Improving Image Steganalyser Performance using Second Order SPAM Features Extracting through Contourlet Transform

C Bala Subramanian, J Hemalatha, S P Balakannan and S Geetha

Abstract: ***The major challenge posed by feature based blind steganalysers is the scheming of useful image features, which offers true existence of the stego noise rather than the natural noise in the images. Despite hundreds of features being applied in the real time implementation, only low detection accuracy could be achieved. Hence, this paper proposes a new model for detecting the stego image coupled with an examination of the task by applying a two-step process. (a) Extraction of the second order SPAM (Subtractive Pixel Adjacency Matrix) as features and the second order SPAM features of coefficients and co-occurrence matrices of sub band images from the contourlet transform. (b) Implementation of the system, based on an efficient classifier, Support Vector Machine which is capable of providing the higher detection rate than the existing classifers. Full- fledged experimentation with huge database of clean and steganogram images produced from seven steganographic schemes with varying embedding rates, and using five steganalysers were carried out in this study. The study shows that the proposed paradigm enhances the detection accuracy rate substantially and validates its efficiency with its better performance even at low embedding rates.***

Keywords **: contourlet transform, steganalyser, steganographic, stego noise.**

I. INTRODUCTION

Steganography is a key concept in digital era which is employed in preserving or hiding the information in a secret manner. Thus, it finds due place in several sensitive and confidential set-ups like defense, confidential communication, media database systems, secret data storing and etc. Yet, as is the case, this steganography has been in the practice for several years since its inception faces the other side of the ethics. This practice has been misappropriated among the terrorists and other illegal exchange of information and databases. According to latest reports, there has been large scale of these unethical and illegal exploitation of steganography. This makes a strong need to protect and safeguard this system by tracking the tools techniques, coding messages, digital medium and other means which help such activities.

In this regard, steganalysis facilitates in detecting the authenticity of an image, i.e. to ascertain whether it possesses hidden information or not. Basically, steganagraphy is able to detect the existence of steganography within the digitally created files. This paper aims at demonstrating how the presence of stego image in select JPEG images can be made and genuineness can be derived.

Steganalysis is viewed and used as a defensive tool to control the use of steganography and promotes the detective measures in segregating the stego shades from the genuine objects within an image. The approach is to examine the level of security with which the steganography technique is provided by invoking relevant quality assessment criteria, simultaneously preventing the defaulters from misappropriating the steganography. Before comprehending more about this, some of the basic features related to the embedding algorithms and the payload can yield the importance of steganalyzer tool. Such an attempt is easily possible with two essential steps such as Feature extraction and, Classification.

i. Feature Extraction- This does the act of extracting every information related to the presence of any message hiding tool. In addition, this facilitates a feature vector.
ii. Classification- In this approach, the feature vector is employed as an input for training the algorithm, chosen from the host of the machine learning algorithms. The implemented algorithm can identify the genuineness of the input digital file so as to spell whether the image is a stego file or clean file.

Basically, when messages are hidden upon images, it is prone to damage the image properties resulting with minute degradations or unforeseen features in the stego image. The current paper deals with steganalysis framework by basing the information in hiding manner, which is treated as an integral part of the steganographic technique. It is shown that such an attempt ends up with collapsing the clean features of the images, able to cover up the digital objects in a manner that more information could be hidden upon the edges or contours.

Revised Manuscript Received on December 16, 2019.
***** Correspondence Author
C Bala Subramanian*, Department of Information Technology, Kalasalingam Academy of Research and Education, Virudhunagar Dt., Tamil Nadu. India. Email: baluece@gmail.com
J Hemalatha, Department of Computer Science and Engineering, Srividya College of Engineering and Technology, Virudhunagar Dt, Tamil Nadu. India. Email: jhemalathakumar@gmail.com
S P Balakannan, Department of Information Technology, Kalasalingam Academy of Research and Education, Virudhunagar Dt., Tamil Nadu. India. Email: balakannansp@gmail.com
S Geetha, School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu. India. Email: geethabaalan@gmail.com

Ultimately, less information finds place in the soft regions of the images.

As a known fact, there are additive categories of data hiding techniques. Based on this fact, a model is implemented on steganographic secret message into the image in the form of additive noise model, preferably in the spatial domain or in the transform domain. For the sake of extended analysis, consideration on parallel non-additive embedding methods is affected. Substitutive embedding takes upon the measure to additively join the difference in pixel existing in stego-image (*S)* and the cover image (*C*), thereby forming $S = C + (S - C)$, yet in an image-dependent way. In order to trace or detect the stego shades, the original cover image can be restored in a straight manner or the suspected stegoimage can be denoised in an indirect manner.

