STM JOURNALS

Journal of
Telecommunication, Switching Systems and Networks

ISSN: 2454-6372
Volume 11, Issue 2, 2024
May–Auagust
DOI (Journal): 10.37591/JoTSSN

https://journals.stmjournals.com/jotssn

Research JoTSSN

Implementing Vault Fortify: Best Practices for Data Protection and Compliance

Abdula Adil[1], Adhnan Mahamood[2], Ajmal M.[3], Ashar Mohammed Cherichi[4], Jalaluddeen B.M.[5,*]

Abstract

In an era marked by heightened concerns over privacy and security, the need for innovative approaches to data sharing platforms has become increasingly imperative. This paper presents StealthChat, a novel solution that combines steganography techniques with peer-to-peer (P2P) architecture to establish a secure and decentralized communication environment. Leveraging TypeScript, StealthChat offers users a seamless and intuitive interface for real-time data sharing while prioritizing privacy and confidentiality. The core architecture of StealthChat is built upon a P2P network model, enabling direct communication between users without reliance on centralized servers. Through dynamic peer discovery mechanisms and efficient data routing protocols, users can establish secure connections and exchange messages in real-time. This decentralized method lowers the risks connected with centralized data storage, making it less vulnerable to possible hacks or breaches while also improving scalability and fault tolerance.

Keywords: StealthChat, steganography, peer-to-peer, data sharing, privacy, security

INTRODUCTION

Vault Fortify is a cutting-edge communication application designed to offer unparalleled security and privacy through stealth chat and file-sharing capabilities using peer-to-peer (P2P) architecture and image steganography. In an era where digital privacy is constantly under threat, Vault Fortify stands out by ensuring that your messages and files are not only encrypted but also hidden within innocuous-looking images. This dual-layer security approach makes it nearly impossible for unauthorized parties to detect the presence of communication or sensitive data [7–9].

The P2P architecture of Vault Fortify eliminates the need for centralized servers, reducing the risk of data breaches and ensuring that communication is direct and secure between users. This decentralized system enhances the robustness of the application by distributing data across a network of nodes, making it resilient to attacks and surveillance. Each user acts as both a client and a server, facilitating a more secure and efficient exchange of information. This ensures that even in the event of a compromised node, the integrity and confidentiality of the communication remain intact [6].

In addition to secure messaging, Vault Fortify leverages image steganography to hide files within digital images. This method embeds data in such a way that it is imperceptible to the naked eye, allowing users to share files covertly. The integration of steganography with the P2P

***Author for Correspondence**
Jalaluddeen B.M.
E-mail: Jalaluddeen_cs@pace.edu.in

[1,2,3,4]Students, Department of Computer Science and Engineering, P A College of Engineering, Mangalore, Karnataka, India
[5]Assistant Professor, Department of Computer Science and Engineering, P A College of Engineering, Mangalore, Karnataka, India

Received Date: June 06, 2024
Accepted Date: July 07, 2024
Published Date: July 18, 2024

Citation: Abdula Adil, Adhnan Mahamood, Ajmal M., Ashar Mohammed Cherichi, Jalaluddeen B.M. Implementing Vault Fortify: Best Practices for Data Protection and Compliance . Journal of Telecommunication, Switching Systems and Networks. 2024; 11(2): 18–24p.

framework ensures that not only is the data transfer secure, but the very existence of the data remains hidden. Vault Fortify thus offers a comprehensive solution for individuals and organizations seeking to protect their digital communications and sensitive information from prying eyes [11–13].

LITERATURE SURVEY

The paper "Image Steganography for Securing Secret Data Using Hybrid Hiding Model" by Sumeet Kaur, Savina Bansal, and Rakesh Kumar Bansal presents a sophisticated approach to enhancing data security through innovative steganographic techniques. The researchers introduce the Image Hiding Encryption and Decryption (IHED) model, a hybrid framework designed to secure data transmission by embedding secret information within digital images. The IHED model primarily employs mid-frequency (MF) values for embedding data, striking a balance between high-frequency and low-frequency methods. High-frequency values can lead to easy detection due to noticeable changes in the image, while low-frequency values may distort the image's visual quality. By utilizing MF values, the IHED model ensures that the modifications remain subtle and less detectable, maintaining the visual integrity of the stego-image while embedding a significant amount of data. To enhance security, the IHED model integrates multiple steganographic techniques, making it more robust against various steganalysis attacks. This layered approach increases the complexity for unauthorized entities attempting to extract or detect the hidden data. The hybrid nature of the model leverages the strengths of different techniques to create a more secure and imperceptible steganographic method [1].

