NOVATEUR PUBLICATIONS

International Journal Of Research Publications In Engineering And Technology [IJRPET]
ISSN: 2454-7875
VOLUME 2, ISSUE 2, Jan. -2016

A STEGANOGRAPHY TECHNIQUE FOR HIDING IMAGE IN IMAGE USING LSB MATCHING REVISITED

Miss. Vaishali V. Jadhav [1], Mrs. P.P.Belagali,[2]
[1](Dr.J.J.Magdum College Of Enggineering, Jaysingpur / Shivaji University,Maharashtra)
[2]((Dr.J.J.Magdum College Of Enggineering, Jaysingpur / / Shivaji University,Maharashtra)

ABSTRACT:

The LSB (Least significant bit) approach is very popular when it comes to steganographic algorithms especially in spatial domain. In most of the existing approaching methods, the obvious choice is to select embedding positions within a cover image mainly have a influence on a pseudorandom number generation without consideration the relationship of size of the secret message and image content itself. Therefore flat regions in the cover image will inevitable be mixed after data hiding even at a tiny embedding rate which may results in poor visual quality or maybe even a low security based on a results of extending research. The usage of LSB matching revisited image steganography with added advantage of edge adaptive scheme.

Keywords - steganography, LSBMR etc.

I. INTRODUCTION

Usage of the internet is increasing day by day and it is welcome move by the information technology sector. Cryptography is technique named to sending or encrypting the messages over secure channel. The cryptography technique is user for encrypt and decrypt the data in order to maintain the secret communication. But it is very unfortunate sometimes it cannot maintain the secrecy of the messages that is sent over communication channel and keeping existence of the secret messages that is sent over communication channel is also important. The technique for doing this is called steganography.

a. Steganography concepts

Steganography is one of the ancient technique, the modern approach to steganography is been developed by the simmons [9], where two inmates have communicated the escape plan over the hatch. Their communication channel was a warden who is to keep them at solitary confinement and she would be able to suspect any type of covert communication [10]. The warden was having rights to inspect all communication made by inmates, and communication can be of two types one is active and other one is passive. A passive type of warden examines communication made by inmates for potentially unsecure messages. If warder suspects a communication contains some hidden information, a passive warden will note same. An active type of warden will try to alter the communication, in order to remove the information [5]

II. DIFFERENT KINDS OF STEGANOGRAPHY

Steganography is supported by all types of digital formats, but some formats having high degree of redundancy are more suitable for steganography. The redundancy is defined as the bits of a particular object that provides accuracy far greater than actually needed for usage of objects and display. The use of redundant bits of an objects are those bits that can be altered without alteration being detected easily, different kinds of images and audio files are more suitable for that. Figure 1 shows the four main categories of file formats that can be used for steganography

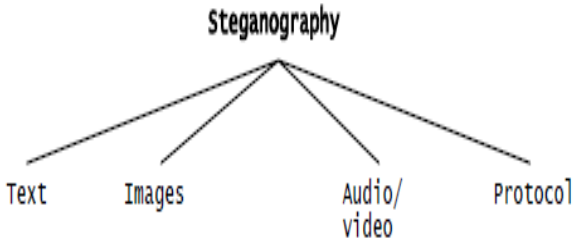

Fig 1: Categories of steganography

A. Image steganography

Images are the most popular objects used for steganography, in the domain of digital images many formats are available and most of them are made for specific applications. Important thing in steganography is for different file format, different steganography technique is used.

B. Image steganography techniques

Image steganography techniques can be divided into two groups:

a. Image Domain (also known as spatial domain) – In this messages are embedded in the intensity of the pixels directly.

b. Transform Domain (also known as frequency domain)- The message is embedded in the image which are already transformed

While working image domain least significant bit (LSB) insertion is very common and simple approach for embedding information in a cover image.
The best steganographic method in the spatial domain is the LSB steganography.

C. . LSB Steganography

Particularly the work is carried out on a LSB for last bitmap image for conveying the secret data. LSB steganography is very simple and convenient to implement. Introduced small perturbations cannot be detected by a human eye. The LSB steganography algorithms are freely available on the internet. Here two major types of LSB steganography are discussed.

a. LSB replacement

LSB replacement is well established steganographic method. In this embedding scheme, only the LSB plane of cover image is overwritten with the secret bit stream according to algorithm implemented or pseudorandom number generator (PRNG). As a result it is possible to have a some structural a symmetry (not decreasing even pixels and increasing odd pixels when hiding the data) is implemented.

b. . LSB matching (LSBM)

LSB matching technique is little bit superior as compared to LSB replacement. In this technique if LSB of the cover image and secret bit does not match, then +1 or -1 is added arbitrarily to corresponding pixel value.

II. LSB matching revisited (LSBMR)

This technique is best and uses pair of pixels as an embedding unit. LSBMR, LSBMR, deal with each given pixel/pixel pair without considering the difference between the pixel and its neighbors. First pixel carries one bit of information & relationship of (odd–even combination) of two pixel values carries another bit of secret message, and the relationship of the two pixel values carries another bit of secret message. By applying this technique the modification rate of pixels can decrease from 0.5 to 0.375 bits pixel (BPP) particularly in the case of a maximum embedding rate. This simply means fewer changes to the cover image even at payload as same as before when compared to two previous techniques.

