4th International Conference on E-Commerce
ICoEC 2017
18-20 SEPTEMBER 2017. PUTRAJAYA, MALAYSIA

Critical Review of Verification and Validation Process in Feature-Based Method Steganography

Roshidi Din*, Sunariya Utama
School of Computing, UUM College Arts and Sciences, Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia

***Abstract**: This paper presents about evaluation measurement through verification and validation in one category of steganography specifically in text domain. It reviews the one of method in text steganography which named feature-based. This method had been developed by previous researcher that to cover hidden message based on uniqueness of letter. Then, the implementation feature-based able to use in several language and a lot of technique possible to paper identifies what kind the measurement that had been used developed as the feature-based method of text steganography.*

Keywords: Text steganography, Feature-based, Verification, and Validation

1. INTRODUCTION

The text document has become one of the important medium that had been established. The needs of text documents are still high especially in the domain of business and academic. It is because a lot of important documentation such as appointment letter, certification, report, confidential document and many any other documents are available in text. The irresponsible intruders may disclose the information to uninvolved parties to check or modify it for abusing that information (Amin et al., 2003). Therefore, text documents should be a concern for most people due to them are exposed to a lot of risks. One of the categories of information security named steganography.

Steganography is known as an associated knowledge of hiding the messages via medium of data to become invisible and undetectable for human sense. Secure private information is critical point of steganography in applying performance as part of information hiding (Iyer & Lakhtaria, 2016). The implementation of steganography itself is divided into two categories. The following Fig1 illustrates various categories of steganography and the focus path of this paper.

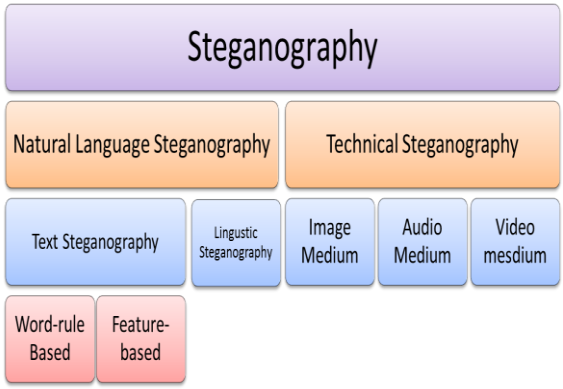

Fig1. Major categories of steganography

Based on Fig 1 is showed the categories in steganography. The first is known as technical steganography which is implemented in other medium such as images, audios, videos and other digitally invisible codes. Secondly is the natural language steganography whereby the implementation of steganography is done in medium of text. The implementation of natural language steganography involves hiding the hidden message in medium of text so that the third party is unable to discover the existences of message in text. In other words, steganography in medium of text can make the secret information invisible and unnoticed for third party to see or detect, and it is directed

* Corresponding author. Tel.: +604-9285003; Fax: +604-9285018.
E-mail: roshidi@uum.edu.my

to the appropriate receivers to apprehend the information. In natural language steganography, there are two other sub-categories. The first is linguistic steganography. This type of steganography is dependable with linguistic order of sentence in the text. The second is text steganography that manipulates the component of text such as word, line, space and other component of text in order to hide the message (Nasab & Shafei, 2011).

This paper focuses on one text steganography category that named feature-based. Feature-based is a method which alters the feature of letter by manipulating in the shape, size, and position of font in the text. Feature-based technique makes the reader difficult to recognize the hidden information in this text. The technique of feature-based make the reader cannot recognize the secret information in this text (Roy & Manamisti, 2011).

However, this paper would elaborate the important think to obtained performance specific requirement of methods is measurement part. The measurements are verification and validation process that used to provide the simpler proofs that a method could achieve in developing system.

This paper is focus on the verification and validation which implemented feature-based method of part technique in text steganography. The several categories parameter verification and validation described in next section

2. IMPLEMANTATION VERIFICATION AND VALIDATION MEASUREMENT

The verification and validation process are used to provide the simpler proofs that a method could achieve better performance in developing system. The verification process is determining the input variables, when the system due process or stop, and the output (Das et al.,2012) Some previous researchers used the measurement of verification in order to measure their study with some parameters.

Wu and Yang (2013) proposed verification measurement in order to reestablishment the interval of algorithm. This measurement checked the presence of algorithm through decoding packet-based codes with compressed sensing via density evaluation.

