

### QUAID-E-AWAM UNIVERSITY OF ENGINEERING, SCIENCE & TECHNOLOGY NAWABSHAH

**(DEPARTMENT OF INFORMATION TECHNOLOGY)**

**Enhancing Image Steganography Techniques for Secure Communication**

(ANDROID BASED PLATFORM)

**SUBMITTED BY:**

**Ubaidullah Qureshi (20IT-16 Group Leader)**

**Waqas Rajput (20IT-07)** **Savera Khan (20IT-64)**

**SUPERVISED BY: Dr. Saima Siraj Soomro**



CERTIFICATE

This is to certify that Mr./ Miss D/o / S/o Roll No. Final year student of Bachelor of Science Information Technology) has completed the Partial requirement of Project / Thesis during session 2023. The Title of the project is "CHATCRED APP" and it is submitted to the Quaid-e-Awam University of Engineering. Science & Technology Nawabshah for the Degree of Bachelor of Science in Information Technology.

Dr. Saima Siraj Soomro Prof. Dr. Mukhtiar Ahmed Memon

External Examiner

# ACKNOWLEDGE

# We extend our heartfelt gratitude to Dr. Saim Siraj Soomro, our supervisor, for her unwavering support in choosing our project topic.

* Her guidance and encouragement were instrumental in our decision-making process throughout the selection of our project idea, leading us to a successful outcome.
* We appreciate our supervisor at Quaid-E-Awam University of Engineering, Science and Technology Nawabshah for her steadfast assistance and direction with our FYP.
* Additionally, we would like to express our thanks to Dr. Saima Siraj Soomro for her support and guidance at various stages, from the research proposal to the final project idea selection.

# DEDICATION

Dedications to **ALLAH SWT**

With blessings, love, and respect for those who helped us reach the level of excellence at which we are all now, we look forward to a bright future.

&

To our respected

#### PARENTS

##### & respected TEACHERS

For their unconditional support & encouragement & inspiration that made us able for this thesis work.

# DECLARATION

I hereby declare that this thesis titled "Image Steganography" is my original work and has not been submitted previously for any academic degree. All the work presented in this thesis has been carried out by me, except where due acknowledgment is made in the text.

I further declare that:

The data, results, and conclusions presented in this thesis are based on my personal research and have been conducted in compliance with academic and ethical standards.

Any sources of information, data, or material used in the completion of this thesis have been properly cited and referenced.

The guidance and support provided by my supervisor, Dr. Saim Siraj Soomro, have been duly acknowledged.

I understand that any violation of this declaration may result in disciplinary actions and affect the recognition of this thesis.

Signed,

[Your Name]

[Your Student ID]

[Department]

Quaid-E-Awam University of Engineering, Science and Technology Nawabshah

[Date]

**Table of Contents**

###### [. I-1](#_bookmark0)

[QUAID-E-AWAM UNIVERSITY OF ENGINEERING, SCIENCE & TECHNOLOGY NAWABSHAH ......... I-1](#_bookmark1) [(DEPARTMENT OF INFORMATION TECHNOLOGY) ......................................................................... I-1](#_bookmark2)

[Group Members: Ubaidullah Qureshi(Group leader 20IT-16)........................................................I-1](#_bookmark3) [Waqas Rajput (20IT-16)................................................................................................................. I-1](#_bookmark4)

[Savera Khan (20IT-64) .................................................................................................................... I-1](#_bookmark5)

[SUPERVISED BY: Dr. Saima Siraj Soomro . ................................................................................ I-1](#_bookmark7)

1. [Introduction........................................................................................................................... I-8](#_bookmark8)
   1. [PROBLEM STATEMENT: ..................................................................................................... I-9](#_bookmark9)
   2. [OBJECTIVES...................................................................................................................... I-10](#_bookmark10)
2. [LITRATURE REVIEW ............................................................................................................ II-11](#_bookmark11)
   1. [Security Considerations........................................................................................................ II-11](#_bookmark12)
   2. [User Experience Considerations .......................................................................................... II-11](#_bookmark13)
   3. [Cross-Platform Compatibility: .............................................................................................. II-12](#_bookmark14)

###### [METHODOLOGY............................................................................................................. III-13](#_bookmark15)

