International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 4, Number 2 (2011), pp. 243-250

http://www.irphouse.com

Disclosure of Hidden Messages using Classifier based on Statistical Moments of Wavelet Characteristic Function

[1]T.S.R. Krishna Prasad, [2]Y.V.N. Tulasi and [3]V. Ramya

[1]Associate Professor, E.C.E. Dept.
Gudlavalleru Engineering College, Gudlavalleru, India
[2]Assistant Professor, C.S.E. Dept.
Gudlavalleru Engineering College, Gudlavalleru, India
[3]M.Tech. Student, Gudlavalleru Engineering College, Gudlavalleru, India
E-mail: vusalaramya@gmail.com

Abstract

In this paper, a method based on multiple features formed by statistical moments of wavelet subband coefficients is proposed. Detection of stego-image created by the steganography based on bit plane complex segmentation (BPCS) has showed a low detection rate. So the evaluation of this method is realized in terms classification error rates using 100 natural images and 100 stego images which are generated by using BPCS steganography. This work proposes to use a support vector machine (SVM) as classifier for BPCS steganography. We have chosen the horizontal and diagonal details of wavelet subband coefficients, since it contains the high frequency components. This is because the data might be hidden in the noisy regions (since stego image should not have any visual artifact) which have high frequency components.

Keywords: Steganography; classification error; support vector machine; wavelet characteristic function.

Introduction

Steganography is a science or art of secret communication and recently digital steganography has become a hot research issue, due to the wide use of Internet as popular communication media. The goal of digital steganography is to conceal covert message in digital material in totally innocent manner. Even though digital images, audio files, video data and all types of digital files can be considered as a cover

material to conceal secret information, in this paper, we consider only digital images as cover material. After hiding a secret message into the cover image, we get an image with secret message: so-called stegoimage, which is transmitted to a receptor via popular communication channels or put on some Internet web-site. To design useful steganography algorithm, it is very important that the stegoimage does not have any visual artifact and it is statistically similar to natural images. If a third party or observer has some suspicion over the stegoimage, steganography algorithm becomes useless.

During the last decade, many steganographic algorithms for digital images have been proposed [1-3]. The image steganography algorithmcan be classified in two classes by its embedding domain: spatial domain embedding method and frequency domain embedding method. LSB embedding technique is one of the popular spatial domain embedding techniques, which message or its encrypted version [4, 5]. The hiding capacity of this technique is directly related with the image size. Principal advantages of the LSB embedding technique are simple implementation, imperceptibility of hidden message to human visual system and high embedding rate of secret data. Some public domain tools, such as S-tools, Invisible Secret and J-Steg, use this technique. However the LSB embedding technique is generally vulnerable to statistical analysis. Frequency domain embedding methods have some advantages and disadvantages respect to spatial domain's one. Principal advantage is robustness against simple statistical analysis and the principal disadvantage is the limitation of the amount of embedded data.

Detecting the presence of hidden data in the cover media files is emerging in parallel with steganography. It has gained prominence in national security and forensic sciences since detection of hidden (ciphertext or plaintext) messages can lead to the prevention of disastrous security incidents. It is a very challenging field because of the scarcity of knowledge about the specific characteristics of the cover media (an image, an audio or video file) that can be exploited to hide information and detect the same. The approaches adopted for this also sometimes depend on the underlying steganography algorithm(s) used. Hiding a message will most likely leave detectable traces in the cover medium. The information hiding process changes the statistical properties of the cover.

Steganography Methods

In this section, we describe some of the existing methods of steganography which are used to generate stego images.

LSB Embedding Method

LSB embedding method is one of the most popular steganography methods due to its simplicity, high embedding capacity and high imperceptibility of secret message. In the LSB embedding method, image is decomposed in bits planes (8 bit planes for 8 bits gray scale images and 24 bits planes for color images), and its least significant bits (LSB) plane is replaced by secret message. Generally secret message is encrypted by any encryption algorithm before its embedding.

DCT Domain Embedding Method

In the DCT Domain embedding method, firstly the cover image is transformed by DCT and then the embedding process is performed in the DCT coefficients instead of in the image pixels. The principal advantage of this method is that it is more secure than the LSB embedding method against many statistic analyses; however the embedding capacity of the secret message is limited by imperceptibility constrains.

Bit Plane Complexity Segmentation (BPCS) Embedding Method

The method of steganography outlined in this paper makes use of the more complex regions of an image to embed data. There is no standard definition of image complexity. In the present paper we adopted a black-and- white border image complexity.

If the border is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4.

