iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: V Month of publication: May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81729

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

# Quietly: A Media-Based Private Messaging App

Saksham[1], Om Shukla[2], Er. Shubham Kumar[3]
*Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Shri Ramswaroop Memorial College of Engineering and Management (SRMCEM) Lucknow, India*

***Abstract: With the rapid growth of digital communication, protecting user privacy has become one of the most important concerns in cybersecurity. Traditional messaging applications mainly rely on encryption techniques, which may still reveal the existence of communication even if the content remains unreadable. This project presents "Quietly," a media-based private messaging application that uses steganography techniques to hide secret messages inside digital media files such as images and audio. The application provides an additional layer of security by concealing the presence of communication itself. The proposed system is developed as an Android-based application with a simple and secure user interface. Users can embed confidential text messages inside media files using steganographic algorithms and share them publicly without raising suspicion. A unique secret key is used for encoding and decoding the hidden message, ensuring that only authorized users can access the information. The application follows a modular and lightweight software architecture to improve performance and scalability. The system aims to provide secure communication for users in public or unsecured environments while maintaining ease of use. Experimental analysis demonstrates that the hidden messages remain visually undetectable and can be successfully recovered using the correct key. The project highlights the effectiveness of combining cybersecurity and steganography concepts in mobile communication systems. Future improvements may include AI-based steganography, cloud integration, and multi-media support for enhanced privacy and security.***

## I. INTRODUCTION

In the modern digital era, messaging applications have become an essential part of daily communication. Millions of users exchange personal, financial, and confidential information through online platforms every day. Although encryption technologies protect message content, attackers can still detect that communication is taking place. This creates a privacy concern in sensitive communications.

Steganography is a cybersecurity technique used to hide secret information within another digital medium such as images, audio, or video. Unlike encryption, which only scrambles the data, steganography conceals the existence of the message itself. This makes it highly useful in secure communication systems.

The proposed project, **"Quietly,"** is an Android-based private messaging application designed to hide messages inside media files. Users can encode secret text into an image or audio file and send it through any public platform. The receiver can decode the message only with the correct secret key. This method provides dual protection through both hidden communication and key-based access control.

The application is developed using a modular software architecture and focuses on simplicity, usability, and privacy. The project demonstrates how cybersecurity concepts can be integrated into mobile applications to improve secure communication in real-world scenarios

## II. LITERATURE REVIEW

Steganography has been widely studied as a method for secure data communication. Researchers have explored different techniques for hiding information inside multimedia files while maintaining media quality and reducing detectability.

Early steganography methods focused mainly on image processing techniques such as Least Significant Bit (LSB) substitution. LSB techniques modify the smallest bits of image pixels to store hidden data without significantly affecting image quality. These methods are simple and efficient but may be vulnerable to image processing attacks.

Several researchers proposed audio steganography methods where secret data is hidden inside audio frequencies. Audio-based approaches provide higher data capacity and better resistance to detection compared to basic image steganography methods. However, they may increase computational complexity.

Mobile-based secure communication applications have also gained popularity due to the increasing use of smartphones. Android provides an efficient platform for implementing secure messaging systems because of its flexibility, open-source environment, and multimedia support.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

## III. METHODOLOGY

The proposed system follows a modular approach for secure message transmission using steganography techniques. The system architecture consists of the following modules:

### A. *User Authentication Module*

This module allows users to access the application securely. Basic authentication methods are used to protect user access and prevent unauthorized usage.

### B. *Message Encoding Module*

The sender enters a secret message and selects a media file such as an image or audio file. The system applies steganography algorithms to embed the hidden text inside the selected media.

The encoding process includes:

- Selecting cover media
- Entering secret text
- Applying secret key
- Embedding message into media
- Generating stego-media output

### C. *Secret Key Module*

A unique key is generated or manually entered during the encoding process. This key is required during decoding to retrieve the original message securely.

### D. *Message Decoding Module*

The receiver uploads the stego-media file into the application and enters the correct secret key. The system extracts the hidden data and displays the original message.

### E. *Android Application Framework*

The application is developed using Android technologies with a lightweight and user-friendly interface. The system architecture ensures modularity and efficient performance.

Working Process

- User selects media file.
- Secret message is entered.
- Secret key is applied.
- Message is hidden inside media.
- Stego-media is shared publicly.
- Receiver uploads media and enters key.
- Hidden message is extracted successfully.

## IV. RESULTS AND DISCUSSION

The developed application successfully demonstrates secure communication using media-based steganography techniques. Messages were embedded inside image and audio files without noticeable changes in media quality.

The experimental results show that:

1) Hidden messages remain visually undetectable.
2) The decoding process works accurately using the correct secret key.
3) Unauthorized users cannot retrieve the message without the key.
4) The Android interface remains simple and user-friendly.

Performance analysis indicates that image-based steganography provides fast execution and efficient storage utilization. Audio-based hiding methods support larger data capacity while maintaining acceptable audio quality.

The project successfully combines cybersecurity principles with mobile application development to provide enhanced privacy during communication. The modular architecture also improves maintainability and scalability for future development.

Some limitations observed include:
1) Large hidden messages may slightly affect media size.
2) Basic steganography methods may be vulnerable to advanced steganalysis attacks.
3) Media compression may reduce message recovery accuracy.

Despite these limitations, the proposed system provides an effective and practical solution for secure communication in public environments.

