SECURE IMAGE STEGANOGRAPHY WITH MINIMUM DISTORTION

Sheeba Herlin [1], and Dr. Kumaravel [2]

[1and2] *IT Department, Bharath University*

[1]sheebaherlin@gmail.com

[2]drkumaravel@gmail.com

Abstract— Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. The secret message is hidden in such a way that no significant degradation can be detected in the quality of the original image. In this paper a new technique for embedding messages inside images is proposed. The pixels for message embedding are chosen such that the distortion introduced after embedding will be minimum. A distortion function is designed to calculate the cost of embedding for each pixel. The function evaluates the cost of changing an image element (e.g., pixel) from directional residuals obtained using a wavelet filter bank. The intuition is to limit the embedding changes only to those parts of the cover that are difficult to model in multiple directions while avoiding smooth regions and clean edges. A technique that introduces less distortion to the carrier image will generally cause changes that are more difficult to detect, and will therefore provide more security.

I. INTRODUCTION

In recent years, steganography has emerged as an increasingly active research area, with information being imperceptibly hidden in images, video, and audio among others. With the wide availability of digital images, and the high degree of redundancy present in them despite compression, there has been an increased interest in using digital images as cover-objects for the purpose of steganography. We use three main terminologies in steganography: the cover image, secret message and the embedding algorithm. The cover image corresponds to the medium in which the message is hidden. Embedding algorithm is the method by which message is hidden within the cover medium. And the cover image with the message hidden inside is known as the stego image.

There are two main challenges in information hiding systems: high payload capacity and high robustness to modification. In steganography robustness means the embedded data should be as immune as possible to modifications from attacks and capacity refers to the amount of information that can be hidden within a given image. There is always a tradeoff between capacity and robustness. When the size of secret message increases there is always a chance for an attack to happen. So the challenge for the designer is to develop an algorithm which would embed messages of large size with minimum possible embedding artifacts introduced [1].

A steganography system is said to be a failure if an attacker detects the possibility of message hidden within it. The basic requirement of any stego system is to conceal the presence of hidden message in it. If the attacker is not able to distinguish between a cover image and a stego image, then that stego system is said to be secure. There are different measures for steganographic security. The most common measure is called detectability of a stego system. Detectability is defined as the relative entropy between the probability distribution of cover image and the stego image. Any steganography system is called 3-secure if the relative entropy of the system is at most. A steganography scheme is said to be perfectly secure if detectability is zero. Reduction in detectability means reduced embedding capacity. Any image steganography scheme should optimize the embedding capacity to achieve minimum possible detectability taking into account the computational overhead [2].

In this paper an algorithm is proposed which will embed with minimum embedding artifacts while maximizing the payload. A set of wavelet filter banks are constructed to measure the cost of embedding for each pixel. wavelet filter banks are constructed using daubechies 8 tap filters. We conducted experiments with different filters and db filters gave the better result. We use filters with the assumption that edges and noisy regions have higher wavelet coefficients and when we embed in those regions, the chance of detectability will be minimum. Filters are used to get the regions with high wavelet coefficients. And the algorithm which we use here will embed in those regions with high value for wavelet coefficients, such that detectability will be minimum.

1.1 Preliminaries

Currently, many practical steganographic algorithms use LSB hiding techniques to hide the message.LSB hiding techniques hide the secret message into the least significant positions of the image pixels,that affect the image resolution, which will reduce the image quality and make the image easy to attack.

1.2 LSB Embedding

The most common method used in steganography is LSB embedding. In this method message is hidden by taking the image pixel and replacing the least significant bit of this pixel by the message bit.LSB replacement is the simplest type of embedding .If the LSB bit of the pixel and the message bit to be hidden are same, and then leave the pixel as it is. Where as if the LSB bit and the message bit are different, then replace the LSB bit of the pixel with the message bit.

1.3 Attacks on the existing systems

There are three types of attacks on stego systems:
a) Visual attacks
b) Structural attacks
c) Statistical attacks

In visual attacks, we will take the bit images and make an analysis on them to find out the difference visually.

