**MS PROJECT REPORT**

ATTACK LSB MATCHING STEGANOGRAPHY BY COUNTING ALTERATION RATE OF THE NUMBER OF NEIGHBOURHOOD GRAY LEVELS

MOHD ZAID ASLAM -2012060

SHUBHANKAR SINGH-2012102

**Abstract**

*This paper proposes an improved method for attacking the LSB matching steganography* .*In this method , the least two significant bit-planes of the cover image would be changed during the embedding in LSB matching steganography and thus the pairs of values do not exist in stego image. In the proposed method, an image is obtained by combining the least two significant bit-planes and divide it into 3×3 overlapped subimages which are grouped into four types according to the count of gray levels. By embedding a random sequence by LSB matching and then computing the alteration rate of the number of elements in T1 , we find that normally the alteration rate is higher in cover image than in the corresponding stego image which is used as the discrimination rule in this method . According to the results we computed and formulated , the proposed algorithm is efficient to detect the LSB matching steganography on uncompressed gray scale images.*

1 Introduction

Steganography is the art of passing information through apparently files in a m anner that the very existence of the message is unknown. It uses the digital media such as text, image, audio, video and multimedia as a carrier (cover) for hiding private information in such a way that the third party cannot detect or even notice the presence of the communication. By embedding secret data into cover object, a stego object is obtained . Steganalysis is the art of discovering and rendering useless the covert messages, hence breaking steganography. A steganalysis detector attempts to detect the presence or absence of an embedded message when presented with a stego signal. The basic rationale ofsteganalysis is that there should be differences between an original cover medium and its stego versions.

LSB-based steganography is a conventional method and can be divided into two classes, the LSB substitution and LSB matching . In LSB substitution , LSBs of the cover pixels are simply overwritten by the secret bit stream . LSB substitution modifies only the least significant bits and generates pairs of values (PoVs) in the stego image. However , LSB matching which is a counterpart of LSB substitution, makes the detection of hidden message much more difficult. . In LSB matching , randomly selected sample value is increased or decreased if its LSB does not match the secret message bit to be embedded.

The LSB matching embedding algorithm is as follows:

Convert the secret data into a stream of bits. Take each pixel of the cover image (possibly in a pseudo-random order generated by a shared secret key): if the LSB of the next cover pixel matches the next bit of secret data, do nothing; otherwise, choose to add or subtract one from the cover pixel value, at random. When the secret message is fewer bits in length than the number of pixels in the cover image, the pseudo-random permutation ensures that changes are spread uniformly throughout the image. The allowable range of pixel values will force the decision of whether to increment or decrement, when the cover pixel is saturated.

The LSB of the cover pixel value finally equals the next bit of the hidden data and PoVs are not equalized. Though a lot of methods have been presented in dfferent papers , the detection of LSB matching algorithm remains unresolved, especially for the uncompressed grayscale images.

In this paper, a method for attacking the LSB matching steganography in uncompressed gray scale images is presented which is an improvement over the other steganalysis techniques which are previously applied in this domain. For a particular given image, an image is obtained by combining the least two significant bit-planes and divided into 3X3 overlapped subimages. According to the count of comprised gray levels, these obtained subimages are grouped into four types, i.e. *T1*, *T2*, *T3*, *T4* where *T1* includes the sub-images in which all the pixels have the same gray value. After embedding the message through LSB matching , the alteration rate of the number of elements belonging to *T1* is computed. It is found that normally the alteration rate is higher in cover image than the value in the corresponding stego image, which will be used as the discrimination rule in the proposed method.

2 Dataset Used

We have computed results for the mentioned algorithm on a dataset of 100 UCID images. Resolution of the images used in our experiments is 512x384 .

3 Algorithm

The algorithm considers only the uncompressed grey level images. Suppose an *M* X *N* grayscale image *I(x, y)* is composed of eight 1-bit planes *Io ~ I7* , ranging from bit-plane 0 for the least significant bit to bit-plane 7 for the most significant bit. The LSB matching method mainly influences the least two significant bit-planes.