This paper is organized in the following structure: Section 2 gives the introduction and the related work. Section 3 makes a detailed presentation on the proposed steganalysis, while the data sources taken for the study and the corresponding results are discussed in Section 4. Section 5 contains conclusive remarks about this study and proposes scope for future work.

II. RELATED WORK

In this section, an analysis of various feature extraction techniques used by steganalyzers in detail is provided. The literature survey is focused mainly on the statistical features derived from several domains classified and employed for this purpose. Thus, the feature extraction techniques come under three categories, viz. feature extraction in the spatial domain, feature extraction in the transform domain and feature extraction in the generic domain.

Avcibas et al. [1] attempted in observing the features related to the lower order bit plane and made an estimation of the resemblance calculations occurred between the images. From their observation they noticed the change in the patterns of the neighbor planes when the images underwent message embedding.

Gul and Kurugollu et al. [8] made an attempt by proposing steganalysis method based on the Singular Value Decomposition (SVD). In this method, a model has been devised in which the SVD transform is utilized for locating the linear dependency of the rows and the columns of image between the adjacent pixels. As a result, in tune with the content independent process, mining of much of the recent features has been affected for achieving global steganalysis.

In the later years, Yu et al. [21] considered spatial features to be in the form of contrast residuals, by designing the diverse filters residuals out of the picked out blocks. Fridrich and Kodovsky [6] came out with a rich model by adopting the sources of thousands of similar and varied features out of the noise component. These rich features were got hold by adopting linear and non-linear high pass filter much above the quantized noise residuals. The logical impact of the image analysis is that there has been a strong dependence between adjoining pixels. In a way, the dependency is exemplified to sturdy way due to the impact of the co-occurrence matrix and Markov transition probability matrix features. There has been a soaring distortion of these features as a result of stochastic amendment of the clean image data. The calculation of probability distribution among the nearest pixels and exclusive emulation of the sharing uniqueness of the data are carried out by Co-occurrence matrix.

Chen et al. [3] proposed a method involving the sensing of stego images by adopting the definitions of empirical matrix in addition to co-occurrence matrix. In similar attempt, the stego detection algorithm related to the spatial domain based on co-occurrence matrix was preferred by

Fridrich et al. [5] and Xuan et al. [20] Wang et al. [18,19] and the stego image classification by Zhang et al. [22]. A wavelet dependency of feature extraction process was visualized by Gireesh Kumar et al. [7]. In this process, there has been a transformation of color image into wavelet decomposition depending upon separable quadrature mirror filter. SVM has been adopted as a classifier for classification of the stego images as there has been a consideration of RGB channels from the initial three probability density function moments as classified features. Mining of two sets of features under the spatial and the DCT domains was carried out by Lie and Lin [14]. In this study, the features considered are Gradient energy under spatial domain and statistical variance of the Laplacian parameters under DCT domain. Utilization of gradient energy has been due to validate the distinction arrived for gray levels in addition to the nearest pixels. Similarly, the purpose of utilizing the statistical Laplacian parameters has been is for evaluating the distinction of dissemination of spectral coefficients.

The justification of considering these proposals lies on the fact that there would be a disclose of the stego traces indication out of these features, more than the basic statistical data or information. At one level, in principle, Steganalysis has been a daunting challenge in making distinction when the image is distorted to identity the stego image and ordinary image. These discussions evolve the existence of spatial domain, transform domain, dimension of the feature set, classifier algorithms, kinds of embedding algorithms and models of classification. Beyond all these factors, only the insertion of the denoising method proved to be an effective technique in extracting the ideal and genuine stego images. Much to the achievement, this denoising approach spells out the features allied with sensitive ideals thereby advancing their performance level. This performance achievement prompted the authors of this paper to design such a model in order to prove its worth and efficiency.

III. DESIGN OF THE PROPOSED STEGANALYSER

A. Working Model of Contourlet

In this research study, the second order SPAM features of coefficients and co-occurrence matrices of sub-band images were extracted from the

contourlet domain. Contourlet transformation is basically defined as a transformation of multi-scale and multi-direction basis having the Laplacian pyramid and directional filter bank. Of these two, multi-direction decomposition is derived from the directional filter bank while the multi-scale decomposition is gathered out of the Laplacian pyramid.