For structural attacks, consider palette based steganography for palette images. Here before embedding data, we reduce the number of colors so that the number of pixel color difference is very less. This is done by changing the palette of the image. When this type of change in characteristic structure can be identified in the stego image, then structural attacks occur

In statistical attacks, we use statistical analysis by some mathematical formula to detect the presence of hidden data. Generally the hidden message is more random than the original data of the image thus finding the formula to know the randomness reveals the existence of data [3].s.

II. PROPOSED SYSTEM

In this paper a new embedding technique is proposed which will embed in those pixels , which when altered gives minimum distortion.In this technique an algorithm to calculate the cost of embedding for each pixel is developed and the embedding is done in such a way that the cost is minimum.

Wavelets and Wavelet Filter banks: In this method, wavelet filter banks are constructed to measure embedding distortion. Fourier Transform (FT) cannot be used for analysis of non-stationary signals, because FT tells us which frequency components exist in the signal, but gives no time information about these frequency components. To solve this problem, STFT was developed. STFT used a window function to “view” a part of non stationary signal as stationary and then perform analysis. However, STFT can have either good time resolution or good frequency resolution, but not both. This problem is related to Heisenberg’s uncertainty principle which states that we cannot have arbitrarily high resolution in both time and frequency domain [5].

To overcome this resolution problem, wavelet transform was developed. Wavelet analysis is performed using contracted and expanded versions of a single prototype function called a wavelet. We can achieve fine time resolution using contracted version of the wavelet, while fine frequency resolution can be achieved using expanded version. In discrete wavelet transform, the scale and resolution are varied, for detailed analysis of the signal. We can obtain signals of different resolution and scale, by passing them through various filters, followed by up sampling and down sampling processing. Signals of different resolution and scale can be achieved by passing them through filter banks [4]. Thus we can use digital filter banks to implement wavelet transform.

In this method, we are using a set of wavelet filter banks to measure embedding distortion. Before constructing wavelet filter banks, we should know about low pass and high pass filters. A high pass filter is an electronic filter that passes high frequency signals and attenuates low frequency components. It is also called a low-cut-filter or bass-cut-filter. Whereas a low pass filter passes low frequency components and attenuates high frequency components. Here a directional filter bank is used to detect edges in local neighborhoods of each pixel. Then the changes in residuals caused by embedding are weighted and aggregated using a specially designed rule such that we get a low embedding cost only when the content is not smooth in any direction.

Before embedding we have to calculate the cost of embedding for each pixel.For this, we construct a set of filter banks using daubechies8 tap filters.It is constructed with low pass and high pass filters. FB(1),FB(2) and FB(3) are the set of filter banks we construct.

FB(1) =h .g’
FB(2) =g. h’
FB(3) =g. g’

That is these filter banks consists of low high, high low and high high decomposition filters respectively.

The support of each one dimensional filter is 16,which gives each filter bank , a size of 16x16.We define the k th directional residual as :R(k)=FB(k)*C where * is the mirror padded convolution and C is the cover image. Mirror padding is used to prevent embedding artifacts at the boundary.

For each pixel cost of changing is calculated by using a set of filter banks. When we apply high pass filter to an image, the high frequency coefficients are filtered out. That is we get the pixels corresponding to edges and noisy regions. When we embed in this regions, chance for detection is less.

Now given a cover image C and stego image S, we define the distortion between both the images as the sum of relative changes of the wavelet coefficients w.r.t the cover image and is given as:

$$D(C,S)=\sum_{k=1}^{3}\sum_{uv}\frac{W_{u,v}^{k}(C)-W_{u,v}^{k}(S)}{e+W_{u,v}^{k}(C)}$$

Where W(C) and W(S) corresponds to the wavelet coefficients in the kth decomposition obtained using the filters, for the cover image and the stego image respectively. From the equation, it is clear that the ratio is smaller when a large cover wavelet coefficient is changed, which corresponds to the edges and noisy regions. That is when pixels in these regions are changed; the chance of detection is less. We develop our embedding algorithm in such a way that the pixels with the small value for the distortion function are taken first for embedding. It is clear that the embedding algorithm discourages making changes in areas where the content is smooth in at least one direction.

