International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Whisper-Steg: Unveil the Hidden

Prof. Laxman Pawar[1], Ansab Ebad[2], Vaibhavi Bankhele[3], Atharva Borse[4], Abhishek Gore[5]

*1 Professor, Department of Computer Engineering, Sinhgad College of Engineering-Vadgaon, Pune, Maharashtra, India

*2,3,4,5 Department of Computer Engineering, Sinhgad College of Engineering-Vadgaon, Pune, Maharashtra, India

---

Abstract - Whisper-Steg represents a ground-breaking project at the intersection of secure messaging and advanced information concealment techniques. This innovative chat application transcends traditional boundaries by seamlessly integrating the art of steganography, offering users a novel and secure platform for communication. The project not only facilitates text and image sharing but introduces an ingenious Image Steganography feature, allowing users to embed confidential information within images. Incorporating an acknowledgment mechanism akin to popular messaging applications like WhatsApp, Whisper-Steg prioritizes the reliability of communication. This feature ensures that users receive confirmation of message delivery, enhancing the overall user experience.

The project dynamically generates cover images based on the size of hidden messages, employing AI algorithms to optimize concealment. This not only enhances the security of the stenographic process but also underscores the project's commitment to leveraging cutting-edge technologies for user benefit. In an era where privacy concerns are paramount, Whisper-Steg embraces steganography and AI-driven solutions and stands as a testament to technological innovation, reshaping the landscape of secure digital communication.

Key Words: Whisper-Steg, Steganography, chat application

1. INTRODUCTION

In the ever-evolving landscape of digital communication, where the preservation of privacy stands as an increasingly paramount concern, the advent of "Whisper-Steg" marks a transformative stride towards redefining secure messaging paradigms. This pioneering project integrates the age-old art of steganography into a contemporary chat application, ushering in a new era of discreet and confidential communication.

Whisper-Steg is meticulously crafted to provide users with a seamless and secure messaging experience, incorporating features that extend beyond conventional text-based conversations. In the vein of widely embraced messaging applications, Whisper-Steg incorporates an acknowledgment mechanism reminiscent of WhatsApp, ensuring that users have assurance of the delivery and receipt of their messages.

A distinguishing feature of Whisper-Steg lies in its integrated Image Steganography, a technique wherein information is concealed within digital images. This method offers users an unparalleled level of confidentiality, as the hidden information remains undetectable to unintended recipients. Whisper-Steg empowers users with the ability to embed secret messages within images, creating a secure channel for confidential communication. Whisper-Steg introduces an innovative cover image generation system driven by artificial intelligence.

As Whisper-Steg pioneers this evolution in secure messaging,

it beckons users into a realm where privacy and innovation harmoniously converge, reshaping the contours of digital communication as we know it.

2. LITERATURE SURVEY

The current state of messaging applications often lacks robust security measures, leaving user data vulnerable to unauthorized access or interception. Traditional messaging platforms may not provide end-to-end encryption, making it easier for third parties to gain access to conversations and private information. Additionally, existing systems may not offer reliable mechanisms for securely transmitting sensitive data, such as images, without compromising their quality or risking distortion. The system comprises three levels of administration: the Central Admin, State Admin, andDistrict Admin, each with distinct roles and to overcome the limitations of the existing system, we introduce "Confidential Chat" - a revolutionary messaging application that prioritizes privacy and security. Our proposed system incorporates advanced features to ensure the confidentiality and integrity of user communications.

End-to-End Encryption: "Confidential Chat" employs robust end-to-end encryption to secure all conversations. This encryption ensures that only the intended recipients can access and decipher the messages, providing a high level of privacy and protection against unauthorized access.

High-Quality Cover Images for Image Steganography: Our system utilizes high-quality cover images for image steganography, enabling users to hide sensitive data within images without compromising the visual quality.

By minimizing distortion, we ensure that the hidden information remains intact while maintaining an aesthetically pleasing appearance.

Acknowledgment Mechanism: "Confidential Chat" includes a reliable acknowledgment mechanism, providing confirmation that messages have been successfully delivered to the intended recipients. This feature enhances the reliability of communication, ensuring that important information reaches its destination without any issues.