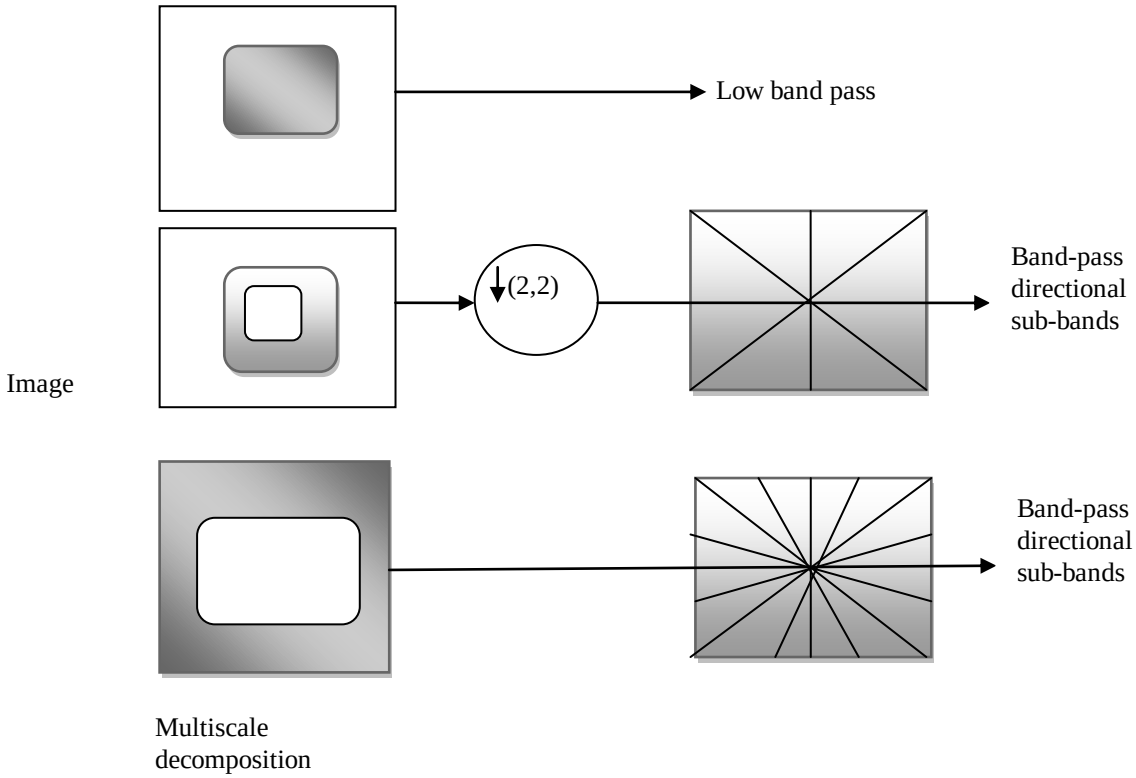

Fig.1 The Contourlet Filter bank

The purpose of employing the Laplacian pyramid is to capture the discontinuity points and to alter the directional filter bank so as to link with the linear structures. Laplacian pyramid was capable of yielding a down sampled low pass version of the actual image as well as the target image. This happened at each level of the process. It is to be noted that of all the three kinds of image, the targeted image has been distinctive from the other two images, such as original image and the predicted image. However, the final output had been a band pass image.

There are two serial building blocks in the decomposition of directional filter bank, viz. i) A two channel quincunx filter bank with fan filters by which a two- dimensional spectrum is portioned into two different directions such as horizontal and vertical and, ii) A shearing operator through which reordering of image samples is achieved. To be concise, contourlet filter bank can be termed as a combination of Laplacian pyramid and the directional bank.

The single level contourlet filter bank is illustrated in Figure 1. From the figure, it can be observed that Laplacian pyramid passes out the band pass images through a directional filter bank. This proves the fact that the directional information can be iterated on the coarse image. To be more clear, such combination is viewed as double iterated filter bank structure as it facilitates the decomposition of an image into directional sub bands at multiple scale.

B. Choice of SPAM Features

Pevny et al. [13] proposed the Subtractive Pixel Adjacency Matrix features by which the independence of the stego noise signal can be developed in a perfect manner. The method involves representation of the difference among the neighbor pixels in the natural images, thereby determining the deviations among the pixel. The model envisages the fact that the deviations are due to natural image pixels encountering steganographic embedding. This particular feature tends to become a filter because it is responsible for suppressing the content of the image and exposure of the stego noise.

a. Extracting the SPAM features

Quite practically, histogram pairs, triplets or set of neighboring pixels define the model for higher order dependences among the image pixels. Yet, in the case of steganalysis, direct collection of features from the histograms becomes very difficult. This is because there are certain unfeasible factors related to this histograms, as mentioned hereunder.

i. There is a strong possibility of exponential growth of the histogram bin numbers e^x, in accordance with the pixel numbers. Further, there is a possibility for the occurrence of the dimensionality problem for the histogram pixel

pairs, which is applicable for an 8 bit grayscale image too.

ii. In certain cases, adjacent pixels appear as completely black or white making the the probability of pixel occurrence to be very low. This constraint makes the estimation of this sort of bins as a noisy affair.