Image *A(x, y)* obtained by combining the least two significant bit-planes is as follows:

*A(x,y) = I0(x,y) + I1(x,y) x 2* *(1<=x<=M, 1<=y<=N)*

According to this , we have only 4 grey levels in the image . In the method 3 x 3 subimage defines the neighborhood of a point *Ai,j(2<=i<=M-1, 2<=j<=N-1)* in *A(x,y)*. The center of the subimage is moved pixel by pixel starting from top left corner. At each position numbers of gray levels in the

3 x 3 subimage are counted. There are four type of subimages :

T1: Including only one gray level. All the pixels in the subimage belonging to this type have the same value.

T2: Including two gray levels. All the subimages in this type have two gray levels.

T3: Including three gray levels. All the subimages in this type have three gray levels.

T4: Including four gray levels. All the subimages in this type have four gray levels.

T5: Including five gray levels.

The probability of a subimage changing from T1 to T2 is much higher than the probability of subimage changing from T2 toT1 . Given an subimage belonging to *T1*, if any one pixel is modified, the probability that the subimage would belong to *Ti(2<=i<=4)* is 100%. However for any subimage belonging to *Ti(2<=i<=4)* initially, if one pixel is modified, the probability that the subimage would belong to *T1* is much less than 100%. Therefore , after embedding the message , *|T1|* decreases, where *|T1|* denotes the number of elements belonging to *T1*.

Suppose *|T1 c|* is the number of elements belonging to *T1* in the cover image *Ic(x,y)* and *|T1s|* is the number of elements belonging to *T1* of the corresponding stego image *Is(x,y)*. Embedding a message sequence again in the cover and stego images by LSB matching gives wo values , us *|T1 c\*|* and *|T1 s\*|*, which is the count of elements belonging to *T1* in the obtained images. The alteration rate is given as:

*kc=(|T1 c|-|T1 c\*|)/|T1 c|* and

*ks=(|T1 s|-|T1 s\*|)/|T1 s|*

It is observed that

*kc > ks.*

Based on the above considerations , the following steps of algorithm can be used for detection :

**(1)** For any given image, calculate *|T1|*.

**(2)** Embed a random sequence with a length *l* into the given image by LSB matching. For example, *l*=0.5 means for every two pixels of the given image, one message bit is embedded.

**(3)** Calculate *|T1\*|* of the newly obtained image.

**(4)** We get the alteration rate *k* by using

*k = (|T1| - |T1\*|)/|T1|*

Comparing the value of *k* with a predetermined threshold, it is possible to determine whether the given image is a stego image.

4 Experimental Results

We demonstrate the performance of our proposed method through experimental results in this section. We have tested our algorithm on 100 UCID images from an uncompressed image database.All the images in UCID are high resolution TIFF files with the size 512×384 or 384×512 and appear to be cut from a variety of uncompressed digital camera images.

Before testing, the images were converted to grayscale using the rgb2gray function of Matlab directly. The random sequence that we use to get the alteration rate *k* is chosen with a length *l*=0.3.

Different payload strengths were used i.e. 25%, 50%, 75%, 100% of the size of the cover image. All these images are discriminated as stego images in our proposed method. A database of 100 images each for different message lengths or payloads is created for the stego images . The results corresponding to different stegoimages (the secret message length *p*=0.25, 0.5, 0.75, 1 respectively) are given.

Since the alteration rate is a dimensionless discriminator, this scheme can be used to detect images with different size. Moreover, for a given detection rate, the threshold is relatively stable for images with different size.

5 Conclusion

In this paper, we have proposed a new method for detection of LSB matching steganography, and tested its performance on a collection of uncompressed grey scale images.

According to the properties of LSB matching a discrimination rule is used to distinguish the cover and stego images, in which the image formed by combining the least two significant bit-planes need to be considered . The main merits of our method are as follows:

(1) According to the properties of LSB matching, we find a novel discrimination rule to distinguish the cover and stego images, in which only the least two significant bit planes need to be considered.

(2) Since the alteration rate is a dimensionless discriminator, we can use our scheme to detect the given images with different size.

6 References

1. Fangjun Huang, Bin Li, Jiwu Huang, “Attack LSB Matching Steganography by counting alteration rate of the numnber of neighbourhood gray levels”, *International Conferenece on Image Processing*, 2007, pp. 401 – 404, 2007

1. Andrew D. Ker, “Steganalysis of LSB Matching in Grayscal Images”,*IEEE Signal Processing Letters*, Vol. 12, No. 6, june 2005