* 1. [Requirements Gathering: .................................................................................................... III-13](#_bookmark16)
  2. [Design: ................................................................................................................................. III-13](#_bookmark17)
     1. [Visual Studio Code............................................................................................................ III-14](#_bookmark18)
     2. [Expo .................................................................................................................................. III-14](#_bookmark19)
     3. [React Navigation............................................................................................................... III-14](#_bookmark20)
     4. [Firebase ........................................................................................................................... III-14](#_bookmark21)
  3. [Development ...................................................................................................................... III-14](#_bookmark22)
  4. [Testing: ................................................................................................................................ III-15](#_bookmark23)
  5. [Project Wrap-Up ................................................................................................................. III-15](#_bookmark24)
  6. [Security Future Development ............................................................................................. III-16](#_bookmark25)

###### [USE CASE DIAGRAM: ..................................................................................................... III-18](#_bookmark26)

1. [Figure 3.1: LOGIN SCREEN Case Diagram .................................................................. III-18](#_bookmark27)
2. [Figure 3.2: SIGNUP SCREEN Use Case Diagram ......................................................... III-19](#_bookmark28)

###### [................................................................................................................................................... III-20](#_bookmark29)

1. [Figure 3.3: CHAT SCREEN Use Case Diagram............................................................. III-20](#_bookmark30)

###### [. I-21](#_bookmark31)

1. [Figure 3.4: BANK Use Case Diagram.......................................................................... III-21](#_bookmark32)
2. [Figure 3.5: Settings Screen Use Case Diagram ......................................................... III-21](#_bookmark33)

###### [SNAPSHOTS OF DATABASE............................................................................................ III-24](#_bookmark34)

[Figure 3.6: Chat record.............................................................................................................. III-24](#_bookmark35)

###### [RESULTS ......................................................................................................................... IV-25](#_bookmark36)

* 1. [Demographic Information ................................................................................................... IV-25](#_bookmark37)
     1. [Gender.............................................................................................................................. IV-25](#_bookmark38)
     2. [Age.................................................................................................................................... IV-26](#_bookmark39)
     3. [Location ............................................................................................................................ IV-26](#_bookmark40)
  2. [Perception of ChatCred App Concept ................................................................................. IV-26](#_bookmark41)
     1. [Based on the Brief Description, How Useful Does ChatCred Sound to You? ................... IV-26](#_bookmark42)
     2. [Willingness to Try ChatCred Once It Is Launched............................................................. IV-26](#_bookmark43)
  3. [Taking a Close Look at How People Feel About ChatCred: ........................................... IV-27](#_bookmark44) [Figure 4.2.1: Performance chart................................................................................................ IV-28](#_bookmark45)
  4. [Snapshots of application ............................................................................................... IV-29](#_bookmark46)

[Figure 4.3.1: Login and Signup screens ..................................................................................... IV-29](#_bookmark47)

[Figure 4.3.2: Main Screen and Chat screen............................................................................... IV-30](#_bookmark48)

[Figure 4.3.3: Select Bank and Login Bank Screen ...................................................................... IV-31](#_bookmark49) [Figure 4.3.4: Bank Screens ........................................................................................................ IV-32](#_bookmark50)

[Figure 4.3.5: Setting screen (logout) ......................................................................................... IV-33](#_bookmark51)

1. [CODE................................................................................................................................... V-34](#_bookmark52)
   1. [LOGIN CODE ............................................................................................................... V-34](#_bookmark53)
   2. [CHAT SCREEN.............................................................................................................. V-37](#_bookmark54)
   3. [Banking code .............................................................................................................. V-43](#_bookmark55)
2. [CONCLUSION ................................................................................................................. VI-52](#_bookmark56)

## Chapter 1: Introduction

### 1.1 Overview of Steganography

* Definition and history
* Difference between steganography and encryption
* Applications and importance in modern communication

### 1.2 Problem Statement

* The need for undetectable communication methods
* Limitations of traditional encryption
* Relevance in the current digital landscape

### 1.3 Objectives

* Development of a robust steganographic algorithm
* Ensuring undetectable embedding of messages
* Creating a user-friendly application

### 1.4 Significance

* Enhancing secure communication
* Protection of digital privacy
* Contribution to information security field

### 1.5 Structure of the Thesis

* Brief overview of each chapter

## Chapter 2: Literature Review

### 2.1 Historical Background

* Early methods of steganography
* Evolution in the digital age

### 2.2 Existing Steganography Techniques

* Overview of common techniques: LSB, DCT, Spread Spectrum
* Comparative analysis

