SYNOPSIS REPORT

Multi-Algorithm Steganography for Secure Data Transmission

By

Name:- Abhinav Kumar
Entry No:- 22bcs003
&
Name:- Sourav Raj
Entry No:- 22bcs091
&
Name:- Suman Kumar Mishra
Entry No:- 22bcs095

Under the Guidance of Dr. Rohit Tanwar

Submitted in partial fulfillment of the requirements for the award of the degree
Of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING

10/09/25

SHRI MATA VAISHNO DEVI UNIVERSITY, KATRA
(School of Computer Science & Engineering)
JAMMU & KASHMIR-182320

1. INTRODUCTION

Solutions that can discreetly conceal information in ways that are both reliable and flexible are needed to meet the growing demands for secure and covert communication in today's digital environment. Current tools frequently limit users to a single steganography method, which reduces flexibility and the ability to compare methods. A comprehensive, user-friendly system that supports a variety of steganography algorithms is required so that users can choose the one that best suits their unique security, robustness, and capacity needs. Our project attempts to address this by creating an Android-based steganography application that allows users to embed and extract secret messages from images using a variety of sophisticated algorithms, including LSB, DCT, DWT, fuzzy logic-based, PVD, palette-based, and mshEdgeGrayFT1.

2. LITERATURE SURVEY

A crucial area of information security that focuses on hiding data in digital media is steganography. Although they are straightforward and have a large capacity, traditional techniques like Least Significant Bit (LSB) modification can be easily detected and manipulated. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are two transform domain techniques that offer enhanced resilience against image compression and attacks. Palette-based methods and Pixel Value Differencing (PVD) are examples of region-based techniques that use color indices or statistical characteristics to conceal data.

Fuzzy logic-based steganography is one recent development that improves security and imperceptibility by identifying the best embedding regions using fuzzy inference systems. For instance, the mshEdgeGrayFT1 algorithm, which combines LSB embedding and Mamdani fuzzy logic for edge-based data hiding in grayscale images, exhibits better performance in terms of robustness and imperceptibility. Collectively, these techniques show how steganography has developed from basic spatial methods to complex, flexible, and hybrid strategies appropriate for a range of real-world situations.

Summary of Literature

- LSB-based steganography is simple and high-capacity but less robust.
- DCT/DWT (transform domain) methods are robust against compression and attacks.

- PVD and palette-based techniques exploit statistical and color properties for increased security and flexibility.
- Fuzzy logic-based methods adaptively select embedding regions for better imperceptibility.
- mshEdgeGrayFT1 leverages fuzzy logic and edge detection for optimal data hiding in grayscale images.
- There is a growing emphasis on modular systems supporting multiple algorithms, enabling users to choose methods based on their needs and allowing comparative analysis.

Together, these studies demonstrate how steganography has advanced from simple LSB techniques to complex hybrid and adaptive strategies. According to the literature, future systems should prioritize usability, versatility, and resistance to digital forensics in addition to security and the invisibility of hidden data.

3. PROBLEM STATEMENT

Solutions that can discreetly conceal information in ways that are both reliable and flexible are needed to meet the growing demands for secure and covert communication in today's digital environment. Current tools frequently limit users to a single steganography method, which reduces flexibility and the ability to compare methods. A comprehensive, user-friendly system that supports a variety of steganography algorithms is required so that users can choose the one that best suits their unique security, robustness, and capacity needs. In order to address this, our project aims to design a web-based steganography system that allows users to embed and extract secret messages from images using a variety of sophisticated algorithms, including LSB, DCT, DWT, fuzzy logic-based, PVD, palette-based, and mshEdgeGrayFT1.

4. OBJECTIVES

The primary objectives of this project are:

4.1. Develop a modular website for image steganography from scratch.

4.2. Implement the following algorithms: LSB, DCT, DWT, Fuzzy Logic-based, PVD, Palette-based, mshEdgeGrayFT1.

4.3. Enable user selection of steganography method prior to encoding/decoding.

4.4. Ensure robust, efficient, and imperceptible data hiding for each supported algorithm.

4.5. Provide comparative analysis tools for evaluating capacity, security, and robustness across methods.

4.6. Design a reusable and extensible core library to facilitate future integration of additional algorithms.

4.7. Create a user-friendly interface with visualization, progress indicators, and comprehensive error handling.

5. METHODOLOGY

The project will follow a structured methodology to ensure a robust and high-quality final product.

5.1. Requirement Analysis

- Identify user needs, security requirements, supported file formats, device/browser constraints, and performance criteria.

5.2. Algorithm Research and Selection

- Develop independent modules for each steganography method: LSB, DCT, DWT, Fuzzy Logic-based, PVD, Palette-based, mshEdgeGrayFT1.
- Ensure each module adheres to a common interface for encoding and decoding.

5.3. Core Algorithm Development

- Build a modular, extensible library for managing algorithms and user selections.

- Integrate UI components for algorithm selection, image handling, and message input/output.

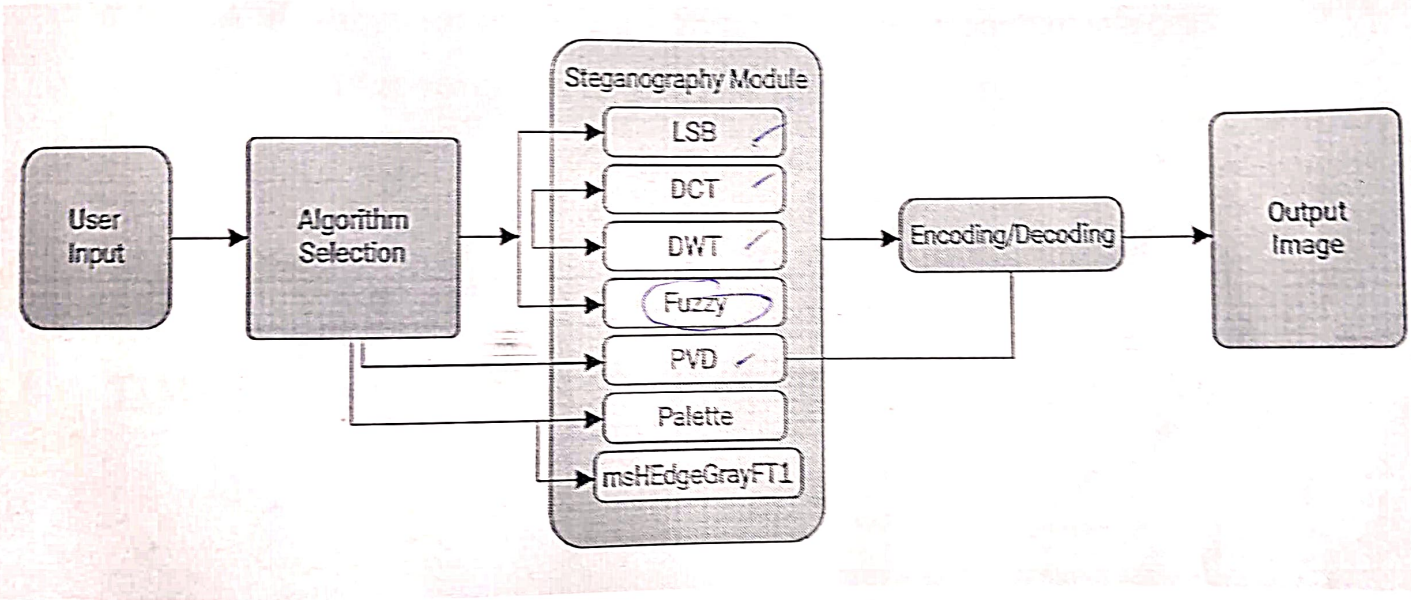
5.4. Testing and Evaluation

- Conduct rigorous testing for correctness, imperceptibility, robustness, and performance.
- Compare results across algorithms using standard metrics (PSNR, SSIM, MSE).

