The ISC Int'l Journal of Information Security

ISeCure

July 2014, Volume 6, Number 2 (pp. 169–181)

http://www.isecure-journal.org

An Extended Feature Set for Blind Image Steganalysis in Contourlet Domain☆

Ehsan Shakeri [1], and Shahrokh Ghaemmaghami [1,*]

[1] *Electrical Engineering Department and Electronics Research Institute, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 1 January 2014
Revised: 22 November 2014
Accepted: 20 December 2014
Published Online: 27 December 2014

Keywords:
Blind Steganalysis, Contourlet Transform, Zernike Moments, Characteristic Function Moments, Statistical Analysis.

ABSTRACT

The aim of image steganalysis is to detect the presence of hidden messages in stego images. We propose a blind image steganalysis method in Contourlet domain and then show that the embedding process changes statistics of Contourlet coefficients. The suspicious image is transformed into Contourlet space, and then the statistics of Contourlet subbands coefficients are extracted as features. We use absolute Zernike moments and characteristic function moments of Contourlet subbands coefficients of the image to distinguish between the stego and non-stego images. Absolute Zernike moments are used to examine the randomness in the test image and characteristic function moments of Contourlet coefficients is used to form our feature set that can catch the changes made to the histogram of Contourlet coefficients. These features are fed to a nonlinear SVM classifier with an RBF kernel to distinguish between cover and stego images. We show that the embedding process distorts statistics of Contourlet coefficients, leading to detection of stego images. Experimental results confirm that the proposed features are highly sensitive to the change made by the embedding process. These results also reveal advantage of the proposed method over its counterpart steganalyzers, in cases of five popular JPEG steganography techniques.

1 Introduction

Steganography refers to the art and science of covert communication through public channels. In fact, steganography attempts to hide the existence of the secret message in seemingly normal data communications [1]. Various types of data may be used for steganographic communications, where digital images are the most popular covers selected by steganographers, particularly over public networks [2]. Due to JPEG format to be often used for efficient transmission, several data embedding tools for images have been designed for JPEG images. Among JPEG steganographic methods, Outguess [3], Model-Based (MB) [4, 5], F5 [6], PQ [7], and NSF5 [8] have received more attention for comparative analysis and benchmarking. In addition, YASS [9] and HUGO [10] steganography schemes are more recent, powerful works to be mentioned in the development of steganographic methods. YASS works completely different from most of the other algorithms, because it does not embed message in DCT

☆ This is an Extended version of the paper, E. Shakeri and S. Ghaemmaghami, "An efficient feature extraction methodology for blind image steganalysis using contourlet transform and zernike moments," *International ISC conference on information security and cryptology*, ISC 2013, August 2013.

* Corresponding author.

Email addresses: shakeri@ee.sharif.edu (E. Shakeri), ghaemmag@sharif.edu (Sh. Ghaemmaghami).

ISSN: 2008-2045

(Discrete Cosine Transform) coefficients. To disable the calibration process, data is hidden in randomly chosen blocks in the image, and then the image is passed on the public network in JPEG format. A further study on YASS, with the goal of improving the embedding rate, was presented in [11]. On the other hand, HUGO steganography limits its embedding changes to parts of image that are difficult to be modeled. Subsequently, it approximately preserves a high-dimensional feature vector [12]. By adaptively embedding in textured or noisy regions and using syndrome coding techniques, it can embed more payloads with low statistical detectability. Having a suspicious image, the goal of image steganalysis is to determine whether the image contains an embedded message or not. Existing steganalysis methods can basically be categorized into *targeted* steganalyzers, designed for some selected steganography schemes, and *blind* steganalyzers, which require no prior information about the steganographic method applied to the stego image. Due to many various types of steganography schemes introduced so far, the blind image steganalysis, that is also known as universal steganalysis, has attracted more attention by the researchers in the area of image steganalysis. Steganalysis, as a two-class pattern classification problem, aims to determine whether a test image is a cover or a stego one. The basic idea of blind steganalysis is to extract some features sensitive to information hiding, and then exploit classifiers for judging whether a given test image contains a secret message. In general, blind steganalyzers work based on learning the differences between statistical properties of cover and stego images. Blind methods extract features from the test image, which probably change after the data embedding. Often, different features are effectively combined into a feature vector that is employed to train a classifier to discriminate between cover and stego images. Generally, using features that are more sensitive to embedding alterations, results in higher detection rate in steganalysis. Accordingly, as a crucial part of blind steganalysis, most methods are focused on selection of features with a high sensitivity to the expected statistical embedding changes. One of the first blind steganalysis methods is proposed by Avcibas *et al.* in 2000 [13]. They use some image quality metrics as the feature to distinguish between stego and non-stego images, and then classify between different embedding techniques. A successful blind steganalysis scheme is presented by Farid *et al.* in 2001 [14]. They decompose an image using separable quadrature mirror filters (QMF) to split the frequency space into multiple scales and orientations. Then, higher-order statistics of subband coefficients and errors in a linear predictor of coefficient magnitude are used as features. These features are fed into a Fisher linear discriminant (FLD) classifier to determine whether the image contains an embedded message. Experimental results shows that this framework have a good performance for detecting stego images generated by Jsteg [15], Ezstego [15] and Outguess [3]. Later, simulation results reported in [16] showed that it is possible to detect stego images generated by LSB (Least Significant Bit) embedding, though at low accuracy. According to the work in [16], statistical moments of subbands coefficients magnitudes of multi-scale, multi-orientation image decompositions, such as wavelet, are useful for blind image steganalysis. The method is extended in [17] for RGB images, where SVM (Support Vector Machine) classifier is used. In [18], image statistics in wavelet domain are used as features that are extracted from the first four PDF moments of high frequency subbands coefficients, their linear prediction error is used as elements of a feature vector to distinguish between the stego and non-stego images. A powerful steganalysis method for detecting JPEG images is proposed by Fridrich, that uses the concept of calibration to increase the features sensitivity to the embedding modifications, while suppressing image-to-image variations [19]. Calibration is a process used to estimate macroscopic properties of the cover image from the stego image. During the calibration, the stego image J_1 is decompressed to the spatial domain, cropped by 4 pixels in both directions, and compressed again with the same quantization matrix. The calibrated features are obtained from an L_1 norm difference between the features calculated for J_1, the stego image, and J_2, the modified stego image, as:

$$f = ||F(J_1) - F(J_2)||_{L_1} \quad (1)$$

where F denotes a composite function that extracts 23 features from both spatial and DCT domains. The key idea for using the L_1 norm to form the DCT features, is to reduce dimensionality of the feature set. In [20], the differences between absolute values of neighboring DCT coefficients are modeled as a Markov process to develop a statistical model for detecting stego images. Four difference arrays are calculated along four directions: horizontal, vertical, diagonal, and minor diagonal. In [21], PEV-274, the Authors investigate the use of L_1 norm for DCT features, and conclude that by using the L_1 norm, some potentially useful information for steganalysis is lost. By replacing the L_1 norm with a higher-dimensional alternative, more information can be preserved, and better classification results are achieved at the expense of increased dimensionality of feature set. They extended DCT features and combined with calibrated Markov features to construct 274-D feature set. The steganalysis results reported in [11] indicate that the 274-D feature set cannot detect YASS reliably. This is not surprising, because the key purpose of YASS was to disable the calibration process. In [22], in addition to discovering

