VOL. 10, NO. 3, FEBRUARY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CAPACITY PERFORMANCE OF STEGANOGRAPHY METHOD IN TEXT BASED DOMAIN

Baharudin Osman, Roshidi Din and Mohd Rushdi Idrus
School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, UUM Sintok, Kedah, Malaysia
E-Mail: bahaosman@uum.edu.my

ABSTRACT

Capacity is one of the performance factors in embedding process of any text steganography methods. A better embedding ratio and saving space ratio offers more text can be hidden inside cover text. This paper tries to evaluate several format based techniques of text steganography based on their embedding ratio and saving space capacity factors. This paper analysed the performance of text steganography methods which are changing in Alphabet Letter Patterns (CALP), Vertical Straight Line (VERT) and Quadruple Categorization (QUAD) methods based on these two factors. Embedding Ratio (ER) and Saving Space Ratio (SSR) is used to measure the performance. It has been identified that VERT method give a good effort performance compared to CALP and QUAD based method. In future, a robustness of text steganography methods should be considered as a next effort in order to find a strength capability on text steganography.

Keywords: text steganography. embedding ratio, saving space ratio, CALP, QUAD. VERT.

INTRODUCTION

Steganography is the arts of science to hide data in a cover media such as text, audio, video and image which is one of sub disciplines in information security field. It is the most popular sub disciplines amongst others such as anonymity, copyright marking and covert channel (Fabien, Petitcolas, Ross & Markus, 1999), (Al-Mualla & Al-Ahmad, 2013). Steganography has played a major significant role in secret communication such as e-national security (Si and Li, 2008), e-military (Din & Azman, 2009), multimedia property (Yusuf, Firoj & Asif, 2012), authentication (Gunawardena, Kulkarni & Gnanasekaraiyer, 2013) etc. Various applications have been implemented in steganography (Hamid et al., 2012), (Kodovsky, Jessica & Vojtech, 2012), (Wang & Jiangqun, 2012). Steganography differs from cryptography which it scrambles messages so they cannot be understood. In short, cryptography is about protecting the content of messages whereas steganography is about concealing the existing messages. Table-1 shows the advantages and disadvantages of both technologies.

Table 1: Comparison between steganography and cryptography (Kaur, Pooja & Harish, 2013), (Vahedi, Vincent & Ian, 2014).

Method types	Message passing	Technology used	Message strength	Technology dependency
Steganography	• Unknown medium	• Litte known • Still being developed for certain formats	• Once detected consider fail	• Non-Technology based (format based)
Cryptography	• Known medium	• Common applied • Most algorithm are known to government departments	• Attack based on algorithm strength (resistant to brute force attack) • Large expensive computing power required for cracking	• Strength based on technology

Steganography is the science of hiding information with the goal is to hide the data from a third party in such way that no one suspects the existence of the message. The word steganography is derived from Greek (steganos + graphy) and it means covered or hidden writing. Actually, steganography is introduced to hide the existence of the communication by concealing a hidden message in an appropriate carrier which is divided into two domains such as technical steganography (image, audio, video, and network packet etc.) and natural language steganography.

There are two aspects of steganography, namely digital steganography and natural language steganography. Digital steganography concentrates on channel capacity which is concerned about a cover medium to hide messages, while natural language steganography concentrates on using written natural language to conceal secret messages (Kaur, Pooja & Harish, 2013). Digital steganography has been carried out on image steganography (Hamid et al., 2012), (Wang & Jiangqun, 2012), (Choudhary, 2013), audio steganography (Zamani, Azizah &Shahidan, 2012), (Nutzinger, 2012), (Adhiya & Swat, 2012), and video steganography (Cao, Xianfeng & Dengguo, 2012), (Bodhak, & Baisa, 2012), (Dasgupta, Mandal & Paramartha, 2012). which have produced good results. Besides, several efforts on steganography system based on digital steganography for hidden and unhidden messages such as Outguess, F5, YASS and MBS (Hamid et al., 2012), (Kodovsky, Jessica & Vojtech, 2012), (Wang & Jiangqun, 2012), (Choudhary, 2013) have also been developed.

