Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 88-95
Published by *Majmuah Enterprise*
www.majmuah.com

The Design Review of Feature-based Method in Embedding the Hidden Message in Text as the Implementation of Steganography

ROSHIDI DIN and SUNARIYA UTAMA
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA
Email: roshidi@uum.edu.my, sunariya.utama1@ahsgs.uum.edu.my| Tel: +60175981306, +601131548575 |

Received: September 14, 2023
Accepted: September 21, 2023
Online Published: September 26, 2023

Abstract

Steganography, the art of concealing secret information within cover media, plays an important role in securing hidden messages and data protection. Text steganography, in particular, involves embedding confidential data within textual content to avoid detection by unauthorised parties. In this paper, it conducts a review of several techniques of feature-based text steganography that concern the conversion of hidden messages into embedded messages in the form of binary bits or other code. It is because most researchers develop the techniques of feature-based with several criteria, embedding one bit, two bits, and other number bits in generating stego text. This paper investigates the design implementation of a feature-based method for embedding hidden messages from the converting process to generate stego text. The highlight of this paper is to figure out the total number of hidden messages in order to embed the binary bits or other code in the text.

Keywords: Embedding process; Extracting process; Stego text

1. Introduction

Insert text here. The steganography is a fascinating and ancient art of secret communication that dates back to ancient civilizations. Steganography involves concealing sensitive information within seemingly innocent data or media to ensure confidentiality and avoid detection. Unlike cryptography, which focuses on encrypting messages to make them unreadable, steganography aims to hide the existence of the message altogether(Din, Bakar, Utama, et al., 2019; Ditta et al., 2020). The primary goal is to make the secret information undetectable to unintended recipients, thus enhancing the security of the communication (Din, Mahmuddin, et al., 2019; Manikandan et al., 2018). Throughout history, steganography has been employed in various forms, ranging from invisible inks and microdots to hidden messages in artwork, music, and even physical objects (Alaqeel & Saleh, 2021). With the advent of the digital era, steganography has found new applications in the world of computers and technology. Digital steganography involves hiding data within digital media, such as images, audio files, videos, and text. By subtly modifying the carrier data, steganographers can embed hidden messages without causing any noticeable changes to the appearance or quality of the media (Singh et al., 2021).

The applications of steganography are diverse and far-reaching. It is used in secure communication to protect sensitive information during transmission. Digital watermarking employs steganographic techniques to embed copyright information into digital media, helping to identify the rightful owners of content (Ahvanooey et al., 2019; Su et al., 2017). Steganography is also relevant in covert operations and data protection, where the ability to hide information is crucial (Siddiqui et al., 2020). Despite its advantages, steganography faces challenges, particularly in the realm of steganalysis - the process of detecting hidden information. As detection techniques advance, steganographers must continually innovate to develop more robust and secure methods (Baawi et al., 2020; Tayyeh et al., 2019).Classification in steganography refers to the categorization and organization of steganographic techniques based on their fundamental principles, applications, and characteristics. Steganography encompasses a wide range of methods, each tailored to specific types of data, carrier media, and objectives (Bajaj & Aggarwal, 2019). The classification of steganography techniques aids in understanding their strengths, limitations, and relevance in various scenarios.

The field of steganography can be broadly divided into two approaches which are digital steganography and natural language steganography (Dhawan & Gupta, 2021; Xiang et al., 2020). For digital steganography, several categories based on the carrier mediums or data type used. Common classifications include:

Image Steganography: Image steganography involves concealing secret information within digital images. Various techniques, such as LSB substitution, pixel value differencing, and transform domain embedding, are used to embed

hidden data into the pixel values or frequency domain coefficients of images (Baby et al., 2015; Din & Qasim, 2019; Ma et al., 2019).

Audio Steganography: Audio steganography deals with hiding information within audio files. This category employs methods like phase coding, echo hiding, and spread spectrum modulation to subtly embed the secret data within the audio signal (Alhaddad et al., 2020; Bansal & Chhikara, 2014; Din & Qasim, 2019).

Video Steganography: Video steganography pertains to concealing information within digital videos. Techniques like frame manipulation, motion vector modification, and 3D transform embedding are used to hide data within video frames or the motion vectors (Su et al., 2017; Zhang et al., 2014)

Network Steganography: Network steganography focuses on concealing information within network communication protocols or traffic. This category includes methods like protocol-level steganography, which hides data in packet headers or payloads during transmission (Wu et al., 2018).

Those are the non-text mediums of steganography, while general steganography is called natural language steganography. Natural language steganography is a method for concealing sensitive or private information in seemingly innocent natural language text. It steganography involves concealing data within textual documents, emails, or social media post (Xiang et al., 2020). Natural language steganography is a specialized form of steganography that involves hiding secret information within natural language text, such as sentences, paragraphs, or documents. Unlike digital steganography methods that conceal data within images, audio, or video, natural language steganography focuses on exploiting the linguistic properties of the text for covert communication (Ammar Odeh et al., 2012; Yang et al., 2019).

In natural language steganography, the goal is to embed the hidden information within the text while maintaining the text's readability, coherence, and grammatical correctness. The challenge lies in finding ways to subtly modify the text so that the presence of the concealed data remains undetectable to casual observers or automated detection systems (Din, Bakar, Sabri, et al., 2019; Tong et al., 2019).This method of linguistic steganography and text steganography Linguistic steganography relies on language-specific properties for concealing data. Linguistic steganography techniques manipulate linguistic features, word frequencies, or sentence structures to embed covert messages within the text while text steganography focuses on concealing the message based on attributes and features of the text message (Nechta, 2018; Xiang et al., 2018). One category of text steganography is the feature-based method that involves manipulating feature representations of data and the uniqueness of the letter to embed a hidden message (Al-Alwani et al., 2007; Muhammad et al., 2021; Utama & Din, 2022). This feature-based method is the main focus of this paper, which reviews several techniques that have been implemented by previous research efforts.

2. Related Works

Feature-based methods in text steganography refer to conceal information by encoding it in a text document's attributes or qualities. The primary goal is to hide the existence of the hidden message in such a way that it remains inconspicuous to unintended recipients. Various feature coding methods have been proposed by research effort. Bajaj and Agarwal (Bajaj & Aggarwal, 2019) utilized the of the technique feature-based method on text steganography in HTML website that embed the hidden message that convert into binary bits in line highlighting on a website's back end. This technique. This technique conceals the hidden message with embed binary bit that 1 bit embed in, ⟨u⟩⟨i⟩⟨/i⟩⟨/u⟩ and 0 bit in ⟨i⟩⟨u⟩⟨/u⟩⟨/i⟩ on the HTML web page text. Alssaadi el al. (Alsaadi et al., 2018) proposed technique of feature-based method on Microsoft excel that focus on the font color of the cell. This technique embeds the hidden message that convert into binary bits, and then turn the number of bitsinto decimal numbers, starting with 0000000 changing to 0 and ending with 111111 changing to 255. Excel table with the decimal based RGB colour embedded. This technique has the large capacity in ms excel that high robustness in RGF color hidden message.

Wu et al. (Wu et al., 2018) utilized the coverless English text that convert the hidden message into binary bits, message, then search for the tag in 6 binary bits (0000000 to 111111). This technique has been ensuring security performance and being difficult to attack. Kouser et al. (Kouser et al., 2016) presented a feature-method that the technique divides hidden messages into two categories based on binary bits. The first category splits the letter with a 0 bit embedded in the letter "grass" and a 1 bit embedded in the letter "sky & root." The second category separated the letter into 11 bit embeddable consonant letters that can be written on the middle two lines, 10 bit embeddable vowel letters that can be written on the middle two lines, 01 bit embeddable on the lower three lines, and 11 bit embeddable on the upper three lines.

Reddy et al. (Reddy et al., 2014) Demonstrated Deoxyribonucleic Acid (DNA) steganography, which uses four alphabets to represent the numbers 00, 10, 10, and 11, respectively. Using a look-up table, the method used to build the DNA structures converts the DNA sequence into readable text. With the use of received text, a rule sequence table search, and DNA sequence, this method was able to decrypt the concealed message. Afterward, based on represented binary in a lookup table, embed the concealed message in binary bits from the DNA sequence. Saad and Algamdi (Saad et al., 2023) proposed the technique on feature-based method by categorizing binary bits in bit mapping in value letter from A to G using ASCII characters. Based on the row and column ASCII model alphabet in the text, the hidden message that embed in cover text. This technique developed by propose robust performance and large capacity in conceal the hidden message in the text.