Useneret al. (2010) developed the software verification proofs in order to supported computer assessment. This software verification could obtain direct pre-evaluation on prospective error assessment in source code.

Meanwhile, validation is generating the expected output from testing process that can prevent problem in systems or applications (Ling, Chen & Liu, 2010)

Arora, Raghunathan, and Jha (2005) evaluated run-time of security program data properties in order to develop framework security assurance towards a wide class of security attack.

Cruickshank, Michael, and Shing (2009) used the validation measurement in software safety requirement in order to validate the development of system protection requirement software. The parameter of validation used for software safety requirement for identify the number of software resultant.

Those are the previous research effort development that using measurement through verification or validation. The function of measurement is to predict the description criteria quality of requirements that will be used in developing the system. There are two kinds of measurement in evaluating performance pf any method which are verification and validation. In general, verification and validation are determined the relation between model and the derived from procedure for several purposes (Sergeant, 2012). Next section elaborated the categories of parameter in verification or validation approach.

3. PARAMETER METRIC USED IN VERIFICATION AND VALIDATION

There are some several of parameter metric in verification and validation that used obtained the result of process in the system. There are some parameter matric able to implements in text steganography, specifically in feature-based method. In verification the parameter metric used show in Table 1 as follows.

Table 1. Parameter metric verification process

No	Verification Metrics	Scholar Sources	Review
1	Correctness input data	(Daso&Funnes, 2007; Oberkampf & Roy, 2010)	It determines the accuracy of data input design that used for experimental design. This analysis is very important in order to ensure the availability of the input data that can be used in the technique. The technique verification that can aid in input data is with check consistency in using model cover text, hidden message and stego key.
2	Presence algorithm	Daso&Funnes, 2007; Catal, 2012; Oberkampf & Roy, 2010)	Presence algorithm is ascertains the availability of the obtained technique in order to develop system in process design. In this research, embedding through the stego key used is the algorithm experimental. Thus, verification in algorithm use will be to make construct synchronous encrypting cover text and hidden message in embedding process and decrypting in the embedding process.
3	Loading velocity	(Oberkampf & Roy, 2010)	Loading velocity is used to determine speed of each technique in embedding process the algorithm hidden message and also check of the speed of normal input environment to get normal text.
4	Examine process evaluation	(Oberkampf & Roy, 2010)	Examine process simulation verification involves type of numerical errors in order to verify the accuracy tools in simulation. These verification measurements will facilitate the process in generating output in form of clear text or stego text in the system.
5	Correctness output data	(Daso&Funnes, 2007; Oberkampf & Roy, 2010; Catal, 2012)	Correctness output data used to determine the correctness the post process simulation in the system. Thus, the output data have to be similar with the input data in experimental design.
6	Contain letter dataset	(Satir&Iskik, 2012)	Contain letter used in order to determine the total number of character cover text, hidden message and stego text. It used to measure the length character datasets.
7	Capacity size dataset	(Majerjak et al., 2013)	Capacity input datasets used determine the size bit of dataset. In text steganography, it can figure out the total size of cover text and hidden message.

Table 1 has showed the the possible of the verifation parameter metric in order to obtain the variable requirement of model in the system.

Meanwhile, Table 2 presented the parameter metric that able can used in validation measurement in order obtain validated result.