User-Friendly Interface: Our proposed system offers an intuitive and visually appealing interface, making it easy for users to navigate and communicate seamlessly. The user-friendly design ensures a smooth user experience across various platforms, promoting effortless and secure communication.

3. METHODOLOGY

In this project the successful integration of image steganography into a feature-rich chat application. Beginning with a meticulous analysis of requirements, the project aims to understand the core functionalities expected, such as text and image sharing, an acknowledgment mechanism akin to popular platforms like WhatsApp, and the innovative inclusion of image steganography. The design phase entails structuring the chat application architecture, delineating the image steganography module's intricacies, and planning the incorporation of artificial intelligence (AI) algorithms for generating cover images tailored to message size. Subsequently, the development phase materializes these designs into a functional system, implementing the chat application, acknowledgment features, the LSB-based steganography module, and the dynamic AI-driven generation of cover images. Rigorous testing, including unit and integration testing, is then conducted to ensure the seamless operation of the system, with a specific focus on evaluating the security and efficacy of the steganography algorithm. Upon successful testing, the deployment phase makes the chat application accessible to users. Comprehensive documentation is prepared to elucidate the system's architecture, design rationale, and user guidelines.

4. SYSTEM DESIGN

UML Diagrams:

1. Use Case Diagram:

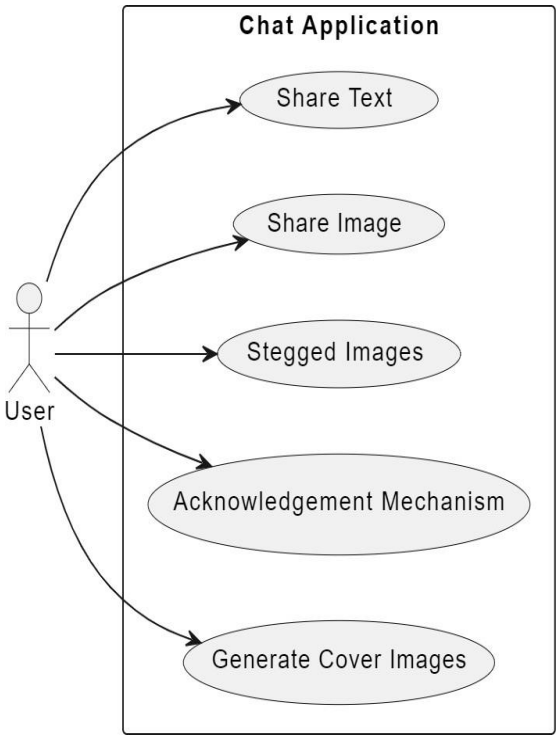

Fig 1: Use Case Diagram

2. Sequence Diagram

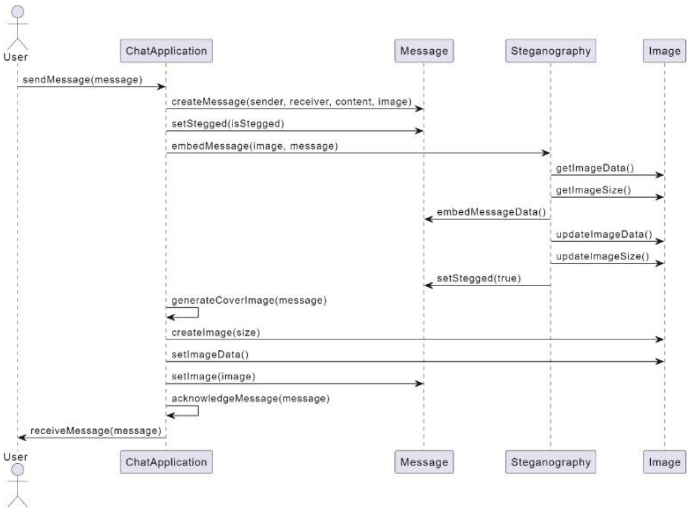

Fig 2: Sequence Diagram

3. Class Diagram:

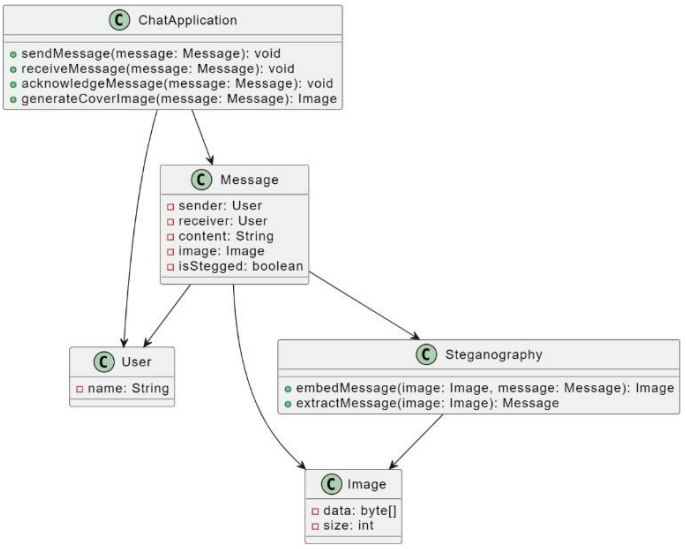

Fig 3: Class Diagram

5. CONCLUSIONS

The "Whisper-Steg" project represents a successful amalgamation of cutting-edge technologies to enhance conventional chat applications. The incorporation of image steganography introduces a layer of covert communication, providing users with a secure and intriguing means of sharing information. The development process, guided by a systematic methodology, ensured the seamless integration of essential features, including text and image sharing, acknowledgment mechanisms, and the innovative steganography module.

The project's utilization of AI for dynamically generating cover images tailored to message sizes underscores a commitment to efficiency and user experience. The LSB-based steganography algorithm, though efficient, necessitates ongoing vigilance to address potential vulnerabilities. The implementation plan, driven by the waterfall model, facilitated a structured and iterative approach, ensuring that each phase was meticulously executed before progressing to the next. The system's architecture, depicted in detailed diagrams and UML representations, reflects the careful consideration given to design and functionality. The sequence diagrams illustrate the intricate interactions between system components, emphasizing the flow of information within the Whisper-Steg environment. As Whisper-Steg enters deployment, it holds promise as a secure, feature-rich chat application, providing users with a novel and secure communication experience. The project's dedication to ongoing maintenance and updates will undoubtedly contribute to its sustainability and continued relevance in the ever-evolving landscape of digital communication. Whisper-Steg stands as a testament to the potential of integrating advanced technologies to redefine the boundaries of secure and engaging communication platforms.

ACKNOWLEDGEMENT

Every work is source which requires support from many people and areas. It gives us proud privilege to complete the Project on "**Whisper-Steg : Unveil The Hidden**" under valuable guidance and encouragement of our guide **Prof. L. B. Pawar.**

We are also extremely grateful to our respected H.O.D. (Comp Dept.) **Dr. M. P. Wankhade** for providing all facilities and every help for smooth progress of our project. We would also like to thank all the **Staff Members** of Comp Engineering Department for timely help and inspiration for completion of the project.

At last, we would like to thank all the unseen authors of various articles on the Internet, helping us become aware of the research currently ongoing in this field and all our colleaguesfor providing help and support in our work.

Future Scope:

The "Whisper-Steg" project opens up exciting avenues for future development and expansion, offering a rich landscape for enhancements and additional features. Some potential future scopes include:

1. Advanced Steganography Techniques: Explore and implement more advanced steganography algorithms beyond LSB, incorporating methods that offer higher security and resistance to detection. This could involve exploring frequency domain techniques, spread spectrum methods, or even exploring the integration of encryption algorithms for added security.
2. Multi-Media Support: Extend the steganography capabilities to support various types of multimedia beyond images. This could involve hiding information within audio or video files, providing users with a broader range of options for covert communication.

