Defence Science Journal, Vol. 60, No. 4, July 2010, pp. 412-414

SHORT COMMUNICATION

Payload Estimation in Universal Steganalysis

Amritha P.P* and Anoj Madathil

Amrita Vishwa Vidyapeetham, Ettimadai, Coimbatore-641 105
*E-mail: *pp_amritha@cb.amrita.edu, anojmadathil@gmail.com*

ABSTRACT

Universal Steganalysis can classify images without the knowledge of steganographic algorithms. This steganalysis will blindly classify an image as cover or not, but finding how much payload embedded, is still an open problem. This paper focuses on the above problem. Firstly, they use features from universal steganlysers and apply principal component analysis to improve the false positive rate. The above features are then used to estimate the payload by using support vector regression. The support vector machine classifier capable of assigning stego images to six popular steganographic algorithm after applying Principal Component Analysis: JP Hide & Seek, PVD, LSB flipping, Outguess, *S*-Tool and F5 is trained. This provides significantly more reliable results compared to their previous work on universal steganalysis. The performance is also evaluated by quantitative steganalysis for six steganographic algorithms.

Keywords: Support vector machine, support vector regression, principal component analysis, steganalysis, payload estimation, image classification, universal steganalysis

1. INTRODUCTION

The objective of steganalysis is to detect the presence of hidden message. Steganography is considered broken when the mere presence of the secret message can be established. Unlike the classical model which is based on Kerckhoff principle, universal steganalysis assume that the steganalyst does not know the specification of the steganographic algorithm used. The investigation is not likely to stop when the use of steganography is discovered. The analyst may want to uncover more details about the hidden information such as the number of modification due to steganographic embedding, because the number of embedding change is correlated with message length, one can obtain valuable forensic information about the type of hidden data or the fact that the message is encrypted. To estimate the relative number of embedding change they use payload steganalysis which are generally built from heuristic principles and always rely on full knowledge of embedding algorithm[1,2].

This paper focuses on reducing the false positive rate compared to the work done in universal steganalysis[3] and then payload estimation of the stego image without the detailed knowledge of the embedding mechanism after the classification as stego. One of the methods[4] for this is to use the features from universal steganalysis and model the relationship between the position of stego image features and the change rate using support vector regression. They incorporate principal component analysis (PCA) to their previous work[3] on universal steganalysis to extract features and hence improving the detection accuracy. They used kernelised version of ordinary linear least square regression (OLS) called support vector regression (SVR). This approach to payload steganalysis has a very important advantage. They can design a steganalyser without any knowledge of the embedding algorithm. All that is required is access to a database of images embedded with a range of known payloads. Such images can be generated if the steganalyst has access to the embedding algorithm but not necessarily to its inner workings. There does have to exist a feature set and a universal steganalyser that can reliably detect the embedding, and the accuracy of the resulting payload steganalyser depends on the sensitivity of the feature set to the attacked steganographic scheme.

2. APPROACH

They have obtained a total of 269 features[3] which gave an accuracy of 70 per cent–80 per cent. Some features were degrading the support vector machine (SVM) classifier accuracy, so PCA was used. Out of these 269 features, using PCA, they got 135 features when trained with SVM which resulted in an accuracy of 80 per cent–95 per cent. After the classification with SVM they used SVR for payload estimation[4]. For payload estimation, the basic method for constructing change rate estimators was used by learning the relationship between feature location and the change rate, using regression on some training set of stego features and their corresponding change rates. The change rate is the ratio between the total number of embedding changes and the number of cover elements that can be used for embedding.

Received 15 September 2009, Revised 23 March 2010

2.1 Support Vector Regression

The main idea behind SVR[5] is to map the model space R^d through a possibly nonlinear data-driven mapping $\phi: R^d \mapsto H$ into dimensional vector space H, where a linear regression is performed. The kernels used in this paper are radial basis function (RBF)

$$K(x_i, x_j) = exp(-\gamma || x_i, x_j ||^2), \gamma > 0 \quad (1)$$

and the polynomial kernel $k(x, x') = (\langle x.x' \rangle_{R^d} + 1)^d$.

The optimisation problem solved by SVR attains the following form

$$\min_{w \in H, b \in R} || w ||_H^2 + c \frac{1}{l} \sum_{i=1}^{l} e(w.\phi(x_i) - b, y_i) \quad (2)$$

where C is a parameter describing the trade-off between complexity of the solution and error on the training set. Ideally, the error function e should be determined from the statistical properties of the noise in features.

$$e_e(\hat{y}, y) = \begin{cases} \left| \hat{y} - y \right| - \varepsilon & if \quad \left| \hat{y} - y \right| > \varepsilon \\ 0 & otherwise \end{cases} \quad (3)$$

Smola and Schoelkopf[5] tested error function and used the ε-insensitive loss. They have tested for different values of parameter C, width of the radial basis kernel. The penalisation parameter C, the width of the RBF kernel γ and ε has a significant influence on the ability of the regressor to generalise.

3. EXPERIMENTAL RESULTS

An evaluation of the universal steganalysis and payload steganalysis for six steganographic algorithms with diverse embedding mechanisms: JP Hide & Seek, PVD, LSB flipping, Outguess, *S*-Tool, and F5 has been presented. The accuracy is evaluated on images with relative payload uniformly distributed on [0, 1], meaning that the length of the message was chosen randomly between zero and the maximum embedding capacity for each algorithm and each image. All experiments were performed on single-compressions grayscale and colour images with quality factor 80 created from a database of 250 images of size 512 x 512 taken from a digital camera. Image dataset was divided into two sets. One set was used exclusively for training the SVR, while the other set was used exclusively for testing its performance.

3.1 Regressor Training

During regressor training, the parameters (C, γ, ε) were estimated by 5-fold and 10-fold cross-validation. Cross-validation accuracy of trained data increases as the iteration increases. In the experiments the authors have used the parameters C = 25, γ = 0.1 and ten-fold cross-validation for the classifier.

Fridrich[4], *et al*. prepared payload steganalysis for each algorithm using SVR. They have analysed the performance of SVR for the six steganographic tool used. Table 1 displays the sample median absolute error (MAE) and bias computed from all estimates. MAE exhibits a high error than bias for all the embedding algorithms. The median absolute error of SVR suggests that the features change almost linearly with the number of embedding changes. From the experimental results using SVM classifier, they concluded from Table 2 that detection accuracy was more compared to their previous work in which PCA was not used. They observed that the classifier trained with 135 features was giving high detection rate to the steganographic algorithms embedded in spatial domain than embedded in the transformed domain.

Table 1. Median absolute error bias support vector regression with radial basis kernel and ε-insensitive loss, on six steganographic algorithms

Algorithms	MAE	Bias
JP Hide & Seek	5.0×10^{-03}	2.2×10^{-04}
PVD	4.8×10^{-02}	-3.0×10^{-03}
Outguess	2.5×10^{-03}	3.0×10^{-04}
LSB Flipping	1.7×10^{-03}	$2.5\times10^{-0.4}$
S-tool	2.04×10^{-03}	-3.0×10^{-03}
F5	4.8×10^{-03}	-2.7×10^{-04}

Table 2. The detection accuracy of SVM classifier using PCA

Embedding algorithms	Message length	DCT features	Merged Markov Features	Pixel features
	Detection accuracy (per cent)			
F5	50	90	92	Between 80-90
	25	85	86.20	
	10	80	80.5	
	cover	96	98	
JP Hide & Seek	25	93.05	90	Between 80-90
	10	85	86.7	
	cover	98	98	
OUTGUESS	50	96.79	96.5	80-85
	25	90.40	89	
	10	84.5	83.7	
	cover	98	99	
PVD	100	88.9	83.50	94
	50	82.03	83.54	90
	25	75.04	84.3	89
	10	70	72	80
	cover	97	97	98
S-Tool	100	89.9	89.05	90
	50	90	85.9	89
	25	85	75	95
	10	79	80	90
	Cover	90	95	100
LSD Flipping	50	78	79	95. 5
	25	76	78.5	93
	10	70	75	90
	cover	96.98	97.6	100

4. CONCLUSION

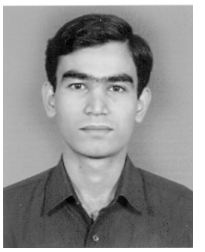
The authors have applied PCA to improve the detection accuracy of SVM classifier and reduced the false positive rate. The performance of SVR-based quantitative steganalysis is also evaluated for six steganographic algorithms.

REFERENCES

1. Fridrich, J. & Goljan, M. Estimation of secret message length in LSB steganography in spatial domain. *In* Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI, Vol. 5306, San Jose, California, 2004. pp. 23-34.
2. Westfied, A. Generic adoption of spatial steganalysis to transform domain. *In* Information hiding, edited by K. Solanki 10th International Workshop, Santa Barbara, CA, Springer-Verlag, New York. June, 2008. pp. 161-77.
3. Amritha, P.P; Jayesh, S. & Yamini, B. Performance study of universal steganalysis based on fisher linear discriminant and multi-class support vector machine classifiers. *In* INDO-US Conference and Workshop on Cyber Security, Cyber Crime and Cyber Forensics, Kochi, India, August 2009.
4. Fridrich, J.; Pevny, T. & Ker, A.D. From blind to quantitative steganalysis, electronic imaging, media forensics and security. *In* Proceedings SPIE, San Jose, CA, January 18-22, 2009. pp. 0C1-0C14.
5. Smola, A.J. & Schoelkopf, B.A. Tutorial on support vector regression. Technical Report, Neuro COLT2 Technical Report NC2-TR-1998-030, 1998.

Contributors

Ms Amritha P.P. is a Research Associate at TIFAC CORE in Cyber Security, Amrita Vishwa Vidyapeetham University, Coimbatore. She received her MTech (Cyber Security) from Amrita Vishwa Vidyapeetham in 2009. She is pursuing PhD in Multimedia Security.



Mr Anoj Madathil is a Junior Research Fellow at TIFAC CORE in Cyber Security, Amrita Vishwa Vidyapeetham University, Coimbatore. He received MCA from University of Calicut in 2009. He is pursuing MS (by Research) at Amrita Vishwa Vidyapeetham.