In contrast, to overcome these constraints, the second order markov chain SPAM features were extracted as features. These features enable the process of obtaining higher order dependence among the selected pixels of the image. With regard to a markov chain SPAM feature, it can be observed that there is an increase of SNR by calculating the residuals of neighbor pixels. It is on this Markov chain that modeling of the dependence between neighboring pixels of the filtered image takes place. In case of a feature –based steganalyzer, the sample transition probability matrix assumes the role of a vector feature. For such arrangements, superscript symbols $(\rightarrow, \leftarrow, \uparrow, \downarrow, \nearrow, \swarrow, \searrow, \nwarrow)$ are engaged to denote the array symbols when the directions of the calculation are illustrated.

The horizontal directions are left with the second order Markov chain calculations which by default become the choice for calculating other direction as well.

1. Calculate a difference array^{D} for left-right horizontal direction.

$$\overrightarrow{\mathrm{Diff}}_{i,j} = I_{i,j} - I_{i,j+1} \quad (1)$$

where, I is an input image $i \in \{1,2,3,\dots m\}, j \in \{1,2,3,\dots n\}$

2. Calculate a first – order markov chain SPAM features F_1 order along a left- right horizontal direction.

$$\overrightarrow{M}_{u1,v1} = \Pr(\overrightarrow{\mathrm{Diff}}_{i,j+1} = u1 | \overrightarrow{\mathrm{Diff}}_{i,j} = v1) \quad (2)$$

where, $u1, v1 \in \{-Td, \dots Td\}$ and Td is the range of differences.
If $\Pr(\overrightarrow{\mathrm{Diff}}_{i,j} = v1) = 0$, then $\overrightarrow{M}_{u1,v1} = \Pr(\overrightarrow{\mathrm{Diff}}_{i,j+1} = u1 | \overrightarrow{\mathrm{Diff}}_{i,j} = v1) = 0$

3. By using a second order markov process, second order markov SPAM features are calculated as follows

$$\overrightarrow{M}_{u,v,a} = \Pr(\overrightarrow{\mathrm{Diff}}_{i,j+2} = u1 | \overrightarrow{\mathrm{Diff}}_{i,j+1} = v1, \overrightarrow{\mathrm{Diff}}_{i,j} = a1) \quad (3)$$

where, $u1, v1, a1 \in \{-Td, \dots Td\}$ .If $\Pr(\overrightarrow{\mathrm{Diff}}_{i,j+1} = v1, \overrightarrow{\mathrm{Diff}}_{i,j} = a1) = 0$ then $\overrightarrow{M}_{u1,v1,a1} = \Pr(\overrightarrow{\mathrm{Diff}}_{i,j+2} = u | \overrightarrow{\mathrm{Diff}}_{i,j+1} = v, \overrightarrow{\mathrm{Diff}}_{i,j} = a) = 0$

The calculation is effected on the assumption that the statistics of a natural image statistics to be symmetric in nature. This assumption makes average separation of the features by the horizontal and vertical matrices. As a result, there is a decrease of feature dimensionality as given below:

$$F_{1,2,3,\dots k} = \frac{[\overrightarrow{M} + \overleftarrow{M} + M^{\downarrow} + M^{\uparrow}]}{4} \quad (4)$$

$$F_{k+1,\dots,2k} = \frac{[M^{\nearrow} + M^{\swarrow} + M^{\searrow} + M^{\nwarrow}]}{4} \quad (5)$$

where, $k = (2Td+1)^2$ for the first order features and $k = (2Td+1)^3$ for the second order features. In addition, reasonably good results occurred with pixel differences of second order SPAM features (Tomá˘s Pevný 2010) with range of $Td = \{-3, \dots, 3\}$. This leads to the choice of $Td = \{-3, \dots, 3\}$ in the second order Markov-chain SPAM features. As a final step, 686 dimensional features were gathered out of an original image and equal amount of features, 686, were collected from the third level coefficients of the contourlet transformation. In all, 1372 dimensional features were extracted.

C. Choice of the Classifier

SVM is a well-known method coming under supervised learning approach, which has a set of training image pairs (x_i, y_i) where $x_i \epsilon R^n$, $y_i \epsilon \{-1,1\}$ where i=1,2…m, while $-1 \epsilon clean, +1 \epsilon stego$ are the derived labels. SVM is utilized for mapping the training vector x_i into higher dimensional.

4. Experimental Results and discussions

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

The primary goal of this experimental study is to analyze the performance discrimination in any steganalytic feature once it was subjected to contourlet transform. The secondary goal is to illustrate the performance classification of the proposed steganalyzer extracted from the charted test image set. The impacts of embedding rate and the effectiveness of the steganalyzer was also analyzed in detail.

A. Preparation of test Images and Schemes

By taking these primary and secondary aspects and other factors into consideration, six popular steganographic methods were selected. This choice was based on LSB embedding and spread spectrum principles. On the other hand, the seventh scheme was based on wavelet domain with a view of validating the capability of the system to encounter any unforeseen stego scheme in the system. Similarly, the eighth scheme was based on “Yet Another Steganography Scheme for JPEG steganography that resists blind steganalysis”. All these systems are ideally suited for experimentation purpose as they possess every diverse data hiding scheme with them. Nevertheless, schemes 7 and 8 have not been applied in training the system with stego patterns. The six schemes employed in this study are classified as under:

scheme **#1** :Digimarc [16]
scheme **#2** : PGS [13]
scheme **#3** : Cox et al.’s [4]
scheme **#4** : S-Tools [2]
scheme **#5** :Steganos [17]
scheme **#6** :JSteg [12]

These are further categorized as:
(1) steganography (#4, #5, #6) or watermarking (#1, #2, #3) purpose;
(2) spatial (#2, #4, #5), or transform (#1, #3, #6) domain operation. Further testing and verification of the effectiveness of the selected features selected were carried out by employing an extra scheme based on thewavelet domain:
(3) scheme **#7**: Kim et al.’smethod [11], scheme #8: Solanki et al.’s YASS method [10].

It has been found that if the number of embedded secret

messages tend to be high, then there is a possibility of patterning the dissimilarity between a cover image and its stego version. Thus, when the detecting capability of a chosen steganalytic classifier is to be done, the wise choice could be the steganography scheme under "payload capacity" (i.e. ratio of number of embedded bits to the number of pixels in an image).

The performance of the proposed method was tested and verified by using a cover image dataset consisting of 300 images with each image having the dimension of 256 × 256. Further, there is an 8-bit gray-level photographic image in each image in the dataset, in addition to the standard test images such as Baboon, Lena, and also images from [9]. The cover images are filled with a whole range of scenes with natural light / night of outdoor/indoor backdrop. The images contained trees, flowers, landscapes, and animals, portraits, e.g., kitchen tools, architectures, ornaments, signs, cars, and neon light etc. As mentioned previously, seven schemes were utilized in this study at varied embedding rates. Thus, the database is filled with the stego versions of these images.

The image processing techniques like JPEG compression (at several quality factors), image sharpening, low-pass filtering, were considerably employed to arrive at a set of separate images. It was observed that a fair and reliable estimation and valuation from a generation procedure could be possible only when the database images are evenly contributed from original or stego. The same is the case with processed images or non-processed images done by way of varied embedding schemes. For this study, by applying the payload capacity techniques, three different ERs were put into trial for each scheme to generate the database. They are (#1) 5%, (#2) 10%, (#3) 20% of the maximum payload capacity. In this context, it is to be remembered that there was a capacity of 300+*(*300×3×8*)* = 7500 (no. of clean cover images)+((no.of images)×(no. of varying payload sizes+1 for clean image set) × (no. of schemes evaluated))images in the whole database.

B. Pre-processing of the Image File

The collection of corresponding co-occurrence matrix of sub band image co-efficients was achieved by applying contourlet transform for the given image signal.

C. Feature Extraction

Feature extraction process involves the calculation of the feature vectors and the respective contourlet coefficients from the cover/stego image. Similarly, the second order SPAM features were calculated from the test images and third level coefficients of contourlet coefficients. The calculation of features was made in accordance with the prescribed procedure marked for the working model of contourlet transform.

D. Classification

Both the clean and stego images of the training dataset enabled the extraction of the feature vectors. The image dataset was trained by serving the resultant feature vectors SVM classifier with Gaussian kernel. Then, the input in the form of the testing image is fed into the SVM classifier to identify whether the input image is stego or clean. The process algorithm is as follows.