Table 2. Parameter metric validation process

No.	Validation Metrics	Scholar Sources	Review
1	Running Time	(Daso&Funnes, 2007; Oberkampf & Roy, 2010; Catal, 2012)	The purpose of running time measurement is to measure the speed of the techniques in how consuming time in process embedding hidden message of feature-based technique. The running time is depending on input rate growth of time.
2	Precision rate	(Daso&Funnes, 2007;Oberkampf & Roy, 2010; Catal, 2012)	The purpose of precision rate is to measure accuracy a definite data system that has been predicted. This parameter measurement is based on four possible outcomes (Kohari& Goyal, 2013; Fawcett 2005). These outcomes are: o *True positives (TP)* When hidden texts that are correctly embedded as stego text. o *True negatives (TN)* When hidden texts that are correctly embedded as non-stego text. o *False negatives (FN)* When hidden text that are incorrectly detected as non-stego text. o *False positives (FP)* When hidden text that are incorrectly detected as stego text. These are outcomes also use in other parameter measurements.
3	Accuracy rate	(Daso&Funnes, 2007;Oberkampf & Roy, 2010; Catal, 2012)	The purpose of accuracy value is measured as arrangement closeness between values that get from technique reference and value obtained by alternative technique.
4	Recall rate	(Daso&Funnes, 2007;Oberkampf & Roy, 2010; Catal, 2012)	The purpose of recall rate is to measure prediction model in set of data and calculate the probability of detection or sensitivities in the text.
5	F-measure rate	(Daso&Funnes, 2007; Catal, 2012; Fawcett, 2005; Oberkampf & Roy, 2010)	The purpose F-Measure rate is to evaluate the performance of embedding and analyzing text for determines to obtain stego text as the output.
6	Correctness output data	(Daso&Funnes, 2007; Oberkampf & Roy, 2010; Catal, 2012)	The accuracy rate is measured as arrangement closeness between values that is generated from technique reference and value obtained by alternative technique.

No.	Validation Metrics	Scholar Sources	Review
7	Statistical possibility	(Daso&Funnes, 2007; Oberkampf & Roy, 2010; Catal, 2012)	There are three parameter metrics to measure inside statistical probability those o Means is to estimate the comparison the computational result with measurement of experimental that considered for prediction accuracy. o Variance is to measure dissemination variable in sample data and delivers the accuracy points of each data. o Standard deviation is to concentrate on average length sample data in each point in order to get original measurement units.

Table 2 has presented the parameter metric that able can used in validation measurement in order obtain validated result.

4. VERIFICATION AND VALIDATION IN TEXT STEGANOGRAPHY

Evaluations of verification and validation process are used to provide the simpler proofs that a method could achieve in developing system. Based on the last decade, the review of implementation feature based text steganography that used evaluation performance through verification and validation processes shown in Table 3 as follows.

Table 3.The evaluation that used in feature-based methods

Feature-based technique	Evolution used		Reviews
	Verification	Validation	
Watermarking based on occlusive in Chinese text (Zhang et al., 2006)	√	-	The technique they are used verified the component, Chinese letter, watermarked hosted rectangular and any other component.
Reversed Fatah in Arabic. (Memon, Khowaja & Kazi, 2008)	√	√	They verified the algorithm used in order to embed binary bits. However, only calculation capacity was used for validation measurement based on stego text and hidden message
Feature coding Indian language (Ghosh & Debnath, 2010)	√		Their study verified model sequence algorithm for embedding binary bits.
Re-Evaluating Chain Code (Alam & Naser, 2013)	-	√	The technique using ANOVA measured variance, standard deviation and F-measure.
ECR (Kateria et al., 2013)	-	√	The technique used only validates the capacity ratio and running time overhead this technique.
Right-to-Left remark and *Left-to-Right* remark (Odeh, Elleite & Faizypour, 2013)	-	√	The study showed the validation of capacity web page for hiding data and total capacity ratio.
Microsoft Word symbol Steganography (Odeh, Elleite, & Faizypour, 2014)	-	√	The discussion on their study showed the validation of total calculation capacity carrier file, capacity ratio and also the show the comparison total of stego text that had been embedded in some news text.
Change alphabet letter pattern (Battacharya et al., 2011)	-	√	The technique their used were measured validation of technique through correlation-coefficient and Jarowinkler distance.
Hypertext markup language (Mahato, Yadav & Khan, 2013)	√	-	The obtained technique introducing and verified the technique with converting algorithm into programing language (HTML).
Email based high Capacity (Kumar, Chand & Singh, 2014)	-	√	The study about this technique only validate the measurement of running time and capacity of the system based on stego text and hidden message.

Based on Table 3, it is shown that three techniques from the previous study have used the verification evaluation and only one used both of the verification and validation evaluation.

5. CONCLUSION

This paper is present the feature-based method of text steganography domain. Then, it elaborates and discusses several parameter metric that use in the verification and validation evaluation of the text steganography domain. This paper also

obtained some proposed technique that used verification or validation evaluation. The primary contribution of this paper is to give a new light on verification and validation approach which in returned would contribute to text steganography domain. Thus, it is expected that a good evaluation performance will be produced in a near future through this paper.

