



A New 3-Bit Hiding Covert Channel Algorithm for Public Data and Medical Data Security Using Format-Based Text Steganography

R. Gurunath, CHRIST University (Deemed), India

 <https://orcid.org/0000-0002-7661-2703>

Debabrata Samanta, CHRIST University (Deemed), India*

 <https://orcid.org/0000-0003-4118-2480>

ABSTRACT

The primary concern of every individual and organization is the security of sensitive information generated via authorized activities; nonetheless, illicit data drawing and extraction by attackers is prevalent, which may be mitigated by covert approaches. Although cypher techniques give excellent protection, they raise suspicion in the eyes of adversaries, resulting in both passive and active assaults on the information sent. Steganography, on the other hand, helps to reduce third-party suspicion. This method conceals sensitive information on cover data and transports it to the targets without skepticism. However, the issue depends entirely on the effectiveness of the embedding method; it must also satisfy other data concealing features such as embedding capacity. As payload grows, so does skepticism. This article handled this issue to lessen suspicion while maintaining embedding capacity. The article proposes a format-based text concealing algorithm, a traditional way for dealing with embedding capacity and invisibility. The authors compared our results to those of other similar current methods. They discovered that theirs are pretty decent—the present study offered both standard public communication security and medical data protection.

KEYWORDS

Data hiding, Embedding Capacity, Format-based method, Medical data protection, Steganography, Third-party suspicion, undetectability

1. INTRODUCTION

The most critical concern in information transmission is security; encrypted data typically offer protection but attracts the attention of unauthorized Internet observers and is a sort of passive information assault. On the internet, attackers may find many tools for extracting information, analyzing

DOI: 10.4018/JDM.324076

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

it, and launching active attacks on encrypted data. The above behavior is cypher text, which is visible to everyone on the transport, causing suspicion. After cryptography privacy protection(Laskar, 2012) (Malina, 2021), the next degree of security is steganography, in which information is encrypted and disguised behind innocuous data and conveyed to the targets, avoiding suspicion. Image, audio, video, text, and network protocols are all examples of benign data(Gurunath R. &, 2021)(Gurunath R. &, 2021). Watermarking technology, like Steganography, conceals data on a cover to safeguard the security of digital documents. Watermarking protects the copyright and ensures the secrecy of the document’s details. The document type might be anything from an image to text(Singh, 2021)(Iwendi, 2020).

Steganography uses a concealed writing method instead of transforming data into an unreadable format for secret communication(Sherly, 2010). Only the transmitter and recipient have access to the hidden message. Steganography derives its name from the Greek words “steganos,” which means “covered,” and “graphia,” which means “writing.” Johannes Trithemius used that name for the first time between 1462 and 1516(Fridrich, 2009).

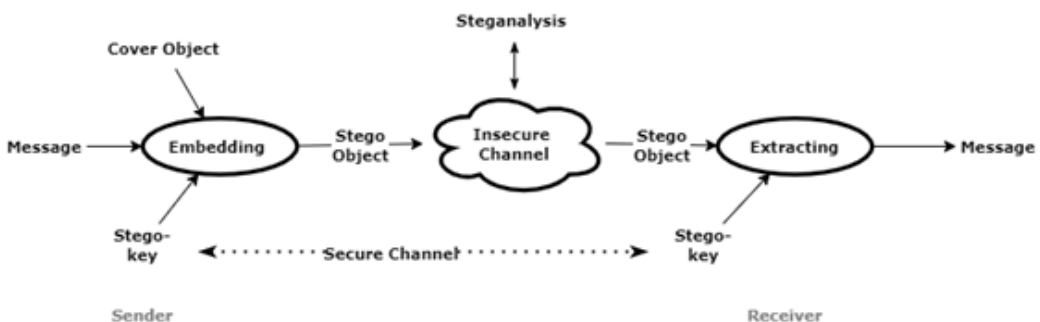
The earliest steganographic techniques were discovered roughly 2500 years ago in ancient Greece when people used to convey secret information by etching it on their shaved heads. When the hair on the head comes back, send that individual to the target to bring the confidential material. During the same period, another example of steganography was embedding the message on a wood surface covered with a wax-like substance to prevent suspicion from other persons during transport(Shin, 2008).

In his ascent to power in ancient India, Chanakya aided the first Mauryan emperor Chandragupta in 283 BC (2303-2395 years ago). He was recognized as a key figure in creating the Maurya Empire. Both Chandragupta and his son Bindusara had Chanakya as their principle counsel. Chanakya proposed a highly evolved and upgraded all-pervasive system of espionage and government. During that period, hidden messages were sent by embedding them in intricately designed puzzles or poems, later carried to the intended recipients(Sarin, 2015).

There are several instances of such early steganography, and a similar concept has been used today as digital data hiding. It is now an element of information technology, alongside cryptography. Concealing, hiding, camouflaging, and embedding data on a text, image, audio, video, and using network protocol are all terms used to describe the modern-day digital steganography process.

The digital steganography process consists of two sub-processes: embedding and extraction (Figure 1), carried out by the transmitter and receiver, respectively. The process’s fundamental purpose is to deliver the message to the intended recipient safely. The message is encoded inside an innocent cover object to avoid detection by third parties, and only the parties involved are aware of how to embed and extract the message. Stego-text results from embedding are comparable to a cover object holding a message and are subsequently sent to the receiver through the Internet (Insecure Channel). The receiver understands how to decode the message from the Stego-object. If a third party suspects the communication, an optional Stego-key can be employed to safeguard it. Stego-key produced by

Figure 1. A typical classical steganography



one of the communication parties using any known method and sent to the other communicating party through a secure channel. However, third-party communication attacks on the Internet cannot be ruled out. They are continually attempting to disrupt the steganography process, known as steganalysis.

Sending patient data across the internet to legitimate recipients is vulnerable to cyber assaults in the medical profession. The most typical response to such instances is to delete private features from clinical notes, such as the patient's name, identification code, gender, and other sensitive data, and replace them with false data. The actual clinical characteristics are to be communicated in a secure setting. Encryption is a popular method for protecting such information. However, arbitrators' suspicions about the cipher data prevail, leading to cryptanalysis and an active attack. The second degree of data protection is required to address such a situation. The second strategy is to use covert channels to deliver the same information. Covert channel transmission is a data concealment strategy that can use an image, video, audio, or text as an object cover.

This work is primarily concerned with Text Steganography. The embedding process might involve changing the text format or changing the meaning of the text. Text steganography is categorized into format-based, random and statistical creation, and linguistic approaches. The format-based focuses primarily on modifying the cover file format, using line-shifting, word-shifting, whitespace, and feature coding methods. Methods for random statistical generation include character sequences and word sequences. Syntactic and semantic approaches are examples of linguistic practices.

The line shift approach of Format-based Steganography is illustrated (Figure 2) here. Line 1 is a formal statement with no changes, while line 2 pushed up a little to incorporate a 0 or a 1 bit. Let us use bit 0 to shift line up, and line 3 shifted down may be considered as a 1 bit. By modifying the structure of the cover file, a series of bits encoded to form the Stego Text containing the hidden message.

Another example of the format-based approach of word shifting (Figure 3). Line 1 is standard text with no changes. Line 2's single and double space insertions imply 0- and 1-bit concealment into the cover text, respectively.

Figure 2. Format-based steganography, example of line shift approach

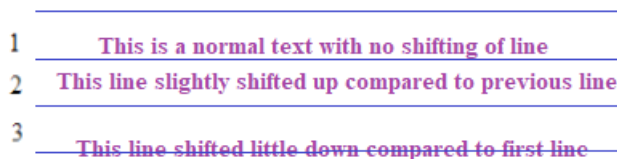
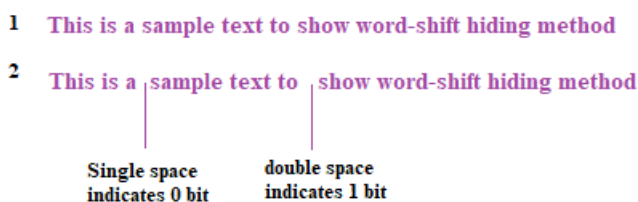


Figure 3. Format-based steganography, example of word shift approach



The format-based data concealing approach is a traditional method that has concerns due to structural changes to the coverttext throughout the embedding process, distorting the cover text to the point of third-party suspicion.

The current study addresses the distortion issue to some extent to overcome it. The research proposes a new approach to format-based data hiding, manages the embedding capacity and the invisibility properties of steganography. The rest of the paper is organized as follows. Section 2 gives an overview of significant research on format-based Steganography and the most current breakthroughs in Steganography, namely IoT, Cloud Computing, Neural Networks, blockchain, and Artificial Intelligence. Section 3 describes a new steganography technique, including message preparation, the actual algorithm, different sub-modules, the Extraction process, and an algorithm illustration. Section 4 presents the results and analysis, Section 5 provides Medical data security, Section 6 Theoretical and Practical Contributions, Section 7 provides shortfalls of the Research, Section 8 gives future work, section 9the paper's conclusion, section 10 provides references.