5.5. Documentation and Demonstration

- Prepare comprehensive documentation and demonstrate the application with real-world use cases.

6. BLOCK DIAGRAM



7. EXPECTED RESULTS

We are looking for a working and efficient Android application that performs steganography on images successfully. The key results will include:

7.1. A fully functional website supporting multiple steganography algorithms.

7.2. Robust implementations of LSB, DCT, DWT, Fuzzy Logic-based, PVD, Palette-based, and mshEdgeGrayFT1 methods.

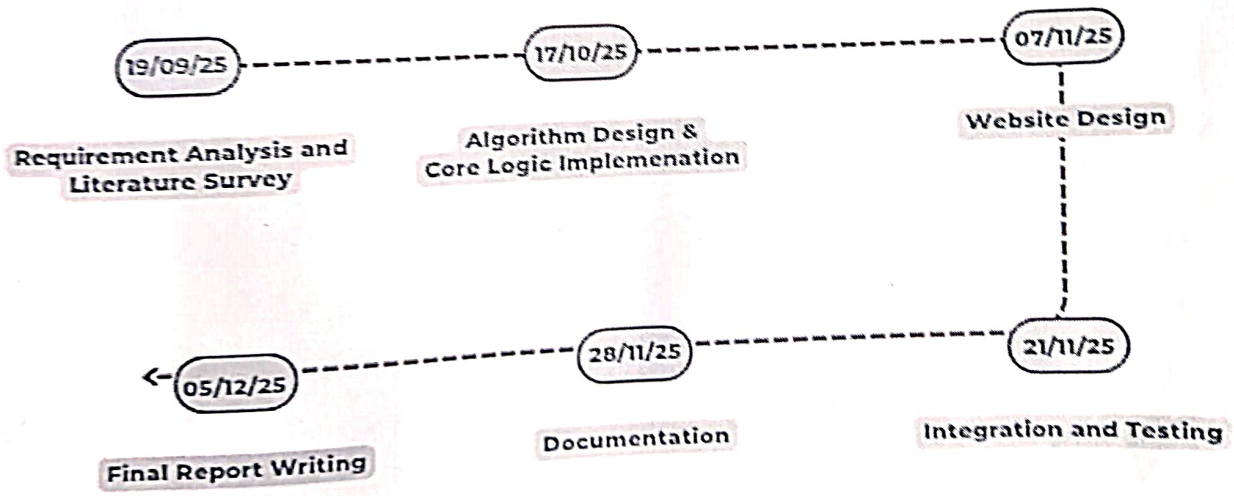
7.3. User-selectable encoding and decoding workflows.

7.4. Comparative results and benchmarks for algorithm selection.

7.5. A reusable, extensible core library for future algorithm integration.

7.6. Comprehensive documentation and user support.

8. TIME SCHEDULE FOR COMPLETION OF THE PROJECT



9. REFERENCES

[1] Kaur, S., Kaur, S., & Singh, G. (2011). A Survey of Digital Image Steganography

[2] Choudhary, P., & Kumar, N. (2019). A Review of Image Steganography Techniques

[3] Swain, D., & Lenka, S. K. (2016). Least Significant Bit (LSB) Embedding Technique using Canny Edge Detection

[4] Fridrich, J., Goljan, M., & Du, R. (2001). Steganalysis of LSB Encoding in Color Images

[5] Muhammad, K., Ahmad, J., & Mehmood, I. (2015). Combined Cryptography and Steganography for Secure Communication

[6] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). A Survey on Transform Domain Techniques of Image Steganography

[7] Petitcolas, F. A. (2003). Robust Image Steganography Based on DWT*DCT

[8] Fridrich, J., Goljan, M., & Du, R. (2001). Steganalysis of LSB Encoding in Color Images

[9] Choudhary, P., & Kumar, N. (2019). A Review of Image Steganography Techniques.

Signature of Students

Signature of Guide

(Dr. Rohit Tanwar)

1. Abhinav Kumar (22BCS003)
2. Sourav Raj (22BCS091)
3. Suman Kr Mishra (22BCS095)