Preserve Imperceptibility and Robustness Performance on Steganography Technique based on StegaSVM-Shifted LBS Model

IOP Conf. Series: Journal of Physics: Conf. Series **1018** (2018) 012009 doi:10.1088/1742-6596/1018/1/012009

Preserve Imperceptibility and Robustness Performance on Steganography Technique based on StegaSVM-Shifted LBS Model

Hanizan Shaker Hussain [1], Roshidi Din[2], Rusdi Idrus[2]

[1]Department of Information Technology, Kulliyyah Muamalat, Kolej Universiti INSANIAH, 09300 Kuala Ketil, Kedah
[2]School of Computing, UUM College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Email: drhanizan@insaniah.edu.my, roshidi@uum.edu.my, rushdi@uum.edu.my

Abstract. In image steganography, the most popular and widely used techniques is the least significant bit (LSB) that hide data into a cover-image in a spatial and discrete cosine transform (DCT) domain as well. Beside the LSB technique, there is other technique that is also influential i.e support vector machine (SVM) normally used to strengthen the embedding algorithm. Whatever techniques used in the image steganography field,the main purpose is to keep the existence of the secret-message secret. This paper designing the new model is proposed called StegaSVM-Shifted LSB model in DCT domain to preserve the imperceptibility and increase the robustness of stego-images**.** The StegaSVM-Shifted LSB model that has been proposed that utilize HVS and embedding technique through Shifted LSB showed a good performance.

Keywords: Image steganography, DCT model, SVM-Shifted

1. Introduction

The importance of information security has increased due to the increased use of computers and the Internet. This increase of utilization also include contributions by one of its exciting subfields i.e. information hiding. Information hiding is a technology where the secret-messages are hidden inside other files in the form of an image [1][2][3]. There are two popular important research fields namely steganography and watermarking. Steganography is a process that involves hiding a message in an appropriate carrier file for example in an image or in an audio file [4] whereas watermarking is used to place a hidden message (e.g. copyright information) in digital media, like images, music or software [5]. This paper focuses on steganography as the domain implementation area. Then, medium of steganography that used in this study is image medium for the process development of the technique in steganography.

Image steganography is a field in information hiding, besides watermarking, that hides and secures secret-messages written inside an innocuous-looking cover-image file. As a sub-field in information security, it is currently used to secure transmission and information storage in many fields like in the military and medical fields. The generic image steganographic model, as shown in Figure 1, contains two main processes, embedding and extracting.

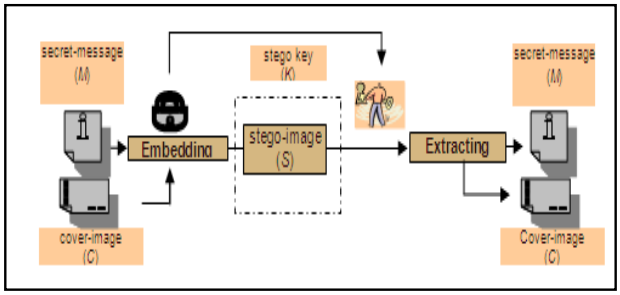

Figure 1. Generic image steganographic model

Based ond Figure 1, A secret-message, *M* will be embedded in a cover-image, *C*; the result is a stego-image, *S* and it is normally sent through a public channel together with a stego-key, K. Then, the recipient will extract the secret-message from the stego-image by using the same stego-key. The terminologies, *secret-message*, *cover-image*, *stego-image* and *stego-key* were agreed to be used in steganoraphy research area at the First International Workshop on Information Hiding held in Cambridge, UK.

In designing steganography algorithms, three requirements are generally considered namely imperceptibility, robustness and payload capacity [4][6][7]. Nevertheless, in image steganography, the most important requirements are imperceptibility and robustness [6][8][9]. These two requirements are important to resist especially two kinds of statistical attacks that is passive and active steganalysis. Many researchers concentrates on passive steganalysis,the attacks only takes actions when the stego-image is found suspicious [10][11]. Meanwhile, active steganalysis is the attacks that attempt to foil all possible covert communications [12][13]. Therefore, this study used StegaSVM-Shifted LSB model is introduced which takes into account. It design consist two main models, StegaSVM classification and StegaSVM-Shifted LSB. In StegaSVM classification, the classified cover-image will be utilized and the non-smooth area, the most appropriate and imperceptible is preferred to be used during the embedding process. StegaSVM classification also will be applied in the extracting process in order to extract the right secret message.

Meanwhile, with the StegaSVM-Shifted LSB model, the proposed technique called Shifted LSB technique will ensure only the least significant bits of DCT coefficients of a cover-image will be utilized to exploit the human visual system (HVS). This Shifted LSB technique is applicable only when it is a case where the original embedding locations a smooth area. Then the technique is applied to shift the embedding position to the nearest best neighbors' LSB. The strength of Shifted LSB technique will be utilized not only in the embedding but also in extracting process. Figure 2 shows the model which highlights the relationship between the two main processes involved and the requirements (i.e. robustness and imperceptibility) to be achieved.

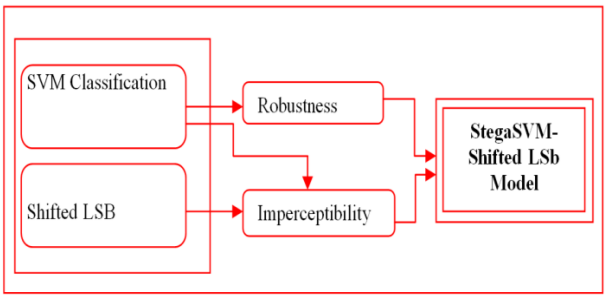

Figure 2. Basic idea of StegaSVM-Shifted LSB model

2. Support Vector Machines

The theory of SVM is based on the idea of structural risk mimization (SRM). SRM is an inductive principle for model selection used for learning from finite training data sets. Basically, SVM uses a linear separating hyperplane to create a classifier with a maximal margin [14]. In cases where given classes cannot be linearly separated in the original input space, the SVM first transforms the original input space into a higher dimensional feature space [15]. In Figure 3 is shown a non-linearly

hyperplane separating. This transformation can be achieved by using various non-linear mapping such as polynomial, radial basis function and sigmoid. Then, the task of a SVM in finding the optimal separating hyperplane in this feature space is simply done [15].

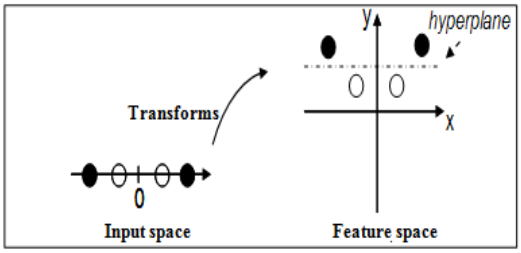

Figure 3. Feature Mapping Transformation

All SVMs algorithms have been applied in watermarking and no work has been done in steganography. These types of algorithms are normally used in the embedding and extracting procedures. All works concentrate on imperceptibility to utilize the SVMs good ability in learning the relationship between hidden-information and cover-image that is useful to be used in embedding and extracting functions [16][18]. All algorithms use images as a secret-messages and applied secret key for robustness and security. All algorithms have used localization approach in their process because the changes are normally done on less sensitive channels to the human eye (the blue and luminance channels) [16][17]. Then the average pixel intensity (localized modification) based on the certain shapes will be computed to determine the changes on the channels. All works use RBF kernel to map the training samples to a higher dimensional feature space.

SVM has a proper learning and generalization capabilities and it shows to be very resistant to the over-fitting problem [19]. Unfortunately, the SVM is rather sensitive to outliers or noises since the penalty term of SVM treats every data point equally in the training process. SVM was originally introduced by Vapnik within the area of statistical utilization [15]. In statistical learning theory, the SVM has been developed for data classification and prediction and it is used in wide range applications such as character recognition [20], text categorization [21], face detection in images [22] and information hiding in images [23].

A thorough review of the literature has revealed that all SVM works in information hiding have been done to utilize the SVM good learning ability to memorize the relationship between a random coefficient and its neighboring coefficients [24][25]. It is mainly used to classify the cover-image and find the suitable area for embedding. Even though SVM has lately been used extensively for image classification in watermarking [25][26] but none has been done in steganography. Only Wu et al. [27] has attempted to introduce SVM in steganography but his work is merely to support vector regression (SVR) to predict the pixel values for embedding rather than classifying the cover-image.

SVM was first initiated by Yu et al. [28] in watermarking by introducing the SVM-based Color Image Watermarking (SCIW) that utilizes the image feature i.e. pixel intensity which is calculated from three difference types of shapes of neighboring pixels for classification. His attempt is fruitful in utilizing SVM to classify the cover-image into smooth and non-smooth areas by using 1024 bits as training bits. For security purposes, he employs a pseudo-random number generator (PRNG) to randomly pick the embedding position before the secret-bits is embedded by modifying the blue channel of color components. The trained SVM is exploited again in the extracting process to acquire the right secret-message. Then, there have been further research to utilize the ability of SVM in spatial domain as proposed by Yu et al. [28].

3. Model of Design

The proposed design begin with a general model that is called StegaSVM-Shifted LSB that involves two main models StegaSVM classification and StegaSVM-Shifted LSB. Hopefully, through this general model description will give the reader a rough idea about the proposed design model. Then, a more detailed description of each model StegaSVM classification and StegaSVM-Shifted LSB can be followed after that. But for the StegaSVM-Shifted LSB, its two main sub-models will be explained one by one starting with StegaSVM-Shifted LSB embedding then StegaSVM-Shifted LSB extracting for the sake of simplicity.

3.1 StegaSVM-Shifted LSB Model

The proposed StegaSVM-Shifted LSB model is as shown in Figure 4. This model contains all main processes involved combining StegaSVM classification, Shifted LSB embedding and Shifted LSB extracting.

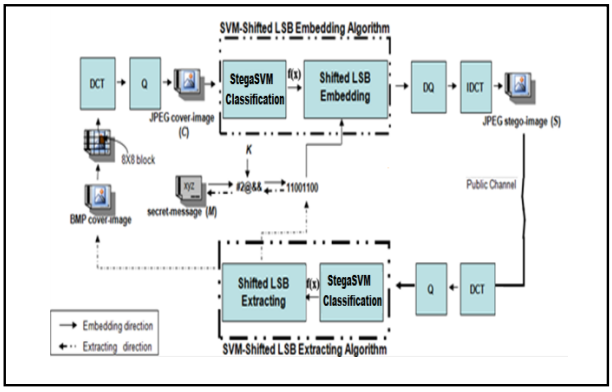

Figure 4. Process of StegaSVM-Shifted LSB Model

Based on Figure 4 this model begin with the BMP cover-image, *C* is first divided into 8x8 non-overlapping blocks. Then, it transformed from space domain to transform domain in order to make it more robust to attacks and remain imperceptible to the human eyes. In the quantization step, all DCT coefficients are divided by the predefined quantization values to modulate the different spectral components on the image. This permutation can equalize the spread of insignificant coefficients. The hybrid techniques of the StegaSVM classification and Shifted LSB will be done through the StegaSVM-Shifted LSB embedding algorithm for cover-image classification and secret-message embedding respectively. The secret bits from the transformed secret-message, *M* will be embedded in the medium frequency of the insignificant coefficients based on the trained SVM before it will be permutated and generated by using a user-defined key, *K*.. The output, stego-image (*S*) will go through inverse DCT and quantization before it can be sent via public channel. The extracting process at the recipient side will involvea reverse of the embedding process called StegaSVM-Shifted LSB extracting algorithm as it employs a symmetric model.

3.2 StegaSVM-Shifted LSB Classification

The StegaSVM classification model works when 256x256 JPEG grayscale cover-image is being read. Image features such as luminance, edge and entropy values will be extracted from the cover-image. Then a dataset will be constructed by classifying it into SVM format. The dataset is comprised of the following set:

SVM::Dataset(label= {1,-1} Data ={luminance, edge,entropy})

The basic concept of StegaSVM classification model is shown in Figure 5 as follow.

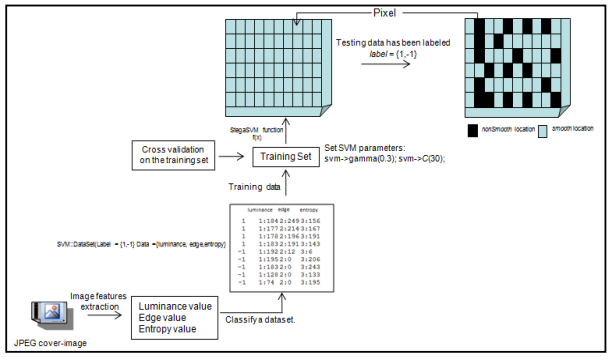

Figure 5. Basic concept StegaSVM-Shifted LSB classification model

The SVM classification contains with two class labels of 1 (smooth) and -1 (non-smooth). While the data is made up of three attributes, namely luminance, edge and entropy arranged in specific columns in Figure 6. The first column for SVM labels, the second column to the first attribute, the second attribute of the third column and the fourth column for the third attribute.

```
      luminance   edge     entropy
  1     1:184 2:249 3:156
  1     1:177 2:214 3:167
  1     1:178 2:196 3:191
  1     1:183 2:191 3:143
 -1     1:192 2:12  3:6
 -1     1:195 2:0   3:206
 -1     1:183 2:0   3:243
 -1     1:128 2:0   3:133
 -1     1:74  2:0   3:195
```

Figure 6. SVM dataset format

The available dataset can then be used as training data in the training set. At this time, SVM parameters should be identified and set i.e. gamma γ and penalty parameter C (e.g. gamma = 0.3 while C = 30). In addition, the percentage of training data points also need to be determined. Not to forget that a cross validation approach should also be done here in order to get an SVM model that is efficient and suitable for image steganography. Through this approach, various combinations of parameters of SVM will be used and tested. The best SVM parameters pairs will be chosen to be used in the testing set.After that, as a result of cross validation activity, a StegaSVM function $f(x)$ will be generated. Then $f(x)$ will be utilized on testing data in the embedding process which eventually resulted a stego-image as a result of the exploitation of smooth (-1) and non-smooth (1) areas.

In designing a suitable StegaSVM classification model with the field of image steganography is being implemented. Designing an appropriate model with the field that is to be investigated (i.e. image steganography) is crucial in order to achieve the desired goals (i.e. a highly imperceptible and robust image steganographic model).

3.3 StegaSVM-Shifted LSB Embedding Model

The StegaSVM-Shifted LSB embedding model process is shown in Figure 7 in this paper.

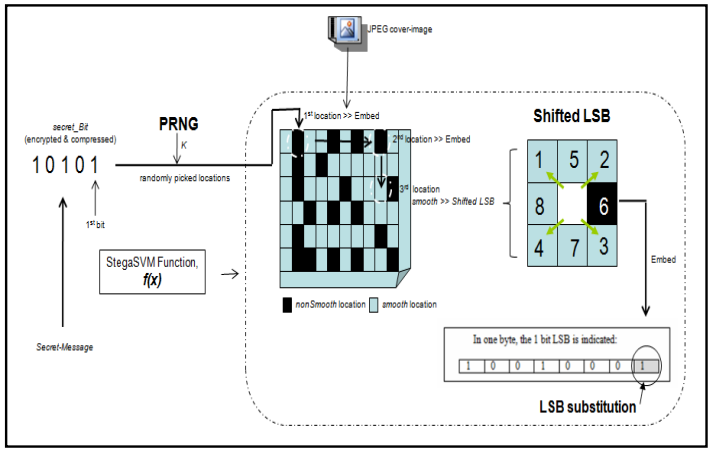

Figure 7. StegaSVM-Shifted LSB embedding model

Based on Figure 7 the sub-model, a a secret-message is first converted into a sequence of bits which is then encrypted and compressed. In Figure 8, sequence of these bits is marked as *secret_Bit*. Then, by using pseudo-random number generator (PRNG) with a secret key, K for any secret-bit, *secret_Bit* = {0,1}, a random embedding location will be obtained. According to Yu *et al.* [28], PRNG is used in the research especially in information hiding because of its simplicity and security purposes. The

embedding process is really depends on the type of embedding location, whether it is smooth (*smooth location*) or non-smooth (*nonSmooth location*). If it is *nonSmooth location* then embed *secret_Bit* by applying the LSB substitution. If it's otherwise, do the Shifted LSB technique that is, either go to 8-neighbors' LSB following the specific sequence, if found any of the first the *nonSmooth location*, embed *secret_Bit*.

