ISSN: 2582-8118 ***Volume 3, Issue 6; Nov 2023***

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYSIS IN SCIENCE AND ENGINEERING

Web: https://www.iarj.in/index.php/ijrase/index

A Study and Reconsideration on Text-Steganography

Sanchita Ghosh
Department of Computer Science & Engineering,
Bengal College of Engineering and Technology,
Durgapur, West Bengal, India.

Rituparna Mondal
Department of Computer Applications,
Techno India University, Salt Lake,
Kolkata, West Bengal, India.

Aparajita Das
Department of Computer Science & Engineering,
Sanaka Educational Trust's Group of Institutions,
Durgapur, West Bengal, India.

Anwesa Naskar
Department of Computer Science & Engineering,
NSHM Knowledge Campus,
Durgapur, West Bengal, India.

Shirsha Mullick
Department of Computer Science and Engineering,
Techno International New Town,
Rajarhat, Kolkata, West Bengal, India.

Siddhartha Chatterjee
Department of Computer Science & Engineering,
NSHM Knowledge Campus,
Durgapur, West Bengal, India.

ABSTRACT

Steganography is a technique that hides confidential information (which we call cover) in some other data without leaving any clear proof of data manipulation. All traditional steganographic techniques have limited ability to hide information. They can hide only 10% (or less) of the cover data. Although most recent research has focused on hiding data in

images, many image solutions are more complex when applied as a cover to natural language text. Different applications are used by different requirements of well-known text steganography algorithms. We require both ultimate hidden and a huge amount of confidential data to be concealed which is defined by a shared petition. There are many approaches in steganography that try to detect statistical discrepancies in coverage in which availability of hidden information is predicted. Writings covering natural language must not only automatically collect analytical data, but also transmit it to the human reader's minds.

KEYWORDS:

Embedded, Cover, Security, Steganography, Confidential.

1. Introduction:

In today's life, the internet has played an important role in the communication and information sharing. Due to the quick improvement in Information Technology and Communication and the Internet, the secureness of the data is decreased day by day. Every day, the secret data has been accommodated and illegal raise of data has crossed the limits. A vital step should be taken to secure the data and information. Steganography combined with encryption will be a powerful and useful tool that provides high level of security [**17**].

Steganography is an art and science in which a message has to be hidden inside another message for no reason so that only the desired recipient can get the address of that message [**4,7**]. The word steganography is originally taken from the Greek words **Steganos** (Covered), and **Graptos** (Writing) [**1,9**]. In the modern sense, steganography usually refers to information or a file hidden inside a digital image, text, video or audio file [**9**]. The primary objective of this technique is not to disclose hidden data to others but to provide certainty regarding the existence of data. The significance of steganographic applications becomes apparent when integrated with a digital image. This integration serves various purposes, such as copyright protection, feature tagging, and clandestine communication. The emphasis is on ensuring the presence of data rather than revealing it, making this technique valuable for applications where data concealment and assurance are paramount [**11**]. Text steganography appears to be the most difficult type of steganography when compared to other types of steganography such as on photos, video files, audio files, and so on, due to the lack of large-scale redundancy of information in a text file. Copyright protection, feature tagging, and covert communication are just a few of the steganographic applications for digital images [**20**]. To identify an image as intellectual property, a copyright notice or watermark might be incorporated into it [**17**].

The watermark can be extracted to identify any unauthorized usage of this image. Based on character replacement of the longest common subsequence entries, this research proposes new approaches for hiding information utilizing Indian languages. This method can be used with any language, but because Indian languages have far more characters than other languages, such as English, it will be much easier to generate words or simple phrases using Indian languages. The purpose of the steganography is not to prevent people from learning the secret information, but rather to prevent others from suspecting that the information exists at all. Basically, steganography is called "Invisible" Communication [**5**].