ACKNOWLEDGEMENTS

This research was financially supported by the Fundamental Research Grant Scheme (FRGS), MOHE under RIMC Grant (SO Code: 13576), Universiti Utara Malaysia.

REFERENCES

Alam, M. N. & Naser, M. A. (2013). Re-evaluating Chain-Code as A Feature Bangla Script. *2013 International Conference on Electrical Information and Communication Technology (EICT),* 1-5.

Arora, D., Raghunatan, A., & Jha, N. K. (2005).Enhancing security through hardware-assisted run-time validation of program data properties. *International Conference on Hardware/Software Codesign and System Synthesis,* 190-195.

Bhattacharya, S., Indu, P., Duta, S., Biswas, A., & Sanyal, G. (2011) Hiding data in text through in alphabet letter patterns (CALP). , *Journal of Global Research in Computer Science, 2*(3), 33-39.ISSN-2229-371X.

Das, H., Jafarpour, A., Orlitsky, A., Pan, S., Suresh, A. T. (2012).On The Query computation and verification of functions.*2012 IEEE International Symposium on Information Theory Proceeding, 2711-2715*.

Dasso, A. & Funes, A. (2007), *Verification, validation, and testing in software engineering.* London: Idea Group Publishing.

Din, R., Samsudin, A. & Lertkrai, P. (2012). A framework component for natural language steganalysis. *International Journal of Computer Theory and Engineering, 4*(4), 641-645.

Fawcett, T. (2005).An Introduction to ROC analysis. *Science direct Pattern Recognition 27,* 861-874.

Iyer, S. S. & Laktharia, K. (2016).New robust and secure alphabet pairing text steganography algorithm. *International Journal of Current Trends in Engineering & Research (IJCTER), 2*(7), *15-21*.

Kataria, S., Sing, K., Kumar, T., & Nehra, M. S. (2013). ECR (Encryption with Cover Text and Reordering) based text steganography. *Proceeding of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013),* 612-616.

Kumar, R., Malik, A., Singh, S. & Chand, S. (2014) A high capacity email based text steganography scheme using huffman compression. *3rd International Conference on Signal Processing and Integrated Networks (SPIN), 53-56*.

Ling, J., Chen, J., & Liu, C. (2008).An automatic mechanism for adjusting validation function.*22nd International Conference on Advanced Information Networking and Applications,* 602-607.

Mahato, S., Yadav, D. K., & Khan, D. A. (2013).A modified approach to text steganography using HyperTextmarkup language.*2012 Third International Conference on Advanced Computing & Communication Technologies,* 40-44.

Majerjak, D., Banoci, V., Broda, M., Bugar, G., & Levicky, D. (2013).Performance evaluation of feature-based steganalysis in steganography.*2013 Conference Radioelectronika,* 377-382.

Memon, J. A., Khowaja, K., & Kazi, H. (2008).Evaluation of steganography for Urdu/Arabic text. *Journal of Theoretical and Applied Information Technology,* 232-237.

Nasab, M., V. & Shafiei, B., M. (2011).Steganography in programming. *Australian Journal of Basic and Applied Sciences*, *5(12),* 1496-1499.

Oberkampf, W. L. & Roy, C. J. (2010).*Verification and validation in scientific computing*. New York: Cambridge University Press.

Odeh, A., Khaled, E., & Feazipour. (2013). Text steganography using language remarks.*2013 ASEE Northeast Section Conference,* 1-7.

Odeh, A., Elleithy, K., & Faezipur, M. (2014). Steganography in text by using MS Word symbols. *Proceeding of zone 1 conference of the American Society Engineering Education,* 1-5.

Satir, E. & Iskik, H. (2012).A Comparison-based on steganography method.*Journal of System and Software,* 85(10), 2385-2394.

Userner, C. A., Gruttman, S., Majchrzak, T. A., & Kuchen, H. (2010). Computer-supported assessment of software verification proof. *International Conference on Educational and Information Technology (ICEIT 2010),* 115-121.

Wu, X & Yang, Z. (2013).Verification-based interval-passing algorithm for compressed sensing. *IEEE Signal Processing Letters, 20 (10),* 934-936.

Zhang, W., Zheng, Z., Pu, G., & Zhuo, H. (2006). Chinese text watermarking based on occlusive components. *2nd Information and Communication Technologies (ICTTA), 1*, 1850-1854