

Journal of Advanced Research Design

ADVANCED RESEARCH DESIGN

Journal homepage: https://akademiabaru.com/submit/index.php/ard ISSN: 2289-7984

Feature-Based Method using Binary Alphabet-Based Technique in Text Steganography

Nik Fatinah N. Mohd Farid^{1,*}, Roshidi Din¹, Nuramalina Na'in¹, Wan Aida Nadia Wan Abdullah¹, Azian Muhamad Adzmi²

- School of Computing UUM College of Arts and Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia
- Department of Media and Communication, College of Social Sciences, KIMEP University, 050010 Almaty, Kazakhstan

ARTICLE INFO

ABSTRACT

Article history:

Received 10 February 2025 Received in revised form 21 March 2025 Accepted 31 July 2025 Available online 11 August 2025

Information security is an important aspect of safeguarding digital assets and ensuring the security of any sensitive information. In this context, steganography is essential in hiding information within apparently harmless carriers such as images, audio files or text, with the goal of avoiding detection by unauthorized parties. Numerous scholars in the past have strived to apply steganography specifically in the text domain, utilizing distinctive feature-based methods to implant letters that camouflage the concealed message within textual content. The majority of feature-based techniques embed a hidden message by converting it into binary bits. This paper introduces a novel featurebased technique that transforms the hidden message into binary bits, representing each text letter with two binary bits across both uppercase and lowercase alphabets. The technique utilizes an alphabet-based sequence table to correlate the sequence number of letters in the hidden message with the corresponding binary bits. This approach anticipates streamlining the embedding process, generating stego text with a concealed message while minimizing the binary bit length required to cover the message. The novel technique is evaluated against previous techniques in terms of both single-bit and dual-bit feature-based techniques. This efficient approach minimizes the binary bit length needed to cover the message, achieving 100% embedding performance in limited sentences of cover text when implementing the feature-based method.

Keywords:

Hidden message; stego key; stego text; word-rule based; digital steganography

1. Introduction

Securing information is crucial in today's technology and communication, especially when sharing data over open networks [1,2]. Ensuring the protection of digital assets is essential, emphasizing the importance of maintaining the security elements of any sensitive information. Steganography, a part of information security, helps with covert communication and data protection. The easy accessibility of information worldwide on open networks, without territorial restrictions, raises concerns due to widespread document fabrication and forgery. This poses significant risks, including losses for individuals, communities, industries and national security. Sharing information online exposes it to

E-mail address: nikfatinah@uum.edu.my

https://doi.org/10.37934/ard.143.1.4354

^{*} Corresponding author



unauthorized users [3-5]. Therefore, using steganography techniques is essential to address these potential problems regarding the implementation of information steganography [6-10].

Steganography is the practice of concealing information to hide signals within messages across various mediums, making them imperceptible to both human vision and automated devices [10,11]. When considering performance in information concealment technology, the goal of steganography is to ensure the protection of hidden information. Throughout history, steganography has been employed to secure covert messages when sharing information in crucial communications [12-15]. The primary objective of utilizing steganography is to conceal sensitive information during different modes of data transfer [15]. Figure 1 provides a visual representation of the categories and hierarchy involved in implementing steganography.

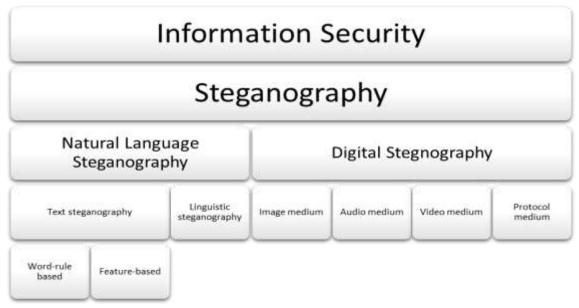


Fig. 1. Steganography field implementation from [19,20]

Based on Figure 1, steganography techniques are classified into two categories with distinct applications: digital steganography and methods utilizing natural language. Digital steganography, falling under the first category, is utilized in non-textual mediums such as images, sounds, videos and protocol channels [16,17]. The second category, referred to as natural language steganography also known as text steganography, primarily employs the steganographic mechanism within text. It is a security technique used to conceal messages within other non-secret text, ensuring that the presence of the hidden message is undetectable to an observer. Unlike encryption, which scrambles data into an unreadable form, text steganography embeds the hidden message directly into the carrier text, making it appear ordinary and innocuous. This entails incorporating the hidden message into the text to evade detection by third parties. In short, natural language steganography effectively conceals the concealed message from potential intruders [18,19]. The implementation of natural language steganography comprises two categories: linguistic steganography and text steganography. In linguistic steganography, textual features specific to language are employed to hide a message within the text, using linguistic variations as principles for embedding the confidential message [20,21].

Meanwhile, text steganography utilizes various text elements like words, text lines, spacing and other textual features to hide confidential messages [22-25]. It exerts no influence on the linguistic structure of text, in contrast to linguistic steganography [26,27]. This divergence is rooted in text steganography's focus on the text's components and criteria rather than linguistic principles during the process of concealing hidden messages [28]. It consists of two methods of text steganography



which are word-rule based method and feature-based method. In world-rule based. The word-rule based method involves manipulating the hidden message by shifting it horizontally and vertically within the text medium. Conversely, the feature-based method conceals the hidden message by leveraging distinctive characteristics of letters, such as adjusting their shape, position, size and form within the textual medium [12,21].

This paper specifically focuses on advancing a feature-based method within text steganography [29]. This method facilitates the concealment of messages by integrating them according to the distinctive characteristics of letters in languages utilizing the A-Z alphabet [18]. The aim of this paper is to contribute to the enhancement and diversification of text steganography techniques, particularly in utilizing feature-based approaches to covertly embedded hidden messages within the text.

2. Related Work

Text steganography, a feature-based approach involves modifying distinct text features using a designated code word. This can be achieved through various methods, such as altering the formatting, using invisible characters or manipulating the structure of sentences. These features include word orientation, whether vertical or horizontal and word length, where the orientation might slightly shift up and down and the code word's length could either contract or expand to incorporate parts of a hidden message within text data [30-32]. The goal is to transmit sensitive information securely without raising suspicion that other communication is taking place. Text steganography is particularly valuable in environments where encryption is monitored or forbidden, providing an alternative method for confidential communication. This study employs a feature-based method, utilizing frequency normalization in columns for embedding letter selection [33]. The concealed message is derived from inter-word spaces and specific text placements, using the Unicode system with paired binary bits. In this method, the Unicode function possesses the ability to hide three characters, providing a total of eight potential pathways for the execution of the hiding process.

Another feature-based technique in steganography applied for concealing information was within the web-page environments. These techniques utilize specific characteristics or attributes of the content to securely embed hidden data. In the context of text steganography, feature-based methods are preferred for their simplicity and effectiveness [34]. By leveraging features inherent to the content, such as structural elements or visual properties, these techniques can subtly encode information within web pages. Other work by Bajaj et al., [35] introduced a feature-based approach for web-page environments, specifically focusing on HTML. It embeds the binary bits of the hidden message within italic and underline tags at the back end of the protocol medium on the website. This method effectively converts a large amount of data into hexadecimal in the HTML source code, making it a robust approach for concealing extensive or lengthy text.

The implementation of feature-based technique also utilizes the ASCII table in embedding process. Naharuddin *et al.*, [36] proposed a feature-based technique involving the mapping of binary bits into elements of the ASCII table to conceal hidden messages. The mapping process establishes the order of binary bits derived from the hidden message, introducing an additional number within the range of 1 to 7. This additional number determines both the column and row for placing the embedded text. Unlike focusing on text length capacity, this technique attains high-capacity functionality by hiding the covert message through row and column positioning. Moreover, Mandal *et al.*, [37] implemented number oriented in English text that adopted from mathematical model in ASCII value. This technique embeds the hidden message using ASCII that convert into number pair of group letter that changes the position the letter to create the stego text. Meanwhile, it extracts the



stego text based on co-ordinate by ascending order of number pair-based value decode accumulated from collection in ASCII value.

Wu et al., [38] proposed a feature-based method utilizing single-bit embedding within a coverless medium. This method embeds the hidden message within text by employing a single binary bit within the same word, utilizing Markov chain principles. This involves altering transitions within the text, leveraging the uniqueness of each word as a location for embedding the binary bit. While this technique demonstrates high-performance effectiveness in text steganography, it does not comprehensively address the transition order of the hidden message within the text. Furthermore, the use of a single binary bit per word simplifies the embedding process, enhancing the algorithm's efficiency. However, this approach may not fully capture the intricate transition patterns required for complete concealment of the hidden message within the text. To enhance the technique's efficacy, future research could explore methods to incorporate additional binary bits per word or refine the Markov chain transition modelling. Additionally, comprehensive testing across various text types and lengths is necessary to evaluate the method's robustness and scalability in real-world applications.

Furthermore, Kataria *et al.*, [39] devised a text steganography solution known as Encryption with Cover Text and Reordering (ECR) using ExOR, which enables quick embedding and extraction. However, the process of integrating the two characters posed challenges in retrieving the enciphered text's original message. This method employed bit 0 to describe cover text and bit 1 for encrypted content, rearranging among eight numbers of binary bits of a random key. Moreover, Bhattacharyya [40] introduced an innovative technique for concealing the hidden message by altering the letter characteristics of the English alphabet. Depending on the binary bit sequence, characters with dots, such as character 'i' or 'j', are embedded into bit 0, while characters 'A', 'a' and 'c' are incorporated into bit 1. This method offers a unique approach to enhance the covert transmission of information within the text domain.

Then, Dulera *et al.*, [30] proposed a method for character concealment using a combination of feature-based and English characters of random character sequences. This technique transforms messages into binary bits, categorizing them based on letter shapes. Curved letters hide bit 0, while letters without curves hide bit 1. The method also involves concealing letters with a vertical line that called VERT technique, where remaining letters are concealed within bit 0 and the vertical line is obscured within bit 1. Additionally, letter types are grouped into four classifications is named as QUAD technique: curved letters are linked to bits 00, letters with a solitary vertical line are associated with bits 10, letters with central horizontal lines are connected to bits 01 and letters with diagonal lines are tied to bits 11. This paper utilizes VERT technique and QUAD technique as the comparison alpha-based technique of feature-based method because utilized as benchmark and comparison technique by previous researchers [34,41,42]. It used VERT technique as single bit and QUAD technique as dual bit representative technique that able to compare with the binary Alpha-based technique as feature coding method.

3. Methodology

The fundamental technique outlined is based on the representative binary table for the Alphabet-based method, as shown in Table 1.



Table 1Alphabet-based representative binary

| Alphabet-based se | • | | |
|-------------------|-------------------------------|----|-----------|
| Letter | Uppercase Number of sequences | | Lowercase |
| Binary bit | 01 | | 10 |
| Represent Binary | Α | 1 | a |
| | В | 2 | b |
| | С | 3 | С |
| | D | 4 | d |
| | E | 5 | е |
| | F | 6 | f |
| | G | 7 | g |
| | Н | 8 | h |
| | 1 | 9 | i |
| | J | 10 | j |
| | K | 11 | k |
| | L | 12 | 1 |
| | M | 13 | m |
| | N | 14 | n |
| | 0 | 15 | 0 |
| | Р | 16 | р |
| | Q | 17 | q |
| | R | 18 | r |
| | S | 19 | S |
| | Т | 20 | t |
| | U | 21 | u |
| | V | 22 | V |
| | W | 23 | w |
| | X | 24 | x |
| | Υ | 25 | У |
| | Z | 26 | Z |

Table 1 serves as a categorical indicator for the types of letters incorporated within the text, distinguishing between uppercase and lowercase letters. In this schema, the binary bit '01' is designated for uppercase letters, while '10' is assigned to lowercase letters. These binary indicators are employed in conjunction with a numerical sequence that enumerates the letters from A to Z. This table will serve as a guide for converting the cover text incorporating the hidden message associating the binary bit and its number of sequences in generating the stego text.

3.1 Binary Alphabet-Based Technique

The technique utilizing a binary alphabet-based system comprises of two distinct stages: embedding and extraction. This methodology involves the construction of a cover text that ingeniously incorporates a concealed message via a specialized binary conversion.

In Figure 2, the flowchart illustrates a steganographic technique for concealing and revealing covert messages within text by manipulating letter capitalization to represent binary data. Initially, the input text is segmented into two parts: the cover text and the hidden message, both of which are converted into binary. Depending on the presence of a steganographic key, the binary digits determine whether uppercase or lowercase letters are employed to discreetly integrate the message within the cover text. The resulting stego text, containing the encoded message, facilitates message extraction by recovering binary bits from the text and converting them back into the original hidden



message, thereby concluding the process. This approach enables secure and clandestine communication by concealing information in plain view.

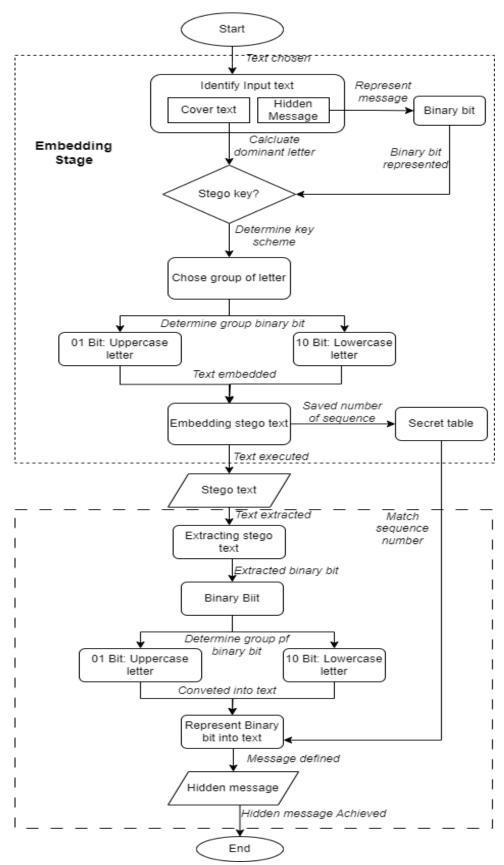


Fig. 2. Flow process of binary alpha-based technique



Unlike the standard binary conversion, which assigns a fixed binary value to each alphabet character as depicted in Table 2, the representational binary differs.

Table 2

Comparison of converting and representing binary bit

| Comparison of converting and representing binary bit | | | | |
|--|-------------------------------------|----------|--|--|
| Hidden Messa | Represent binary | | | |
| | 01000100 01100001 01110100 01100001 | 01101010 | | |
| Data | | | | |

Table 2 shows hidden message with the word 'Data' used 32 binary bits in the normal conversion process. Meanwhile, the binary alphabet-based technique only uses eight number bits to represent the word "Data" as the hidden message. For instance, an uppercase 'D' is encoded as '01000100', while a subsequent lowercase 'a' is encoded as '01100001' and the process continues to the end of the message. However, this form of conversion may limit the efficiency of data embedding due to its increased predictability and uniform structure [43]. Moreover, the transparent methodology of data conversion to binary format might increase the detectability of the encoded message, potentially making it more vulnerable to steganalysis techniques [44].

The main process of the binary alpha-based technique consists of two processes with are embedding and extracting process as the stages in executing to implement this technique as feature-based method.

3.2 Stage I: Embedding

The initial phase of the binary alphabet-based technique is characterized by the transmission of a concealed message embedded within a selected cover text. The pivotal mechanism of this strategy requires the precise alignment of the embedded letters within the cover text. Thus, the construction of a cover text that embodies the exact sequence of concealed letters, inclusive of both uppercase and lowercase forms, is crucial. During this phase, a conversion procedure is undertaken to derive the representational binary bit. This involves a systematic transformation of the hidden message into an alphabet-based representation, which is subsequently converted into representational binary bits.

3.3 Stage II: Extracting

The second stage of the alphabet-based technique is the extraction process, which is fundamentally concerned with the unveiling of the encoded messages from their representational binary bit form. This stage comprises the reversal of the prior embedding process. The methodology initiates with the transformation of the representational binary bits into their corresponding alphabet-based representatives. This step is a critical precursor to the ultimate objective of the extraction phase: to elucidate and present the originally concealed message in a discernible format.

4. Results and Discussion

The comprehensive procedure of the proposed technique was illustrated in Figure 3. It begins with the embedding process in determining the cover text and hidden message that represent binary bits. Moreover, the process involves extracting the number of sequences from both the hidden message and the binary bit list in the Alphabet-based technique table. The binary bit is then embedded in the cover text, utilizing one selected letter to generate the stego text. In the extraction phase, the stego text is restored to unveil the binary bit by referencing the Alphabet-based technique



table. Then, the binary will be matched with the number of sequences in the Alphabet-based technique table to discover the hidden message. Thus, the implementation of the proposed technique is called Alphabet-based represent binary of feature-based method in text steganography.

I. Embedding Stage

Hidden message: "Data"

Covertext: "Development and implementation system in technology"

Conversion Table:

| Hidden Message | D | а | t | а |
|-------------------------------|---|----|----|----|
| Alphabet-based representative | | 1 | 20 | 1 |
| Represent Binary | | 10 | 10 | 10 |

Embedded Text (Stego text) and their corresponding position:

D⁰¹evelopment a¹⁰nd implement¹⁰a¹⁰tion system in technology



II. Extracting Stage

Stego text:

Development and implementation system in technology

Conversion Table:

| Represent Binary | 01 | 10 | 10 | 10 |
|-------------------------------|----|----|----|----|
| Alphabet-based representative | | 1 | 20 | 1 |
| Hidden Message | | а | t | а |

Hidden message: Data

Fig. 3. The overview of implementation of alphabet-based technique with two stages embedding and extracting through example

In Figure 3, it shows the implementation of binary Alphabet-based technique that differ with the standard technique of feature-based technique that convert the hidden message into binary bits. In this technique, every character letter, whether uppercase or lowercase, serves as a carrier for hidden messages within the text. During the embedding process, each letter from the hidden message corresponds to the same letter in the cover text. Notably, uppercase letters represent '01' bits, while lowercase letters represent '10' bits, integrating them discreetly into the cover text. The number of bits from the hidden message is concealed within the cover text using matching character letters. Subsequently, these embedded numbers ordered by letters, are stored in a secret table within the system post embedding or extracting process.



Furthermore, this paper considers the VERT and QUAD technique as the comparison of with this technique. The VERT technique as the single bit hiding process and QUAD technique as dual bit technique of feature-based method in hiding the binary bit in generate the stego text. These two techniques compare the performance with the proposed technique using evaluation letter used and binary bit embedded that become the important process in feature-based method. The evaluation used the cover text from Figure 3 with sentence "Development and implementation system in technology" and hidden message "Data" in processing in hide the text. For two techniques the hidden message "Data" convert into binary bit "01000100 01100001 01110100 01100001" with a total of 32 numbers. In VERT technique, it used single bit implementation that has to embed 32 number binary bits in the cover text, while QUAD technique as dual bit that has to embed 32 number binary bits in 16 letters for generating the stego texts. However, the Alpha-based only used eight binary bits that has to embed only four letters in embedding process. The comparison of technique shows in Table 3.

Table 3Result comparison of alpha-based technique with other technique of feature-based method

| Techniques | Total binary bit | Expected binary embedded | Letter used | % Binary bit embedded |
|--------------------|------------------|--------------------------|-------------|-----------------------|
| VERT | 32 | 32 | 21 | 65.63% |
| QUAD | 32 | 16 | 11 | 68.75% |
| Binary Alpha-based | 8 | 4 | 4 | 100.00% |

Table 3 shows the comparison the three techniques of feature-based technique in embedding the binary bits in the cover text. Binary Alpha-based technique achieves 100% binary bit embedded performance that the letter used and expected binary bit has same number with four numbers. Meanwhile, the VERT technique achieves 65.63% that only 21 letters used that should be embedded 32 binary bits. Then, the QUAD technique achieves 68.75% that 16 binary bit that used only 11 letters used in embedded process that means lost some of binary bits in generating the stego text. Based on this performance, it seems the binary Alpha-based technique has the accurate embedding process with limited the cover texts.

5. Conclusion

In conclusion, this paper introduced a novel feature-based method known as Alphabet-based binary representation for generating stego text by utilizing both uppercase and lowercase letters. The technique employs a specialized table, the Alphabet-based Sequence table, to assign binary representations (01 for uppercase and 10 for lowercase) to each letter. During the embedding process, the numerical order of letters is utilized, allowing the hidden message to be seamlessly integrated into the cover text. The proposed approach effectively utilizes character letters as hidden messages, with the representation of uppercase and lowercase letters as 01 and 10 bits, respectively. A key distinction between the Alphabet-based binary representation technique and common feature-based methods lies in the conversion of hidden messages into binary bits. The paper demonstrates this by comparing the binary representation of the word "Data" using the conventional method (32 bits) and the proposed Alphabet-based technique (8 bits), highlighting the efficiency of the latter.

