STEGANALYSIS OF REAL TIME IMAGE BY STATISTICAL ATTACKS

SWAGOTA BERA
Dept. of Electronics and Telecommunication Engineering, Chhattisgarh Swami Vivekananda Technical University, DSCET, Durg
Bhilai, Chhattisgarh, India

MONISHA SHARMA
Dept. of Electronics and Telecommunication Engineering, Chhattisgarh Swami Vivekananda Technical University, DSCET, Durg
Bhilai, Chhattishgarh, India

Abstract:
Steganalysis is a technique for the detection of the secret informations embedded in the another image known as cover image and if possible the secret text is tried to recover. In this paper, two techniques are used for the detection of the hidden data. Firstly, detection done by comparing the histogram of the stego & cover image in which the attacker knows about the cover image without the knowledge of the coding algorithm of the stego image & secondly in the image smoothening technique, the probability distribution function is used for the detection. Based on the difference in statistical parameter of the stego image with cover image detection is done.

Keywords: Steganography, Steganalysis, MATLAB, Cover image, Stego image

1. Introduction

Steganalysis is the art of Science which deals with the detection & destruction of the secret image[1]. Many advances are already done in the steganography but still its analysis part is not well developed[2]. Various approaches are discussed by the different researchers. Broadly, there are two approaches to the problem of steganalysis, one is to come up with a steganalysis method specific to a particular steganographic algorithm. The other is developing techniques which are independent of the steganographic algorithm to be analyzed. A steganalysis technique specific to an embedding method would give very good results when tested only on that embedding method, and might fail on all other steganographic algorithms.

As reported by the USA TODAY AP by Jack Kelley that in 1998, a hardcore terrorist Osama bin laden and is associates used the steganography technique to hide the information related to the bombing of two U.S embassies in East Africa. The photographs of the terrorist targets and positioning instructions had been send by hiding in the sports chart room, phonographic bulletin board and other web sites[3]. So, it becomes very essential to work in the area of the detection of the hidden data. The technique involving in the detection of the hidden informations in normal image is known as as Steganalysis. Now working as hacker is becoming more important than working in the field of hiding techniques to provide security in the national and international level. In the present work, more stress have been given to the Steganalysis than Steganography. So, attempt has been made to develop and implement few Steganalysis techniques.

In this detection technique, the statistical distributions of the LSB’s of the incoming image is observed. For Example Histogram of an image is the first order statistical attack. The detection using the information histogram analysis is useful against basic LSB techniques. Statistical tests can reveal that an image has been modified by determining that its statistical properties deviate from a norm. Some tests are independent of the data format and measure only the entropy of the redundant data. Expect images with hidden data to have higher entropy [8].

1.2 Embedding Algorithm based steganalysis Techniques

In this technique, we first look at steganalysis techniques that are designed with a particular steganographic embedding algorithm in mind. For decoding we must known the coding algorithm. Complete recovery of the secret data is possible[6,7].
1.3 Universal Steganalysis Techniques

A more general class of steganalysis techniques pioneered independently can be designed to work with any steganographic embedding algorithm, even an unknown algorithm. Such techniques have subsequently been called Universal Steganalysis techniques or Blind Steganalysis Techniques. Such techniques essentially design a classifier based on a training set of cover-objects and stego-objects arrived at from a variety of different algorithms. Classification is done based on some inherent “features” of typical natural images, which can get violated when an image undergoes some embedding process. Prediction accuracy can be interpreted as the ability of the measure to detect the presence of a hidden message with minimum error on average. The feature should be independent on the type and variety of images supplied to it[7].

2. Literature survey

Survey of IEEE research papers in the present field is done. The research in this field is started from 1995. A brief introduction is given about the papers.

The analysis of the security of Least Significant Bit (LSB) embedding for hiding messages in high-color-depth digital images is done. A powerful steganalytic technique is introduced that enables us to reliably detect the presence of a pseudorandom binary message randomly spread in a color image. The probability of both false detections and missing a secret message is estimated. The method is based on statistical analysis of the image colors in the RGB cube. It is shown that even for secret message capacities of 0.1-0.3 bits per pixel, it is possible to achieve a high degree of detection reliability [8].

A new steganalytic technique based on the difference image histogram aimed at LSB steganography is proposed. Translation coefficients between difference image histograms are defined as a measure of the weak correlation between the least significant bit (LSB) plane and the remained bit planes, and then used to construct a classifier to discriminate the stego-image from the camera image. The algorithm can not only detect the existence of hidden messages embedded using sequential or random LSB replacement in images reliably, but also estimate the amount of hidden messages exactly. Experimental results show that for raw lossless compressed images the new algorithm has a better performance than the RS analysis method and improves the computation speed significantly [9].

The detection of LSB steganography is a question of common interest in the research of steganalysis techniques. In this paper, the distribution of the difference between the current pixel value and its neighborhood average pixel value is statistically modeled, and then the variance of this statistical distribution is defined as a measurement of image smoothness. Based on the analysis of the effects on the image smoothness brought by message embedding and LSB plane flipping, a new steganalytic technique capable of reliable detection of spatial LSB steganography is proposed. The algorithm can exactly estimate the amount of hidden messages and detect the existence of hidden messages embedded in the image simultaneously. Experimental results show that the proposed algorithm is effective [10].

3. Methodology

On the basis of universal detection approaches the statistical attacking algorithm is designed using the MATLAB software and implemented to the stego image database.

3.1 Problem definition

Given a Stego image.

To detect whether the incoming image is containing any secret data or not by knowing the cover image information.

3.1.1 Assumptions

1) Cover image may be Color, Gray level and may be of different extensions.

2) In Steganalysis coding, the dimensions of the analysis algorithm must be less than the dimensions of the Stego image.

3.2 Statistical attack: histogram analysis

Each pixel in an image has a color which has been produced by some combination of the primary colors red, green and blue (RGB). Each of these colors can have a brightness value ranging from 0 to 255 for a digital image with a
A RGB histogram results when the computer scans through each of these RGB brightness values and counts how many are at each level from 0 to 255. The histogram of a digital image shows the distribution of its pixel intensities. Let $X$ is a grayscale (achromatic) image. The single pixel is denoted as $X_s$ where $s$ is the subset of $S$ is a positioning the lattice $S$. Generally, we will assume that $X_s$ takes on the discrete values from 0 to −1 where typically $L=256$\[^{[12-13]}\].

The histogram of the image $X$ is then given by

$$h(i) = \sum_{s=2S}^S X_s (X_s - i) \quad (1)$$

So, $h(i)$ computes the number of the pixels that take on the value $i$.

A typical histogram of an 8-bit image is shown in the Fig.3.1. The height of the histogram at any particular point shows the number of the pixels or area of the image that has that intensity \[^{[14]}\].

### 3.2.1 Algorithm for the statistical attack: histogram analysis

1. Read the stego image.
2. Convert the RGB image into grayscale image.
3. Read the cover image.
4. Convert RGB image into grayscale image.
5. Find the histogram of both the image.
6. Calculate the execution time & memory space requirement.

### 3.3 Statistical attack: image smoothening

In view of the characteristic of LSB steganography, we introduce the concept of the image smoothness to evaluate the effect on the image quality of message embedding. Denote the intensity value of the image $I$ at the position $(i,j)$ as $I(i,j)$, and the local neighbor is defined as a $K\times K$ window centered on the current pixel where $K$ is an odd number. Define the difference variable $XI(i,j)$ as the difference between the current pixel value and the average value over its local neighbor.

$$X_I(i,j) = I(i,j) - \frac{1}{(K^2 - 1)} \sum I(l+m,j+n) \quad (2)$$

Where $m,n=-(K-1)/2$ to $(K-1)/2$ & $(m,n)$ not equal to 0,0

Consider the probability distribution of the difference variable $XI$, the probability density function of $XI$ is denoted as $f(x)$. The variance of the difference variable $XI$ reflects the degree to which the pixel value deviates from its neighborhood average pixel value, and can be used as a measurement of the image smoothness. So the image smoothness of a natural image $I$ can be defined as

$$SMI = \sigma^2 = \int f(x) \cdot x^2 \, dx \quad (3)$$

$SMI$: - Image smoothness of a natural image $I$.