4. Discussion

In this model, various types of cover-images (i.e different image complexities) have been used; Lena, Baboon, Uitm and Clock. As for the secret-message, the size that has been used is 1024bits for all types of cover-images. Meanwhile, for the cover-image classification, the value of *C* has been set to 30 while the value of γ is set at 0.5. Then, in Table 1 shows cover-images with high image complexities, Lena dan Baboon have recorded the highest PSNR; 49.86 and 49.33 respectively. This is followed by Uitm cover-image with PSNR of 48.89 whereas the cover-image that has low image complexities, that is Clock, recorded the lowest PSNR with 47.68.

Table 1. PSNR of different types of cover images

Types of cover-images	Different Image Complexities	PSNR
Lena	High	49.86
Baboon	High	49.33
Uitm	Moderate	48.89
Clock	Low	47.68

High image complexities actually represents image with more striking colors, more shades, the combination of lots of light and dark colors, or there will be many lines or edges. For example, Lena and Baboon images have many different color combinations that cover almost the entire surface of the image. So, from here it has formed more edges and line areas that can be called as non-smooth areas that are more secured to use for embedding in the Shifted LSB operation. So with that, they have a higher PSNR values compared to other images of more than 49dB. Meanwhile,Uitm cover-image has a moderate level of image complexities because it has a uniform color of black only.It is similar to the Clock cover-image that has plain bright colors, that is why the smooth areas are higher compared than non-smooth area. So, when there are not many non-smooth areas that can be utilized in the Shifted LSB operation, then the recorded result of PSNR value is quite low for both cover-images.

This display the StegaSVM-Shifted LSB model, all cover-images, even the one with different cover-image complexities (high or low image complexities) are still able to maintainthe quality of a cover-image after the embedding process. This can be done through the capability of the proposed techniques of StegaSVM classification to successfully classify the cover-image into a better location for embedding. In addition, through the Shifted LSB operation,using a better location that is identified for embedding and extracting process was proven a successful effort. Embedding technique randomly and uniformly throughout the cover-image applied by the proposed model also enhance cover-image quality. In addition, this model has also been successful in reducing the impact of non-random changes to avoid secret-message from being easily detected. The increase in secret-message size can lead to quality decline in certain cover-image. It becomes clearer when the size of the secret-message is equal to 2048bits; it shows that the cover-image with the size of 256x256 could not afford to accommodate the large secret-message.

5. Conclusions

A model called StegaSVM-Shifted LSB was designed and developed in this chapter.In this chapter, the design was initiated with a description of the main model, namely StegaSVM-Shifted LSB. Then, the next description is broken down into three sub-models that are StegaSVM classification, StegaSVM-Shifted LSB embedding and StegaSVM-Shifted LSB extracting. The StegaSVM classsification model had the activities involved were to extract image features, construct training dataset, select kernel, implement cross-validation and execute SVM training set. The technique would shift the embedding position to the nearest best neighbors' LSB when it wasa case where the location was a smooth area. In the StegaSVM-Shifted LSB extracting model, the same Shifted LSB technique would also be applied in finding the actual embedding location for extracting process.

References

[1] J. He, S. Tan, T. Wu. On the Security of Steganographic Techniques. International Congress on Image and Signal Processing, (2008) 716-719.
[2] M. T. Siponen, H. Oinas-Kukkonen, H. A Review of Information Security Issues and Respective Research Contributions. Database for Advances in Information Systems, (2007) 60-80.
[3] C.-C. Chang, T.-S. Chen, L.-Z. Chung. A Steganographic Method Based Upon JPEG and Quantization Table Modification. International Journal of Information Sciences (2002) 123-138.
[4] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, P. M. Review: Digital Image Steganography: Survey and Analysis of Current Methods. Journal Signal Processing, (2010). 727-752.
[5] Y.-G Fu, R.-M. Shen, L.-P. Shen, X.-S. Lei. Reliable Information Hiding Based on Support Vector Machine. International Journal of Informatica, (2005) 333-346.
[6] N. Sathisha. Embedding Information in DCT Coefficients Based on Average Covariance. International Journal of Engineering Science and Technology, (2011) 3184-3194.
[7] P. M. Santi, M.K. Kundu. Genetic Algorithms for Optimality of Data Hiding in Digital Images. Bio-Inspired Information Hiding, (2009) 361-373.
[8] M. A. Younes, A. Jantan, A. A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion. International Journal of Computer Science and Network Security (2008) 247-254.
[9] Y. K. Lee, L. H. Chen. (2000). A Secure Robust Image Steganographic Model. The Conference on Information Security, (2000) 275-284.
[10] L. Bin, H. Junhui, H. Jiwu, Q. S. Yun. A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing , (2011) 142-172.
[11] J. He, S. Tan, T. Wu. On the Security of Steganographic Techniques. International Congress on Image and Signal Processing, (2008) 716-719.
[12] R. Din, A. Shamsudin. Digital Steganalysis: Computational Intelligence Approach. International Journal of Computers, . (2009) 161-166.
[13] R. Chandramouli. A Mathematical Framework for Active Steganalysis. *Multimedia Systems*, (2003) 303–311.
[14] T. Joachims. Support Vector and Kernel Methods. In C. S. Department, SIGIR 2003 Tutorial. Cornell University (2003).
[15] V. Kecman. Learning and Soft Computing. London: The MIT Press. (2001).
[16] S. Huang, W. Zhang. Digital Watermarking Based on Neural Network and Image Features. *International Conference on Information and Computing Science*, (2009) 238 – 240.
[17] M. Jamzad, Z. Z. Kermani. Secure Steganography Using Gabor Filter and Neural Networks. *Transactions on Data Hiding and Multimedia Security*, (2008) 65-71.
[18] K. Naoe, Y. Takefuji. Damageless Information Hiding Using NN on YcbCr Domain. *International Journal of Computer Science and Network Security, (2008).*
[19] C. Campbell. Kernel Methods: A Survey of Current Techniques. *New Computings* (2002) 63-84.
[20] C.-L. Liu, K, Nakashima, H. Sako, H. Fujisawa. Handwritten Digit Recognition: Benchmarking of State-of-the-Art Techniques. *Pattern Recognition*, (2003) 2271-2285.
[21] T. Joachims. Text Categorization with Support Vector Machines: Learning with Many Relevant Features. *European Conference on Machine Learning*,(1998) 137-142. Chemnitz, Germany.
[22] E. Osuna, R. Freund, F. Girosit. Training Support Vector Machines: An Application to Face Detection . *IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* (2002) 130-136. San Juan , Puerto Rico: IEEE Computer Society.
[23] L. Li, W.-Y Ding, J.-Y. Li. A Novel Robustness Image Watermarking Scheme Based on Fuzzy Support Vector Machine. *The 3rd IEEE International Conference on Computer Science and Information Technology* (2010) 533 – 537.
[24] S. Ramly, S. A. Aljunid, H.S. Hussain, H. S. SVM-SS Watermarking Model for Medical Images. *Digital Enterprise and Information Systems*, (2011) 372-386.
[25] F. Meng, H. Peng, Z. Pei, J. Wang. A Novel Blind Image Watermarking Scheme Based on

Support
Vector Machine in DCT Domain. *International Conference on Computational Intelligence and Security* , (2008) 16 - 20.

[26] H.-H. Tsai, H.-C. Tseng, Y.-S. Lai. Robust Lossless Image Watermarking Based on A-Trimmed Mean Algorithm and Support Vector Machine. *The Journal of Systems and Software*, (2010) 1015–1028.

[27] H.-C. Wu, K.-C. Liu, J.-D. Chang, C.-H. & Huang. An Image Steganographic Scheme Based on Support Vector Regression (SVR). *Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications,* (2008) 519 - 524.

[28] P.-T. Yu, H.-H. Tsai, D.-W. Sun. Digital Watermarking of Color Images Using Support Vector Machine. *National Computer Symposium (NCS'03), (2003).* Taichung.