Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 2, August 2018, pp. 747~754
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i2.pp747-754

Evaluation Review on Effectiveness and Security Performances of Text Steganography Technique

Roshidi Din[1], Sunariya Utama[2], Aida Mustapha[3]
[1,2]School of Computing UUM College Arts and Sciences, Universiti Utara Malaysia,
06010, Sintok, Kedah, Malaysia
[3]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia,
Parit Raja, 86400 Batu Pahat, Johor, Malaysia

Article Info

Article history:

Received Feb 11, 2018
Revised Apr 27, 2018
Accepted May 1, 2018

Keywords:

Feature-based
Word-rule based
Line-shift coding
Word-shift coding
Language-based
Letter-based

ABSTRACT

Steganography is one of the categories in information hiding that is implemented to conceal the hidden message to ensure it cannot be recognized by human vision. This paper focuses on steganography implementation in text domain namely text steganography. Text steganography consists of two groups, which are word-rule based and feature-based techniques. This paper analysed these two categories of text steganography based on effectiveness and security evaluation because the effectiveness is critically important in order to determine that technique has the appropriate quality. Meanwhile, the security is important due to the intensity performance in securing the hidden message. The main goal of this paper is to review the evaluation of text steganography in terms of effectiveness and security that have been developed by previous research efforts. It is anticipated that this paper will identify the performance of text steganography based on effectiveness and security measurement.

Corresponding Author:

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

1. INTRODUCTION

The state of privacy condition in communication is at risk in this current global era. The presence of intruders in the communication technology is possibly qualified anyone to retrieve information without permission. The irresponsible intruders may disclose the information to uninvolved parties to check or modify it for abusing that information [1]. In order to increase interest in personal conversations by third parties using the open source system on Internet, it is essential to take further measures to confirm the protection properly. One of the resolutions in dealing with the issue is steganography.

Steganography is one of the sub-disciplines of information hiding that is defined as the art and science of covering message so that the existence of a message has not been discovered. It becomes the proper options for users to share information without any known by any other party so only sender and the exact receiver are able to know the information. The implementation of steganography is able to hide the information in several medium such as text, audio, video, image [2]. The categories of steganography show in Figure 1.

Following Figure 1, this paper is considering the implementation of steganography using the text as medium to cover hidden message. This type of steganography is known as text steganography, which focuses to conceal messages by manipulating the element in text such as, word, space, line and other characters in the sentence of text [3].

The development of techniques in text steganography consists of two kinds of techniques; word-rule based and feature-based. Word-rule based is the technique that embeds the hidden message based on word pattern by shifting in the text. The word-rule based techniques consist of line-shift coding and word-shift coding. For the line-shift coding, it hides the hidden message with a vertically shifting hidden message in text lines. Whereas word-shift coding hides the hidden message with horizontally shifting the hidden message in the length between words [4].

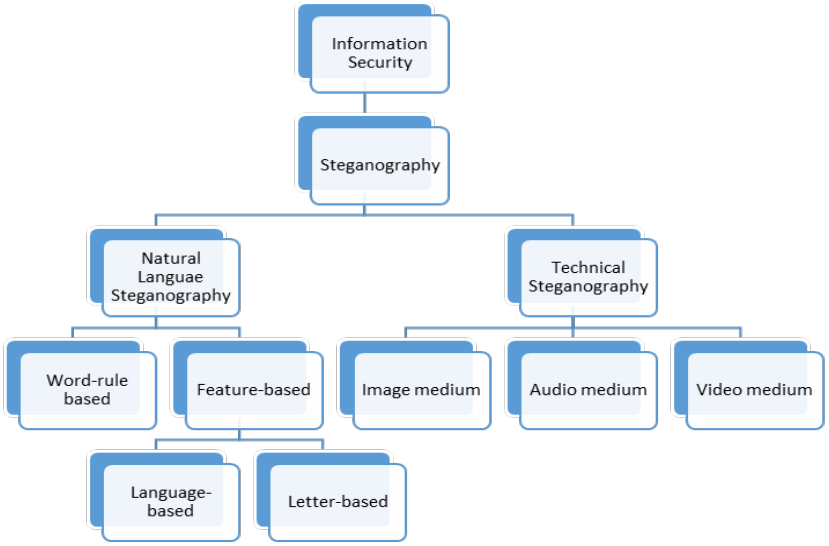

Figure 1. Major category of steganography

For feature-based technique, it alters the feature of the letter by manipulating in the shape, size, and position of the font in the text. The feature-based technique makes the reader difficult to recognize the hidden information in this text [5]. Then, due to the characteristic of this technique, feature-based can be used by many researchers based on the character of language in the world. Based on current effort research about feature-based technique, it consists of two categories; language based that can be used only in certain language and letter based that can be used in any language that uses A until Z letter. The classification of word-rule based and feature-based as text steganography shows in Figure 2.

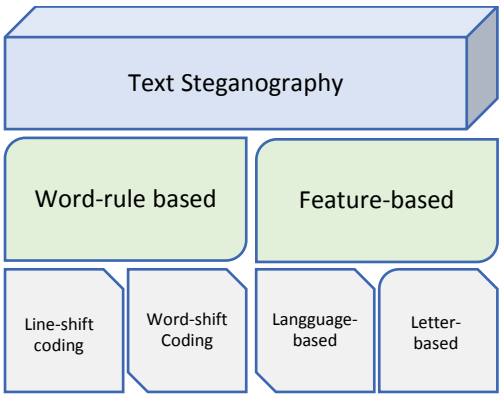

Figure 2. Major category of implementation of steganography

Figure 2 has shown the category of text steganography that is the focus of study in this paper. It classified any kind of techniques in word-rule based and feature-based based on category, then identify the issue in the technique.

2. EVALUATION REVIEW IN TEXT STEGANOGRAPHY

Essentially, the critical issue on the existence of text steganography method is easily discovered [6]. The detectors can discover the hidden messages exist in the text, if they notice the changes of the letter in the analysed text [7]. Also, the hidden messages which have been embedded will be lost, if the detector changes the text [8]. The detectors can do so if changes are done to the text such as deleting some letter or words, modifying its content, retyping, and other changes that directly make the hidden message vanish in the text.

According to this issue, there are two problems discovered by previous researchers in letter-based technique, which are the lack of effectiveness in developing the text steganography method [9] and low security for covering text in order to hide hidden message [10]. Thus, this paper concerns how the influences of the effectiveness and security in term of development of text steganography implementation.

2.1 Effectiveness of Steganography Performance

The effectiveness performance is the indicators to aim achievement based on some measurement such as appropriateness, access system and quality performance [11]. In term of comparison, effectiveness is a claimed the appropriate result in on performance system has improved than other previous systems. In other words, if the quality performance is better than others are, it means the system used is effective and more deserved to be used in a specific application [12].

In text steganography, effectiveness is critically important factor to review in order to develop the technique [13]. It is because steganography can be the options for processing in securing messages. Therefore, it has to recognize further that steganography is effective to use in securing messages as part of information hiding. Specifically, for text steganography because covering message in text domain is more useful than other medium [9]. Those are viewing from most of important information in business and education usually is in domain of text [13].

Therefore, one of considering of this paper is about reviewed the performance of text steganography that measure that relate with effectiveness of development technique from the previous researchers effort. The effectiveness of text steganography performance is be viewed in side of accuracy in hide the hidden message, quality performance and appropriateness development technique.

2.2 Security of Steganography Performance

Steganography as a part of information security also influences in those aspects in security [14]. Securing the hidden message that embeds in the text to transmit toward the exact receiver is the significant point in text steganography. Therefore, rule of security in text steganography is so critical in process development of text steganography [15]. In security performance, confidentiality, integrity and availability of information has turn into the inevitability for the development and implementation for system process [16]. Then, the security in information hiding has major issue about existences of hidden message for sending information that can called availability of data [17].

This paper considers about security fundamental in text steganography in term of confidentiality, integrity and availability as the data securing information. The implication of three data information security has illustrated in Figure 3.

