WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Chat Application with Image Steganography and Real-Time Collaboration Features: A Review

[1] Anthony Anup, [2] Bhoma P, [3] Nandan M, [4] Shakthi T L, [5] Dr Anitha D B

[1,2,3,4] Student, Department of CSE (Data Science), ATME College of Engineering, Mysuru, Karnataka, India
[5] Head of Department, Department of CSE (Data Science), ATME College of Engineering, Mysuru, Karnataka, India

ABSTRACT:

This review paper explores the intersection of secure chat applications, image steganography, and real-time collaboration features. In today's digital landscape, safeguarding user privacy and data integrity in online communication has become a critical necessity. Steganography, the art of concealing messages within seemingly innocuous digital media, provides a unique layer of covertness by hiding the existence of the message itself, unlike traditional cryptography which only scrambles the message content. This paper surveys current advancements in secure chat platforms and image steganography techniques, including Least Significant Bit (LSB) algorithms and various transform domain approaches. Methodologies for both secure messaging applications and real-time chat platforms are analyzed, with attention to their architectural designs, security protocols such as AES and RSA, and user functionalities. The key finding reveals a notable research gap: while individual components are highly developed, comprehensive systems that effectively integrate robust image steganography for covert communication with rich real-time collaboration features remain scarce. Existing secure chat applications predominantly rely on cryptographic encryption alone, overlooking the added privacy afforded by steganography's ability to conceal message existence, while steganography implementations often lack the full spectrum of real-time collaboration functionalities. This review identifies the technical and practical challenges in bridging this gap and underscores the novelty and necessity of developing an integrated solution that prioritizes both covertness and seamless real-time interaction.

Keywords: Image Steganography, Secure Chat, Data Privacy, Real-Time Collaboration, Screen Sharing

1. INTRODUCTION

The pervasive nature of digital communication in the modern era has made secure and private online interactions an indispensable necessity. From personal conversations to sensitive corporate and governmental exchanges, the integrity and confidentiality of transmitted information are constantly under threat from cyber-attacks, eavesdropping, and unauthorized access. This escalating demand for robust security measures has propelled the evolution of protection techniques, primarily cryptography and steganography.

Cryptography, derived from Greek words meaning "confidential writing," transforms plaintext into unreadable ciphertext, ensuring that messages are indecipherable without the correct key. While highly effective in securing content, its visible scrambling often raises suspicion, inherently indicating the presence of sensitive information.

In contrast, steganography meaning "covered writing" is the art and science of concealing covert messages within seemingly innocuous digital media such as images, audio, or video files. Its paramount objective is imperceptibility, ensuring that the hidden message remains undetectable to unauthorized observers, thereby masking the very existence of the communication. This unique capability offers an additional layer of privacy, particularly crucial in scenarios demanding complete covertness. Some systems further enhance security by adopting a dual-layer approach that combines AES encryption with LSB-based steganography to strengthen confidentiality and integrity.

At the same time, real-time chat applications have revolutionized communication by enabling instant connections regardless of geographical boundaries. Platforms such as WhatsApp, Signal, and Slack have become integral to daily life, facilitating seamless text, image, and even video exchanges. However, these conventional chat platforms, while offering basic encryption, often fall short in providing the advanced, covert security that steganography can offer. Vulnerabilities ranging from data interception to identity theft underscore the continuous need for enhanced measures.

This review paper aims to comprehensively examine existing research and developed systems at the intersection of secure chat applications, image steganography, and real-time collaboration features. By analyzing methodologies, advantages, and limitations of current approaches, it identifies critical gaps in the literature and proposes a path toward more integrated and robust solutions for secure and covert real-time digital communication.

2. LITERATURE REVIEW

To understand the current landscape of secure chat applications integrated with steganography, it is essential to examine prior research across both domains. Existing studies have primarily focused either on enhancing the security and privacy of digital communication through cryptographic methods or on developing steganographic techniques for covert message transmission. Several researchers have proposed innovative architectures for chat platforms that emphasize encryption, scalability, and usability, while others have explored image steganography methods such as Least Significant Bit (LSB) substitution, frequency-domain transforms, and hybrid encryption-steganography models. By systematically reviewing these works, we can identify the strengths, limitations, and gaps in existing approaches, laying the foundation for designing a more comprehensive solution that integrates both secure real-time communication and covert data hiding. The following literature survey summarizes the key contributions, methodologies, and findings of notable studies in this field.