2. LITERATURE SURVEY

2.1 Related works

Format-based Steganography methods alter the physical structure of the text to embed data. Although the modified properties will not reflect the human eye, some OCR systems can identify them. Because alterations such as moving a line-up and down, word shifting, and inserting whitespaces are methods for hiding data on a cover text. In feature-based approaches, data embedding is done by modifying the feature of the words(Naharuddin, 2018). However, any word processing or OCR application can easily recognize the variations.Sadie et al. 2020(Sadié, 2020)presented colour coding methods for incorporating data in format-based steganography. Some colours are used in the embedding process to colour the text within the cover text. Even though this procedure produces a high embedding capacity, suspicion cannot rule out. Lian et al.(Liang & Iranmanesh, 2016),suggested using whitespace to embed data on a cover text word document. The paper's idea is to incorporate five spaces at random locations in a line of text. A key connects the whitespace characters with the specific message bits. The alterations are removed if viewed in a word editing tool. linguistic Steganography by substituting the word with synonym (Kang, Wu, & Zhang, 2020), generative text using LSTM network(Chaw, 2019), generative text using RNN method (Hamzah, Khattab, & Bayomi, 2021), Linguistic steganography method based on word-indexing compression techniques (Xiang, Wu, Li, & Yang, 2018), hiding data using parts-of-speech tagging(Liu, Wu, & Xin, 2017).

Method of white space Steganography conceals data on cover information by modifying the cover's current layout. Human perception to recognize alterations is inferior, and this is due to the volume of the information encoded. However, these alterations readily are undone by utilizing word processing software's tracks changes. Even if the volume of message concealment exceeds a certain threshold, human vision can quickly detect it.(Khosravi, 2019)(Krishnan, 2017).

The study by (Majeed, 2021) increases the message volume in a pdf document by selecting the option justified formatted text. In the beginning, Huffman coding employed to analyze the data, and a few lines from the cover text used for embedding. Stego key is used to strengthen security even further.

Recent examples of cutting-edge format-based text Steganography include: Line-Shift and word-shift (Roy, 2011), data concealment based on whitespace technique (Liang O. W., 2016), character spacing technique (Shah, 2020), feature coding technique steganography by (Taha, 2020) using Arabic texts, Pseudo-spacing and feature coding by (Al-Nofaie, 2021), Arabic text steganography using Unicode characters (Ditta, 2018), (El Rahman, 2019) suggested data hiding capital letters, punctuation, and whitespace at the start and end of the text, and Chinese text data hiding (Wang, 2021).

2.2 Advancement in Steganography

2.2.1 IOT and Steganography

As the use of IoT grows, so does the number of security risks associated with IoT data; due to the complexity and low memory requirements. However, research on IoT steganography is still in its early stages. Fatima Djebbar et al. (2017) proposed an audio steganography approach for IoT that is noise-tolerant, uses less memory and can conceal a good quantity of payload data (Djebbar, 2017). Ahmed A et al. (2018) offer a technique for embedding payload using quantum Steganography on IoT (Abd El-Latif, 2018), mobile edge computing (Thota, 2018) and Image Steganography on IoT (Ding, 2020), IoT healthcare steganographic application (Hashim, 2020), RFID Steganography (Khan, 2021), securing communication of IoT in 5G network steganography (Fang Y. T., 2020), (Ray, 2021) are some of the research innovations in IoT Steganography.

2.2.2 Cloud Computing and Steganography

People relied on native system memory for everything earlier, from floppy discs to hard discs, pen drives, and even portable HDDs. Because of the way today's software systems work, we can't have our software, memory, or services. Thanks to cloud computing, we can tune our organization by hiring every resource from cloud computing with little infrastructure. There are more significant security worries now than there were previously. To safeguard our data in the cloud, we employ cryptography and security procedures. However, it is insufficient, and the use of steganography has ushered in a new era in security along with encryption; research into concealing data on cloud networks may offer the necessary security (Gurunath & Kumar, 2015). This category includes several steganography advancements that use cloud computing—big data and steganography. On cloud networks, Mrinal Kanti et al. suggested hiding data on images. When a user needs to save a file on the cloud, the sensitive file's properties are encoded in an image, then sent to the cloud storage. As a result, this capability conceals information about a specific file to be stored from unauthorized Internet observers (Sarkar, 2014) Hassan Reza et al. proposed a steganography-based strategy for mobile cloud computing security. Secure hybrid image Steganography algorithm in private cloud was proposed by (Alkadi, 2017), which has the flavor of genetic algorithm.

2.2.3 Machine Learning and Steganography

Thanks to advances in machine learning and deep learning techniques, it can now automate manual operations. The key idea is that the system learns the algorithm with sufficient input using machine learning techniques. It would always produce the best results. Steganography and machine learning have been promising attempts in this respect. The most pleasing aspect is that the system makes an appropriate Stego object instead of sending cover data for concealing. The created Stego is secure.

2.2.4 Neural Networks and Steganography

Using a neural network on classic steganography methods increases the data hiding abilities, imperceptibility, and robustness of the resulting Stego-text. The results of recurrent neural networks and convolution neural networks are encouraging. When compared to traditional hiding strategies, the results are promising. In this article of Yang et al. (Yang Z. W., 2019) TS-RNN, A text steganalysis-based method used a TSteg data set to train the RNN model, which included Chinese and English texts from (Yang Z. W., 2018), and (Fang T. J., 2017) respectively. By altering the number of bits per word in both ways, the Steganography sequence may be reduced at a different rate. Three RNN hidden layers and 300 LSTM were utilized in this technique, with a detection threshold of 0.5. The neurons employ the tanh activation function, a non-linear activation function. The learning rates are set to 0.001 with a batch size of 128. The authors compared the algorithm to three other methods: methods (Meng, 2009), (Samanta, 2016), and (Din, 2015) respectively. Precision, recall, F1-Score, and accuracy are some of the classification models used to assess the model's capabilities. The RNN

method employs LSTM in the hidden layers to avoid the radiant descent issue(Gurunath R. &, 2021). According to the authors, the detection value increases as the rate of embedding increases.

Huixian Kang et al.(Kang H. W., 2020)Proposed a steganography technique based on LSTM and Attention Mechanism. The Steganalysis resistance is provided via an LSTM-based Steganographic process of producing Steganographic texts and embedding the secret on them. Because the text it generates is semantically qualified and raises no suspicions. By integrating an extensive database of words to train the network, LSTM Networks are used to produce automatic text creation for steganography. Several kinds of research have shown that this is an excellent topic for the future(W. Dai, 2010)(Moraldo., 2014)(T. Fang, 2017). RITS proposed by, Yan et al.(Yang Z. Z., 2018) , an RNN version of text steganography based on Reinforcement learning, is proposed in this work. Based on an input sentence, a real-time interactive text generates semantically consistent and syntactically accurate word sequences. While generating the semantically right phrase, the data hiding procedure was merged. This is accomplished by choosing the most semantically correct word.

2.2.5 Block Chain and Steganography

To protect sensitive data, blockchain technology may be applied to Steganography. Steganography works better with Black chains since they are tamper-proof, forgery-proof, and undetectable. The study by Wei She et al. suggests using blockchain to convey personal data over covert routes. Using format-based Steganography, the whitespace approach; the hash value of the text is inserted into a cover text file. The Stego-text is sent across hidden channels in the blockchain network. All nodes in the peer-to-peer network receive the block; however, only the station that meets the credentials may extract the data (She, 2021). On a cover multimedia, (Takaoglu, 2021)developed a Robust Hybrid blockchain and steganography paradigm.

2.2.6 Medical Data Security and Steganography

Medical data leak is arguably one of the most severe challenges in today's medical profession. Medical data breach reports are produced; in 2020, the worst Health Care Data breaches revealed (25 per cent more than 2019). Patients' data and protected health information(PHI) are the primary objectives of these intrusions. According to the U.S. Department of Health and Human Services (HHS), more than 29 million medical data reports have been exposed or compromised.

These cyber-attacks result from a lack of data protection, more susceptible network systems, phishing, malware, and other factors (Journal, 2021). An effort was made to increase the security of patients' data by adding two levels of protection, which may reduce third-party suspicion. Hureib and colleagues(Hureib, 2020)presented a technique for Increasing the security of medical data by combining elliptic curve encryption with picture steganography. The doctor's comments regarding the patient's in addition to the patient's data. Karakiş et al (Karakiş, 2015)presented image steganography in which the patient's data and the doctor's comments are all inserted in a cover file, i.e. Magnetic Resonance pictures. The method relies on fuzzy logic and similarity. Pandey(Pandey, 2020), proposed a Steganography genetic algorithm for securing medical data. Mansour et al(Mansour, 2019)(Wu, 2021), devised a method to prevent assaults on patients' biomedical information. The research proposes a discrete Riplet Transformation technique for hiding patient data in medical cover photos. For additional security, the RSA algorithm is utilized. Ogundokun et al (Ogundokun, 2021), proposed an LSB image Steganography to hide and protect medical data.