2. Related work:

Traditional linguistics has used written text generation (sometimes with the addition of so-called "style templates") and semantically identical word alternatives to hide messages in an existing source. Wayner [**29**] proposed the use of controversial context-free grammar as a way to produce steganographic text without sacrificing artificial and terminological accuracy [**17**].

Note that the accuracy of the semantics can only be guaranteed if the verbatim grammar implements a semantically consistent text preparation. Chapman and Davida have improved the general generation of tag-correct text by artificially creating large corporations of proportional data to create grammatical "style templates". These templates were used to create text that contained not only grammatical and lexical variations, but also permanent registers and "styles" that could possibly be read by a human observer [**9**]. Chapman et al later discovered a method that developed well-known plastics as a literally equivalent alternative to encoding messages. As mentioned in Atallah et. al for-watermarking schemes, concealment of driving information specifically is a recent innovation. Wayner is based on a clear text that is accurately numerical in nature. Watermarking is concerned with hiding information in cover media such that the hidden data are robust to alterations and adjustments.

Practically, steganography and cryptography are two techniques of secure transmission over the Internet. Cryptography scrambles a message to conceal its contents; steganography conceals the existence of secret message [**23**]. Mostly, however, the linguistic style of steganography is comparatively restricted. Tongue damage is relatively easy to detect. It doesn't take much to edit a text to allow the local speaker to decide to be non-collective. Furthermore, even artificial and grammatical writings can interrupt spiritual barriers [**9**]. Some general categories of related work are given below:

Spatial Domain Technique: In spatial domain steganography method, for hiding the data some bits are directly changed in the image pixel values. Most used method in this category is least significant bit [**22**].

Transform Domain Based Technique: These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in transform domain is widely used for robust watermarking [**22**].

LSB (Least Significant Bit) Embedding: Reconsideration techniques that involve modifying the least significant bits of characters in the text to embed information. LSB embedding is a common and relatively simple method used in text steganography [**15,21**].

Vector Embedding: Utilizing a vector embedding approach, this method employs a robust algorithm conforming to codec standards such as MPEG-1 and MPEG-2. The process involves embedding audio information into pixels of frames within a host video, leveraging the H.264/AVC Video coding standard. The algorithm incorporates a motion vector component feature for embedding control, serving as the clandestine carrier for the information. Importantly, the embedded data is designed not to noticeably impact the visual and statistical invisibility of the video sequence [**22**].

Machine Learning Based Approaches: Investigate research that incorporates machine learning algorithms for text steganography. This could involve using models to automatically generate steganographic content or detect hidden information [**24**].

Masking and Filtering: This technique conceals data through image marking, making it particularly useful when watermarks seamlessly blend into the image. Instead of concealing data in the noisy portions, it strategically embeds information in the more prominent regions of the image. The watermarking process is seamlessly integrated into the image, allowing application without concern for image degradation. This approach is applicable to both 24-bit and grayscale images [**22**].

Encryption and Number System Based Approaches: In this paper, a novel scheme is proposed for the concealment of secret messages through the implementation of a sophisticated model based on the number system. The proposed method involves skillfully embedding the secret message within the numerical framework, ensuring a covert and secure means of communication. Here the recipient in this context possesses exclusive knowledge of the secret message, the concealment method, and the procedure for extracting the information. Meanwhile, the sender is also well-informed about the encoding technique employed and understands how it is applied to discreetly embed the secret message within the text [**11,25**].

3. Classification of Steganography:

Recently, the use of Internet has grown exponentially. One of the major areas that attract people is security, which is subject to the Internet, in which communication is targeted. Now a day the most popular technique for hiding data for security purposes is to get better consciousness than encryption. For this reasons encryption decryption is more concern than hiding a data technique. Various methods are used to communicate secretly, including encryption, coding, etc. Steganography is a system of hiding data within each other's data; in this manner nobody else is aware of its presence. This is an important advantage of steganography in comparison to another coding system. Maximum techniques of steganography work on text, image, audio, video, etc. So, there are four main types of steganography [**1,4**].