The definition of image complexity is given by eq.(1) as

$$\alpha = k/ \text{ (The max possible B-W changes in the image)} \quad (1)$$

Where, k is the total length of black-and-white border in the image. So, the value ranges over $0 \le \alpha \le 1$.

The process of segmenting an image into informative and noise-like regions is performed using the complexity measure. For gray scale cover image, a number of binary images can be produced by bit-plane decomposition, and the complexity segmentation performed on each bit-plane. If the complexity threshold is denoted by α_{TH}, noise-like regions are defined as regions having a complexity value α_{TH} or greater, and informative regions are defined as regions having a complexity value that is less than α_{TH}. In typical BPCS steganography, the noise-like regions are replaced by the secret data and leave the informative regions alone. This method embeds secret message not only into LSB plane but also into upper bit planes.

Since BPCS Steganography embedding technique is difficult to detect, we have chosen this for hiding the secret message. Thus we made our analysis on the stego images that are generated by using BPCS embedding technique which is proposed in [6].

Designing a Classification System based on Pattern Recognition

There are various stages involved in the design of a classification system for a 2-class image classification task. The following five stages will be explicitly considered:

- Data collection for training and testing
- Feature generation
- Feature selection
- Classifier design
- Performance evaluation

Data collection

A number of different images must be chosen for both the training and the test set. We have used the uncompressed image dataset which has been proposed in [7]. There are more than 1000 images in the dataset. We generated stego images by using BPCS steganography embedding algorithm for 100 images. Out of 200 images, 70% images are used for training purpose and remaining 30% are used for testing purpose. Fig.1. shows one of the natural image and its corresponding stego image.

Figure 1: Natural image(left) and its corresponding stego image(right).

Feature generation

De-correlation of wavelet transform

The histograms of all wavelet subbands only reflect the statistical distribution of coefficients in the subband, but it doesn't reflect the correlation of the coefficients within this subband. The wavelet transform is well known for its capability of multi-resolution decomposition and coefficients de-correlation. It is known that for discrete wavelet transform, different high frequency subbands within one level will be uncorrelated to each other. The features extracted from one high frequency subband are thus uncorrelated to that extracted from another high frequency subband at the same level. Therefore, features from different dimensions most likely uncorrelated to each other. From this point of view, this multi-dimensional feature vector will be suitable to represent the image for steganalysis purpose.

Statistical Moments of wavelet subband coefficients

In order to get the feature, the subbands decomposed by Haar wavelets until two levels were used. Therefore, there are 8 subbands, denoted by LL1, HL1, LH1, HH1, LL2, HL2, LH2, HH2. The first three moments for each of subbands and the test image, denoted by LL0, result a vector with 27 features.

The formula for calculating statistical moments for each subband coefficient is given below

$$\mu_n = \sum_{i=0}^{L-1} (z_i - m)^n \, p(z_i) \tag{2}$$

Where z_i is a discrete random variable that denotes intensity levels in an image, $p(z_i)$,i=0,1,2,…L-1 be the corresponding normalized histogram, L is the number of possible intensity values, n is the moment order, and m is the mean:

$$m = \sum_{i=0}^{L-1} z_i \; p(z_i) \tag{3}$$

Feature selection

Of the 27 generated features, some may turn out not to be very informative or some may exhibit high mutual correlation. In the latter case, there is no point in using all of them because they do not carry complementary information. Moreover, one has to keep in mind that the number of features, *l* (i.e., the dimension of the feature space in which the design of the classifier will take place), must be relatively small with respect to the number of training/test points to ensure good generalization performance of the designed classifier. A rule of thumb is to keep *l* less than one-third of the training points. In our case, we chose *l* = 12 i.e., we have chosen the horizontal and diagonal details since it contains the high frequency components. This is because the data might be hidden in the noisy regions (since stego image should not have any visual artifact) which have high frequency components.

Classifier design

SVM (Support Vector Machine) is a powerful tool for pattern classification. With introduction of kernel tricks in SVM, it has become a very popular in machine learning community. In some cases, the given data is not directly classifiable. Such cases can be solved by transforming the given data to higher dimensional space in such a way that in transformed domain, the classification is much easier. Kernel tricks help this without actually transforming features to higher dimensional space which is in [8].

