Analysis Review of Feature-Based Method in Term of Verification and Validation Performance

Roshidi Din, Sunariya Utama
School of Computing UUM College Arts and Sciences, Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia.
roshidi@uum.edu.my

***Abstract*—The categories of information named steganography has become the options of securing hidden message that wouldn't be detected by intruders or third party. Implementation steganography able to develop in several domains and this paper focuses on text domain of steganography. This paper particularizes the implementation one of the category of steganography in text domain that measures the evaluation performance through verification and validation approaches. It reviews one of the methods in text steganography called feature-based. This method has been established by previous researcher effort that to cover hidden message based on characteristic of letters in the text. This paper identifies the type of measurement that has been used developed as the feature-based method of text steganography. It anticipated the identification of evaluation performance through verification and validation can able to use as procedure the measurement performance in steganography implementation.**

***Index Terms*—Natural Language Steganography; Text Steganography; Evaluation Performance; Parameter Metric.**

I. Introduction

The influence of text document is critically important media that has been recognized in any domain such as business and academic. Most important documentation such as appointment letter, certification, report, confidential document and other documents are existing in text domain. The irresponsible invaders possibly reveal the important message to uninvolved parties to modify it for abusing that messages [1]. Therefore, text documents should be a concern for most people due to them being exposed to a lot of risks. For example, the intruders can occasionally temper with information in these documents for their own interests. The text document which commonly contains confidential information becomes their target in order to discover the secret information which could be used for prohibited purposes. One of the categories in information security named steganography is proposed to overcome the issue in this paper.

Steganography is art and science implementation knowledge of hiding the messages via medium of data to become invisible and undetectable to human sense. Protected private information is a critical point of steganography in applying performance as part of information hiding [2]. The execution of steganography performance is divided into two main categories. The following Figure 1 exemplifies steganography category and the focus path of this paper.

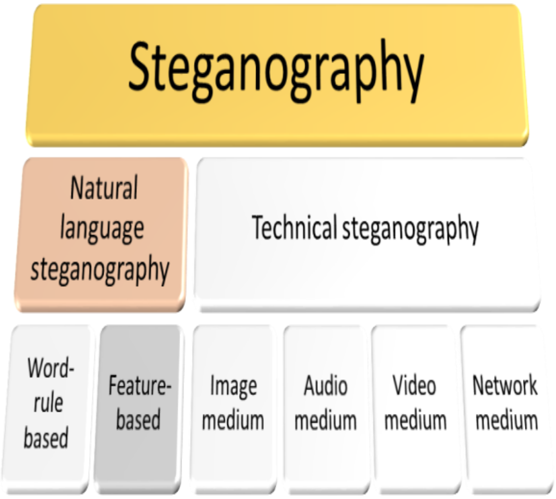


Figure 1: Major categories of steganography

Based on Figure 1 it is shown that there are to the categories in steganography. The first is known as technical steganography which is implemented in other media such as images, audios, video, network performance and other digitally undetectable codes. Secondly is the natural language steganography in which 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 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 [3].

This paper focuses on one text steganography category is named feature-based. Feature-based is a method which alters the feature of letter by manipulating the shape, size, and position of font in the text. This technique covers hidden message based on pattern letter or length of the word that conceals and seem nothing changes happen in the text [3]. It makes the reader difficult to recognize the hidden information in text as well as unable to recognize the secret information in this text [4].

It also elaborates the substantial object to acquired performance specific requirement of methods is measurement part. The evaluations are verification and validation process that used to provide the simpler proofs that a method could achieve in developing the system. The majority of development is used evaluation phase that is illustrated in Figure 2 as follows.

