International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 5, Aug - Sep 2016; 15-24

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

STEGANALYSIS ON IMAGES BASED ON THE CLASSIFICATION OF IMAGE FEATURE SETS USING SVM CLASSIFIER

S. DEEPA[1] & R. UMARANI[2]

[1]Assistant Professor, Department of Computer Science, Government Arts College, Dharmapuri, Tamil Nadu, India

[2]Associate Professor, Department of Computer Science, Sri Sarada College for Women, Salem, Tamil Nadu, India

ABSTRACT

The two popular schemes used for image steganography are spatial domain embedding and transform domain embedding. Most of the steganographic techniques either use spatial domain or transform domain to embed the secret message. This work is about attack on Modern spatial domain image steganography. The previous work evaluates the performance of five state of the art content-adaptive steganographic techniques. Since WOW is believed to be a strong steganographic method which will with stand against attacks, this work, does steganalysis on WOW stego images. This paper attempts to detect the stego images created by WOW algorithm by using Chen Feature set, Subtractive Pixel Adjacency Mode (SPAM) Feature set and Ccpev Feature set. It uses a SVM based classifier to detect the stego images.

KEYWORDS: Steganography**,** Steganalysis, SVM-Ccpev, SVM-Chen, SVM Classifier, SVM-SPAM

INTRODUCTION

Steganography is a Two-Step Process:

Step 1) Creating a stego image which is a combination of message and carrier

Step 2) Extracting the message from the stego image

Variations are in the techniques that are used to generate the stego image using the carrier and the message. There are different categories of methods in spatial domain, (i) LSB steganography, (ii) RGB based steganography, (iii) pixel value differencing steganography, (iv) Mapping based steganography, (v) Palette based steganography, (vi) collage based steganography, (vii) Spread spectrum steganography, (viii) Code based steganography, and (ix) others.

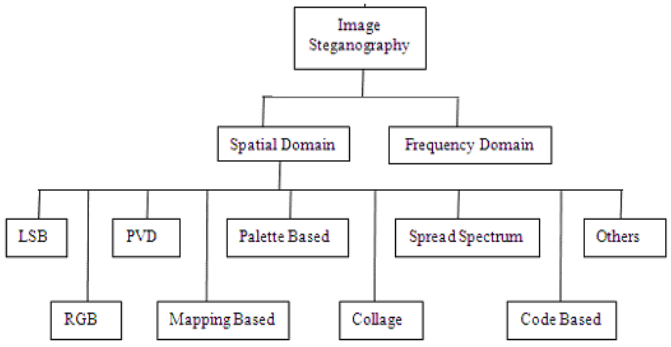

Figure 1: Spatial Domain Image Steganography Techniques

STEGANALYSIS

Steganalysis is the practice of attacking steganography methods for the detection, extraction, destruction and manipulation of the hidden data in a stego object.

Detection is enough to foil the very purpose of steganography even if the secret message is not extracted because detecting the existence of hidden data is enough if it needs to be destroyed. Detection is generally carried out by identifying some characteristic feature of images that is altered by the hidden data. A good steganalyst must be aware of the methods and techniques of the steganography tools to efficiently attack.

Classification of attacks based on information available to the attacker:

- Stego only attack: only stego object is available for analysis.
- Known cover attack: both cover and stego are known.
- Known message attack: in some cases message is known and analyzing the stego object pattern for this embedded message may help to attack similar systems.
- Chosen stego attack: steganographic algorithm and stego object are known.
- Chosen message attack: here steganalyst creates some sample stego objects from many steganographic tools for a chosen message and analyses these stego objects with the suspected one and tries to find the algorithm used.
- Known stego attack: cover object and the steganographic tool used are known.

IMPLEMENTATION OF THE SVM BASED STEGO IMAGE DETECTION

SVM Classifier

In machine learning, support vector machines (SVMs) are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked for belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier.

THE PROPOSED SVM NEURAL NETWORK BASED STEGANALYSIS METHODS

Steps of SVM-Chen Classification Method

- Input: WOW Stego Images[1] and Non Stego Images
- Extract Chen-486[2,3], Spam-6864[4] and Ccpev-548[5] Features of Non-Stego Images and Stego Images at Different Bits Per Pixel (0.2 bpp, 0.4 bpp, 0.6 bpp, 0.8 bpp)
- It results in 3 set of features for Non stego Images and 4 set of features with stego images at 4 level of hiding for every feature extraction method
- For SVM-chen classification, use the chen-486 features of the non-stego image (from step 2) and the chen-486 features of stego images at 4 level of hiding
- For k=1 to 10
- Train the SVM neural network with randomly selected 70% of data mentioned in step 4

- classify the remaining 30% of data using the trained SVM network of step 6
- Performance(k)=Estimate the Performance()
- End
- Find average performance from Performance(k)

Steps of SVM-Spam Classification Method

- For SVM-spam classification Method, use spam-686 features in the 4th step of the above mentioned algorithm.

Steps of SVM-Ccpev Classification Method

- For SVM-ccpev classification Method, use ccpev-548 features in the 4th step of the above mentioned algorithm.

The Block Diagram Explaining Overall Model

The following block diagram gives the generalized model of the proposed Steganalysis system.

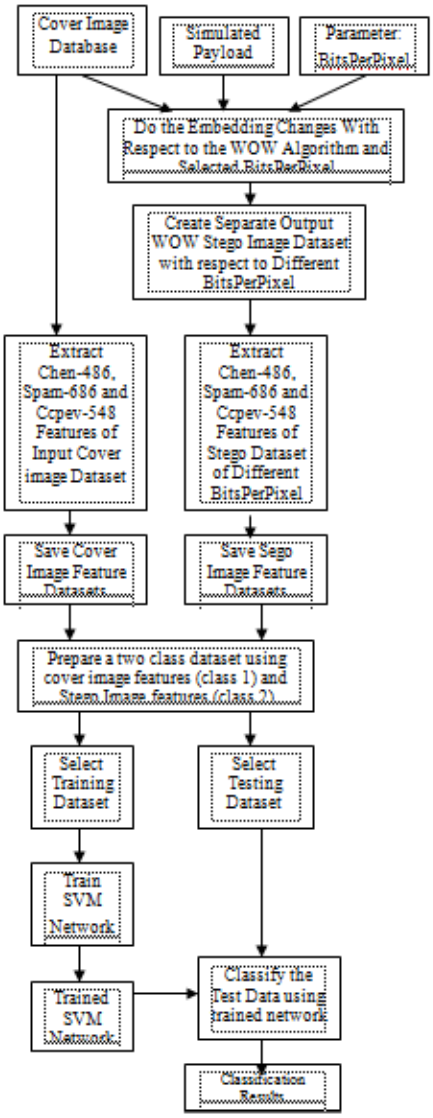

Figure 2: The Proposed Steganalysis system

THE RESULTS OF STEGANALYSIS AND DISCUSSIONS

About the Used Image Database

The Images used for this evaluation were originally taken from the BOWS Image Dataset. BOWS (Break Our Watermarking System) was a Contest organized within the activity of the Watermarking Virtual Laboratory (Wavila) of the European Network of Excellence ECRYPT. In fact, the original dataset contains 10,000 images. But the proposed system uses a subset of cover images from BOWS database that were previously used in another work named "Gibbs Construction in Steganography[6]". This system uses around 500 images to evaluate the performance of the proposed steganalysis model. It uses cover images feature sets extracted using three different feature extraction algorithms and stego images feature sets extracted using three different feature extraction algorithms at 4 different level of hiding such as 0.2 bpp, 0.4 bpp, 0.6 bpp and 0.8bpp.

The Output Result with Wow Steganograpy Algorithm[7] (At 0.04 Bits Per Pixel)

As a general convention, Lenna image has been used to demonstrate the performance of the WOW algorithm at the level of hiding at 0.40 bits per pixel.