## V. CONCLUSION AND FUTURE WORK

The project "Quietly: A Media-Based Private Messaging App" presents an effective solution for secure communication using steganography techniques. The application hides secret messages inside digital media files and provides key-based decoding for authorized access. Unlike traditional messaging systems, the proposed approach conceals the existence of communication itself, thereby improving user privacy and security.

The Android-based implementation demonstrates that steganography can be integrated successfully into modern mobile applications with minimal complexity and efficient performance. The system achieves secure message transmission while maintaining simplicity and usability.

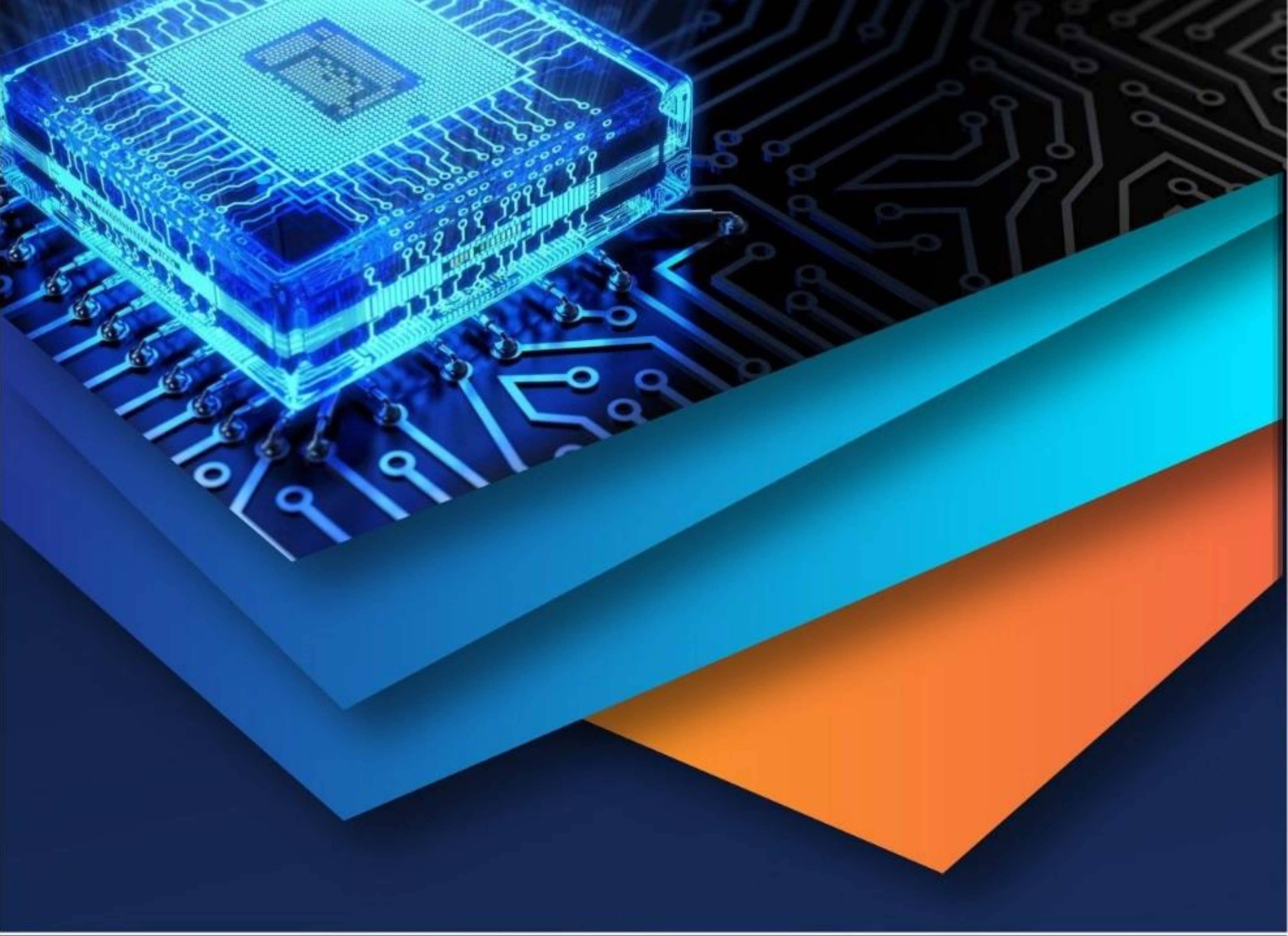
### *A. Future Work*

The project can be enhanced further by implementing:
1) AI-based intelligent steganography methods
2) Video steganography support
3) End-to-end encryption integration
4) Cloud storage and synchronization
5) Multi-user secure communication
6) Biometric authentication for decoding
7) Advanced anti-steganalysis protection

These improvements can increase security, scalability, and real-world applicability of the system.

## REFERENCES

[1] "Steganography." Wikipedia Available: https://en.wikipedia.org/wiki/Steganography
[2] Google "Android Developers Documentation." Available: https://developer.android.com
[3] OpenAI "ChatGPT." Available: https://chat.openai.com
[4] Johnson, N. F., and Jajodia, S., "Exploring Steganography: Seeing the Unseen," IEEE Computer Journal, vol. 31, no. 2, pp. 26–34, 1998.
[5] Katzenbeisser, S., and Petitcolas, F., Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000.
[6] Provos, N., and Honeyman, P., "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY