Sheltered Data Group For Monetary Data

Muniyan D[1], Santhosh Kumar I[2], Shabeer basha S[3], Needhu C[4]
[1, 2, 3] Dept of Computer Science and Engineering
[4]Associate Professor, Department of Computer Science and Engineering
[1, 2, 3, 4] Jerusalem College of Engineering, Chennai.

Abstract- *In this era of a digitally driven world, securing online communication is essential to protect sensitive information. Steganography is a powerful technique that conceals messages within digital media such as images or audio files, ensuring covert data transmission. This paper explores the fundamental concepts of digital steganography, highlighting its necessity and various forms. It specifically examines the Least Significant Bit (LSB) substitution method, Blowfish encryption, and LSB Matching, which embed secret data within the least significant bits of an image. Additionally, a comparative analysis is conducted between LSB and other steganographic techniques based on cover media quality, imperceptibility, and performance metrics. Furthermore, an estimation is made regarding the maximum amount of data that can be embedded in an image without noticeable distortion. This study emphasizes the significance of steganography in enhancing digital security and ensuring secure communication over the internet.*

I. INTRODUCTION

In an era where digital communication has become an integral part of daily life, securing sensitive information is more critical than ever. With the increasing risks of cyber threats, unauthorized access, and data breaches, the need for robust security mechanisms has grown substantially. While encryption ensures data confidentiality by transforming information into unreadable formats, it often raises suspicion when detected. Steganography, on the other hand, provides a discreet alternative by embedding secret messages within non-secret digital media such as images or audio files, making them virtually undetectable.

This paper focuses on digital steganography techniques, emphasizing their significance in secure communication. The primary objective is to analysis the effectiveness of different steganographic methods, with a particular focus on the Least Significant Bit (LSB) substitution, Blowfish encryption, and LSB Matching. Additionally, hybrid methods combining these techniques are considered to optimize security and imperceptibility.

II. OVERVIEW

This project explores digital steganography as a method for secure communication by hiding secret data within digital media like images. It focuses on techniques such as Least Significant Bit (LSB) substitution, Blowfish encryption, and LSB Matching, comparing them with advanced methods like DCT, spread spectrum, and adaptive steganography. The goal is to evaluate each method based on imperceptibility, data capacity, and robustness. Results show that combining encryption with steganography enhances security while maintaining media quality. The study highlights steganography's importance in protecting data in today’s digital world.

III. EXISTINGSYSTEM

Image steganography is the process of embedding text, images, or videos within a cover image without visible changes. Traditional methods like LSB have been effective, but with the rise of deep learning, new techniques have emerged to improve security and efficiency. Deep learning-based steganography can be classified into three categories: traditional methods, Convolutional Neural Networks (CNNs), and Generative Adversarial Networks (GANs). These methods enhance the ability to hide and extract data while resisting detection. This paper explores these approaches, along with the datasets used, experimental setups, and evaluation metrics. A summarized table is provided for easy reference. By analysing trends, challenges, and future directions, this study aims to guide researchers in developing more secure and efficient steganography techniques.

IV. PROPOSEDSYSTEM

Steganography is a technique used to hide messages in images or audio, ensuring secure communication. This project focuses on the Least Significant Bit (LSB) method, a widely used approach in digital steganography. To enhance data security and minimize image distortion, we compare LSB with advanced techniques like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Blowfish encryption, and LSB Matching. These methods aim to improve data hiding efficiency while maintaining image quality. The study evaluates them using metrics like PSNR

and SSIM to measure distortion and detectability. The goal is to embed more data securely without noticeable changes, strengthening digital privacy and protection against detection.

V. PROBLEM STATEMENT

Protecting sensitive information is crucial in the digital age, where data breaches and cyber threats are increasingly common. While encryption plays a vital role in securing data by making it unreadable to unauthorized users, it often signals the presence of confidential information, which can draw unwanted attention. Steganography, on the other hand, provides an additional layer of security by concealing data within seemingly innocuous media files, such as images, audio, or video, thereby reducing the likelihood of detection.
However, the main challenge in steganography lies in embedding information without noticeably altering the quality of the cover media or significantly reducing the size of the hidden message. Striking a balance between imperceptibility, robustness, and payload capacity is essential for effective steganographic techniques. This paper explores and compares both traditional and advanced steganographic methods, aiming to identify approaches that offer improved media quality, greater concealment, and higher data capacity while maintaining resistance to detection and tampering.

VI. BLOCK DIAGRAM

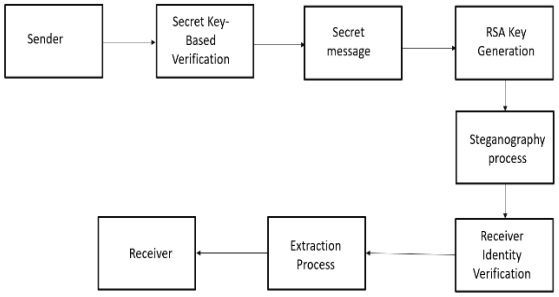

Figure 1: Block Diagram

VII. ARCHITECTURE DIAGRAM

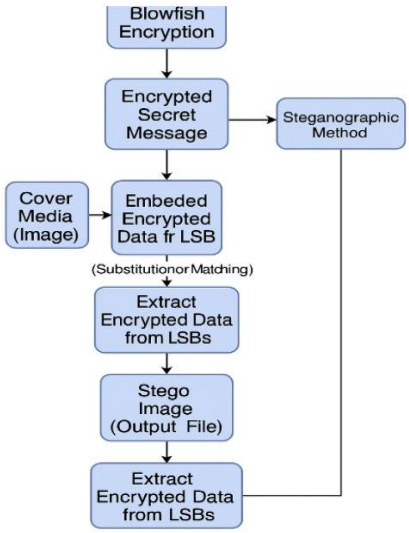

Figure 2: Architecture Diagram

VIII. WORKING MODEL

1.Least Significant Bit (LSB) Substitution:

LSB substitution is one of the most common steganographic techniques, where secret data is embedded by modifying the least significant bits of image pixels. The advantage of this method is its simplicity and minimal impact on image quality, but it is vulnerable to statistical attacks.

2.Blowfish Encryption with Steganography:

Blowfish encryption enhances security by encrypting the message before embedding it. This ensures that even if the steganographic content is detected, the actual message remains protected.

3. LSB Matching:

LSB Matching modifies pixel values probabilistically to embed data, reducing the detectability of steganographic content. This approach improves security compared to traditional LSB substitution.

4.Discrete Cosine Transform (DCT) Steganography:

DCT-based techniques operate in the frequency domain, modifying the coefficients of an image's frequency components to hide information. This method offers improved robustness against compression and transformations.

5. Spread Spectrum Steganography:

Spread spectrum steganography applies principles of spread spectrum communications, distributing the embedded data across multiple frequency components, thereby improving resistance against noise and attacks.

6. Transform Domain Techniques:

Transform domain methods such as wavelet-based steganography employ transformations like Discrete Wavelet Transform (DWT) to hide data in frequency coefficients, enhancing resistance to detection.

7. Adaptive Steganography:

Adaptive steganography modifies embedding based on image characteristics, optimizing imperceptibility and security.

IX. COMPARATIVE ANALYSIS OFTECHNIQUES

To evaluate the effectiveness of these techniques, we analyze key performance metrics:

Imperceptibility: Measures the impact of steganographic embedding on cover media quality.

Payload Capacity: Determines the amount of data that can be embedded without noticeable distortion.

Robustness: Assesses the resistance of steganographic techniques to attacks.

Technique	Imperceptibility	Payload Capacity	Robustness
LSB Substitution	High	High	Low
Blowfish + LSB	High	Moderate	High
LSB Matching	Moderate	Moderate	High
DCT Steganography	High	Low	High
Spread Spectrum	Moderate	Low	Very High
Transform Domain	High	Low	Very High
Adaptive Steganography	Very High	Moderate	High

Figure 3: Analysis OfTechniques

X. RESULTS AND DISCUSSION

`While steganography offers a promising approach for secure communication, it is not foolproof. Techniques such as steganalysis can detect hidden messages, necessitating the continuous evolution of steganographic methods.

The integration of machine learning in steganography detection and prevention has gained interest. Future research could focus on adaptive steganographic techniques that use artificial intelligence to determine optimal embedding patterns, enhancing security and efficiency.

Additionally, hybrid steganographic techniques combining multiple methods, such as DCT-based embedding with LSB substitution, could offer a balance between capacity, security, and imperceptibility. The development of real-time steganographic systems for practical applications remains an open research area.

XI. CONCLUSION

This study highlights the importance of digital steganography in secure communication. By comparing LSB substitution, Blowfish encryption, LSB Matching, DCT-based methods, spread spectrum steganography, transform domain techniques, and adaptive steganography, it provides insights into their strengths and limitations. Steganography remains a valuable tool for data security, and continued research is essential for enhancing its effectiveness in the face of advancing steganalysis techniques.

XII. FUTURE WORK

Future work can focus on improving steganography by combining LSB, DCT, and DWT for better security and image quality. Advanced encryption like AES and RSA can strengthen data protection. AI can help find the best hiding spots, while new techniques can defend against attacks. Expanding steganography to videos, audio, and cloud storage can enhance its applications. Blockchain can also be used to ensure message integrity and prevent tampering, making hidden communication even more secure.

XIII. ACKNOWLEDGEMENT

We would like to thank Assistant Professor. Ms.C.Needhu.,M.E,M.B.A, Department of Computer Science and Engineering, for her continuous support and guidance.

REFERENCES

[1] Johnson, N. F., &Jajodia S. (1998). Exploring steganography: Seeing the unseen. IEEE Computer.
[2] Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy.

[3] KatzenbeisserS &Petitcolas F. A. (2000). Information hiding techniques for steganography and digital watermarking. Artech House.
[4] Fridrich, J. (2009). Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press.
[5] Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital Watermarking.Morgan Kaufmann Publishers.
[6] Liu, F., & Sung, A. (2013). A survey on steganalysis techniques.IEEE Transactions on Signal Processing.
[7] V. Sathya, K Balasubramaniyam, N Murali “Data hiding in audio signal, video signal text and JPEG Images" IEEICAESM 2012.Mrach 30-3 I 2012, pp74l -746.
[8] Lee, Y., Chen, L. “High capacity image steganography model”, IEEE Proceedings on Vision, Image and Signal Processing 2000, 147, 3, 288-294.
[9] Y. He, et al., "A real-time dual video stream for Video-on-Demand” Journal of Electronics and Communication vol. 66, pp. 305-312, 2012.