3.1. Text–Steganography: Text - Steganography is the topmost complex type of steganography. This is due to the absence of additional information in the text file, while the image or sound file has too much redundancy [**1,2**].

3.2. Image –Steganography: In Image Steganography, the confidential information like text, picture or video is hidden inside a cover figure. This type of technique uses pixel strength to conceal messages [**12,13**]. Any image steganography system has four essential properties: robustness, capacity, imperceptibility, and security to test its effectiveness [**24**].

3.3. Audio/Sound–Steganography: Sound steganography is a technology that modifies an audio stream in an undetectable way in order to deliver secret information. It is the technology of enclosing audio or secret text in a host message. The features of the host message prior to steganography and the stego message following steganography are identical. It is also very robust in nature but with limitation of the amount of data one can

hide. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography [**22**]. The different technology of audio steganography is: (i) Spread Spectrum [**23**]. (ii) Low Bit Encoding and [**12**] (iii) Phase Coding [**13,20**].

3.4. Video–Steganography: Video steganography is a method for concealing files or other data in digital video formats. Video, which is a collection of visuals, is utilized as a vehicle for printed text [**20**]. The information that is accessible to the human eye in each picture in the movie is hidden using a discrete cosine transformation (DCT), which typically has a value between 6.668 and 7. Have none at all. Video steganography employs AVI, MPEG, H.264, and other video formats [**13,14**].

We explain individual types of Text-Steganography and compare it. Fig.1 shows various techniques of text steganography.

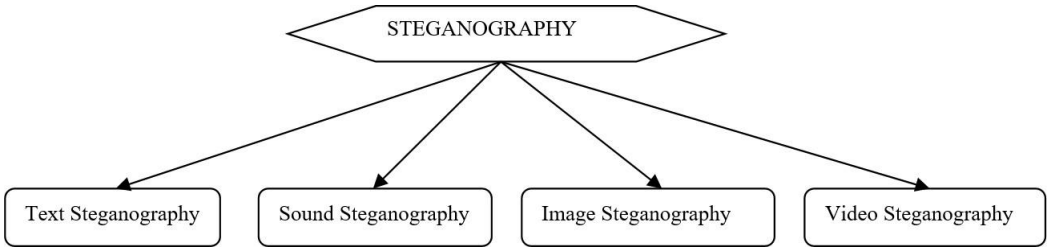

Fig.1: Classification of Text Steganography

4. Concept of Text Steganography:

Depending on the cover media used to implant hidden data, steganography can be categorized as picture, text, audio, or video steganography. Text steganography can range from modifying the formatting of an existing text to changing the words inside a text to creating a new text. To generate understandable writings, random character sequences or context-free grammars are used [**14**].

Due to the lack of redundant information found in image, audio, or video files, text steganography is thought to be the most difficult. The structure of text documents is identical to what we see, whereas the structure of other sorts of documents, such as pictures, is distinct from what we see. As a result, we can conceal information in such papers by altering the structure of the document without affecting the output. The message was then sent securely without any doubt [**15**].

An image or an audio file can be altered in ways that are undetectable; however, a casual reader can mark a text file with an extra letter or punctuation. Text files require less memory to store, and they are faster and easier to communicate than other forms of steganographic technologies.

Text steganography can be divided into three categories: Linguistic approaches, format-based random and statistical generation [**3,7**]. Fig. 2 shows the mechanism of text steganography.