Time Taken for Embedding: 2.48 sec, Change Rate: 0.0781, PSNR: 59.2358

Figure 3: The Performance with Respect to Different Bpp for Visual Analysis

TABLE OF RESULTS

The following are the numerical outputs of the performance of the classifier in terms of different metrics.

Table 1: Performance of SVM-Chen (Chen486 Features)

Iteration	Precision	F Score	Sensitivity	Specificity	Accuracy	Error Rate
1	73.81	83.75	96.77	8.33	72.09	27.91
2	78.05	85.26	93.94	10.00	74.42	25.58
3	83.33	84.30	85.29	33.33	74.42	25.58
4	77.50	84.85	93.75	18.18	74.42	25.58
5	82.05	86.37	91.18	22.22	76.74	23.26
6	82.86	80.24	77.78	14.29	67.44	32.56
7	74.29	75.01	75.76	10.00	60.47	39.53
8	76.67	70.18	64.71	22.22	55.81	44.19
9	88.57	85.87	83.33	42.86	76.74	23.26
10	67.50	77.02	89.66	7.14	62.79	37.21
Avg	**78.46**	**81.29**	**85.22**	**18.86**	**69.53**	**30.47**

Table 2: Performance of SVM-Spam (Spam 686 Features)

Iteration	Precision	F Score	Sensitivity	Specificity	Accuracy	Error Rate
1	100.00	100.00	100.00	100.00	100.00	0.00
2	97.14	98.55	100.00	90.00	97.67	2.33
3	97.22	98.59	100.00	88.89	97.67	2.33
4	94.29	97.06	100.00	81.82	95.35	4.65
5	97.22	98.59	100.00	88.89	97.67	2.33
6	100.00	100.00	100.00	100.00	100.00	0.00
7	100.00	100.00	100.00	100.00	100.00	0.00
8	97.22	98.59	100.00	88.89	97.67	2.33
9	97.37	98.67	100.00	85.71	97.67	2.33
10	100.00	100.00	100.00	100.00	100.00	0.00
Avg	**98.05**	**99.01**	**100.00**	**92.42**	**98.37**	**1.63**

Table 3: Performance of SVM-Ccpev (Cpev548 Features)

Iteration	Precision	F Score	Sensitivity	Specificity	Accuracy	Error Rate
1	78.05	87.67	100.00	25.00	79.07	20.93
2	80.49	87.96	96.97	20.00	79.07	20.93
3	85.37	92.11	100.00	33.33	86.05	13.95
4	78.57	88.00	100.00	18.18	79.07	20.93
5	85.00	90.63	97.06	33.33	83.72	16.28
6	87.50	90.84	94.44	28.57	83.72	16.28
7	81.08	84.34	87.88	30.00	74.42	25.58
8	85.71	85.50	85.29	44.44	76.74	23.26
9	92.31	94.70	97.22	57.14	90.70	9.30
10	70.73	81.65	96.55	14.29	69.77	30.23
Avg	**82.48**	**88.34**	**95.54**	**30.43**	**80.23**	**19.77**

Performance of the Classifier or Stego Detection System

The following graph shows the performance of the stego image classifier or stego image detection system in terms of Error Rate. As shown in the figure, the proposed SVM-spam provided excellent performance than other two proposed models.

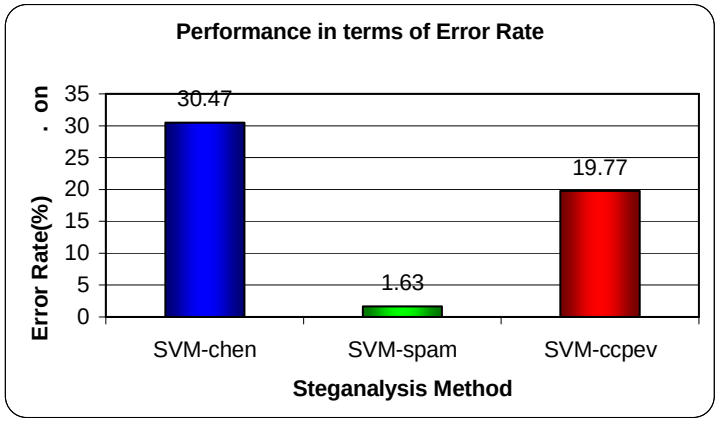

Figure 4: The Performance in Terms of Error Rate

The following graph shows the performance of the stego image detection system in terms of Accuracy. As shown in the figure, the proposed SVM-spam model provided excellent performance than other two proposed models