$truestego^{+} = \{all\ the\ stego\ images\},$
$truestego^{-} = \{all\ the\ clean\ images\},$
$estimatedstego^{+} = \{all\ the\ images\ rated\ as\ stego\},$
$estimatedstego^{-} = \{all\ the\ images\ rated\ as\ celan\}.$

We identified the subsequent metrics to evaluate the proposed steganalyser performance.

$$True\ Positive\ Rate\ (TPR) = \frac{estimatedstego^{+}}{estimatedstego^{+} + truestego^{+}} \quad (6)$$

$$False\ Positive\ Rate\ (FPR) = \frac{estimatedstego^{-}}{estimatedstego^{-} + truestego^{-}} \quad (7)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

$$Precision = \frac{estimatedstego^{+}}{estimatedstego^{+} + estimated\ stego^{-}} \quad (9)$$

$$Recall = TPR = \frac{estimatedstego^{+}}{estimatedstego^{+} + truestego^{+}} \quad (10)$$

$$F - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (11)$$

V. RESULTS AND DISCUSSION

Table 1 and 2 illustrate the error rates derived from the study. The recital of the proposed second order SPAM features, extracted from Contourlet transform using SVM classifier, are listed in Table 1. Also illustrated are the extracted features from contourlet transformation and non-contourlet transformation. The results obviously prove that despite the second order SPAM features providing a strong set of features related to the classified stego images, the features extracted out of contourlet provides the desired improvement in image detection. To be clearer, the topmost 93.74% accuracy was possible for Digimarc, with the proposed contourlet based approach followed by 92.68% spread spectrum achieved in Solanki et al. When the schemes of Jsteg, Soalnki et al. were analyzed, there has been an achievement of 95.51%, 95.71% and 94.90% PD by PGS. Further, this accounts to less efficiency in defending the proposed study. The proposed scheme has an edge over the false alarm rates of the schemes proposed by Steganos, and Cox et al. The proposed scheme achieved the overall performance rate of 93.74% which is considerably remarkable. Thus, the proposed scheme of steganalysis proves to be a promising method for the universal application.

The recitals at various message hiding rates of features extracted from contourlet and without from contourlet transform are listed in Table 2.. The experimental results gave the following observations:

a) It is clear that various transformation schemes, DCT, DFT, curvelet, contoulet, ridgelet are there in image processing. These schemes are endowed with certain extracted features from contourlet

transformation, which is ideally suited for steganalysis. The contourlet transformation enables the exposure of the stego noise in an image.

b) Experimentation was carried out on the basis of several unrestricted embedding schemes, which proves that steganalysis is carried out without any binding.

c) The experiment was carried out on voluminous databases, containing clear and stego images, which were generated by eight schemes under steganography. Four embedding payloads were also employed in the schemes

Table- I: Comparison of classification results of Second order SPAM features extracted between with contourlet transform and without contourlet transform

Embedding Methods	Second order SPAM features extracted from the contourlet transform and using SVM classifier											
	Accuracy		TP Rate		FP Rate		Precision		Recall		F-Measure	
	WOC	WC	WOC	WC	WOC	WC	WOC	WC	WOC	WC	WOC	WC
Digimarc	89.27	93.74	93.12	93.75	27.27	28.57	93.62	93.75	93.12	93.75	93.36	93.75
PGS	91.07	92.31	94.85	94.90	33.33	21.05	94.85	95.86	94.85	94.90	94.85	95.37
Cox *et al.*'s	90.08	91.30	93.94	94.85	38.39	33.23	93.66	95.88	93.94	94.85	93.79	95.36
S-Tools	90.49	91.47	92.59	94.14	30.00	23.53	93.75	95.74	92.59	94.14	93.16	94.93
Steganos	85.48	87.46	91.13	91.61	39.97	38.73	91.12	93.73	91.13	91.61	91.12	92.65
JSteg	90.49	91.78	93.32	95.51	28.57	29.41	95.65	94.85	93.32	95.51	94.47	95.17
Kim *et al.*	87.66	88.31	90.34	92.05	27.71	24.32	94.92	93.72	90.34	92.05	92.57	92.87
Solanki et al.	90.00	92.68	94.19	95.71	35.71	32.66	94.19	96.08	94.19	95.71	94.19	95.89

WOC – without contourlet transform

WC – with contourlet transform

Table- II: Classification rate for investigation sets at different embedding rates by the proposed method

