Borneo International Journal eISSN 2636-9826; Vol. 6 (4); 2023; 16-24
Published by *Majmuah Enterprise*
www.majmuah.com

A Review of Feature-based Technique in Text-based Steganography

SITI NORUSSAADAH BINTI MOHD SALLEH, ROSHIDI DIN, and NUR HARYANI ZAKARIA

School of Computing, UUM College of Arts and Sciences, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: ssaadah84@gmail.com, roshidi@uum.edu.my, haryani@uum.edu.my | Tel: +6012346789 | Fax: +608123456 |

Received: Oct 03, 2023
Accepted: Oct 20, 2023
Online Published: Dec 01, 2023

Abstract

Text steganography is one of the major forms of data security in communication. It is widely applied in the modern digital era for securely transferring confidential and private data without raising any suspicions. The well-known technique in text steganography called feature-based is used to conceal information. This technique manipulates and alters some features of characters in the cover message before sending it out to the intended recipient. The modifications are ensured won't compromise the integrity of the secret message. This paper presents an overview of the feature-based technique used in the text domain. The review is conducted according to approaches applied in the feature-based technique. Hence, the main aim of this paper is to review the technique used and highlight the strengths and weaknesses of each technique used in text steganography for safely hiding the secret message. The conclusion emphasizes how the feature-based technique is advantageous for providing data protection by avoiding the detection of third parties during the delivery of the information.

Keywords: steganography, text, feature-based, message, information.

1. Introduction

With the advancement of today's communication systems, securing the data is considered a crucial factor to be fulfilled when delivering or transferring information. It has become one of the most crucial issues in digital communication. Therefore, steganography is identified as one of the schemes used to provide the security of data. Steganography is a mechanism used to conceal information without knowing the existence of the message by others. Steganography is particularly useful in hiding and transferring the hidden message from the source to the destination. Thus, steganography can be applied for a range of purposes in scientific, social, and government applications such as for military, private banking, and online voting (Ansari et al., 2019). According to (Abraham & Gundla, 2019; Mann & Goswami, 2017), steganography is helpful and can be commonly applied in private and confidential communication, preservation of classified data, protection of data modification, e-trade commerce, media, systems for databases, and digital watermarking. The application differs in what function of the steganography is used in each system.

2. Steganography Domain

As communication concerns the safety of information passing from one to another, steganography provides a platform to guarantee that security can be supplied in the communication process. Steganography needs to give security in the transferring process of immense information. Indeed, the word steganography is derived from Greek. The first word is steganos which means hide and the second word is graphy which means writing. The combination of both words gives a literal meaning of hidden writing. Thus, steganography can be described as the technique of hiding the message by embedding secret information through a secure communication channel. There are two classifications of steganography: digital steganography and natural language steganography, which can be represented in Figure 1.

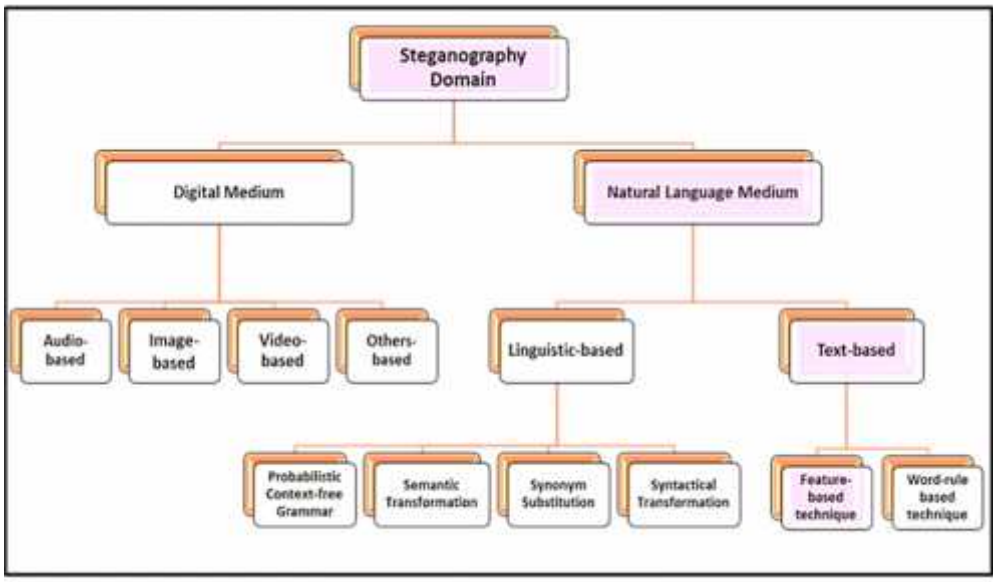

Figure 1: Classification of Steganography Domain.