Figure 5: The Performance in Terms of Accuracy

The following graph shows the performance of the stego image detection system in terms of Sensitivity.

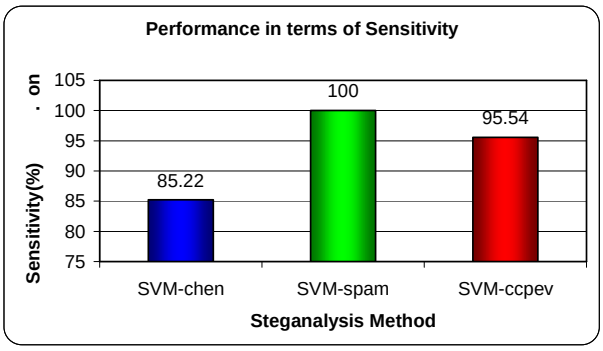

Figure 6: The Performance in Terms of Sensitivity

As shown in the above figure, the proposed SVM-spam model provided excellent performance than other two proposed models. Here high value of sensitivity case of SVM-spam signifies that the system was able to classify all the non-stego images correctly with 100% accuracy.

The following graph shows the performance of the stego image detection system in terms of Specificity. As shown in the figure, the proposed SVM-spam model provided excellent performance than other two proposed models. Here high value of specificity in the case of SVM-spam signifies that the system was able to classify all the-stego images correctly with high accuracy.

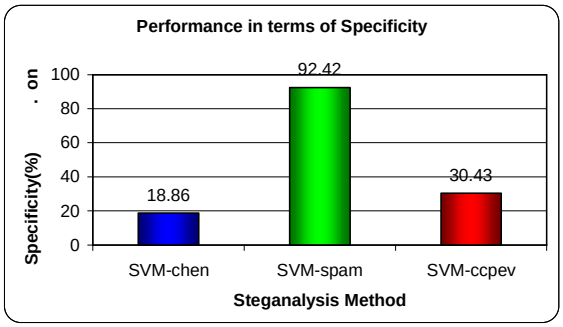

Figure 7: The Performance in Terms of Specificity

The following graph shows the performance of the stego image detection system in terms of F-Score. As shown in the figure, the proposed SVM-spam model provided excellent performance than other two proposed models. Here high value of F-Score in the case of SVM-spam signifies that the system was able to classify all the stego images as well as non-

stego images with high accuracy.

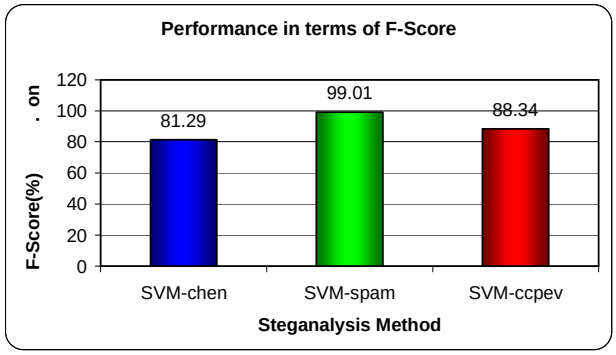

Figure 8: The Performance in Terms of F-Score

The following graph shows the performance of the stego image detection system in terms of Precision. As shown in the figure, the proposed SVM-spam model provided excellent performance than other two proposed models. Here high value of Precision in the case of SVM-spam signifies that the system was able to classify all the stego images with high accuracy.