The text steganography algorithm developed by Kumar et al. (Kumar et al., 2014) uses the email sender picture address. With a compression ratio that combines coding transform it enhanced the hidden volume. To boost unpredictability, the approach places a number of random letters before the "@" symbol in email addresses. The method performs exceptionally well in email contexts when it comes to concealment. However, the randomness of this method since the email address contains a random element has an impact on its security.The technique presented by Odeh et al. (A Odeh et al., 2014) makes use of numerous unseen character symbols, such as zero width joiners, right and left remarkers between letters, and zero width joiners those adding on of table variations to steganography carrier file data, to cover four bits in word symbols. Using a stego key and input carrier, this technique created a symbol table and a binary representation for hidden bits to be inserted into the text. The benefits include not changing the file format and not requiring specific tools to cover data. This algorithm technique, which is now being used with a particular language, is expected to expand the configuration technique so that it may be used with any text language.

3. General Implementation of Feature-based Method

Feature-based methods are implemented as part of text steganography to facilitate message communication between sender and specific receiver to avoid unauthorized people. The technique mostly conceals the hidden message by embedding the binary bits that are embedded into the cover text to generate the stego text. However, some techniques also utilised the other numbers beside binary bits, converting hidden messages based on the ASCII table, Unicode, decimal stream, and so on. The analogy design of the implementation of the feature-based method in order to conceal hidden messages in the text is shown in Figure 1.

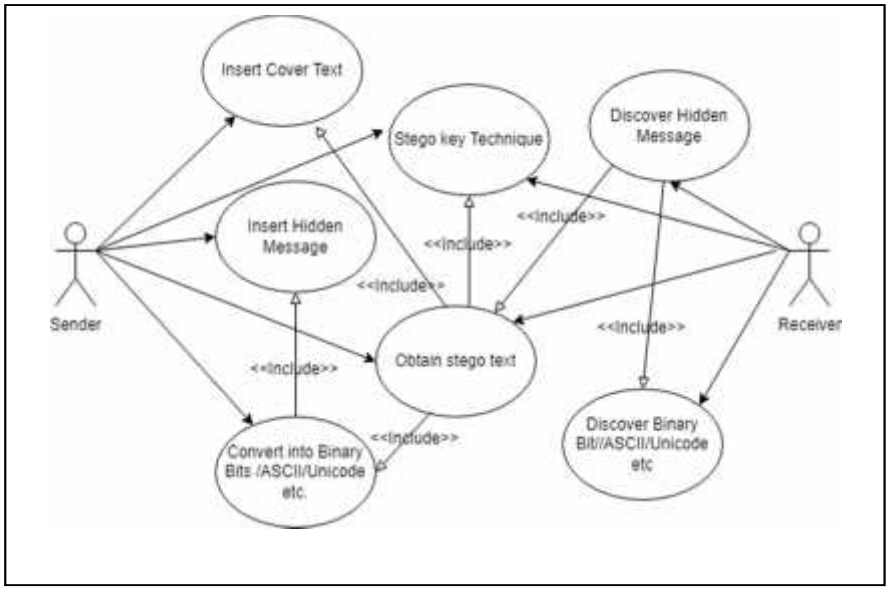

Figure 1: Use case diagram implementation technique of feature-based method

In Figure 1, it shows the general design of technique in feature-based method in form of use case diagram. Figure 1 displays the communication between sender receiver that utilize several use cases function. Each use case function of the feature-based method is defined as:

a) *Insert cover text*: This use case is instructed the sender to insert the cover text as medium to hide the hidden message in several letter with unique figure in the text.