how calibration works, they conclude that when a non-calibrated version of the PEV-274 feature set is used, YASS becomes significantly more detectable. Another Markov process based JPEG steganalysis is proposed by Chen in 2008, which uses both the intra-block and inter-block correlations among JPEG coefficients [23]. Modern steganography schemes such as HUGO limits its embedding changes in textured or noisy regions that preserves a very high-dimensional feature vector. To capture a larger number of dependencies among image elements, we need to use more complex statistical descriptors and a high-dimensional feature vector. The Work in [24] proposes an ensemble classification scheme with lower complexity, which is shown to be especially suitable for steganalysis with higher-dimensional feature sets. If the embedding process is modeled by additive noise under an independence assumption, the histogram of the stego is a convolution of the noise probability mass function and the original histogram image. In [25], it is shown that the embedding process resembles lowpass filtering of the histogram, hence makes it smoother. To catch this embedding effect, they define and use center of mass (COM) of histogram characteristic function as feature. They show that for an embedding scheme with a non-increasing characteristic function (CF), the COM decreases or remains the same after embedding the data. The research in [26] points out that the COM feature is essentially the first CF moment of the image, and then a steganalysis method based on the statistical moments of wavelet characteristic function is proposed. The authors theoretically conclude that statistical moments of wavelet characteristic function are more sensitive to embedding changes, and then show that higher detection accuracy can be achieved in steganalysis of some typical embedding schemes. They rely on the fact that embedding noise makes histogram of image smoother, thus the moments of the wavelet characteristics function can reflect this change better than the PDF moments. In [27], the statistical moments of wavelet characteristics function from the test image and the prediction-error image for wavelet subbands are used as features. The main idea to use the prediction-error image is to erase the image content, and the prediction algorithm is expressed as follows:

$$\hat{x} = \begin{cases} max(a,b) & c \leq min(a,b) \\ min(a,b) & c \geq max(a,b) \\ a+b-c & otherwise \end{cases} \quad (2)$$

where a, b, and c are contents of neighboring pixel x, and $\hat{x}$ is the predicted value of x. Experimental results shows that prediction-error images could intensify the changes caused by the embedding through reducing the effect of the diversity of natural images.

In [28], Chen *et al.* extended the work in [26], and extracted statistical moments of wavelet characteristics function derived from both image pixel array and JPEG coefficients array as features. In addition to the first-order histogram, the second-order histogram is employed. Gul *et al.* [29] proposed singular value decomposition (SVD) based features for the steganalysis of PQ (perturbed quantization) embedding method in images introduced in [7]. They showed that the PQ embedding process distorts linear dependencies of neighboring pixel values that affect the SVD features, so they could detect the PQ data hiding scheme. They counted number of linearly dependent rows or columns by checking zero values at a certain index for 50% overlapping windows over a given image. In another work, Gul *et al.* [30] introduced a blind steganalysis method in order to detect spatial domain steganographic algorithms. Their method uses singular values calculated over image sub-blocks and employs content independency provided by a Wiener filtering process. Another spatial domain steganalysis method for detection of steganographic schemes that embed in the spatial domain is proposed by Pevny *et al.* in 2010 [31]. They model differences between adjacent pixels using first-order and second-order Markov chains. In most cases of image steganography, the message embedded in the image is converted to pseudo-random data, so the embedding process increases randomness of the image. Hence, a higher detection performance is expected to achieve by using the statistical moments of the image in a noise sensitive domain for steganalysis. Zernike moments are based on the radial polynomials that have been shown to be ideal for regional representation of images through orthogonal, geometrically invariant statistical characterization [32, 33]. Also, Zernike moments are sensitive to noise present in the image [34]. The work reported in [35] examined noise sensitivity of Zernike moments. They conclude that these moments are sensitive to noise, where higher order moments are more sensitive to noise. In [32], for texture feature extraction, Contourlet transform is initially applied to the image, and then Zernike moments are calculated for each subband as the feature selection process. We take this idea and use noise sensitivity of Zernike moments, and the power of these moments to capture the image properties. In [36], Zernike moments of DWT (discrete wavelet transform) subbands coefficients of the suspicious image is used as features for watermark detection. According to this research, there is a difference between these features for stego and non-stego images, while they are sensitive to the embedding changes. This work confirms that the Zernike moments are sensitive to the embedding noise. Our investigation, however, shows that these features are not suitable enough for the use in blind image steganalysis, when used alone. In [37], the first

four PDF moments of eight subbands in the third level of Contourlet transform and the first four moments of their linear prediction error of these subbands coefficients are used as features. Then, these 64 values construct a feature vector to distinguish between the stego and cover images. A blind color image steganalyzer is proposed in [38], in which the statistical features of Contourlet coefficients and co-occurrence matrices of subband images are used as features. To reduce the number of features, Analysis of Variance (ANOVA) method is used, and the selected features are fed into a nonlinear SVM to distinguish between stego and clean images. Experimental results show high sensitivity of Contourlet and co-occurrence matrix features to the embedding noise. The Contourlet transform has the ability to capture smooth contours of the images and uses Laplacian pyramid for multiscale decomposition and the directional filter bank for directional decomposition [39, 40]. It satisfies the property of anisotropy and can effectively capture geometrical structures in the textural images that wavelets fail to capture. The key advantage of Contourlet transform, as compared to wavelets, is that a sparser representation is achieved by Contourlet transform. This means that majority of the Contourlet coefficients have amplitudes close to zero, so the moments of Contourlet coefficients could be more sensitive to the embedding changes [37]. Considering these Contourlet transform properties and comparing the results given in [14, 37], we can conclude that the Contourlet transform is quite effective in blind image steganalysis. In this paper, we use the Contourlet transform and the Zernike moments for image representation and extract statistical features from Contourlet coefficients in three paths. First, the image is decomposed into three levels from finest to coarsest, and then 12 directional subbands are used for feature extraction. Next, we compute the Zernike moments for each subband and construct Zernike energy vector, from which we compute mean and variance that form first part of our feature set. For the second part of the feature set, as mentioned in [37], the first three moments of difference between actual and linear predicted coefficients in third level subbands are used. Finally, characteristic function moments of Contourlet coefficients, relating to n derivatives of the histogram, are used to form our feature set. Subsequently, an SVM classifier is employed to classify stego and non-stego images. Experimental results confirm that the proposed scheme improves performance of steganalysis over its counterpart steganalysis methods, proposed in [14, 19, 30, 37], for five typical JPEG steganography schemes, Outguess [3], MB1 [4], MB2 [5], PQ [7] and NSF5 [8]. The rest of the paper is organized as follows: Section 2 gives a brief review of the Contourlet transform and Zernike moments. In Section 3, we introduce the proposed feature extraction method and the idea behind it in detail. Experimental results are reported and discussed in Section 4. Finally the conclusion is given in Section 5.

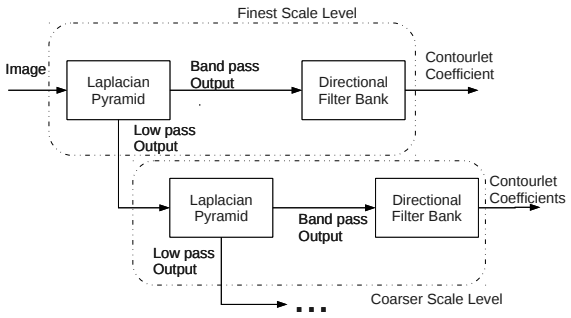

Figure 1. Basic structure of contourlet decomposition.

2 Image Representation

In this section, we provide a brief review of the Contourlet transform and Zernike moments and explain why these transforms are useful in blind image steganalysis.