The first category, which is digital steganography consists of various mediums known as audio, image, video, and others. There is a lot of research done in digital steganography based on media such as image steganography (Duan et al., 2023; M. S. Taha et al., 2022), audio steganography (Alsolami, 2022; Mohammad et al., 2023), and video steganography (Fan et al., 2022; Salunkhe & Bhosale, 2023). Besides, network steganography (Bistarelli et al., 2023; Heßeling et al., 2022) was also studied by previous scholars as one of the domains in the steganography area. Meanwhile, the second category is natural language steganography which is focused on hiding the information in natural language while ensuring there is no modification in the meaning of the message. There are two divisions of natural language which can be referred to as linguistic-based steganography and text-based steganography. The first division of natural language which is linguistic-based steganography deals with hiding the message in the natural text that makes use of the syntactic or semantic properties without causing the alteration in grammar that leads to the unnatural message (Chaw, 2019; Fang et al., 2017; Figueira, 2022). It can be specified further into four categories: Probabilistic context-free grammar (PCFG), semantic transformation, synonym substitution, and syntactical transformation. The second division of natural language is known as text-based steganography which is the mechanism that uses the text as a cover medium for hiding the message based on the line manipulation, spaces, characters, or any other features of the given message. There are two techniques applied in text steganography which can be identified as feature-based technique and word-rule-based technique.

The first technique, which is a feature-based technique conceals the secret message through modification of the characters and features in the text before sending it to the intended recipient. It involves the alteration of the text features. Accordingly, the letter in the alphabet can be modified such as by shifting the point in characters i and j, varying the strike of characters f and j, and extending or abbreviating the end of some portion of certain characters, for example, h, d, b, etc. (Al-Nofaie & Gutub, 2019; El Rahman, 2019). Besides, other selection of features for instance font style, size, and the color of the text also can be changed to disguise the characters in the message (Ahvanooey et al., 2019; Akbar et al., 2020). Thus, the feature-based technique provides numerous preferences of the features in text for hiding the secret message. On the other hand, the second technique which is the word-rule-based technique hides the secret message through the utilization of word patterns such as text shifting. This word-rule-based can be further categorized into line-shift coding and word-shift coding. Line-shift coding involves shifting the positions of text lines vertically to embed the secret message while word-shift coding is done by shifting horizontally and varying the space between words (Alsaidi et al., 2020; Makhdoom et al., 2022; Nirmatha & Amaresan, 2017).

3. Feature-based Technique used in Text Steganography

A feature-based technique is one of the techniques used in text steganography. A voluminous study has been done in this area considering the previous research that addresses feature manipulation mechanisms (Azeem et al., 2019; Chaudhary, Dave, & Sanghi, 2016; Ditta et al., 2022; Khan et al., 2015; Shaker et al., 2017). This technique alters the cover document such that it causes minimal distortion and ensures the size of both the stego text and cover text are

comparable. Thus, it is significant to clearly choose and substitute just immaterial segments of the cover document in order to stay away from doubt. Hence, the following subsection elaborates on the feature-based technique that has been used in text steganography.

3.1 Diacritics-based

Diacritics (harakaat) in the cover text are used as a way to conceal hidden information. The application of diacritics is optional or additional to the characters used in a cover text. Various ways of locating the diacritics such as by inversing (Memon et al., 2008) and multiple utilization (Ahmadoh & Gutub, 2015) to increase the capacity of concealment. Nevertheless, the inverse diacritics lead to the problem of non-standard diacritic usage. It requires a new font for the implementation of these inverse diacritics (Gutub & Al-Nazer, 2010; Malalla & Shareef, 2017). Besides that, the necessity for the cover text to be fully diacritics is also a disadvantage as most text nowadays provides no diacritics (Shakir & Mahdi, 2023). Even though the capacity of concealment is increased, the robustness level is low (Alanazi et al., 2020a, 2021) thus security is being compromised through the diacritics-based technique.

3.2 Kashida-based

This technique exploits the extension characters (Kashida) to embed the hidden information in the cover text message (Al-Nazer & Gutub, 2009; Gutub & Al-Nazer, 2010; Taha et al., 2018). Kashida is placed between the connected characters in the text. The utilization of Kashida is preferred as its existence has no impact on the text content. However, the Kashida-based technique causes a low level of robustness as the extension characters can be effortlessly discarded from stego text (Alifah Roslan et al., 2022; Bensaad & Yagoubi, 2013). The placement of Kashida must consider the condition of the characters of the text. Only characters categorized as connected letters are used so that Kashida can be added between them. Thus, it will lead to the increment of Kashida to embed the hidden information. At the same time, it causes an increment in the file size and alteration of the look of the text (Alanazi et al., 2020b; Hamzah et al., 2019; Tayyeh et al., 2019).

3.3 Unicode-based

The hidden information is embedded in Unicode text documents by applying the feature of the Unicode Standard. Several approaches are used to hide secret messages such as the utilization of unique representation codes for a word and non-printing of two characters called zero width non joiner (ZWNJ) and zero width joiner (ZWJ) (Alanazi et al., 2020b; Baawi et al., 2017; Ditta et al., 2018; Odeh et al., 2014). The Unicode-based technique keeps the appearance of the cover text remains unchanged. The stego text can be stored in various formats of text files due to no alteration through operations such as copy and paste amid computer programs. Nevertheless, the use of unique representation codes (Baawi & Mokhtar, 2018) requires an algorithm in order to avoid the shape corruption of the texts (Mohamed, 2014). Furthermore, Unicode-based also depends on a special or designated font mechanism (Baawi et al., 2020) to enhance the performance of text steganography. Besides that, the technique has low robustness due to its position for embedding amongst characters (Ahvanooey et al., 2019). Moreover, it suffers the increment in the size of the stego text which is caused by the application of certain coding systems towards characters before concealing it in the stego content (Khami, 2017) and not integrated with the compression feature to enhance its capacity (Baawi & Mokhtar, 2018).

3.4 Article-based

The way of embedding and producing stego text is through incorporating application or English Language articles along with special code generation. The hidden information is first encoded using code representation called Secret Steganography Code for Embedding (SSCE) before being embedded into a cover text message. The embedding technique is through article insertion such as articles “a” or “an” with the nonspecific nouns (Banerjee et al., 2011). Thus, the focus is on the words’ initial character of the cover text to determine hidden bits. For instance, bit 0 is embedded using the article “a” while bit 1 is embedded using the article “an” (Chaudhary, Dave, Sanghi, et al., 2016). The purpose of the special code is to increase the security level of stego text. In addition, the technique provides a good embedding capacity. However, the dependency on consonant and vowel words can be a constraint for the embedding process.

3.5 Changing in Alphabet Letter Pattern

CALP is based on the variation of alphabet patterns (Bhattacharyya et al., 2011). It modifies the features of English letters to embed binary bits. It makes use of alphabets i, j, a, A, and c which are divided into two groups to embed hidden bits 0 and 1. The basic modification of the letters is not simply detectable. Thus, CALP can provide better security and display robustness as it achieves minimal degradation of text. Nevertheless, the dependency on the characters provided becomes the limitation in the process of concealing the secret message. Furthermore, the imperceptibility level is low due to the slight alteration of character patterns through the embedding process (Naqvi et al., 2018).

3.6 Curve Subheading (CURVE) and Vertical Straight Line (VERT)

CURVE and VERT are based on a combination of features in English letters (Dulera et al., 2011) where the bits are concealed through manipulation of the letter's shapes including the curve subheading, and the vertical straight line. CURVE hides the message according to the alteration of letter shape which falls into two groups, one for the curved letters and the other one for the non-curved letters. The group that holds curved letters is used to embed hidden bit 0. Meanwhile, the other group that holds non-curved letters is used to embed hidden bit 1. On the other hand, the VERT method hides the message based on the structure of the letters which are vertical straight lines. There are two groups involved, one group that carries letters with multiple or no vertical lines used to embed hidden bit 0 and the other group that carries letters with one vertical line used to embed hidden bit 1. Both methods can extend the level of randomness thus providing high security. As the embedding process relies on the length of the cover text and the paragraphs, it becomes the constraint to this technique.

3.7 Capital-based

The hidden information is embedded in the capital letters of the cover text. For instance, three characters consisting of capital letters are required to hide one character in the embedding process (Bhaya et al., 2013). Another exploitation of capital letters is through the introduction of special encoding called Capital Alphabet Shape Encoding (CASE) (Chaudhary et al., 2013) The hidden information is converted into bits form and proceeds with its corresponding ASCII character before being embedded into the cover text. Therefore, the cover text certainly requires only the presence of capital letters which then increases the size of the cover text along with the increment of secret text (Kingslin & Kavitha, 2015). Besides, other symbols and numbers are not considered for concealment.

3.8 Write-based

The technique that is based on the write ability feature (Kouser et al., 2016) exploits the shapes of characters to embed hidden information. It depends on the way of writing the characters used in the cover text. The ability to write in one flow or not along with the condition of lines and curves of characters are considered to hide bits 0 and 1. However, this situation creates a problem as it is constrained by the non-uniform occurrence of the characters in the cover text to conceal the hidden information.

3.9 ASCII-based

The way of embedding the secret message is through the incorporation of ASCII characters equivalent such as studied by (Ahvanooey et al., 2018; Azeem et al., 2019; Iyer & Lakhtaria, 2016; Naharuddin et al., 2018). The process of embedding that utilizes ASCII code characteristics becomes a disadvantage as it is dependable on ASCII characters (Muhammad et al., 2020) in order to hide the secret message. Besides that, the application can be easily detected after concealment.

3.10 Summary

To sum up, a feature-based technique is utilized by previous researchers to hide the message. With the modification of characters and features in text, this technique has the ability to hide data concerning a lesser amount of cover message. Accordingly, the next section will discuss further their advantages and disadvantages in comparison among the techniques used for text-based steganography.

4. Discussion

As mentioned above, the feature-based technique used in text steganography is reviewed which has been emphasizing the advantages and drawbacks. Therefore, the strengths and weaknesses of each technique used can be concluded in Table 1.

Table 1: Comparison of feature-based technique for strengths, and weaknesses

Technique	Strengths	Weaknesses
Diacritics-based	⦁ The implementation is easy with considerable capacity. ⦁ The output file can be in a flexible format. (Ahmadoh & Gutub, 2015; Bensaad & Yagoubi, 2013; Thabit et al., 2021)	⦁ The capacity threshold needs to be quantified to avoid too many diacritics shown in the text. ⦁ A necessity for the cover text to be fully diacritics. ⦁ Low security and robustness. ⦁ Computational time is high. (Alanazi et al., 2020a, 2021; Bensaad & Yagoubi, 2013; Shakir & Mahdi, 2023)
Kashida-based	⦁ No change in the appearance of the text, thus decreasing the level of suspicions. ⦁ A better capacity limit and could be utilized in printed forms with a diverse font style. (Al-Nazer & Gutub, 2009; Gutub & Alaseri, 2019; Shaker et al., 2017)	⦁ The possibility of attaching Kashida depends on the connected characters in a word. ⦁ Increase the size of the cover text. ⦁ Low robustness. ⦁ Complexity of algorithm in the extraction process. (Al Azzawi, 2019; Alghamdi & Berriche, 2019; Ditta et al., 2022; Thabit et al., 2021)
Unicode-based	⦁ No change in the appearance of the text by the embedding process. ⦁ No requirement for a special format of text. (Al-Nofaie et al., 2019; Ali, 2010)	⦁ Enlarge the size of the cover text and stego text. ⦁ Needs a special algorithm to avoid shape corruption. (Al Azzawi, 2019; Ditta et al., 2018; Khami, 2017; Mohamed, 2014)
Article-based	⦁ Achieve minimum degradation of stego text. ⦁ Better security by providing encryption with code generation before embedding. (Banerjee et al., 2011)	⦁ Not focusing on delivering meaningful text and the right format. ⦁ Depending on consonant and vowel words for implementation of the embedding process. (Torvi et al., 2016)
CALP	⦁ The structural modification is not easily detectable and recognizable by the viewers. ⦁ Applicable to any language other than English. ⦁ Able to provide embedding capacity at a high level. (Bhojane & Kadoke, 2015; Shetty, 2017)	⦁ Insufficient to give adequate concealed limit since it is constrained by the dependency of characters' presence. ⦁ The imperceptibility level is low due to minor changes in character patterns during the process of embedding the secret message. (Naqvi et al., 2018)
CURVE	⦁ Provide security with randomness. ⦁ Regardless of whether somebody sees it, they can't interpret it until they realize the concealing algorithm. (Chaudhary, Dave, & Sanghi, 2016)	⦁ Constrained by the dependency on message length and passages to hide the secret message. (Srinidhi & ShivaKumar, 2017)
VERT	⦁ Hiding messages through character modification along with random sequence characters increases the randomness. Thus, it contributes to elevating security with minimal overhead. (Baawi et al., 2018)	⦁ Compromise the safety of secret messages once the applicability of the technique is known to outsiders. (Kouser et al., 2016)
Capital-based	⦁ Stego text remains unchanged if the compression process / copy and paste in computer programs happens. (Chaudhary et al., 2013)	⦁ A requirement for the presence of capital letters to hide more secret messages. ⦁ Low capacity. ⦁ Increase the size of the cover text. (Kataria et al., 2013; Kingslin & Kavitha, 2015)
Write-based	⦁ Enhancement of capacity. ⦁ Able to resist text formatting. (Kouser et al., 2016)	⦁ Restricted by the non-uniform occurrence of the characters in the cover text.

ASCII-based	) Increase performance in terms of capacity.) Achieve a stego message similar to the original cover message. (Azeem et al., 2019; Naharuddin et al., 2018)	) A requirement for ASCII characters and utilizes a complex approach.) Easily detect the changes in characters. (Muhammad et al., 2020)

Based on the details in Table 1, each technique clusters the letter sets depending on the attribute of the characters. The characters are being altered and manipulated in order to conceal secret information. As the feature-based technique focuses on character manipulation, the dependency on the characters provided can become the factor that contributes to the strength or weakness in the process of concealing the secret message. The requirement for certain characters can be a constraint to the technique for hiding messages securely.

5. Conclusions

This paper presents an overview of the feature-based technique in the text steganography domain. Then, it continues with a review of the feature-based technique used in text-based steganography. Furthermore, the paper also highlights the strengths and weaknesses of each technique. Based on the literature, the embedding capacity and character dependency have been emphasized in the strengths and weaknesses. Thus, the real challenge in the feature-based technique is to acquire capacity with the optimum condition while reducing the dependence on characters for the concealment process. Thus, it is expected that an enhancement will be made in the near future to lessen the dependency on characters in order to hide messages safely.

References

Abraham, J., & Gundla, R. (2019). Survey on the different hiding types and techniques in steganography. *Journal of The Gujerat Research Society*, *21*(14), 174–180.

Ahmadoh, E. M., & Gutub, A. A.-A. (2015). Utilization of two diacritics for Arabic text steganography to enhance performance. *Lecture Notes on Information Theory*, *3*(1), 42–47. https://doi.org/10.18178/lnit.3.1.42-47

Ahvanooey, M. T., Li, Q., Hou, J., Mazraeh, H. D., & 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

Ahvanooey, M. T., Li, Q., Hou, J., Rajput, A. R., & Chen, Y. (2019). Modern text hiding, text steganalysis, and application: A comparative analysis. *Entropy*, *21*(4), 355. https://doi.org/10.3390/e21040355

Akbar, F. C., Purboyo, T. W., & Latuconsina, R. (2020). A study of text steganography methods. *ARPN Journal of Engineering and Applied Sciences*, *15*(2), 369–372. https://doi.org/10.36478/JEASCI.2020.369.372

Al-Nazer, A., & Gutub, A. (2009). Exploit Kashida adding to Arabic e-text for high capacity steganography. *IEEE International Conference on Network and System Security*, 447–451. https://doi.org/10.1109/NSS.2009.21

Al-Nofaie, S., Gutub, A., & Al-Ghamdi, M. (2019). Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces. *Journal of King Saud University - Computer and Information Sciences*, *33*(8), 963–974. https://doi.org/10.1016/j.jksuci.2019.06.010

Al-Nofaie, S. M. A., & Gutub, A. A.-A. (2019). Utilizing pseudo-spaces to improve Arabic text steganography for multimedia data communications. *Multimedia Tools and Applications*, *79*, 19–67. https://doi.org/10.1007/s11042-019-08025-x

Al Azzawi, A. F. (2019). A multi-layer Arabic text steganographic method based on letter shaping. *International Journal of Network Security & Its Applications*, *11*(01), 27–40. https://doi.org/10.5121/ijnsa.2019.11103

Alanazi, N., Khan, E., & Gutub, A. (2020a). Efficient security and capacity techniques for arabic text steganography via engaging unicode standard encoding. *Multimedia Tools and Applications*, *80*, 1403–1431. https://doi.org/10.1007/s11042-020-09667-y

Alanazi, N., Khan, E., & Gutub, A. (2020b). 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

Alanazi, N., Khan, E., & Gutub, A. (2021). Involving spaces of Unicode standard within irreversible Arabic text steganography for practical implementations. *Arabian Journal for Science and Engineering*, *46*(9), 8869–8885. https://doi.org/10.1007/s13369-021-05605-8

Alghamdi, N., & Berriche, L. (2019). Capacity investigation of Markov chain-based statistical text steganography: Arabic language case. *Proceedings of the 2019 Asia Pacific Information Technology Conference*, 37–43. https://doi.org/10.1145/3314527.3314532

Ali, A. E. (2010). A new text steganography method by using non-printing Unicode characters. *Engineering & Technology Journal*, *28*(1), 72–83.

Alifah Roslan, N., Izura Udzir, N., Mahmod, R., & Gutub, A. (2022). Systematic literature review and analysis for Arabic text steganography method practically. *Egyptian Informatics Journal*, *23*(4), 177–191. https://doi.org/10.1016/j.eij.2022.10.003

Alsaidi, N., Alshareef, M., Alsulami, A., Alsafri, M., & Aljahdali, A. (2020). Digital steganography in computer forensics. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(5), 54–61.

Alsolami, E. A. (2022). Audio steganography method using least significant bit (LSB) encoding technique. *Journal of Theoretical and Applied Information Technology*, *100*(12), 3913–3922.

Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2019). A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security*, *11*(1), 11–25. https://doi.org/10.5815/ijcnis.2019.01.02

Azeem, M., Cai, Y., Rana, K. G., Shaukat, Z., & Ditta, A. (2019). A secure and size efficient approach to enhance the performance of text steganographic algorithm. *IEEE 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, 402–407. https://doi.org/10.1109/ICMTMA.2019.00095

Baawi, S. S., & Mokhtar, M. R. (2018). Enhancement of text steganography technique using Lempel-Ziv-Welch algorithm and two-letter word technique. *International Conference of Reliable Information and Communication Technology*, 525–537. https://doi.org/10.1007/978-3-319-99007-1

Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2017). New text steganography technique based on a set of two-letter words. *Journal of Theoretical and Applied Information Technology*, *95*(22), 6247–6255.

Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2018). A comparative study on the advancement of text steganography techniques in digital media. *ARPN Journal of Engineering and Applied Sciences*, *13*(5), 1854–1863.

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), 012125. https://doi.org/10.1088/1757-899X/870/1/012125

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

Bensaad, M. L., & Yagoubi, M. B. (2013). Boosting the capacity of diacritics-based methods for information hiding in Arabic text. *Arabian Journal for Science and Engineering*, *38*(8), 2035–2041. https://doi.org/10.1007/s13369-013-0576-3

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 (JGRCS)*, *2*(3), 33–39.

Bhaya, W., Rahma, A. M., & AL-Nasrawi, D. (2013). Text steganography based on font type in MS-Word documents. *Journal of Computer Science (JCS)*, *9*(7), 898–904. https://doi.org/10.3844/jcssp.2013.898.904

Bhojane, A. B., & Kadoke, P. A. (2015). A survey on steganography techniques. *International Journal of Science and Research (IJSR)*, *4*(5), 1537–1542. https://doi.org/10.5120/17105-7746

Bistarelli, S., Ceccarelli, M., Luchini, C., Mercanti, I., & Santini, F. (2023). A survey of steganography tools at layers 2-4 and HTTP. *18th International Conference on Availability, Reliability and Security*, 1–9. https://doi.org/10.1145/3600160.3605058

Chaudhary, S., Dave, M., & Sanghi, A. (2016). Aggrandize text security and hiding data through text steganography. *IEEE 7th Power India International Conference (PIICON)*, 1–5.

Chaudhary, S., Dave, M., Sanghi, A., & Manocha, J. (2016). An elucidation on steganography and cryptography. *ACM International Conference Proceeding Series*, 1–6. https://doi.org/10.1145/2905055.2905249

Chaudhary, S., Mathur, P., Kumar, T., & Sharma, R. (2013). A Capital shape alphabet encoding (CASE) based text steganography. *Conference on Advances in Communication and Control Systems*, *2013*(Cac2s), 120–124.

Chaw, A. A. (2019). Text Steganography in letter of credit (LC) using synonym substitution based algorithm. *International Journal of Advance Research and Development (IJARND)*, *4*(8), 59–63.

Ditta, A., Azeem, M., Naseem, S., Gulzar Rana, K., Adnan Khan, M., & Iqbal, Z. (2022). 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*, *34*(5), 2180–2191. https://doi.org/10.1016/j.jksuci.2020.07.010

Ditta, A., Yongquan, C., Azeem, M., Rana, K. G., Yu, H., & Memon, M. Q. (2018). Information hiding: Arabic text steganography by using Unicode characters to hide secret data. *International Journal of Electronic Security and Digital Forensics*, *10*(1), 61–78. https://doi.org/10.1504/IJESDF.2018.089214

Duan, X., Li, B., Yin, Z., Zhang, X., & Luo, B. (2023). Robust image steganography against lossy JPEG compression based on embedding domain selection and adaptive error correction. *Expert Systems with Applications*, *229*, 120416. https://doi.org/10.1016/j.eswa.2023.120416

Dulera, S., Jinwala, D., & Dasgupta, A. (2011). Experimenting with the novel approaches in text steganography. *International Journal of Network Security & Its Applications (IJNSA)*, *3*(6), 213–225.

https://doi.org/10.5121/ijnsa.2011.3616

El Rahman, S. A. (2019). Text approaches using similarity of English font styles. *International Journal of Software Innovation (IJSI)*, *7*(3), 29–50. https://doi.org/10.4018/IJSI.2019070102

Fan, P., Zhang, H., & Zhao, X. (2022). Robust video steganography for social media sharing based on principal component analysis. *Eurasip Journal on Information Security*, *2022*(1), 1–19. https://doi.org/10.1186/s13635-022-00130-z

Fang, T., Jaggi, M., & Argyraki, K. (2017). Generating steganographic text with LSTMs. *55th Annual Meeting of the Association for Computational Linguistics, Proceedings of the Student Research Workshop*, 100–106. https://doi.org/10.18653/v1/P17-3017

Figueira, J. (2022). *A survey on semantic steganography systems*. 1–7. http://arxiv.org/abs/2203.12425

Gutub, A. A.-A., & Al-Nazer, A. A. (2010). High capacity steganography tool for Arabic text using 'Kashida.' *International Journal of Information Security (ISeCure)*, *2*(2), 107–118.

Gutub, A., & Alaseri, K. (2019). Hiding shares of counting-based secret sharing via Arabic text steganography for personal usage. *Arabian Journal for Science and Engineering*, *45*(4), 2433–2458. https://doi.org/10.1007/s13369-019-04010-6

Hamzah, A. A., Khattab, S., & Bayomi, H. (2019). A linguistic steganography framework using Arabic calligraphy. *Journal of King Saud University - Computer and Information Sciences*, *33*(7), 865–877. https://doi.org/10.1016/j.jksuci.2019.04.015

Heßeling, C., Keller, J., & Litzinger, S. (2022). Network steganography through redundancy in higher-radix floating-point representations. *17th International Conference on Availability, Reliability and Security*, 1–7. https://doi.org/10.1145/3538969.3544429

Iyer, M. S. ., & Lakhtaria, K. (2016). New robust and secure alphabet pairing text steganography algorithm. *International Journal of Current Trends in Engineering & Research (IJCTER)*, *2*(7), 15–21.

Kataria, S., Singh, B., Kumar, T., & Shekhawat, H. S. (2013). PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) based text steganography. *International Conference on Advances In Computer Sciences*, 175–182.

Khami, M. J. (2017). Unlimited size of english plain text-in-text hiding algorithm. *International Journal of Computer Science and Engineering (IJCSE)*, *6*(1), 89–96. http://www.iaset.us/view_archives.php?year=2016&jtype=2&id=14&details=archives

Khan, S., Sankineni, R., Balagurunathan, P., Shree, N. S. D., & Balasubramanian, A. (2015). Czech text steganography method by selective hiding technique. *Proceedings of the World Congress on Engineering (WCE)*, *I*, 4.