b) *Insert hidden message*: This use case is instructed the sender to insert the hidden message as the main information that have to receive for receiver.
c) *Convert hidden message*: This use case is instructed the sender to convert the hidden message inform of binary bits ASCII table, Unicode, decimal stream that has to embed to the cover text.
d) *Stego key technique*: This use case is instructed the sender and receiver as the share key that check the uniqueness feature of letter in cover text that is embedded by binary bits ASCII table, Unicode, decimal stream and so on.
e) *Obtain stego text*: This use case is instructed the sender and receiver that generate the conceal message in text that had been embedded in cover text.
f) *Discover binary bits ASCII table, Unicode, decimal stream or other codes*: This use case is instructed the receiver to extract the binary bits and other code before convert again the hidden message that get from utilize the stego key technique.
g) *Discover hidden message*: This use case is instructed the receiver to discover again the exact hidden message from sender that convert the discover code from generate stego text.

Those are general technique execution of feature-based method in conceal the hidden message that send by sender to receiver by receiver that conceal from human and machine vision. The main concern of this paper is the converting hidden message become the binary bit and code to generate stego text.

4. Discussion of Hidden Message

This paper considers about the review about the design implementation of convert the hidden message into binary bit or other code by previous research efforts. Figure 2 display the previous research technique in converting hidden message in generating stego text.

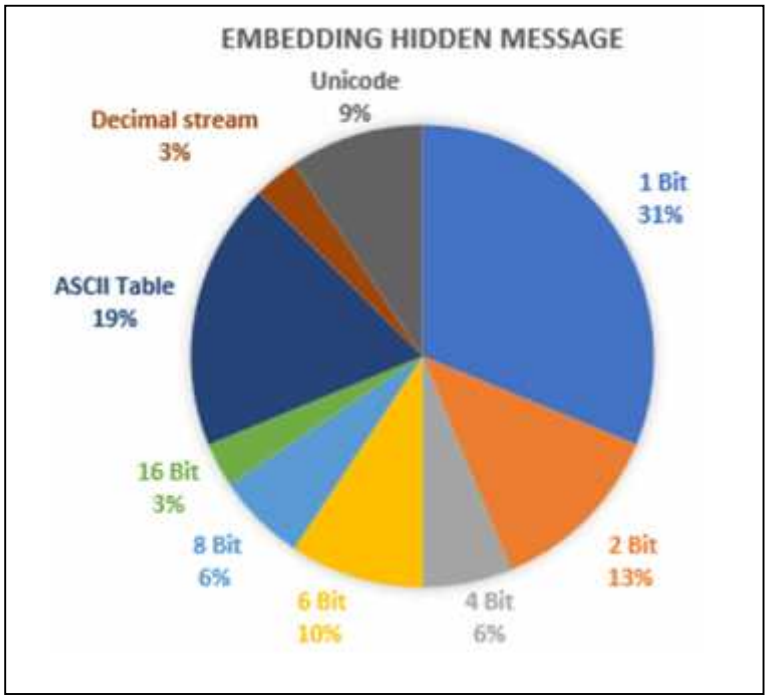

Figure 2: The previous research efforts in converting embed hidden message in last decade (2011-2023)

Based on Figure 2, it displays the embedding hidden message by previous researchers from 2011 until the present that consists of six embedding process techniques. The first conversion was by embedding one bit in the text (31%), followed by embedding the cover text using converting ASCII from hidden messages (19%). The embedding of the hidden message with two bits and six bits achieves the same percentage of 10%, then embeds using Unicode into cover text for 9%. Moreover, the embedding into cover text uses four binary bits and eight binary bits with 6%. Then, the least percentage is embedding the hidden message by converting to 16 binary bits and a decimal stream at 3%. Then, the specific techniques of feature-based method that ulitize the several embedding hidden message in the text in Table 1