3. PROPOSED 3-BIT HIDING ALGORITHM

The proposed technique conceals three bits at each iteration and may divide into modules and submodules. Message Block Preparation, Main Algorithm, eight separate submodules, and Extraction Algorithm are all included. The suggested strategy may use in any area; however, the research focuses on two: Online Social Media (OSN) and Clinical-Data covert channels. The following technique

may concentrate on OSN and the adjustments required to handle the medical data security given in a separate section called “3-bit Hiding for Medical Application.”

3.1 Message Block Preparation

This 3-bit Hiding algorithm includes a message preparation step that prepares a secret message (M) for embedding, shown in Figure 4. The selected message transforms to a binary stream, with bits encoded in the cover text. The binary bit lengths are stored in a variable (m); if the m value is not a multiple of three, a leading 0 bit must be inserted. Divide m by three and store it to (M^1), which results in some 3-bit blocks. Each cycle of the embedding process consumes three bits at a time. For this, an M^b array is created, with each element carrying three bits.

3.2 3-Bit Hiding Algorithm

The 3-bit Hiding algorithm is a data concealing approach on format-based Steganography, one of the traditional encoding flavors. The main idea is to change the text structure to embed data. The alterations usually do not expose the concealed text within it, but they cast doubt on the Stego content. It is up to the method’s quality to deal with any form of suspicion. This approach embeds three bits in the cover text at the desired place. The embedding position is determined using a random function with a narrow range of values. The system is adaptable and can manage how much text is hidden; the more data inserted, the more structural alterations occur, raising suspicion. This technique, based on 3-bit representations, employs eight distinct concealing mechanisms. Each approach embeds bits in the range of 000, 001, 010 up to 111. Before data hiding, a suitable cover file (Cfile) is selected for data hiding (Figure 5). In our situation, we used data from Twitter. The Cover file should contain the

Figure 4. Message preparation module

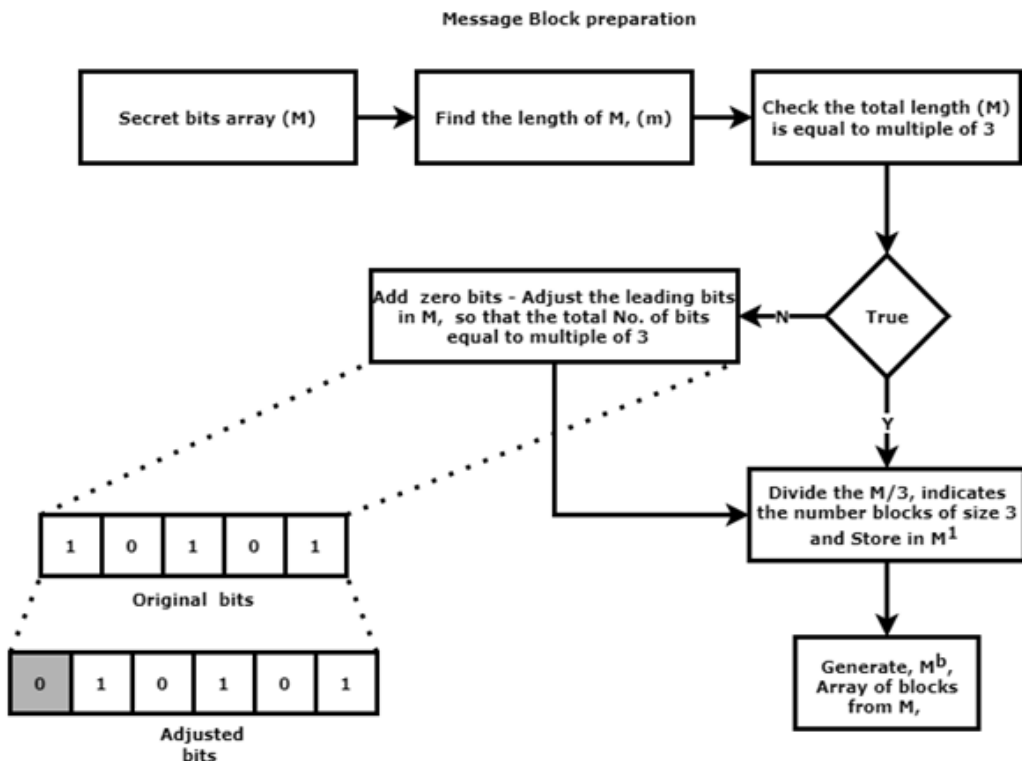
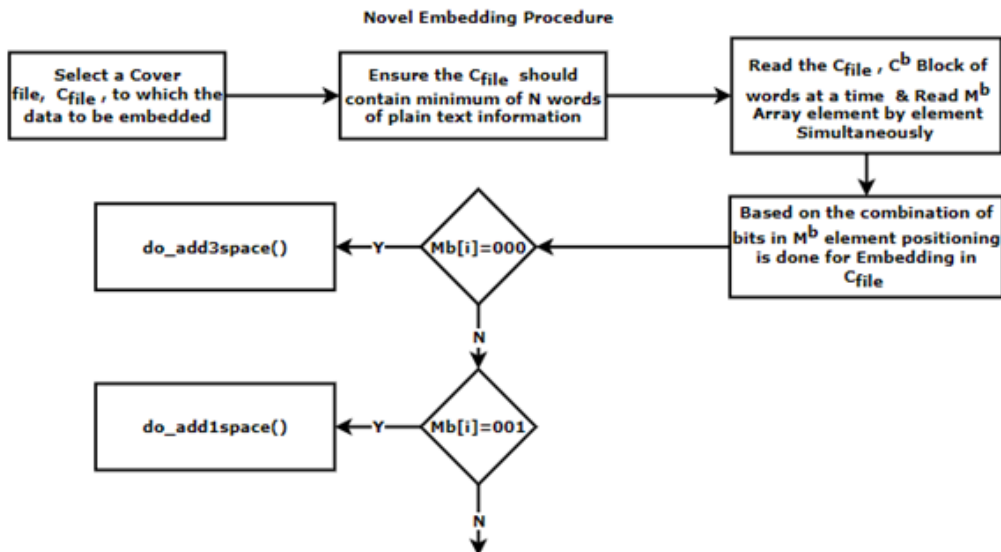


Figure 5. Proposed 3bit hiding steganographic algorithm (part-A)



desired number of words(N), calculated based on the number of 3-bit blocks available in the message and a fixed range of words.

A range of words from the cover file and the initial message block from the Mb array should be read for data concealment (message preparation). The position of hiding the data is done using the random function of range 1-4, meaning for every four words, and 3bits of data to be embedded. Assume, if the bits read are 000 in the first iteration, the algorithm adds three spaces to the calculated location in the cover file. If the bits is 001, add one space; if the bit is 010, add two spaces. If the bit value is 111 (Figure 6), then hyphenstuff. 011 shrinkfont, 100 shftwordup, 101 shftworddown, 110 apostrophesuff, and hyphenstuff if the bit value is 111. Similarly, one of these bits is read in each iteration, and the appropriate module is run with the effect of hiding. This action will be repeated until the final block of the message has been read, and at each iteration, the cover file for the following set of words will also be read. Finally, Stego text generated may be distributed via social media networks, where the intended receiver can extract the secret message using an extraction algorithm.

3.3 3- bit Extraction Algorithm

This method's extraction mechanism (Figure 7) works backwards to recover the embedded message from the Stego-text. The technique uses Stego-text as input and iteratively scans N-words. It recognizes the changes made to the N-words and extracts the appropriate 3-bit data. The identification of characters and other feature changes to obtain 3-bits. If the character is a single space, the value 001 is in the Ebits array. The same may apply to other formatting options. When all N groups of words have scanned and retrieved, the Ebits array utilized to convert the binary bits to ASCII characters. Before conversion, the total bits deducted from m (the original number of bits), and the difference recorded in the 'diff' variable. The 'diff' function used to delete the 'Ebits' array's leading 'diff' number of bits.

3.4 Submodules

When a block of bits retrieved from the Mb array, a particular submodule invoked to determine the embedding location in the cover file's N words. The procedure controlled by a random function with a limited range of values ranging from 1 to N. One of eight operations used to achieve the embedding (Figure 8). For example, if the Mb array element is 001, the submodule do_ add1space

Figure 6. Proposed 3bit hiding steganographic algorithm (part-B)

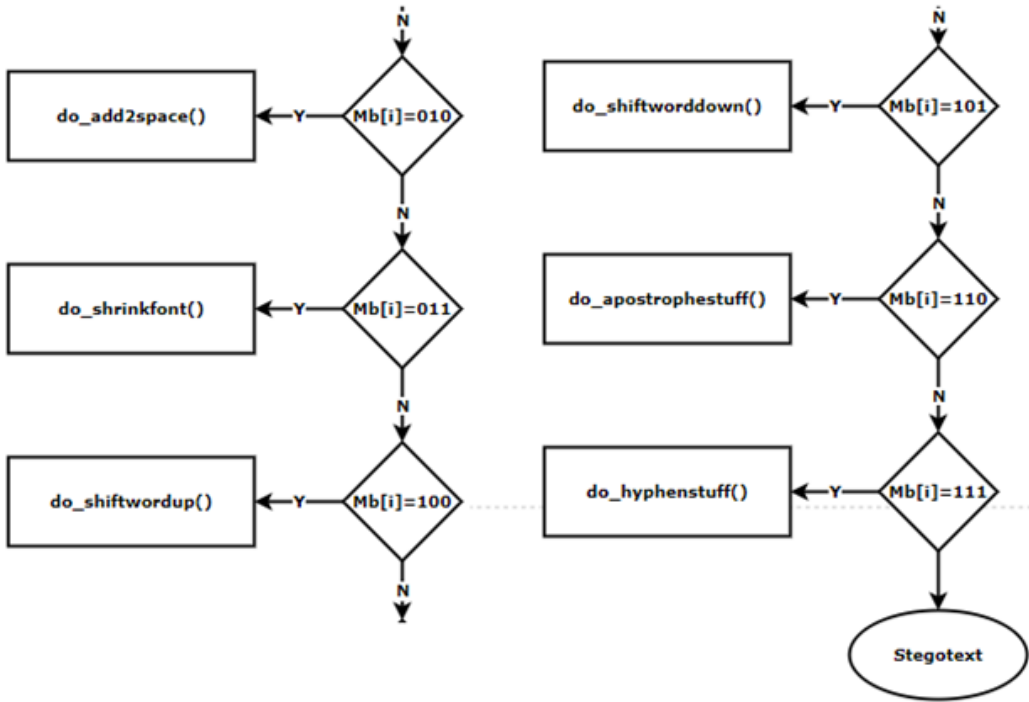
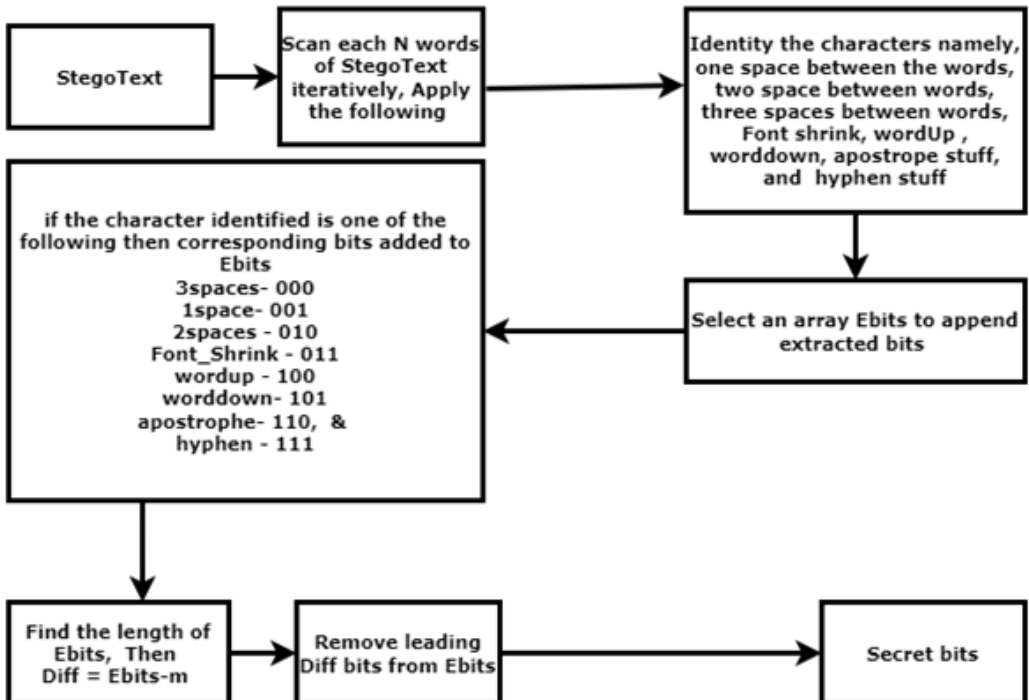


Figure 7. proposed 3-bit extraction algorithm



() invoked. After determining the embedding location through random function, a single space added to disguise the 001 bit in the cover text. This technique repeated for every combination of 3-bit data and embedding processes. The Shrinkfont module reduces the font size of the word by 0.5. When the bits recovered as 001, 010, and 000, the addspace module embeds either a single double or three spaces. When the bits retrieved as 100, 101, the shiftwordup and shiftworddown modules move the word position slightly up or down. Similarly, when the Mb array returns 110 or 111, an apostrophe or hyphen is embedded in the cover text at the calculated location.

3.5 Illustration of Proposed 3-bit Hiding Algorithm

The 3-bit Hiding algorithm’s operation depicted as an example in the graphic shown in Figure, which includes original text extracted from Twitter data as a cover file. The final Stego-text after the embedding procedure presented. The arrows denote that certain 3bit information is hidden based on the bit combination. The message is “hidden,” which contains six characters and transformed into binary sequence bits. To embed the message, the binary stream divided into three bits. The first instance of the three-bit data, ‘011,’ denotes a shrinkfont operation that embeds 011 by reducing the font for the third word. The embedding location determined by a random function with a range of 1-4. (as explained in the algorithm). Similarly, the process repeated until all of the triplets have been exhausted.

4. RESULTS AND ANALYSIS

Texts always have fewer redundant bits than images and audio; thus, it is very difficult to embed significant amounts of data. Because of the design of images, a great volume of a message may be inserted. Human eyesight cannot easily recognize those alterations. However, to embed more data in text, a huge text cover file is required. Our solution employs format-based text steganography, which necessitates structural modifications to the cover file in order to disguise the contents. The embedding

Figure 8: Eight sub modules each embeds 3-bits into the cover text

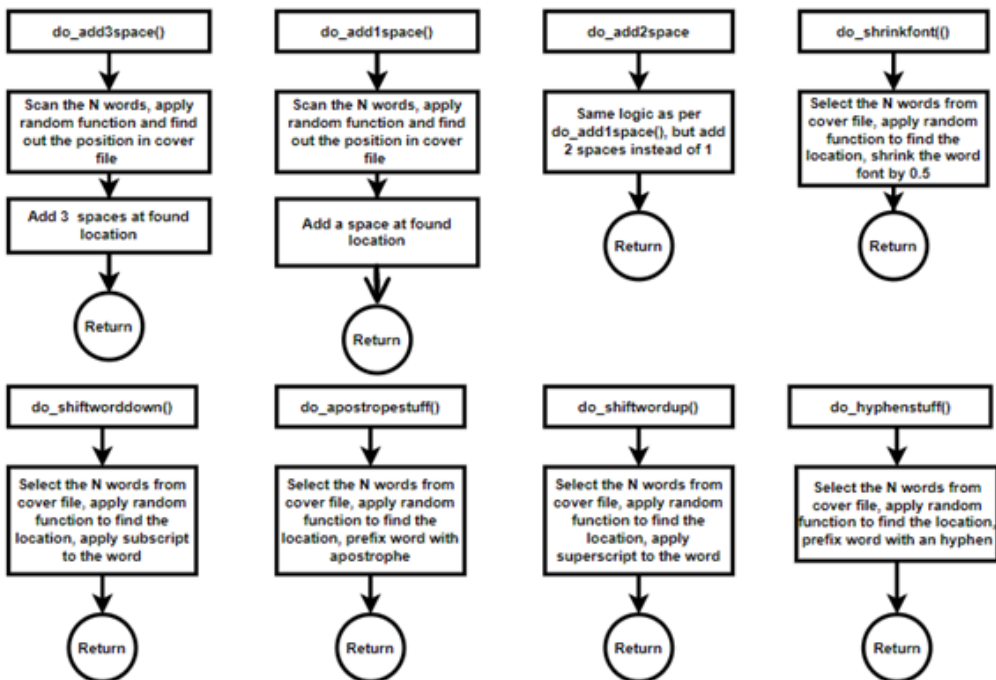


Figure 9. Illustrated example of proposed Algorithm using twitter data

Original Cover text (Twitter)

Located about 10 minutes from Kundasang town, Sosodikon Hill offers an easy hike suitable for beginners. Make sure to go before 7AM so you can enjoy a perfect view of the majestic Akinabalu! Enjoy the scenery with the cool weather, misty air, and the perfect view of Mount Kinabalu from Sosodikon Hill, Kundasang. One of the most beautiful highlands in Malaysia. It's a must-visit when in Sabah.

Stego-Text with Embedded Message

Located about ⁰¹¹10 minutes from ⁰¹⁰Kundasang town, Sosodikon Hill offers an ⁰⁰⁰easy hike ¹¹⁰ suitable for beginners. Make ¹⁰⁰sure to go before 7AM ¹⁰¹so you can enjoy a perfect view of the majestic Akinabalu! Enjoy the scenery with the cool weather, misty air, and the perfect view of Mount Kinabalu from Sosodikon Hill, Kundasang. One of the most beautiful highlands in Malaysia. It's a must-visit when in Sabah.