Natural language steganography is the art of using natural language to conceal secret message (Mansor, Din & Azman, 2010). Currently, there are two groups of natural language steganography environment namely text steganography, and linguistic steganography (Baharudin et al, 2013), (Din, 2014), (Din, Che Ani & Azman, 2012), (Kaleem, 2012). Several types of text steganography methods which are line-shift coding, word-shift coding (Singh, Rajat & Agarwal, 2012), (Sharma & Shweta, 2013) and feature coding (Govada et al., 2012), (Majercak et al., 2013), (Chhikara & Latika, 2013) have been explored.

Meanwhile, several categories of linguistic steganography methods have been identified such as using probabilistic context-free grammars to generate cover text, synonym substitutions, syntactic transformations, semantic transformations, and generating cover text using hybrid techniques (Chhikara & Latika, 2013), (Gardiner, 2014), (He, 2012).

A linguistic method considers the linguistic properties of the text to modify it. A linguistic structure is used to hide the data where the syntax or semantic of the language is used. In syntactic method, such as punctuation, comma and full stop are placed in a proper place in the document, whereas semantic method will replace the synonym word. In order to be a good text steganography, methods use should consider at least two capacity factors of the hidden text against cover text which are embedding ratio and saving space ratio factors. Thus, this paper tries to evaluate several methods of text steganography on format based techniques. These methods will be examined both from their embedding ratio and saving space ratio of the capacity text.

Therefore, the main objective of this paper is to analyze the capacity performance of text steganography methods based on these two capacity factors. The rest of the paper is organized as follows. First section describes a problem formulation of text steganography. The next section, presents the methods uses on text steganography, capacity factors and dataset uses in this experimental study and followed by the discussion result of the experimental study. Finally the conclusion and summarisation of this paper is discussed at the end of the section.

Text steganography formulation

A general idea of steganography process can be show as in Figure-1.

Figure-1. A general formula of Steganography process.

Firstly, the original message also known as hidden message will be concealed in cover message by applying an embedding algorithm (using key) to produce an embedded message which known as stego text. A sender will send stego text via a communication channel to receiver. Finally, receiver needs to use a recovering algorithm to extract the embedded message to obtain the hidden message. A key is used to control the hiding process so as to restrict detection and/or recover of the embedded data to parties who know it. The relationship of the process can be written as

$$m' = \{m, c, k\}$$

where

m' message that hold the hidden data
m original message or covert message that one wishes to send
c text used to hide the covert message
k function used to hide and unhide the hidden data

A keyword hidden text, cover text, stego key and stego text will be used to represent an original message, cover message, key and embedded message respectively in further discussion. Based on Figure-2, a stego text (m') is obtained by embedding a hidden text (m) within a cover text (c) using a stego key function (k). In this example, the cover text (c) was embedded with a hidden message using a key function. A key function is injected in the embedding process to hide the hidden message to produce a stego text.

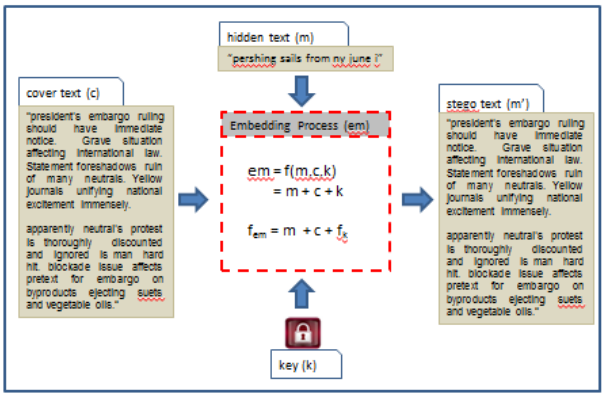


Figure-2. An embedding process of Stego text.