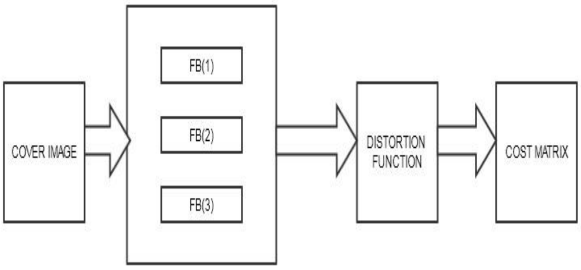


Fig 1.Computing cost matrix

Embedding algorithm

The procedure of data hiding in the embedding algorithm works as follows:

Input: Image file and text file.
Output: Text embedded image

Procedure:

Step 1: Take the input image and calculate the cost of embedding for each pixel.
Step 2: Find the length of input message.
Step 3: Sort the cost array in increasing order
Step 4: Take each pixel from the sorted array
Step 5: Change the lsb of the pixel until the length of message is over.
Step 6: Stop

Here we start with the input image, and the output will be the stego image with message hidden within it. Input images are taken from BOSS database[6]. Cover image is taken and the cost of embedding for each pixel is calculated using filter banks. After calculating the cost matrix, the values inside it are sorted, preserving the actual positions. Next, find the length of the message to be hidden. Then take each pixel value from the sorted array and replace the LSB of the pixel by looking at the message bit. If the LSB of the cover image and the message bit to be hidden matches, then take the next pixel. Otherwise, change the least significant bit of the cover image.

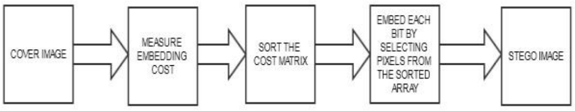


Fig 2: Block diagram for embedding algorithm

Extraction Algorithm

The procedure for extracting messages inside images is as follows:

Input: Stego-Image, Message length
Output: Message

Algorithm:
Step 1: Calculate the cost matrix for the image
Step 2: Sort the cost array
Step 3: Find the LSB of each image pixel from the cost array until the length of the message
Step 4: Concatenate the LSB’s
Step 5: Return the message after concatenating.

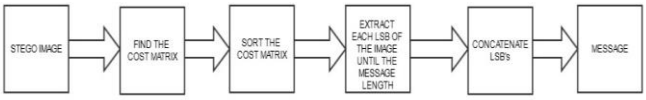


Fig 3: Block diagram for message extraction

III. EXPERIMENTS AND RESULTS

In this section, some experiments are carried out to prove the efficiency of the proposed system. The proposed technique has been simulated using the MATLAB-07 program platform. A set of 8-bit grayscale images of size 512 × 512 are used as the cover-image to form the stego-imageTo ensure that the reproduction of your illustrations is of a reasonable quality, we advise against the use of shading. The contrast should be as pronounced as possible.

Experiments were conducted with images from BOSS database [6]. The strength of the stego system is checked with statistical steganalysis tools. Chi square test and RS steganalysis were conducted on the results and the strength of the stego system is verified [7].

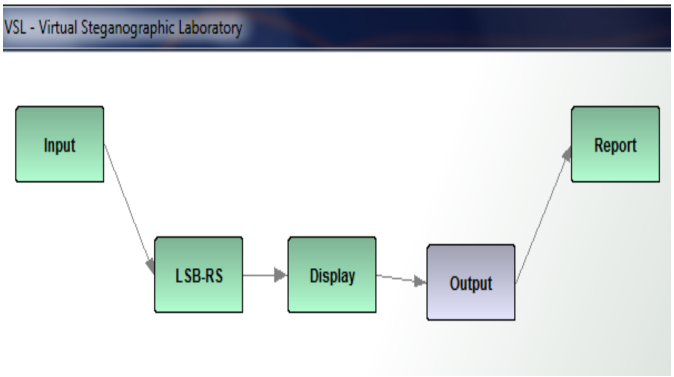
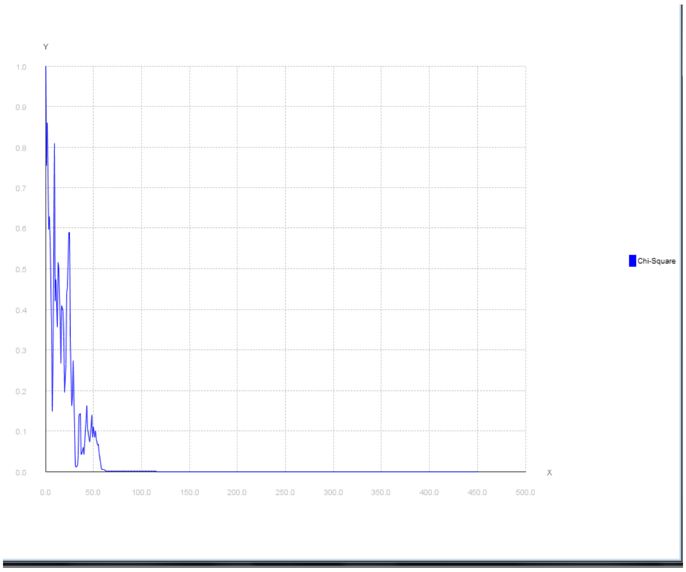