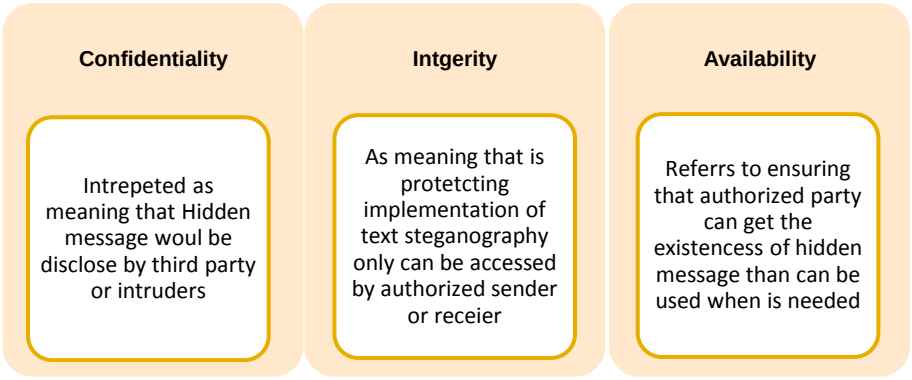

Figure 3. Fundamental category of security towards iimplementation of text steganography

Based on Figure 3 is plainly showed the considering implementation security in text steganography. This paper figure it out influencing security based on confidentiality, integrity or availability in maintain that in process securing this time.

In short, this paper classifies the several techniques in word-rule based and feature-based as category text steganography. Then, it identify the issue of each technique in term of effectiveness in development the technique and the security in order to cover hidden message as the text steganography technique.

3. WORD-RULE BASED TECHNIQUE

The implementation of word-rule based technique is divided into two ways of hiding the message. The first technique, line-shift coding can be embedded vertically hidden message to conceal the message in the text. Meanwhile second technique, word-shift coding can embedded horizontally the hidden message to conceal the message in the text. The evaluation performances of word-rule based technique is based on the effectiveness and security performance. In security performance is clearly seem divided in to confidentiality, integrity and availability. The evaluation of word-rule base shown in Table 1.

Table 1. Word-rule based technique implementation

No.	Technique	Justification	Evaluation
Line-Shift Coding			
1.	Shifting second line [14]	Shifted 1/300 inches the second line in each page up and down	In security (availability): this technique easy to attack that make lost existences of hidden message
2.	Line-shifted up and down [19]	Embed of differential and between baseline and two centroids of adjacent lines.	In security (integrity): Easy to detect hidden message
Word-shift coding			
3.	Unique shaped [5]	Develop the unique shaped in some degree of text shifted vertically	In security (confidentiality): Low security technique in embed hidden message
4.	Word-shift coding [14]	stored the horizontal shifting code in several words that conserves the state and able to be apply in text file and pictures	In security (confidentiality): Easy to detect hidden message
5	Alteration the length of image word [15]	hidden the secret by shifting horizontally the words and text image can use this method based on alteration the length of images word	In effectiveness: Consuming much time processing
6	Neighbour difference [19]	The technique divided the different length of two consecutives to embed the hidden message when 0 bit for unchanged space and 1 bit for changed neighbour difference	In effectiveness: complex process development in embedding and extracting in hidden message
7.	Distribution white space [20]	justifies the document and not shifted the first and last word on each line of text, then distributed white space used attribute word spacing	In effectiveness: limited portion to hide information.
8.	Encode matrix for instant message (IM) [21]	Encode of matrix based on online chat and inferior of encoded shipping adjacent letters for hidden message in plain English text.	In effectiveness: redundancy in hiding message easily happened
9.	Integrated inter character [22]	Adjusts the characters and words in document and distributed both of sides randomly.	In effectiveness: limited portion to hide information.
10.	Advanced encryption standard (AES) algorithm [23]	represents binary form the secret data to accomplish the process and small quantum increasing or decreasing the covers distance depend on the conforming amount bit in secret binary data	In effectiveness: low and complex algorithm performance

Based on Table 1, word-rule based technique can develop with other additional techniques. Those techniques have own process of embedding and some drawback that relate with effectiveness and security performance in implementation of this technique:

1. In term of effectiveness performance, in word-rule based has taking a long time in process embedding in covering hidden message [5]. Then, the technique also has issue in process development process has complex embedding and extracting, redundancy happened and has limited portion for covering message [15, 19, 20, 21, 22, 23] that possibly influencing the quality performance of effectiveness technique.
2. In term of security the word-rule based technique has evaluation drawback in confidentiality that claim has low security in embedding that possible can be detect by third party [5, 14]. In availability some techniques is easy to attack that possibly make hidden message lost after embedding process [14].

