ANALYSIS OF STENOGRAPHY TECHNIQUES

Sandeep Kaur[1], Dr. Ashwani Sethi[2]
[1]Research Scholar, [2]Professor
[1,2] Department of Computer Science & Engineering
[1,2] Guru Kashi University, Talwandi Sabo

Abstract

Stenography techniques, integral to rapid transcription and information encoding across sectors like judiciary, journalism, and healthcare, have evolved significantly from traditional shorthand systems to modern digital solutions. Ransacking for just the right article is foremost preferred and is sort of challenging to look out to support the current requirements. With the advancement in technology day by day, the occurrence of hacking is increasing very often. In these modern times, the area of cybersecurity is in desperate need of prevention from hacking. Gone are those days when firewalls were handy to protect your data. We are required to try to do this individually to prevent cybercrime. According to Kaspersky Labs, a cyber-breach typically costs $1.23 million. This document aims to provide the most straightforward methods for aiding in data security through concealment. Because of frequent hacking and common weaknesses, data security has grown to be a critical concern. There are numerous methods for encapsulating and hiding data. Data protection techniques include steganography and cryptography. Stenography continues to progress in the face of a digitally driven information ecosystem, with challenges such as standardizing notation and incorporating AI into transcribing operations solved.

Keywords: *Stenography, Techniques, Hacking, Data Hiding, Cybersecurity*

1.INTRODUCTION

Information management in a variety of disciplines has relied on stenography, a profession that includes the quick transcription of spoken language into shorthand or coded form, for millennia. Its beginnings can be traced to the ancient era, when scribes used symbols and abbreviations to efficiently record talks and conversations. The demand for precise and quick documentation has grown throughout the ages, especially in places like newsrooms, legislative assemblies, and courts where exact reporting is essential. This has led to the evolution of stenography. In the history of stenography, the creation of formal shorthand systems during the 19th and 20th centuries—particularly those created by Isaac Pitman and John Robert Gregg—marked a critical turning point.

These techniques established systematic ways to encode spoken language by syllables or phonetically, enabling proficient transcriptionists to attain astonishing transcribe speeds without sacrificing accuracy. Statoscopes have become essential in court cases, journalism, and other fields where quick information gathering and distribution are required in this day and age.

Digital technologies have revolutionized the stenography environment in recent decades. With the integration of speech recognition algorithms and advanced data processing capabilities, modern stenographic devices and software have significantly expedited the transcribing process. The speed and accuracy of transcription have increased thanks to these developments, which have also allowed stenography to be used in new fields like accessibility services, live captioning, and subtitling. Even in this day and age of digital communication and information technology, stenography is still relevant because of its ongoing evolution. The analysis of stenographic techniques today takes a wide range of factors into account, such as how well shorthand systems adjust to various languages and dialects, how artificial intelligence is incorporated to enhance transcription accuracy, and how training methodologies are continuously developed to guarantee competency in both traditional and digital stenography. Proficiency in these dynamics is essential for practitioners looking for dependable and effective ways to record and preserve spoken language in real-time scenarios.

2. REVIEW OF LITREATURE

Al-Harbi et al. (2020) examine the security implications of steganography based on DNA. This type of steganography uses DNA sequences' tremendous capacity and biological complexity to conceal information. In comparison to conventional steganographic techniques, DNA-based methods are deemed more robust and imperceptible by the researchers, who offer a thorough study of the numerous strategies employed in this field. According to their research, DNA steganography offers a viable method for secure communication by using the special and complex characteristics of DNA sequences to encrypt messages in a way that is difficult to decipher without the use of complex algorithms or specialized biological knowledge.

Alyousuf and Din (2020) give a thorough analysis of word-rule and feature-based text steganography techniques. In order to insert concealed messages, feature-based approaches modify particular language elements like punctuation, font styles, or letter locations. Conversely, word-rule based methods encode information using pre-established rules and patterns found in the text. The authors discuss the advantages and disadvantages of each strategy, pointing out that whereas feature-based strategies can be more subtle and have larger payload capacities, they frequently call for more complicated algorithms and may be more easily discovered through statistical analysis. On the other hand, word-rule based solutions may have less capacity and flexibility but tend to be more straightforward and reliable. The significance of striking a balance between imperceptibility, capacity, and security in text steganography is highlighted by this review.

Dhawan and Gupta (2021) provide an overview of the several steganography data security strategies, encompassing a broad spectrum of approaches and media. The survey groups techniques according to how they are used in steganography—text, image, audio, and video. The writers offer a thorough evaluation of the advantages and disadvantages of each method, taking into account elements like robustness, security, capacity, and imperceptibility. The report emphasizes how steganography is constantly changing and how new developments are required to meet new security issues. To improve overall data security, the authors advocate for integrated approaches that incorporate a variety of strategies.

Din and Qasim (2019) Examine several steganographic analysis methods for use with image and audio files. The paper offers a thorough analysis of the techniques used to find hidden information in various kinds of media. The efficiency of several techniques, including statistical analysis, machine learning, and signal processing, in identifying steganographic content is explored. The authors draw attention to the difficulties posed by each approach, especially with regard to computational complexity and accuracy. The research highlights the necessity for sophisticated analytical tools to properly detect hidden data due to the growing sophistication of steganographic techniques.

Frank (2024) gives a summary of modern steganographic methods that are specifically used with text data. The study describes how several approaches—such as linguistic, format-based, and semantic techniques—embed hidden information into textual content and classifies them. The trade-offs between detectability, payload capacity, and complexity are highlighted by Frank. Format-based strategies work with the appearance of the text, whereas linguistic techniques concentrate on changing the grammatical structure without impacting the meaning. Through subtle meaning modifications, semantic approaches incorporate information. The paper emphasises the significance of creating strategies that are invisible and resistant to detection, highlighting developments in these approaches and their consequences for secure communication.

3. METHODOLOGY

This section covers an image-concealing technique that stores our message in an image file. The main goal is to employ steganography to increase security while requiring less storage at the same time. The program generates two canvases: one with an uploaded image and the other with user-entered text of the same size. Then, it looks at each pixel in the text canvas, and if it finds black, it knows that pixel is also a part of the message. It will locate the pixel at the exact location on your image canvas and make sure that the RGB's green value finishes in an extremely high seven. If it detects white or transparent, it can verify that the pixel in question on your image canvas is not on the text entered and that its green value does not terminate in 7. After doing this to the entire image, we obtain a picture in which, aside from the places where it would spell a message, every pixel's green value ends during a 7. By using the pixels of the uploaded image, the decode function reverses the foregoing process by hiding every pixel where it finds no green value, terminating at 7.

This type is quite easy to use. The user must type a message into a text field in the first step. The user then needs to upload an image from his system after entering that message. The text and the image overlap as soon as the image is uploaded, leaving us only able to see the image. The text and image have the same dimensions, meaning that only the image is visible because their width and height are equal. We refer to this stage as the encryption phase. The user must then download this image. The user can decrypt the downloaded file to view the concealed message. The user must upload the downloaded image for it to be decrypted; after it has, the output will show the message that was input.

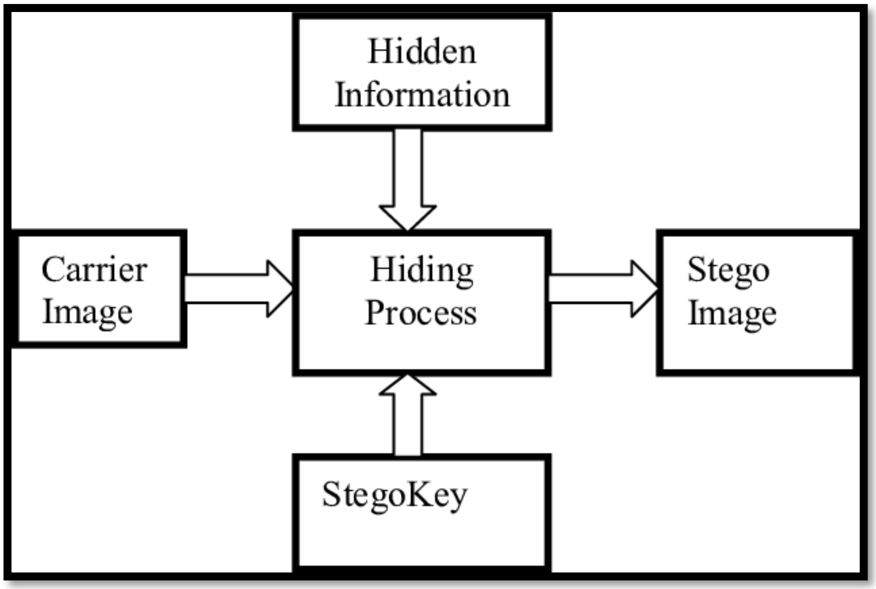


Figure 1: Process of Image Steganography

4. IMPLEMENTATION AND RESULT

The diagram that follows makes it easy to understand how we did things:

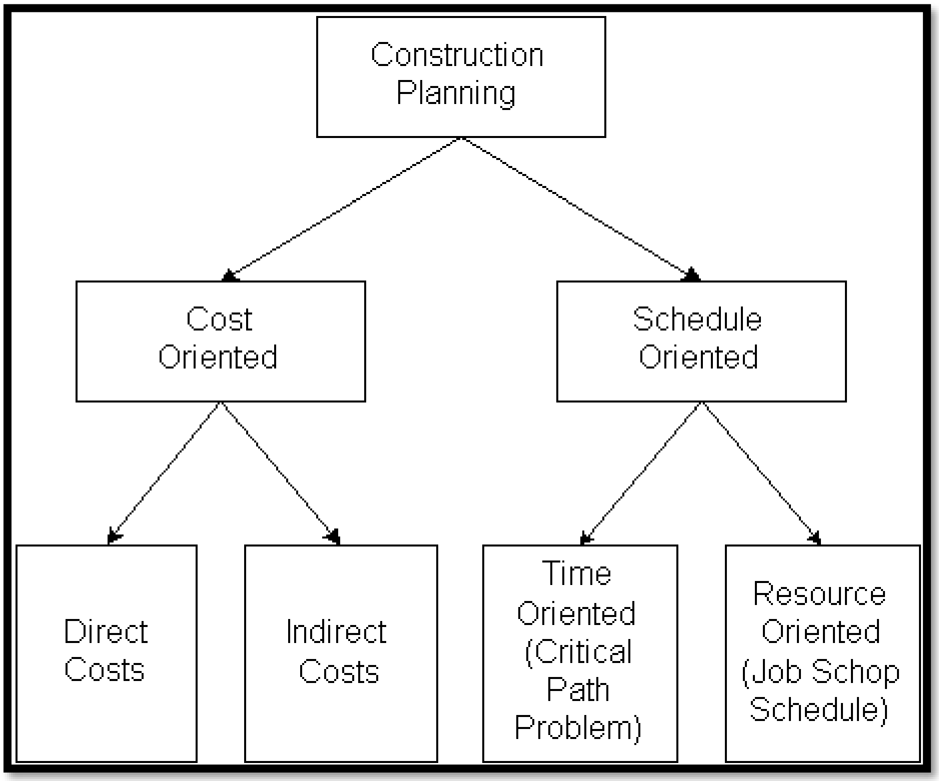
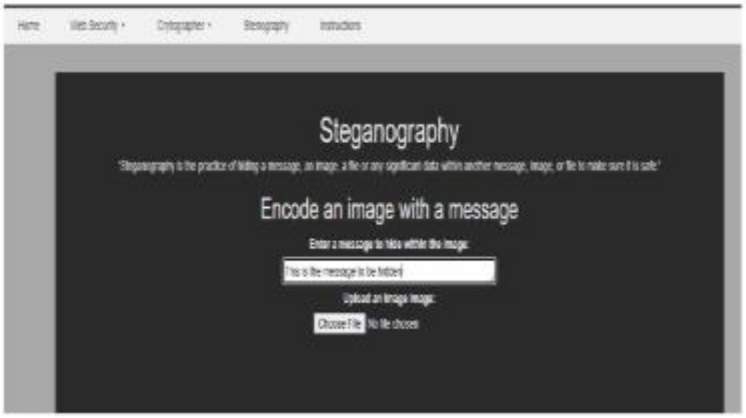


Figure 2: Working of the Project

The actions that must be taken are as follows:

Enter your message: -

The user must type the message they wish to hide in the text area that appears.



Steganography

"Steganography is the practice of hiding a message, an image, a file or any significant data within another message, image, or file to make sure it is safe"

Encode an image with a message

Enter a message to hide within the image:

This is the message to be hidden

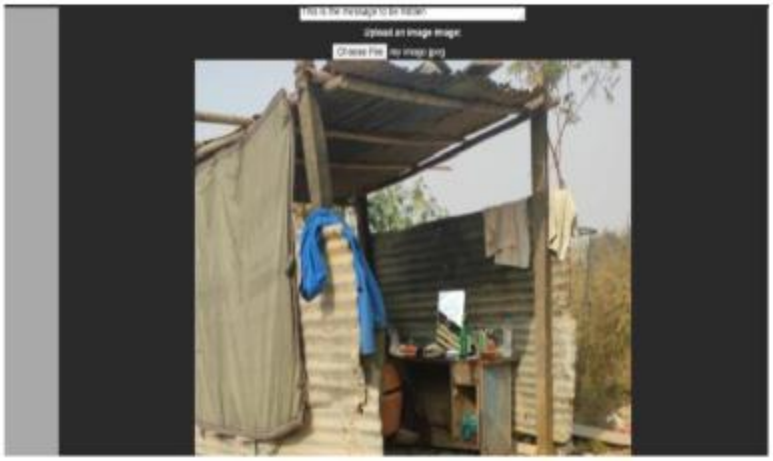
Upload an image image:

No file chosen

Figure 3: This is the message to be hidden" was written in the text field.

Upload your image: -

The next step is to upload an image to carry out encryption after typing the text.



This is the message to be hidden

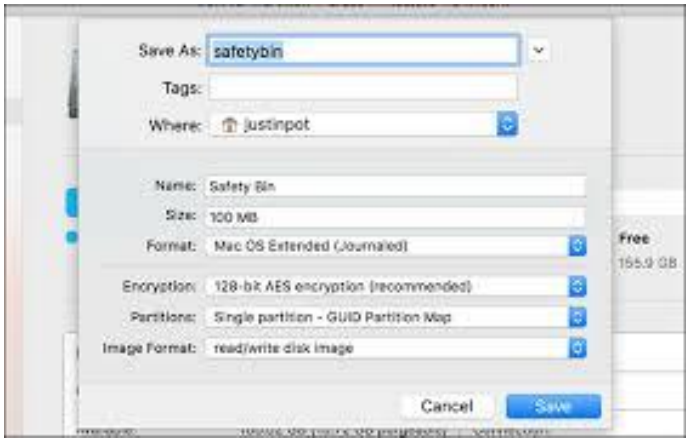
Upload an image image:

my image.jpeg

Figure 4: Picture uploaded: "my image.jpeg"

Download the encrypted image

After the picture is uploaded, the text and the picture overlap and have the same height and width. The encrypted image must then be downloaded by the user.



Save As: safetybin

Tags:

Where: justinpot

Name: Safety Bin

Size: 100 MB

Format: Mac OS Extended (Journaled)

Encryption: 128-bit AES encryption (recommended)

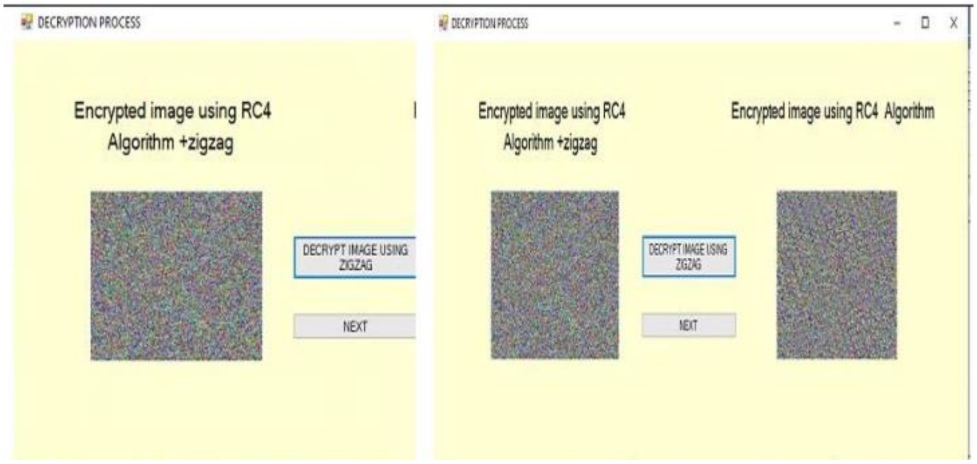
Partitions: Single partition - GUID Partition Map

Image Format: read/write disk image

Figure 5: The picture was downloaded and saved as "encrypted image.png."

Upload the new image for decryption

The user can access the hidden message by decrypting the image after it has been downloaded. The user must upload the downloaded image in order to decode it.

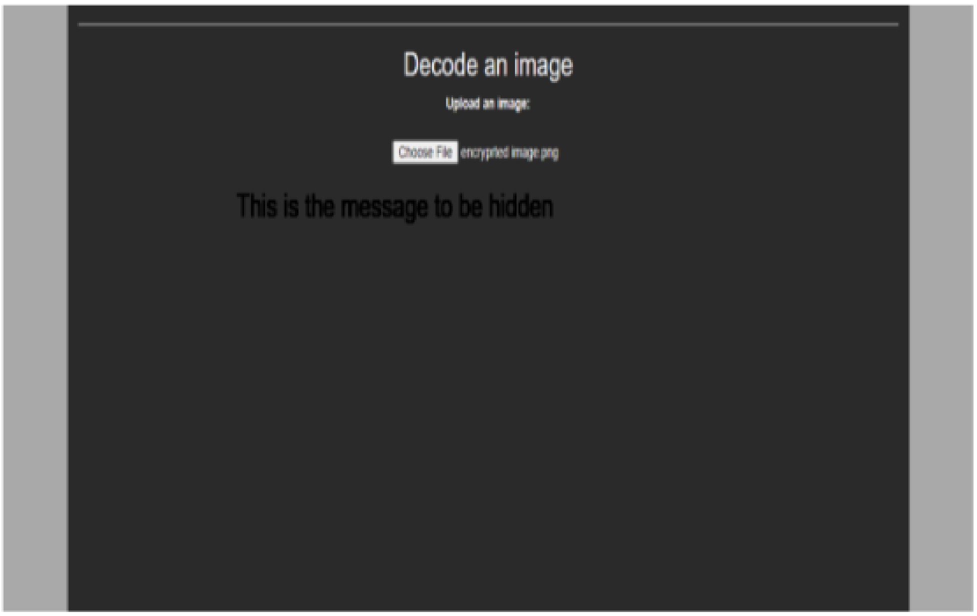


DECRYPTION PROCESS
Encrypted image using RC4 Algorithm +zigzag
DECRYPT IMAGE USING ZIGZAG
NEXT
DECRYPTION PROCESS
Encrypted image using RC4 Algorithm +zigzag
Encrypted image using RC4 Algorithm
DECRYPT IMAGE USING ZIGZAG
NEXT

Figure 6: submitting the encrypted picture for analysis.

Hidden message displayed:

The secret message appears after decryption of the encrypted image upon upload.



This is the message to be hidden

Figure 7: Hidden message displayed

5. CONCLUSION

Steganography techniques have advanced and developed to improve data security across media. Image concealing using steganography is an effective method for enhancing data security with minimal storage requirements. Embedding a secret message in an image's green pixels keeps it concealed and secure. Create two canvases with an uploaded image and user-entered text, then manipulate green pixel values to encode the message. It's easy to use: type the message, submit an image, download the encrypted image, then upload it again for decryption. The implementation shows how steganography may securely and efficiently conceal and disclose information. The successful completion of this project shows that steganography can safeguard data with ease of use and strong security. These studies demonstrate the importance of steganography in secure communication and the need for continual development to overcome evolving detection strategies and improve steganographic methods.

REFERENCES

1. *Al-Harbi, O. A., Alahmadi, W. E., & Aljahdali, A. O. (2020). Security analysis of DNA based steganography techniques. SN Applied Sciences, 2(2), 172.*
2. *Alyousuf, F. Q. A., & Din, R. (2020). Analysis review on feature-based and word-rule based techniques in text steganography. Bulletin of Electrical Engineering and Informatics, 9(2), 764-770.*
3. *Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2), 63-87.*
4. *Din, R., & Qasim, A. J. (2019). Steganography analysis techniques applied to audio and image files. Bulletin of Electrical Engineering and Informatics, 8(4), 1297-1302.*
5. *Frank, E. (2024). Steganography Techniques for Text Data (No. 13258). EasyChair.*
6. *Hameed, R. S., Abd Rahim, B. H. A., Taher, M. M., & Mokri, S. S. (2022). A literature review of various steganography methods. Journal of Theoretical and Applied Information Technology, 100(5).*
7. *Juneja, M., & Sandhu, P. S. (2013). A new approach for information security using an improved steganography technique. Journal of Information Processing Systems, 9(3), 405-424.*
8. *Kumar, M., Kumar, S., & Nagar, H. (2020). Comparative analysis of different steganography technique for image or data security. International Journal of Advanced Science & Technology (IJAST), 29(4).*
9. *Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. Mathematics, 9(21), 2829.*
10. *Matted, S., Shankar, G., & Jain, B. B. (2021). Enhanced image security using stenography and cryptography. In Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020 (pp. 1171-1182). Springer Singapore.*
11. *Pandey, B. K., Pandey, D., Gupta, A., Nassa, V. K., Dadheech, P., & George, A. S. (2023). Secret data transmission using advanced morphological component analysis and steganography. In Role of data-intensive distributed computing systems in designing data solutions (pp. 21-44). Cham: Springer International Publishing.*

12. *Sahu, M., Padhy, N., Gantayat, S. S., & Sahu, A. K. (2022, September). Performance analysis of various image steganography techniques. In 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA) (pp. 1-6). IEEE.*

13. *Saraswati, K., & Sharma, P. S. (2021). A literature survey on stenography approach based on different lsb technique. no, 2, 1-6.*

14. *Yahya, A. (2019). Steganography techniques for digital images. Cham: Springer International Publishing.*

15. *Yahya, A., & Yahya, A. (2019). Steganography techniques. Steganography techniques for digital images, 9-42.*