PixelCrypt – A Secure Steganography Tool

MASTER OF COMPUTER APPLICATIONS

of

Visvesvaraya Technological University

By

VARUN KUMAR

1BI24MC157

Under the Guidance of

Internal Guide:

Sandarsh Gowda M
Assistant Professor
Department of MCA
BIT, Bengaluru.

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS

BANGALORE INSTITUTE OF TECHNOLOGY

(An Autonomous Institution under VTU)

K. R. Road, V. V. Pura, Bengaluru – 560004

October - 2025

BANGALORE INSTITUTE OF TECHNOLOGY

(An Autonomous Institution under VTU)

K.R. Road, V.V. Pura, Bengaluru-560004

Vision

To establish and develop the Institute as a centre of higher learning, ever abreast with expanding horizon of knowledge in the field of engineering and technology, with entrepreneurial thinking, leadership excellence for life-long success and solve societal problem.

Mission

- Provide high quality education in the engineering disciplines from the undergraduate through doctoral levels with creative academic and professional programs.
- Develop the Institute as a leader in Science, Engineering, Technology and management, Research and apply knowledge for the benefit of society.
- Establish mutual beneficial partnerships with industry, alumni, local, state and central governments by public service assistance and collaborative research.
- Inculcate personality development through sports, cultural and extracurricular activities and engage in the social, economic and professional challenges.

BANGALORE INSTITUTE OF TECHNOLOGY

(An Autonomous Institution under VTU)

K.R. Road, V.V. Pura, Bengaluru-560004

Department of Master of Computer Applications

Vision

To transform young graduates into skilled computer professionals to meet Industrial and societal needs.

Mission

- To enhance the Teaching learning process to meet quality education in the field of Computer applications
- To impart the knowledge in current technologies to meet the industrial needs
- To inculcate ethical values and leadership qualities for the betterment of society

PEO's

PEO1: To develop quality application software with innovative ideas to meet the industrial requirements

PEO2: To imbibe the current technologies and to adopt in computing profession as per the changing needs

PEO3: To progress in their career with leadership qualities and ethical values that enhances self and societal growth

PROGRAM OUTCOME (POs)

Post Graduates will be able to:

1. **Foundation Knowledge:** Apply knowledge of mathematics, programming logic and coding fundamentals for solution architecture and problem solving.
2. **Problem Analysis:** Identify, review, formulate and analyses problems for primarily focusing on customer requirements using critical thinking frameworks.
3. **Development of Solutions:** Design, develop and investigate problems with as an innovative approach for solutions incorporating ESG/SDG goals.
4. **Modern Tool Usage:** Select, adapt and apply modern computational tools such as development of algorithms with an understanding of the limitations including human biases.
5. **Individual and Teamwork:** Function and communicate effectively as an individual or a team leader in diverse and multidisciplinary groups. Use methodologies such as agile.
6. **Project Management and Finance:** Use the principles of project management such as scheduling, work breakdown structure and be conversant with the principles of Finance for profitable project management.
7. **Ethics:** Commit to professional ethics in managing software projects with financial aspects. Learn to use new technologies for cyber security and insulate customers from malware**.**
8. **Life-long learning:** Change management skills and the ability to learn, keep up with contemporary technologies and ways of working.

TABLE OF CONTENTS

SYNOPSIS

1. ABSTRACT / EXECUTIVE SUMMARY

The "PixelCrypt" project is an advanced, real-time web application designed to provide truly secure and covert communication for everyday users. The application addresses the fundamental security flaw in most online tools by implementing a client-side encryption model. A user's secret message is first encrypted directly in their browser using military-grade AES-256, ensuring that the unencrypted, plaintext data never leaves their local machine. This encrypted data is then sent to a server, which performs LSB (Least Significant Bit) steganography to hide it invisibly within an image file. As a publicly deployed MERN stack application, PixelCrypt serves as a practical, zero-knowledge tool that provides plausible deniability and makes high-level cybersecurity accessible to a non-technical audience.

