Indonesian Journal of Electrical Engineering and Computer Science
Vol. 12, No. 1, October 2018, pp. 233~238
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i1.pp233-238

The Embedding Performance of StegSVM Model in Image Steganography

Hanizan Shaker Hussain[1], Roshidi Din[2], Mohd Hanif Ali[3], Nor Balqis[4]
[1,3,4]Kulliyyah Muamalat dan Sains Pengurusan, Universiti Islam Antarabangsa Sultan Abdul Halim Mu'adzam Shah, 09300, Kedah, Malaysia
[2]School of Computing (SOC), CAS, Universiti Utara Malaysia 06010 Sintok, Kedah, Malaysia

Article Info

Article history:

Received May 21, 2018
Revised Jul 10, 2018
Accepted Jul 25, 2018

Keywords:

Image steganography
Least significant bit
Discrete cosine transform

ABSTRACT

This paper focuses on one of the areas of information hiding which is image steganography. It proposes the StegSVM model as an embedding technique in steganography that has exploited human visual system through Shifted LSB that shows an expected performance. The performance of this technique evaluation is based on imperceptibility and robustness of the technique compared to the other previous models in image steganography doamin. Thus, the result shows that the proposed StegSVM model is promising. For further work, it is suggested that the other image domain through other intelligent methods should be investigated.

Corresponding Author:

Roshidi Din,
Kulliyyah Muamalat dan Sains Pengurusan,
Universiti Islam Antarabangsa Sultan Abdul Halim Mu'adzam Shah,
09300, Kedah, Malaysia.
Email: roshidi@uum.edu.my

1. INTRODUCTION

The concept of exchanging hidden information causes concerns in the field of information security [1]. Therefore, several methods have been applied for this purpose including cryptography, steganography, and watermarking to establish hidden communication. Secret data can be concealed in different cover media such as image, video, audio, and written text [2]. However, among all these methods, steganography has lately acquired more attention and becoming increasingly important in the field of computer security. It is a process that involves hiding messages in other messages [1] while watermarking is using to hide the secret messages in various medium [2]. The key difference between steganography and watermarking is that the goal of steganography is more to covert communication [3], which is why, the fundamental requirement of steganographic algorithm is that messages hidden inside any carrier file should not be sensible to human beings. The goal of watermarking on the other hand, is to ensure the hidden message always remains present in the digital media to provide solid proof of ownership [4], [5]. In this study, the focus is generally on steganography and specifically on image steganography. In fact, image steganography is the most popular and widely applied technique today [6-8]. Among the factors that led to this situation is because most business today are using digital images as the main medium to disseminate information to be more attractive such as in advertising and so on. There are two popular kinds of domain images that are normally used in image steganography, namely spatial and transform domains. In spatial domain the secret-message is directly embedded into the pixels of the cover-image, for example, by LSB substitution. Meanwhile, in transform domain the cover-image is first transformed into coefficients such as

discrete cosine transform (DCT), discrete fourier transform (DFT) and discrete wavelet transform (DWT) domains [6], [8]. However, the most popular and extensively used in image steganography is DCT domain [3], [4], [7]. This is because DCT domain relatively consumes less power and has shown to be uncorrelated due to energy compaction into just one coefficient i.e. DC coefficient while compressing the coefficients values, and this makes it possible to construct relatively simple algorithms [7].

Most of images types have been used as the cover-image in these domains like Bitmap File Format (BMP), Joint Photographic Experts Group (JPEG) and Graphics Interchange Format (GIF) images with JPEG being the most common image format for Internet and local usage since it provides a large compression ratio and maintains high image quality [12-14]. According to Cheddad [7], image steganography is the field that remains untested and very few of companies and associations have published the requirements of the steganography algorithm evaluation. This is because the target of the steganography scheme evaluation should be clearly identified based on it purposes. As mentioned earlier, imperceptibility and robustness are the prominent criterias in evaluating the steganographic technique. Therefore, this paper proposes the model that has been developed is StegSVM in steganography. It evaluates this model in comparison with the robustness and impercecptibilty of the technique in steganography.