Fig: Experimental set up of RS Steganalysis

RS steganalysis was conducted on images using virtual steganographic laboratory and the outputs proved the resistance of the stego system against RS steganalysis[8].

Chi square test was also conducted on the output images. The results of chi square test was compared with the results which used various other methods for embedding.



.

Fig: Result of chi-square test on a stego image which used normal lsb embedding

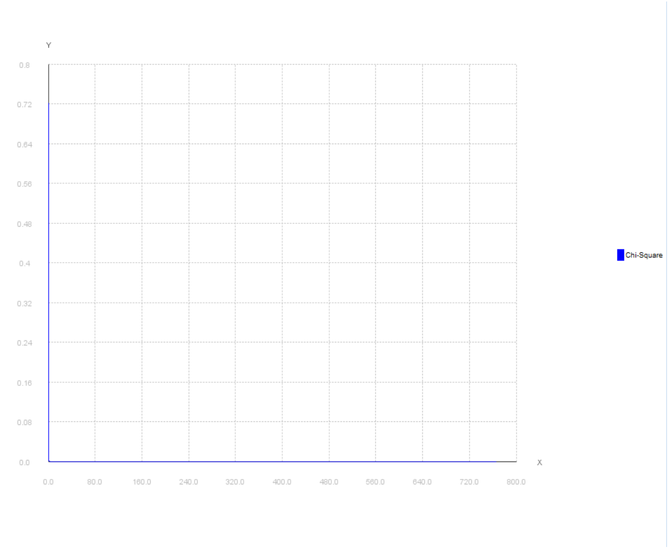


Fig: Result of chi-square test on a stego image which used new method for embedding

IV. CONCLUSION AND FUTURE WORK

This paper proves that embedding distortion can be minimized by restricting embedding changes to textures while avoiding smooth areas .Wavelet filter banks measures the embedding distortion in an effective way. The smoothness of the image is evaluated in multiple directions using the filter banks. Hence cost matrix which we get from the distortion function is more accurate. The Strength of the steganographic system is verified by different steganalysis tools. Due to the novel design of distortion function, we obtain good results. Future works include using better directional filter banks to get a more effective design of the distortion.

REFERENCES

[1] R Bobme, Advanced Statistical Steganalysis. Springer-Verlag, Berlin (2010)

[2] T Filler and J Fridrich : Design of adaptive steganographic schemes for digital images. Information Hiding ,9 th International Workshop volume 4567, Lecture Notes In Computer Science(2007)

[3] Andreas Westfeld and Andreas Pfitzmann: Attacks on steganographic systems. Dresden University Of Technology (1999)

[4] M. Siffuzzman , M.R.Islam and M.S.Ali: Wavelet Transform And Its Advantages Compared To Fourier Transform. Recent Trends and Developments. Journal Of Physical Sciences, Vol. 13. Bangladesh (2009)

[5] Martin Vetterli.: Wavelets And Filter Banks: Theory And Design. IEEE Transactions On Signal Processing. Vol. 40. (1992)

[6] T Filler T Penvy and T.Bass: Break Our Steganography Systems. http://www.agents.cz/boss (July 2010)

[7] Jessica Fridrich, Miroslav Goljan.: Practical Steganalysis Of Digital Images.http://ws2.binghamton.edu/fridrich/Research/steganalysis01.pdf

[8] Jessica Fridrich, Miroslav GoljanPenvy and Rui Du: Reliable Detection Of LSB Steganography In Color and Gray Scale Images. IEEE Multimedia. Vol.8(2001)