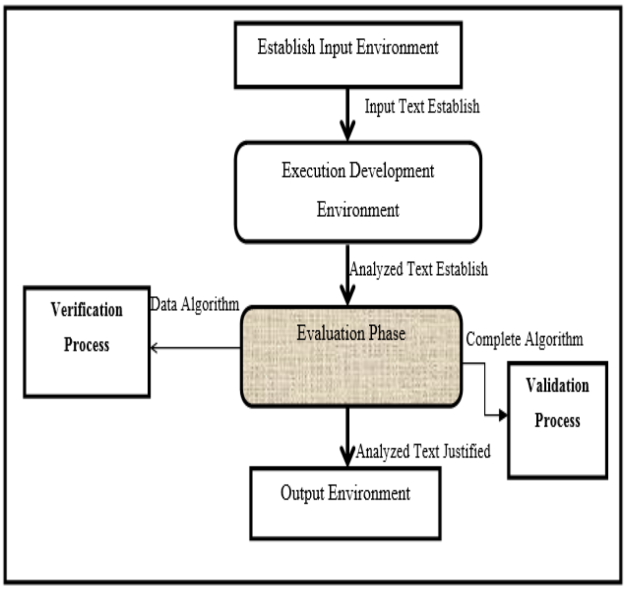


Figure 2: Major Design of evaluation procedures in process development

Figure 2 shows most of researcher effort in procedure of design development of system. This paper focuses on the verification and validation which implemented feature-based method of part technique in text steganography. It specified the evaluation phased implement after the development process in order to acquire the output of the system.

Therefore, evaluation performance especially through verification and validation approaches is necessary to obtain the proper output result. Several categories parameter verification and validation will be described in next section.

II. Evaluation through Verification and Validation Performances

The important thing in order to fulfil essential and specific requirement of methods is the evaluation procedures. The function of evaluation is to predict the quality of requirements that will be used in developing the system. There are two vital procedures in evaluating performance of any method which are verification and validation. In general, verification and validation are determined by selecting relationship between models derived from several producers [5]. Verification and validation process are used to provide the simpler proofs that a method could achieve better performance in developing system.

The verification and validation processes are used to provide simpler proofs so 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. Verify the requirement exceptionally important to prevent expense impact and build the framework system [6]. Besides that, Ghuman and Lassig [7] used verification measurement for requirements of system and application in approving correctness evaluation of the system in data source and for checking the model of systems. Then, Alves et al. [8] also identify requirement system using verification process for gathered data in order to observe behaviour of system in executed simulation process. Then, Rogovchenko et al. [9] used verification for formulizing requirement for identifying relationship to fulfil each requirement that can be used through in simulation.

Verification can define the implementation of the correct model. According to Xinhua et al. [10] that developed model verification for verifying the structure of process in each rule for checking possible problem through evaluating matching rules and the fact of the process. Then, Sergeant [5] confirmed computerized model verification by determining measurement of program computer is correct to implement. Moreover, Chen et al. [11] using verification task for applied model perform verified that provided useful insight system to design the system. Some previous researchers used the measurement of verification in order to measure their study with some parameters.

Wu and Yang [12] proposed verification measurement in order to reestablishment the interval of the algorithm. This measurement checked the presence of algorithm through decoding packet-based codes with compressed sensing via density evaluation. The main objective of this verification efficiently implemented the better performance algorithm and lowered complexity in process decoding simulation.

Usener et al. [13] 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. The verification processes measured the algorithm and logic source code using some transformation rules such as rule for skip, rule for assignments, rule for sequencing, rule for conditionals, rule for while loops. This verification anticipated can prevent time-consuming during process assessment in computer support.

Rahmat, Kamel and Yahya [14] investigated the correctness data in signature of sensor performance. The technique of verification involved four phases of measurement. First, data acquisition is recycled as input device sensor. Second, feature extraction is consideration of extracted the data glove. Third, matching is used to measure the similarity input feature and identity model. Fourth, the decision is to imply the calculation of a decision threshold when matching gets similarity.

Those are some researcher effort that used evaluation verification approach in order to verify the performance in some area research domain. Besides, various researchers also used some validation in order to evaluate the output system. According to Marincic et al. [15] that performed validation for design element in the structured model is based on verification activities and validate confidence with verification result. Then, Sergeant et al. [5] defined validation as the substation that model on computerized applicability keeps acceptable range accuracy consistent with the envisioned application of the model in the domain.

Validation can guarantee the final system reflect directly encouragement constancy and quality for established requirement in delivering the system [8]. Then, validation through testing assured representative of an expected outcome or result. According Ling et al. [16] used validation testing functionalities and error point with analyzing input system to check construction system from the beginning.