One of the main aspects should be considered when discussing the embedding process of any text steganography methods is the capacity of hidden text and cover text. At least, there are two capacity factors of the hidden text against cover text which are embedding ratio and saving space ratio factors. It is because a better embedding ratio and saving space offers; a more text can be hidden. Then, these factors will determine the capability of the stego text based on the embedding process. Since the capacity of the hidden text and cover text is one of the important factors, several studies have been done in order to measure fitness's performance of text steganography. However, a result shows that only a limited amount of hidden text can be embedded into cover text (Grace, Rao & Kiran, 2012), (Bennett, 2004). Thus, this paper tries to evaluate several methods of text steganography on format based technique such as CALP, VERT and QUAD based (Souvik et al., 2011), (Shraddha, Devesh & Aroop, 2011).

Experimental design

Firstly, this section discusses the design of the model used in text steganography domain. Then, it is followed by the discussion of the selected methods uses in text steganography during embedding process. After that,

the performance of the selected methods will be examined based on their embedding ratio and saving space factors. Finally, their performance will be compared in order to find the best fit performance among each other.

Model design

This study is divided into four steps which started with embedding process of text steganography, following with the methods used on text steganography, the measurement of the capacity factor and ended with the utilization of dataset used. Figure-3 illustrates the design of model used in this study.

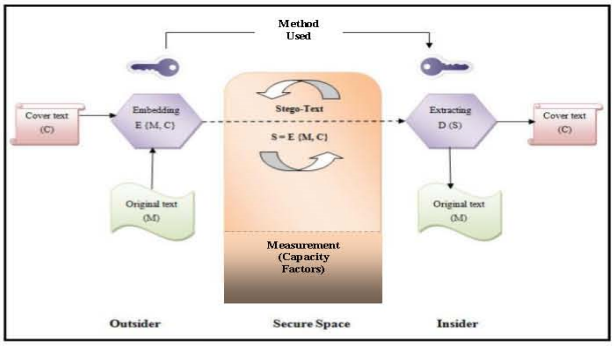


Figure-3. An illustration of model design.

The capacity of hidden text is used to measure the performance of stego text. The more hidden text can be embedded into the cover text will offer a better embedding and saving space ratio. This ratio will be discussed in the next section.

Method used

Three methods have used in this work namely Changing in Alphabet Letter Patterns (CALP), Vertical Straight Line (VERT) and Quadruple Categorization (QUAD). These methods use text file containing hidden text and this hidden text is converted to binary bits before applying in embedding process. CALP method is tries to manipulate English letters by mapping the binary sequence of the hidden text through pattern changes of several letter of the cover text during embedding process. These pattern changes have been incorporated using some unused symbols of the ASCII number system.

Meanwhile, VERT use English letters which divided into two group as shown in Table-2 based on straight vertical line in a characters as the basis to group each letters. The letters contain one vertical straight line is identified as G1 group which will hide 1 bit hidden data. Whereas, a letter contain more than one single line or do not contain a vertical straight line is identified as G2 group will hide 0 bit hidden data.

Table-2. A group of VERT.

Group	Letters
G1	B, D, E, F, I, J, K, L, P, R, and T
G2	A, C, G, H, M, N, O, Q, S, U, V, W, X, Y, and Z

Finally, QUAD method utilizes an English letters into four group based on the letters pattern whether the letter has a curve, middle horizontal straight line, single vertical line or multiple straight vertical line. Each of these group will hide a bits either 00 bits, 01 bits, 10 bits or 11 bits depend on which group of the letter used belongs.

Capacity factor

In this analysis, two factors of the capacity measurement have been used which are Embedding Ratio (ER) and Saving Space Ratio (SSR).

i. Embedding Ratio (ER)

Embedding ratio is used to determine the total fitness of hidden text can be embedded in cover text. This analysis is very important for steganographer to understand the fitness capability of cover text.

$$ER = \left[\frac{Total\ Bits\ of\ Stego\ Text - Total\ Bits\ of\ Cover\ Text}{Total\ Bits\ of\ Cover\ Text + Total\ Bits\ of\ Hidden\ Text} \right] X\ 100\%$$

$$ER = \left[\frac{Total\ Number\ of\ Embedded\ Bits}{Total\ Bits\ of\ Expected\ Stego\ Text} \right] X\ 100\%$$

$$Percent\ Embedded\ Bits\ (\%) = \frac{\sum_{i=1}^{1<m<2000} a_i}{\sum_{i=1}^{1<n<100} b_i} \times 100\%$$

Where

a = Total Number of Embedded Bits
b = Total Bits of Cover Text

ii. Saving Space Ratio (SSR)

Saving space ratio is used to determine the total space of text that can be saved during embedding process in cover text. This analysis is very important for steganographer to understand the capability of maximum space of key used that can be utilized in cover text in order to embed the hidden text.

$$SSR = \left[\frac{Total\ Bits\ of\ Expected\ Stego\ Text - Total\ Bits\ of\ Stego\ Text}{Total\ Bits\ of\ Expected\ Stego\ Text} \right] X\ 100\%$$

$$SSR = \left[\frac{Total\ Number\ of\ Saving\ Space\ Bits}{Total\ Bits\ of\ Expected\ Stego\ Text} \right] X\ 100\%$$

$$Percent\ Saving\ Space\ Bits\ (\%) = \frac{\sum_{i=1}^{1<m<100} a_i}{\sum_{i=1}^{1<n<100} b_i} \times 100\%$$

where

a = Total number of saving space bits

b = Total bits of expected Stego Text

Dataset selection

A text dataset is one of the important components of the benchmarking steganography methods. Therefore, this study uses a dataset of single cover text with various sizes of hidden text. In order to evaluate the text steganography methods, the 710.144 bytes of cover text has been used with the sixteen hidden texts known as single phase as shown in Table-3. The analysis and result will discusses in the next section.

Table-3. The size of cover text and hidden text for single phase.

Phase / Text Types	Single Phase
Cover Text (bytes)	710.144
Hidden Text (bytes)	86, 124, 163, 203, 241, 278, 315, 353, 393, 430, 470, 511, 550, 588, 626, 663

Experimental result

This section described the result of experiment performance on CALP, VERT and QUAD methods based on the aforementioned phases. The discussion of this section is divided into two parts. The first part discusses the distribution of Normal Stego Text (NST) and followed by the comparison of CALP, VERT and QUAD methods based on NST distribution

Distribution of NST

This experiment is to obtain the distribution of NST based on the embedding process of the cover text and the hidden text. NST is the total size of cover text and hidden text of each analysed text by using the embedding formula as shown in Figure-1, where

Hidden Text + Cover Text + Key = Stego Text

In this case, the StegoText is representing NST without using any key value. Table-4 show a part of NST values after embedding process using 9 various size of hidden text with a constant value of cover text size of 710.144.

Table-4. Sample values of NST.

Cover Text	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144
Hidden Text	86	124	165	203	241	278	315	353	391
NST	796.144	834.144	875.144	913.144	951.144	988.144	1025.14	1063.14	1101.14

The next discussion used all sixteen various values of hidden text as shown in Table-3 with a fixed values of hidden text size of 710.144. The distribution of NST values will be compare with the CALP, VERT and QUAD method.

Figure-4 has presented the distribution of NST by using 710.144 bytes of cover text with sixteen various size of hidden text as shown in Table-3. The figure shown that the minimum and maximum size of NST are 796.144 and 1373.144 bytes respectively. It is found that the size of NST consistently increases with the increment in size of hidden text by remaining the size of cover text. The value of each NST was compared with the others performance method (CALP,VERT and QUARD) that will be discuss in the next part.

