data Hiding:

The data i.e. generated bit stream is hidden into available embedding units of cover image. Here we use LSBMR method for data hiding. The cover image with hidden secret image is called stego image. This stego image is stored as shown in Fig4.9 The angle of rotation and secret key i.e. password are also hidden in the cover image.

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

Case #1: $LSB(x_i) = m_i$ & $f(x_i,x_{i+1}) = m_{i+1}$
$(x'_i, x'_{i+1}) = (x_i, x_{i+1})$;

Case #2: $LSB(x_i) = m_i$ & $f(x_i,x_{i+1}) \neq m_{i+1}$
$(x'_i, x'_{i+1}) = (x_i, x_{i+1}+r)$;

Case #3: $LSB(x_i) \neq m_i$ & $f(x_i-1,x_{i+1}) = m_{i+1}$
$(x'_i, x'_{i+1}) = (x_i-1, x_{i+1})$;

Case #4: $LSB(x_i) \neq m_i$ & $f(x_i-1,x_{i+1}) \neq m_{i+1}$
$(x'_i, x'_{i+1}) = (x_i+1, x_{i+1})$;

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}

X_i', X'_{i+1}= pixel pair after data hiding.

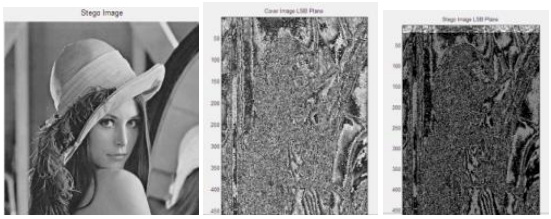

Fig 4.9 Stego Image and LSB Plane of Cover Image & stego Image

DOI 10.17148/IJARCCE.2016.5304

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

4.3 Data Extraction

Then the image is decrepted to find hidden data. This data is in the form of array. This array is used to reconstruct the secret image. This decrypted secret image is " as shown in Fig. 4.10.

Fig. 4.10 Decrypted secrete Image

Here we use LSBMR method for data hiding. The cover image with hidden secret image is called stego image. This stego image is stored. The angle of rotation and secret key i.e. password are also hidden in the cover image.

To decrypt the secret image from stego image we have to enter password i.e. secret key. If secret key matches then we get angle of rotation from key. With the help of this angle we rotate the each block anticlockwise.

Region Selection and embedding capacity using threshold T:

1. The LSBMR scheme uses a pair of pixels as an embedding unit. In this LSB of first pixel carries on bit of secret image and relationship (odd-even combination) of the two pixel values carries another bit of secret image. In such a way the modification rate of pixels can decrease from 0.5 to 0.375 bits / pixel (bpp) in the case of maximum embedding rate i.e. fewer changes to cover image.
2. One of the important properties of LSBMR method is that it can first choose the sharper edge regions for data hiding according to size of secret image by adjusting threshold value T.
3. According to LSBMR scheme two secret bits can be embedded into each embedding unit. Therefore for a given secret image threshold T is determined for region selection.

The threshold T must be

$$\mathbf{T} = \mathbf{arg\,max}\{\mathbf{2} \times |\mathbf{EU(t)}| \geq |\mathbf{M}|\}$$

Where M = size of secret image
|EU(t)| = Total number of elements in set of EU(t)
EU(t) = set of pixel pairs

4. For the lower embedding rates only sharper edges with in the cover image are used, while keeping smooth regions as they are, by adjusting threshold T. When embedding rate increases more regions can be released by increasing the threshold T means T becomes larger for more embedding units.

When T = 255 all the embedding units within the cover image become available. In such case LSBMR achieve the maximum embedding capacity i.e. 100%.

For different values of T region selection in cover image is shown as below.

Fig. For T=120

Cover Image Embedding size = 14241 Bytes

Fig. For T=100

Cover Image Embedding size = 83521 Bytes

Fig. For T=80

Cover Image Embedding size =57121 Bytes

Fig. For T=60

Cover Image Embedding size = 39601 Bytes

Fig. For T=50

DOI 10.17148/IJARCCE.2016.5304

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Cover Image Embedding size = 23409 Bytes
Sumary of the Experiment 1 is shown in Table 4.1.

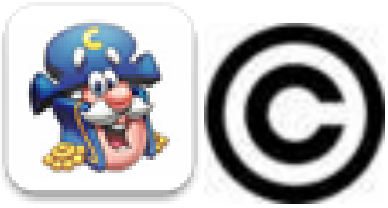

Fig Secrete Image 1 & Secrete Image 2

TABLE 4.1: ANALYSIS OF ALGORITHM [For T = 80]

Cover Image	Secrete image	Embedding Rate	Bits Available	Bits Hidden	PSNR in dB
1	1	36.1957	795675	28800	58.3121
1	2	25.1359	795675	20000	59.4442

V. EXPERIMENT II

The above said algorithm is also verified using the following cover images and secret images. The cover image is Mandir image and secret images are shown below.

Fig. . Cover Image(2) (Mandir) for second experiment

TABLE 5.2: ANALYSIS OF ALGORITHM

Cover Image	Secrete image	Embedding Rate	Bits Available	Bits Hidden	PSNR in dB
2	1	38.4000	750000	28800	58.1361
2	2	26.6667	750000	20000	59.3171

VI. CONCLUSION AND FUTURE WORK

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.

REFERENCES

[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]. [4] J. Mielikainen, “LSB matching revisited,” IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.
[5]. A. Ker, “Improved detection of LSB steganography in grayscale images,” in Proc. Inf. Hiding Workshop, Springer LNCS, vol. 3200, 2004, pp. 97–115.
[6]. “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.
[7]. A. Westfeld, “Detecting low embedding rates,” in Proc. Inf. Hiding Workshop, Springer LNCS, vol. 2578, 2002, pp. 324–339.
[8]. A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” in Proc. 3rd Int. Workshop on Information Hiding, 1999, vol. 1768, pp. 61–76.
[9]. 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.
[10]. 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.
[11]. “Edge Adaptive Image Steganography Based on LSB Matching Revisited “Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE