A Novel Method for Secure Image Steganography

S. Anjana and P.P. Amritha

Abstract Steganography is the science that involves communicating secret data in an appropriate multimedia carrier. 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 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, 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, therefore providing more security.

Keywords Steganography · Steganalysis · Wavelets · Filter banks

1 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

S. Anjana (✉) · P.P. Amritha
TIFAC CORE in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, India
e-mail: anjanaossery9@gmail.com

P.P. Amritha
e-mail: ammuviju@gmail.com

L.P. Suresh et al. (eds.), *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, Advances in Intelligent Systems and Computing 324,
DOI 10.1007/978-81-322-2126-5_17

message is hidden. Embedding algorithm is the method by which message is hidden within the cover medium. 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 a 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]. Detectability of a steganographic system 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 [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 [2] 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, then leave the pixel as it is, whereas 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: Visual attacks, statistical attacks, and structural attacks. The following sections give a brief idea of these attacks.

1.3.1 Visual Attacks

The majority of steganographic algorithms embed messages replacing carefully selected bits by message bits. The idea of visual attacks is to remove all parts of the image covering the message. The human eye can now distinguish whether there is a potential message or still image content [2].

1.3.2 Statistical Attacks

The idea of the statistical attack is to compare the theoretically expected frequency distribution in steganograms with some sample distribution observed in the possibly changed carrier medium. The degree of similarity of the observed sample distribution and the theoretically expected frequency distribution is a measure of the probability that some embedding has taken place. The degree of similarity is determined using the chi-square test.

1.3.3 Structural Attacks

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 [3]. 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.

2 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, 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 [4].

Before embedding, we have to calculate the cost of embedding for each pixel. For this, we construct a set of filter banks using daubechies 8-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.

$$\begin{aligned} \mathrm{FB}(1) &= h \cdot g^t. \\ \mathrm{FB}(2) &= g \cdot h^t. \\ \mathrm{FB}(3) &= g \cdot g^t \end{aligned} \tag{1}$$

The filter banks consists of low–high, high–low, and high–high decomposition filters, respectively, in Eq. (1). The support of each one-dimensional filter is 16, which gives each filter bank, a size of 16 × 16. We define the kth directional residual as follows:

$$R(k) = \mathrm{FB}(k) * C. \tag{2}$$

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 these 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 distortion is given as follows:

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

where $W(C)$ and $W(S)$ correspond to the wavelet coefficients in the kth decomposition obtained using the Eq. (2), for the cover image and the stego-image, respectively. From the Eq. (3), it is clear that the ratio is smaller when a large cover wavelet coefficient is changed, which corresponds to the edges and noisy regions [5]. 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 [6] (Fig. 1).

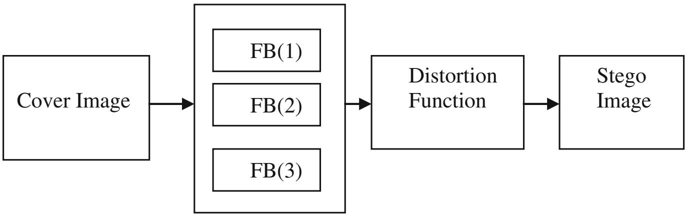

Fig. 1 Computing cost matrix

Embedding algorithm

The procedure of data hiding in the embedding algorithm works is 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.
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.

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 [7]. 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 match, then take the next pixel. Otherwise, change the least significant bit of the cover image.

Extraction Algorithm

The procedure for extracting messages inside images is as follows:

Input: Stego-image, Message length.
Output: Message.

Procedure:

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.

3 Experiments and Results

The proposed technique has been simulated using the MATLAB-07 platform. A set of 8-bit grayscale images of size 512 × 512 are used as the cover image to form the stego-image.

Experiments were conducted with images from BOSS database [8]. 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 [9].

RS steganalysis was conducted on images using virtual steganographic laboratory and the outputs proved the resistance of the stego system against RS steganalysis [10] (Fig. 2).

Chi-square test was also conducted on the output images. The results of chi-square test were compared with the results which used various other methods for embedding. The test was conducted on maximal length embedded images (i.e., all the pixels were embedded with message bits). A plot of probability of embedding with percentage of pixels embedded was obtained from chi-square test. Even though maximal length embedding was done, only a small percentage of pixels were detected to contain embedded bits. Also the values of chi-square statistics were large, which correspond to cover images [1]. False positiveness was comparatively small.

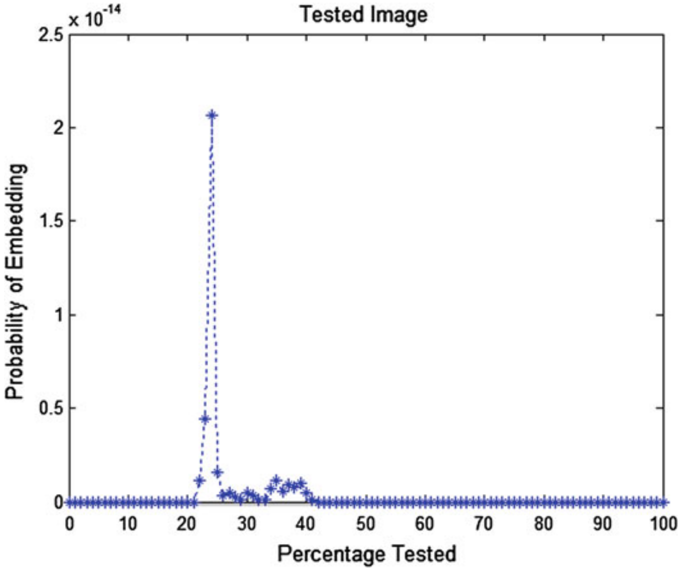

Fig. 2 Result of chi-square test on a stego-image obtained using the proposed method

Table 1 Performance evaluation of algorithm

Embedding rate (%)	Distortion	Coding loss	PSNR
50	12,402.7	9.98	50.97
60	13,356.9	9.91	55.67
70	17,257.9	10.58	45.98
75	12,829.37	9.67	59.34

3.1 Performance Evaluation

The above table gives the amount of distortion, PSNR, and the coding loss obtained on three different test images. Total distortion is a sum over the embedding costs where the pixel is changed. Coding loss is found as the ratio of actual payload with theoretically best possible payload (Table 1).

4 Conclusions 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 measure 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 obtained 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, Berlin, 2010)
2. A. Westfield, A. Pfitzmann, *Attacks on Steganographic Systems* (Dresden University Of Technology, 1999)
3. T. Filler, J. Fridrich, Design of adaptive steganographic schemes for digital images. In Information Hiding, 9th International Workshop (2007)
4. M. Siffuzzman, M.R. Islam, M.S. Ali, Wavelet transform and its advantages compared to fourier transform. Recent trends and developments. J. Phys. Sci. 13 (2009)
5. J. Fridrich, V. Holub, Digital image steganography using universal distortion (2013)
6. J. Fridrich, V. Holub, Designing steganographic distortion using directional filters. Air force Office of Scientific Research (2013)
7. M. Vetterli, Wavelets and filter banks: theory and design. IEEE Trans. Sig. Proces. 40 (1992)

8. T. Filler, T. Penvy, T. Bass, Break our steganography systems: the ins and outs of organizing BOSS. In Information Hiding, pp. 59–70 (2010)
9. J. Fridrich, M. Goljan, Practical steganalysis of digital images-state of the art. In *Proceedings of SPIE*, vol. 4675, pp. 1–13 (2002)
10. J. Fridrich, M. Goljan, R. Du, Reliable detection of LSB steganography in color and gray scale images. IEEE Multimedia 8 (2001)