Arora, Raghunathan, and Jha [17] evaluated run-time of security program data properties in order to develop framework security assurance towards a wide class of security attack. The run-time security data validated in order to ascertain compilation and execution time in software security for preventing time-consuming in memory requirement software. Then, this kind of evaluation is useful for enhancing the development of performance system is more accurate and faster.

Cruickshank, Michael, and Shing [18] 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 was Rapid Action Surface to Air Missile (RASAM) metric for identifying the number of software resultant. This parameter determined percentage software to assume as the software system success and percentage software safety requirement to utilize the set similarity of a software-intensive system.

Those are the past scholar's effort implementation using evaluation process 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 of any method which are verification and validation. In general, verification and validation determine the relation between model and they derived from the procedure for several purposes [8]. It elaborates the categories of the parameter in verification or validation processes in the next section.

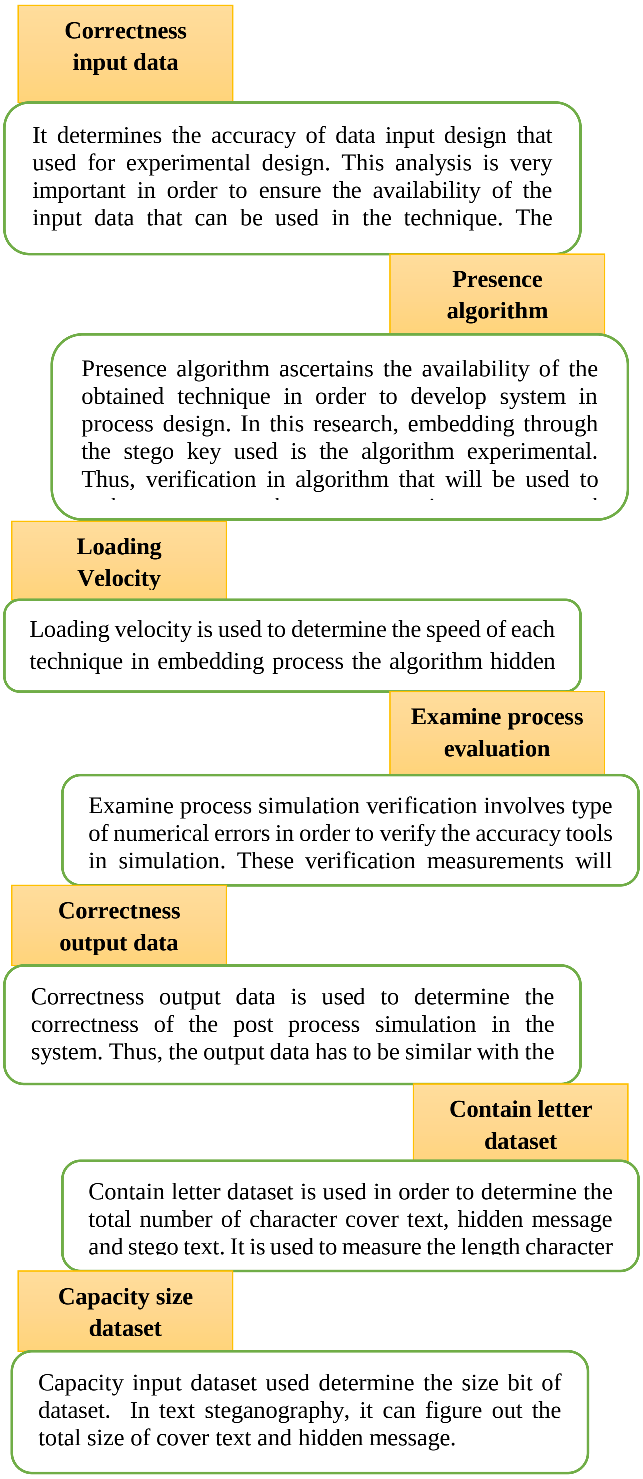
III. Parameter Verification and Validation Performances

There are several parameters metric in verification and validations that are used obtain the result of the process in the system. There are some parameters metric that are able to be implemented in text steganography, specifically in the feature-based method. In verification the parameter metric reviewed are correctness input data, presence algorithm, loading velocity, examine process evaluation, correctness output data, contain letter dataset, and capacity size dataset. Those some parameter in verification that able to demonstrate in evolution procedure of the text domain.