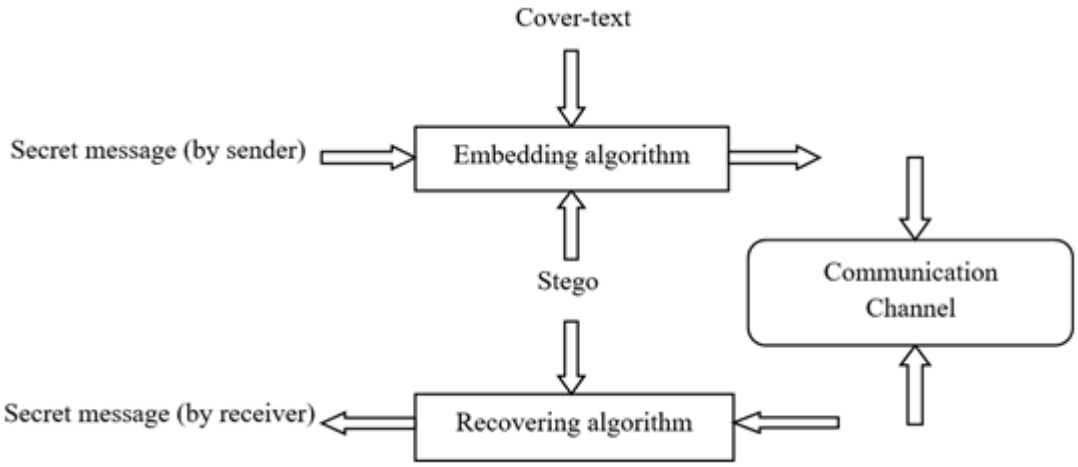

Fig.2: The Mechanism of Text Steganography

5. Several Techniques of Text Steganography:

5.1 Word Spelling:

We use this process to hide information in English language. In these processes, Word Spelling in American (US) language is explained different from British language (UK). To give an example: Organize have other spellings in UK (Organize) and US (Organize). This process is suitable for a field where both US & UK terms are rarely used. In this process, if one does not know the method of both, but easily detects, then our data is hidden [**2**].

There is a slight difference between the spelling word of American and British language, like in American language (Color) and in British language (Colour), small changes of "u" only, which becomes easy to detect. New Synonym Text technique is higher confidential process than this technique, since in New Synonym technique we use various words like (Soccer) in American language and (Football) in British language. It is clear that those who use the two words synonymously cannot easily understand [**28**].

5.2 Semantic Method:

This process is same as the word spelling process. Though the small variation is that, in this technique, we can use words that are synonymous with words, which are why special words are used, which hides the information in the text [**15**]. This is also secure data (OCR) in case of applying or using the identification program. We have a lot of advantages out there. So, a most confident technique is needed, because if anyone has a lot of orders or commands in their language, they can easily detect the hidden data [**2**].

5.3 Line Shifting Method:

In this technique, the text lines are moved to other extent (such as each and every line moves 1/300 inch up and down) and by discovering an identical form of text the information is get hidden [**14**].

This distance measuring device and the mandatory modification will be initiated to eliminate the information which is hidden. Additionally, if Character Recognition Program (OCR) is used, the printed data is damaged. This technique is beneficial for hard copy of text, as OCR is not used on printed tests [**2**].

5.4. Abbreviation:

Another way to hide information in the text is to use shorthand steganography. In this process, very less data is hidden in the text, specifically; only a few amounts of information can be hidden in the text. We can conceal very small amount of secret information in hundreds of lines. This technique is extensively used in poems to hide figures, by defining other meanings of a word, etc [**2**].

5.5 Word Shifting Method:

In this technique, the confidential message is hidden by converting the words horizontally, so that the right or the right do not represent a slight 0 and 1, respectively, and in the text the data is hide by changing the distance between the words. This practice is suitable for texts where the spacing between words is not the same. This process can be underestimated, as it is common to change the spacing between words to fill in the line. But if anyone knows about algorithms related to word shifting method, easily get hidden data [**2**].

5.6 Syntactic Process:

In this process, by changing some punctuation marks like comma (,), full stop (.), semi colon (;), quotes (“) in appropriate position, anyone can conceal data in a text file. The requirements of this process are the identification of appropriate places or endowments.

The advantage of this method is that there is almost no amount of information to secure the data. For example: In any poem or paragraph we identify full stop (.) as 0 and comma (,) as 1for securing data in it and sending it to the users [**2,26**].

5.7 New Synonym Text Method:

In the process, some words with their synonyms are used to secure the secret message in the text file. In the word spelling method, the spelling changes very little but in the new synonymous technique, various types of words are used for the same number. Some words in English have different terms in the United States (US) and the United Kingdom (UK). For e.g., “Movie” has other term in UK as (Flim) and in US as (Movie).

This process is more useful than the method of spelling the word, because this technique has various types of words, which are not easily understood [**2**]. In the spelling technique, different types of spelling words are used like in US (faculty) and in UK (staff).

The disadvantage of this method is that it takes a little time because we have to search synonyms of words and replace it until we get the appropriate results [**27**]. Fig. 3 shows several techniques of hiding message.

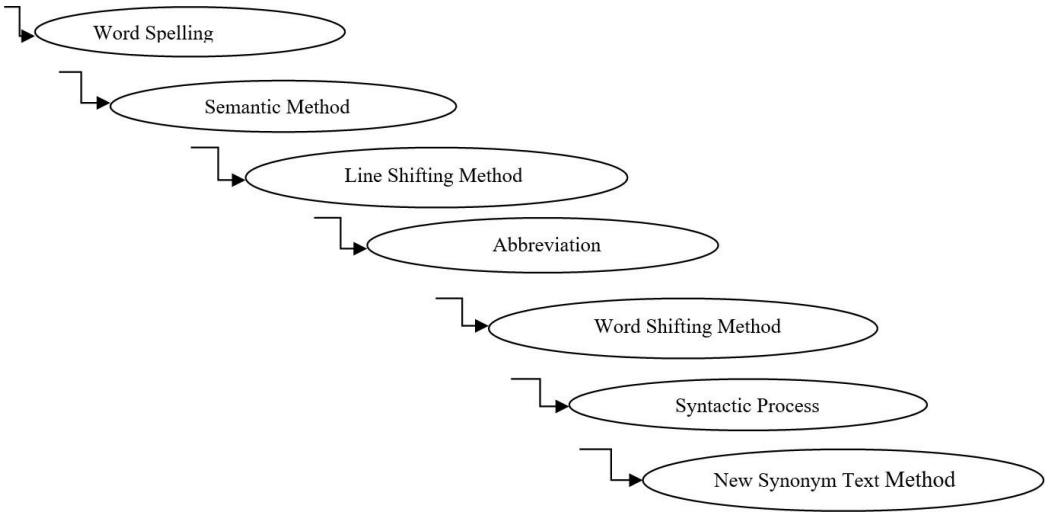

Fig.3: Several Techniques of Hiding Message

6. Hiding Text Mechanism:

Since everyone can read, encrypting text in impartial sentences is unlikely to be effective. In the previous sentence if you take the first letter of each word, you will see that it is not impossible and very easy.

There are many ways to secure information in text file. The first letter algorithm used here is very insecure, because the knowledge of the system used automatically reveals the secret to you. The downside is that there are many common techniques to keep secrets within plain text [**9,10**].

Many techniques include rules such as modifying the order of a text, using every ninth character, or changing the amount of white space after lines or between words. Successfully, the last technique was used and even after printing and copying a text on paper ten times, the encrypted message can be retrieved [**9**].

Another efficient way to encrypt a text is to use a publicly available cover source, book, or newspaper, and use code that contains, for example, a line number, a page number, and a letter and include number.

In this way, no information hidden inside the server will lead to a hidden message. Discovering it depends entirely on gaining knowledge of the secret key.

Focused on the embedding method employed to obscure sensitive information within the cover text [**19**]. There are three basics categories of text steganography that are format-based methods, random and statistical generation and linguistic methods [**6,8**].

6.1. Format-Based Methods:

Physical formatting of text in format-based ways is used as a place to conceal data. Format-based techniques [**18**] usually edit existing text to conceal the steganographic text [**16**]. A format-based text steganography method is also known as open space method [**30**].