Table 1: Several techniques of embedding hidden message in feature-based method

No.	Embedding in the Text	Techniques on Feature-based Method
1	Embedding 1 bit	Curve subheading, vertical straight line (Dulera et al., 2011a), Change alphabet letter pattern (Bhattacharyya et al., 2011), Encryption with cover text (Kataria et al., 2013), Back end interface web (Mahato et al., 2013), Character pair text (Akotoye et al., 2018), HTML web page (Bajaj & Aggarwal, 2019), Arabic text cryptography (Ditta et al., 2020), Zero-width joiner (Alanazi et al., 2020), Polynomial encryption (Guan et al., 2022)
2	Embedding 2 bit	Quadruple characterization(Dulera et al., 2011b), Secret steganography code for embedding (Banerjee et al., 2011), Content-based feature (Kouser et al., 2016), AITSteg via social media (Taleby Ahvanooey et al., 2018)
3	Embedding 4 bit	Right remark, left remark (Ammar Odeh et al., 2014), Alphabet pairing text (Iyer & Lakhtaria, 2016b)
4	Embedding 6 bit	Coverless English text (Wu et al., 2018), Font color Ms Excel (Alsaadi et al., 2018)
5	Embedding 8 bit	Huffman compression (Malik et al., 2017), Deep learning of Arabic text (Siddiqui et al., 2020)
6	Embedding 16 bit	Coloring spacing normalization (Thabit et al., 2022)
7	Embedding based ASCII Table	Alphabet pairing text of ASCII (Iyer & Lakhtaria, 2016a), English text using number oriented (Mandal et al., 2017), Binary digit mapping on ASCII (Naharuddin et al., 2019), Secret sharing message system (Sharma et al., 2020), Webometric text steganography (Yaghobi & Sajedi, 2021), Binary mapping using ASCII (Saad et al., 2023)
8	Embedding using decimal stream	Multilayer partially homomorphic (Naqvi et al., 2018)
9	Embedding based Unicode	Unicode standard seamless (Alanazi et al., 2020), Unispach Xor and Shift (Taka, 2021), Unicode character in multilingual (Baawi et al., 2020)

Table 1 shows several technique of fetuare-based method that utilized in last decade (2021-2023) that embed the hidden message into text. The total number of embedding processes by using one bit with 10 research efforts, embedding two bits with four research efforts and embedding four bits with two research efforts. It follows by embedding six bits with three research efforts, embedding eight bits with two research efforts and embedding 16 bits with only one research efforts. Then, embedding using ASCII table with six research efforts, decimal streang with only one research effort and using Unicode with three research efforts. In short the highest embedding process is embed one bit hidden message and the lowest are embedding 16 bit and using decimal stream with only one previous research effort.

5. Conclusions

In conclusion, this paper reviews the utilisation of the precious research effort in developing a feature-based technique for converting the hidden message into a binary bit or code embedding message. It discovers the most efficient embedding process for hidden messages into binary bits that embed 1 bit into the text later. Then, it follows with the order of the embedding hidden message by ASCII table, embedding two bits, six bits, four bits, and eight bits in order of the total number of embed processes. The least-embedded hidden message by using 16-bit binary and decimal streams is based on a review of previous research efforts in the last decade. This paper expectedly contributes to more consideration of implementation feature-based techniques, such as embedding the binary bit and code into the text-based that is important for the stego key in generating stego text.

Acknowledgments

The authors would like to express our grateful to School of Computing of Universiti Utara Malaysia. This paper was supported by Universiti Utara Malaysia.

References

Ahvanooey, M. T., Li, Q., Hou, J., Rajput, A. R., & Chen, Y. (2019). Modern text hiding, text steganalysis, and applications: A comparative analysis. *Entropy*, *21*(4), 1–29. https://doi.org/10.3390/e21040355

Akotoye, F. X. K., Yakavor, Y. E., Kwofie, J., & Tirogo, F. La. (2018). Character Pair Text Steganography based on

the enhanced Paragraph Approach. *IEEE 7th International Conference on Adaptive Science and Technology (ICAST)*, 1–5. https://doi.org/10.1109/ICASTECH.2018.8507117

Al-Alwani, W., Mahfooz, A. Bin, & Gutub, A. A. A. (2007). A Novel Arabic Text Steganography Method Using Extensions. *Proceeding of World Academy of Science, Engineering and Technology*, *1*(3), 483–486.