### 2.3 Related Work

* Review of significant research papers
* Innovations and limitations in previous studies

### 2.4 Gaps in Current Research

* Identified challenges and areas for improvement

## Chapter 3: Methodology

### 3.1 Theoretical Framework

* Underlying principles of steganography
* Rationale for chosen methodology

### 3.2 Proposed Algorithm

* Compression, encryption, and embedding process
* Detailed steps and flowcharts

### 3.3 Tools and Technologies

* Software and hardware used
* Justification for their selection

### 3.4 Implementation Plan

* Step-by-step development process
* Milestones and timelines

## Chapter 4: Design and Development

### 4.1 System Architecture

* High-level design of the system
* Components and their interactions

### 4.2 User Interface Design

* Design principles
* Wireframes and mockups

### 4.3 Encoding Algorithm

* Detailed implementation of compression, encryption, and LSB embedding

### 4.4 Decoding Algorithm

* Detailed implementation of LSB decoding, decryption, and decompression

## Chapter 5: Implementation

### 5.1 Development Environment

* Setup and configuration
* Development tools and IDEs

### 5.2 Coding

* Key code snippets and explanations
* Handling errors and exceptions

### 5.3 Integration

* Combining encoding and decoding modules
* Ensuring seamless functionality

### 5.4 Testing

* Test cases and scenarios
* Unit testing, integration testing, and system testing

## Chapter 6: Results and Analysis

### 6.1 Encoding Performance

* Efficiency and speed of encoding process
* Comparison with existing techniques

### 6.2 Decoding Accuracy

* Success rate of message retrieval
* Error rates and mitigation strategies

### 6.3 Security Analysis

* Robustness against detection and attacks
* Comparative security analysis

### 6.4 User Feedback

* Usability testing results
* User satisfaction and suggestions

## Chapter 7: Discussion

### 7.1 Interpretation of Results

* Insights gained from performance and security analysis
* Implications for real-world applications

### 7.2 Limitations

* Identified weaknesses and constraints
* Factors affecting performance and security

### 7.3 Recommendations

* Improvements for future research
* Practical recommendations for users

## Chapter 8: Conclusion

### 8.1 Summary of Findings

* Recap of key results and achievements

### 8.2 Contributions to the Field

* Novel aspects and advancements made

### 8.3 Future Work

* Suggested areas for further research
* Potential developments in steganography

## Chapter 9: References

### 9.1 Bibliography

* Comprehensive list of all sources cited

### 9.2 Additional Reading

* Suggested readings for deeper understanding

## Chapter 10: Appendices

### 10.1 Code Listings

* Complete source code of the project

### 10.2 User Manual

* Instructions for using the developed application

### 10.3 Additional Figures and Tables

* Supplementary data and illustrations

### 10.4 Glossary

* Definitions of technical terms and concepts used in the thesis

By structuring the thesis in this manner, readers will gain a comprehensive understanding of image steganography, from theoretical foundations to practical implementation and analysis, providing a robust framework for further research and application in the field.

# CHAPTER 1: INTRODUCTION

**Abstract**

Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme .

# **1.1 Problem Statement**

# In an era where digital communication is ubiquitous, the need for secure and private communication channels is paramount. Traditional encryption methods, while effective in protecting the contents of a message, often signal the presence of sensitive information, potentially attracting unwanted attention. Steganography offers an additional layer of security by obscuring the existence of the message itself. However, developing a steganographic method that is both secure and undetectable presents significant challenges. This thesis addresses these challenges by proposing a robust algorithm for image steganography, aimed at enhancing the security and undetectability of hidden messages.

# **1.2 Objectives**

# The primary objectives of this thesis are:

# To develop an efficient and secure image steganography algorithm that minimizes the detectability of hidden messages.

# To integrate compression and encryption techniques to enhance the security of the steganographic process.

# To create a user-friendly application that allows for easy encoding and decoding of messages within digital images.

# To evaluate the performance and security of the proposed algorithm through rigorous testing and analysis.

# **1.3 Significance**

# The significance of this research lies in its potential to advance the field of information security. By developing a novel steganographic algorithm that effectively hides the presence of a message, this research contributes to the protection of digital privacy and secure communication. The proposed method's integration of compression and encryption techniques aims to provide a comprehensive solution that addresses both security and efficiency. Moreover, the development of a user-friendly application ensures practical applicability, making it accessible for everyday use.