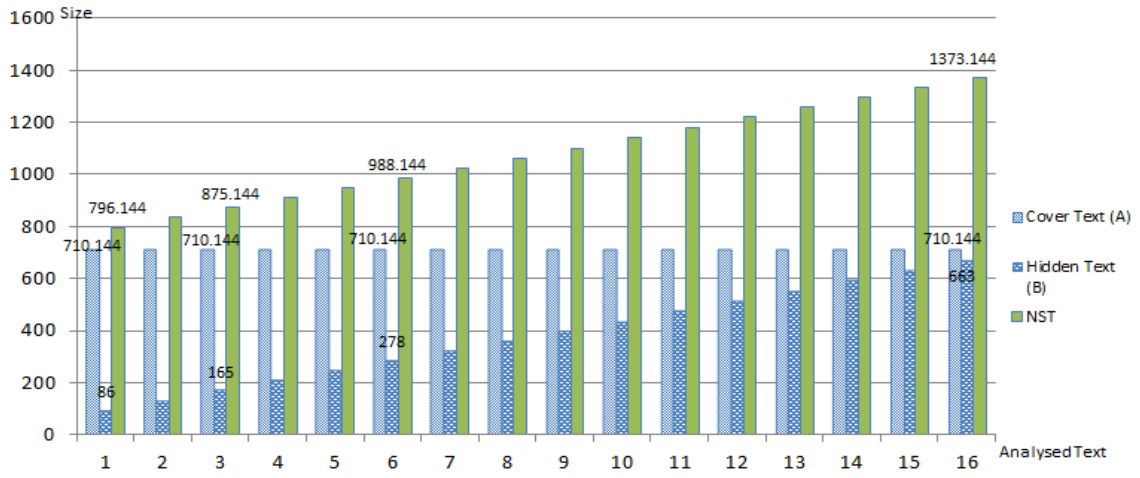


Figure-4. The distribution of NST after the embedding process of Hidden text

.

The performance of methods used

This experiment is to measure the performance of CALP, VERT and QUAD methods compared to the distribution of NST. Figure-4 shows the distribution of stego text using CALP method with the distribution of NST.

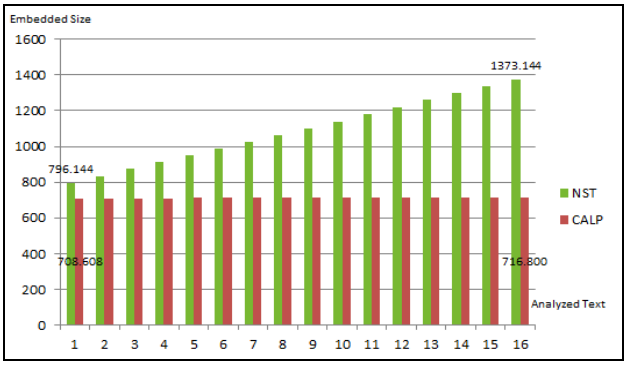


Figure-5. Stego text using CALP method versus NST.

Based on the figure above, the minimum and maximum score of stego text for CALP method are 708.608 and 715.80 bytes respectively. Compared to NST, the minimum and maximum score are 796.144 and 1373.144 respectively. It is found that the distribution of stego text using CALP method varies within the range of 1.15% whereas the distribution of NST gradually increases at almost 72.47% throughout the analysed text. For example, after embedding process, the size of NST using 86 byte of hidden text increases to 796.144, however by using CALP method, the size of stego text decrease to 708.608.
It means that, the CALP method change the size of stego text with a small value compared to NST.

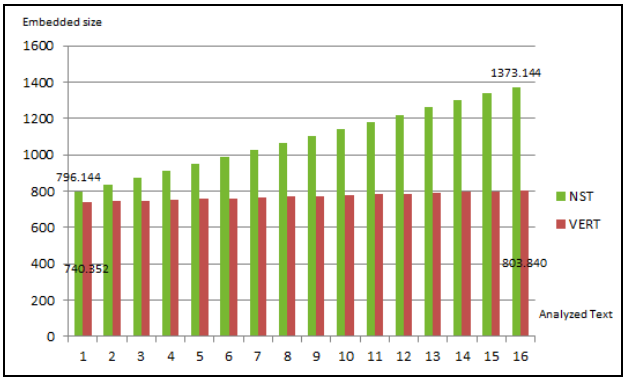


Figure-6. Stego text using VERT method versus NST.

Figure-6 shows the minimum and maximum score of stego text for VERT method is 740.352 and 803.840 bytes respectively while comparing to NST, the minimum and maximum score is 796.144 and 1373.144 respectively. It is found that the percentage ratio of stego text using VERT method maintains at almost 8.58%. Meanwhile, the percentage ratio of NST gradually escalated at almost 72.47% throughout the analysed text.