4. FEATURE-BASED TECHNIQUE

Feature-based method 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 [5]. Then, due to the characteristic of this technique, feature-based has used by many researchers based on character of language in the world named language-based. In this paper, the language-based implementation has classified such as English, Arabic, Persian, Chinese and Hindi languages. Then, the technique of feature-based text steganography that used in any language using A-Z letter named letter-based. Besides, the classification of feature-based technique based on the evaluation performance of effectiveness and security (confidentiality, integrity and availability) that shown in Table 2.

Table 2. Feature-based technique implementation

No.	Technique	Justification	Evaluation
Language-based (English language)			
1.	Machine translation [24]	Translates the transmitted text but allow the source to keep on secret. The sender and receiver used key idea to hide information behind translation-based steganography in natural language translation.	In effectiveness: High possibility error encode algorithm
2.	Mark up letter [25]	Markup letter resolve the secret bits to recover distance of hidden message. embeds the file with has no unwanted symbols in secret information	In security (integrity): Low security technique in embed hidden message
3.	Secret steganography code for embedding (SSCE) [26]	Substitute vowels and consonant based on grammatical sequence for cover text and then hidden message put in indefinite article for embedded in mapping information from non-particular English.	In effectiveness: Dependable with vowel words.
4.	Right-to-Left Remark and Left-to-Right remark [27]	Hide the information this method convert to binary bits while 00 bits for add nothing, 01 bits for ad Right-to Left Remark (U200F), 10 bits for Left-to-Right Remark (U200E), and 11 bits combination of U200F and U200E	In security (confidentiality): Low flexibility that executed by appropriate user
5.	Deoxyribonucleic Acid (DNA) steganography [9]	Represent binary bit 00, C for binary bits 10, G for binary bits 01, and T for binary bits 11 transform DNA sequence into chipper text using look-up table.	In effectiveness: Limited scope requirement process embedding
6.	Right remark, Left remark, Zero width joiner, and Zero width joiner [28]	The algorithm used stego key and input carrier for created symbol table and binary representation for hidden bits to embed in the text	In effectiveness: Depending with others technique (ASCII and Unicode)
7.	Encryption with Cover Text and Reordering (ECR) [29]	Reorders eight bit random key with 0 bits describes cover text and 1 bit describes encrypted text.	In effectiveness: complex process development in embedding and extracting in hidden message
Language-based (Arabic & Persian language)			
8.	Letter point in novel Arabic [30]	uses binary bits when 1 bits are pointed letter with extension in Arabic character and for unpointed letter hold 0 bits with extension	In effectiveness: Only the characters with extension can embed the stego text.
9.	Vertical displacement of the point [31]	Encode the number bits while the 0 bit encode for letter without the point or dot and 1 bit for encode letter with the point.	In security (availability): Retyping remove the hidden message
10.	Reversed Fatah [32]	Uses reversed Fatah to embed the hidden message that convert into binary bits.	In security (availability): Retyping remove the hidden message
11.	Secret key table encryption (SKT) and Characteristic Code Mapping (CCM) [33]	Uses vowel letters to connected consonant of word and designed part of punctuation to hide the information	In security (confidentiality): Low security technique in embed hidden message
Language-based (Chinese language)			
12.	Rectangular region [34]	Uses simple algorithm that based on content and method based on mathematical expression and automatic generation in Chinese letter.	In effectiveness: Medium letter for embed is limited.
13.	Simple substitution method (SSM) and high efficient substitution method (HESM) [35]	Changes the traditional form corresponds to 1 bits and the unchanged feature correspond to 0 bits. It assumed the stego message based on bit what it is 0 bits or 1 bits and extracted the feature if appear in substitution dictionary.	In security (confidentiality): Low security technique in embed hidden message

