International Journal of Research in Advent Technology (IJRAT)
Vol. 1, No. 3, October 2013, ISSN: 2321–9637

Steganography Based on LSB Insertion Technique

P.U.Deshmukh[1] Prof.Tareek pattewar [2]
[1,2]Computer Engineering Dept.
R. C. Patel Institute of Technology
North Maharashtra University
[1] priyanka.deshmukh78@gmail.com

ABSTRACT:

Least significant bit technique is one of the popular techniques. In steganography,least significant bits of cover are altered by the secret data bits. But changing the LSB's of pixels in smooth regions in the cover image at lower embedding rate will forms the poor visual quality and asymmetry into the stegos ,hence anyone can easily detect the secret data from cover. Instead of using smooth regions, edge regions from the cover are selected for data embedding purpose. In our proposed method, edge regions are selected according to size of secret message and difference between the pixel pairs. Using such a new scheme will helps to increase visual and statistical artifacts of stegos there by improving the goal of steganography.

Keywords: *Content-based steganography; least-significant- bit (LSB)-based steganography; steganalysis.*

1. INTRODUCTION

Embedding secret data that is hiding data into medium is often referred to as steganography. Steganography can be applied electronically by taking a binary file and some sort of cover that is often a sound or image file and combining both to obtain a "stego-object".Steganography is the tech. for hiding data in digital media like images,audio,video etc. steganalysis is the tech. by which it will expose the presence of hidden secret messages in those stego media that is digital media. If a steganalytic algorithm find whether a given media is a cover or not with a higher probability ,the steganographic system is considered broken.Steganography will be considered more successful when chances of finding hidden secret message through given media very low. There are two properties, undetectability and embedding capacity, should be carefully considered when designing a steganographic algorithm. If large amount of secret data is embedded in to a cover, then more chances of detecting the hidden message through stego.Undetectability means probability of finding hidden data from a stego should be more in case of steganography keeping the embedding rate high.. In this paper, we consider digital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain.

At the beginning their objectives have required the user to provide the original cover as well as the stego-object. The best regions to hide are first identified in that original cover, then these areas are mapped across to the stego-object and then the hidden data is retrieved. Though, to provide the original object is not safe, since taking the differences between the two objects would be enough to suspect the presence of the hidden data.

1.1. *LSB replacement,LSBM,LSBMR*

By using pseudorandom number generator LSB of pixels are changed by the secret bits.Beause of which asymmetry will introduced and one can easily find the presence of secret data by some methods like chi -squared attack regular/singular groups (RS) analysis,sample pair analysis , and the general framework for structural steganalysis.In LSB matching (LSBM) there is a small change as compare to that of LSB replacement [1].It will just checks the secret bit with that of LSB of the cover image, then+1 or -1is randomly added to the corresponding pixel value. In such a case, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry that is introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM. In LSB replacement and in LSBM tech only it will consider pixel values but in case of LSBMR(LSB matching revisited) ,it will consider pair of pixels as an embedding unit, in which the LSB of the first pixel carries one bit of secret message, and the relationship of the two pixel values carries another bit of secret message. This tech helps to avoid LSB replacement style asymmetry, and hence it should make the detection of secret message through cover more difficult than the LSBM approach.

LSB replacement, LSBM, LSBMR are the methods which consider pixel/pixel pair they are not deal with difference between the pixel and its neighbors. Where as in edge adaptive schemes hiding secret bits are done by replacing the LSB of a cover according to the difference values between a pixel and its four touching neighbors.
This tech. modifies the LSB of image pixels when hiding data, it can be easily detected by different steganalytic algorithms, such as the RS analysis .Hiding data through sharper edges of cover but still the security issues are poor.

In LSB based algorithms selection is mainly determined by a PRNG while it is not considering the relationship between the image content and the size of the secret message. Because of which, these tech. can spread the secret information over the entire stego object randomly even at low embedding rate. But according to analysis and extensive experiments, we find that such embedding methods yield poor security or visual quality of the stego images. For increasing security and visual quality we are using edge adaptive scheme and apply it to the LSBMR-based method[1].

2. STEGANOGRAPHIC ALGORITHMS

Different steganographic methods such as LSB based that are LSBM (LSB matching), LSBMR (LSB matching revisited),some edge based methods adaptive edges with LSB (AE-LSB) , and hiding behind corners (HBC) and our proposed method we are going to examine. For LSB based methods process of hiding data is same that is they are using the PRNG(pseudo random number generator).By which it is travelling through the cover ,it will select pixel and will replaces the LSB of pixels .It will replaces the lower order planes keeping the higher order planes preserved. Same in case of LSBMR, in which according to PRNG it will travel through the cover select the pixel then will match LSB of pixel with secret bit which we are going to embed accordingly will add +1 or -1 to pixel value. In case of LSBMR it will again going to use PRNG by which it will select pixel pairs, first secret bit is added to LSB of first pixel and next secret bit is added to LSB of relationship between the pixels.

2.1. *PSNR, wPSNR, Avg. rate of modification*

Table.1. Avg.PSNR, Avg.wPSNR,Avg.Rateof Modification over 10 images

Embedding rates	Stganographic algorithms		Average PSNR	Avg. wPSNR	Avg. rate of modificati on
10%	LSB based	LSBM	59.2	60.3	0.04900
		LSBMR	61.3	62.0	0.04750
	Edge based	AE-LSB	45.0	53.3	0.02340
		HBC	60.0	65.0	0.04270
	Proposed		62.3	70.0	0.03290
30%	LSB based	LSBM	57.0	62.9	0.1295
		LSBMR	65.2	77.0	0.1195
	Edge based	AE-LSB	51.2	53.2	0.0723
		HBC	54.9	52.1	0.1213
	proposed		58.2	63.3	0.1146
50%	LSB based	LSBM	55.1	64.0	0.1973
		LSBMR	65.2	57.0	0.0195
	Edge based	AE-LSB	51.2	54.7	0.1542
		HBC	53.9	59.2	0.1258
	proposed		54..6	57.2	0.1983

Table1shows average PSNR, average wPSNR, and the modification rate over 10 stego images with different steganographic algorithms and embedding rates.

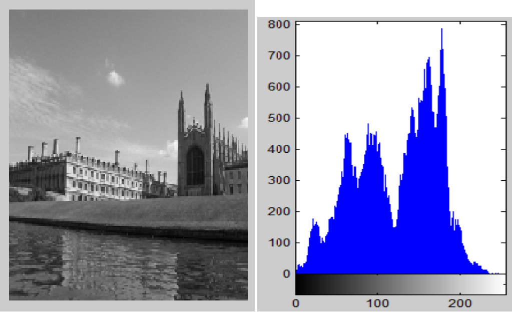

Fig.1. Original Image

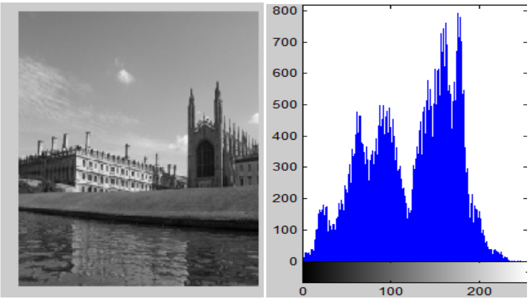

Fig.2. LSBM

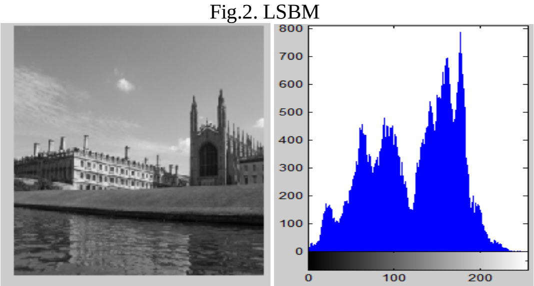

Fig.3. LSBMR

In the LSB of pixels positioned in edge regions mostly shows more random characteristics, and they are statistically alike to the distribution of the secret information bits .Hence, it is predictable that fewer detectable artifacts and visual artifacts would be left in the edge regions after data hiding. Also, the edge information is extremely dependent on image content, Because of which it will make detection of secret message harder. Proposed method keeps the smooth regions preserved and embeds the secret bits into edge regions as far as possible .The HBC method possesses this property.