2. STEGSVM MODEL EVALUATION

Usually, Peak-Signal-to-Noise-Ratio (PSNR) is utilized to verify the perceptual transparency and fidelity of image steganography algorithms. It gives a measure of the statistical differences between a cover-image and stego-image. PSNR is good in providing qualitative rank order scores as long as the same content and the same algorithm are used [15]. The higher the PSNR value, the more effective the technique is. As such, the technique can be said effective if the PSNR value is more than 40dB. Cheddad et al. (4) have stated that if the PSNR value falls below 30dB, it indicates that the quality of the image is fairly low since the distortion caused by the embedding is noticeable. Consequently, a high quality stego-image should attempt for 40dB and above. Furthermore, a greater PSNR value means a lower degree of image distortion after the secret-message is embedded. In determining the degradation with respect to the host image, the researcher applies the PSNR metric (Peak Signal-to Noise Ratio) and MSE (Mean Square Error) to measure the distortion produced after the embedding process [16-17]. It is defined as:

$$\text{PSNR} = 10 \log_{10} \left(\frac{C_{\max}^2}{MSE}\right)$$

$$\text{MSE} = \frac{1}{PQ} \sum_{x=1}^{P} \sum_{y=1}^{Q} (S_{xy} - C_{xy})^2 \quad (1)$$

where x and y are the image coordinates, *P* and *Q* are the dimensions of the image, S_{xy} is the generated stego-image and Cxy is the cover image, as shown in Figure 1. PSNR is often expressed on logarithmic scale in decibels (dB) [4].

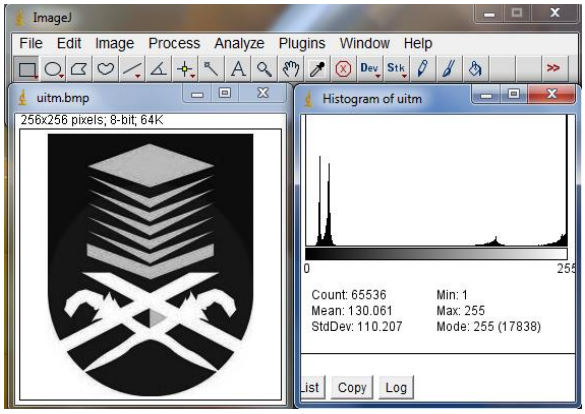

Figure 1. ImageJ application in analysing image

There are two kinds of metrics that can be used in order to evaluate the robustness of secret-message, the Normalized Cross-Correlation (NC) and Similarity Ratio (SR). Both of these metrics are described in the next sections, respectively.

The robustness of the secret-message can be evaluated using the Normalized Cross-Correlation (NC) between the original secret-message and the extracted secret-message. The NC is evaluated by varying the strength of each degradation process which is defined as:

$$NC = \frac{\sum_{x=1}^{P}\sum_{y=1}^{Q}[M(x,y).M^{'}(x,y)]}{\sum_{x=1}^{P}\sum_{y=1}^{Q}[M(x,y)]^2} \quad (2)$$

where, M = secret-message; M' = extracted secret-message

In order to test the robustness, the Similarity Ratio (SR) can be calculated between original and watermarked images. It can be achieved by using the following equation:

$$SR = \frac{S}{S+D} \quad (3)$$

The number of matching pixel and another different pixel values are represented by S and D respectively. If the value of SR is closed to 1, its shows the robustness of watermark is better and preserved [22].

According to Tsai et al. [23] NC has been commonly used as a metric to evaluate the degree of similarity between two compared images because of these two advantages. It is less sensitive to linear changes in the amplitude of illumination in the two compared images that makes measurement more accurate ii) It is confined in the range between -1 and 1 that the setting of threshold value is much easier because it involves the calculation of a smaller number. It is well known that NC can be efficiently implemented in the transform domain rather than spatial domain [24]**.** The NC value can be easily evaluated by using NC application as shown in Figure 2 as follows [20].

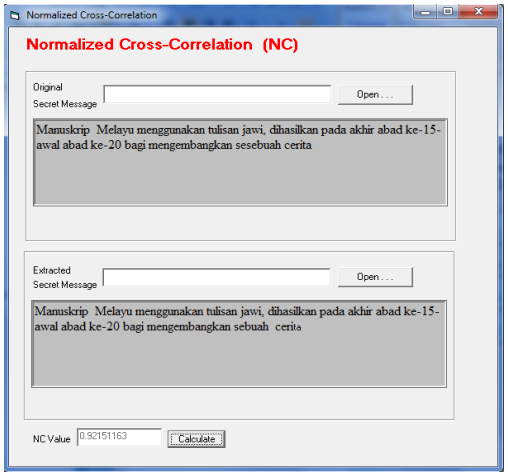

Figure 2. Normalized Cross-Correlation

Therefore, PSNR and NC have been selected to be used in this research to measure the imperceptibility of cover-image and the robustness of secret-message respectively. For the PSNR, the ImageJ application will be used as a tool to measure the cover-image [21]. Its power and flexibility allow it to be used as a research tool by scientists in various disciplines [25], including image information hiding. Meanwhile, the NC Tool has been chosen to be used in order to find the NC values between the original and the extracted secret-message. It has been used because of the availability and also as a convenient sample.