The Fig.3.2 (a) shows the input image and the Fig.3.2 (b) shows the statistical (normal) distribution of the difference variable $XI$ for the image.
The larger the value of the image smoothness $SM_I$ is, the more intensively the pixel value deviates from its neighborhood average pixel value, and the weaker the smoothness of the image is. For the LSB Embedding reduces the smoothness of the image, we expect that the stego-image with secret message embedded have a larger image smoothness value as stated by the $SM_I$ value [15].

3.3.1 Algorithm for the statistical attack: image smoothening

Step 1. Read the stego image $I$ and convert it into gray scale image.
Step 2. Convert the pixel value into binary form.
Step 3. Select the pixel $I(i,j)$ row wise.
Step 4. Find out the 8-neighbours of the pixel $I(i,j)$.
Step 5. Find the mean of all the neighbors.
Step 6. Find the difference $XI(I,j)$ of the mean & $P$ using “Eq.(2)”.
Step 7. Find the variance and normal distribution plot $f(x)$ using “Eq.(3).
Step 8. Apply the same step for the cover image also.
Step 9. Calculate the execution time & memory space requirement.

4. Result & analysis

4.1 Steganalysis by statistical attack: histogram analysis

Four stego images are used for the implementation of the first order statistical attack i.e the histogram analysis. The resultant graphs and figures are represented in the Fig.4.1. In this method of analysis for the detection of the secret image it is considered that the analytic is having the information about the cover image along with the incoming stego image.
Fig. 4.1 Steganalysis of Stego Images using Histogram Analysis: (a), (d), (g) & (j) Stego Images, (b), (e), (h) & (k) Histogram of Cover Images, (c), (f), (i) & (l) Histogram of Stego Images.
4.2 Steganalysis by statistical attack: image smoothening

Four stego images are used for the implementation of the first order statistical attack i.e. the histogram analysis. The resultant graphs and figures are represented in the Fig.4.2. In this method of analysis for the detection of the secret image, it is considered that the analytic is having the information about the cover image along with the incoming stego image.

(a)

(b)

(c)

(d)
The figure in Fig.4.1 the **histogram analysis:** known cover image steganalysis of the cover & its stego images are shown for the above eight images. There seem the differences in the value of the pixel intensity in the range 0 to 255 for the cover image and its stego image. Though the two images are visibly similar but the variations in the pixel value is there. This indicates that there is the possibility of the hidden data embedded in the image. If the distortion occurs after the detection program is implemented then it is detected that the images may containing the hidden data otherwise not.

The figure in Fig.4.2 the **image smoothness:** known cover image steganalysis of the cover & its stego images are shown for the above eight images. The normal distribution graph of the cover images and its stego images are having different value. Though the two images are visibly similar but the variations in the pixel value as indicated by the distribution graph. This indicates that there is the possibility of the hidden data embedded in the image. If the variations in the graph occurs after the detection program is implemented then it is detected that the images may containing the hidden data otherwise not.

5. **Conclusion**

Although attacks specific to an embedding method are helpful in coming up with better embedding methods, their practical usage seems to be limited. Since given an image we may not know the embedding technique being used, or even we might be unfamiliar with the embedding technique. Thus universal steganalysis techniques seem to be the real solution since they should be able to detect stego images even when a new embedding technique is being employed. So, statistical technique is discussed in the paper which based on the detection of the hidden data knowing the statistical parameter of the cover image. The variations in the statistical parameter are the basis of the detection of the secret data.

**References**