Paras Kumar et al. Introduces a web chat platform that integrates steganography using the Least Significant Bit (LSB) algorithm to conceal messages within images. It is developed with the MERN stack (MongoDB, Express.js, React.js, and Node.js) and leverages Socket.io for real-time communication. The application's architecture includes user authentication, real-time chat, steganography embedding, and database management with MongoDB. A key contribution of this work is embedding confidential messages within image files, making the hidden data imperceptible to observers. Its comparison with WhatsApp, Signal, Telegram, and Slack demonstrates the unique advantage of steganography in covert communication. Future improvements suggested include video chat, group chat, and more advanced embedding techniques.[1]

Nurhayati et al. Presents a solution that secures electronic messages by combining LSB steganography with Advanced Encryption Standard (AES). Messages are first encrypted using AES and then embedded into image pixels' least significant bits. The paper emphasizes criteria such as imperceptibility, fidelity, and recoverability. It demonstrates that the digital image quality remains nearly unchanged while the hidden messages are fully retrievable. This dual-layer approach provides a stronger defense, as even if the message is detected, AES encryption prevents unauthorized reading.[2]

Dr M.N Nachappa et al. Reviews different steganography techniques across image, audio, video, and text domains. It identifies digital images as the most effective carrier medium due to their ubiquity. Applications highlighted include secret communications, copyright protection, and feature tagging. Techniques such as Fractional Fourier Transform (FrFT), RC4-enhanced LSB, and Integer Wavelet Transform (IWT) are discussed. The review stresses key properties such as transparency, robustness, and payload capacity, along with the importance of stego-keys for secure extraction.[3]

Satish Singh et al. Focuses on developing a chat application emphasizing cryptographic security but without steganography. The system, built on Django for the backend and HTML, CSS, and JavaScript for the frontend, uses the N-TEA encryption algorithm for message protection. It supports both public and private chats, with encrypted messages transmitted and decrypted at the receiver's end. The paper stresses the necessity of encryption for real-time communication security and highlights threats such as identity theft and eavesdropping.[4]

SC Mataraarachchi et al. Developes a system for transmitting highly confidential messages, particularly targeting military and government use cases. It combines AES encryption with spatial-domain steganography and image processing. Encrypted text is converted into ciphertext, mapped onto pixel values, and transmitted as a random image. Even if intercepted, the message appears meaningless to outsiders. The system also includes secure key mapping, login, and user registration modules. It critiques existing messaging platforms like MSN Messenger, Yahoo Messenger, Facebook Messenger, and WhatsApp for their vulnerabilities and emphasizes the superior confidentiality of its hybrid model.[5]

S.Gomathi et al. Presents a dual-layer secure messaging platform combining AES encryption and LSB steganography. The methodology involves encrypting user messages with AES, embedding them into cover images or audio files, and transmitting them to recipients who can extract and decrypt them with a shared key. Evaluation metrics such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Bits Per Pixel (BPP) demonstrate that the system maintains high image quality while ensuring data security. The paper highlights its suitability for sensitive applications like military and corporate communication.[6]

Harrison Carranza et al. Details a chat system built with Python's Tkinter library. It employs RSA for key exchange and AES for message encryption, ensuring robust end-to-end security. The system architecture uses a client–server model where public keys are distributed by the server, and only recipients with matching private keys can decrypt the communication. A unique feature is the encrypted storage of chat history, making the saved files unreadable without the key. While the system demonstrates strong cryptographic practices, it does not incorporate steganography as an added security layer.[7]

Nargis Shaikh et al. Presents the design and implementation of a scalable chat application developed with the MERN stack. The platform offers real-time messaging, private chats, and user authentication using JWT. It also includes features like chat rooms, responsive design, and secure login mechanisms. The paper emphasizes the scalability of MERN-based applications and highlights improved performance through React.js and Node.js. However, despite its comprehensive chat functionalities, the system does not employ steganography, relying only on authentication and encryption.[8]