The evaluation is based on the value between the StegSVM model with the existing SVM classification models or with the LSB substitutions techniques, or with kinds of image processing attacks. As mentioned earlier, imperceptibility and robustness are the two most important criteria [24, 25, 16] in evaluating an image steganography. The imperceptibility and robustness of StegSVM is based on the comparison between first, the proposed and existing model and second, between the proposed model and

other models of LSB substitution. For both of these experiments, the secret-message size has been set to 1024bits while the penalty value of parameter C and gamma is set to 30 and 0.5 respectively.

3. RESULT AND DISCUSSION

The result of PSNR by comparing two types of LSB techniques: Shifted LSB and Direct LSB Substitution is shown in Table 1. Shifted LSB is applied with the usage of StegSVM while Direct LSB Substitution technique is represented by using another tool that is StegaMage.

Table 1. PSNR of different LSB substitution

Types of cover-images	PSNR	
	Shifted LSB (StegSVM)	Direct LSB Substitution (StegaMage)
Lena	49.86	32.76
Baboon	49.33	31.45
Uitm	48.89	29.01
Clock	47.68	28.91

According to Table 1, it clearly illustrates the usage of Shifted LSB technique resulted in having much higher PSNR for all types of cover-image. The value for all PSNR for Shifted LSB technique reached 40 and above compared to another technique. The highest PSNR is 49.86 through Lena cover-image and the lowest is 47.68 for Clock cover-image. Meanwhile, for Direct LSB Substitution technique, the highest PSNR value is only at 32.76. and the lowest is at 28.91 for Clock cover-image. LSB Shifted technique shows that, it is not only succeeded in embedding randomizing implementation, but it also makes sure that the embedding location is secured compared to direct LSB substitution. As for robustness, the proposed model will be evaluated based on the comparison of the value of normalized cross-correlation (NC) for extracted secret-message between first, the proposed and existing models. Second is between the proposed model and other models of LSB substitution. Third is the comparison between the results of image processing attacks on the proposed and existing models. As for these three experiments, the size for the secret message has been justified to 1024 bits while the value for penalty parameter C and gamma is 30 and 0.5 respectively. Then, in Table 2 the shifted LSB technique recorded higher NC value as representative in robustness between the proposed model and other model of LSB.

Table 2. NC of different LSB substitution models

Types of cover-images	PSNR	
	Shifted LSB (StegSVM)	Direct LSB Substitution (StegaMage)
Lena	1.00	0.92
Baboon	1.00	0.95
Uitm	0.99	0.87
Clock	0.98	0.84

Based on Table 2, the comparison proposed model with Direct LSB Substitution Technique with the value range from 0.98 to 1.0. Simultaneouly, Direct LSB Substitution Technique recorded NC value that is much lower, being the highest value is 0.95 and the lowest is 0.84. Lena and Baboon Cover-image recorded higher NC value for both techniques compared to other cover-image. It is found that the NC value is much higher in comparison between the proposed model, the existing models and different LSB substitution method. In Table 3, after a few image processing attacks, the extracted secret-message is valued using NC.

Table 3. NC of different kinds of image processing attacks

Image Processing Attacks	Comparison of Methods		
	Blind SVM	FSVM	StegSVM
Low-Pass Filtering	0.95	0.97	0.98
Salt& Pepper Noise	0.72	0.97	0.98
JPEG Attack	0.95	0.96	0.96

Based on Table 3, StegSVM model showed NC values that are high for all types of image steganography attacks. The highest NC is for low-pass filtering and salt-pepper noise, which is 0.98 for both. As for JPEG attack, the proposed model recorded NC value equals to 0.96. Meanwhile, for FSVM, the NC value is between 0.97 until 0.96 and as for Blind-SVM, the NC value is between 0.72 - 0.95. The NC value is affected after image processing attacks as it recorded much higher value compared to two other methods, namely Blind SVM and FSVM.

4. CONCLUSION

This paper performed the evaluation of the proposed model StegSVM model compared to the other model through imperceptibility and robustness of the technique. StegSVM model were acceptable in which it shows a higher quality steganography, thus enhancing the performance of existing works. In extracting process, by exploiting the SVM learning ability, the right secret-bits can be recovered. Based on each experiment, it shows StegSVM model has a better performance than the previous models. For further work, it is suggested that the other image domains through other intelligent methods should be investigated.