2.1 Contourlet Transform

Contourlet transform is a simple directional extension to the wavelet transform using non-separable and directional filter banks that recently proposed for image representation and analysis [39]. A simple structure of Contourlet transform is shown in Figure 1. According to this figure, the Contourlet transform is made of two main filter banks by combining the Laplacian pyramid with a directional filter bank. Laplacian pyramid filter is used to construct a multiscale representation of an image. Then, the subband images from these filters are fed into a directional filter bank to give the directional details at each level. The output values from the directional filter banks at each level are known as Contourlet coefficients. The key idea of the Contourlet transform is to find more directional details of the image by dividing each highpass subband of the wavelets into more than two directions [37]. In Contourlet transform by first applying a multiscale transform, followed by a local directional transform, we can obtain a sparser expansion for images. Thus, as compared to the wavelet analysis, the Contourlet transform can give a sparser representation of the image, due to a larger number of near-zero coefficients produced. Comparing wavelet and Contourlet representations of an image shown in Figure 2, we can see how Contourlet transform can effectively represent a smoother contour with fewer coefficients, and a sparser representation. Sparsity property of the Contourlet transform, as compared to wavelet, makes it more sensitive to small changes caused by the data embedding. Often, edges are used for data embedding

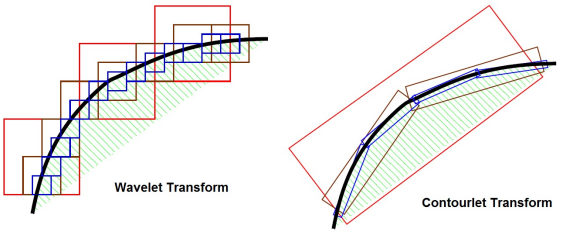

Figure 2. Comparing representation of smooth contour by wavelet and Contourlet transform [40].

in some steganography scheme. The Contourlet transform is sensitive to edges, duo to directionality and anisotropic properties of this transform. Therefore, the Contourlet transform is more effective for image steganalysis, as compared to wavelet transform, to achieve higher performance in terms of detection accuracy. The research in [37] shows that, Contourlet based steganalysis method can give a better detection accuracy than the method proposed in [18] in the wavelet domain. This research also shows that by using Contourlet transform of an image, instead of wavelet transform, we expect to improve the performance of steganalyzers that extract features in wavelet domain.

2.2 Zernike Moments

In [41], Zernike moments are introduced based on a set of complex polynomials over the interior of the unit circle, i.e., $x^2+y^2=1$. We denote the set of these polynomials by $V_{nm}(x,y)$. The Zernike moments of order n with repetition m for a digital image function can be expressed as [42]:

$$A_{nm}=\frac{n+1}{\pi}\sum_x\sum_y f(x,y)\cdot V^*_{nm}(\rho,\theta),\quad x^2+y^2\le 1 \tag{3}$$

where n is a non-negative integer, m is an integer, and they must satisfy the following constraints:

$$n\ge 0,\quad |m|\le n,\quad n-|m|=2k \tag{4}$$

These complex polynomials are orthogonal, in order to satisfy the orthogonality constraint, and are defined as:

$$V_{nm}(x,y)=V_{nm}(\rho,\theta)=R_{nm}(\rho,\theta)\cdot exp(j\cdot m\cdot\theta) \tag{5}$$

where ρ Length of vector from origin to (x,y) point. θ Angle between vector p and x axis in clockwise direction. $R_{nm}(\rho)$ radial polynomial and given by:

$$R_{nm}(\rho)=\sum_{s=0}^{n-|m|/2}(-1)^s\cdot\frac{(n-s)!}{s!\cdot(\frac{n+|m|}{2}-s)!\cdot(\frac{n-|m|}{2}-s)!}\cdot\rho^{n-2s} \tag{6}$$

It is noted that these real value radial polynomials should satisfy the symmetrical property of index m, that is:

$$R_{n,-m}(\rho)=R_{n,m}(\rho). \tag{7}$$

In fact, Zernike moments are the projection of the image onto these basis functions, where the pixels mapped on the outside of the unit circle are not used in the computation. Based on (7) and (7), we can say $V^*_{n,-m}(\rho,\theta)=V_{n,m}(\rho,\theta)$, and from (3), we conclude that:

$$A_{n,-m}=A^*_{n,m} \tag{8}$$

which we will use later. As mentioned earlier, Zernike moments work well for representing an image, and it is very useful in pattern recognition. The noise sensitivity of the Zernike moments has been investigated in [35], and it is shown that these moments are quite sensitive to noise, which increases at higher orders of moments. This suggests that the noise in the image can be reflected effectively by the Zernike moments. Hence, these moments could be reasonable candidates for steganalysis as features sensitive to the randomness brought to the image by the embedding process.

3 Proposed Feature Extraction Method

Advantage of using statistics of Contourlet coefficients to extract features sensitive to the embedding of noise-like data has been investigated in [36, 37]. These works show that Contourlet based steganalysis method can give a higher accuracy of detection than the counterpart methods in the wavelet domain. The key advantage of Contourlet transform, as compared to wavelets, is that a sparser representation is achieved by Contourlet transform that makes the moments of Contourlet coefficients more sensitive to the embedding process. Also, the Contourlet transform is sensitive to edges, as a critical place for data embedding in many steganography schemes. These fascinating properties of Contourlet transform persuade us to develop a steganalyzer based on statistics of Contourlet coefficients. We choose the coarser subbands due to more resolutional and directional properties of this transform. In this work, we use eight directions on third level and four directions on second level Contourlet transformation. So, we have 12 directional subbands as sources of the feature extraction process. As shown in Figure 3, the suspicious image is decomposed by Contourlet transform, and then the statistical features are extracted in three paths. First, absolute Zernike moments of Contourlet subbands coefficients of the image are used to examine randomness in the test image. In the second path, linear prediction error of each Contourlet subband is used to reflect the change in correlation of neighboring Contourlet coefficients caused by the embedded noise. Finally, characteristic function moments of Contourlet coefficients, relating to n derivatives of the histogram, is used to form our feature set that can catch the changes made to the histogram. Details about each part of our steganalyzer

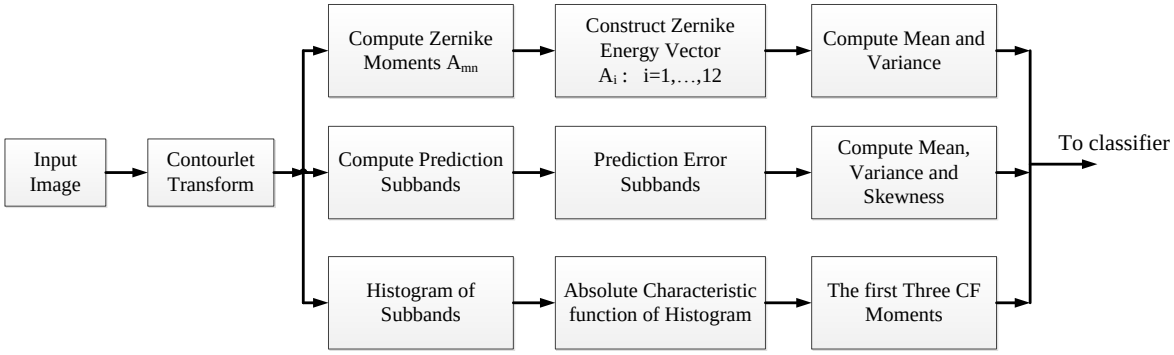

Figure 3. Proposed feature extraction method for an input image.

are given in the following.

3.1 Zernike Moments Based Features

We assume that the image steganography is similar to an additive noise embedding process [25, 43]. In Contourlet domain, this is expressed as:

$$X = S + Z \tag{9}$$

where X is the stego signal, S, is the cover signal, and Z is the embedded noise. This noise is often assumed to be iid independent of S. In [37], the first four PDF moments of eight subbands in the third level of Contourlet transform are used as features. In the proposed method, to intensify sensitivity of features to the embedding change, as discussed earlier, we first compute the Zernike moments of each subband and construct the Zernike energy vector, and then we use statistical moments of these vectors as features. The Zernike moments of order n with repetition m for each specific subband can be shown as:

$$X_{nm} = S_{nm} + Z_{nm} \tag{10}$$

where X_{nm}, S_{nm}, Z_{nm} denote the Zernike moments of order n with repetition m for stego, cover, and the embedded noise, respectively. We have Z_{nm} defined as:

$$Z_{nm} = \frac{n+1}{\pi} \sum_i \sum_j V^*_{nm} \cdot Z(i,j) \tag{11}$$

Basically, there is no restriction on the order of the Zernike moments of a given image. Lower order Zernike moments reflect the gross shape features that are not often used for data embedding, where higher order moments capture the fine details of the image. In fact, high frequency details are presented by higher order moments that are more sensitive to noise. According to the work in [35], phase of the Zernike moments are not useful for the classification purposes. We have checked statistical moments of the phase values of the Zernike moments and found out that these features are not sensitive to the embedding changes. So, in this work, we use absolute value of the Zernike moments of order 15, and exclude the first four moments. According to (6):

$$|A_{n,-m}| = |A_{n,m}| \tag{12}$$

We use absolute value of the Zernike moments, thus only the cases that $m \geq 0$ needs to be considered. We define the Zernike energy vector by these moments for subbband i as:

$$A_i = \left[|A_{3,1}|^2, |A_{3,3}|^2, \ldots, |A_{15,15}|^2\right], \quad i = 1, 2, \ldots, 12 \tag{13}$$

Here, we use the mean and variance of the Zernike vector for each subband as feature. Therefore, we obtain $2 \times 12 = 24$, features. It is to be noted that the design parameter of Zernike based features requires choosing the order of Zernike moments participated in Zernike energy vector. Due to the stochastic nature of this problem, giving a theoretical analysis to compute the best order of Zernike moments to reach the highest detection performance could be quite sophisticated, if not infeasible. However, as mentioned earlier, lower order Zernike moments reflect the gross shape features that are not suitable for feature extraction, while computing higher order moments is time consuming. To investigate the problem and finding a reasonable range of n, we conducted experiments to evaluate the detection performance of the features using Zernike moments for different values of n. We found that using moments up to order n, where $9 < n < 18$, could better balance between the performance and the computational complexity. We used 1400 different images and their stego version with F5 steganography at the embedding rate of 10%. We randomly selected 1000 images from each set for training and 400 remaining images for test. In Table 1, we report detection rate of Zernike based features when using the absolute value of Zernike moments of order n, excluding the first four moments. As seen in this Table, it is appropriate to choose the Zernike moments of order 15 and exclude the first four moments. By expanding our condition and other steganography schemes, the order 15 could be a reasonable choice.

Table 1. Comparison of detection accuracy versus the order of Zernike moments against F5 steganography.

Order	Number of moments	Detection accuracy
10	32	59.4
11	38	57.1
12	45	61.3
13	52	68.9
14	60	75.2
15	68	76.8
16	77	75.9
17	86	76.5

3.2 Prediction Error Subband

According to [40], the subband coefficients are correlated to their spatial orientation and scale neighbors. Therefore, the second set of statistics collected from Contourlet transform are based on the errors in an optimal linear predictor of coefficient magnitude that is used to reflect the change made to correlation of neighboring Contourlet coefficients due to the embedded noise. This idea initially proposed by Farid *et al.* in [14]. We can denote the low-frequency subband, vertical subband, horizontal subband, and diagonal subband at scale $i = 1, \cdots, n$ as A_i, V_i, H_i and D_i, respectively. Take the prediction subband of H_i as an example, then its linear predictor for the magnitude subband in a subset of all possible neighbors can be given as [14]:

$$\begin{aligned}\hat{H}_i(x,y) = {} & w_1 H_i(x-1,y) + w_2 H_i(x+1,y) \\ & + w_3 H_i(x,y-1) + w_4 H_i(x,y+1) \\ & + w_5 H_{i+1}(x/2,y/2) + w_6 D_i(x,y) \\ & + w_7 D_{i+1}(x/2,y/2) \end{aligned} \quad (14)$$

where w_k denotes scalar weighting values. This linear relationship may be expressed more compactly in matrix form as: $\overrightarrow{H} = Q\overrightarrow{w}$, where the column vector $\overrightarrow{w} = (w_1, \ldots, w_7)^T$ consists of the scalar weighting values, the vector $\overrightarrow{H}$ contains the coefficient magnitudes of $H_i(x,y)$, and the columns of the matrix Q contains the neighboring coefficient magnitudes. The coefficients that minimize the squared error of the estimator are given as:

$$\overrightarrow{w} = (Q^T Q)^{-1} Q^T H \quad (15)$$

Thus the log error of the linear predictor can be expressed as:

$$\overrightarrow{E_H} = \log \overrightarrow{H} - \log Q\overrightarrow{w} = \log \frac{|\overrightarrow{H}|}{|Q\overrightarrow{w}|} \quad (16)$$

We call the subbands, whose coefficients are the error of prediction, as the prediction error subbands. This idea exploited for feature extraction in Contourlet domain by Sajedi and Jamzad [37], and experimental result revealed the superiority of the prediction error of Contourlet subbands over the prediction error wavelet subbands. We employ the first three moments of linear prediction error with linear prediction coefficients for eight subbands at the third level of Contourlet transform and use these 24 values as features for steganalysis.

3.3 Absolute Characteristic Function Moments

By modeling the embedding process as additive noise, under an independence assumption, the histogram of the stego is obtained by a convolution of the noise probability mass function and the original histogram image. The work in [26] pointed out that the moments of the wavelet characteristic function could reflect the embedding alterations better than the PDF moments, due to the smoothing effects of the random data embedding. In [43], the authors showed that by using a Generalized Gaussian Distribution (GGD) model for wavelet coefficients, the absolute CF moments of wavelet coefficients outperform the PDF moments for blind image steganalysis. Also, in [44], it is proved via four theorems, that if the feature extraction sources approximately follow the Gaussian distribution before and after data embedding, the CF moments outperform PDF moments for steganalysis. In general, coefficients of multiresolution transforms, such as wavelet and Contourlet coefficients, do not exhibit Gaussian distribution. It is shown in [45] that the Contourlet transform in detail subband coefficients can be modeled using a zero-mean GGD. A GGD is given as:

$$P_{\alpha,\beta}(s) = \frac{\beta}{2\alpha\Gamma(\frac{1}{\beta})} exp\{-(\frac{|s|}{\alpha})^{\beta}\},\ \alpha > 0, \beta > 0, s \in R \quad (17)$$

where $\Gamma(.)$ is the Gamma function, α is the scale parameter, and β is the shape parameter. The Gaussian and Laplacian PDFs are special cases of GGD with $\beta = 2$ and 1, respectively. Figure 4 shows histogram of one of the 2^{nd} scale subbands of image and its stego obtained from PQ steganography at the embedding rate of 10%. As shown, the embedding noise reduces the peakiness of the histogram of Contourlet coefficients. As mentioned earlier, it is proved in [43] that the CF moments of the coefficients subbands outperform the PDF moments for steganalysis, if the coefficients of the transform follow Gaussian or generalized Gaussian distributions. In fact, the amount of peakiness of the histogram of Contourlet coefficients is reduced by the embedding process. We use this idea in the Contourlet domain and exploit the CF moments of the Contourlet coefficients as features for blind image steganalysis. Characteristics function for a random se-