Given a set of training points, x_i, with respective class labels, $y_i \in \{-1,1\}$, $i = 1, 2, \ldots, N$, for a 2-class classification task, compute a hyperplane so as to get eq.(4)

$$\text{Minimize } J(w, w_0, \xi) = \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{N} \xi_i \tag{4}$$

$$\text{Subject to } w^T x_i + w_0 \geq 1 - \xi_i \text{, if } x_i \in w1 \tag{5}$$

$$w^T x_i + w_0 \leq 1 + \xi_i \text{, if } x_i \in w2 \tag{6}$$

$$\xi_i \geq 0 \tag{7}$$

The margin width is equal to $2/\|w\|$. The margin errors, ξi, are nonnegative; they are zero for points outside the margin and on the correct side of the classifier and

positive for points inside or outside the margin and on the wrong side of the classifier (This can be verified by a close inspection of the constraints in Eqs. (5) and (6). *C* is a user-defined constant. The necessary condition is given in eq.(7). Minimizing the cost is a trade-off between a large margin and a small number of margin errors. It turns out that the solution is given as a weighted average of the training points given in eq.(8)

$$w = \sum_{i=1}^{N} \lambda_i y_i x_i \tag{8}$$

The coefficients λi are the Lagrange multipliers of the optimization task and they are zero for all points outside the margin and on the correct side of the classifier. These points therefore do not contribute to the formation of the direction of the classifier. The rest of the points, with nonzero λi's, which contribute to the buildup of *w*, are called *support vectors*.

For training of SVM, we used 70% of the images database and for testing purpose we have used the remaining 30% of the images.

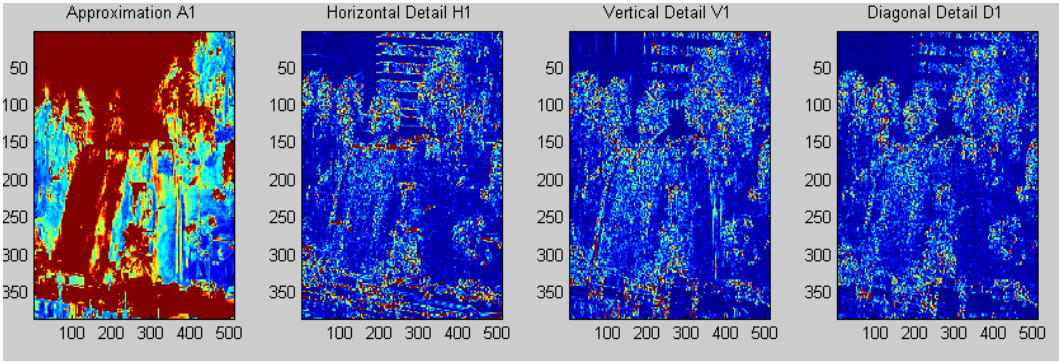
Performance evaluation

The performance of the classifier, in terms of its error rate, is measured against the test data set. Finally, average out the number of errors committed by the *N* different test points is evaluated.

Results

To evaluate this method, first we performed the two level haar wavelet decomposition of the natural image and its corresponding stego image. Fig.2 shows the eight subbands of the natural image and fig.3 shows the eight subbands of the stego image which is shown in fig.1.

Then we calculated first three statistical moments of the subbands. Similarly we have done for all the 200(100 natural and 100 stego images) considered. Then we have selected some of the important features based on our observation which is proposed earlier. These selected features of 70% of the images are used for training of the SVM classifier and remaining 30% of the images are used for testing it. We got classification error of 0.15 while testing.



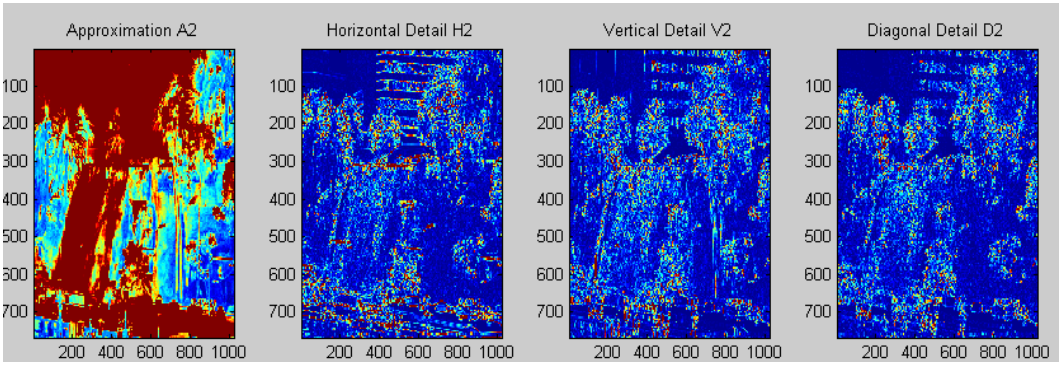


Figure 2: Subbands of natural image.

