Journal of Advanced Research in Applied Sciences and Engineering Technology

https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Performance Review of Feature-Based Method in Implementation Text Steganography Approach

Sunariya Utama[1], Roshidi Din[1,2,*]

[1] School of Computing UUM College Arts and Sciences, Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia
[2] Mahathir Mohamad Institute of Thoughts Univerisiti Utara Malaysia 06010 UUM Sintok Kedah Darul Aman, Malaysia

ABSTRACT

Steganography is part of information hiding as the knowledge in science system that covers confidential messages via text, image, audio and video. Many researchers' effort implemented steganography in the text domain using the feature-based method concerning uniqueness letters to embed that conceal the hidden message. This paper intends to review the achievement performance that is used in feature-based method. This paper aim to concern specifically on performance of robustness, security and capacity in implementation feature-based method of text steganography. Therefore, this paper reviews the implementation some performance that achieve by previous researcher in developing feature-based method of text steganography.

Keywords:
Hidden message; stego text;
robustness; security

Received: 26 August 2022 **Revised: 18 Oct. 2022** **Accepted: 19 Oct. 2022** **Published: 31 October 2022**

1. Introduction

The information security is an important issue in modern technology and communication in transmitting data in the open network currently [1,2]. Anyone can access the information from anywhere in the globe on an open network because there are no territorial restrictions on access [3, 4]. As a result, sharing information over the Internet exposes it easily able to access by unauthorized users [5,6]. There for one of part implementation information security is anticipated to overcome these expected problems is name steganography [7,8].

Steganography is defined as the art and science of concealing signals through information mediums so that they are invisible to the human vision and automated equipment [9,10]. The goal of steganography execution when using performance as a component of information concealing technology is to protect the hidden information[11,12]. In order to safeguard secret messages in two-way communication, the concept of application steganography has been employed since the beginning of time [13-15]. The primary goal of steganography application is to mask sensitive information in various data transfer modes [16].

* *Corresponding author.*
E-mail address: roshidi@uum.edu.my

https://doi.org/10.37934/araset.28.2.325333

Steganography techniques are divided into two groups: digital steganography and approaches using natural language. There are two primary types of steganography implementation. Digital steganography falls within the first group and is used in non-text media like pictures, sounds, videos, and protocol mediums [17,18] The second type, called natural language steganography, uses the steganography mechanism in text as opposed to the first. It involves embedding the concealed message in the text to hide it from third-party detection. In short, natural steganography can hide the hidden message from intruder [19,20].Two categories make up the application of natural language steganography: text steganography and linguistic steganography. The first is linguistic steganography, which makes use of textual features that are linguistic in nature [21]. It conceals a message that is related to language text and other linguistic variations of the rule for embedding the private message [22]. Figure 1 exemplifies several categories of steganography implementation.

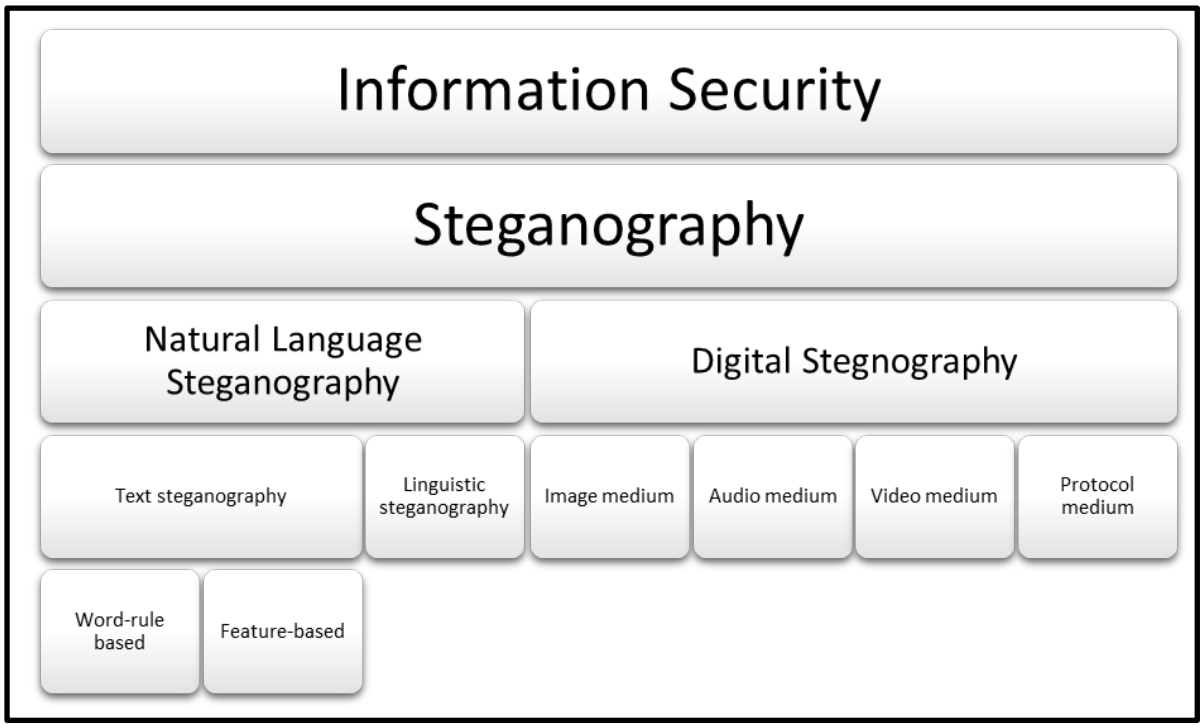

Fig. 1. Steganography field Implementation [23,24]

Figure 1 the field of steganography that shows hierarchy knowledge from information security until some method on text steganography.

Text steganography, which uses text components including words, lines of text, space, and other text properties to conceal the confidential and hidden message, is the second way of natural language steganography [25,26]. This study focuses on the feature-based approach development for text steganography [27]. By embedding the message based on the distinctive qualities of letters and any languages that employ A-Z letters in a message, the hidden messages might be hidden using this technique [16,28].

2. Related Work

As part of text steganography, feature-based is modifies a text's distinctive features based on a code word. It might slant slightly up and down, or the length of the code word might shorten or lengthen in order to embed portions of a hidden message that can be buried in text data [29-31] Ali-Shah [32] utilized the feature-based method using frequency normalization in column in choose the

letter embedding. It embeds the hidden message based inter word and space of text in correct position using Unicode system with dual binary bits. The Unicode function in this technique able to hide three characters and eight possible path to execute hiding implementation.

Bajaj and Aggarwal [33] proposed the implementation of feature-based web page environment that focus on HTML. It embedded the hidden message in italic and underline tags in back end of the webpage. This technique able to accommodate large capacity of data that converted into hexadecimal in source page code of HTML. The hidden message becomes smaller that able cover easier in the cover text.

Naharuddin [34] proposed the mapping binary bits in covering the hidden message using ASCII table as the part of technique of feature-based. The mapping creates the number of order binary bits that converted from hidden message with add number 1-7 to determine and row column of position of embedding text. This technique achieves high-capacity performance that conceals the hidden message based on row and column rather then cover text length capacity.

Akotoye *et al.*, [35] proposed the feature-based method using character pair text technique. The hidden message converts into binary bits that is embedded in the first the last letter on the sentence of text. This technique improves the capacity ratio with using character pairs key in stego text after the first and the last letter is embedded in the text.

Kumar *et al*., [36] developed a text steganography algorithm that boosted hiding volume with a compression ratio using a combination of Burrows Wheeler Transform (BMT)+Move to Front (MTF) encoding +LWZ coding. This technique is implemented based on email sender address that use to increase unpredictability, this technique places a number of random letters before the email address sign (@). This method was divided into two parts. The first step is the embedding step, which created another matrix D in sequences to select pertinent text from the buried message. The four binary bits of transformed text are converted into stego text by decoding the MTF and obtaining the BMT from the original text.

Kataria *et al*., [37] developed a text steganography solution that can produce very quick embed and extract is called encryption with cover text and Reordering (ECR) employing ExOR. The operation processes as well as integrate two character difficult to fetch enciphered text original message. With 0 bits describing cover text and 1 bits describing encrypted content, this method reordered an eight-bit random key.

Bhattacharyya *et al.* [38] developed a method for hiding information by changing the English alphabet's letter patterns. Based on the binary bit sequence, a letter like I or j that is a character in the alphabet and has a point is embedded in 0 bits, whereas the characters a, c, and an are embedded in 1 bits.

Dulera *et al.,* [29] created a technique to hide the character by combining feature-based and random character sequence based on a characteristic of the English language that transformed the message to binary bits. These approaches divide binary bits into three categories based on the shapes of the letters, using letters with curves for hidden 0 bits and letters without curves for hidden 1 bits. Technique based on a vertical line in a letter with the other letters buried in 0 bits and the vertical line hidden in 1 bits. The last technique divides the type of letter into four groups, such as curved letters for use with 00 bits, letters with central horizontal lines for use with 01 bits, letters with one vertical line for use with 10 bits, and letters with diagonal lines for use with 11 bits. These methods are difficult for the user to understand, impossible to decode, and resistant to text reformatting and retyping. However, these methods contain flaws that a program could easily detected by third party.

3. Performance Review of Feature-based Method

The performance of feature-based method considers two-way communication that achieve in implementation the technique on text steganography. There are three performances have a contradiction relation in development text steganography that show in Fig. 2.

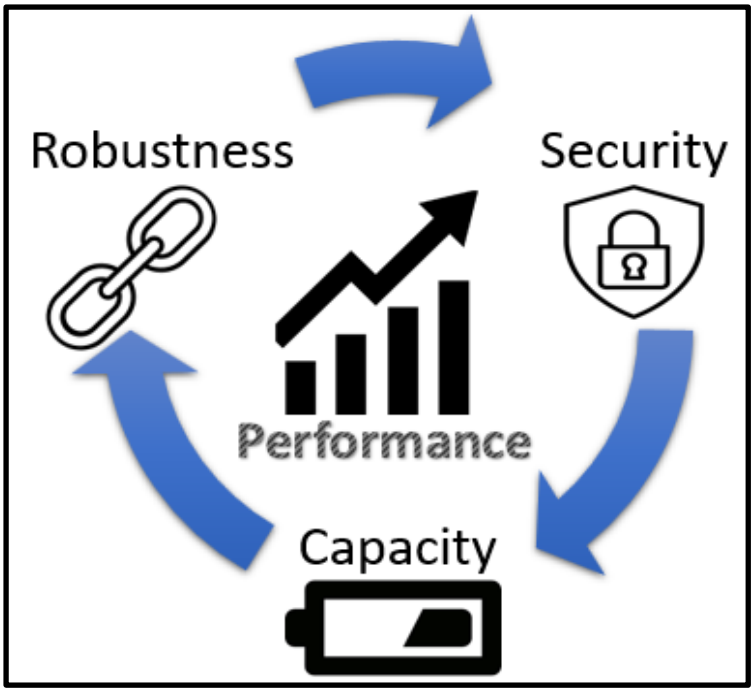

Fig. 2. The relation performances in development steganography in text domain [39]

Figure 2 shows the contradiction performance that achieves the development text steganography, such as robustness, security, and capacity [11]. Robustness is resistant to alteration the personal information from modification. Security is a crucial indicator of how much sensitive information is hidden from intruders. Capacity is the quantity of private information it can deliver to the recipient in the stego text [40,41]. It is called contradiction performance because if the technique achieves one or two specific performances, it will decrease the other performance. For example, if the techniques achieve high security performance, it will lead in decrease the robustness and capacity performances of technique [39,42]. Therefore, this paper reviews several techniques of feature-based method that concern on robustness, security, capacity, and other performances. It considers the high performance and lack performance that is achieved in feature-based method that show in Table 1.

Table 1 shows the performance in several techniques of feature-based method that display the high performance and lack performance that is achieved. It clearly seems in Table 1, there is no technique that able to achieve high performance in robustness, security, and capacity. In Unispach Xor Shift, Polynomial encryption using Chinese Text and Arabic text Unicode techniques achieved the high performance in capacity but lack in security performance. Then, Character spacing normalization and alphabet pairing techniques has high performance in robustness and capacity, but lack in security performance. In AITSteg technique of feature-based has high performance in security and capacity, but lack in robustness performance. This condition states the three relations performance is contradictive each other in develop the technique of feature-based method. Table 1 also consider

the other performance that high in effective algorithm and fast embedding process then lack performance that only applicable in web page, complex algorithm, and time-consuming process. Moreover, the calculation performance in developing technique of feature-based method displays in Figure 3.

Table 1
Performance technique of feature-based method in last decade

No	Feature-based	Robustness	Security	Capacity	Other performance
1	Arabic text in Unicode technique [24]	–	✗	✓	–
2	Polynomial encryption using Chinese Text [43]	–	✗	✓	–
3	Webometric text steganography [44]	–	✓	–	✗ only apply in web page environment
4	Unispach Xor Shift Cipher [45]	–	✗	✓	–
5	Using zero-width joiner (ZWJ) and Kashida in Arabic text [28]	–	✓	✗	–
6	Character spacing normalization [32]	✓	✗	✓	–
7	Unicode character in multilingual [46]	–	–	✓	✗ Complex algorithm
8	Arabic text using text steganography and cryptography [42]	–	✓	–	✗ Complex algorithm
9	Secret sharing message system [47]	✗	✓	–	–
10	Coverless steganography Single Bit Rules [48]	–	✗	–	✓ It has effective algorithm
11	Binary Mapping [34]	–	–	✓	✗ Easy to detect changes letter
12	HTML Web page steganography [33]	✓	✗	–	–
13	Font color MS excel [12]	✗	–	✓	✗ Easy to detect changes letter
14	Character pair text [49]	–	–	✓	✗ Easy to detect changes letter
15	AITSteg Via social media [50]	✗	✓	✓	–
16	Multilayer Partially Homomorphic [51]	✗	–	✓	–
18	English text using number oriented [52]	✗	✗	–	✓ Fast embedding process
19	Huffman Compression [53]	–	✗	✓	–
20	Content-based Feature extraction [54]	✗	✗	✓	–
21	Alphabet Pairing Text [55]	✓	✗	✓	–
22	Compression ratio in Email [36]	–	–	✓	✗ Complex algorithm
23	Encryption with Cover Text and Reordering [37]	✗	–	✓	–
24	Back-end interface web page [56]	–	–	✓	✗ Time consuming process

✓: *High performance* ✗: *Lack performance* –: *No performance*

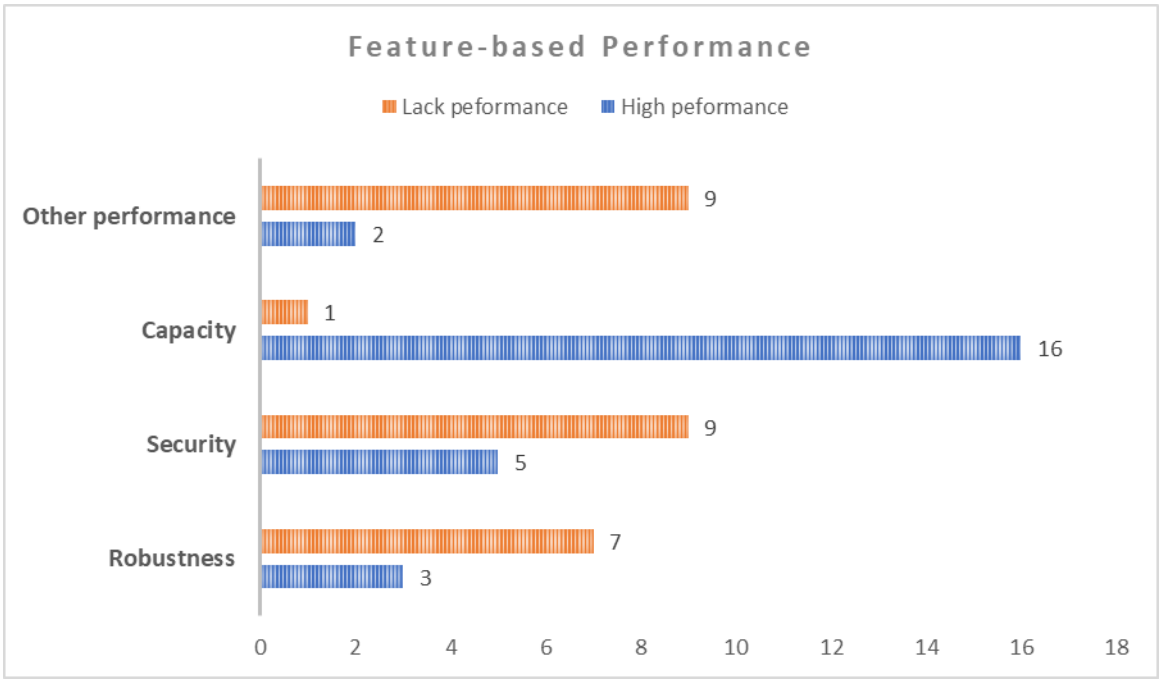

Fig. 3. The graph of achievement performance feature-based method in last decade

Figure 3 shows the number of achievements in development feature-based method in last decade. Based on Fig. 3, the most of high performance that achieve is capacity performance with 16 techniques, the second is security performance that achieved by nine techniques, the third is robustness with three techniques, and the last is other performance (effective algorithm and fast embedding process). For the opposite, several techniques also lack in those are performance that mostly lack in security performance and other performance (dependable webpage, complex algorithm, and time-consuming process) with nine techniques. Then, if following the lack performance in robustness with seven techniques and the last is capacity with only one technique. Thus, the review of achievement performance in implementation of feature-based method as the part text steganography.

4. Conclusions

The paper aims at the text steganography category in reviewing the feature-based method's performance in text steganography. It focuses on the three performances in developing feature-based method robustness, security, and capacity techniques. Those are three performances in which the contradiction relation each other when one or two techniques perform the expected result, then the other has become lacking in the evaluation techniques. This paper reviews several techniques of feature-based methods that evaluate the robustness, security, capacity, and other performances concerned by previous researchers.

This paper discovers the high performance that achieves mostly on capacity performance, followed by security, as the second and third are robustness and last is other performances (effective algorithm and fast embedding process). Meanwhile, the lack of performance is mostly in security and other performance (dependable webpage, complex algorithm, and time-consuming process). It concludes that robustness, security, and capacity performances are the major performance that has been considered in developing the technique of feature-based method in text steganography. For

future work, it is expected to propose the technique in a feature-based method that can achieve high performance in robustness, security, and capacity as part of text steganography.

Acknowledgement
This research was supported by Ministry of Higher Education (MOHE) of Malaysia through RIMC, Universiti Utara Malaysia (UUM).

References

[1] Al-Nofaie, Safia Meteb Awad, and Adnan Abdul-Aziz Gutub. "Utilizing pseudo-spaces to improve Arabic text steganography for multimedia data communications." *Multimedia Tools and Applications* 79, no. 1 (2020): 19-67.

[2] Baby, Della, Jitha Thomas, Gisny Augustine, Elsa George, and Neenu Rosia Michael. "A novel DWT based image securing method using steganography." *Procedia Computer Science* 46 (2015): 612-618. https://doi.org/10.1007/s11042-019-08025-x

[3] Jaafar, Nurulaini, Siti Rohani Mohd Nor, Siti Mariam Norrulashikin, Nur Arina Bazilah Kamisan, and Ahmad Qushairi Mohamad. "Increase Students' Understanding of Mathematics Learning Using the Technology-Based Learning." *International Journal of Advanced Research in Future Ready Learning and Education* 28, no. 1 (2022): 24-29.

[4] Nor, Siti Rohani Mohd, Adina Najwa Kamarudin, and Nurul Aini Jaafar. "Comparison on the Student's Performances during Physical and Online Learning in Financial Mathematics Course." *International Journal of Advanced Research in Future Ready Learning and Education* 28, no. 1 (2022): 1-8.

[5] Abikoye, Oluwakemi Christiana, and Roseline Oluwaseun Ogundokun. "Efficiency of LSB steganography on medical information." *International Journal of Electrical and Computer Engineering (IJECE)* 11, no. 5 (2021): 4157-4164. https://doi.org/10.11591/ijece.v11i5.pp4157-4164

[6] Kouser, Saeeda, and Aihab Khan. "A Novel Feature Extraction Approach: Capacity Based Zero-Text Steganography." *Int. J. Inf. Technol. Secur* 3 (2017): 85-99.

[7] D. Stoyanov, Z. Taylor, and D. Hutchison, *and Ophthalmic Medical*, vol. 1. Springer International Publishing, 2018.

[8] Din, Roshidi, Rosmadi Bakar, Sunariya Utama, Jamaluddin Jasmis, and Shamsul Jamel Elias. "The evaluation performance of letter-based technique on text steganography system." *Bulletin of Electrical Engineering and Informatics* 8, no. 1 (2019): 291-297. https://doi.org/10.11591/eei.v8i1.1440

[9] Ahvanooey, Milad Taleby, Qianmu Li, Xuefang Zhu, Mamoun Alazab, and Jing Zhang. "ANiTW: A novel intelligent text watermarking technique for forensic identification of spurious information on social media." *Computers & Security* 90 (2020): 101702. https://doi.org/10.1016/j.cose.2019.101702

[10] Sadat, Elaheh Sadat, Karim Faez, and Mohsen Saffari Pour. "Entropy-based video steganalysis of motion vectors." *Entropy* 20, no. 4 (2018): 244. https://doi.org/10.3390/e20040244

[11] Naqvi, Nuzhat, Aliya Tabassum Abbasi, Rasheed Hussain, M. Aihab Khan, and Basheer Ahmad. "Multilayer partially homomorphic encryption text steganography (MLPHE-TS): a zero steganography approach." *Wireless Personal Communications* 103, no. 2 (2018): 1563-1585. https://doi.org/10.1007/s11277-018-5868-1

[12] Alsaadi, Husam Ibrahiem, Maad Kamal Al-Anni, Rafah M. Almuttairi, Oguz Bayat, and Osman Nuri Ucan. "Text steganography in font color of MS excel sheet." In *Proceedings of the First International Conference on Data Science, E-learning and Information Systems*, pp. 1-7. 2018. https://doi.org/10.1145/3279996.3280006

[13] Din, Roshidi, Sunariya Utama, and Aida Mustapha. "Evaluation review on effectiveness and security performances of text steganography technique." *Indonesian Journal of Electrical Engineering and Computer Science* 11, no. 2 (2018): 747-754. https://doi.org/10.11591/ijeecs.v11.i2.pp747-754

[14] Adnan, Nur Fatimah, Kee Quen Lee, Hooi Siang Kang, Keng Yinn Wong, and Hui Yi Tan. "Preliminary investigation on the energy harvesting of vortex-induced vibration with the use of magnet." *Progress in Energy and Environment* 21 (2022): 1-7. https://doi.org/10.37934/progee.21.1.17

[15] Adin, Khaled Sharaf, Sharafaddin Saleh, and Bilkis Zabara. "The Quality of Stormwater in Sana'a City from the Perspective of Integrated Water Resources Management." *Journal of Advanced Research in Technology and Innovation Management* 3, no. 1 (2022): 1-10.

[16] Yaghobi, Shabnam Rahber, and Hedieh Sajedi. "Text steganography in webometrics." *International Journal of Information Technology* 13, no. 2 (2021): 621-635. https://doi.org/10.1007/s41870-020-00572-z

[17] Taha, Ahmed, Aya S. Hammad, and Mazen M. Selim. "A high capacity algorithm for information hiding in Arabic text." *Journal of King Saud University-Computer and Information Sciences* 32, no. 6 (2020): 658-665. https://doi.org/10.1016/j.jksuci.2018.07.007

[18] Valandar, Milad Yousefi, Peyman Ayubi, and Milad Jafari Barani. "A new transform domain steganography based on modified logistic chaotic map for color images." *Journal of Information Security and Applications* 34 (2017): 142-151. https://doi.org/10.1016/j.jisa.2017.04.004

[19] Yang, Zhongliang, Yongfeng Huang, and Yu-Jin Zhang. "A fast and efficient text steganalysis method." *IEEE Signal Processing Letters* 26, no. 4 (2019): 627-631. https://doi.org/10.1109/LSP.2019.2902095

[20] Chang, Ching-Yun, and Stephen Clark. "Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method." *Computational linguistics* 40, no. 2 (2014): 403-448. https://doi.org/10.1162/COLI_a_00176

[21] Nechta, Ivan V. "New steganalysis method for text data produced by synonym run-length encoding." In *2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE)*, pp. 188-190. IEEE, 2018. https://doi.org/10.1109/APEIE.2018.8545230

[22] Singh, A. P., S. Moudgil, and S. Rani. "An Acquaintance to Text-Steganography and its Methods." In *Journal of Physics: Conference Series*, vol. 1950, no. 1, p. 012005. IOP Publishing, 2021. https://doi.org/10.1088/1742-6596/1950/1/012005

[23] Wang, Peipei, Yun Cao, and Xianfeng Zhao. "Segmentation based video steganalysis to detect motion vector modification." *Security and Communication Networks* 2017 (2017). https://doi.org/10.1155/2017/8051389

[24] Alshamsi, Adeel, Salem Albaloushi, Mohammed Alkhoor, Hamed Almheiri, and Nedal Ababneh. "Enhancing Arabic Text Steganography Based on Unicode Features." *International Journal of Computing and Digital System* (2021). https://doi.org/10.1145/3456146.3456148

