Research Article

Disbursal of Text Steganography in the Space of Double-Secure Algorithm

Yahya Khan,¹ Ali Algarni,² Aisha Fayomi,² and Abdullah M. Almarashi ²

¹Department of Electrical Engineering and Information Science, School of Information Science and Technology, University of Science and Technology of China, Hefei, China

²Faculty of Science, Department of Statistics, King Abdulaziz University, Jeddah, Saudi Arabia

Correspondence should be addressed to Abdullah M. Almarashi; aalmarashi@kau.edu.sa

Received 29 September 2021; Accepted 1 November 2021; Published 29 December 2021

Academic Editor: Lazim Abdullah

Copyright © 2021 Yahya Khan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Hackers reveal sensitive information from encrypted conversations as the globe has become one community. As a result, steganography and cryptography are used together to safeguard sensitive data more effectively than previous approaches and newly developed algorithms. A double-secure algorithm for text steganography (DSTS) is the safest approach compared to the paragraph hiding method (PHM) and capital alphabet shape encoding (CASE) method. In this context, the paragraph hiding method uses ASCII coding, which is not a standard method, and the CASE method has a security issue that if someone understands its applicability, it can be easily attacked. DSTS algorithm overcomes its limitations by using UTF-16 coding and enhances the security of CASE with a one-time pad (OTP). The one-time pad is a theoretically unbreakable cryptographic method. Still, it is not feasible for long messages, however, it is usable for short messages such as a password or intelligence agency's more secure messages. DSTS degrades the average hiding capacity in a PHM from 2.06% to 1% due to UTF-16 coding. Using the UTF-8 method, the authors have improved MDSTS and the CMPHM by 6.49% and 7.76% hiding capacity, which outperforms in existing procedures; in the CMPHM, there is one reason for the improvement in hiding capacity is using the LZW compression method. CMPHM algorithm optimization standard deviation is less than that of the HPM, DSTS, and MDSTS, ultimately increasing speed.

1. Introduction

The Internet has increased digital communication. Different types of people use the internet for various purposes; therefore, digital communication is not safe. According to [1], it is challenging to save yourself from online attackers. The latest forecast from Gartner Inc. says worldwide information security spending reached \$93 billion in 2018 and an estimated \$124 billion in 2019 [2]. Establishing reliable communication between two parties which share confidential data is difficult due to the probability of attacks and unplanned changes during an active transmission over an unsafe network. The attacker's critical success is to achieve confidential data from a system to understand; then, they have been modified or used for future attacks, as shown in Figure 1 [3].

However, using either cryptography or steganography can secure our hidden information. A word's meaning is

changed; the data are altered into cipher codes that a layperson cannot readout. Cryptography's downside is that it is directly applied to text, while steganography is applied via an innocent object called cover carrier (e.g., text, image, audio, or video). Steganography uses different media carriers such as image, video, audio, and text for concealing confidential data [4]. In digital communication, text steganography plays a vital role by hiding data in cover text in an innocent-looking way with less memory and high speed [5]. Most of the existing text-based literature pays attention to the achievement of high hidden capacity rather than high robustness and invisibility of the stego message. However, current techniques have a tradeoff between high embedding capacity and invisibility; if one method successfully achieves one trait, it lacks others, automatically [6]. Hybrid approaches of cryptography and steganography are more secure than single-text steganographic or cryptographic

FIGURE 1: The hacking attack on confidential data.

methods [7]. This method provides a two-layer protocol for hiding confidential information. The first layer did not allow modification in a cover object, while the second layer hid data in a multiple-cover object. Scholars have used various algorithms and methods in the literature to protect confidential data transmission, but information security is still a challenge. Agarwal [8] has proposed algorithms, missing letter puzzles, hiding data in the wordlist act on ASCII value instead of a binary value; therefore, their hiding capacity is maximum. A double-secure algorithm for text steganography (DSTS) [9] is the safest approach than the paragraph hiding method (PHM) and capital alphabet shape encoding (CASE) method.

However, due to randomly generated cover text, these methods are exposed to structural attacks. The more secure algorithm is the paragraph hiding method [8], which uses a natural-looking cover text, i.e., it takes a cover text from any book or newspaper; but still, a more secure text steganographic method than the current approach is needed. Consequently, a double-secure algorithm for text steganography [9] is the safe method due to combining the best features of the paragraph hiding method with text steganography based on the feature coding method [10], even though it downgrades the current paragraph hiding approach's average hiding capacity from 2.06% to 1%. The enhancement in the capacity of the double-secure algorithm for text steganography has improved the average hiding capacity with MDSTS from 1% to 3.98% with UTF-16 and 6.49% with UTF-8. Similarly, the CMPHM improved 4.63% with UTF-16 and 7.76% with UTF-8 due to the removal of redundancy in the paragraph approach's secret messages using the LZW method. The CMPHM has more capacity for private messages with three security layers than the hybrid PHM.

1.1. Existing Methods. Cryptography is altering data or messages into codes to make it difficult for the layperson to understand. However, in steganography, confidential data are hidden except for the sender and receiver. The word steganography originates from "steganographia," which infers "confidential" or "secret writing." Therefore, steganography is the skill and discipline of writing secret messages so that no one suspects the data's existence apart from the sender and receiver [11]. Different steganography types hide confidential data in audio, video, image, and text covers. Text steganography is more challenging due to

redundancy but uses less memory and higher speed than other steganographic methods. For text hiding methods, three main issues are to be considered: capacity, security, and robustness. The capacity refers to a carrier media's capability to confidentially stock data; the capacity ratio can be calculated as the number of secret data bytes divided by the number of cover text bytes. Security is the hackers' skill to figure out or suspect hidden data with no trouble. The robustness mentions protecting the unseen data from exploitation, mainly transmitted through the network [12]. Different information security experts presented some popular text steganography approaches to incorporate capacity, security, and robustness. Text steganography is classified into structural or format-based techniques, linguistic techniques, and random and statistical production, as shown in Figure 2 [13].

1.1.1. Structural Technique. Linguistic methods can change the syntax and semantics features of the text. Words, sentences, verbs, nouns, adverbs, and adjectives formulate a text. Linguistic techniques have two types, syntactic and semantic. Synonyms, abbreviations, and similarities of words have been used by the semantic method, and secret bits are hidden in the cover message [14]. Optical character recognition software or retyping attacks cannot hide hidden messages using semantic methods [15]. These techniques change cover letters, which create a suspect in the reader's mind. Semantic methods counter structural attacks with high invisibility, low hiding capacity, and increased robustness, while syntactic forms alter cover messages without changing the text content's meaning [16]. The syntactical-based algorithms have low hiding capacity, high invisibility, and increased robustness against structural attacks but are exposed to visual attacks.

1.1.2. Random and Statistical Production. This method can be classified into compression and random cover methods. The compression method is a subtype of the random and statistical method [17]. The compression-based methods use an algorithm such as Huffman coding, and the Lempel-Ziv-Welch (LZW) compression method uses lossless compression techniques to conceal confidential data in cover messages of text steganography. Compression methods with high invisibility, maximum hiding capacity, and low robustness counter structural attacks.

FIGURE 2: Different types of text hiding techniques.

The random cover method is a subtype of the random and statistical method. The random cover uses secret message statistical structures to generate the cover message [18]. These methods perform with high robustness against visual attacks, but the problem of random cover-based techniques is low invisibility and low capacity [8,19]. Furthermore, they have great computational difficulty in producing the cover message during the embedding/extraction process.

The interword spacing and interparagraph spacing combined method is a new method for text steganography, and the secret message's length is dynamically generated [20]. But, any word processor can detect and delete the spaces. The newly proposed combined algorithms of one-time cryptography and text steganography missing letter puzzles and hiding data in the word list use ASCII value, and the randomly generated cover text is exposed to structural attacks. By contrast, the paragraph hiding method in [8] is more secure due to using a natural-looking cover text compared to the randomly generated cover text but needs additional security in text stenography such as text steganography based on the feature coding method [10] that secure hiding data from visual attacks and structural attack. Therefore, the DSTS [9] algorithm has included CASE as a third security layer. Still, on the other side, it has a low average hiding capacity of 1% compared to the paragraph method with 2.06%. Hence, the DSTS method needs further investigation for average hiding capacity, improvement, and removal of redundancy. The algorithm for text steganography addresses this problem in two parts; one is MDSTS, and the other is the CMPHM.

2. Methodology

Our methodology has twoparts to improve the average hiding capacity of the current method.

- (1) Modified double-secure algorithm for text steganography (MDSTS)
- (2) Compression modified paragraph hiding method (CMPHM)

2.1. MDSTS. As we know that the DSTS algorithm has a low average hiding capacity and MDSTS improves DSTS capacity from 1 bit per word to 4 bits for a word in the cover text, that modification is called modified DSTS. So, the hiding capacity of MDSTS increases four times that of the DSTS algorithm. MDSTS also enjoys three security layers (modified CASE layer, one-time pad cryptography, and modified paragraph hiding method).

2.2. New Algorithm of the Modified Paragraph Hiding method (MPHM). The modified paragraph hiding method (MPHM) modifies the existing paragraph hiding method [8]. The paragraph approach hides 4 bits per word in the cover text, and the existing method can hide only one bit per word in the text carrier. So, MPHM increases the hiding capacity of the existing process. The algorithm of the MPHM is mentioned in the following (Algorithms 1 and 2).

2.3. Block Diagram of Modified DSTS. Figure 3 shows a block diagram of modified DSTS. The first block is an encoding function that encodes the confidential data; the 2nd block is an encrypted function, which encrypts the encoded data and generates a one-time pad key; the 3rd block is a hiding function that hides the enciphered data and generates a stego key; then, the stego text is sent to the network; the 4th block is a seeking procedure which unhides the stego text with the stego key; the 5th block is a deciphering function which deciphers data with the key; and the 6th block is a decoding process which gives the original data.

2.4. Compression Modified Paragraph Hiding method(CMPHM). The 2nd part of this research uses the LZW compression method with a modified paragraph approach to further improve its hiding capacity. The compression method removes redundancy in the messages of a modified paragraph approach. The compression module is a subtype of text steganography and acts as a third security layer described in [21]. The proposed method's framework is shown in the following. Figure 4 shows the compression module using the modified paragraph approach.

- (1) Get a cover file
- (2) Convert the confidential message to its binary equivalent (bin)
- (3) Read a word from the cover file and write it in a stego file.
- (4) Skip that word that has the same start and end letters, and then, read the next word from the cover text
- (5) Repeat 4 times
 - (a) Read a bit (x) from the bin b .
 - (b) S = start letter of the word, and E = end letter of the word
 - (c) If $x = 0$, write S in the stego key
 - (d) Else if $x = 1$, write E in the stego key
- (6) End repeat
- (7) Repeat 3 to 6 times until the end of the bin file
- (8) Send the stego key and stego text to the receiver

ALGORITHM 1: Hide algorithm 1.

- (1) Read the word from the stego file
- (2) If the start and end letter of the word are the same, then skip it and read the next word from the stego file
- (3) Select the beginning and end character of the word
 - (a) Read the letter from the stego key
 - (b) If $c = s$, then $b = 0$
 - (c) Else if $c = e$, then $b = 1$
- (4) Repeat four times
- (5) End repeat
- (6) Write b to file
- (7) Execute the abovementioned file till the end of the key
- (8) Convert the binary file to the character file

ALGORITHM 2: Seek algorithm 1.

FIGURE 3: Modified DSTS.

The first block is the compressing function, which compresses the confidential data. The 2nd block is the encrypted function, which enciphers the compressed data with a one-time pad key. The 3rd block is a hiding function which hides the enciphered data and generates a stego key; then, the stego text and keys are sent to the network. The 4th block is a seeking procedure which unhides the stego text with the stego key. The 5th block is a deciphering function

which deciphers data with the encipher key. The 6th block is a decompressing function which gives the original data.

3. Test Run

We have confidential data, “eye,” to be hidden in a cover text. After encoding, the confidential data change into an encoding format “00” and then into the enciphered format

FIGURE 4: Compression module using the modified paragraph approach.

“çÈM.” Figure 5 demonstrates the cover text, and Figure 6 illustrates the stego text file. It can realize that the two documents are identical.

4. Experimental Result

We implemented the algorithms in C# language using BenchmarkDotNet=v0.12.1, OS = Windows 10 Intel Core i5-6300U CPU 2.40 GHz (Skylake), 1 CPU, and 4 logical and 2 physical cores. NET Core SDK = 5.0.101. This section analyses the experimental results and benchmarks the proposed approaches' performance with other text steganographic methods.

The mean and standard deviation in Table 1 show that the compression module using the modified paragraph approach standard deviation is less than a paragraph algorithm and modified DSTS, demonstrating its higher optimization and speed.

4.1. Capacity. Steganographic performance is the calculation in terms of capacity, security, and robustness. Capacity shows how much secret information the algorithm can send. Security is an essential factor that shows how much confidential data is hidden from the attackers. Robustness measures the ability to protect personal data from modification. Capacity is the amount of confidential data in a carrier text. The capacity relationship is the division of the quantity of concealed bytes over the cover text size in bytes [12].

$$\text{Capacity ratio} = \frac{(\text{amount of hidden bytes})}{(\text{size of the cover text in bytes})} \quad (1)$$

Supposing one character resides one byte in memory, the capacity ratio multiplied by 100 is called the percentage capacity. Different messages are given below.

- (1) Eye (3 bytes).
- (2) Blue eyes (10 bytes).
- (3) Blue eyes and black eyes (25 bytes).
- (4) Searching eye drops for eye problems in the home (50 bytes).

- (5) Some eye specialists suggest using eye drops for eye problems (63 bytes).
- (6) Some eye specialists suggest using eye drops for eye problems in bad weather and advise washing eyes (100).
- (7) Some eye specialists suggest using eye drops for eye problems in bad weather and advise washing eyes with cold water in summer. Some medical doctors recommend using sunglasses on sunny days in the summer season (204). Table 2 shows the hiding capacity of 7 different messages in the cover text for the first, second, and third methods [8], DSTS, modified DSTS, and compression module using the modified paragraph approach.

Table 3 shows the average percentage hiding capacity of different text steganography approaches and proposed methods. The proposed method's average hiding capacity is higher using the UTF-16 method, except for missing letter puzzle and wordlist, and it works on the ASCII method, and the randomly generated cover text is exposed to structural attack in the paragraph approach using the UTF-8 method.

Table 4 presents the seven embedded messages. The experimental result demonstrates that the cover text for the text steganography method increases with the length of secret messages. In contrast, the compression module using the modified paragraph approach cover text increases less due to redundancy in secret messages. So, the compression module using the modified paragraph approach saves embedding space.

5. Equation of Similarity

$$\text{Jaro-Winler}(s1, s2) = \text{Jaro}(s1, s2) + (L \times p(1 - \text{Jaro}(s1, s2))),$$

$$\text{Jaro}(s1, s2) = \frac{1}{3} \times \left(\frac{m}{|s1|} + \frac{m}{|s2|} + \frac{m-t}{m} \right). \quad (2)$$

FIGURE 5: The cover text.

FIGURE 6: The stego text file.

TABLE 1: Comparing the mean and standard deviation of different approaches.

Types	Mean (μs)	Standard deviation (μs)
Missing letter puzzle	589.9	18.67
Hiding data in the wordlist	262.7	24.89
Paragraph hiding approach	650.6	41.01
A novel approach	249.7	17.02
MDSTS	656.9	48.72
CMPHM	698.3	37.25

The algorithm's similarity was tested using Jaro–Win-
 kler, which examines how the cover text and the secret text
 are very similar to each other. The Jaro score is a similarity
 distance.

s_1 and s_2 are the cover file and the stego file (two strings)
 whose similarity is to be calculated. L is the length of a
 common prefix (maximum 4 characters), p is the scaling
 factor whose standard value is 0.1, m represents the number

TABLE 2: Percentage capacity of the proposed approaches over the seven experimental samples.

Approaches	I	II	III	IV	V	VI	VII
Missing letter app	2.88	5.40	9.09	8.79	8.60	8.71	8.83
Wordlist approach	2.94	5.55	8.33	8.79	8.84	8.95	8.93
Paragraph hiding method	1.96	1.92	2.06	2.00	2.08	2.12	2.13
DSTS approach	1.00	.943	1.02	.996	1.008	1.003	1.005
MDSTS	4	3.77	4.08	3.98	4.032	4.012	4.020
CMPHM	4	3.77	4.84	4.55	4.68	4.96	5.64

TABLE 3: Average percentage capacity of the techniques (having av. % capacity = 1).

Missing letter approach	Wordlist approach	CMHM	MDSTS	HPM	White steg
7.6	7.67	4.63 (UTF-16), 7.76 (UTF-8)	3.98 (UTF-16), 6.49 (UTF-8)	2.06 (ASCII), 1.95 (UTF-8)	1.87
SMS texting	Feature coding	Word map	Spam texting	Word shift	DSTS
1.71	1.47	1.46	1.16	1.03	1 (UTF-16), 1.66 (UTF-8)

TABLE 4: Comparing the cover text size of the proposed approaches for secret messages.

Message length in bytes	MDSTS (cover text length)	Compressed message length in bytes	CMPHM (cover text length)
1	3	296	3
2	10	1061	10
3	25	2437	21
4	50	5030	44
5	63	6251	54
6	100	9973	81
7	202	20118	143

of matching characters of strings, and t is the number of transpositions. Two characters are similar if their distance is not more than $\max(|s1|, |s2|)/2 - 1$. String 1's every character is matched with every character of string 2. Jaro score 0 means that the strings are not similar, and 1 means they are the same. Table 5 shows that the missing letter puzzle has 0.97 similarities. Table 6 compares the average hiding capacity methods using the UTF-8 method.

Table 7 shows the paragraph hiding method, DSTS, modified DSTS, and compression module using the modified paragraph method (CMPHM). The approach has an average Jaro score of 1, which shows these methods can send data without suspicion due to the natural-looking cover text.

6. Discussion

The comparative study shows that missing letter puzzles and wordlist approaches work on the ASCII value of the embedded character, rather than its binary equivalent. It uses a randomly generated cover text exposed to structural attack. Consequently, the average paragraph hiding method's capacity is lower than that of the missing letter puzzle and wordlist approaches. DSTS is the most secure algorithm compared to the paragraph hiding method, but with the most inadequate average hiding capacity of 1% than 2.06% of the paragraph hiding approach; therefore, it needs to enhance the hiding capacity of the DSTS algorithm. The experimental result of MDSTS is 3.98%, with 1.92% higher

TABLE 5: Jaro score of 7 samples of embedded data.

7 Messages	CS1	CS2	CS3	CS4	CS5	CS6	CS7
Jaro score	0.98	0.98	0.97	0.97	0.97	0.98	0.97

than the average hiding capacity of the paragraph hiding method and 2.98% higher than that of the DSTS. The CMPHM has an experimental result of 4.63%, which is 0.65% higher than that of the MDSTS, 2.57% higher than that of the paragraph hiding method, and 3.63% higher than that of the DSTS method. Using the UTF-8 method, the authors have further improved DSTS hiding capacity to 1.66%, PHM hiding capacity to 1.95%, MDSTS to 6.49%, and CMPHM to 7.76%. The experimental result of Table 4 demonstrates that the cover text of many techniques increases with secret message's size. Using the CMPHM removes redundancy in secret messages, so hiding capacity increases, and with lower cover text decreases the stego text which is the best method for a slow network.

The proposed MDSTS is far better than the existing methods as it does not use extra white spaces or misspelled words to conceal the message. It uses CASE encoding, which is better than feature coding, provides security against visual attacks, and uses a natural-looking cover text to protect against structural attacks. The CMPHM also uses two steganographic text methods, one compression method, and the other MPMH. Therefore, stego files with both proposed

TABLE 6: Comparing the average hiding capacity methods using the UTF-8 method.

Message length	Cover text length (bytes)	Capacity (%)	DSTS
Gomal University (18 bytes)	1291	1.4	
Agriculture University Dera Ismail Khan (40 bytes)	2308	1.7	
Peshawar University, Peshawar, k. P. k, Pakistan (43 bytes)	2440	1.76	
University of Science and Technology, China, Hefei (49 bytes)	2749	1.78	
Average hiding capacity of DSTS using UTF-8		1.66	
Gomal University (18 bytes)	319	5.6	MDSTS
Agriculture University Dera Ismail Khan (40 bytes)	577	6.93	
Peshawar University, Peshawar, k.P.k, Pakistan (43 bytes)	618	6.80	
University of Science and Technology, China, Hefei (49 bytes)	741	6.61	
Average hiding capacity of MDSTS using UTF-8		6.49	
Gomal University (18 bytes)	959	1.9	PHM
Agriculture University Dera Ismail Khan (40 bytes)	2034	2.0	
Peshawar University, Peshawar, k.P.k, Pakistan (43 bytes)	2148	2.0	
University of Science and Technology, China, Hefei (49 bytes)	2544	1.9	
Average hiding capacity of the PHM using UTF-8		1.95	
Gomal University (18 bytes)	220	8.18	CMPHM
Agriculture University Dera Ismail Khan (40 bytes)	526	7.60	
Peshawar University Peshawar, k.P.k, Pakistan (43 bytes)	577	7.4	
University of Science and Technology, China, Hefei (49 bytes)	623	7.86	
Average hiding capacity of the CMPHM using UTF-8		7.76	

TABLE 7: Comparison of existing processes with the proposed methods.

Approaches	Cover	Works on	A. V. capacity (%)	Security	Av. Jaro
Missing letter puzzle	Letter puzzle	ASCII number	7.62	Secure	0.97
Wordlist approach	List of words	ASCII number	7.67	More secure	1
CMPHM	Natural-looking cover text	Binary number UTF-16	4.63		1
MDSTS	Natural-looking cover text	Binary number UTF-16	3.98		1
PHM	Natural-looking cover text	Binary number	2.057		1
DSTS approach	Natural-looking cover text	Binary number UTF-16	1		1
DSTS approach	Natural-looking cover text	Binary number UTF-8	1.66		1
PHM	Natural-looking cover text	Binary number UTF-8	1.95		1
MDSTS	Natural-looking cover text	Binary number UTF-8	6.49		1
CMPHM	Natural-looking cover text	Binary number UTF-8	7.76		1

ways will not create any doubt about the existence of a secret message if opened with a word processor, and the OCR technique cannot destroy confidential information. The MDSTS and CMPHM also use a one-time pad encipher key that any brute force attack cannot break, so it is the most secure algorithm. Therefore, it is safe to send a password and pin code on internet using the proposed methods. The CMPHM is faster when the secret message size increases, which is proved by algorithm optimization. So, the MDSTS and CMPHM satisfy the steganographic capacity and imperceptibility. Thus, these methods recognize and develop these two significant parts of the steganographic scheme.

7. Conclusions

We have investigated different methods using UTF-16 and UTF-8. Still, the problem with UTF-16 is that the hiding capacity of text steganography decreases by 50% with this method, which is evident from our experimental results. Nowadays, modern encoding and decoding methods use UTF-8. All cryptographic techniques use it as a standard method; our experimental results show that the CMPHM uses the UTF-8 method, and the hiding capacity improves 3.13% greater than

with the UTF-16 method, 4.63%. Hence, the CMPHM on one side is a more secure method enjoying three-layer security and another side with higher space than the predecessor methods. The OCR technique cannot destroy confidential information in the proposed techniques. These methods use a natural-looking cover text, so the structural attack cannot disclose data. This method can be used for pin passwords and is most specific for intelligence agencies using the secure network for key distribution. Still, for future direction, we need to improve its cap further with more practical ways of cryptography than the one-time pad, which is impractical for large messages and has the burden of the key distribution [22–26].

Data Availability

The numerical dataset used to perform the study presented in the paper can be obtained from the corresponding author on request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. KEP-PhD-48-130-38. The authors, therefore, acknowledge the DSR for technical and financial support.

References

- [1] S. Almuhammadi and A. Al-Shaaby, "A survey on recent approaches combining cryptography and steganography," in *Proceedings of the Sixth International Conference on Information Technology Convergence and Services*, Sydney, Australia, February 2017.
- [2] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk-analyzing past and present economic impact on predicting future developments in IoT risk analysis and IoT cyber insurance," pp. 3–9, 2018.
- [3] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: combining cryptography and steganography," *International Journal of Computer Application*, vol. 9, 2010.
- [4] K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Multimedia Tools and Applications*, vol. 30, no. 1, pp. 55–88, 2006.
- [5] W. Bhaya, A. M. Rahma, and D. Al-Nasrawi, "Text steganography based on font type in MS-word documents," *Journal of Computer Science*, vol. 9, 2013.
- [6] L. Y. Por, K. Wong, and K. O. Chee, "UniSpaCh: a text-based data hiding method using Unicode space characters," *Journal of Systems and Software*, vol. 85, pp. 1075–1082, 2012.
- [7] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: a short survey in IOP conference series: materials science and engineering," *IOP Conference Series Materials Science and Engineering*, Article ID 052003, 2019.
- [8] M. Agarwal, *Text Steganographic Approaches: A Comparison*, <http://arxiv.org/abs/1302.2718>, 2013.
- [9] Y. Khan, "Double secure algorithm for text steganography," *International Journal of Grid and Distributed Computing*, vol. 14, no. 1, pp. 1756–1770, 2021.
- [10] S. Chaudhary, M. Dave, and A. Sanghi, "Text steganography based on feature coding method," *ACM International Conference Proceeding Series*, vol. 12-13, 2016.
- [11] M. Khairullah, "A novel text steganography system in cricket match scorecard," *International Journal of Computer Application*, vol. 21, no. 9, pp. 43–47, 2011.
- [12] F. Al-Haidari, A. Gutub, K. Al-Kahsah, and J. Hamodi, "Improving security and capacity for Arabic text steganography using "Kashida" extensions," in *Proceedings of the 2009 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 396–399, Rabat, Morocco, May 2009.
- [13] K. Bennett, "Linguistic steganography: survey, analysis, and robustness concerns for hiding information in a text," 2004.
- [14] B. Gupta Banik and S. K. Bandyopadhyay, "Novel text steganography using natural language processing and part-of-speech tagging," *IETE Journal of Research*, vol. 66, no. 3, pp. 384–395, 2020.
- [15] M. Khairullah, "A novel steganography method using transliteration of Bengali text," *Journal of King Saud University—Computer and Information Sciences*, vol. 31, no. 3, pp. 348–366, 2019.
- [16] M. Fateh and M. Rezvani, "An email-based high capacity text steganography using repeating characters," *International Journal of Computers and Applications*, vol. 43, pp. 1–7, 2018.
- [17] A. Malik, G. Sikka, and H. K. Verma, "A high capacity text steganography scheme based on huffman compression and color coding," *Journal of Information and Optimization Sciences*, vol. 38, no. 5, pp. 647–664, 2017b.
- [18] A. Malik, G. Sikka, and H. K. Verma, "A high capacity text steganography scheme based on LZW compression and color coding," *Engineering Science and Technology, an International Journal*, vol. 20, no. 1, pp. 72–79, 2017a.
- [19] A. M. Hamdan and A. Hamarsheh, "AH4S: an algorithm of text in text steganography using the structure of omega network," *Security and Communication Networks*, vol. 9, no. 18, pp. 6004–6016, 2016.
- [20] L. Y. Por and B. Delina, "Information hiding: a new approach in text steganography," in *Proceedings of the WSEAS International Conference on Mathematics and Computers in Science and Engineering*, Hangzhou, China, April 2008.
- [21] N. Alanizy, A. Alanizy, N. Baghoza, M. AlGhamdi, and A. Gutub, "3-Layer pc text sca image steganography," *Journal of Research in Engineering and Applied Sciences*, vol. 3, no. 4, pp. 118–124, 2018.