Nandhini Subramanina et al. Provides a survey of traditional and modern image steganography techniques. It contrasts steganography with cryptography, stressing that while cryptography conceals the content of a message, steganography hides its very existence. The paper reviews methods such as Least Significant Bit substitution and frequency-domain approaches, along with their strengths and weaknesses. It also discusses evaluation criteria such as imperceptibility, payload, and robustness. The review concludes that while many improvements have been made, challenges such as steganalysis resistance and balancing capacity with invisibility remain open issues.[9]

Mr.Sachin Bansal et al. Describes a chat application implemented using ReactJS on the frontend and Firebase on the backend. The application supports features such as user login, chat room creation, user blocking, message deletion, and real-time notifications. Its architecture uses bidirectional client–server communication, enabling messages to be broadcast instantly to all participants. The platform ensures smooth and user-friendly interaction but does not attempt to incorporate steganography or hybrid cryptographic models, instead depending on Firebase's built-in authentication and encryption mechanisms.[10]

Avantika Bisht et al. Surveys a wide range of image steganography methods, including LSB substitution and transform-domain methods like Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), and Discrete Cosine Transform (DCT). It highlights key advantages of image steganography, such as imperceptibility, robustness, and plausible deniability. The review also evaluates the performance of different methods using metrics like PSNR, MSE, and Structural Similarity Index (SSIM). While identifying promising approaches, it emphasizes the ongoing challenge of resisting advanced steganalysis attacks.[11]

[Mohammed A. Saleh .Provides a detailed classification of steganographic methods into spatial and transform domain categories. The paper discusses spatial methods such as LSB, Pixel Value Differencing (PVD), and Gray-Level Modification (GLM), and transform-domain methods like DCT and DWT. It also introduces modified LSB-based approaches such as LSBraille and MLSB that attempt to improve imperceptibility and security. The review highlights trade-offs between embedding capacity, security, and robustness, underscoring the need for balanced solutions in practical applications.[12]

3. OUTCOME OF LITERATURE REVIEW

The survey of existing works reveals that significant progress has been made independently in both secure chat applications and image steganography, though their integration is still limited.

In the domain of steganography, prior studies demonstrate how practical chat systems can embed secret messages in images using Least Significant Bit (LSB) methods. These works highlight that steganography can be applied in real-time systems, though scalability and feature expansion remain challenges. Other approaches confirm that combining cryptographic algorithms such as AES with LSB steganography enhances confidentiality. Even if hidden data is detected, the encrypted form of the message ensures that it remains unreadable without the correct key, providing a dual layer of protection. Comprehensive reviews of steganographic techniques further categorize them by parameters such as imperceptibility, robustness, and data payload. These studies establish that while many methods exist, trade-offs remain between invisibility and embedding capacity. Hybrid security models that integrate cryptography, steganography, and image processing demonstrate that layered mechanisms achieve higher resistance to interception compared to traditional encrypted messaging platforms. Performance evaluation is also emphasized, with empirical metrics like PSNR and MSE proving that high image quality can be maintained while embedding secret data, which is crucial for practical deployment.

Other surveys explore multiple steganographic methods ranging from LSB substitution to transform-domain techniques, concluding that frequency-domain methods like DWT and DCT offer stronger robustness but at the cost of reduced payload capacity. Extensions of this work highlight that while modified LSB variations improve imperceptibility, no single technique fully satisfies all requirements of capacity, invisibility, and robustness simultaneously.

Turning to real-time chat applications, several studies illustrate how modern frameworks such as Django, Python-based systems, MERN stack, and ReactJS with Firebase emphasize encryption and authentication as primary security mechanisms. These platforms provide strong confidentiality and usability features, including private chats, group messaging, notifications, and user management. However, they remain largely dependent on cryptographic techniques alone and do not incorporate steganography to conceal the existence of sensitive communication.

Overall, the reviewed works show that while steganography and secure chat systems are individually well-developed, very few attempts have been made to combine the concealment power of steganography with the collaborative capabilities of real-time chat applications. This gap highlights a promising research direction for developing integrated solutions that ensure both secrecy of communication and invisibility of its very existence.

4. RESEARCH GAPS

The reviewed literature indicates that research on secure communication has largely progressed along two separate paths: the development of advanced steganographic methods and the design of robust real-time chat applications. Steganography research has shown that techniques such as Least Significant Bit (LSB) substitution, hybrid models with encryption, and transform-domain approaches can effectively conceal messages while maintaining acceptable image quality. However, these methods are often evaluated only in terms of embedding and extraction, without consideration for real-time deployment or integration into collaborative communication platforms. Similarly, cryptography-based chat applications have evolved into highly scalable and secure systems, leveraging frameworks such as Django, MERN, and Firebase to support features like private chats, group messaging, notifications, and user management. Yet, these applications focus primarily on encryption for confidentiality and neglect the covert capabilities of steganography, leaving the presence of sensitive communication detectable.

This separation creates a critical gap: while steganography provides invisibility and cryptography ensures confidentiality, very few systems combine these two domains into a unified solution. Existing steganographic studies lack practical integration into real-time chat environments, and modern chat applications remain limited to encryption alone. As a result, there is an underexplored opportunity to design a comprehensive platform that merges the imperceptibility of steganography with the collaborative and scalable features of real-time chat applications. Such an approach would enable both secrecy of content and concealment of communication itself, addressing limitations in current secure messaging technologies.

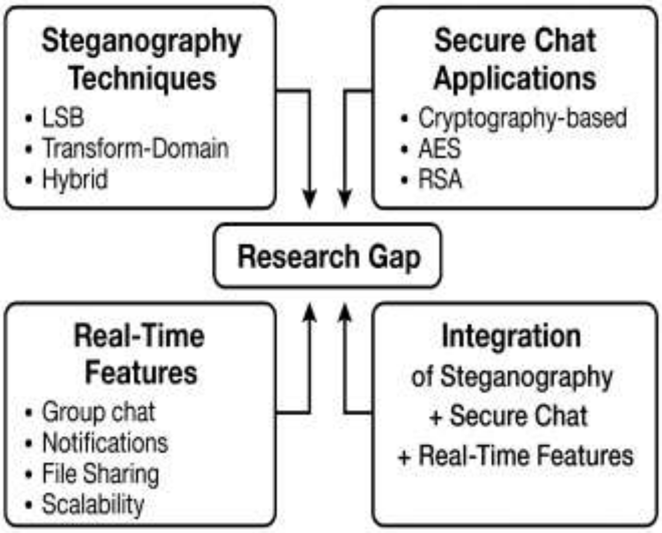

Figure 1 Existing Research Gaps

The Figure 1 illustrates how existing research has progressed along two parallel directions: secure chat applications (focused on cryptographic encryption, scalability, and usability) and image steganography (focused on imperceptibility, robustness, and embedding capacity). The absence of integration between the two highlights the key research gap that motivates this review.

5. LIMITATIONS AND CHALLANGES

Designing a secure chat application that integrates both steganography and real-time collaboration features presents a number of technical and practical obstacles. One major limitation is the trade-off between payload capacity and imperceptibility. Increasing the amount of hidden data often reduces visual quality, making detection easier and undermining the covert objective of steganography. Similarly, robustness is a concern, since many steganographic methods remain vulnerable to simple image processing operations such as compression, resizing, or filtering, which may corrupt or destroy the embedded message.

Another challenge arises from computational complexity. Dual-layer approaches, where cryptographic algorithms like AES are combined with steganography techniques such as Least Significant Bit (LSB), provide stronger confidentiality but also introduce overhead. The sequence of encryption, embedding, extraction, and decryption can lead to noticeable delays, conflicting with the real-time responsiveness expected in chat systems. Frequency-domain methods like DWT and DCT, though more resistant to certain attacks, further exacerbate this problem by demanding higher computational resources that may hinder scalability.

Performance trade-offs extend beyond processing power. Real-time chat systems depend on immediacy, and embedding operations risk slowing down message delivery. Likewise, advanced algorithms often achieve better concealment at the expense of speed, creating tension between security and user experience. Key management adds another layer of complexity: securely generating, distributing, and storing cryptographic keys becomes more challenging when combined with steganographic operations.

Usability also poses a limitation. While embedding messages in images is effective technically, integrating such a feature into a seamless user interface that feels natural to non-technical users is difficult. Additional concerns include storage and bandwidth, as encrypted and embedded files may be significantly larger than normal, placing pressure on system efficiency and scalability. Finally, secure authentication and session management remain essential for any chat application, and introducing steganography must not compromise these critical workflows.

In summary, the core challenges lie in balancing imperceptibility, robustness, and payload with real-time performance, managing the increased computational and infrastructural requirements, ensuring strong key distribution, and maintaining a user-friendly design. Overcoming these limitations is crucial for creating a practical, secure chat application that successfully merges covert communication with modern collaboration features.

6. CONCLUSION

This review paper has explored the current landscape of secure chat applications and image steganography, examining their strengths, weaknesses, and potential for integration. Existing research shows that steganography provides the ability to conceal messages within digital images, offering imperceptibility and plausible deniability, while cryptographic methods like AES and RSA ensure that content remains unreadable to unauthorized users.

At the same time, modern chat applications built on frameworks such as MERN, Django, and Firebase have demonstrated strong scalability, real-time performance, and rich collaboration features like group chats, notifications, and secure authentication.

However, despite these advancements, a significant gap remains. Current chat platforms focus heavily on encryption, leaving communications visibly identifiable as sensitive data, while steganographic systems excel in covert data hiding but often lack the real-time interactivity and usability of modern chat ecosystems. The combination of both approaches is still underdeveloped, with only limited attempts showing proof-of-concept integrations.

The main challenges involve balancing payload capacity, imperceptibility, and robustness in steganography, while also ensuring real-time performance, secure key management, scalability, and user-friendly integration. Overcoming these barriers will require efficient algorithms, optimized architectures, and seamless interfaces that make covert communication practical for everyday users.

In conclusion, the next step for research and development lies in designing a unified system that seamlessly merges advanced image steganography with full-fledged real-time collaboration features. Such a solution would not only protect message content but also conceal the very existence of sensitive communication, setting a new standard of security and privacy in digital interactions.

Acknowledgment:

We would like to express our gratitude to all faculty members for their support and helpful feedback. A special thanks goes to the authors of the studies we reviewed your contributions greatly shaped our understanding

REFERENCES

[1] P. Kumar, P. Saini, and G. Singh – "TEXT-IT: A Secure Web Chat Application," Note: The specific conference proceedings, location, and full date (e.g., "in Proc. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)

[2] N. Nurhayati, and S. S. Ahmad – "Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm," in Proc. 2016 4th International Conference on Cyber and IT Service Management.

[3] Dr. M. N. Nachappa, and V. K. R. P. – "Image Steganography Applications for Secure Communications," International Journal of Innovative Science, Engineering & Technology ,May 2019.

[4] S. Singh, S. Singh, and A. Sharma – "Real-Time Web-Based Secure Chat Application using Django," International Journal of Advances in Engineering and Management (IJAEM, April 2023.

[5] S. C. Mataraarachchi, and N. Wedasinghe – "DATA SECURITY SYSTEM FOR CHAT APPLICATIONS USING CRYPTOGRAPHY, STEGANOGRAPHY AND IMAGE PROCESSING," in Proc. 11th International Research Conference, General Sir John Kotelawala Defence University

[6] S. Gomathi, and C. Radhika – "A secure messaging application using steganography and aes encryption: A dual-layer secure messaging system," The Scientific Temper,

[7] H. Carranza, M. Bustamante, A. Carranza, and S. Muniganti – "Secure Chat Application with an End-to-End Encryption," in Proc. 2024 10th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'24), Barcelona, Spain, August 19-21, 2024.

[8] N. Shaikh, J. Mandviwala, H. Mali, P. Pardhe, S. Mehta, and P. Patil – "Chat-With-Me: A MERN-based real-time chat Application," International Journal of Research and Analytical Reviews (IJRAR), April 2023.

[9] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane – "Image Steganography: A Review of the Recent Advances," IEEE Access, 2021.

[10] S. Bansal, S. D. Sharma, S. K. Jha, S. Tomar, and R. Pandey – "Real Time Chat Application," [Publication details not available in source].

[11] A. Bisht, A. Singla, and K. Joshi – "A Review on Image Steganography Techniques," International Research Journal on Advanced Engineering Hub (IRJAEH), July 2024.

[12] M. A. Saleh – "Image Steganography Techniques - A Review Paper," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), September 2018