[25] Tong, Yongju, YuLing Liu, Jie Wang, and Guojiang Xin. "Text steganography on RNN-Generated lyrics." *Mathematical Biosciences and Engineering* 16, no. 5 (2019): 5451-5463. https://doi.org/10.3934/mbe.2019271

[26] Beroual, Abdesselam, and Imad Fakhri Al-Shaikhli. "A review of steganographic methods and techniques." *International Journal on Perceptive and Cognitive Computing* 4, no. 1 (2018): 1-6. https://doi.org/10.31436/ijpcc.v4i1.56

[27] Tu, Shanshan, Xinyi Huang, Yao Huang, Muhammad Waqas, and Sadaqat Ur Rehman. "SSLSS: Semi-supervised learning-based steganalysis scheme for instant voice communication network." *IEEE Access* 6 (2018): 66153-66164. https://doi.org/10.1109/ACCESS.2018.2879328

[28] Alanazi, Norah, Esam Khan, and Adnan Gutub. "Efficient security and capacity techniques for Arabic text steganography via engaging Unicode standard encoding." *Multimedia Tools and Applications* 80, no. 1 (2021): 1403-1431. https://doi.org/10.1007/s11042-020-09667-y

[29] Dulera, Shraddha, Devesh Jinwala, and Aroop Dasgupta. "Experimenting with the novel approaches in text steganography." *arXiv preprint arXiv:1203.3644* (2012). https://doi.org/10.5121/ijnsa.2011.3616

[30] Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." *Information Security Journal: A Global Perspective* 30, no. 2 (2021): 63-87. https://doi.org/10.1080/19393555.2020.1801911

[31] Chaudhary, Sunita, Meenu Dave, and Amit Sanghi. "Text steganography based on feature coding method." In *Proceedings of the International Conference on Advances in Information Communication Technology & Computing*, pp. 1-4. 2016. https://doi.org/10.1145/2979779.2979786

[32] Shah, Syed Tahir Ali, Aihab Khan, and Afaq Hussain. "Text steganography using character spacing after normalization." *Int. J. Sci. Eng. Res* 11 (2020): 949-957. https://doi.org/10.14299/ijser.2020.02.05

[33] Bajaj, Ishita, and Rajesh Kumar Aggarwal. "Steganography using HTML Web Pages as a Carrier: A Survey." In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*. 2019. https://doi.org/10.2139/ssrn.3351033

[34] Naharuddin, Alfin, Adhi Dharma Wibawa, and Surya Sumpeno. "A high capacity and imperceptible text steganography using binary digit mapping on ASCII characters." In *2018 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, pp. 287-292. IEEE, 2018. https://doi.org/10.1109/ISITIA.2018.8711087

[35]Akotoye, F. X. K., Y. E. Yakavor, J. Kwofie, and Fahd-La Tirogo. "Character Pair Text Steganography Based on the Enhanced." In *2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/ICASTECH.2018.8507117

[36] Kumar, Rajeev, Satish Chand, and Samayveer Singh. "An Email based high capacity text steganography scheme using combinatorial compression." In *2014 5th international conference-confluence the next generation information technology summit (confluence)*, pp. 336-339. IEEE, 2014. https://doi.org/10.1109/CONFLUENCE.2014.6949231

[37] Kataria, Sahil, Tarun Kumar, Kavita Singh, and Maninder Singh Nehra. "ECR (encryption with cover text and reordering) based text steganography." In *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*, pp. 612-616. IEEE, 2013. https://doi.org/10.1109/ICIIP.2013.6707666

[38] Bhattacharyya, Souvik. "Hiding data in text through changing in alphabet letter patterns (calp)." *Journal of Global Research in Computer Science* 2, no. 3 (2011).

[39] Febryan, Aryfandy, Tito Waluyo Purboyo, and Randy Erfa Saputra. "Steganography methods on text, audio, image and video: a survey." *International Journal of Applied Engineering Research* 12, no. 21 (2017): 10485-10490.

[40] Khan, Yahya, Ali Algarni, Aisha Fayomi, and Abdullah M. Almarashi. "Disbursal of Text Steganography in the Space of Double-Secure Algorithm." *Mathematical Problems in Engineering* 2021 (2021). https://doi.org/10.1155/2021/7336474

[41] Khusairy, Nabiha Mohd, and Hairul Nizam Ismail. "Social Impact Assessment in Measuring Environmental Sustainability in Tourism Project Development: Trends in the Existing Literature." *Journal of Advanced Research in Technology and Innovation Management* 3, no. 1 (2022): 11-15.