Secret word: **hidden (6 chars)**

Binary values : (no prefix 0)

011 010 000 110 100 101 100 100 011 001 000 110 010 101 101 110 (6X8=48bits ; 48/3=16Blocks, 4words /iteration)

capacity and the appearance of the cover file must always be in some proportion; otherwise, third-party doubt arises due to cover file distortion.

This paper compares our methodology to other methods, represented numerically in Table 1 and graphically in Figure 10. We chose Cover Twitter data (Malaysia) of same size to evaluate the performance of our algorithm and compared it to other approaches. The author (Dulera, 2012) uses the quadruple approach to arrange English letters based on their characteristics. There are four groups, and their identifiers are A, B, C, and D; curved letters, letters with a central horizontal straight line, letters with one vertical straight line, and letters with a diagonal line. Each group is designated by the bits 00, 01, 10, 11, and these are the bits that are hidden when a character of that kind is present in the cover file. The author (Shahreza, 2006) uses feature coding to embed data based on the features of Persian letter features using the Persian language. The embedding bits are added one at a time, with a 0-bit indicating the lack of the feature and a 1-bit indicating the existence of the feature. In order to test the performance of this method, we used a specific feature of the English language and obtained the results shown in the Table 1 and (Kamaruddin, 2018). For all approaches, the covertext data is 3568 bits. The embedding procedure was applied to all techniques and yielded hidden message bits 105 (our method), 118,75, and 57.

The analysis reveal that our technique outperforms feature coding and the Inter-Word Space method, outperforming the Quadruple method by lowering third-party suspicion. Because by simply lowering the N value (presently 4), it is feasible to increase the embedding capacity more than the Quadruple technique. As we go, the Stego text gets increasingly distorted, raising third-party suspicion. As a result, data hiding properties always proportionate, and keep the properties balanced to minimize possible steganalysis by third parties.

4.1 Equation 1: Embedding Ratio

$$\text{Embedding Ratio} = \frac{\text{Total Embedding bits}}{\text{Total Expected Stego bits}} * 100\%$$

Table 1 provide an embedding ratio for all techniques in addition to embedding capacity. The embedding ratio (Equation 1) is the total number of embedding bits divided by the size of the Stego text, and it reflects the embedding volume concerning the Stego text. Equation 1 expresses the embedding ratio relationship.

The graph inFigure 10depicts the variance in embedding capacity between our approach and others. Even though it is format-based, the quadruple technique tested for analysis employed a different method. The other two strategies, feature coding and inter-word spacing, fared less than our method. Our proposed method can do even better in terms of embedding capacity, but the invisibility of steganography is compromised. As a result, balancing embedding capability with imperceptibility is critical.

Our Steganography method has been tried in conjunction with the other approaches stated above. The data set utilized to carry out this experiment is Twitter data. Several Twitter media samples were utilized to assess the volume of embedding capacity and embedding ratio. Figure 9depicts one such sample cover with concealed data. Several samples of text with varying volumes are used as covers for this analysis.

Table 1. Comparison of Steganography approaches with our approach – Trial-1

Steganographic Approaches	Cover text size bits	Hidden message bits	Stego Text Size	Embedding Ratio
Our Proposed 3-bit hiding Method	3568	105	3669	2.86
Quadruple method (Dulera, 2012)	3568	118	3682	3.2
Feature Coding (Shahreza, 2006)	3568	75	3639	2.06
Inter-word space method (Kamaruddin, 2018)	3568	57	3621	1.57

Figure 10. Performance of Proposed Format-based Steganography Algorithm Vs other Approaches(Trial-1)

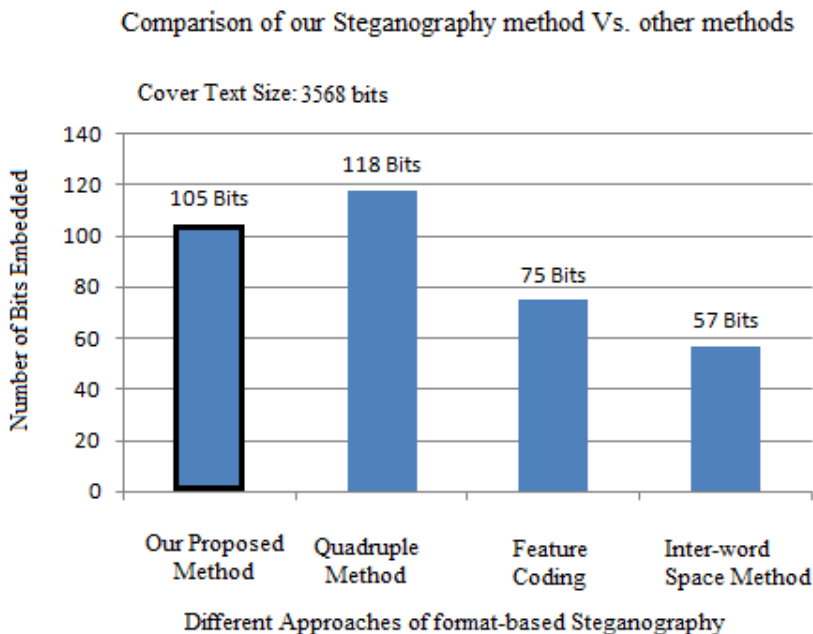


Table 2. Comparison of Steganographic approaches with our approach – Trial-2

Steganographic Approaches	Cover text size bits	Hidden message bits	Stego Text Size	Embedding Ratio
Our Proposed 3-bit hiding Method	7200	225	7425	3.03
Quadruple method	7200	246	7446	3.30
Feature Coding	7200	160	7360	2.17
Inter-word space method	7200	120	7320	1.64

The details of the trial-1 with a cover size of 3568 bits (446 characters including spaces) are shown in Table 1. We were able to conceal 105 bits (13 characters). one additional one-bit was added to make the length of the bit stream a multiple of three.

Similarly, using Equation 1, we calculated an embedding ratio of 2.86. Other approaches were tested along the same lines, using the same cover text size bits. Table 1 shows a comparison of the results achieved with our approach and other methods. Figure 10 depicts it visually using a bar graph.

Table 2's Trial-2 demonstrates an increase in cover text volume to 7200 bits (900 characters including spaces). We evaluated for increased cover volume and message size, and our technique outperformed two other ways in embedding capacity and embedding ratio (0.17 in our method). The relative embedding ratios of all approaches are determined in Table 3. When compared to other approaches, our suggested method has the good embedding ratio (Figure 10). This demonstrates that as the volume of cover data rises, so does the quantity of embedding volume.

4.1.1 Data Set

As previously stated, the data sets utilized for the proposed 3-bit Hiding steganography approach include Twitter data. The sample data is displayed in Figure 11 (News, 2019).

The data sets gathered via Twitter, as well as the approach tested in our instance employing social media datasets. There are too many individuals and messages viewed on Online Social Networks. These cover text modifications intended for a single individual or a small intended group. Ninety-nine per cent of users are ordinary consumers who are unconcerned about the material exchanged on social media networks (Gurunath R. K., 2021). The remaining 1% of the population may be interested in steganalysis; arbitrator analysis will not succeed most of the time. As a result, the Stego material displayed is safe.

5. 3-BIT HIDING STEGANOGRAPHY FOR MEDICAL APPLICATION

The proposed text steganography method is ideal for medical data security. The size of the carrier cover file determines the size of the message hidden. The 3-bit Hiding method safeguards sensitive

Table 3. Improved Embedded Ratio of Proposed Format-based steganography Algorithm Vs other Approaches

Steganography Approaches	Embedding Ratio Trial-1	Embedding Ratio Trial-2	Improvement in Embedding Ratio
Our Proposed 3-bit hiding Method	2.86	3.03	0.17
Quadruple method	3.2	3.30	0.10
Feature Coding	2.06	2.17	0.11
Inter-word space method	1.57	1.64	0.07

Figure 11. performance of our method with regard to Embedding Ratio



Figure 12. Sample datasets used for the embedding (News, 2019)

Sample 1 (Featured in: Malaysia morning news for November 19)

About Malaysia morning news. Malaysia morning news roundup is the most comprehensive hand-curated selection of Malaysia English language news headlines published. Each weekday we scour hundreds of local and international news sites and websites to find the most recent Malaysia English language news today. We filter out the dull, the boring, the repetitive, and the click-bait and package all of the Malaysia daily news that you need to know to start

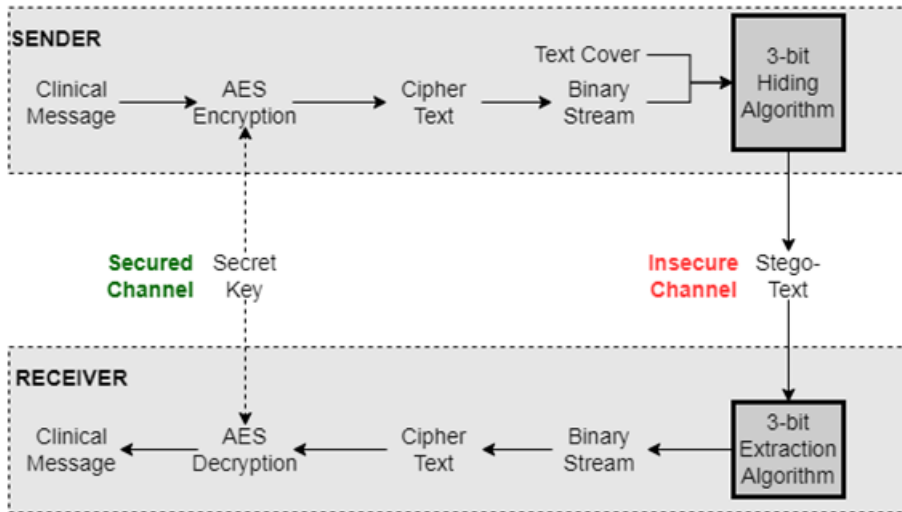
Sample 2 (Featured in: Malaysia morning news for November 19)

We clearly identify the source of all the Malaysia news headlines, whether it is behind a paywall, a media release, or whether the news site uses annoying pop-up advertising or auto-play video, in case those things annoy you too. If a website uses particularly invasive pop-up adverts, we'll tell you. This enables you to make an informed choice of whether you want to learn more by clicking directly through to the original Malaysia news article.

clinical data of patients and doctors' recommendations from opponents and the data encapsulated in a cover file. The cover file selected is any regular medical/clinical/other data file. It must be an English text file—the carrier cover file delivered to targets via social media or the primary channel like email (Ch, 2016).

The 3-bit Hiding Algorithm (Figure 12) requires two parameters: a cover file and the binary stream containing the message to be hidden. AES (Advanced Encryption Standard) encryption protects the message before being hidden on a cover file. Encryption turns the message to an unreadable format or cypher text. The key used is a shared key for both the sender and the recipient and distributed through a secure channel. The obtained encrypted text from the AES algorithm is converted to a

Figure 13: Medical data embedding and extraction through proposed 3-bit hiding algorithm



binary stream and subjected to the 3-bit Hiding method. A carrier (any medical/clinical/other data file) is selected and fed into the algorithm. The algorithm’s entire operation is described in the section “Proposed 3-bit Hiding Algorithm.” The method produces a Stego-text. The Stego-text is often sent to the chosen targets via an unsecured connection or the public Internet. Third-party suspicion, steganalysis, and attacks on the Stego-text occur at this location. The Stego-text is subjected to the proposed 3-bit Extraction technique at the receiver location, yielding a binary stream. The encrypted text is translated to ASCII. The encrypted text passed into the AES decryption process to recover the message (secure medical data). AES decryption uses a shared key communicated across the secure channel (Vijayakumar, 2019).

6. THEORETICAL AND PRACTICAL CONTRIBUTIONS

The scholarly community is encouraged by this study, which also provides further proof in support of format-based text steganography. The current approach introduces the concept of 3-bit embedding. The approach makes use of a various existing format-based methods, such as word-shift, line-shift, shift-word-up, shift-word-down, and open-space. In addition, the algorithm introduces three new techniques: shrink-font, hyphen-stuff, and apostrophe-stuff. This study further emphasizes embedding ratio compare to other methods mentioned above. The approach comprising of message preparation, Embedding procedure, and an extraction procedure.

Although, in image steganography, there are several strategies that conceal multiple bits at once in the cover image. For example, research carried out by (Li, 2009), (Sathish Shet, 2017) conceals multiple bits in image.

Text in contrast, our method of concealing several bits at once into a cover is a unique for format-based text steganography. There are few Multiple bit text data hiding is demonstrated in the literature. One of the two important papers as follows: (Kumar, 2015) provides a concept of 2bit, 3bit, and 4-bit encoding. The utilization of Unicode space characters serves as the cornerstone of this method. Although multiple bit encoding is theoretically conceivable, the unanticipated gaps that are produced in this technique after embedding actually lead to more visual attack. In order to mask 2-bit data, (Yadav, 2015) suggested a different approach, quadruple categorization based on feature coding was successful in embedding two bits at a time. This method involves a large cover

file in order to conceal the data. When compared to our technique, this strategy produces a lower embedding ratio than some other ways.

Our model employed the various approaches of format-based text steganography listed at the beginning of this section to conceal data. The previously mentioned methods use quadruple classification and Unicode space characters, respectively, to conceal data, which is a type of method described in the preceding paragraph. Consequently, we claim that our strategy is a unique one. This paper's "Results and discussion" section demonstrates the uniqueness of our methodology in comparison to other approaches.

In the section titled "3-bit Hiding Steganography for Medical Application" of this paper, we discuss the practical advantages of our proposed 3-bit concealing methodology and explain how it may be used in the medical industry. The technique may also be used to any industry where secret messages are sent. It is possible to use the method to set up covert communications. However, an application comparable to MS Word may remove the concealments if the formatting settings are enabled and editable. Therefore, these techniques are suitable for taking a manual print on paper or delivering Stego data as an image on social media networks.

According to (Alvesson, 2007), it is vital to evaluate the broad applicability of new research models and processes in line with theory-building literature in order to better grasp the context and how it could alter how ideas are received. This is especially true when long-held beliefs start to disintegrate since these breaks foster the growth of new knowledge.

7. SHORTFALLS OF THE RESEARCH

In our current research though, when compared to other current approaches, our method showed a slight increase in embedding capability. The problem is that as the message volume grows, the imperceptibility feature of steganography affects, resulting in third-party mistrust. This applies to all existing methods. As a result, there is a requirement for a balance between imperceptibility and embedding capacity.

8. FUTURE WORK

This article may provide valuable, interesting insights for those researchers who are always reading papers of this sort. This article's approach arose from improving the embedding capacity while keeping the undetectability attribute steganography in mind. The algorithm may be enhanced further in the 4-bit embedding to boost embedding capacity. Furthermore, this traditional method may be improved using artificial intelligence, RNN, LSTM, etc., to improve performance.

9. CONCLUSION

Initially, the objective was to expand the embedding capacity. We developed a novel technique, the 3-bit Hiding Algorithm, based on a sort of traditional data hiding approach known as format-based text steganography. However, as the algorithm was tested with varied Twitter data, our carrier text distorted as the payload rose. As the format-based method's guiding concept, when embedding occurs, the structure of the carrier text changes. Our suspicions were aroused by the Stego-text created. Then we made a minor adjustment to the algorithm and reduced the payload capacity, resulting in significantly improved Stego-text. Our technique fared better than the other two methods. Finally, when the payload is greater, suspicion cannot be ruled out. The algorithm may be used in a wide range of areas where secret messages are transmitted over covert channels. This article presents two such applications, one for the general public or any individual who wishes to communicate their data secretly, and the other

for medical data security. Patients'/medical data is susceptible and should not be accessible by third parties; only the intended persons should use it. In this regard, the proposed strategy is beneficial.

DATA AVAILABILITY

The evaluation data that support the findings of this study are available on request from the corresponding author.

DISCLOSURE

The funder had no role in the design of the study; in the collection, analyses, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

No funding available for this research.

REFERENCES

- Abd El-Latif, A. A.-E.-A. (2018). Secure quantum steganography protocol for fog cloud internet of things. *IEEE Access : Practical Innovations, Open Solutions*, 6, 6. doi:10.1109/ACCESS.2018.2799879
- Ahmed, U. e., Srivastava, G., & Lin, J. C.-W. (2021). A Machine Learning Model for Data Sanitization. *Computer Networks*, 189, 107914. doi:10.1016/j.comnet.2021.107914
- Al-Nofaie, S. G.-G. (2021). Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces. *Journal of King Saud University-Computer and Information Sciences*, 963-974.
- Alkadi, I. (2017). Application and Implementation of Secure Hybrid Steganography Algorithm in Private Cloud Platform. *Journal of Computer Science Application and Information Technology*, 2(2), 4. doi:10.15226/2474-9257/2/2/00105
- Alvesson, M., & Kärreman, D. (2007). Constructing mystery: Empirical matters in theory development. *Academy of Management Review*, 32(4), 1265–1281. doi:10.5465/amr.2007.26586822
- Ch, R. (2016). Squint Pixel Steganography: A Novel Approach to detect Digital Crimes and recovery of medical images. [IJDCF]. *International Journal of Digital Crime and Forensics*, 8(4), 37–47. doi:10.4018/IJDCF.2016100104
- Chaw, A. (2019). ext steganography in Letter of Credit (LC) using synonym substitution based algorithm. *Int. J. Adv. Res. Dev.*, 4, 59–63.
- W. Dai, Y. Y. (2010). Text steganography system using markov chain source model and DES algorithm. *Journal of*, 5(7), 785-792.
- Din, R. Y. (2015). Performance analysis on text steganalysis method using a computational intelligence approach. *In Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics*, (pp. 19-20). IEEE.
- Ding, X. X., Xie, Y., Li, P., Cui, M., & Chen, J. (2020). Image Steganography Based on Artificial Immune in Mobile Edge Computing With Internet of Things. *IEEE Access : Practical Innovations, Open Solutions*, 8, 8. doi:10.1109/ACCESS.2020.3010513
- Ditta, A. Y. (2018). Information hiding: Arabic text steganography by using Unicode characters to hide secret data. *International Journal of Electronic Security and Digital Forensics*, 61-78.
- Djebbar, F. &.-A. (2017). Lightweight noise resilient steganography scheme for Internet of Things. *GLOBECOM 2017-2017 IEEE Global Communications*, (pp. 1-6).
- Dulera, S. J. (2012). Experimenting with the novel approaches in text steganography. arXiv preprint arXiv:1203.3644.
- El Rahman, S. A. (2019). Text steganography approaches using similarity of English font styles. [IJSI]. *International Journal of Software Innovation*, 7(3), 29–50. doi:10.4018/IJSI.2019070102
- Fang, T. J. (2017). Generating steganographic text with LSTMs. *arXiv Preprint*.
- Fang, Y. T. (2020). Securing Data Communication of Internet of Things in 5G Using Network Steganography. *International Conference on Artificial Intelligence and Security*, (pp. pp. 593-603). Springer. doi:10.1007/978-3-030-57881-7_52
- Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press. doi:10.1017/CBO9781139192903
- Gurunath, R. (2021). A novel approach for semantic web application in online education based on steganography. *International Journal of Web-Based Learning and Teaching Technologies*, 17(4), 13. doi:10.4018/IJWLTT.285569
- Gurunath, R. (2021). Advances in Text Steganography Theory and Research: A Critical Review and Gaps. In S. P. al., *Multidisciplinary Approach to Modern Digital Steganography* (p. 380). IGI Global.
- Gurunath, R. (2021). Insights into Artificial Neural Network techniques, and its Application in Steganography. *Journal of Physics*, 8.

- Gurunath, R. (2021). Insights into Artificial Neural Network techniques, and its Application in Steganography. *Journal of Physics*, 8.
- Gurunath, R., & Kumar, K. (2015). SaaS Explosion leading to a New Phase of a Learning Management System. *IJCRR*, 7(22).
- Gurunath, R. A., Alahmadi, A. H., Samanta, D., Khan, M. Z., & Alahmadi, A. (2021). A novel approach for linguistic steganography evaluation based on artificial neural networks. *IEEE Access : Practical Innovations, Open Solutions*, 9, 15. doi:10.1109/ACCESS.2021.3108183
- Gurunath, R. K., Klaib, M. F. J., Samanta, D., & Khan, M. Z. (2021). Social Media and Steganography: Use, Risks and Current Status. *IEEE Access : Practical Innovations, Open Solutions*, 9, 10. doi:10.1109/ACCESS.2021.3125128
- Hamzah, A., Khattab, S., & Bayomi, H. A. (2021). linguistic steganography framework using Arabic calligraphy. *J. King Saud Univ.-. Comput.*, 33, 865–877.
- Hashim, M. M., Rhaif, S. H., Abdulrazzaq, A. A., Ali, A. H., & Taha, M. S. (2020). Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography. *IOP Conference Series. Materials Science and Engineering*, 881(1), 012120. doi:10.1088/1757-899X/881/1/012120
- Hureib, E. S. (2020). Enhancing medical data security via combining elliptic curve cryptography and image steganography. *International Journal of Computer Science and Network Security*, 20(8), 1–8.
- Iwendi, C. e., Jalil, Z., Javed, A. R., Reddy G, T., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks. *IEEE Access : Practical Innovations, Open Solutions*, 8, 72650–72660. doi:10.1109/ACCESS.2020.2988160
- Kamaruddin, N. S., Kamsin, A., Por, L. Y., & Rahman, H. (2018). A review of text watermarking: Theory, methods, and applications. *IEEE Access : Practical Innovations, Open Solutions*, 6, 6. doi:10.1109/ACCESS.2018.2796585
- Kang, H., Wu, H., & Zhang, X. (2020). Generative text steganography based on LSTM network and attention mechanism with keywords. *Electron. Imaging*, 291.
- Kang, H. W. (2020). Generative text steganography based on LSTM network and attention mechanism with keywords. *Electronic Imaging, Society for Imaging Science and Technology*, 291-1 to 291-7.
- Karakış, R. G., Güler, İ., Çapraz, İ., & Bilir, E. (2015). A novel fuzzy logic-based image steganography method to ensure medical data security. *Computers in Biology and Medicine*, 67, 172–183. doi:10.1016/j.combiomed.2015.10.011 PMID:26555746
- Khan, H. A., Abdulla, R., Selvaperumal, S. K., & Bathich, A. (2021). IoT based on secure personal healthcare using RFID technology and steganography. *Iranian Journal of Electrical and Computer Engineering*, 11(4), 3300. doi:10.11591/ijece.v11i14.pp3300-3309
- Khosravi, B. K. (2019). A new method for pdf steganography in justified texts. *Journal of information security and applications*, 61-70.
- Krishnan, R. B. (2017). An overview of text steganography. *Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)* (pp. 1-6). IEEE.
- Kumar, R. C. (2015). An efficient text steganography scheme using Unicode Space Characters. *International Journal of Forensic computing. Science*, 8–14.
- Laskar, S. A. (2012). High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems*, 57.
- Li, C. T., Li, Y., & Wei, C.-H. (2009). Protection of digital mammograms on PACSs using data hiding techniques. *International Journal of Digital Crime and Forensics*, 1(1), 75–88. doi:10.4018/jdcf.2009010105
- Liang, O., & Iranmanesh, V. (2016). Information hiding using whitespace technique in Microsoft word. *International Conference on Virtual System & Multimedia (VSMM)*, (pp. 17–21). Kuala Lumpur, Malaysia.
- Liang, O. W. (2016). Information hiding using whitespace technique in Microsoft word. *International Conference on Virtual System & Multimedia (VSMM)* (pp. 1-5). IEEE. doi:10.1109/VSMM.2016.7863183

- Liu, Y., Wu, J., & Xin, G. (2017). Multi-keywords carrier-free text steganography based on part of speech tagging. *Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, (pp. 29–31). IEEE. doi:10.1109/FSKD.2017.8393096
- Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A Review on Text Steganography Techniques. *Mathematics*, 9(21), 2829. doi:10.3390/math9212829
- Malina, L. E., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevicius, R., Affia, A.-A. O., Laurent, M., Sultan, N. H., & Tang, Q. (2021). Post-Quantum Era Privacy Protection for Intelligent Infrastructures. *IEEE Access : Practical Innovations, Open Solutions*, 9, 36038–36077. doi:10.1109/ACCESS.2021.3062201
- Mansour, R. F., & Abdelrahim, E. M. (2019). An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications. *Multidimensional Systems and Signal Processing*, 30(2), 791–814. doi:10.1007/s11045-018-0575-3
- Meng, P. H. (2009). Linguistic steganography detection algorithm using statistical language model. *International conference on information technology and computer science*. IEEE.
- Moraldo., H. (2014). An approach for text steganography based on markov chains. *Preprint arXiv*.
- Naharuddin, A. W. (2018). A high capacity and imperceptible text steganography using binary digit mapping on ASCII characters. *International Seminar on Intelligent Technology and Its Applications (ISITIA)*, (pp. 287–292).
- Men, S. (2019, November). Malaysia Morning News for November 21. *Asian News Today*. <https://aseanewstoday.com/2019/malaysia-morning-news-for-november-21-3/>
- Ogundokun, R. O., & Abikoye, O. C. (2021). A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography. *International Journal of Digital Multimedia Broadcasting*, 2021, 1–8. doi:10.1155/2021/8827055
- Pandey, H. M. (2020). Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. *Future Generation Computer Systems*, 111, 213–225. doi:10.1016/j.future.2020.04.034
- Ray, A. M. (2021). IoT Security Using Steganography. *Multidisciplinary Approach to Modern Digital Steganography*, 191–210.
- Roy, S. (2011). A novel approach to format based text steganography. *international conference on communication. Computers & Security*, 511–516.
- Sadié, J. K. (2020). *A high capacity text steganography scheme based on permutation and color coding*. Sorbonne University.
- Samanta, S. D. (2016). *A real time text steganalysis by using statistical method*. *IEEE international conference on engineering and technology*. ICETECH.
- Sarin. (2015, Oct). *Chanakya Arthashastra-Greatest book on spying and secret agencies*. Chanakya Arthashastra. <https://mallstuffs.com/Blogs/BlogDetails.aspx?BlogId=414&BlogType=Spiritual&Topic=Chanakya%20Arthashastra-Greatest%20book%20on%20spying%20and%20secret%20agencies>
- Sarkar, M. K. (2014). Enhancing data storage security in cloud computing through steganography. *International Journal of Network Security*, 5(1), 13.
- Sathish Shet, K. A., Aswath, A. R., Hanumantharaju, M. C., & Gao, X.-Z. (2017). Design and development of new reconfigurable architectures for LSB/multi-bit image steganography system. *Multimedia Tools and Applications*, 76(11), 13197–13219. doi:10.1007/s11042-016-3736-0
- Shah, S. T. (2020). Text steganography using character spacing after normalization. *International Journal of science and Engineering Research*, 949–957.
- Shahreza, M. (2006). A new approach to Persian/Arabic text steganography. *IEEE/ACIS International Conference on Computer and Information Science*, (pp. 310–315). IEEE. doi:10.1109/ICIS-COM SAR.2006.10
- She, W. H. (2021). A double steganography model combining blockchain and interplanetary file system. *Peer-to-Peer Networking and Applications*, Springer, 3029–3042.

- Sherly, A. P. (2010). A compressed video steganography using TPVD. *International Journal of Database Management Systems*, 67-80.
- Shin, F. (2008). *Digital Watermarking and Steganography: Fundamentals and Techniques* (1 ed.). CRC Press.
- Singh, A. K., Thakur, S., Jolfaei, A., Srivastava, G., Elhoseny, M., & Mohan, A. (2021). Joint Encryption and Compression-Based Watermarking Technique for Security of Digital Documents. *ACM Transactions on Internet Technology*, 21(1), 1–20. doi:10.1145/3414474
- Taha, A. H. (2020). A high capacity algorithm for information hiding in Arabic text. *Journal of King Saud University-Computer and Information Sciences*, 658-665.
- Takaoğlu, M. Ö., Özyavaş, A., Ajlouni, N., Alshahrani, A., & Alkasasbeh, B. (2021). A Novel and Robust Hybrid Blockchain and Steganography Scheme. *Applied Sciences (Basel, Switzerland)*, 11(22), 19. doi:10.3390/app112210698
- Thota, C. S. (2018). Centralized fog computing security platform for IoT and cloud in healthcare system. *Fog computing: Breakthroughs in research and practice*. IGI Global.
- Vijayakumar, V. P., Priyan, M. K., Ushadevi, G., Varatharajan, R., Manogaran, G., & Tarare, P. V. (2019). E-health cloud security using timing enabled proxy re-encryption. *Mobile Networks and Applications*, 24(3), 1034–1045. doi:10.1007/s11036-018-1060-9
- Wang, K. Y. (2021). A Coverless Text Steganography by Encoding the Chinese Characters' Component Structures. [IJDCF]. *International Journal of Digital Crime and Forensics*, 1–17.
- Wu, J. M.-T., Srivastava, G., Lin, J. C.-W., & Teng, Q. (2021). A Multi-Threshold Ant Colony System-Based Sanitization Model in Shared Medical Environments. *ACM Transactions on Internet Technology*, 21(2), 1–26. doi:10.1145/3408296
- Xiang, L., Wu, W., Li, X., & Yang, C. (2018). A linguistic steganography based on word indexing compression and candidate selection. *Multimed. Tools Appl.*, 28969–28989.
- Yadav, V. K. (2015). A novel approach of bulk data hiding using text steganography. *Procedia Computer Science*, 1401–1410.
- Yang, Z. W. (2018). TS-CNN: Text steganalysis from semantic space based on convolutional neural network. *arXiv preprint*.
- Yang, Z. W., Wang, K., Li, J., Huang, Y., & Zhang, Y.-J. (2019). TS-RNN: Text steganalysis based on recurrent neural networks. *IEEE Signal Processing Letters*, 26(12), 1743–1747. doi:10.1109/LSP.2019.2920452
- Yang, Z. Z. (2018). Rits: Real-time interactive text steganography based on automatic dialogue model. *In International Conference on Cloud Computing and Security*, (pp. 253-264). doi:10.1007/978-3-030-00012-7_24

R. Gurunath is employed as an assistant professor in the department of Computer Applications at the Dayananda Sagar College of Arts, Science, and Commerce in Kumaraswamy Layout, Bangalore-78. He is also the college's IQAC Coordinator. He is currently doing his PhD at Christ University Bangalore. His research focuses on information security and information concealment. He has rich experience in teaching, administration and research. He has lectured on interesting subjects including "network security and cryptography", Internet technologies, data communication and networks, mobile computing, network programming, cyber security, and current programming languages. He has made a habit of obtaining certificates in his field of study, for which he has been recognized nationally as a "NPTEL Discipline Star". He authored a work related to COVID during the COVID-19 period, and his name was included to the WHO database. He is currently a reviewer for IGI-Global, a journal organization. He has coordinated events for the institution that deal with intellectual property rights, research methodology, funding for research, extension activities, international conferences, ISR activities, and on numerous other topics. He has published 17 research publications in journals and conferences with renowned publishers as IEEE Access, IEEE Xplore, Springer Link, Taylor & Francis, IOPScience, Scrivener Publishing LLC and others. In conjunction with universities in India and abroad, he has written articles, some of which were financed initiatives. He has authored an operating system book for the VTU Engineering curriculum.

Debabrata Samanta is presently working as an Assistant Professor, at the Department of Computational Information Technology, Rochester Institute of Technology, Kosovo, Europe. He obtained his Ph.D. in Computer Science and Engg. from the National Institute of Technology, Durgapur, India, in the area of SAR Image Processing. He is keenly interested in Interdisciplinary Research & Development and has experience spanning fields of SAR Image Analysis, Video surveillance, a Heuristic algorithm for Image Classification, Deep Learning Framework for Detection and Classification, Blockchain, Statistical Modelling, Wireless Adhoc Networks, Natural Language Processing. He has successfully completed six Consultancy Projects. He has received funding of 8,110 USD under Open Access, Publication fund. He has received funding under International Travel Support Scheme in 2019 for attending the conference in Thailand. He has received Travel Grant to speaker at conferences, seminars, etc for two years from July 2019. He is the owner of 22 Patents (4 Design Indian Patents and 2 Australian patents Granted, 16 Indian Patents published) and 2 copyright. He has authored and co-authored over 217 research papers in an international journal (SCI/SCIE/ESCI/Scopus) and conferences including IEEE, Springer, and Elsevier Conference proceedings. He received "Scholastic Award" at the 2nd International Conference on Computer Science and IT application, CSIT-2011, Delhi, India. He is a co-author of 13 books and the co-editor of 12 books, available for sale on Amazon and Flipkart. He has presented various papers at international conferences and received Best Paper awards. He has the author and co-authors of 08 Book Chapters. He also serves as acquisition editor for Springer, Wiley, CRC, Scrivener Publishing LLC, Beverly, USA., and Elsevier. He is IEEE Senior Member, an Associate Life Member of the Computer Society of India (CSI), and a Life Member of the Indian Society for Technical Education (ISTE). He is a Convener, Keynote speaker, Session chair, Co-chair, Publicity chair, Publication chair, Advisory Board, and Technical Program Committee member in many prestigious International and National conferences. He has invited speakers at several Institutions. Dr. Samanta is presently working as an Assistant Professor, at the Department of Computational Information Technology, Rochester Institute of Technology, Kosovo, Europe. He obtained his Ph.D. in Computer Science and Engg. from the National Institute of Technology, Durgapur, India, in the area of SAR Image Processing. He is keenly interested in Interdisciplinary Research & Development and has experience spanning fields of SAR Image Analysis, Video surveillance, a Heuristic algorithm for Image Classification, Deep Learning Framework for Detection and Classification, Blockchain, Statistical Modelling, Wireless Adhoc Networks, Natural Language Processing. He has successfully completed six Consultancy Projects. He has received funding of 8,110 USD under Open Access, Publication fund. He has received funding under International Travel Support Scheme in 2019 for attending the conference in Thailand. He has received Travel Grant to speaker at conferences, seminars, etc for two years from July 2019. He is the owner of 22 Patents (4 Design Indian Patents and 2 Australian patents Granted, 16 Indian Patents published) and 2 copyright. He has authored and co-authored over 217 research papers in an international journal (SCI/SCIE/ESCI/Scopus) and conferences including IEEE, Springer, and Elsevier Conference proceedings. He received "Scholastic Award" at the 2nd International Conference on Computer Science and IT application, CSIT-2011, Delhi, India. He is a co-author of 13 books and the co-editor of 12 books, available for sale on Amazon and Flipkart. He has presented various papers at international conferences and received Best Paper awards. He has the author and co-authors of 08 Book Chapters. He also serves as acquisition editor for Springer, Wiley, CRC, Scrivener Publishing LLC, Beverly, USA., and Elsevier. He is IEEE Senior Member, an Associate Life Member of the Computer Society of India (CSI), and a Life Member of the Indian Society for Technical Education (ISTE). He is a Convener, Keynote speaker, Session chair, Co-chair, Publicity chair, Publication chair, Advisory Board, and Technical Program Committee member in many prestigious International and National conferences. He has invited speakers at several Institutions.