Meanwhile, validation the parameter metric that reviewed such as; running time, presence algorithm, accuracy rate, recall rate, f-measure rate, and statistical possibility. First, the description of verification performance that has reviewed is shown in Figure 3.

Figure 3 shows the possibility of the verification parameter metric in order to obtain the variable requirement of the model in the system. Next, there is parameter metric of validations which able to use in text steganography show in Figure 4 as follow.

Figure 4 illustrated some parameter that can use invalidation process. Generally, validation is generating the expected output from a testing process that can prevent the problem in systems or applications [16]. These parameter metrics that had been used by some researchers in the system developed. The parameter metric that has been validating in the system is deserved to use after developing the technique in evaluation performance.



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

Presence algorithm 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 that will be used to

Loading velocity is used to determine the speed of each technique in embedding process the algorithm hidden

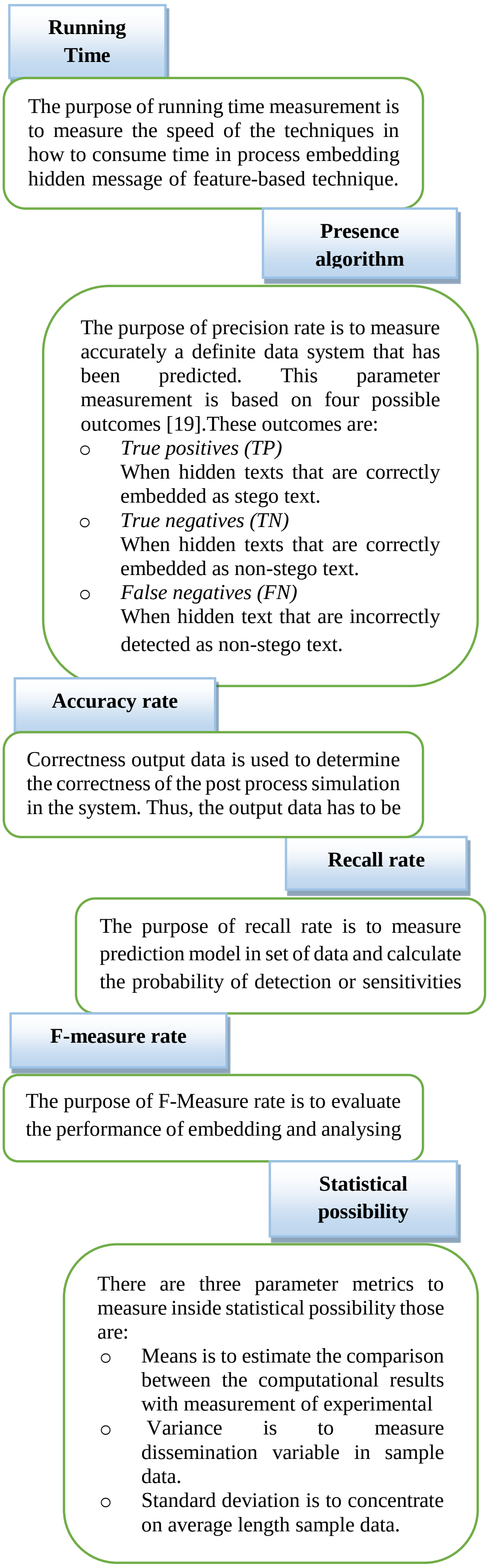
Examine process simulation verification involves type of numerical errors in order to verify the accuracy tools in simulation. These verification measurements will

Correctness output data is used to determine the correctness of the post process simulation in the system. Thus, the output data has to be similar with the

Contain letter dataset is used in order to determine the total number of character cover text, hidden message and stego text. It is used to measure the length character

Capacity input dataset used determine the size bit of dataset. In text steganography, it can figure out the total size of cover text and hidden message.

Figure 3: Parameter metric verification process



Running Time

The purpose of running time measurement is to measure the speed of the techniques in how to consume time in process embedding hidden message of feature-based technique.