The execution process of the Alphabet-based binary representation technique within the feature-based method involves embedding and extracting processes. The embedding process integrates binary bits into generating the stego text by choosing particular letters from the cover text.



Subsequently, during the extraction process, the stego text extract the hidden message becomes apparent by aligning the binary bits with the sequences found in the Alphabet-based technique table.

Moreover, the performance of the binary Alpha-based technique is compared with two techniques: the VERT technique, which uses a single bit and the QUAD technique, which uses dual bits. The two techniques only achieve 65.63% for the VERT technique and 68.75% for the QUAD technique in terms of binary bit embedding performance. Meanwhile, the binary Alpha-based technique achieves 100% binary bit embedding performance, accurately embedding bits in the stego text despite the limited text available. This implementation of the binary Alpha-based technique demonstrates its effectiveness within the broader context of feature-based methods for text steganography.

6. Future Work

As part of the trajectory for future research in text steganography, the current study prompts an intensified scrutiny of security measures inherent in the Alphabet-based represent binary technique. Augmenting the safeguarding mechanisms against potential threats necessitates a meticulous exploration of incorporating supplementary encryption or obfuscation methodologies. This strategic fortification aims to elevate the resilience of the system, ensuring heightened protection of concealed messages against unauthorized access. Furthermore, the imperative for a comprehensive robustness analysis becomes evident, demanding an in-depth evaluation of the Alphabet-based represent binary technique's performance across heterogeneous conditions. This entails an investigation into its adaptability to diverse text types, languages and potential adversarial attacks. A systematic assessment of the method's resilience against common steganalysis approach is necessary to clarify its overall effectiveness and pinpoint any potential vulnerabilities.

Simultaneously, the inquiry into the potential integration of the Alphabet-based technique with other steganographic methods or embedding algorithms emerges as a noteworthy avenue for further investigation. Delving into the intricacies of merging multiple approaches offers the prospect of forging a sophisticated and resilient framework for information hiding. This line of inquiry seeks to create hybrid techniques that leverage the distinct strengths of individual methods, concluding in heightened security and broader applicability across varied contexts. In essence, these articulated propositions for future research endeavours aspire to propel the Alphabet-based technique toward enhanced security, adaptability and efficacy within the dynamic realm of text steganography.

Acknowledgement

This research was funded by the Universiti Utara Malaysia (UUM) under *Geran Penjanaan Penyelidikan* 2024. (SO Code: 21657).

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. https://doi.org/10.1007/s11042-019-08025-x
- [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/10.1016/j.procs.2015.02.105
- [3] 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
- [4] Kouser, Saeeda and Aihab Khan. "A Novel Feature Extraction Approach: Capacity Based Zero-Text Steganography." *International Journal on Information Technologies & Security* 9, no. 3 (2017).