Table 2. Feature-based technique implementation (con't)

Language-based (Hindi language)			
14.	Binary string [35]	Uses longest common subsequence so to hide the message with minimal modification the feature of letter.	In effectiveness: Limited medium to embedding hidden message
15.	Specific matra [37]	The hidden message and translated length of compressed to binary bits containing matra	In security (confidentiality): Low security technique in embed hidden message
16.	Numerical code [38]	Every letter in this technique encode based on represent four binary bits and has to consider the first letter to decode the information by chipper phrase.	In security (availability): Retyping remove the hidden message.
17.	Finite state machine (FSM) [39]	Embed the binary string with the *Finite State Machine* (FSM) to describe alteration function and transformable symbols in every category. To embed binary 0 bits select next symbol of transformable from same category, otherwise select next symbol of transformable does not same and apply the transformation	In effectiveness: Algorithm complex and consuming much time
18.	Chain code using *ANOVA* [40]	Translate code into the number signified one pixel to next pixel converts part of the chain and concatenated to form a chain.	In security (confidentiality): Low security technique in embed hidden message
19.	Hindi Text using Matraye [41]	The vowel and matra add to consonant in Hindi letter, while matra itself ad in bottom and top of the consonant. The bottom matra hide 0 bits and the top matra hide 1 bits.	In effectiveness: Complex classification of dividing letters.
Letter-based			
20	Change alphabet letter pattern (CALP) [6]	Hidden message embedded based on binary bits categorization those are; the letter I and j are character in alphabet have pointed are embedded in 0 bits and 1 bits embedded in character a, c and A	In effectiveness:Dependable with number of letter used convert
21	Curve subheading (CURVE), vertical straight line (VERT), and quadruple characterization [7]	Embed the message based on form of letter from the three techniques. Two techniques (CURVE and VERT) convert into 1 and 0 bits, while other technique (Quadruple) converts into 00, 01, 10, and 11.	In security (confidentiality): Easy to detect hidden message.
	Back end interface web page [42]	Hiding the information based on HTML attributes using binary bit when 1 bits for two sequent attributes of same tags and 0 bits for two sequent attributes of different tags.	In security (confidentiality): easy to detect with discover the HTML code
22	Compression ratio in Email [43]	Adds some random letter before the '@' symbol of email ids to magnify randomness	In effectiveness: Only use for email environment
23	Huffman Compression in Email Based [44]	Set the hidden message in four fonts before '@' symbol cover the hidden message after '@' in email address.	In effectiveness: Only use for email environment
24	Alphabet Pairing Text [2]	Arrange with across the message that consists of 4 parts that have 2 binary bits	In effectiveness: Algorithm Complex and Depending with ASCII.

Based on Table 2, it is showed the list of feature-based technique that analysed the performance in term of effectiveness and security:

1. In term of effectiveness performance feature-based techniques, the review of evaluation has some drawback such as it has problem in algorithm development [25], [36], [38], dependable with some requirement [6, 28, 30], and some technique only able to use in some environment [43,44] Those are evaluation it is possibly influencing the quality performance of effectiveness technique.
2. In security, the evaluation performance of feature-based technique has quite similar with word rule based like confidentiality that claim low security and easy to detect of hidden message exist in the text [7, 27, 33, 35, 41]. Then, in security about viability component the existences critical has the problem while retyping process make the hidden message lost or do not exist the text [31, 32,38].

5. CONCLUSIONS

This paper is evaluating the category of the text steganography that consists of two groups that are word-rule based and feature-based techniques. It identifies both techniques where the word-rule based

consists of line-shift coding and of word-shift coding. Meanwhile, the feature-based technique comprises of two categories that are language-based and letter-based. This paper evaluates the performance of those techniques in terms of effectiveness and security. It is because the evaluation of effectiveness is useful to discover proper development process of technique. On the other hand, the security's performance are consists of confidentiality, integrity, and availability which have been evaluated in order to analyse the existences oh hidden message. Thus, in future work, it is anticipated that a text steganography technique will be developed which has proper performance based on evaluation of the effectiveness and security.