ACKNOWLEDGEMENT

This study would like to thank the MoHE Malaysia for grant fund under the FRGS with S_O Code - 13576, and RIMC of Universiti Utara Malaysia, Kedah.

References

[1] C. C. Chang, T. S. Chen and L. Z. Chung.2002. *A Steganographic Method Based Upon JPEG and Quantization Table Modification*. International Journal of Information Sciences, 2002; 123-138
[2] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt. *Review: Digital Image Steganography: Survey and Analysis of Current Methods*. Journal Signal Processing, 2010; 727-752.
[3] Y. G. Fu, R. M. Shen, L. P. Shen, and X. S. Lei.2005. *Reliable Information Hiding Based on Support Vector Machine.* International Journal of Informatica. 2005; 333-346.
[4] S. Shen, H. Zhang, D. Feng, Z. Cao, J. Huang. Survey of Information Security. *Science in China Series F: Information Sciences*, 2007; 273-298.
[5] H. Wang and S. Wang, S. 2004. Cyber Warfare: Steganography vs. Steganalysis. *Communications of the ACM* , 76-82.
[6] 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.
[6] T. Morkel, J.H. Eloff and M. S. Olivier. An Overview of Image Steganography. *Annual Information Security South Africa Conference.* Sandton, South Africa: M S Olivier. 2005
[8] M. A. Younes and A. Jantan. *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] E. Cole.. *Hiding in Plain Sight: Steganography and the Art of Covert Communication.* New York: John Wiley Publishing Inc. 2003
[10] N. Sathisha. *Embedding Information in DCT Coefficients Based on Average Covariance.* International Journal of Engineering Science and Technology. 2011; 3184-3194.
[11] Z. Li, K. Lu, X. Zeng, X. Pan. 2010. *A Blind Steganalytic Scheme Based on DCT and Spatial Domain for JPEG Images.* Journal of Multimedia .2010; 200-207.
[12] J. Fridrich. 2004. Featured-Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes. *International Workshop on Information Hiding.* 2004; 67-81.
[13] E. Marini, F. Autrusseau, P. Le Callet and P. Campisi, P. 2007. *Evaluation of Standard Watermarking Techniques*. Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents. 2007; 142-155.
[14] N. I. Wu and M. S. Hwang. *Data Hiding: Current Status and Key Issues.* International Journal of Network Security , 2007; 1-9.
[15] N. Jiang. A Novel Analysis Method of Information Hiding. *International Congress on Image and Signal Processing*. 2008; 621-625. Hainan: IEEE Computer Society.
[16] A. A. Gutu. *Pixel Indicator Technique for RGB Image Steganography*. Journal of Emerging Technologies in Web Intelligence, 2010; 56-64.
[17] B. Kaipa and S. A. Robila. 2010. Statistical Steganalyis of Images Using Open Source Software. *International Conference on Applications and Technology*. 2010; 1-5. IEEE Computer Society.
[18] 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.
[19] C. Schneider, W. Rasband and K. Eliceiri. 2012. *NIH Image to ImageJ: 25 years of image analysis*. Nature Methods. 2012; 671–675.
[20] C. W. Hsu, C. C. Chang and C. J. Lin. 2009. *A Practical Guide to Support Vector Classification.* Bioinformatics. 2009; 1-15.

[21] H. H. Tsai, H. C. Tseng and 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.
[22] J. P. Lewis. 1998. *idiom.* Retrieved November 16, 2012, from Vision Interface: http://www.idiom.com/~zilla/Papers/visionInterface/.
[23] R. Din, A. Samsudin. *Intelegent steganalytic system: Appication on natural lanugae environment.* WSEAS transaction on System and control. 2009; 4(8): 379-388.
[24] R. Din, Z.C. Ani, A. Samsudin. *A Formulation of conditional states on steganaysis approach*. WSEAS transaction on mathematic. 2012; 11(3): 173-182.
[25] R. Din, A. Samsudin, T.Z.T. Muda, A. Amphawan. M.N. Omar. Fitness value based evaluation algorithm approach for text steganalysis model. *International journal of mathematic models and methods in applied science*. 2013; 7(5): 551-558.
[26] Hanizan Shaker Hussain, Roshidi Din, Rusdi Idrus. Preserve Imperceptibility and Robustness Performance on Steganography Technique based on StegaSVM-Shifted LBS Model, *Journal of Physics: Conference Series*, 2018; 1018: 1 – 8.