2. INTRODUCTION

2.1 BACKGROUND

In the modern digital world, standard encryption protects a message's content but visibly marks it as a secret, attracting unwanted attention. Steganography, the art of hiding data in plain sight, offers a more covert solution. However, the migration of such tools to the web has created a new vulnerability: server-side processing, where users must trust unknown servers with their private data. This project leverages modern full-stack web technologies to solve this issue, architecting a system where the most critical security operation—encryption—happens securely on the client-side.

2.2 MOTIVATION

The primary motivation for this project is to build a steganography tool that is both genuinely secure and publicly accessible. Most online tools force a dangerous trade-off between convenience and privacy. This project is driven by the challenge of building a real-world, "zero-knowledge" application where user privacy is mathematically guaranteed, not just promised. By creating a professional-grade, deployed web application, we aim to

demonstrate the correct way to architect secure web services and provide a trustworthy tool for private communication

2.3 DOMAIN OVERVIEW

- Domain: Cybersecurity, Full-Stack Web Development
- Sub-domains: Applied Cryptography, Steganography, Secure Web Architecture, Client-Side Security.
- Technologies Used:
    - Frontend (Client-Side): React.js, CryptoJS (for AES encryption).
    - Backend (Server-Side): Python with Flask or FastAPI (for the steganography API).
    - Core Algorithms: AES-256, Least Significant Bit (LSB).

3. PROBLEM STATEMENT

3.1 PROBLEM IDENTIFICATION

There are two core problems with existing data hiding solutions. First, standard encryption lacks the stealth required for covert communication. Second, almost all existing online steganography tools are architecturally insecure, as they require users to upload their unencrypted secret messages to a server, creating a massive privacy vulnerability and a single point of failure.Existing tools are often either too complex for the average person or are untrustworthy online services with no transparency.

3.2 PROBLEM ANALYSIS:

A secure, real-time solution requires an architecture that never exposes plaintext user secrets to the server. The central challenge is to separate the cryptographic operations from the steganographic ones. The system must be designed so that:

- Encryption and decryption happen exclusively within the user's browser.
- The server's only role is to perform the steganography on data that is already encrypted and meaningless to it.
- The application is deployed and available for real-time public use without compromising this security model.

4. LITERATURE REVIEW

4.1 RELATED WORK

A review of existing tools reveals two flawed categories. Command-line utilities like Steghide are secure but are too complex for the average person. Most online web tools, while user-friendly, are critically insecure due to their server-side processing model, where plaintext secrets are transmitted over the internet, creating an unacceptable risk.

4.2 RESEARCH GAP

The significant research gap is the lack of a publicly deployed, real-time steganography web application that implements a zero-knowledge, client-side encryption architecture. Existing online tools fail to address the fundamental user trust issue. This project, PixelCrypt, fills this gap by demonstrating and building a production-ready, secure web application that correctly handles user data, making it a novel contribution to accessible and secure privacy tools.

5. OBJECTIVES

5.1 PRIMARY OBJECTIVE

To design, develop, and deploy a full-stack, real-time web application that allows users to securely hide messages in images, architected with client-side AES-256 encryption to ensure user secrets are never exposed to the server.

5.2 SECONDARY OBJECTIVES:

- To implement the AES-256 encryption and decryption logic entirely on the client-side using JavaScript (React).
- To build a lightweight backend API in Python whose sole responsibility is to perform LSB steganography on pre-encrypted data.
- To create a seamless and intuitive user interface that makes these complex security operations easy for anyone to use.

- To successfully deploy the frontend and backend applications to cloud platforms for public, real-time access.

6. HARDWARE / SOFTWARE SPECIFICATION

Hardware Requirements

- **Client-Side:** Any modern computer or mobile device with a web browser.
- **Server-Side:** A cloud hosting platform (e.g., Vercel for frontend, Render/Heroku for backend) with a basic resource tier (512MB RAM, 1vCPU).

Software Requirements

- **Operating System (Server): Linux.**
- **Frontend Framework: React.js.**
- **Client-Side Crypto Library: CryptoJS.**
- **Backend Framework: Python with Flask or FastAPI.**
- **Server-Side Image Library: Pillow (PIL Fork).**
- **Version Control & Deployment: Git, GitHub.**