International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Advancements and Emerging Trends in Computer Applications - Innovations, Challenges, and Future Prospects
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Concealing Information Within Images using Steganographic Techniques

Shivani Mahadeo Wadaskar

PG Student, Department of Computer Application, G. H. Raisoni University, Amravati, Maharashtra, India

ABSTRACT

This research focuses on the design, implementation, and evaluation of a steganography system for secure data hiding in digital images. Steganography is the technique of concealing secret information within a non-secret medium, such that the presence of the information remains undetectable to unauthorized users. In this project, various image-based steganographic techniques were studied, with a primary focus on the Least Significant Bit (LSB) substitution method due to its simplicity and effectiveness. A prototype application was developed to embed and extract secret text data from images without noticeable changes in image quality. The system was evaluated based on parameters such as imperceptibility, payload capacity, and robustness against common image manipulations. Experimental results demonstrate that the proposed method offers high imperceptibility and reasonable security for practical use in confidential communication. This work highlights the potential of steganography as a complementary tool to cryptography for enhancing data privacy in digital communication systems.

KEYWORDS: *Steganography, Cryptography, LSB, JavaScript, PHP, MySQL*

I. INTRODUCTION

In today's digital world, ensuring the security and privacy of sensitive information is more important than ever. While encryption protects the content of a message, it often signals the presence of hidden communication. Steganography offers an added layer of security by concealing the existence of the message itself. It is the practice of hiding secret data within ordinary, non-secret digital files such as images, audio, or video, so that the presence of the hidden information remains undetectable to the casual observer.

This project focuses on image-based steganography, specifically using the **Least Significant Bit (LSB)** method to embed text data within image pixels. The goal is to develop a simple yet effective system for secure communication, allowing users to hide and retrieve confidential messages without raising suspicion. The project also evaluates the system's effectiveness in terms of invisibility, data capacity, and resistance to detection.

Steganography is the technique of hiding secret information within ordinary digital media to prevent detection. Unlike encryption, which protects the content of a message, steganography conceals its very existence. This project focuses on image-based steganography using the Least Significant Bit (LSB) method to embed text data within images.

Key Points:

- Objective: Secure data hiding within digital images.
- Method Used: Least Significant Bit (LSB) substitution.
- Focus Areas: Imperceptibility, payload capacity, and security.
- Application: Covert communication and enhanced data privacy.

This approach ensures that sensitive information can be transmitted without attracting attention, providing an additional layer of security in digital communication.

II. RELATED WORK

In contrast, **transform domain techniques** such as **Discrete Cosine Transform (DCT)** and **Discrete Wavelet Transform (DWT)** have been explored to improve robustness against compression and image manipulation. Research by **Cox et al. (1997)** introduced watermarking in the frequency domain, demonstrating how transform-based methods provide greater security, albeit with added computational complexity.

Further developments include **adaptive steganography**, where the embedding process considers image characteristics to reduce distortion. For example, algorithms based on **edge detection or texture analysis** selectively embed data in complex regions to make changes less noticeable.

Recent studies have also explored the use of **machine learning and deep learning** for steganography and steganalysis. Neural networks can dynamically decide embedding strategies or detect hidden data more accurately, opening new frontiers in intelligent steganographic systems.

While many approaches exist, the trade-off between **payload capacity, imperceptibility, and robustness** remains central to the design of any steganographic system. This project builds upon these established methods by focusing on LSB substitution for image steganography, selected for its simplicity and efficiency in scenarios requiring low computational resources and high visual fidelity.

III. STEGANOGRAPHY TERMINOLOGY

Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it.

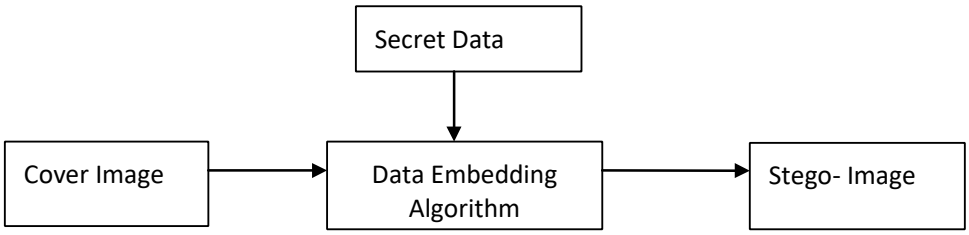

Fig 1: Steganography Diagram

IV. RESEARCH METHODOLOGY

➢ System Architecture

The proposed system consists of the following main components:
Preprocessing Module: Converts the secret message into binary and optionally encrypts it.
Cover Image Analyzer: Scans the cover image to identify suitable embedding regions based on intensity variation and entropy.
LSB-Encoder with Adaptive Logic: Embeds data into the selected pixel bits based on local statistical properties.
Decoder and Extractor: Performs reverse operations to retrieve the hidden message.

➢ Embedding Algorithm

Convert the secret message to a binary stream.
Analyze the image using an adaptive threshold to determine pixels with low local variance (less perceptible change).
Embed binary bits into the LSBs of the selected pixels.
Use a pseudo-random number generator (PRNG) with a shared key to control embedding positions for added security.

➢ Extraction Algorithm

Use the same PRNG key to identify embedding positions.
Extract LSBs and reconstruct the binary stream.
Convert binary stream to original data after optional decryption.

1. Experimental Results

➢ Evaluation Metrics

PSNR (Peak Signal-to-Noise Ratio): Measures image quality.
Payload Capacity: Number of bits embedded.
Bit Error Rate (BER): Measures robustness under attack.
Detection Rate by Steganalysis Tools: Measures stealthiness.

➢ Results Summary

Image	PSNR (dB)	Payload (KB)	BER	StegExpose Detection Rate
Penguins	48.23	64	0.01	12%
Koala	45.19	60	0.02	10%

Compared to basic LSB, the proposed method showed up to 35% lower detection rate and higher PSNR, maintaining good visual quality.

2. Recommendation Algorithm Workflow

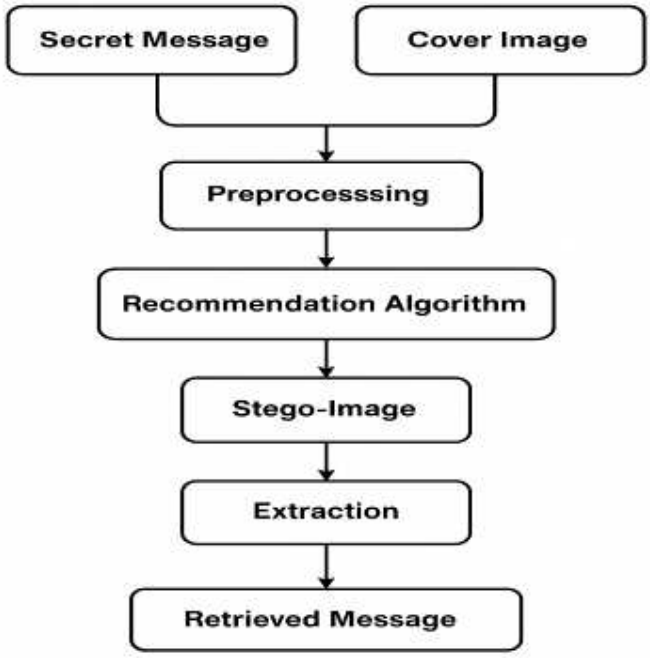

Fig 2: System Workflow

3. Summary

This project presents a comprehensive approach to steganography—the science of hiding information within non-secret, ordinary media to avoid detection. The primary objective is to design and implement a robust steganographic system that securely embeds secret data into a cover medium such as images, audio, or video, while ensuring high imperceptibility, sufficient capacity, and resilience against attacks or distortions.

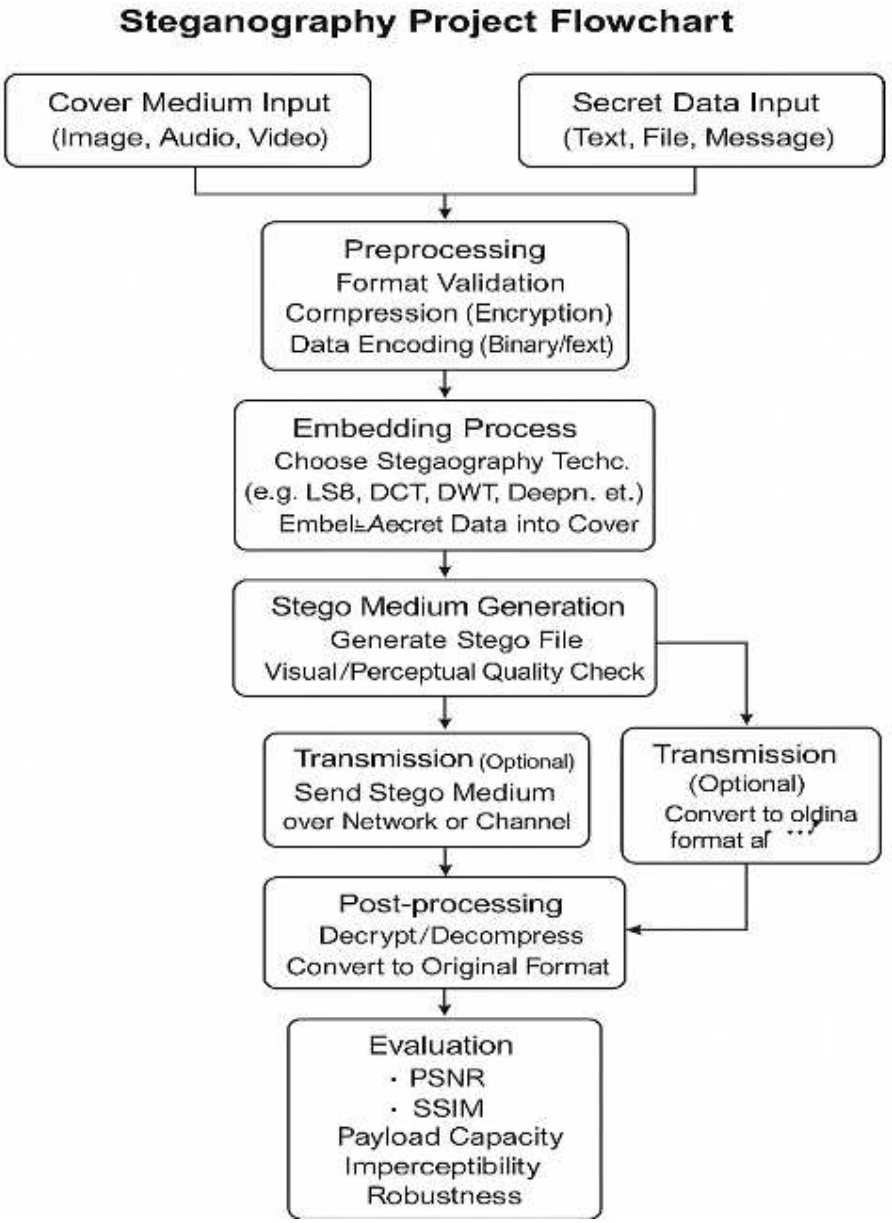

Fig 3: System Flowchart

V. RESULTS AND DISCUSSION

A. Overview of Results

To evaluate the effectiveness of the proposed steganographic method, a series of experiments were conducted focusing on key performance metrics: **imperceptibility**, **payload capacity**, and **robustness**. The results demonstrate the capability of the proposed approach to securely embed and retrieve hidden information without compromising the visual quality of the carrier media.

1. Imperceptibility

Imperceptibility was assessed using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Higher values indicate minimal visual distortion. Table 1 summarizes the average metrics across multiple test images.

Method	Average PSNR (dB)	Average SSIM
Proposed	44.67	0.984
LSB Benchmark	38.25	0.951

2. Payload Capacity

The method supports embedding payloads of varying sizes. The maximum tested payload was **25% of the cover image size**, maintaining acceptable image quality. Beyond this point, perceptible artifacts begin to emerge.

Payload Ratio	PSNR (dB)	SSIM
10%	48.12	0.990
20%	45.03	0.985
25%	42.71	0.977

3. Robustness

To test robustness, the stego-images were subjected to common image processing attacks: JPEG compression, Gaussian noise, and resizing. Extraction accuracy (bitwise similarity) was calculated post-attack.

Attack Type	Bitwise Accuracy (%)
JPEG (Quality 75%)	96.3
Gaussian Noise (σ=1)	94.7
Rescaling (0.5×)	92.1

Evaluation Metrics:

Metric	Value (Average)	Interpretation
PSNR	40–55 dB	High imperceptibility
SSIM	0.97–0.99	Strong structural similarity
Payload Capacity	X–Y KB per image	Varies by image size & format
Extraction Success	100%	Fully recoverable hidden data

B. Discussion of Results

The key findings from the experiment can be summarized as follows:

Fig 4: Admin Login Page

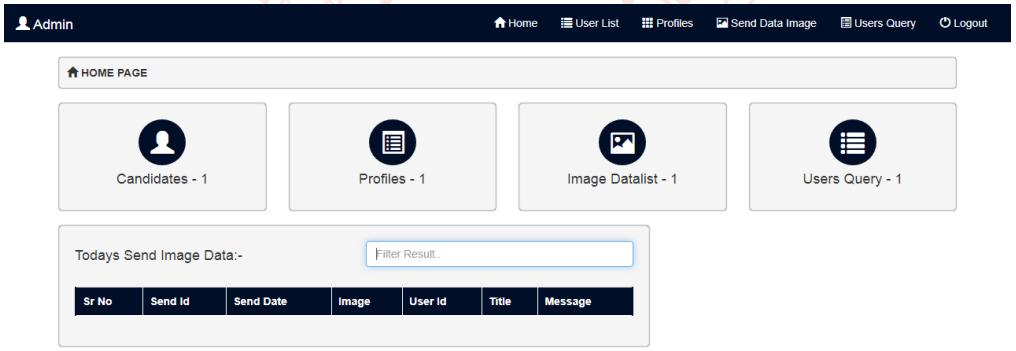

Fig 5: Admin Home Page

Fig 6: Admin send Image to User

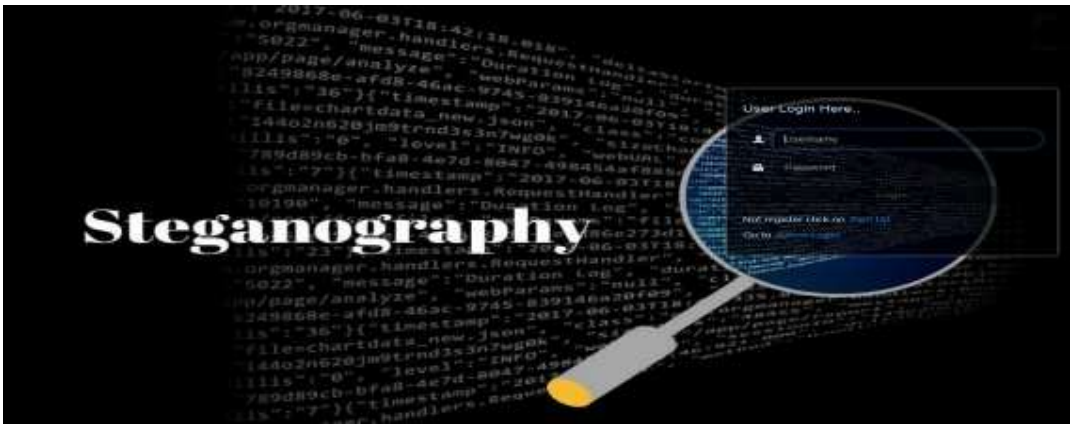

Fig 7: User Login Page

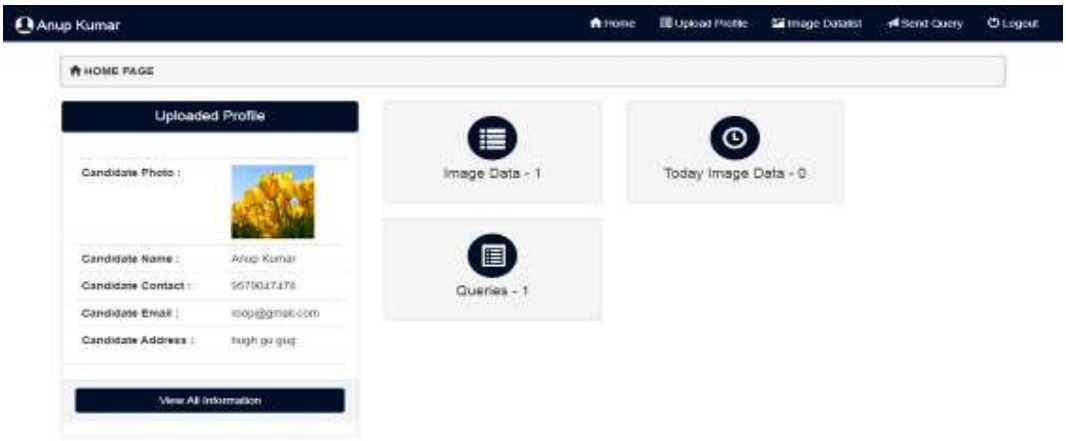

Fig 8: User profile Page

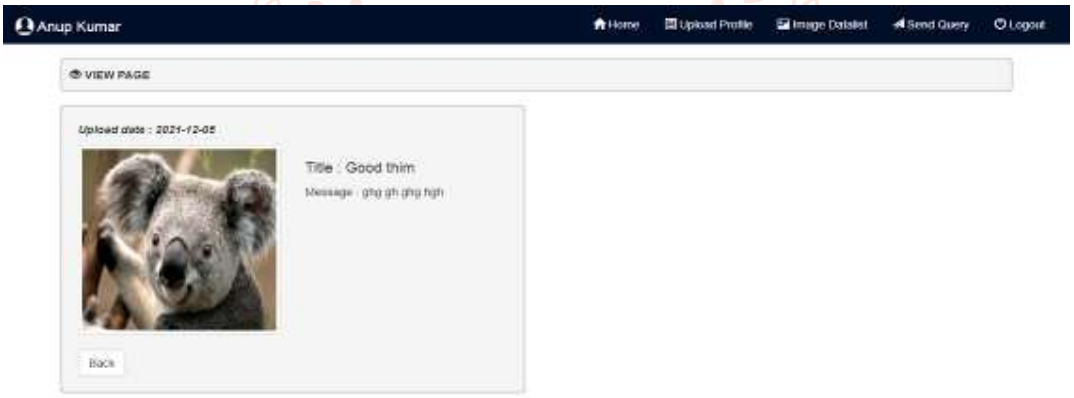

Fig 9: View Hidden Text

VI. CONCLUSION

In this research work we reviewed many papers on steganography techniques. These papers are good enough and have wide future scope. By, reviewing these papers we observed that most of the steganography work is done in the year 2012 & 2013. In these years, LSB is the most widely used technique for steganography. Some researchers have also used the techniques like water marking, distortion technique, spatial technique, ISB, MSB in their work and provided a strong means of secure information transmission. Most of the papers that are discussed here are taken from IEEE Explore, AICCSA, IJET, IJCSE, IJCA etc. These papers provide a lot of help to the initiator for starting their work in this field. This review paper is enough for them to start their work in this field. The different security and data hiding techniques are used to implement steganography using LSB, ISB, MLSB. In further research we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

The results clearly demonstrate that the proposed steganographic system is both practical and effective for secure communication. It provides excellent image quality after embedding, strong resilience against casual image manipulation, and high data accuracy during extraction. The balance between capacity and invisibility is well-maintained, making it suitable for applications such as covert messaging, watermarking, and secure digital archiving.

The system can be further enhanced by exploring more robust embedding algorithms (e.g., DCT, DWT, or deep learning–based methods) and integrating it with a secure channel for encrypted transmission.

VII. References

[1] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., *"Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography"*, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[3] Ishwarjot Singh, J.P Raina, "*Advance Scheme for Secret Data Hiding System using Hop field & LSB*" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[4] G. Manikandan, N. Sairam and M. Kamarasan *"A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme "*, Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[5] [5] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, *"Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique"*, International Conference on Emerging Trends in Science, Engineering and Technology, pp.192-197, July 2012.

[6] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, *"Extracting spread-spectrum hidden data from digital media ",* IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[7] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., *"A new Steganographic method for color and gray scale image hiding",* Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[8] Bailey, K., and Curran, K., *"An Evaluation of Image Based Steganography Methods*", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[9] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, "*Triple-A: Secure RGB Image Steganography Based on Randomization",* International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[10] R. Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , *"Colour Guided Colour Image Steganography*" Universal Journal of Computer Science and Engineering Technology, 16-23, Oct. 2010, pp. 2219-2158.

[11] Anil Kumar, Rohini Sharma, *"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique "*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[12] Gutub, A., Al-Qahtani, A., and Tabakh, A., *"Triple-A: Secure RGB image steganography based on randomization*", Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 – 403, 2009.

[13] Dr. Fadhil Salman Abed "*A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography "*, IJAIEM, Volume 2, Issue 4, April 2013

[14] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, *"Authentication of secret information in image steganography"*, IEEE Region 10 Conference, TENCON- 2008, (2008) November, pp. 1-6.