3. Enhanced Security Measures: Integrate more robust security measures to safeguard against potential attacks. This might include the implementation of encryption algorithms for both text and images, ensuring that even if the steganography is detected, the content remains secure.
4. Real-time Collaboration Features: Expand the chat application to support real-time collaboration features, such as document sharing, collaborative editing, and synchronized multimedia experiences. This would elevate Whisper-Steg to a comprehensive communication and collaboration platform.
5. User Authentication and Authorization: Implement robust user authentication and authorization mechanisms to enhance the overall security of the application. This could involve biometric authentication, two-factor authentication, or other advanced security measures.
6. Cross-Platform Compatibility: Develop versions of the application compatible with different operating systems and devices to ensure widespread accessibility. This could involve creating dedicated applications for mobile platforms and desktop environments.
7. User Interface Improvements: Continuously enhance
   the user interface (UI) and user experience (UX) to make the application more intuitive and user-friendly. Incorporate user feedback to identify areas of improvement and refine the design accordingly.
8. Cloud Integration: Explore the integration of cloud services for data storage and synchronization, enabling users to seamlessly access their chat history and stenographic content across multiple devices.
9. Machine Learning for Image Analysis: Implement machine learning algorithms for image analysis to detect any suspicious patterns or anomalies in images, thereby enhancing the security and reliability of the steganography process.
10. Community and Social Features: Introduce community and social features within the application, such as group chats, forums, or channels, fostering a sense of community among users.

These future scopes collectively contribute to the evolution of Whisper-Steg as a sophisticated and versatile communication platform, staying ahead of emerging trends and user expectations in the dynamic landscape of digital communication.

REFERENCES

1. Srushti S Yadahalli, Shambhavi Rege and Dr. Reena Sonkusare," Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques", Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020), IEEE,2020.
2. K. Thangadurai and G. Sudha Devi," An analysis of LSB Based Image Steganography Techniques", 2014 International Conference on Computer Communication and Informatics (ICCCI -2014).
3. Zhi-Hui Wang, The Due Kieu, chin chen chang and Ming-Chu Li," Emoticon-based Text Steganography in Chat", 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications, IEEE, 2009.
4. Moses Oyaro Okello," Steganalysis of Chat based Steganography", doi:10.20944/preprints202302.0298.v1, 2023.
5. Emmanuel O. Ojei, Sylvanus O. Anigbogu and Gloria Anigbogu," Least Significant Bit Based Image Steganalysis System using Java API", International Journal of Advances in Engineering and Management (IJAEM), Volume 3, Issue 5 May 2021.

6. Vikas Singhal, Yash Kumar Shukla and Navin Prakash," Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-8, June 2020.
7. Okello, M. O. (2022). Optimal Covert Communication Techniques. International Journal of Informatics and Applied Mathematics, 5 (1), 1-26. DOI: 10.53508/ijiam.1073205
8. Kakungulu-Mayambala, R. (2008). Phone-tapping & the Right to Privacy: A Comparison of the Right to Privacy in Communication in Uganda & Canada. In BILETA Conference.
9. Atuhaire, E. (2021). Artificial intelligence and the right to privacy in Uganda (Doctoral dissertation, Makerere University).
10. P. P. S. Parekh, J. Patel, and D. Sahu, "Comparison of steganography techniques in medical application."
11. O. C. Williams, "What are the cybersecurity risks of artificial intelligence generated steganography?" Ph.D. dissertation, Utica College, 2019.
12. I. Diop, S. Farssi, O. Khouma, H. Diouf, K. Tall, and K. Sylla, "New steganographic scheme based of reed-solomon codes," International Journal of Distributed and Parallel Systems, vol. 3, no. 2, p. 81, 2012.
13. *Steganography*, 2020, [online] Available: https://en.wikipedia.org/wiki/Steganography.
14. H. Shi, X.-Y. Zhang, S. Wang, G. Fu and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning", *Proc. Int. Conf. Comput. Sci*, pp. 31-43, 2019.
15. N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", *Computer*, vol. 31, no. 2, pp. 26-34, Feb. 2015.
16. S. Gupta, G. Gujral and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography", *Int. J. Comput. Eng. Manage.*, vol. 15, no. 4, pp. 40-42, 2012
17. [8] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman encoding", *Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci.*, pp. 14-18, Mar. 2012
18. Z. Qu, Z. Cheng, W. Liu and X. Wang, "A novel quantum image steganography algorithm based on exploiting modification direction", *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 7981-8001, Apr. 2019.
19. N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography", *Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, pp. 1-5, Nov. 2016.