Alanazi, N., Khan, E., & Gutub, A. (2020). Functionality-Improved Arabic Text Steganography Based on Unicode Features. *Arabian Journal for Science and Engineering*, *45*(12), 11037–11050. https://doi.org/10.1007/s13369-020-04917-5

Alaqeel, A. I., & Saleh, M. S. (2021). Developing a Performance-based Tool for Arabic Text Steganography. *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*, *2*. https://doi.org/10.1109/NCCC49330.2021.9428837

Alhaddad, M. J., Alkinani, M. H., Atoum, M. S., & Alarood, A. A. (2020). Evolutionary detection accuracy of secret data in audio steganography for securing 5G-enabled internet of things. *Symmetry*, *12*(12), 1–18. https://doi.org/10.3390/sym12122071

Alsaadi, H. I., Al-Anni, M. K., Almuttairi, R. M., Bayat, O., & Ucan, O. N. (2018). Text steganography in font color of MS excel sheet. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3279996.3280006

Baawi, S. S., Nasrawi, D. A., & Abdulameer, L. T. (2020). Improvement of "text steganography based on unicode of characters in multilingual" by custom font with special properties. *IOP Conference Series: Materials Science and Engineering*, *870*(1). https://doi.org/10.1088/1757-899X/870/1/012125

Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. *Procedia Computer Science*, *46*(Icict 2014), 612–618. https://doi.org/10.1016/j.procs.2015.02.105

Bajaj, I., & Aggarwal, R. K. (2019). Steganography using HTML Web Pages as a Carrier: A Survey. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3351033

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2011). Novel text steganography through special code generation. *Proceedings of International Conference on Systemics, Cybernetics and Informatics (ICSCI-2011)*, 298–303.

Bansal, D., & Chhikara, R. (2014). Performance evaluation of steganography tools using SVM and NPR tool. *4th International Conference on Advanced Computing and Communication Technologies, ACCT 2014*, 483–487. https://doi.org/10.1109/ACCT.2014.17

Bhattacharyya, S., Indu, P., Dutta, S., Biswas, A., & Sanyal, G. (2011). Hiding Data in Text Through Changing in Alphabet Letter Patterns (CALP). *Journal of Global Research in Computer Science*, *2*(3).

Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal*, *30*(2), 63–87. https://doi.org/10.1080/19393555.2020.1801911

Din, R., Bakar, R., Sabri, R. S., Darus, M. Y., & Elias, S. J. (2019). Performance analysis on secured data method in natural language steganography. *Bulletin of Electrical Engineering and Informatics*, *8*(1), 298–304. https://doi.org/10.11591/eei.v8i1.1441

Din, R., Bakar, R., Utama, S., Jasmis, J., & Elias, S. J. (2019). The evaluation performance of letter-based technique on text steganography system. *Bulletin of Electrical Engineering and Informatics*, *8*(1), 291–297. https://doi.org/10.11591/eei.v8i1.1440

Din, R., Mahmuddin, M., & Qasim, A. J. (2019). Review on Steganography Methods in Multi-Media Domain. *International Journal of Engineering & Technology, 8 (1.7) (2019) 288-292 International*, *8*(August), 6.

Din, R., & Qasim, A. J. (2019). Steganography Analysis Techniques Applied to Audio and Image Files. *Bulletin of Electrical Engineering and Informatics*, *8*(4), 1297–1302. https://doi.org/10.11591/eei.v8i4.1626

Ditta, A., Azeem, M., Naseem, S., Gulzar Rana, K., Adnan Khan, M., & Iqbal, Z. (2020). 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*. https://doi.org/10.1016/j.jksuci.2020.07.010

Dulera, S., Jinwala, D., & Dasgupta, A. (2011a). Experimenting with the Novel Approaches in Text Steganography. *International Journal of Network Security & Its Applications*, *3*(6), 213–225. https://doi.org/10.5121/ijnsa.2011.3616

Dulera, S., Jinwala, D., & Dasgupta, A. (2011b). Experimenting with the Novel Approaches in Text Steganography. *International Journal of Network Security & Its Applications*, *3*(6), 213–225.

Guan, B., Gong, L., & Shen, Y. (2022). A Novel Coverless Text Steganographic Algorithm Based on Polynomial Encryption. *Security and Communication Networks*, *2022*, 1–12. https://doi.org/10.1155/2022/1153704

Iyer, S. S., & Lakhtaria, K. (2016a). Clustering Algorithm for Text Steganography. *International Journal of Advanced Research in Computer and Communication Engineering*, 74–77. https://doi.org/10.17148/IJARCCE

Iyer, S. S., & Lakhtaria, K. (2016b). New robust and secure alphabet pairing Text Steganography Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(7), 15–21.

Kataria, S., Singh, K., Kumar, T., & Nehra, M. S. (2013). ECR (encryption with cover text and reordering) based text steganography. *Image Information Processing (ICIIP), 2013 IEEE Second International Conference On*, 612–

616.

Kouser, S., Khan, A., & Qamar, E. (2016). A Novel Content-Based Feature Extraction Approach : Text Steganography. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(12), 916–923.

Kumar, R., Chand, S., & Singh, S. (2014). An Email based high capacity text steganography scheme using combinatorial compression. *International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, 336–339.

Ma, Y., Luo, X., Li, X., Bao, Z., & Zhang, Y. (2019). Selection of Rich Model Steganalysis Features Based on Decision Rough Set α-Positive Region Reduction. *IEEE Transactions on Circuits and Systems for Video Technology*, *29*(2), 336–350. https://doi.org/10.1109/TCSVT.2018.2799243

Mahato, S., Yadav, D. K., & Khan, D. A. (2013). A Modified Approach to Text Steganography Using HyperText Markup Language. *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, 40–44. https://doi.org/10.1109/ACCT.2013.19

Malik, A., Sikka, G., & Verma, H. K. (2017). Engineering Science and Technology , an International Journal A high capacity text steganography scheme based on LZW compression and color coding. *Engineering Science and Technology, an International Journal*, *20*(1), 72–79. https://doi.org/10.1016/j.jestch.2016.06.005

Mandal, K. K., Koley, S., & Dhar, S. (2017). A Mathematical Model for Secret Message Passing using Steganography. *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), January*. https://doi.org/10.1109/ICCIC.2016.7919527

Manikandan, G., Bala Krishnan, R., Rajesh Kumar, N., Narasimhan, D., Srinivasan, A., & Raajan, N. R. (2018). Steganographic approach to enhancing secure data communication using contours and clustering. *Multimedia Tools and Applications*, *77*(24), 32257–32273. https://doi.org/10.1007/s11042-018-6237-5

Muhammad, M. H., Hussain, H. S., Din, R., Samad, H., & Utama, S. (2021). *Review on feature-based method performance in text steganography*. *10*(1), 427–433. https://doi.org/10.11591/eei.v10i1.2508

Naharuddin, A., Wibawa, A. D., & Sumpeno, S. (2019). A High Capacity and Imperceptible Text Steganography Using Binary Digit Mapping on ASCII Characters. *Proceeding - 2018 International Seminar on Intelligent Technology and Its Application, ISITIA 2018*, 287–292. https://doi.org/10.1109/ISITIA.2018.8711087

Naqvi, N., Abbasi, A. T., Hussain, R., Khan, M. A., & Ahmad, B. (2018). Multilayer Partially Homomorphic Encryption Text Steganography (MLPHE-TS): A Zero Steganography Approach. *Wireless Personal Communications*, *103*(2), 1563–1585. https://doi.org/10.1007/s11277-018-5868-1

Nechta, I. V. (2018). New Steganalysis Method for Text Data Produced by Synonym Run-Length Encoding. *2018 14th International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering, APEIE 2018 - Proceedings*, 188–190. https://doi.org/10.1109/APEIE.2018.8545230

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.

Odeh, A., Alzubi, A., Hani, Q. B., & Elleithy, K. (2012). Steganography by multipoint Arabic letters. *2012 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–7. https://doi.org/10.1109/LISAT.2012.6223209

Odeh, A., Elleithy, K., Faezipour, M., & Background, A. (2014). Fast Real-Time Hardware Engine for Multipoint Text Steganography. *IEEE Long Island Systems, Applications and Technology (LISAT) Conference*.

Reddy, R. P. K., Nagaraju, C., Subramanyam, N., & Ntroduction, I. (2014). Text Encryption Through Level Based Privacy using Dna Steganography. *International Journal of Emerging Trends & Technology in Computer Science*, *3*(3). 168-172

Saad, E., Al, N., & Algamdi, A. (2023). Survey steganography applications. *As-Salam Journal for Engineering and Technology*, 69–75.