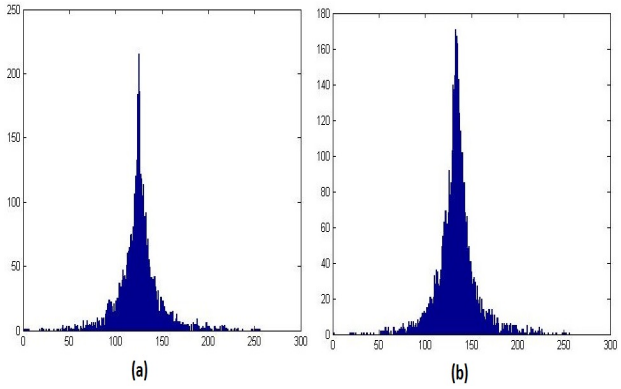

Figure 4. Distribution of Contourlet coefficients: (a) histogram of the subbands in 2^{nd} scale coefficients of image. (b) histogram of its stego of the same subbands obtained from PQ steganography at 10% embedding rate.

quence $X = (x_1, x_2, \cdots, x_n)$, with probability density function $P_X(x)$, defined as:

$$\Phi_X(\omega) = E\{e^{j\omega x}\} = \int_{-\infty}^{+\infty} p_X(x) e^{j\omega x} dx \qquad (18)$$

The n^{th} moment of the characteristic function can be obtained from:

$$M_n = E(x^n) = \int_{-\infty}^{+\infty} \phi_X(\omega) \omega^n d\omega \qquad (19)$$

The absolute CF moments can be given as:

$$M_n^A = \int_{-\infty}^{+\infty} |\phi_X(\omega)||\omega|^n d\omega \qquad (20)$$

In order to calculate the empirical absolute CF moments, we estimate the PDF, $P_X(x)$, by an M-bin histogram $h(m)|_{m=0}^{M-1}$. We denote variable number of histogram in the horizontal axis by $K = 2^{\lceil \log_2 M \rceil}$, then The K-point CF, can be computed from [44]:

$$\phi_X(k) = \sum_{m=0}^{M-1} h(m) e^{\frac{j2\pi mk}{K}}, \quad k = 0, 1, \ldots, K-1 \qquad (21)$$

In fact, $\phi_X(k)$ is the discrete form of $\phi_X(\omega)$, which can be obtained from FFT computation. According to[43], using normalized CF moments reduces the overlap between the range of CF moments of the cover and stego image, which improves the discrimination power of features. The n^{th} absolute normalized moment of discrete CF can be defined as [26]:

$$\bar{M}_n^A = \frac{\sum_{k=0}^{\frac{K}{2}-1} |\phi_X(k)| k^n}{\sum_{k=0}^{\frac{K}{2}-1} |\phi_X(k)|} \qquad (22)$$

A key concern for improving the performance of our steganalyzer is the number of moments that participate in the analysis. In [43], via extensive experiments and using the Bhattacharyya distance, it is concluded that using just the first three moments is enough and it is not necessary to increase the number of moments for improving the detection accuracy of steganalyzer. Here, we use the first three absolute moments of characteristics function for 12 directional subbands of Contourlet transform, thus we obtain $3 \times 12 = 36$ features for steganalysis. We merge these features with the Zernike based features and the first three moments of linear prediction error with linear prediction coefficients in the third level of Contourlet subbands, and then use these 84 values as features for steganalysis. These features are fed to a nonlinear SVM classifier with a Radial Basis Function (RBF) kernel to distinguish between cover and stego images.

4 Experiments and Discussion

To evaluate the proposed steganalysis method, we used 1400 different color images including different kinds of images taken from CorelDraw image database [48]. All the images were converted to gray level images of the size 512×512 and saved in JPEG format with quality factor of 80. All the experiments were done using Matlab R2010a. To construct stego images, random data are embedded into images using Outguess [3], MB1 [4], MB2 [5], PQ [7] and NSF5 [8] steganography methods. For evaluating the embedding methods, three stego image sets at different embedding rates are generated. We embed random messages at rates 10%, 20%, and 40% for each steganography methods in our experiments. It is to be noted that, due to the limited capacity of the Outguess algorithm [3], the embedding rate is set to 5%, 10%, and 20% to make the stego image sets. If, for a given image, the bpc (Bits Per non-zero AC DCT Coefficients) rate is greater than the maximal bpc rate bpc_{max}, we take bpc_{max} as the embedding rate. In case of PQ steganography, because of the nature of the method, recompressed image without data embedding is used as cover image to minimize the effect of the JPEG recompression. In [46], detection accuracy of the PQ is investigated in two cases, with a single-compressed image as cover and a double-compressed as cover image. In the first case, detection of PQ is possible, while in the second case, the detection rates of PQ method are in a range of random guess. Also, for each steganography scheme a mixed stego database by combining different embedding rates is used. We report the detection rate of each case based on averaging the results obtained from five runs of the test. We randomly select 1000 images from each set for training and 400 images for test, and extract the ROC (receiver operating characteristic) curves of steganalyzers. We use the SVM classifier with RBF kernel to evaluate performance of the proposed steganalysis method, which is implemented using LibSVM toolbox [47]. According to the research in [46], Wavelet-based steganalyzer (WBS) [18] and Feature-based steganalyzer (FBS) [19] are two powerful blind steganalysis methods. For compar-

ison, the methods given in [14, 19, 30, 37], denoted as WBS, FBS, SVBS and CBS, respectively, are also implemented. The first four PDF moments of nine high frequency wavelet subbands magnitude and phase statistics and their linear prediction error are used as features in [14], 23 calibrated features of spatial and DCT domains are used as features in [19], singular value decomposition based features are used as features in [30], and the first four PDF moments of the Contourlet subbands coefficients, plus statistical moments of log prediction error subband coefficients of the Contourlet transform are used in [37], to create features set of this steganalyzer. Also, the methods given in [20, 23, 31] are implemented. We list results of our experiments with the proposed method and the methods given in [14, 19, 20, 23, 30, 31, 37] for Outguess, MB1, MB2, PQ and NSF5 steganography methods in tables 2-6. The performance of the steganalyzers are given by TP and FP, which stand for true positive rate and false positive rate of the steganalyzers, respectively.

The arithmetic average of T_P and T_N are listed in these tables as the detection accuracy. According to the Table 2-6, we can see that in most cases, the proposed method outperforms the methods given in [14, 19, 30, 31, 37]. It is clear that our proposed scheme outperforms WBS, CBS, SVBS methods by a significant margin and is better than FBS steganalysis by a smaller margin, except for the Outguess steganography scheme that FBS works better than the proposed method. By using this steganalysis scheme, at least 5%, 2%, 8% and 6% improvements is achieved in detection accuracy, as compared to the results of WBS, FBS, SVBS, and CBS methods, respectively. We figure out that the Zernike moments statistics are more sensitive to the embedding, as compared to wavelet and Contourlet coefficients. In other words, the embedding changes make significant changes to Zernike moments that effectively enable the classifier to distinguish between stego and cover images. However, the methods given in [20, 23], that are the most powerful steganalyzers for detecting JPEG images, outperform our method in case of MB1, MB2, and

Table 2. Comparison of detection rates of steganalyzers in case of outguess steganography(%).

Embedding Rate(bpc)	0.05	0.1	0.2	Combined Embedding rate
WBS	69.4	75.2	81.7	77.3
FBS	76.5	81.6	88.5	73.2
SVBS	58.9	61.1	63.4	61.7
CBS	71.3	77.9	82	78.9
[20]	84.5	87.3	91.1	85.6
[23]	87.7	90.2	96.8	90.5
[31]	56.4	64.7	70.1	62.8
Proposed	79	83.7	85.3	82.1

Table 3. Comparison of detection rates of steganalyzers in case of MB1 steganography(%).

Embedding Rate(bpc)	0.1	0.2	0.4	Combined Embedding rate
WBS	58.8	67.1	71.5	66.5
FBS	56.7	74.5	83.6	76.8
SVBS	54.9	63.5	70.1	62.2
CBS	59.6	66.7	74.9	68.3
[20]	85.9	90.6	95	92.3
[23]	87.1	92.5	97.4	93.5
[31]	52.3	61.7	65.3	60.1
Proposed	74.2	79.6	81.1	78.3

Table 4. Comparison of detection rates of steganalyzers in case of MB2 steganography(%).

Embedding Rate(bpc)	0.1	0.2	0.4	Combined Embedding rate
WBS	58.5	68.7	72.1	67.3
FBS	58.4	67.3	74.5	69.1
SVBS	56.1	62.9	68.4	65
CBS	61.8	71.5	77.6	70.9
[20]	84.3	88.5	93.1	89.6
[23]	85.6	90.9	96.8	91.5
[31]	52.2	59.7	64.9	61.5
Proposed	64.9	70.8	79.3	73.7

Table 5. Comparison of detection rates of steganalyzers in case of PQ steganography(%).

Embedding Rate(bpc)	0.1	0.2	0.4	Combined Embedding rate
WBS	51.2	54.1	65.2	58.9
FBS	53.6	55.9	67.4	60.3
SVBS	69.7	73.6	79.1	72.1
CBS	58.4	60.9	70.5	63.8
[20]	70.1	74.7	76.3	73.6
[23]	69.5	76.5	77.8	75
[31]	55.2	62.8	63.6	60.5
Proposed	72.5	77.1	80.5	76.9

Table 6. Comparison of detection rates of steganalyzers in case of NSF5 steganography(%).

Embedding Rate(bpc)	0.1	0.2	0.4	Combined Embedding rate
WBS	49.8	52.3	55.6	55.2
FBS	55.4	59.8	65.1	61.4
SVBS	55.1	57.4	60.1	57.9
CBS	53.9	55.6	57.5	57.1
[20]	48.5	53.6	53.8	52.8
[23]	52.1	54.5	56.4	53.7
[31]	48.3	51.9	54.2	52.5
Proposed	58.6	63.1	64.9	62.3

Outguess steganography schemes. Due to the sparsity property of the Contourlet coefficients, and noise sensitivity of the Zernike moments, the proposed features effectively reflect the statistical changes after embedding. According to Table 5, the average accuracy of our scheme against PQ steganography methods is relatively satisfactory even for low embedding rates, where the average accuracy is about 76.9%. As seen in Table 5, the best detection rate against PQ steganography can be achieved by the proposed method, and the second best for detecting the PQ is the method given in [23]. The third best, is the method given in [20], followed by the SVBS as the fourth steganalyzer for detecting the PQ. The other four methods are weak in detecting the PQ steganography. These results confirm superiority of our method over its counterpart steganalyzers for the PQ steganography scheme. By comparing results of the tests with WBS and CBS methods, we can conclude that the Contourlet transform is more effective in blind image steganalysis, due to higher sensitivity of Contourlet coefficients to statistical alterations made by the embedding process. We see that SVBS is a powerful method for detecting the PQ steganography, but does not work quite well in case of other steganography schemes. Another conclusion from these results is that, FBS is a good steganlyzer for detecting Outguess, MB1, and MB2, especially at high embedding rates, but this method is unable to detect PQ and NSF5 at low embedding rates. Also, the methods given in [20, 23], which are the most powerful steganalyzers for detecting MB1, MB2, and Outguess steganography, are not strong enough to detect PQ and NSF5 at low embedding rates. In case of NSF5 method, the proposed features are not more effective. This indicates that in NSF5 method, noise caused by the embedding has little effect on statistics of Contourlet coefficients, so the Zernike moments and other statistics of Contourlet subbands are not helpful. In fact, the Zernike moments and other statistical moments of Contourlet transform are effective features, when the Contourlet coefficients can reflect the embedding noise effectively and, in this case, using the Zernike moments could make it possible to get better classification rates, when comparing to case that features are extracted directly by the statistical moments of the Contourlet subbands. We remind that NSF5 embedding is currently one of the most secure algorithms for JPEG image steganography that uses the wet paper codes to minimize the change made to the image statistics. By comparing results of experiments using the proposed method, and the method given in [37], we conclude that we can improve performance of this steganalyzer using statistics of the Zernike vector instead of the statistical moments of Contourlet subbands directly. Another investigation is to get an overall estimate of the computational complexity of each steganalysis method. Table 7 shows the run time evaluation of the proposed method and other steganalyzers, where the average values of the run time are obtained from steganalysis of 250 sample images. As a result, we can see that the CBS (Contourlet Based Steganalysis) method is less time consuming than others, and our proposed method is the third best and better than SVBS and FBS methods.

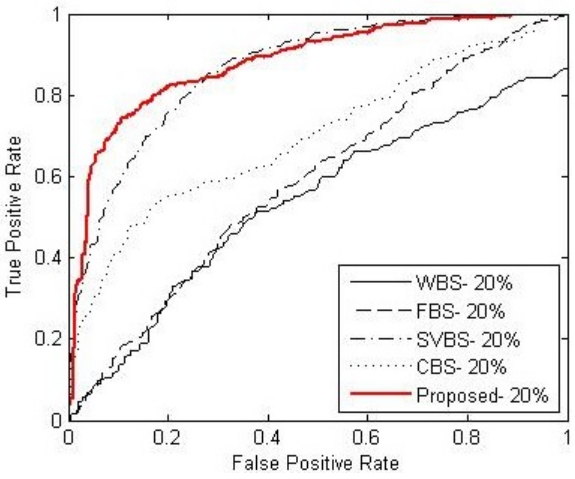

Figure 5. Roc curves of steganalyzers for PQ steganography at embedding rate of 20%.

Table 7. Comparison of time evalution of steganalysis methods (seconds).

Steganalysis method	Average time(seconds)
WBS	1.8
FBS	5.2
SVBS	6.35
CBS	1.45
Proposed	4.85

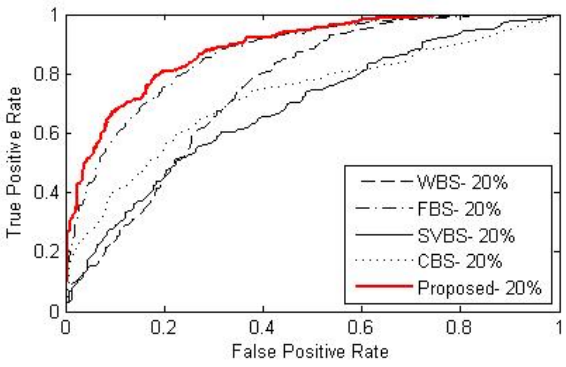

Figure 6. Roc curves of steganalyzers for MB1 steganography at embedding rate of 20%.