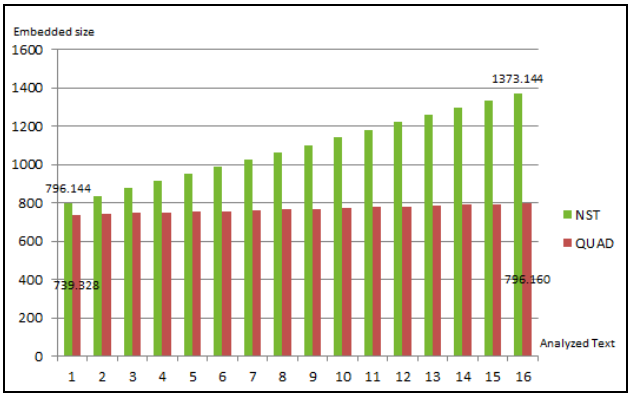
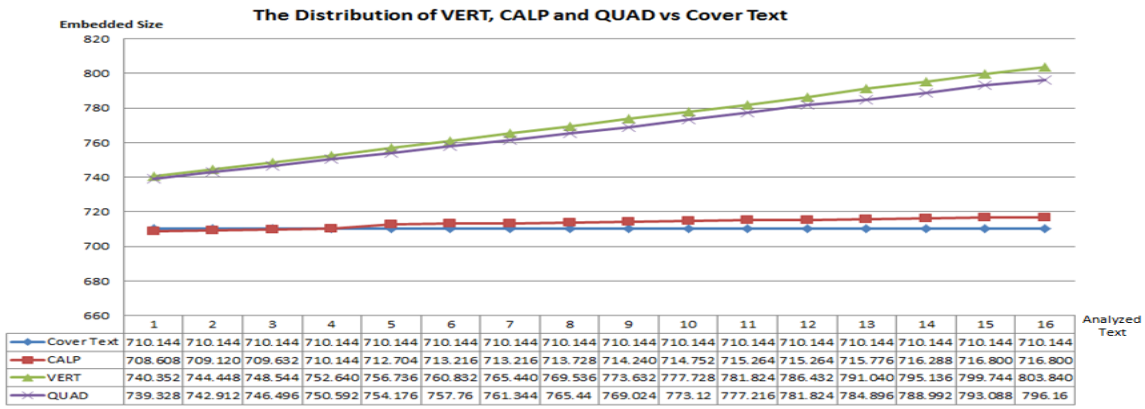


Figure-7. Stego text using QUAD method versus NST.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Cover Text	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144	710.144
CALP	708.608	709.120	709.632	710.144	712.704	713.216	713.216	713.728	714.240	714.752	715.264	715.264	715.776	716.288	716.800	716.800
VERT	740.352	744.448	748.544	752.640	756.736	760.832	765.440	769.536	773.632	777.728	781.824	786.432	791.040	795.136	799.744	803.840
QUAD	739.328	742.912	746.496	750.592	754.176	757.76	761.344	765.44	769.024	773.12	777.216	781.824	784.896	788.992	793.088	796.16

Figure-8. A distribution of VERT, CALP and QUAD versus cover text.

In Figure-7 above, it shows the minimum and maximum score of stego text for QUAD method is 739.328 and 796.160 bytes respectively. In contrast to NST, the minimum and maximum score is 796.144 and 1373.144 respectively. It is observed that the percentage ratio of stego text using QUAD method maintains at almost 7.69%. At the same time the percentage ratio of NST gradually rose at almost 72.47% throughout the analysed text.

FINDING AND DISCUSSION

This section summarizes the finding corresponding to the experimental result. Table-5 has shown the performance of score values between NST and stego text of each methods.

Table-5. Summary of experimental result.