Sharma, A., Singh, P. K., & Kumar, Y. (2020). An integrated fire detection system using IoT and image processing technique for smart cities. *Sustainable Cities and Society*, *61*, 102332. https://doi.org/10.1016/j.scs.2020.102332

Siddiqui, G. F., Iqbal, M. Z., Saleem, K., Saeed, Z., Ahmed, A., Hameed, I. A., & Khan, M. F. (2020). A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. *IEEE Access*, *8*, 181893–181903. https://doi.org/10.1109/ACCESS.2020.3028315

Singh, A. P., Moudgil, S., & Rani, S. (2021). An Acquaintance to Text-Steganography and its Methods. *Journal of Physics: Conference Series*, *1950*(1). https://doi.org/10.1088/1742-6596/1950/1/012005

Su, Y., Yu, F., & Zhang, C. (2017). Digital video steganalysis based on a spatial temporal detector. *KSII Transactions on Internet and Information Systems*, *11*(1), 360–373. https://doi.org/10.3837/tiis.2017.01.019

Taka, F. R. S. (2021). Text Steganography based on Noorani and Darkness. *Journal of Information Hiding and Multimedia Signal Processing*, *12*(3), 127–139.

Taleby Ahvanooey, M., Li, Q., Hou, J., Dana Mazraeh, H., & Zhang, J. (2018). AITSteg: An innovative text steganography technique for hidden transmission of text message via social media. *IEEE Access*, *6*, 65981–

65995. https://doi.org/10.1109/ACCESS.2018.2866063

Tayyeh, H. K., Mahdi, M. S., & AL-Jumaili, A. S. A. (2019). Novel steganography scheme using Arabic text features in Holy Quran. *International Journal of Electrical and Computer Engineering*, *9*(3), 1910–1918. https://doi.org/10.11591/ijece.v9i3.pp1910-1918

Thabit, R., Udzir, N. U. R. I., & Gutub, A. A. (2022). CSNTSteg : Color Spacing Normalization Text Steganography Model to Improve Capacity and Invisibility of Hidden Data. *IEEE Access*, *10*, 65439–65458. https://doi.org/10.1109/ACCESS.2022.3182712

Tong, Y., Liu, Y., Wang, J., & Xin, G. (2019). Text steganography on RNN-Generated lyrics. *Mathematical Biosciences and Engineering*, *16*(5), 5451–5463. https://doi.org/10.3934/mbe.2019271

Utama, S., & Din, R. (2022). Performance Review of Feature-Based Implementation Text Steganography Approach Method. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *2*(2), 325–333.

Wu, Y., Chen, X., & Sun, X. (2018). Coverless steganography based on english texts using binary tags protocol. *Journal of Internet Technology*, *19*(2), 599–606. https://doi.org/10.3966/160792642018031902028

Xiang, L., Yang, S., Liu, Y., Li, Q., & Zhu, C. (2020). Novel linguistic steganography based on character-level text generation. *Mathematics*, *8*(9), 1–18. https://doi.org/10.3390/math8091558

Xiang, L., Yu, J., Yang, C., Zeng, D., & Shen, X. (2018). A word-embedding-based steganalysis method for linguistic steganography via synonym substitution. *IEEE Access*, *6*(c), 64131–64141. https://doi.org/10.1109/ACCESS.2018.2878273

Yaghobi, S. R., & Sajedi, H. (2021). Text steganography in webometrics. *International Journal of Information Technology (Singapore)*, *13*(2), 621–635. https://doi.org/10.1007/s41870-020-00572-z

Yang, Z., Huang, Y., & Zhang, Y. J. (2019). A Fast and Efficient Text Steganalysis Method. *IEEE Signal Processing Letters*, *26*(4), 627–631. https://doi.org/10.1109/LSP.2019.2902095

Zhang, H., Cao, Y., Zhang, W., Yu, N., & Zhao, X. (2014). Video Steganography with Perturbed Macroblock Partition. *Proceeding of the 2nd ACM Workshop on Information Hiding and Multimedia Security*, 115–122.