Embedding Methods	Features extracted from contourlet transform	Embedding Methods	Features extracted from contourlet transform
Digimarc		**Steganos**	
5% of Max payload	89.2	*5% of Max payload*	85.42
10% of Max payload	90.2	*10% of Max payload*	85.90
20% of Max payload	91.3	*20% of Max payload*	86.99
40% of Max payload	93.74	*40% of Max payload*	87.46
PGS		**Jsteg**	
5% of Max payload	90.20	*5% of Max payload*	86.68
10% of Max payload	92.12	*10% of Max payload*	88.63
20% of Max payload	92.20	*20% of Max payload*	89.63
40% of Max payload	92.31	*40% of Max payload*	91.78
Cox *et al.*'s		**Kim *et al.***	
5% of Max payload	89.36	*5% of Max payload*	82.32
10% of Max payload	89.99	*10% of Max payload*	84.3
20% of Max payload	91.00	*20% of Max payload*	85.3
40% of Max payload	91.30	*40% of Max payload*	88.31
S-Tools		**Solanki et al.**	
5% of Max payload	90.2	*5% of Max payload*	83.9
10% of Max payload	90.3	*10% of Max payload*	84.10
20% of Max payload	90.25	*20% of Max payload*	86.2
40% of Max payload	91.47	*40% of Max payload*	92.68

thereby making the method ideal for real time application.

d) It is a known fact that SVM comes under standard classification engine in a pattern recognition problem. Similarly, in the proposed method SVM aided in a great manner by providing the necessary classification rate.

VI. CONCLUSION

This paper dealt with the coinage of a steganalysis system which utilized the contourlet transform in extracting the features. So far, there have been many works which have come out with various image procession transformations yielding better results. To be

more universal, innovative, cost-efficient, feasible and reliable, in this paper, the contourlet transform has been proposed and tried. It is also
known that features can be extracted directly from an image by applying the second order SPAM. By extending the approach, this paper attempted to extract SPAM features of coefficients andco-occurrence matrices of sub band images. This is to prove the improved efficiency and better performance of the application of Contourlet transform in image detection for stego noise. Thus, this study has validated the better performance rate in detection than the existing classifiers.

REFERENCES

1. Avcibas, I., Kharrazi,M., Memon, N., Sankur, B.: Image steganalysis with binary similarity measures. EURASIP J. Appl. Signal Process. 17, 2749–2757 (2005)
2. Gul, G., Kurugollu, F.: SVD-based universal spatial image steganalysis. IEEE Trans. Inf. Forensics Secur. 5(2), 349–353 (2010).
3. Yu, J., Li, F., Cheng, H., Zhang, X.: Spatial steganalysis using contrast of residuals. IEEE Signal Process. Lett. (2016). https:// doi.org/10.1109/LSP.2016.2575100.
4. Fridrich, J., Kodovsky, J.: Rich models for steganalysis of digital images. IEEE Trans. Inf. Forensics Secur. 7(3), 868–882 (2012).
5. Chen, X., Wang, Y., Tan, T., Guo, L.: Blind image steganalysis based on statistical analysis of empirical matrix. In: Proceedings of the 18th International Conference on Pattern Recognition (ICPR), Hong Kong, China, pp. 11–7–10 (2006).
6. Fridrich, J., Kodovsky, J., Holub, V., Goljan, M.: Steganalysis of content-adaptive steganography in spatial domain. In: Proceedings of the 13th International Workshop on Information Hidings, Prague, Czech Republic. LNCS, vol. 6958, pp. 102–112 (2011).
7. Xuan, G., Shi, Y.Q., Huang, C., Fu, D., Zhu, X., Chai, P.: Steganalysis using high-dimensional features derived from co-occurrence matrix and class-wise non principal components analysis (CNPCA). In: Proceedings of the 5th International workshop on Digital Watermarking, vol. 4283, pp. 49–60 (2006).
8. Wang, P., Wei, Z., Xiao, L.: Fast projections of spatial rich model feature for digital image steganalysis. Soft Comput. (2016a). https://doi.org/10.1007/s00500-015-2011-z
9. Wang, P., Wei, Z., Xiao, L.: Pure spatial rich model features for digital image steganalysis. Multimed. Tools Appl. 75(5), 2897–2912 (2016b).
10. Zhang, Y., Luo, X., Yang, C., Liu, F.: Joint JPEG compression and detection-resistant performance enhancement for adaptive steganography using feature regions selection. Multimed. Tools Appl. 76(3), 3649–3668 (2017).
11. Gireesh Kumar, T., Jithin, R., Shankar, D.D.: Feature based steganalysis using wavelet decomposition and magnitude statistics. In: Proceedings of International Conference on Advances in Computer Engineering, pp. 298–300 (2010).
12. Lie,W.-N., Lin, G.-S.: A feature-based classification technique for blind image steganalysis. IEEE Trans. IFS (2005). https://doi.org/10.1109/TMM.2005.858377.
13. Pevny, T., Bas, P., Fridrich, J.: Steganalysis by subtractive pixel adjacency matrix. IEEE Trans. Inf. Forensics Secur. (2010). https://doi.org/10.1109/TIFS.2010.2045842.
14. PictureMarc, Embed Watermark, v 1.00.45. Digimarc Corp
15. Kutterand, M., Jordan, F.: JK-PGS (Pretty Good Signature). Signal Processing Laboratory, Swiss Federal Institute of Technology (EPFL), Lausanne. http://ltswww.epfl.ch/ kutter/watermarking/JK PGS.html (1998).
16. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. 6(12), 1673–1687 (1997).
17. Brown, A.: S-Tools Version 4.0. http://members.tripod.com/ steganography/stego/s-tools4.html
18. Steganos Security Suite. http://www.steganos.com/english/steganos/download.htm
19. Korejwa, J.: Shell 2.0. http://www.tiac.net/users/korejwa/steg.htm
20. Kim, Y.S., Kwon, O.H., Park, R.H.: Wavelet based watermarking method for digital images using the human visual system. Electron. Lett. 35(6), 466–468 (1999)
21. Kaushal, S., Anindya, S., Manjunath, B.S.: YASS: yet another steganographic scheme that resists blind steganalysis. In: 9th International Workshop on Information Hiding, Saint Malo, Brittany, France, June (2007)
22. Images.http://www.cl.cam.ac.uk/~fapp2/watermarking/ benchmark/image_database.html