2.2. *HBC method*

However, the HBC method just modifies the LSBs while keeping the most significant bits unaffected; Hence, it can be regarded as an edge adaptive case of LSB replacement, and the LSB replacement style asymmetry will also occur in their stegos. Hide Seek uses a arbitrary seed to pick the order in which it will write to the pixels. Hide Seek is much safer than Blind Hide, but does not necessarily leave the image in a improved state. The noise introduced by Hide Seek is arbitrarily located and often causes the resulting stego-image to look speckled. Hide Seek and Blind Hide is much obvious to the human eye in big blocks of colour – whereas single modified pixel stands out amongst its consistent neighbors'. This is presented by the Laplace formula. The Laplace formula calculates the difference between a pixel and its four touching neighbors. The magnitude of the formula increases with the colour difference and this can be used to find out steganography by counting the number of pixels at a given magnitude. Untouched images are more likely to contain a huge number of pixels with zero magnitudes because of which there is no cause for small arbitrary variations to occur in huge blocks of colour.In case of HBC will use th Battlesteg method. BattleSteg means *Battle*ships *Steg*anography and is done by playing an augmented game of Battleships to find out the best areas to hide. In this method, the *h*% of highest filter values is considered as ‘ships’. ‘Shots’ are arbitrarily picked pixel positions on the cover, until ship is found there called as a hit. After a hit is done , the series of shots are observed around the ships area.. BattleSteg is expected to avoid pixels in large blocks of colour than Hide Seek, hence it possesses security.

3. PRPOSED METHOD

In our proposed scheme, it will first initialize some parameters, and hence does data preprocessing and region selection, and then it will find the capacity of those selected regions. If these regions are adequate for hiding our secret message, then we will perform data hiding on these selected regions. After that, it does some post processing to get the stego image. Or else we again need to continue the same process. Parameters that we are using for pre and post processes may be different for different image content and secret message for retrieving the data that is secret bits will get firstly the parameters from the stego object. It then does some preprocessing and identifies the regions that have been used for data hiding. After that, it obtains the secret message.

3.1. ***Data Embedding***

For embedding the secret data into cover we need to divide it into non overlapping blocks or pixel. We rotate the block by some degree in the range of (0,90,180,270).By which degree we are going to rotate it it is decided by some key. That is we are doing the raster scanning of the image. After that some non overlapping embedding units are observed that are the consecutive pixels such as $x_{i,}$ $x_{(i+1)}$ .Where we are going to embed our secret data.

In our proposed method we are using LSBMR method. According to LSBMR, 2 secret bits can be inserted into the consecutive pixels. For which suppose we are taking 2 consecutive pixels that are x_{i} ,$x_{i+1.}$ Also selecting the region for data hiding purpose we need to set some threshold values.
Suppose the threshold is T .

Also we need to set the difference between the pixel pair. Suppose t is the difference between the pixel pair. And let EU(t) be the set of pixel pairs whose difference is greater than or equal to the‘t’.EU(t) can be calculated as below

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

For calculating the threshold value of T we are using the formula

T=arg max$\{2^*| \text{EU}(t) |\geq |M|$

|M| is the size of message M that is the secret message. Here we are performing the data hiding process on the embedding unit of pixel pair. The embedding unit is selected by secret key randomly. For hiding the secret data to the selected embedding unit should be done according to following cases.

$$\text{LSB}(x_i)=m_i ,\ \& \ f(x_i ,x_{i+1})=m_{i+1}$$
$$(x'_i , x'_{i+1})= (x_i ,x_{i+1}) \qquad (1)$$

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

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

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

Where m_i and m_{i+1} are the secret data bits which we are going to hide . The function f is calculated by

f(a,b)=LSB(a/2+b) .

‘r’ is a arbitrary value in {-1,+1}and (x'_i , x'_{i+1}) are the pixel pairs which are modified after the data hiding process is done .

After this embedding process of secret data bits the resulting image is divided into the non overlapping blokes of pixels. This image is again rotated with some degrees. Here we are doing the same process that we have done before embedding the secret data into the image.

When we are performing the data retrieving step we have to follow the same step that we have done before data hiding that is we have to again divide the image into non overlapping blocks of pixels. Then again rotate the image by some random degrees according to the secret key. After which the image is again rearranged by row vector. We will get the embedding units with non overlapping regions.

Using the secret key will have to select the pixel pairs whose difference is equal to or greater than that of ‘*t*’. Suppose x_i', and x'_{i+1} are the two consecutive pair of pixels. From which we will retrieve the two message bits say m_i and m_{i+1} as below

m_i=LSB(x_i) and m_{i+1}=LSB($x_i'/2 + x'_{i+1}$)

3.2. *Data Extraction*

The process of extracting the secret bits from the given stego image is opposite to that of the embedding process. In the process of embedding we will select the pair of pixels, hide the message bits to the LSB’s of two pixel pairs. And modifies the pixel value. Where in case of Data extraction will again select the region where the secret data is hidden and then will extract the two secret message bits from the LSB’s of pixel pair.