ACKNOWLEDEMENT

We would like thank to Prof. Dr. Huda Ibrahim, Dean of School of Computing, Universiti Utara Malaysia (SoC CAS UUM) and Director of Awang Had Salleh Graduate School (AHSGS) for their moral support for the realization of this work. This research is jointly supported by the Fundamental Research Grant Scheme (FRGS), MoHE under SO Code 13576 Universiti Utara Malaysia and Vot 1557 Universiti Tun Hussein Onn Malaysia.

REFERENCES

[1] MM Amin, S Ibharahim, M Salleh, MR Katmin, "Information using steganography". Research report, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, 2003.

[2] SS Iyer, K Laktaria, "New robust and secure alphabet pairing text steganography algorithm". *International Journal of Current Trends in Engineering & Research*, 2016; 2(7): 15–21.

[3] C Chang, S Clark, "*Practical linguistic steganography using contextual Synonym Substitution and Vertex Colour Coding*". Proceedings of the Conference on Empirical Methods in Natural Language Processing, 2010: 1194-1203.

[4] 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), 2014: 53-56.

[5] S Roy, M Manasmiti, "A novel approach to format based steganography". ICCCS'11, 2011: 511-517.

[6] S Bhattacharya, P Indu, Duta, SA Biswas, G Sanyal, "Hiding data in text through in alphabet letter patterns (CALP)". *Journal of Global Research in Computer Science*, 2011; 2(3): 33-39.

[7] S Dulera, D Jinwala, A Dasgupta, "Experimenting with the novel approaches in text steganography". *International Journal of Network Security & Its Applications*, 2011; 3(6): 213-225.

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

[9] PKR Reddy, C Nagaraju, N Subramanyam, "Text encryption through level based privacy using DNA steganography". *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 2014; 3(3): 168-172.

[10] X Sun, P Meng, Y Ye, L Hang, "*Steganography in Chinese text*". International Conference on Computer Application and System Modeling (ICCASM), 2010; 8: 651-655.

[11] Productivity Commission Staff Research Note, "On efficiency and effectiveness: some definition". Productivity Commission, 2012: 1-14.

[12] M H Jopri, A R Abdullah, M Manap, MR Yusoff, T Sutikno, MF Habban, " An Improved Detection and Classification Technique of Harmonic Signals in Power Distribution by Utilizing Spectrogram", *International Journal of Electrical and Computer Engineering (IJECE)*, 2017; 7(1): 12-20.

[13] M Kathuria, S Gambhir, "Improvement of Quality of Service Parameters in Dynamic and Heterogeneous WBAN", *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*. 2016; 4(4): 299-306.

[14] MV Nasab, BM Shafiei, "Steganography in programming". *Australian Journal of Basic and Applied S ciences*, 2009; 5(12): 1496-1499.

[15] P Mahajan, H Gupta, "*Improvision of security in image steganography using DWT, Huffman encoding & RC4 based LSB embedding*". 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016: 523-529.

[16] SD Torvhi, KB Shivakumar, R Das, "*An unique data security using text steganography*". 3rd International Conference on Computing for Sustainable Global Development (INDIACom). 2016: 3834-3838.

[17] A Mohamed Divan Masood, SK Muthusundar, "Cryptographic Hashing Method using for Secure and SimilarityDetection in Distributed Cloud Data", *Indonesian Journal of Electrical Engineering and Computer Science*.2018; 9(1): 107-110.

[18] D Popa, E Simion, "*Enhancing security combining biometrics and cryptography*". International Conference on Electronics, Computers and Artificila Intelegence (ECAI). 2017: 1-7.

[19] H Sing, PK Sing, K Soraha, "*A Survey on text steganography*". Proceeding *of* 3rd National Conference; INDIACom-Computing for Nation Development, 2009: 1-6.