AUTHORS PROFILE

C Bala Subramanian received his Bachelor of Engineering in Electronics and Communication Engineering from Anna University, Chennai by 2006. He received his master of Engineering in Applied Electronics from Anna University, Chennai by 2008. He is pursuing Ph.D degree Information Technology with Kalasalingam University in He is working as an Assistant Professor in the Department of Computer Science Engineering, Kalasalingam Academy of Research and Education. His areas of interest are Image and Signal Processing, Sensor Networks, Adhoc Networks.

J Hemalatha received the B.E and ME degree in Computer Science and Engineering under Anna University Chennai in 2007 and 2013. She is completed Ph.D. degree in Information and Communication Engineering with Anna University, Chennai in 2019. She is currently working as an Associate Professor in the Department of Computer Science and Engineering at Srividya College of Engineering and Technology, Virudhunagar, India. She has published more papers in reputed International Conferences and Journals. Also is an author of the book chapter: Combating Security Breaches and Criminal Activity in the Digital Sphere, A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series by IGI Global. Her research interests include Digital steganography, Steganalysis, Machine Learning and Image Processing

S P Balakannan received his Ph.D. degree from the Department of Electronics and Information Engineering at Chonbuk National University, South Korea (2010). He has received his master degree (5 years integrated) from the Department of Computer Science and Engineering, Bharathiar University, India, in the year 2003. He has worked as a Project Assistant in Indian Institute of Technology (IIT), Kharagpur, India from 2003 to 2006. Currently, he is working as Associate Professor in the Department of Information Technology, Kalasalingam Academy of Research and Education, Tamilnadu, India. His areas of interest include Wireless Network, Network Coding, Cloud & Green Computing, Cryptography, and Mobile Communication.

Dr. S.Geetha received the B.E., and M.E., degrees in Computer Science and Engineering in 2000 and 2004, respectively, from the Madurai Kamaraj University and Anna University of Chennai, India. She obtained her Ph.D. Degree from Anna University in 2011. In July 2004, she joined the Department of Information Technologyat Thiagarajar College of Engineering, Madurai, India. Before joining TCE she was in the Department of Computer Science and Engineering at the Karunya University, Coimbatore, India. She has published more than 40 papers in reputed IEEE International Conferences and refereed Journals. She joins the review committee for IEEE Transactions on Information Forensics and Security and IEEE Transactions on Image Processing. She was an editor for the ICCIIS 2007–1st Indian Conference on Computational Intelligence and Information Security. She was an editor for the Combating Security Breaches and Criminal Activity in the Digital Sphere, A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series by IGI Global. Her research interests include multimedia security, intrusion detection systems, machine learning paradigms and information forensics. She is a recipient of University Rank and Academic Topper Award in B.E. and M.E. in 2000 and 2004 respectively.