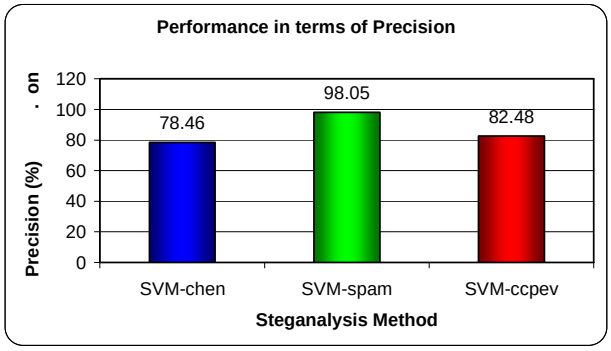

Figure 9: The Performance in Terms of Precision

Comparison of Performance with Previous Methods

In the following table and graph, the results of the compared algorithms (1) Ensemble classifier, (2) FLD classifier, (3) Ridge Regression, (4) LSMR Optimization and (5) LASSO were taken from the paper " Is Ensemble Classifier Needed for Steganalysis in High-Dimensional Feature Spaces?[8]". In that paper, a ensemble classifier, based on Fisher Linear Discriminant base learners, was introduced specifically for steganalysis of digital media, which currently uses high-dimensional feature spaces. Presently it is probably the most used method to design supervised classifier for steganalysis of digital images because of its good detection accuracy and small computational cost. It has been assumed by the community that the classifier implements a non-linear boundary through pooling binary decision of individual classifiers within the ensemble. That previous work challenges this assumption by showing that linear classifier obtained by various regularizations of the FLD can perform equally well as the ensemble. Moreover it demonstrates that using state of the art solvers linear classifiers can be trained more efficiently and offer certain potential advantages over the original ensemble leading to much lower computational complexity than the ensemble classifier.

The following table shows the performance of proposed methods and previous methods in terms of probability of error.

Table 4: Performance in Terms of Probability of Error

Sl. No	Steganalysis Method	Probability of Error
1	Ensemble classifier	0.3196
2	FLD classifier	0.3289
3	Ridge Regression	0.3402
4	LSMR Optimization	0.3267
5	LASSO	0.3694
6	SVM-chen	0.3047
7	SVM-spam	0.0163
8	SVM-ccpev	0.1977

The following graph shows the performance of proposed methods and previous methods in terms of probability of error. As shown in this graph, the SVM-chen method performed almost equal to some of the previous methods, SVM-ccpev performed better than all the previous methods. But the performance of SVM-spam was very good and it provided very lower probability of error.

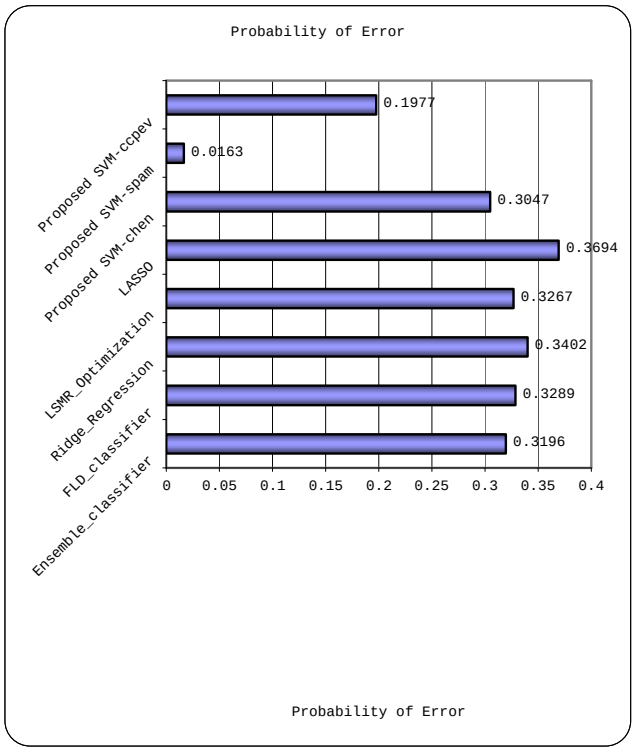

Figure 10: The Performance in Terms of Probability of Error

The improvement in performance in the proposed model is due to three important aspects.