A. LSBMR used for Data embedding & Data extraction

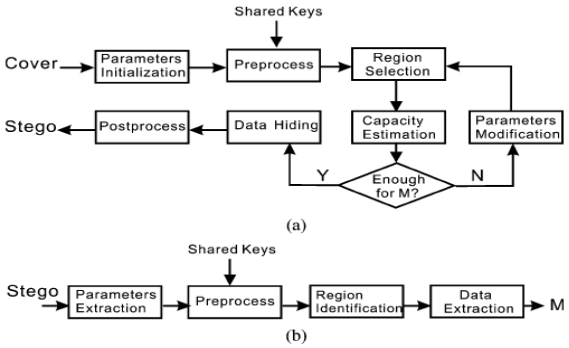

Fig: 2 Data embedding & Data extraction

a. Data embedding with LSBMR

The flow diagram of LSBMR is given in Fig. No.2. There are two stages, first stage is called as data embedding stage and second stage is called as data extraction stage. In first stage some parameters are initialized, which can be useful for subsequent data preprocessing and selection of region and then the capacity of those selected regions. If the regions are large in size for burying the given secret message M, then data burying or hiding can be performed in selected regions. At the final stage, processing is done for getting the stego image. If this process is not happening then algorithm must be designed for revision of the parameters, and further processing should be as earlier should be carried out. In general, such side information can be embedded into a predetermined region of the image.

b. Data extraction with LSBMR

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.

III. Data embedding & Data extraction algorithms using LSBMR

In this LSBMR (Least significant bit matching revisited), a region adaptive scheme is implemented. The absolute difference between two adjacent pixels is the criterion for region selection, and use LSBMR as the data hiding algorithm.

A. Preprocessing

The cover image of size m x n is divided into non overlapping blocks Bz X Bz. Each block is rotated by random degree in the range of {0,90,180,270}.The angle of

rotation 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).

Fig 4.1 shows gray image with blocks rotated

Benefits of the random rotation.

Security is improved as it can prevent the detector from getting the correct embedding units without the rotation key, (k1) .

Both horizontal and vertical edges (pixel pairs) within the cover image can be used for data hiding.

Fig. 3 Gray Image with blocks rotated

B. Region selection

According to this scheme, two secret bits can be embedded into each embedding unit. The threshold T for region selection for given message M 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 Image M

Fig 4. Secrete Image to be hidden

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

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

C. Data Embedding

The data hiding for each unit(Xi, Xi+1) 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 & $f(x_i, xi_{+1}) \neq m_{i+i}$**
$(x_i', xi_{+1}') = (x_{i,}, x_{i+1}+r)$

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

d. **LSB (x_i) ≠ m_i & $f(x_i\text{-}1, x_{i+1}) \neq m_{i+i}$**
$(x_i', xi_{+1}') = (x_i+1, x_{i+1})$

Here

m_i and m_{i+1} = two secret bits to be embedded.

(x_i', x'_{i+1})= pixel pair after data hiding

Function f is, f(a,b)= LSB ([a/2]+b)

r= random value in {-1,+1}

Fig 5 Stego Image

D. Postprocssing

After data hiding work is completed divide the resulting image (fig. no.5) into non overlapping blocks (Bz x Bz). Then the blocks are rotated in arbitrary manner to generate random number of degrees based on key, but the random degrees are opposite in direction sometimes. Then at last two parameters (T, Bz) are embedded into a preset region which is not used for data hiding.

E. Data Extraction

First the side information, i.e., the block size Bz and the threshold T is extracted from the stego image The stego image is divided into Bz X Bz blocks. Then the blocks are 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 i.e. secret image (Fig 4.4) is extracted completely.

Fig. 6 Recovered Secrete Image

V. Properties of LSBMR method

By adjusting threshold T it can first choose the sharper edge regions for data hiding according to the size of the secret image. The larger the size of secret bits to be embedded, the larger the threshold T .When T is 255, all the embedding units within the cover becomes 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

VII. Conclusion

There is natural existence of some smooth regions in natural images, which may causes the LSB of cover images not to be completely random or it may be even to contain some texture information. If embedding technique is used for messages in these regions, the LSB of stego images becomes more random and research data is to believe it is easy to detect. The LSBMR scheme is firstly used for embedding the secret messages particularly into the sharper edge regions adaptively according to a threshold depends on the size of the secret message and gradients of content edges. However, research shows that implemented idea while writing this paper can be extended for any other steganographic methods such as audio/video steganography in the spatial or may be in frequency domains, especially 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]J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Area in Communications*, May 1998

[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] Simmons, G., "The prisoners problem and the subliminal channel", *CRYPTO*, 1983

[10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", *Proceedings of the 2nd International Workshop on Digital Watermarking*, October 2003

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

[11] 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.

[12] 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.

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