Kingslin, S., & Kavitha, N. (2015). Evaluative approach towards text steganographic techniques. *Indian Journal of Science and Technology*, *8*(29), 1–8. https://doi.org/10.17485/ijst/2015/v8i1/84415

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.

Makhdoom, I., Abolhasan, M., & Lipman, J. (2022). A comprehensive survey of covert communication techniques, limitations and future challenges. *Computers and Security*, *120*. https://doi.org/10.1016/j.cose.2022.102784

Malalla, S., & Shareef, F. R. (2017). A novel approach for Arabic text steganography based on the " BloodGroup " text hiding method. *Engineering, Technology & Applied Science Research*, *7*(2), 1482–1485.

Mann, M., & Goswami, S. (2017). Improved steganography method for secured data sharing. *International Journal of Computer Applications*, *166*(12), 29–34. https://doi.org/10.5120/ijca2017914147

Memon, J. A., Khowaja, K., & Kazi, H. (2008). Evaluation of steganography for Urdu / Arabic text. *Journal of Theoretical and Applied Information Technology (JATIT)*, *4*(3), 232–237.

Mohamed, A. A. (2014). An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. *Egyptian Informatics Journal*, *15*(2), 79–87. https://doi.org/10.1016/j.eij.2014.04.002

Mohammad, H., Science, D., & Rahman, M. (2023). Audio steganography with intensified security and hiding capacity. *European Chemical Bulletin*, *12*(10), 162–173. https://doi.org/10.48047/ecb/2023.12.10.013

Muhammad, M. H., Hussain, H. S., Din, R., Samad, H., & Utama, S. (2020). Review on feature-based method performance in text steganography. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 427–433. https://doi.org/10.11591/eei.v10i1.2508

Naharuddin, A., Wibawa, A. D., & Sumpeno, S. (2018). A high capacity and imperceptible text steganography using binary digit mapping on ASCII characters. *IEEE International Seminar on Intelligent Technology and Its Application (ISITIA)*, 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

Nirmatha, T. . M., & Amaresan, S. (2017). Text stenography using computer fonts. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, *4*(9), 9–12.

Odeh, A., Elleithy, K., & Faezipour, M. (2014). Steganography in text by using MS Word symbols. *Proceedings of the*

2014 Zone 1 Conference of the American Society for Engineering Education, *April*, 1–5. https://doi.org/10.1109/ASEEZone1.2014.6820635

Salunkhe, S., & Bhosale, S. (2023). RI-CDVS: Robust and imperceptible compressed domain video steganography using H.265 Codec. *SN Computer Science*, *4*(4), 357. https://doi.org/10.1007/s42979-023-01681-9

Shaker, A. A., Ridzuan, F., & Pitchay, S. A. (2017). Text steganography using extensions Kashida based on the moon and sun letters concept. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(8), 286–290. www.ijacsa.thesai.org

Shakir, N. S., & Mahdi, M. S. (2023). Using special letters and diacritics in steganography in holy Quran. *Iraqi Journal for Computers and Informatics*, *49*(2), 1–8.

Shetty, N. P. (2017). An amended RSA algorithm for secure communication. *Journal of Engineering and Applied Sciences*, *12*(23), 6189–6194.

Srinidhi, G. A., & ShivaKumar, K. B. (2017). Secured biometric signal transfer using steganography. *International Journal of Engineering and Technology (IJET)*, *9*(3S), 618–622. https://doi.org/10.21817/ijet/2017/v9i3/170903s093

Taha, A., Hammad, A. S., & Selim, M. M. (2018). A high capacity algorithm for information hiding in Arabic text. *Journal of King Saud University - Computer and Information Sciences*, *32*(6), 658–665. https://doi.org/10.1016/j.jksuci.2018.07.007

Taha, M. S., Rahem, M. S. M., Hashim, M. M., & Khalid, H. N. (2022). High payload image steganography scheme with minimum distortion based on distinction grade value method. *Multimedia Tools and Applications*, *81*(18), 25913–25946. https://doi.org/10.1007/s11042-022-12691-9

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. I., Md Yasin, S., Asmawi, A., Roslan, N. A., & Din, R. (2021). A comparative analysis of Arabic text steganography. *Applied Sciences (Switzerland)*, *11*(15). https://doi.org/10.3390/app11156851

Torvi, S. D., ShivaKumar, K. B., & Das, R. (2016). An unique data security using text steganography. *IEEE 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 3834–3838.