[20] LLi, L Huang, X Zhao, W Yang, Z Chen, "*A statistical attack on kind of word-shift text steganography*". International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008: 1503-1507.

[21] M Liu, Y Guo, L Zhou, **"***Text steganography based on online chat*" . Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009: 807-811.

[22] H Yang, AC Kot, "*Text document authentification By integrating inter character and ppace watermarking*". IEEE International Conference on Multimedia and Expo (ICME). 2004: 955-959.

[23] A Altagani, B Bary, "*A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and word-shift coding protocol*". International Conference on Computing, Electrical, and Electronic Engineering (ICCEE). 2013: 134-140.

[24] R Stutsman, MJ Atallah, C Grothoff, K Grothoff, "*Lost in just translation*", Proceeding of the 21st Annual ACM Symposium on Applied computing (SAC), Dijon, France, 2006: 338-345.

[25] XG Sui, H Luo, "A New steganography method based on Hypertext" *National Key Lab of Modern Signal Processing, Southwest Inst of electron & telcom*, 2004: 181-184.

[26] I Banerjee, S Bhattacharya, G Synal, "*Novel text steganography through special code generation*". International Conference Systematic, Cybermetics and Informatics, 2011: 298-303.

[27] A Odeh, E Khaled, M Feazipour, "*Text steganography using language remarks*". ASEE Northeast Section Conference, 2013: 1-7.

[28] A Odeh, E Khaled, M Feazipour, "*Steganography in text by using MS Word symbols*". Proceeding of zone 1 conference of the American Society Engineering Education, 2014: 1-5.

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

[30] AAA Gutub, MM Fattah. "A novel Arabic text steganography method using letter point and extention". *International Journal of Computer, Information, Systems and Control Engineering*, 2007: 1(3): 483-486.

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

[32] JA Memon, K Khowaja, H Kazi, "Evaluation of steganography for Urdu/Arabic text". *Journal of Theoretical and Applied Information Technology*, 2008: 232-237.

[33] M Talip, A Jamal, GW Qiang, "*A proposed steganography method to Uyghur script*". International Conference on Cyber- Enabled Distributed Computing and Knowledge Discover, 2012: 125-128.

[34] W Zhang, Z Zheng, G Pu, H Zhuo. "*Chinese text watermarking based on occlusive components*". 2nd Information and Communication Technologies (ICTTA), 2006.

[35] X Sun, P Meng, Y Ye, L Hang. "*Steganography in Chinese text*".International Conference on Computer Application and System Modeling (ICCASM). 2010; 8: 651-655.

[36] SCD Ghosh, NC Debnath. "*LCS based text steganography through Indian languages*". International Conference on Computer Technology and Development. 2010: 53-57.

[37] S Changder, NC Debnath, D Ghosh, "*A new approach to hindi text steganography by shifting matra*". International Conference on Advances in Recent Technologies in Communication and Computing. 2009: 199-202.

[38] M Pathak, "A new approach for text steganography using Hindi numerical code*"*. *International Journal of Computer Application*. 2010; 1(8): 56-59.

[39] SSC Das, G Debnath, "*Text steganography through Indian language using feature coding method*". International Conference on Computer Technology and Development (ICCTD). 2010; 2: 501-506.

[40] MN Alam, MA Naser, "*Re-evaluating Chain-Code as a Feature Bangla Script*". International Conference on Electrical Information and Communication Technology (EICT). 2013: 1-5.

[41] TP Nagarhalli, JW Bakal, N Jain, "A Survey of Hindi text steganography". *International Journal of Scientific & Engineering Research*. 2016; 7(3): 55-61.

[42] S Mahato, DK Yadav, DA Khan, "*A modified approach to text steganography using HyperText markup language*". Third International Conference on Advanced Computing & Communication Technologies. 2012: 40-44.

[43] R Kumar, S Chand, S Sing, "*An email based high capacity text steganography scheme using combinatorial compression*". 5th International Conference- Confluence The Next Generation Information Technology Summit (Confluence). 2014: 36-339.

[44] 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). 2014: 53-56.