# **1.4 Structure of the Thesis**

# This thesis is organized into ten chapters, each focusing on different aspects of the research:

# **Chapter 1:** Introduction - Provides an overview of steganography, the problem statement, objectives, significance, and structure of the thesis.

# **Chapter 2:** Literature Review - Reviews the history of steganography, existing techniques, related work, and identifies gaps in current research.

# **Chapter 3:** Methodology - Describes the theoretical framework, proposed algorithm, tools and technologies, and implementation plan.

# **Chapter 4:** Design and Development - Details the system architecture, user interface design, encoding algorithm, and decoding algorithm.

# **Chapter 5:** Implementation - Covers the development environment, coding, integration, and testing processes.

# **Chapter 6:** Results and Analysis - Presents the performance of the encoding process, accuracy of decoding, security analysis, and user feedback.

# **Chapter 7:** Discussion - Interprets the results, discusses limitations, and provides recommendations for future research.

# **Chapter 8:** Conclusion - Summarizes findings, contributions to the field, and future work.

# **Chapter 9**: References - Lists all sources cited in the thesis.

# **Chapter 10:** Appendices - Includes code listings, user manual, additional figures and tables, and a glossary of technical terms.

**Chapter 2: Literature Review**

**2.1 Historical Background**

* **Early Methods of Steganography**

Steganography has a rich history that dates back to ancient civilizations. Early methods included writing messages on wooden tablets and then covering them with wax, tattooing messages on the shaved heads of messengers, and using invisible ink made from substances like lemon juice. These techniques relied on physical media and manual processes, which were effective for their time but limited by the materials and knowledge available.

* **Evolution in the Digital Age**

The advent of digital technology revolutionized steganography. With the development of computers and digital communication, new methods emerged that could embed information within digital files such as images, audio, and video. Digital steganography leverages the vast amount of data and the redundancy in digital media to hide information in ways that are imperceptible to human senses and difficult to detect with automated tools. This evolution has made steganography more versatile and secure, adapting it to modern communication needs.

**2.2 Existing Steganography Techniques**

**Overview of Common Techniques**

1. **Least Significant Bit (LSB) Embedding:** This technique involves modifying the least significant bits of the pixels in an image to embed the secret message. Since these bits contribute minimally to the overall appearance of the image, the changes are usually imperceptible.
2. **Discrete Cosine Transform (DCT):** Used primarily in JPEG images, this technique involves modifying the DCT coefficients of the image. The changes are made in the frequency domain, which can provide better robustness against various image processing operations.
3. **Spread Spectrum:** This technique spreads the hidden information across a large bandwidth, making it more resilient to noise and interference. It is similar to methods used in secure wireless communications.

**Comparative Analysis**

Each of these techniques has its strengths and weaknesses. LSB embedding is simple and efficient but may be vulnerable to detection and extraction. DCT-based methods offer better robustness but are more complex to implement. Spread spectrum techniques provide high security but may require more computational resources and can impact the quality of the host media. The choice of technique depends on the specific requirements of the application, such as the desired balance between security, robustness, and complexity.

**2.3 Related Work**

**Review of Significant Research Papers**

A considerable body of research has been conducted on steganography, exploring various methods and their applications. For example, Rosziati Ibrahim and Teoh Suk Kuan (2011) proposed a method that combines compression and encryption with LSB embedding to enhance security and reduce detectability. Other significant studies have explored the use of wavelet transforms, adaptive algorithms, and hybrid approaches that combine multiple techniques.

**Innovations and Limitations in Previous Studies**

While these studies have contributed valuable insights and advancements, they also have limitations. Many focus on specific types of media or attack scenarios, and few provide comprehensive solutions that address both security and usability. Some methods, while highly secure, are computationally intensive or result in noticeable degradation of the host media. Others may be susceptible to sophisticated detection techniques or fail to provide adequate robustness against various types of image processing.

**2.4 Gaps in Current Research**

**Identified Challenges and Areas for Improvement**

Despite the progress made in the field of steganography, several challenges remain. These include:

* **Detectability:** Ensuring that the presence of hidden messages is undetectable by both visual inspection and statistical analysis.
* **Robustness**: Developing methods that can withstand various types of image processing, such as compression, resizing, and cropping.
* **Security:** Enhancing the security of the hidden messages against extraction or tampering by unauthorized parties.
* **Efficiency:** Balancing the trade-offs between security, robustness, and computational efficiency to create practical, real-world applications.

**Chapter 3: Methodology**

**3.1 Theoretical Framework**

* **Underlying Principles of Steganography**

Steganography is the practice of hiding a secret message within a non-suspicious carrier, such as an image, in such a way that the presence of the message is not detectable. The main principles involve:

1. **Imperceptibility:** The hidden message should not be noticeable within the carrier medium.
2. **Robustness**: The hidden message should remain intact even if the carrier medium undergoes transformations such as compression or resizing.
3. **Capacity:** The carrier medium should have enough space to hide the desired amount of data without degrading the quality of the medium.

* **Rationale for Chosen Methodology**

The chosen methodology combines the strengths of existing steganographic techniques while addressing their limitations. By integrating compression, encryption, and LSB embedding, the proposed algorithm aims to enhance security and robustness without compromising the imperceptibility of the hidden message.

**This approach leverages the following rationale:**

1. Compression reduces the size of the secret message, making it harder to detect and easier to embed.
2. Encryption ensures that even if the hidden message is discovered, it cannot be read without the secret key.
3. LSB Embedding is chosen for its simplicity and minimal impact on the carrier image’s appearance, making the hidden message imperceptible to human eyes.

**3.2 Proposed Algorithm**

**Compression, Encryption, and Embedding Process**

The proposed algorithm involves three main processes: compression, encryption, and embedding. These processes are executed in the following steps:

1. **Compression:** The secret message is compressed to reduce its size and make it less detectable.
   1. **Input:** Secret message
   2. **Output**: Compressed message
2. **Encryption:** The compressed message is encrypted using a secret key to ensure its confidentiality
   1. **Input:** Compressed message, secret key
   2. **Output:** Encrypted message
3. **LSB Embedding:** The encrypted message is embedded into the least significant bits of the pixels in the carrier image.
   1. **Input:** Encrypted message, carrier image
   2. **Output:** Stego-image (image with embedded message)

**The algorithm can be visualized with the following flowchart:**

|  |
| --- |
| **Start**  **|**  **v**  **Compress the secret message**  **|**  **v**  **Encrypt the compressed message with the secret key**  **|**  **v**  **Embed the encrypted message into the LSB of the carrier image pixels**  **|**  **v**  **Output the stego-image**  **|**  **End** |

**3.3 Tools and Technologies**

* **Software and Hardware Used**

**Software:**

1. **Java:** For developing the steganography application due to its platform independence and robust libraries.
2. **Android Studio:** For building and testing the mobile application.
3. **OpenCV:** For image processing tasks.
4. **Git:** For version control.

**Hardware:**

1. **Development Machine:** High-performance laptop/desktop for development and testing.
2. **Android Device:** For testing the mobile application in real-world scenarios.

**Justification for Their Selection**

1. **Java:** Chosen for its extensive library support and ease of integration with Android.
2. **Android Studio**: The official integrated development environment (IDE) for Android application development, providing comprehensive tools for coding, debugging, and testing.
3. **OpenCV:** A powerful library for real-time computer vision tasks, essential for efficient image processing.
4. **Git:** Ensures efficient version control and collaborative development.

**3.4 Implementation Plan**

Step-by-Step Development Process

1. **Requirement Analysis:**
   1. Identify the functional and non-functional requirements.
   2. Define the scope of the project.
2. **Design:**
   1. Create the architecture and design the algorithm.
   2. Develop flowcharts and diagrams to visualize the process.
3. **Development:**
   1. Implement the compression, encryption, and embedding algorithms in Java.
   2. Integrate the algorithms into an Android application using Android Studio.
   3. Implement user interfaces for encoding and decoding messages.
4. **Testing:**
   1. Perform unit testing to ensure each component works correctly.
   2. Conduct integration testing to ensure the system works as a whole.
   3. Test the application on various Android devices to ensure compatibility.
5. **Deployment:**
   1. Prepare the application for release.
   2. Deploy the application to the Google Play Store or other distribution platforms.

**Milestones and Timelines**

**Month 1-2:** Requirement analysis and design.

**Month 3-5:** Development of compression, encryption, and embedding algorithms.

**Month 6:** Integration into Android application.

**Month 7:** Testing and debugging.

**Month 8:** Deployment and documentation.