	Min	Max	CALP Method		VERT Method		QUAD Method	
			Min	Max	Min	Max	Min	Max
Normal StegoText	796.144	1373.144	708.608	716.800				
	796.144	1373.144			740.352	803.840		
	796.144	1373.144					739.328	796.160

From the Table-5 it can be concluded that percentage ratio changes of stego text distribution using CALP, VERT and QUAD methods value remains maintain between 1% to 9% from throughout analysed text. However, the percentage ratio changes of NST distribution value dramaticaly increase up to 72.47% throughout analysed text.

Figure-8 shows that the first four distribution of stego text using CALP method was below or equal to cover text size then it started to increase steadily from the fifth to the end of the distribution of stego text using CALP method. In contrast, the distributions of stego text using VERT and QUAD methods were above the cover text size. This shows that the CALP method performed better in the embedding process to produce stego text compared to VERT and QUAD method. It may be influenced by the embedded space of the CALP method is lower compared to the embedded space of the QUAD and VERT methods. However, the performances of these three methods are still lower than NST.

In conclusion, the change in the embedded size remains constant for the three methods when the capacity size for both cover text and hidden text is smaller compared to the capacity size on cover text and hidden text which are big in scale.

CONCLUSIONS

In this paper, three types of text steganography methods have been evaluated. It has been identified that CALP method gives a better effort performance compared to VERT and QUAD method. However, VERT and QUAD methods give a quite similar result for embedding ratio and saving space performance compare to CALP. The results also show that all of the methods are able to perform consistently with the utilization of hidden text and cover text. In future, this paper proposes to evaluate a robustness of each method in order to find a strength capability on text steganography from steganalysis activities.

REFERENCES

Adhiya, K. P. and Swati A. P. (2012). Hiding Text in Audio Using LSB Based Steganography, In Proceeding of Information and Knowledge Management, vol. 2, no. 3, pp. 8-14.

Al-Mualla, M., Al-Ahmad, H. (2013). Information Hiding: Steganography and Watermarking, retrieve from http://emirates.org/ieee/information_hiding.pdf on December 12, 2013.

Baharudin, O., Din, R., Tuan Zalizam, T. M. and Omar, M. N. (2013). A Performance of Embedding Process for Text Steganography Method, In Proceedings of the ISP '13, (12th WSEAS International Conference on Information Security and Privacy), pp.115-119.

Bennett, K. (2004). Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text, Purdue University, CERIAS Tech. Report.

Bodhak, P. V. and Baisa L. G. (2012). Improved Protection In Video Steganography Using DCT & LSB", International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, pp. 31-37.

Cao, Y., Xianfeng, Z. and Dengguo, F. (2012). Video steganalysis exploiting motion vector reversion-based features, Signal Processing Letters, IEEE, vol. 19, no. 1, pp. 35-38.

Chikara, R. and Latika, S. (2013). A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted, International Journal of Engineering and Innovative (IJEIT), vol. 3, no. 4.

Choudhary, K. (2013). Image steganography and global terrorism, IOSR Journal of Computer Engineering, vol. 1, pp. 34-48.

Dasgupta, K., Mandal, J. K. and Paramartha, D. (2012). Hash Based Least Significant Bit Technique for Video Steganography (HLSB), International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 1, no. 2, pp. 1-10.

Din R. (2014). Designing the Key Detection of Text Steganalysis Based, Advanced Science Letters, vol. 20, no. 1, pp.158-163.

Din R., Che Ani, Z. and Azman, S. (2012). A formulation of conditional states on steganalysis approach, In Proceeding of WSEAS Transactions on Mathematics, vol. 11, no. 3, pp. 173-182.

Din R. and Azman, S. (2009). Digital Steganalysis: Computational Intelligence Approach, International Journal of Computers 3, vol. 3, no. 1, pp. 161-170.

Fabien, A., Petitcolas, P., Ross, J. A., and Markus G. K. (1999). Information Hiding-A Survey, In Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, pp. 1062-1078.

Gardiner, J. (2014). StegChat: A Synonym-Substitution Based Algorithm for Text Steganography, Retrieve from http://www.cs.bham.ac.uk/~nagarajs/papers/J.gardiner-MScReport.pdf.

Govada, S. R., Bonu, S. K., Manjula, D. and Meka, J. S. (2012). Text Steganography with Multi level Shielding, International Journal of Computer Science Issues (IJCSI), vol. 9, issue 4, no. 3, pp. 1694-0814.