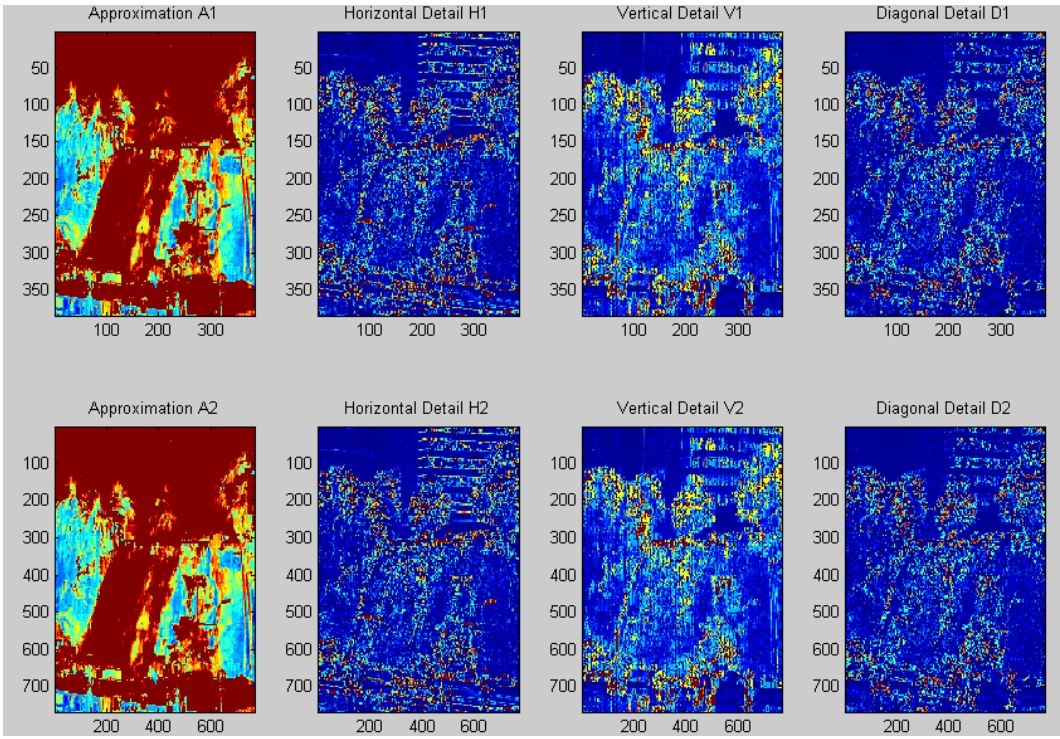


Figure 3: Subbands of stego image.

Conclusion

In this paper, a performance of this method has been observed for 100 natural images and their corresponding 100 stegoimages generated by BPCS steganography methods. This method is based on statistical moments of wavelet subband coefficients as features for analysis, that result in a feature vector with 12 characteristics, it includes the first three moments of the selected subband coefficients with the 2-level Haar wavelet decomposition. To perform a reliable analysis about a suspicious image,

several methods must be combined. Also more reliable steganalysis method for frequency domain embedding steganography must be developed and analyzed.

References

[1] Q. Cheng and T. Huang, “An Additive Approach to Transform domain Information Hiding and Optimum Detection Structure”, IEEE Trans. on Image Processing, vol. 12, no. 2, pp. 221-229, 2003.

[2] L. Marvel, C. Boncelet and C. Retter, “Spread Spectrum Image Steganography”, IEEE Trans on Image Processing, vol. 8, no. 8, pp.1075-1083, 1999.

[3] H. Noda, J. Spaulding, M. Shirazi, M. Niimi and E. Kawaguchi, “BPCS” Steganography Combined with JPEG2000 Compression”, Proceedings of Pacific Rim Workshop on Digital Steganography, pp. 98-107, 2002.

[4] W. Lie and L. Chang, “Data Hiding in images with adaptive numbers of least significant bits based on human visual system”, in Proc. IEEE Int. Conf. Image Processing, pp. 286-290, 1999.

[5] T. Chen, C. Chang and M. Hwang, “A Virtual Image Cryptosystem based upon Vector Quantization”, IEEE Trans. on Image Processing, vol.7, no.10, pp. 1485-1488, 1998.

[6] S.T.Maya, M.N.Miyatake, R.Medina, ”Robust Steganography using Bit Plane complexity” 1st International Conference on Electrical and Electronics Engineering, 2004.

[7] G. Schaefer and M. Stich (2004) "UCID - An Uncompressed Colour Image Database", Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, pp. 472-480, San Jose, USA, 2004.

[8] Sergios Theodoridis, Konstantinos Koutroumbas, “An Introduction to Pattern Recognition: A MATLAB Approach”, 2010.