© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717721

# Forensic and Cryptic Communication

RESHAM K S[1], HITHESH GOWDA PM[2], KRISHNA R[3], RAKSHITH S[4], ARNOLD S[5]
[1]*Asst Professor, Department of Computer Science & Engineering Mysuru Royal Institute of Technology, Mandya, Karnataka, India.*
[2,3,4,5] *Student, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India.*

***Abstract-*** ***Forensic cryptic communication refers to the identification, analysis, and interpretation of hidden, encrypted, or disguised communication used in digital environments. With the rapid advancement of communication technologies, cybercriminals increasingly use encryption, steganography, coded language, and anonymous platforms to conceal illegal activities. This paper presents a comprehensive study of cryptographic techniques, steganography, forensic communication analysis, and modern tools used in digital investigations. It also highlights challenges such as end-to-end encryption, dark web anonymity, and lack of standardized analysis frameworks. The study proposes an integrated forensic approach combining cryptanalysis, steganalysis, and behavioural analysis to improve the detection of cryptic communication.***

***Index Terms: Cryptography, Steganography, Digital Forensics, Cryptanalysis, Communication Analysis, Cybercrime***

## I. INTRODUCTION

Digital communication has become a fundamental part of modern life. However, it has also created opportunities for cybercriminals to hide illegal activities using cryptic communication techniques. These techniques include encryption, steganography, coded symbols, emojis, and anonymous messaging platforms. Forensic cryptic communication focuses on detecting and interpreting such hidden messages to support cybercrime investigations. Traditional forensic approaches are often insufficient due to strong encryption and advanced hiding techniques. Therefore, modern forensic systems must integrate multiple analysis techniques to effectively identify hidden communication.

## II. PROBLEM STATEMENT

One of the reasons that intruders can be successful is that most of the information they acquire can be read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media, but adding large amount of data using steganography is not possible and less secure. In our project we use the sparse encoding and Reversible Data Hiding (RDH) in encrypted images to pay attention for privacy, security and protection, to provide a way to store large amount of data, and also hide the original image. So that the data hidden as well as the original image are both secure. Also to better explore the correlation between neighbour pixels, we propose to consider the patch-level sparse representation when hiding the secret data.

## III. OBJECTIVES

The objective of this project, Data Hiding in Encrypted Images Using Patch-Level Sparse Representation, is to develop a secure and efficient technique for embedding secret information within encrypted images. The method aims to provide a large capacity for data hiding while ensuring perfect recovery of both the secret data and the original cover image. This approach is highly relevant in military, medical, and legal applications where even the smallest loss of information is unacceptable. With growing concerns about privacy, cover owners often encrypt images before transferring them to data managers. At the same time, data managers may need to embed authentication information or steganographic messages without having access to the original image content. This project addresses this need by enabling data hiding directly within encrypted images. The proposed approach creates a sparse domain by compressing the LSBs of the encrypted image, which provides additional space for

embedded data. The goal is to ensure secure transmission of information through cloud platforms without fear of data leakage, hacking, or unauthorized access.

- To study cryptographic techniques used in secure communication
- To analyze steganography methods for hidden data
- To examine forensic techniques for communication analysis
- To evaluate tools used in cryptanalysis and steganalysis
- To design a system for detecting cryptic communication
- To identify challenges and research gaps

## IV. METHODOLOGY

1.User Interface Design: The application interface is designed in a simple way, so that the user interaction with the application is not cumbersome. To connect with application, user must give their valid username and password only than the user is able to connect to the application. If the user already exits he can directly login into the application, else user must register their details such as username, password and Email id, into the application.

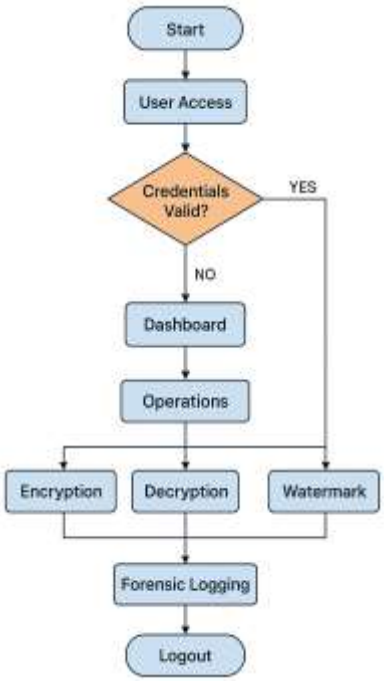
2.Generate Hash Value Using SHA 256 Module: The Secure Hash Algorithm 256 is a computer security cryptographic algorithm. The SHA-256 compression function operates on a 512-bit message block and a 256-bit intermediate hash value. It is essentially a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key.

3.Reversible data hiding Module: This module works in the receiver side of the application. Once the receiver provides the valid hash key received through his e-mail, all the encoding process done in the sender side will be reversed in the receiver side, it decodes and provides the hidden data.