Grace, M. V., Rao, M. S. and Kiran, J. S. (2012). Hiding the Text Information Using Stegnography, International Journal of Engineering Research and Applications (IJERA), vol. 2, Issue 1, pp. 126–131.

Gunawardena, S., D. Kulkarni, and Gnanasekaraiyer, B. (2013). A Steganography-based framework to prevent active attacks during user authentication", In proceeding of the ICCSE (8th International Conference of Computer Science & Education) on IEEE, pp. 383-388.

Hamid, N., Abid, Y., Badlishah, A. R., and Al-Qershi M. O. (2012). Image Steganography Techniques: An Overview", International Journal of Computer Science and Security(IJCSS), vol. 6, no. 3, pp. 168.

He, L., Xiaolin, G., Reifeng, W., Biqing, X. and Chang H. (2012). A Hybrid Natural Language Information Hiding System, Research journal of Elektronika Ir Elektrotechnika, vol. 18, no. 9, pp. 95-100.

Kaleem, M. K. (2012). An Overview of Various Forms Of Linguistic Steganography And Their Applications In Protecting Data, Journal of Global Research in Computer Science, vol. 3, no. 5 pp. 33-38.

Kaur, B., Pooja, N. and Harish, K. (2013). Steganography Techniques: Concepts and Overview, International Journal of Computer Science and Communication Engineering (IJCSCE), vol. 2, 2013.

Kodovsky, J., Jessica F. and Vojtech H. (2012). Ensemble classifiers for steganalysis of digital media, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 432-444,.

Majercak, D., Vladimir, B., Martin, B., Gabriel, B. and Dusan, L. (2013). Performance evaluation of feature-based steganalysis in steganography, In proceeding of Radioelektronika, (IEEE 23rd International Conference on Radioelektronika), pp. 377-382.

Mansor, S., Din, R. and Azman S. (2010). Analysis of Natural Language Steganography, International Journal of Computer Science and Security (IJCSS), vol. 3, no. 2, pp. 113.

Nutzinger, M. (2012). Real-time attacks on audio steganography, Journal of Information Hiding and Multimedia Signal Processing, vol. 3, no. 1, pp. 47-65.

Shraddha, D., Devesh, J. and Aroop D. (2011). Experimenting with the Novel Approaches in Text Steganography, International Journal of Network Security and Its Applications (IJNSA), vol. 3, no. 6.

Si, H. and Li, C. (2008). Maintaining Information Security in E-Government through Steganology, Department of Computer Science, University of Warwick, UK.

Singh, P., Rajat, C., and Agarwal, A., (2012). A Novel Approach of Text Steganography based on null spaces, IOSR Journal of Computer Engineering (IOSRJCE), vol. 3, no. 4, pp. 11-17.

Sharma, P. and Shweta, G. (2013). Steganography Techniques, International Journal of Engineering, vol. 2, no. 4.

Souvik, B., Pabak, I., Sanjana, D., Indradip, B. and Gautam S. (2011). Hiding Data in Text Changing in Alphabet Letter Patterns, Journal of Global Research in Computer Sciences, vol. 2, no. 3.

Vahedi, E., Vincent, W.S. and Ian F. B. (2014). An Overview of Cryptography, in Crisis Management: Concepts, Methodologies, Tools and Applications, IGI Global, USA.

Wang, C. and Jiangqun, N. (2012). An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients, In proceeding of the ICASSP (IEEE International Conference on Acoustics, Speech and Signal Processing), pp. 1785-1788.

Yusuf, P., Firoj, P. and Asif, P. (2012). An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection, The International Journal of Multimedia & Its Applications (IJMA), vol. 2, pp. 21-38.

Zamani, M., Azizah A. M. and Shahidan, M. A. (2012). Efficient Embedding for Audio Steganography, In proceeding of the EDSCM (2nd International Conference on Environment, Economics, Energy, Devices, Systems, Communications, Computers, Mathematics), pp. 195-199.