Presence algorithm

The purpose of precision rate is to measure accurately a definite data system that has been predicted. This parameter measurement is based on four possible outcomes [19].These outcomes are:

- *True positives (TP)*
  When hidden texts that are correctly embedded as stego text.
- *True negatives (TN)*
  When hidden texts that are correctly embedded as non-stego text.
- *False negatives (FN)*
  When hidden text that are incorrectly detected as non-stego text.

Accuracy rate

Correctness output data is used to determine the correctness of the post process simulation in the system. Thus, the output data has to be

Recall rate

The purpose of recall rate is to measure prediction model in set of data and calculate the probability of detection or sensitivities

F-measure rate

The purpose of F-Measure rate is to evaluate the performance of embedding and analysing

Statistical possibility

There are three parameter metrics to measure inside statistical possibility those are:

- Means is to estimate the comparison between the computational results with measurement of experimental
- Variance is to measure dissemination variable in sample data.
- Standard deviation is to concentrate on average length sample data.

Figure 4: Parameter metric validation process

IV. Performance Verification and Validation in Feature-Based Text Steganography

The important thing in order to fulfill the essential and specific requirement of methods is the evaluation procedures. The function of evaluation is to predict the quality of requirements that will be used in developing the system. Measurements of verification and validation processes are used to provide the simpler proofs that a method could achieve in developing the system. Based on the last decade, the review of implementing feature-based text steganography that used evaluation performance through verification and validation processes is shown in Table 1 as follows.

Table 1
The evaluation that used in the feature-based method

Feature-based technique	Evaluation approach		Description
	Ver	***Val***	
Watermarking based on occlusive in Chinese text [20]	**Yes**	**No**	The technique that verified the component, Chinese letter, watermarked hosted rectangular and any other component.
Reversed Fatah in Arabic. [21])	**Yes**	**Yes**	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 [22]	**Yes**	**No**	Their study verified model sequence algorithm for embedding binary bits.
Re-Evaluating Chain Code [1]	**No**	**Yes**	The technique used ANOVA measured variance, standard deviation and F-measure.
ECR [23]	**No**	**Yes**	The technique used only validates the capacity ratio and running time overhead this technique.
Right-to-Left remark and Left-to-Right remark [24]	**No**	**Yes**	The study showed the validation of capacity web page for hiding data and total capacity ratio.
Microsoft Word symbol Steganography [25]	**No**	**Yes**	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 [26]	**No**	**Yes**	The technique used was measured validation of technique through correlation-coefficient and Jaro Winkler distance.
Hypertext markup language [27]	**Yes**	**No**	The obtained technique introduced and verified the technique by converting the algorithm into programing language (HTML).
Email based high Capacity [28]	**No**	**Yes**	The study about this technique only validated the measurement of running time and capacity of the system based on stego text and hidden message.

**Ver = Verification, Val = Validation*

Based on Table 1 is clearly seem in the description which is a parameter that used in measured the feature-based method. This study simplifies the criteria the measurement which is the group verification or validation because those researchers only mention the parameter used. The most of techniques used validation measurement in order to validate the developed technique of feature-based in text steganography. Meanwhile, the three techniques from the previous study that used verification measurement and only one technique developed both of measurement in term of verification and validation.

V. Conclusion

This paper has discussed one of the domain one methods of text steganography, which is feature-based. This method elaborates the measurement of several other proposed methods through verification and validation approaches. There are various parameter metric as the evaluation performance that possible to evaluate the domain on this paper. Furthermore, this paper in a grouping with the previous researchers effort in the equivalent focus subject. The main contribution of this paper is to contribute a new light on verification and validation approach which in returned would subsidize to text steganography domain. Thus, it is expected that is expected evaluation performance able to produce in a close future through this appraisal in this paper.

Acknowledgment

This research was financially supported by the Research Grant Scheme, MoHE under RIMC Grant, Universiti Utara Malaysia.

References

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

[2] S.S. Iyer, and K. Laktharia. “New robust and secure alphabet pairing text steganography algorithm”. *International Journal of Current Trends in Engineering & Research (IJCTER),* vol. 2 no. 7, pp. 15-21, 2016.

[3] M. Y. Elmahi and M. H. Sayed, “Text Steganography Using Compression and Random Number Generators,” vol. 6, no. 6, pp. 259–263, 2017.

[4] S. Roy and M. Manasmiti “A novel approach to format based steganography”. *ICCCS’11,* pp. 511-517, 2011.

[5] R.G. Sergeant. An introduction to verification and validation of simulation models. *Proceeding of the 2013 Winter Simulation Conference,* pp. 321-327, 2014.

[6] Nazir, S., Motla, Y. H., Abbas, T., Khaton A., Jaben, J., Iqra, M., & Bakhtar, K. (2014). A process improvement in requirement verification and validation using ontology. *IEEE Systems Journal,* 1-8.

[7] W. A. Ghuman and J. Lassig, . Verification requirement for secure reliable cloud computing. *2013 IEEE Third International Conference on Cloud and Green Computing,* pp. 143-150, 2013.

[8] M. C. B. Alves D. Drusinsky and J. B. Michael. “End-to-End Formal Specification, Validation, and Verification Process: A Case Study of Space Flight Software”. *IEEE Systems Journal,* vol. 7 no. 4, 632-641, 2013.

[9] L. B. Rogovchenko, P. Fritzon, A. Garo and A. Tundis. Requirement verification and dependency tracing during simulation in modelica. *2013 8th EUROSIM Congress on Modelling and Simulation*, pp. 561-565, 2013.

[10] L. Xinhua, W. Weida, and L. Wenjian An intelligent methodology for business process model verification. *2007 IEEE International Conference on Control and Automation FrB6-2 Guangzhou, CHINA*, pp. 2381-2385, 2007.

[11] Y. S. W. Chen, and P. Hsiung, Y Lan,, Y. Hu, and S. Chen. “Formal modeling and verification for network-on-chip. *IEEE Systems Journal, pp.* 299-304, 2010.

[12] X. Wu and Z. Yang. “Verification-based interval-passing algorithm for compressed sensing”. *IEEE Signal Processing Letters,* vol. 20 no. 10, pp. 934-936, 2013.

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

[14] R. Rahmat, N.S. Kamel, and N. Yahya. “Subspace-based signature verification technique using reduced-sensor data glove”. *2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009),* pp. 83-88, 2009.

[15] J. Marincic, A. Mader, and R. “Wieringa Validation of embedded system verification models”. *IEEE Journal Systems*, 48-54, 2011.

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

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

[18] K.J. Cruickshank, J.B. Michael and M. T.Shing. “A validation metrics framework for safety-critical software-intensive Systems’. *System of System Engineering*, 2009.

[19] T. Fawcett. “An Introduction to ROC analysis”. *Science direct Pattern Recognation v*ol. 27, *pp.* 861-874, 2005.

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

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

[22] S.C.D. Ghosh and N. C. Debnath. “LCS based text steganography through Indian languages.” . *International Conference on Computer Technology and Development,* pp. 53-57, 2010.

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

[24] A. Odeh, A. Alzubi, Q.B. Hani, and K. Elleithy. Steganography by multipoint Arabic letters. *Systems, Applications and Technology Conference (LISAT), 2012 IEEE Long Island* , pp. 1-7, 2012.

[25] A. Odeh, K. Elleithy, M. Faezipur. “Steganography in text by using MS Word symbols”. *Proceeding of zone 1 conference of the American Society Engineering Education,* pp. 1-5, 2014.

[26] S. Bhattacharya, P. Indu, S. Duta, A. Biswas, and G. Sanyal. “Hiding data in text through in alphabet letter patterns (CALP)”. , *Journal of Global Research in Computer Science,* vol. 2 no. 3,33-39, 2011.

[27] S. Mahato, D. K. Yadav, and D. A. Khan. “A modified approach to text steganography using HyperText markup language”. *2012 Third International Conference on Advanced Computing & Communication Technologies,* pp. 40-44, 2013.

[28] R. Kumar, A. Malik, S. Singh, S. Chand. “A high capacity email based text steganography scheme using huffman compression”. *3rd International Conference on Signal Processing and Integrated Networks (SPIN),* pp. 3-56, (2012)