[42] Ditta, Allah, Muhammad Azeem, Shahid Naseem, Khurram Gulzar Rana, Muhammad Adnan Khan, and Zafar Iqbal. "A secure and size efficient algorithm to enhance data hiding capacity and security of cover text by using unicode." *Journal of King Saud University-Computer and Information Sciences* (2020).

[43] Guan, Bo, Lichun Gong, and Yanzhao Shen. "A Novel Coverless Text Steganographic Algorithm Based on Polynomial Encryption." *Security and Communication Networks* 2022 (2022). https://doi.org/10.1155/2022/1153704

[44] Sajedi, Hedieh, and Shabnam Rahbar Yaghobi. "Information hiding methods for E-Healthcare." *Smart health* 15 (2020): 100104. https://doi.org/10.1016/j.smhl.2019.100104

[45] Por, Lip Yee, KokSheik Wong, and Kok Onn Chee. "UniSpaCh: A text-based data hiding method using Unicode space characters." *Journal of Systems and Software* 85, no. 5 (2012): 1075-1082. https://doi.org/10.1016/j.jss.2011.12.023

[46] Baawi, Salwa Shakir, and Dhamyaa A. Nasrawi. "Improvement of "Text Steganography Based on Unicode of Characters in Multilingual" by Custom Font with Special Properties." In *IOP Conference Series: Materials Science and Engineering*, vol. 870, no. 1, p. 012125. IOP Publishing, 2020. https://doi.org/10.1088/1757-899X/870/1/012125

[47] Sharma, Amit, Pradeep Kumar Singh, and Yugal Kumar. "An integrated fire detection system using IoT and image processing technique for smart cities." *Sustainable Cities and Society* 61 (2020): 102332. https://doi.org/10.1016/j.scs.2020.102332

[48] Wu, Ning, Poli Shang, Jin Fan, Zhongliang Yang, Weibo Ma, and Zhenru Liu. "Research on coverless text steganography based on single bit rules." In *Journal of Physics: Conference Series*, vol. 1237, no. 2, p. 022077. IOP Publishing, 2019. https://doi.org/10.1088/1742-6596/1237/2/022077

[49] Akotoye, F. X. K., Y. E. Yakavor, J. Kwofie, and Fahd-La Tirogo. "Character Pair Text Steganography Based on the Enhanced." In *2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/ICASTECH.2018.8507117

[50] Ahvanooey, Milad Taleby, Qianmu Li, Jun Hou, Hassan Dana Mazraeh, and Jing Zhang. "AITSteg: An innovative text steganography technique for hidden transmission of text message via social media." *IEEE Access* 6 (2018): 65981-65995. https://doi.org/10.1109/ACCESS.2018.2866063

[51] Naqvi, Nuzhat, Aliya Tabassum Abbasi, Rasheed Hussain, M. Aihab Khan, and Basheer Ahmad. "Multilayer partially homomorphic encryption text steganography (MLPHE-TS): a zero steganography approach." *Wireless Personal Communications* 103, no. 2 (2018): 1563-1585. https://doi.org/10.1007/s11277-018-5868-1

[52] Mandal, Kunal Kumar, Santanu Koley, and Sudipto Dhar. "A mathematical model for secret message passing using Steganography." In *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pp. 1-6. IEEE, 2016. https://doi.org/10.1109/ICCIC.2016.7919527

[53] Malik, Aruna, Geeta Sikka, and Harsh K. Verma. "A high capacity text steganography scheme based on LZW compression and color coding." *Engineering Science and Technology, an International Journal* 20, no. 1 (2017): 72-79. https://doi.org/10.1016/j.jestch.2016.06.005

[54] Kouser, Saeeda, Aihab Khan, and Ejaz Qamar. "A Novel Content-Based Feature Extraction Approach: Text Steganography." *International Journal of Computer Science and Information Security* 14, no. 12 (2016): 916.

[55] Iyer, S. S., and Kamaljit Lakhtaria. "New robust and secure alphabet pairing text steganography algorithm." *International Journal of Current Trends in Engineering & Research (IJCTER)* 2, no. 7 (2016): 15-21.

[56] Mahato, Susmita, Dilip Kumar Yadav, and Danish Ali Khan. "A modified approach to text steganography using HyperText markup language." In *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, pp. 40-44. IEEE, 2013. https://doi.org/10.1109/ACCT.2013.19