The ROC curves of the proposed steganalysis method and the counterpart schemes for PQ steganography are shown in Figure 5. The results indicate that our method comes with a higher performance for detecting the PQ steganography, as compared to the methods given in [14, 19, 20, 23, 30, 31, 37], especially at lower embedding rates. The average detection accuracy of our method for detecting the PQ steganography is about 77.1% for the embedding rate of 20%, where at least a 3.5% improvement in detection is achieved using the proposed method, as compared to its counterparts. A similar comparison between the performance of our method and that of its counterparts for MB1 steganography at embedding rates of 20% is presented in Figure 6. This figure demonstrates superiority of our scheme, for MB1 steganography, over the steganalysis methods given [14, 19, 30, 37]. We also conducted another experiment to make an overall comparison between the selected well-known steganalyzers and the proposed method. In this experiment, we constructed stego image sets by combining 1400 stego images from Outguess, MB1, MB2, PQ, and NSF5 steganography methods. The results of this experiment are given in Table 8, which shows that our method is superior to the methods given in [14, 19, 30, 31, 37], while inferior to the methods given in [20, 23]. As mentioned earlier, the two latter methods are the most powerful steganalyzers for detecting stego JPEG images. However, as shown in Table 5, our method outperforms these two methods in case of the PQ steganography, though by a small margin.

5 Conclusions

A blind image steganalysis scheme, based on statistical moments of Contourlet transform and Zernike moments, has been presented in this paper. The suspicious image is decomposed by Contourlet transform, and then the statistics features are extracted from three paths. First, absolute Zernike moments of Contourlet subbands coefficients of the image are used to examine randomness in the test image

Table 8. Comparison of detection rates of steganalyzers in case of combined steganography images.

Embedding Rate(bpc)	0.05	0.1	0.2
WBS	55.2	58.7	65.5
FBS	57.9	62.3	69.6
SVBS	58.5	59	65.4
CBS	61.3	66.2	75.1
[20]	48.5	53.6	53.8
[23]	69.4	78.9	84.7
[31]	56.7	56.8	64.9
Proposed	65.5	71.4	79

that affects the reflection of changes caused by the embedding process. We shape the Zernike energy vector by higher order moments and use mean and variance of these vectors in each subband as features. In the second path, linear prediction error of each Contourlet subband is used to reflect the correlation changing of neighboring Contourlet coefficients caused by the embedded noise. Finally, characteristic function moments of Contourlet coefficients, relating to n derivatives of the histogram, are used to form our feature set that can catch the changes made to the histogram. Contourlet, as a multi-resolution transform with sparsity property, and the Zernike moments for getting a higher sensitivity to noise are used. We have compared the proposed steganalyzer to the methods introduced in [14, 19, 30, 37]. Experimental results for five well-known types of JPEG image steganography have confirmed that the proposed features are more effective in blind image steganalysis and improve the detection accuracy of steganalysis, as compared to four well-known steganalyzers given in [14, 19, 30, 37].

References

[1] S. Katzenbeisser and F. A. P. Petitcolas, "Defining Security in Steganographic Systems," *in Proc. of the SPIE, Security and Watermarking of Multimedia Contents IV*, vol. 4675, pp. 50-56, 2002.

[2] M. Kharrazi, H. T. Sencar and N. Memon, "Image Steganography and Steganalysis:Concepts and Practice," *Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore*, 2004.

[3] N. Provos, "Defending against statistical steganalysis," *in 10th USENIX Security Symposium*, 2001.

[4] P. Sallee, "Model-based steganography," *in Proc. of International Workshop on Digital Watermarking*, Seoul, Korea, 2003.

[5] P. Sallee, "Model-based methods for steganography and steganalysis," *International Journal of Iamges and Graphics*, vol. 5, pp. 167-190, 2005.

[6] A. Westfeld, "F5: a steganographic algorithm: High capacity despite better steganalysis," *presented at the 4th International Workshop on Information Hiding*, 2001.

[7] J. Fridrich, M. Goljan and D. Soukal, "Perturbed quantization steganography with wet paper codes," *in Proc. ACM Multimedia Security Workshop*, pp. 4-15, 2004.

[8] J. Kodovsky, J. Fridrich and T. Pevny, "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities," *in Proc. of the 9th ACM Multimedia Security Workshop*, pp. 3-14, 2007.

[9] K. Solanki, A. Sarkar and B. S. Manjunath, "YASS: yet another steganographic scheme that resists blind steganalysis," *in 9th International Workshop on Information Hiding*, 2007.

[10] T. Pevny, T. Filler and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," *in 12th International Workshop on Information Hiding*, 2010.

[11] A. Sarkar, K. Solanki and B. S. Manjunath, "Further Study on YASS: Steganography Based on Randomized Embedding to Resist Blind Steganalysis," *in Proc. of SPIE Security, Steganography and Watermarking of Multimedia Contents*, 2008.

[12] J. Fridrich, J. Kodovsky, V. Holub and M. Goljan, "Steganalysis of Content-Adaptive Steganography in Spatial Domain," *in 13th International Conference on Information Hiding*, Vol. 6958, pp. 102-117, 2011.

[13] I. Avcibas, N. Memon and B. Sankur, "Steganalysis of watermarking techniques using image quality metrics," *in Proc. of the SPIE, Security and Watermarking of Multimedia Contents II*, vol. 4314, pp. 523531, 2000.

[14] H. Farid, "Detecting steganographic messages in digital images," Technical Report TR2001-412, Dartmouth College, Hanover, NH, 2001.

[15] R. Machado, EZStego. [Online]. Available: http://www.ezstego.com.

[16] H. Farid, "Detecting hidden messages using higher-order statistical models," *in: Proc. of IEEE International Conference on Image processing*, vol. 2, pp. 905908, 2002.

[17] H. Farid and S. Lyu, "Detecting hidden messages using higher-order statistics and support vector machines," *in Proc. of fifth International Information Hiding Workshop, Lecture Notes in Computer Science*, vol. 2578, Springer, Berlin, pp. 340354, 2002.

[18] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inf. Forensics Secur*, vol.1, no.1, pp.111-119, 2006.

[19] J. Fridrich, "Feature-Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes," *Information Hiding*, vol. 3200, ed: Springer Berlin / Heidelberg, pp. 67-81, 2005.

[20] Y. Shi, C. Chen and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," *in J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, editors, Information Hiding, 8th International Workshop*, vol. 4437, pp. 249264, 2006.

[21] T. Pevny and J. Fridrich, "Merging Markov and DCT Features for Multi-Class JPEG Steganalysis," *in SPIE, Electronic Imaging, Security, Steganography and Watermarking of Multimedia contents*, vol. 6505, 2007.

[22] J. Kodovsky and J. Fridrich, "Calibration revisited," *in Proc. of the 11th ACM workshop on Multimedia and security*, pp. 6374, 2009.

[23] C. Chen and Y.Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," *in Circuits and Systems, IEEE International Symposium on*, pp. 30293032, 2008.

[24] J. Kodovsky, J. Fridrich and V. Holub, "Ensemble classifiers for steganalysis of digital media," *Information Forensics and Security, IEEE Transactions on*, vol. 7, pp. 432444, 2012.

[25] J. Harmsen and W. Pearlman, "Steganalysis of additive noise modelable information hiding," *in Proc. of Security Steganography and Watermarking of Multimedia Contents V, SPIE*, vol. 5020, pp. 131-142, 2003.

[26] G. Xuan, Y. Shi and J. Gao, "Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions," *in Proc. of 7th international Information Hiding Workshop, Lecture Notes in Computer Science. Berlin, Germany: Springer*, vol. 3727, pp. 262-277, 2005.

[27] Y. Shi, G. Xuan and J. Gao, "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network," *Multimedia and Expo, IEEE International Conference on*, pp. 4-8, 2005.

[28] C. Chen, Y. Shi, W. Chen and G. Xuan, "Statistical Moments Based Universal Steganalysis using JPEG 2-D Array and 2-D Characteristic Function," *Image Processing, IEEE International Conference on*, pp. 105-108, 2006.

[29] G. Gul, A. Dirik and E. Avcibas, "Steganalytic Features for JPEG Compression-Based Perturbed Quantization," *Signal Processing Letters, IEEE*, vol. 14, pp. 205-208, 2007.

[30] G. Gul and F. Kurugollu, "SVD-Based Universal Spatial Domain Image Steganalysis," *Informa-*

tion Forensics and Security, IEEE Transactions on, vol. 5, pp. 349-353, 2010.
[31] T. Pevny, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *Information Forensics and Security, IEEE Transactions on*, vol. 5, pp. 215224, 2010.
[32] M. A. L. Vijilious and V. S. Bharathi, "Texture Feature Extraction Approach to Palmprint using Nonsubsampled Contourlet Transform and Orthogonal Moments," in *International Journal of Future Computer and Communication*, vol. 1, no. 3, 2012.
[33] T. W. Lin and Y. F. Chou, "A Comparative Study of Zernike Moments for Image Retrieval," *16th IPPR Conference on Computer Vision, Graphics and Image Processing*, 2003.
[34] G. Chen and Y. Xie, "Rotation invariant feature extraction by combining denoising with Zernike moments," *Wavelet Analysis and Pattern Recognition (ICWAPR)*, pp. 186-189, 2010.
[35] C. H. Teh and R. T. Chin, "On image analysis by the methods of moments," *Pattern Analysis and Machine Intelligence,* vol. 10, no. 4, pp. 496-513, 1988.
[36] M. Abolghasemi, H. Aghaeinia and K. Faez, "Data Hiding Detection Based on DWT and Zernike Moments," *in 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, 2007.
[37] H. Sajedi and M. Jamzad, "CBS: Contourlet-based steganalysis method," *Journal of Signal Processing Systems*, vol. 61, pp. 367-373, 2010.
[38] M. Sheikhan, M. Pezhmanpour and M. Moin, "Improved contourlet-based steganalysis using binary particle swarm optimization and radial basis neural networks," *Neural Computing and Applications*, vol. 21, pp. 1717-1728, 2012.
[39] M. N. Do and M. Vetterli, "The Contourlet transform: an efficient directional multiresolution image representation," *IEEE Trans. Image Processing* , vol. 14, no. 12, pp. 2091-2106, 2005.
[40] D. D. Y. Po and M. N. Do, "Directional multiscale modeling of images using the contourlet transform," *IEEE Trans. Image Processing*, vol. 15, no. 6, pp. 1610-1620, 2006.
[41] F. Zernike, Physica, vol. 1, p. 689, 1934.
[42] A. Khotanzad and Y. H. Hong, "Invariant Image Recognition by Zernike Moments," *IEEE Trans. on Pattern Analysis and Machine Intelligence,* pp. 489-497, 1990.
[43] Y. Wang and P. Moulin, "Optimized feature extraction for learning based image steganalysis," *IEEE Trans. Inf. Forensics Secur,* vol. 2, no. 1, pp. 31-45, 2007.
[44] L. Xiangyang, L. Fenlin and L. Shiguo, "On the Typical Statistic Features for Image Blind Steganalysis," *Selected Areas in Communications, IEEE Journal on*, vol. 29, pp. 1404-1422, 2011.
[45] H. Qu, Y. Peng and W. Sun, "Texture Image Retrieval Based on Contourlet Coefficient Modeling with Generalized Gaussian Distribution," *ISICA 2007, Springer, Heidelberg*, vol. 4683, pp. 493-502, 2007.
[46] M. Kharrazi, H. T. Sencar, and N. Memon, "Performance Study of Common Image Steganography and Steganalysis Technique," *Journal of Electronic Imaging, 15(4):041104-1-041104-16*, 2006.
[47] C.-C. Chang and C.-J. Lin, "LIBSVM: A Library for Support Vector Machines," . [Online]. Available: http://www.csie.ntu.edu.tw/~cjlin/libsvm.
[48] CorelDraw Software, www.corel.com.

Ehsan Shakeri was born in 1988 in Tehran, Iran. He received his B.S. in Electrical Engineering from Shahed University of Technology (2011) and his M.S. in Secure Communications from Sharif University of Technology (2013). He is now a member of digital signal processing researcher in institute of communication research. His main research interests are signal processing, cryptology, security, data hiding, and digital communication.

Shahrokh Ghaemmaghami received B.S. and M.Sc. degrees from Electrical Engineering Department of Sharif University of Technology, Tehran, Iran, and Ph.D. from Queensland University of Technology, Brisbane, Australia. He is an associate professor of signal processing at Sharif University of Technology. Dr. Ghaemmaghami has been leading many large research projects and his research interests lie in the areas of signal processing and information hiding.

The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 197)
http://www.isecure-journal.org

Persian Abstract

یک روش نهان‌کاوی کور تصویر در حوزه کانتورلت برمبنای یک مجموعه ویژگی‌های توسعه داده شده

احسان شاکری[1] و شاهرخ قائم‌مقامی[1]

[1]دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

هدف اصلی نهان‌کاوی تصویر کشف وجود اطلاعات مخفی در تصویر نهانه است. در این مقاله یک روش نهان‌کاوی کور تصویر در حوزه کانتورلت معرفی می‌کنیم و سپس نشان می‌دهیم که عمل درج، آماره‌های ضرایب کانتورلت تصویر را تغییر می‌دهد. تصویر مشکوک به حوزه کانتورلت انتقال داده شده و سپس آماره‌های ضرایب کانتورلت تصویر به عنوان خصوصیات کشف نهان‌کاوی استفاده می‌شوند. قدرمطلق ممان‌های زرنایک و ممان‌های تابع مشخصه‌ی ضرایب زیرباندهای کانتورلت برای تشخیص تصویر نهانه به‌کار می‌رود. قدرمطلق ممان‌های زرنایک برای بررسی میزان تصادفی بودن تصویر مورد تست و ممان‌های تابع مشخصه‌ی ضرایب زیرباندهای کانتورلت برای بررسی میزان تغییرات در هیستوگرام ضرایب زیرباندهای کانتورلت بکار گرفته شده‌است. سپس، این مجموعه خصوصیات به یک SVM غیرخطی با هسته‌ی RBF اعمال شده تا تصویر مشکوک شناسایی گردد. نشان می‌دهیم که عمل درج آماره‌های ضرایب کانتورلت تصویر را تغییر می‌دهد که این نکته می‌تواند به عنوان کلیدی برای شناسایی تصویر نهانه باشد. نتایج شبیه‌سازی تایید می‌کند که خصوصیات معرفی شده نسبت به تغییرات ناشی از عمل درج بسیار حساس هستند. همچنین، نتایج شبیه‌سازی بیانگر برتری روش پیشنهادی بر روش‌های نهان‌کاوی مورد مقایسه در مقابل ۵ روش نهان‌نگاری معروف در حوزه JPG است. بهبود حاصل شده در نتایج عمدتاً به‌دلیل حساسیت بالای ممان‌های زرنایک به نویز درج است که بطور متوسط حدود ۴ درصد بهبود در عمل تشخیص نهانه داریم.

واژه‌های کلیدی: نهان‌کاوی کور، تبدیل کانتورلت، ممان‌های زرنایک، ممان‌های تابع مشخصه، تحلیل‌های آماری.