## V. SYSTEM ARCHITECTURE

The system architecture defines how various modules interact to provide secure message transmission and forensic traceability. The architecture is divided into four main functional layers:

1User Interaction Layer Provides the interface for sending and receiving messages. Allows user login/registration, message input, and file upload. Cryptographic Layer Performs encryption and decryption of the message. Implements hybrid cryptographic logic (substitution, confidentiality and message integrity. Steganography / Data Hiding Layer • Embeds encrypted text into a cover medium (image, text container, etc.). Uses simple LSB or bit-manipulation-based hiding for secure covert communication. Extracts hidden data during message retrieval. Forensic Tracking & Logging Layer Captures metadata such as timestamp, user ID, hash values, and message signatures. Generates logs used for digital forensic investigation. Tracks message flow from sender to receiver.




## VI. KEY TECHNOLOGIES

A. Cryptography Symmetric (AES, DES)
- Asymmetric (RSA, ECC)
- Hashing (SHA-256, MD5)

B. Steganography Image-based hiding (LSB)
- Audio/video hiding

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717721

- Text-based hiding

C. Communication Forensics Email header analysis
- Email header analysis
- Social media monitoring
- Network packet analysis

## VII. TOOLS USED

- Autopsy / EnCase – Disk forensics
- Wireshark – Network analysis
- Hashcat – Password cracking
- StegExpose – Steganography detection
- Cellebrite UFED – Mobile forensics

## VIII. APPLICATIONS

- Terrorist communication tracking
- Fraud detection
- Digital evidence analysis
- Law enforcement intelligence

## IX. CHALLENGES

- Dark web anonymity
- Large volume of data
- Lack of standardized frameworks
- Difficulty in detecting social media steganography

## X. FUTURE SCOPE

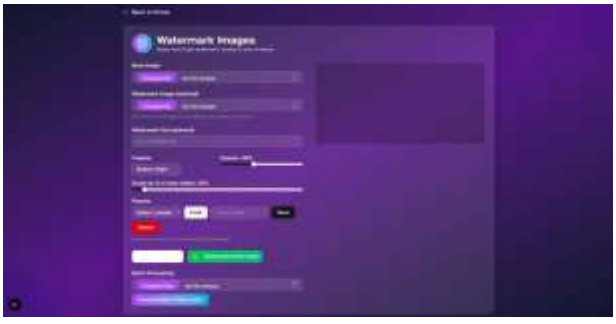
- AI-based cryptic communication detection
- Advanced steganalysis tools
- Real-time forensic monitoring systems
- Integration with cloud forensics

A comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation. The implemented Reversible method can be enhanced in future by using the following provisions after embedding, when there is lot of change in the pixel to retain nearest original value and also we improve the security in Sparse encoding system, suppose the user want to send his data to one user through Gmail id and it prevents malicious user.

## XI. CONCLUSION

This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file. The main aim of this project is to provide a wide range of security to the user so that they can send the data through cloud to any user without the fear of hacking their data. The data or information is hided in a image and the image is completely split into number of pieces as desired by the user and then the data is split into parts and stored in these parts of the image and then randomly merged and then combined and a cover image is added to that image and is encrypted and a key is generated. The user can now send this image to the other user in the cloud and the key is sent through mail. So the other user can access the data.





© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717721

REFERENCE

[1] Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2020.

[2] Menezes, A., van Oorschot, P., & Vanstone, S. Handbook of Applied Cryptography. CRC Press, 2018.

[3] Bishop, M. Introduction to Computer Security. Addison-Wesley, 2019.

[4] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2019.

[5] Garfinkel, S. L. "Digital Forensics Research: The Next 10 Years." Digital Investigation, vol. 7, 2020.

[6] Provos, N., & Honeyman, P. "Hide and Seek: An Introduction to Steganography." IEEE Security & Privacy, 2018.

[7] Johnson, N. F., Duric, Z., & Jajodia, S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures. Springer, 2021.

[8] Kessler, G. C. "An Overview of Cryptanalysis." Journal of Digital Forensics, Security and Law, 2020.

[9] Singhal, N., & Raina, J. "Comparative Analysis of AES and RSA Algorithms." International Journal of Computer Science, 2021.

[10] Liu, H., & Sung, A. "A Comparative Study of Text Steganography Techniques." Journal of Information Security, 2019.

[11] Zawoad, S., & Hasan, R. "Digital Forensics in the Cloud: Challenges and Research Directions." ACM Computing Surveys, 2022.

[12] Reith, M., Carr, C., & Gunsch, G. "An Examination of Digital Forensic Models." International Journal of Digital Evidence, 2020.

[13] Bhavsar, R. & Waghmare, P. "Steganalysis Techniques for Digital Images." IEEE Access, 2019.

[14] NIST. "Guide to Integrating Forensic Techniques into Incident Response." NIST SP 800-86, 2021.