Interacting spaces or invisible characters, deliberately spelling out the entire distribution of text, and resizing fonts are some of the many formatting techniques used in text steganography.

Some of these processes, such as deliberate misspellings and spacing, can sometimes fool human readers who ignore misinterpretations, but can often be easily detected by a machine [**10,11**].

6.2. Random and Statistical Methods:

To avoid comparing it with a well-known plain text, stenographers always support to preparing their own cover texts. Although this often solves the problem of attacking a known core, the features of the prepared text can still raise suspicions that the text is illegal.

Such a generation usually attempts to mimic some feature of the general text by approaching some statistical divisions found in the original text [**16**].

Text can hide information from stenography to a point of view that randomly shows a series of characters. Of course, this setting is far from random for both the sender and the recipient of the message, but it must be random for everyone who intercepts the message [**10**].

However, not only should it be known randomly, but since we are also concerned with the fact that it is a stenographic phrase, it does not look suspicious. Random sets of characters that all fall into the same set of character but have no clear meaning can really raise a warning [**9,10**].

6.3. Linguistic Methods:

Actual, original dictionary items can be used to encode one or more bits of information in each word to solve the problem of identifying non-literal continuity [**16**].

This may include a map codebook between lexical objects and bit configurations, or words (lengths, letters, etc.) encoding hidden information. However, there is trouble in both. A string of words that have no semantic diagram, and no comprehensible semantic connection. Both humans and computers can know the same thing [**10**].

This method needs proper identification of places where the signs can be inserted. Another linguistic steganography method is semantic method. In this method the synonym of words for some pre-selected are used. The words are replaced by their synonyms to hide information in it [**18**]. Fig. 4 shows the classification of text steganography.

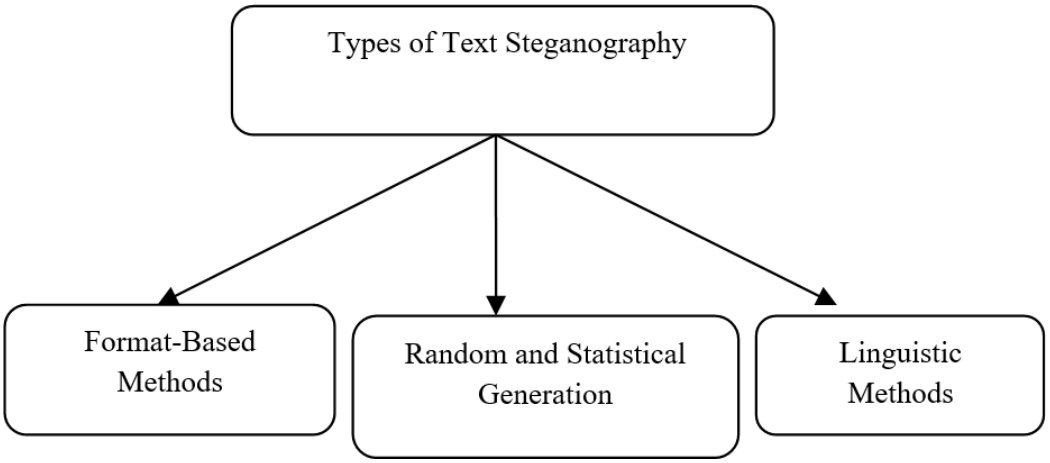

Fig.4: Types of Text Steganography

7. Comparison Study:

Table.1: Table shows the Comparison between the various techniques of Text Steganography

Features	Format Based methods	Random and Statistical Generation	Linguistic Method
Uses	The physical formatting oftext is used as a space to hide information in this process [16].	These methods are used to automatically produce cover text based on statistical properties of language [9].	The aim of this method is to conceal knowledge in natural language text. Synonym substitution is one of the most important transformations in linguistic steganography [9].
Based on	UniSpach is a format-oriented approach based onspace character manipulation that is recommended for text steganography in MicrosoftWord documents that use Unicode Space Characters [19].	Random and statistical generation is based on character sequences and words sequences [18,19].	To secure the secret message, the linguistic approach based on a data compression technique [8,9].
Goal	The aim of this approach isto create a copy protection technique with a large capacity for cover objects [8].	The aim of this approach is to increase cover object capability in order to reduce communication costs [10].	The aim of this approach is to have a high embedding ability while also increasing the protection of the embedded secret message and minimize the transmission costs [10].

8. Conclusion:

Due to its large circulation on the Internet today, text staging has a clear expectation. Finally, at last we decide that, using the proposed algorithm, we can increment the accommodation of the covered material by a fixed length compared to the existing algorithm. In addition to covert communication, this process can also be used to prevent invalid repetition and to allocate text, especially in electronic text.

Besides being used in electronic writing, this method can also be appealed to photocopy documents. For this purpose, after hiding the data in it, we print the documents. To extract data from a photocopy document, we identify it and hide the embedded or attached data from the computer. In future, work should focus on improving the robustness of decoding algorithms. Because of this, the secured data will be deleted after deleting the spaces with word processing software.

9. Future Scope:

Concealing data within text holds diverse applications, ranging from copyright verification and authentication to annotation. Incorporating copyright information directly into the text serves as a strategy for safeguarding intellectual property, particularly in the face of the escalating prevalence of electronic distribution. The integration of annotation within the text can play a role in tamper protection. For instance, encoding a cryptographic hash of a document into the text enables straightforward verification of its integrity–a quick assessment of whether the file has undergone any alterations. Verification tasks, such as authenticity checks, can be efficiently delegated to a server. In such a scenario, the server would respond with a determination of "authentic" or "unauthentic" based on the verification outcome. Text-based steganography finds an intriguing application in the reconstruction of printed documents. This practice becomes vital in scenarios where a document is physically damaged, as the loss of critical information is inevitable. Extracting data from the damaged section and using it to reconstruct the document becomes an effective strategy for recovering the lost information. Beyond document reconstruction, data hiding in text extends to embedding instructions for autonomous programs. For instance, an email server can be programmed to inspect electronic messages for concealed instructions. The server may then decide whether to accept or reject the message based on the presence or absence of hidden data. This approach empowers organizations with mail servers to prevent the inadvertent export of confidential documents, thus ensuring the security of sensitive information. The multifaceted applications of data hidden in text underscore its significance in addressing various challenges related to information security, integrity, and confidentiality.

References:

1. Rani, N., & Chaudhary, J. (2013). Text steganography techniques: A review. *International Journal of Engineering Trends and Technology (IJETT)*, *4*(7), 3013-3015.
2. TITS, B. Text-Steganography: Review Study & Comparative Analysis.
3. Chaudhary, S., Dave, M., & Sanghi, A. (2016, August). Text steganography based on feature coding method. In *Proceedings of the International Conference on Advances in*

Information Communication Technology & Computing (pp. 1-4).
4. Bhattacharyya, D., Das, P., Mukherjee, S., Ganguly, D., Bandyopadhyay, S. K., & Kim, T. H. (2009). A secured technique for image data hiding. In *Advances in Security Technology: International Conference, SecTech 2008, and Its Special Sessions, Sanya, Hainan Island, China, December 13-15, 2008. Revised Selected Papers* (pp. 151-159). Springer Berlin Heidelberg.
5. S.Gupta and R.Jain,"An innovative method of Text Steganography,"2015 Third International Conference on Image information Processing (ICIIP), Waknaghat, India, 2015, pp. 60-64.
6. R.B.Krishnan, P.K.Thandra and M.S.Baba,"An overview of text steganography,"2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, 2017, pp.-1-6.
7. M.Saritha, V.M.khadabadi and M.Sushravya,"Image and text steganography with cryptography using MATLAB,"2016 International Conference on Signal processing, Communication, Power and Embedded system (SCOPES).
8. K.F.Rafat, "Enhanced text steganography in SMS," 2009 2nd international Conference on Computer, Control and Communication, Karachi, Pakistan, 2009, pp. 1-6.
9. Dr.Nidhal K.El Abbadi, Kufa University, IRAQ, New Algorithm for Text in Text Steganography, January, 2008.
10. Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M.K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.
11. Mandal, K. K., Chatterjee, S., Chakraborty, A., Mondal, S., & Samanta, S. (2020). Applying encryption algorithm on text steganography based on number system. In *Computational Advancement in Communication Circuits and Systems: Proceedings of ICCACCS 2018* (pp. 255-266). Springer Singapore.
12. Paul, T., Ghosh, S., & Majumder, A. (2022). A study and review on image steganography. In *Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021* (pp. 523-531). Springer Singapore.
13. Biradar, R. L., & Umashetty, A. (2016). A survey paper on steganography techniques. *High Impact Factor*, *9*(1), 721-722.
14. Singh, H., Singh, P. K., & Saroha, K. (2009, February). A survey on text based steganography. In *Proceedings of the 3rd National Conference* (Vol. 3, No. 3, pp. 332-335). Bharati Vidyapeeth's Institute of Computer Applications and Management.
15. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Digital image steganography: Survey and analysis of current methods. *Signal. Process.* **2010**, *90*, 727–752.
16. Choudry, K. N., & Wanjari, A. (2015). A survey paper on video steganography. *International Journal of Computer Science and Information Technologies*, *6*(3), 2335-2338.
17. Narayana, V. L., & Kumar, N. A. (2018). Different techniques for hiding the text information using text steganography techniques: A survey. *Ingénierie des Systèmes d'Information*, *23*(6).
18. Bhattacharyya, S. (2011). A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. *Journal of global research in computer science*, *2*(4).
19. Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., Roslan, N. A., & Din, R. (2021). A comparative analysis of Arabic text steganography. *Applied Sciences*, *11*(15), 6851.
20. Fkirin, A., Attiya, G., & El-Sayed, A. (2016). Steganography literature survey, classification and comparative study. *Communications on Applied Electronics*, *5*(10), 13-22.

21. Kaur, N., & Behal, S. (2014). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International journal of engineering trends and technology*, *11*(8), 388-392.
22. Arya, A., & Soni, S. (2018). A literature review on various recent steganography techniques. *International Journal on Future Revolution in Computer Science & Communication Engineering*, *4*(1), 143-149.
23. Ahvanooey, M. T., Li, Q., Hou, J., Mazraeh, H. D., & Zhang, J. (2018). AITSteg: An innovative text steganography technique for hidden transmission of text message via social media. *IEEE Access*, *6*, 65981-65995.
24. Al Hussien, S. S., Mohamed, M. S., & Hafez, E. H. (2021). Coverless image steganography based on optical mark recognition and machine learning. *IEEE Access*, *9*, 16522-16531.
25. S. Koley, K.K. Mandal, A novel approach of secret message passing through text steganography, in International Conference on "Signal Processing, Communication, Power and Embedded System (SCOPES—2016)", Issue—III, 3–5 Oct 2016, pp. 21–26. 978-1-5090-46201/16/$31.00 ©2016 IEEE, ISBN CPF16H12-PRT/978-1-5090-4619-5.
26. Bennett, K. (2004). Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text. *CERIAS Tech Report 2004-13*.
27. Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2008, August). A new synonym text steganography. In *2008 international conference on intelligent information hiding and multimedia signal processing* (pp. 1524-1526). IEEE.
28. Shirali-Shahreza, M. (2008, February). Text steganography by changing words spelling. In *2008 10th international conference on advanced communication technology* (Vol. 3, pp. 1912-1913). IEEE.
29. Peter Wayner. "Disappearing Cryptography: Information Hiding: Steganography and Watermarking", Morgan Kaufmann, 2nd edition edition, 2002.
30. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.