4. ANALYSIS

Steganographic method selects edge region where it is going to hide the secret data. T is the threshold for selecting the regions for hiding. Accordingly it will adjust the value of threshold T .The value of threshold is adjusted according to size of message we are going to embed .Is suppose the size of data to be hidden is large then the value of threshold should be small so that more and more edge region should made available to hide the data into the cover. That is in our proposed method the embedding capacity of cover get increases. This is the one of the best property of proposed method. When the value of T is so small we can release more regions to embed the data into cover. But whenever threshold value T is so small large amount of regions are available that means we can embed more data into cover but in that case we will be using the sharper edges along with the smoother regions into the cover and then it will reduces overall visual quality of stegos. In another case if embedding rate is low that means we want embed small amount of secret data into the cover then will choose only the sharper edge regions to hide the secret data, then visual quality of our stego will get increases. No one can easily detect that something is hidden into the cover image.

In Table I for the average PSNR, it is observed that the LSBMR method performs finest because it employs the 1 embedding method. Its alteration rate is lesser than the others except for the AE-LSB method. The value of PSNR is not depending on the location of the altered pixels. The average PSNR of our proposed technique will be somewhat inferior to that of LSBMR since some embedding units require to be remodified to assure that the correct data pulling out in the proposed method.

In case of average wPSNR, the performances of the HBC and our proposed methods are same and frequently outperform the others. The cause is that the altered pixels using both techniques all the time locate at the sharper edges within covers while it preserves the smoother regions after data hiding, the weighting for the changes in sharper regions is lesser than those in smoother regions, which means the values of wPSNR should turn out to be superior than those of stegos with the arbitrarily embedding techniques.

When we consider the average modification rate, the AE-LSB scheme is always the lowest. The cause is that according to the hiding method of AE-LSB, the average payload capability for each single pixel is the largest among the schemes, which means that smaller number of pixels, need to be altered at the same embedding capability.

Finally, the object qualities including PSNR and wPSNR of our stegos are most excellent amongst the five Algorithms.

Our method changes the LSB’s of the pixel pairs, but the changes are done at the sharper edges it will keep the smoother regions as it is, hence the visual artifacts are not disturbed and will increases the quality of stegos. In case of LSBM and LSBMR it may disturbs the LSB’s of smoother regions hence the visual artifacts get affected, asymmetry get introduce into the stegos and hence steganography works poorly. The LSB’s which are altered for LSBM, LSBMR are more random that is smoother regions are also get affected. In case of HBC mostly the smooth regions are preserved. For AE-LSB less smooth regions will be disturbed as its rate of modification rate is low as we have mentioned in Table I.

5. CONCLUSION

Image steganography has gotten more popular press in recent years than other kinds of steganography, possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. Adaptive LSB substitution method is used to hide data efficiently and securely in an image. In this project, various types of images are used as cover image and all types of data such as video, audio; etc has been stored and retrieved with good accuracy. Adaptive LSB technique performs more efficiently in both security and accuracy aspects than the traditional LSB technique.

In most previous steganographic schemes selection of pixel pair is decided by the PRNG ,in that case it will never consider the relationship between the size of message which we are going to embed .In that case ,may be smooth regions are also get affected and it will results in easily detection of secret message through the stego. For protecting the visual artifacts in cover images, we have proposed a new method in which we can firstly insert the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message.

References

[1] Weiqi Luo; Fangjun Huang ;Jiwu Huang .(2010): Edge Adaptive Image Steganography Based on LSB MatchingRevisited .IEEETransaction on Information Forensics and Security, vol. 5, No. 2, pp. 201-214.

[2]Kathryn Hempstalk. Hiding Behind Corners:Using Edges in Images for Better Steganography.
Hamilton, New Zealand.

[3]Mielikainen, J. (2006): LSB matching revisited. IEEE Signal Process. , vol. 13, no. 5, pp. 285–287.

[4]Westfeld, A; Pfitzmann, A.(1999):Attacks on steganographic systems. Proc. 3rd Int. Workshop on Information Hiding, vol. 1768, pp.61–76.

[5]Fridrich, J;Goljan, M; Du,R.(2001):Detecting LSB steganography in color, and gray-scale images.IEEE Multimedia, vol. 8, no. 4, pp.22–28.

[6]Dumitrescu,S; Wu,X; Wang, Z.(2003):Detection of LSB steganography via sample pair analysis. IEEE Trans. Signal Process., vol. 51, no. 7, pp. 1995–2007.
.