- [5] Ahmed, Moustafa Abdelrahman Mahmoud, Syahril Anuar Idris, Nur Arzilawati Md Yunus, Fazlina Mohd Ali and Hazrina Sofian. "CyberShield Framework: Attacks and Defense Modelling for Cybersecurity in Internet of Things (IoT)." *International Journal of Advanced Research in Computational Thinking and Data Science* 4, no. 1 (2024): 30-39. https://doi.org/10.37934/ctds.4.1.3039a
- [6] Din, Roshidi, Ahmad Hamid Shakir, Sarmad Hamzah Ali, Alaa Jabbar Qasim Almaliki and Sunariya Utama. "Exploring Steganographic Techniques for Enhanced Data Protection in Digital Files." *International Journal of Advanced Research in Computational Thinking and Data Science* 1, no. 1 (2024): 1-9. https://doi.org/10.37934/CTDS.1.1.19
- [7] Abas, Azizi, Roshidi Din and Fazli Azzali. "Enhancing Secured QR Code Large Storage Capacity through Steganography and Compression Techniques." *International Journal of Advanced Research in Computational Thinking and Data Science* 5, no. 1 (2025): 28-49. https://doi.org/10.37934/ctds.5.1.2849
- [8] Stoyanov, Danail, Zeike Taylor, Francesco Ciompi, Yanwu Xu, Anne Martel, Lena Maier-Hein, Nasir Rajpoot et al., eds. Computational Pathology and Ophthalmic Medical Image Analysis: First International Workshop, COMPAY 2018 and 5th International Workshop, OMIA 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 16-20, 2018, Proceedings. Vol. 11039. Springer, 2018.
- [9] 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
- [10] 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
- [11] 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
- [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] 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
- [15] 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
- [16] 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
- [17] 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
- [18] 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
- [19] 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
- [20] 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
- [21] 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
- [22] Wang, Peipei, Yun Cao and Xianfeng Zhao. "Segmentation based video Steganalysis to detect motion vector modification." *Security and Communication Networks* 2017, no. 1 (2017): 8051389. https://doi.org/10.1155/2017/8051389
- [23] Alshamsi, Adeel, Salem Albaloushi, Mohammed Alkhoori, Hamed Almheiri and Nedal Ababneh. "Enhancing Arabic Text Steganography Based on Unicode Features." *Int. J. Com. Dig. Sys* 11, no. 1 (2022). https://doi.org/10.12785/ijcds/110155



- [24] Tong, Yongju, Y. 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
- [25] 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
- [26] Alghamdi, Nujud and Lamia Berriche. "Capacity investigation of Markov chain-based statistical text steganography: Arabic language case." In *Proceedings of the 2019 Asia Pacific information technology conference*, pp. 37-43. 2019. https://doi.org/10.1145/3314527.3314532
- [27] 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.
- [28] Thabit, Reema, Nur Izura Udzir, Sharifah Md Yasin, Aziah Asmawi and Adnan Abdul-Aziz Gutub. "CSNTSteg: Color spacing normalization text steganography model to improve capacity and invisibility of hidden data." *IEEE Access* 10 (2022): 65439-65458. https://doi.org/10.1109/ACCESS.2022.3182712
- [29] 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
- [30] 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
- [31] 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
- [32] 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
- [33] Shah, ST Ali, Aihab Khan and Afaq Hussain. "Text steganography using character spacing after normalization." *Int. J. Sci. Eng. Res* 11, no. 2 (2020): 949-957. https://doi.org/10.14299/ijser.2020.02.05
- [34] Alyousuf, Farah Qasim Ahmed and Roshidi Din. "Analysis review on feature-based and word-rule based techniques in text steganography." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 764-770. https://doi.org/10.11591/eei.v9i2.2069
- [35] 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
- [36] 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
- [37] 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
- [38] Wu, Yulei, Xianyi Chen and Xingming Sun. "Coverless steganography based on english texts using binary tags protocol." *Journal of Internet Technology* 19, no. 2 (2018): 599-606.
- [39] 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
- [40] Bhattacharyya, Souvik. "Hiding data in text through changing in alphabet letter patterns (calp)." *Journal of Global Research in Computer Science* 2, no. 3 (2011).
- [41] Din, Roshidi, Reema Ahmed Thabit, Nur Izura Udzir and Sunariya Utama. "Traid-bit embedding process on Arabic text steganography method." *Bulletin of Electrical Engineering and Informatics* 10, no. 1 (2021): 493-500. https://doi.org/10.11591/eei.v10i1.2518
- [42] Majumder, Anandaprova and Suvamoy Changder. "An Automated Cover Text Selection System for Text Steganography Algorithms." In *Intelligent Cyber-Physical Systems Security for Industry 4.0*, pp. 33-55. Chapman and Hall/CRC, 2022. https://doi.org/10.1201/9781003241348-3
- [43] Abbass, Ahmed Abdulrudah, Hussein Lafta Hussein, Jasim Hussein Lafta Kaabi and Róbert Tornai. "American standard code for information interchange mapping technique for text hiding in the RGB and gray images." (2022). https://doi.org/10.11591/ijece.v12i3.pp2812-2817
- [44] Yu, Long, Yuliang Lu, Xuehu Yan, Yue Jiang and Jiayu Wang. "Generative Text Secret Sharing with Topic-Controlled Shadows." *Security and Communication Networks* 2022, no. 1 (2022): 7189130. https://doi.org/10.1155/2022/7189130