- The use of SVM neural network based classifier
- The use of best extracted features from three state of the art feature extraction algorithms
- The use of Mixed class stego image features of images with different bpp hiding for training the SVM neural network

CONCLUSIONS

This paper successfully implemented a stego data generation framework and generated WOW based stego image datasets at different bpp level of hiding. Further, using the cover images and all the different stego image datasets, it created feature sets of cover images as well as the stego images of different bpp level of hiding. These feature sets were created using three different feature detection algorithms.

The three stego detection methods were named as SVM-chen, SVM span and SVM-sspev with respect to the feature extraction method used in the design. All the three implemented steganalysis methods performed better than the compared previous works. But the performance of SVM-spam was very good and it provided very lower probability of error and outperformed all other compared algorithms with a significant difference in performance.

REFERENCES

1. V. Holub et al (Dec 2012), "Designing steganographic distortion using directional filters", in Proc. IEEE WIFS, (Tenerife, Spain).
2. C. Chen et al (May 2008), “JPEG image steganalysis utilizing both intrablock and interblock correlations”, IEEE ISCAS, International Symposium on Circuits and Systems.
3. Y. Q. Shi et al (July 2006), "A Markov process based approach to effective attacking JPEG steganography," Information Hiding, 8th International Workshop, Springer-Verlag, New York.
4. Tomas Pevny et al (2010), “Steganalysis by Subtractive Pixel Adjacency Matrix”, IEEE Trans. on Info. Forensics and Security.
5. Tomas Pevny et al, “Merging Markov and DCT features for multiclass JPEG steganalysis”, In E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX.
6. T. Filler et al (Dec 2010), “Gibbs Construction in Steganography”, IEEE Transactions on Information Forensics and Security
7. S. Deepa et al (Jan 2016), “An Evaluation on Modern Spatial Domain Steganography Algorithms”, International Journal of Computer Science Engineering and Information Technology Research, Vol 6, Issue 1.
8. Remi Cogranne et al (Nov 2015), “Is Ensemble Classifier Needed for Steganalysis in High-Dimensional Feature Spaces?” IEEE International Workshop on Information Forensics and Security (WIFS), DOI: 10.1109/WIFS.2015.7368597.
9. Database Reference: http://bows2.ec-lille.fr/

AUTHOR'S DETAILS

Deepa S has completed her M.C.A. from Vysya College, affiliated to Periyar University, Salem. She received her M.Phil. Degree from Bharathidasan University, Tiruchirapalli. She is currently working as an Assistant Professor in Computer Science Department, Government Arts College, Dharmapuri and pursuing Ph.D. in Periyar University as part time. Her area of interest is information security, detection and prevention of Steganalysis, user authentication. Her research outputs include 4 papers in international journals and presented 1 paper in National Conference.

Dr. R. Uma Rani has completed her M.C.A. from NIT, Trichy and did her M.Phil. from Mother Teresa University, Kodaikanal. She received her Ph. D. from Periyar University, Salem. She is working as Associate Professor in Department of Computer Science, Sri Sarada College for women, Salem. Her research interest includes Information Security, Data Mining, Fuzzy Logic and Mobile Computing. She has published 121 papers in National and International journals and conferences and received best paper award for "Enhancement of data security through obscurity" by VIT, India and security paper award for "Security through obscurity" by infosecwriters.com. She is co-author of the books - Information Technology in Management, problem solving techniques and grid computing and published e-book on Corel draw tips and techniques. She was the PI for MRP funded by UGC. She acted as chair person and as resource person in National and International conferences. She is active in a variety of professional bodies and also a member in computer society of India, member in board of studies of computer science in Vinayaka Missions University, Salem, and also member in editorial board of various international journals.