Universal Steganalysis Using Higher Order Statistics for Image Databases

Sonali S.Ekhande
Walchand College of Engg, Sangli
+91 9850133324
sonalisurve2007@gmail.com

Shefali.P.Sonavane
Walchand College of Engg., Sangli.
+91 9850574868
k_shefali@yahoo.co.in

P .J .Kulkarni
Walchand College of Engg., Sangli
+91 9960347507
pjk_walchand@rediffmail.com

ABSTRACT
The purpose of image steganalysis is to detect the presence of hidden message in cover photographic images. Supervised learning is an effective and commonly used method to cope with difficulties of unknown image statistics and unknown steganography. Present paper proposes; a universal approach for steganalysis for detecting presence of hidden messages embedded within digital images. This paper describes wavelet like decomposition to build higher order statistical model of natural images. SVM are then used to discriminate between clean and stego images. Review of typical method presented in this paper shows encouraging improvement. However, the present paper focuses on the fact that derivation of features in higher order statistical model is computationally intensive. Therefore it is proposed to evaluate the features' usefulness and select the most relevant ones.

Categories and Subject Descriptors
Information Security: Features – secret communication, data hiding, steganography, universal steganalysis, supervised learning.

General Terms
Security, Verification.

Keywords
Information Hiding, Steganography, Steganalysis, Image statistics, Support Vector Machine (SVM).

1 INTRODUCTION
Information hiding has been a hot research area in recent years. Early research has been focused on steganography to establish secret channel between two parties.

The goal of steganography is to embed within an innocuous looking cover medium (image, audio, video, etc.) a message so that casual inspection of the resulting medium will not reveal the presence of message [1][2]. Today steganography is an active research area due to abundance of digital media serving as cover signals, and availability of public communication network as internet. By secretly embedding information into innocent cover signal, transmitter hopes that message will reach the receiver without suspicion.

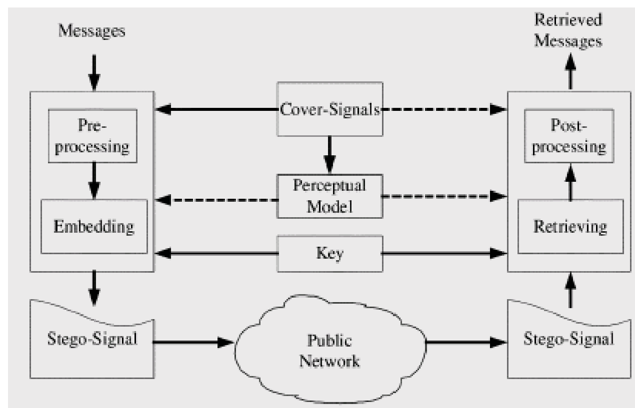

Figure 1. Illustration of information hiding process

Fig. 1 illustrate the flow of most information hiding [3] processes. If sender wants to transmit a message to a receiver through a public channel, a chosen material called cover-signal, is modified to create the stego signal by embedding desired messages. In practical application, messages are usually hidden in random position after being ciphered by using an encryption algorithm (with secret key) to achieve the goals of statistical undetectability and authorized access. After the stego signal is received, the hidden message can be extracted by using the same key with/without knowledge of the original cover signal.

Steganalysis aims at detecting presence of hidden information from stegosignals. Steganography introduces different artifact into images and leaves specific fingerprints. Hence steganographer faces difficult challenge of preserving statistics of all image features after data embedding and the steganalyzer faces the opposite problem of finding same features whose statistics are changed by data embedding.

Current steganalysis method fall broadly into two categories: embedding specific [4] or universal [5].Universal steganalysis attempts to detect the presence of an embedded message independent of embedding algorithm and ideally image format. With ever growing number of steganography tools, universal approaches are necessary to perform generic steganalysis. Aim of this paper [6] is to describe scheme for detailed analysis of steganographic procedure i.e. a universal steganalysis method for detecting presence of hidden messages. The approach taken here relies on building higher-order statistical models for natural images and looking for deviations from these models. Across a large number of natural images, there exist strong higher-order statistical regularities within a wavelet-like decomposition. The embedding of a message significantly alters these statistics and thus becomes detectable. Support vector machines are employed to detect these statistical deviations.

2 IMAGE STATISTICS

The decomposition of images using basis functions that are localized in spatial position, orientation and scale (e.g., wavelet) have proven extremely useful in image compression, image coding, noise removal and texture synthesis. One reason is that such decompositions exhibit statistical regularities that can be exploited.

2.1 2.1 Image Representation

Wavelet decompositions localize image structure in both space and frequency. The images are decomposed into three scales through separable quadrature mirror filters (QMF) to obtain nine sub bands (horizontal H_i , vertical V_i, diagonal D_i for i=1,2,3). As illustrated in fig.2 the decomposition splits the frequency space into multiple orientations and scales. For a color (RGB) image, the decomposition is applied independently to each color channel. The resulting sub bands are denoted as Vc,, Hc , and Dc where c={r; g; b}.

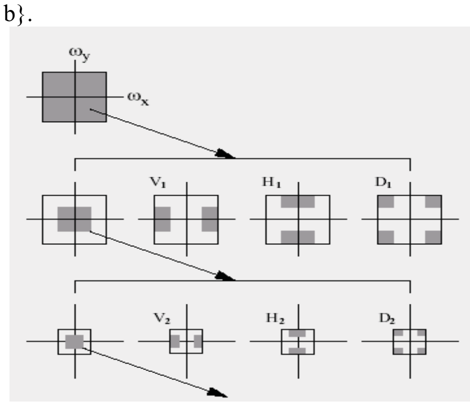

Figure 2. Decomposition of frequency space

2.2 Magnitude Statistics

Given this image decomposition, the statistical model is composed of the mean, variance, skewness and kurtosis of the sub band coefficients at each orientation, scale and color channel.

In statistics, mean is a way to describe the location of a distribution, whereas the variance is a way to capture its scale or degree of being spread out. Skewness, the third moment is measure of asymmetry of the probability distribution of real valued random variable. So an understanding of skewness of the dataset indicates whether deviation from mean is going to be positive or negative. Kurtosis, the fourth moment is measure of peakedness. Higher kurtosis means more of the variance is due to infrequent extreme deviation as opposed to frequent modestly-sized deviation.

While these statistics characterize the basic coefficient distributions, they are unlikely to capture the strong correlations that exist across space, orientation, scale and color. For example, edges tend to extend spatially and across multiple scales. As such, if a large coefficient is found in a horizontal sub band, then it is likely that its left and right spatial neighbors in the same sub band will also have a large value. Similarly, a large coefficient at scale i might indicate a large value for its parent at scales i + 1.Since wavelet coefficient possess strong intra and inter sub band dependencies, prediction error sub bands exploit these dependencies as follows.

Take a sub band coefficient $H_i(j ,k)$ as an example , where, (j, k) denotes the spatial coordinates at scale i . The magnitude of $H_i(j, k)$ can be linearly predicted by those of its parent $H_{i+1}(j/2, k/2)$; neighbors $H_i(j+1, k)$, $H_i(j, k+1)$, $H_i(j-1, k)$ and $H_i(j, k-1)$; cousins $D_i(j ,k)$ and $V_i(j, k)$; and aunts $D_{i+1}(j/2, k/2)$ and $V_{i+1}(j/2, k/2)$. If we denote the predicted magnitude as p|Hi(j, k)| .

Then, the logarithmic error $eH_i(j ,k)$ is given by [7],

$$e\, H_i(j ,k) = \log(|Hi(j ,k)|) – \log(p|H(j ,k)|)$$

This defines an error sub band eHi that corresponds to H_i . One can similarly define the error sub bands eV_i and $eD_{i.}$ at scales i=1,2,3 . The prediction errors for a cover image and its stego image have different statistics, which are useful in steganalysis .It is from this error the additional statistics namely mean, variance, skewness and kurtosis are collected. For each orientation, scale and color sub band, a similar error metric and error statistics are computed.

For a decomposition with scales i = 1,….,n, the total number of basic coefficient statistics is 36(n - 1) (12(n - 1) per color channel) and the total number of error statistics is also 36(n - 1),yielding a total of 72(n – 1) statistics. These statistics form the feature vector to be used to discriminate between clean and stego image.

3 CLASSIFICATION

From the measured statistics of a training set of clean and stego image, the goal is to determine whether a test image contains a hidden message. Support vector machine (SVM) classifier is employed [6, 8] for classification. We briefly describe, in increasing complexity, three classes of SVMs.

The first, linear separable case is mathematically the most straight-forward. The linear separable SVM classifier amounts to a hyper plane that separates the positive and negative exemplars.

The second, linear non-separable case, contends with situations in which a solution cannot be found in the former case, and is most similar to a FLD. Non-linear SVMs afford such a classifier by first mapping the training exemplars into a higher (possibly infinite) dimensional Euclidean space in which a linear SVM is then employed.

The third, non-linear case, affords the most flexible classification accuracy. OC SVM is trained on data from only one class by computing a bounding hyper sphere (in the projected high-dimensional space) that encompasses as much of the training data as possible, while minimizing its volume.

4 DISCUSSION

This paper reviews the work presented in [6]. The database consists of nearly 40,000 natural images for training and testing. The messages are embedded using Jsteg, Steghide, Jphide, Outguess and F5 with four different message sizes. For the nonlinear SVM the average detection accuracy is 78.2% (100%cover capacity), 64.5%(78%cover), 37.0%(20% cover) and 7.8%(5%cover) as per Farid. When compared with approach of Fridrich[9], the presented approach has an advantage of being applicable to JPEG,GIF and TIFF formats. However this approach seems to be more effective at lower embedding rates, Fridrich approach is more effective at higher embedding rate.

A review of this method indicated that the results of the method are encouraging, but there are several fundamental questions one may ask: Which moment features are more informative in terms of discriminating between cover images and stegoimages? Is there a mathematical explanation for the superiority of these features? Until which point, does steganalysis performance improve with the number of features used? These questions are all related to a crucial ingredient of any machine-learning system. It is to be also noted that derivation of higher order statistical features is computationally intensive. All features are not equally valuable to the learning system. Furthermore, using too many features is undesirable in terms of classification-performance due to the curse of dimensionality [10].

One cannot reliably learn the statistics of too many features with given a limited training set. Hence it is needed to evaluate the features' usefulness and select the most relevant ones. This is primarily focused in our research work.

5 ACKNOWLEDGMENTS

This work is related to the project supported by Department of Science & Technology, Delhi, India [SR/FTP/[ETA]-35/2005] in the area of Data Hiding & Information Security.

6 REFERENCES

[1] D. Kahn, "The history of steganography", in Proc. Information HidingFirst International Workshop, Cambridge, U.K., 1996.

[2] R. Anderson and F. Petitcolas, "On the limits of steganography", IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 474–481, 1998.

[3] Wen-Nung Lie and Guo-Shiang Lin "A feature based classification technique for blind image steganalysis", IEEE Transaction on multimedia, vol.7 ,no.6 ,Dec 2005 .

[4] N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software", in Lecture Notes in Computer Science, vol 1525, 1998, pp. 273–289.

[5] S. Lyu and H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines", presented at the 5th Int.Workshop on Information Hiding, Noordwijkerhout, The Netherlands, 2002.

[6] S. Lyu and H. Farid "Steganalysis using higher order image statistics", IEEE Transaction on information forensic and security ,vol 1,no.,1 March 2006.

[7] Ying Wang and Pierre Moulin "Optimized feature extraction for learning based image steganalysis" IEEE Transaction on information forensic and security ,vol 2,no 1, March 2007.

[8] C. Burges, "A tutorial on support vector machines for pattern recognition".

[9] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes", presented at the 6th International Workshop on Information Hiding, Toronto, ON, Canada,

[10] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern Classification, 2nd ed. New York: Wiley, 2001.