The paper "Data Vaults for Blockchain-Empowered Accounting Information Systems" by Muhammad Imran Sarwar and colleagues presents a novel framework that integrates blockchain technology with Accounting Information Systems (AIS) to enhance data security and integrity. The proposed system leverages data vaults, which are secure storage units, backed by the immutable and decentralized nature of blockchain technology. This integration ensures that financial and accounting data remain tamper-proof and transparent, thus increasing trustworthiness and reducing the risk of data breaches [2]

The paper "Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm" by Bijeta Seth, Surjeet Dalal, Dac-Nhuong Le, and their co-authors, addresses the critical issue of security in cloud data storage systems. This research introduces a hybrid cryptographic protocol that combines the Paillier and Blowfish encryption algorithms to enhance data security and efficiency in cloud environments.

The proposed system leverages the strengths of both symmetric and asymmetric encryption methods. Blowfish, a symmetric encryption algorithm, is known for its speed and efficiency, making it suitable for encrypting large volumes of data. On the other hand, Paillier is an asymmetric encryption algorithm that supports homomorphic encryption, which allows computations on encrypted data without decryption. By integrating these two algorithms, the system aims to reduce computational overhead and ciphertext size, thus optimizing the performance of cloud storage [3].

The paper "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions" by Ishu Gupta, Ashutosh Kumar Singh, Chung-Nan Lee, and Rajkumar Buyya offers an in-depth exploration of the current landscape of data security in cloud computing. Recognizing the growing reliance on cloud services for data storage and processing, the authors systematically review the multitude of techniques developed to safeguard sensitive information from unauthorized access and breaches. The paper begins by outlining the critical challenges associated with data protection in cloud environments, such as data breaches, loss of control over data, and compliance with data privacy regulations. These challenges underscore the necessity for robust security measures to ensure that data remains confidential, integral, and available [4]

The paper "Combination of Steganography and Cryptography: A Short Survey" by Mustafa Sabah Taha et al. (2019) provides a comprehensive review of the integration of steganography and

cryptography to bolster data security. This synergistic approach aims to exploit the strengths of both methods to protect sensitive information from unauthorized access and detection.

Steganography, the practice of hiding the existence of a message, is traditionally used to embed information within digital media, such as images, audio files, or video streams, in a way that is imperceptible to the human eye and standard detection techniques. Cryptography, on the other hand, focuses on encrypting the content of the message, transforming it into an unreadable format that can only be deciphered by those possessing the appropriate decryption key. The survey details the benefits of combining these two methods, which significantly enhances security [5]

MATERIALS AND METHODS

Algorithms

The Least Significant Bit (LSB) Algorithm

The Least Significant Bit (LSB) algorithm is a steganography technique used to hide data within digital media, such as images, audio files, and videos, by subtly modifying the least significant bits of the media's data. This method leverages the fact that altering the least significant bit of a byte causes minimal changes that are typically imperceptible to human senses, making it an effective tool for covert communication.

In the context of an image, the LSB algorithm operates by modifying each pixel's color components: red, green, and blue (RGB). Each of these components is usually represented by an 8-bit value, ranging from 0 to 255. To embed secret data, the algorithm replaces the least significant bit of each color component with bits from the secret message. Since the least significant bit represents the smallest possible change in the color value, this modification does not significantly alter the image's overall appearance, ensuring that the hidden data remains undetected.

The process of extracting the hidden data is straightforward. The receiver retrieves the least significant bits from the modified pixels and reassembles them to reconstruct the original message. For example, if the original pixel values are (10101100, 11001101, 11110010) and the secret data bit is 1, the modified pixel values might become (10101101, 11001101, 11110010). This slight alteration in the least significant bit is generally unnoticeable, allowing the image to maintain its visual integrity while securely embedding the hidden data.

METHODOLOGY

Data Encryption

The data encryption methodology utilizes advanced steganography algorithms to ensure maximum security and confidentiality. By embedding encrypted data within digital media such as images, audio files, or videos, an additional layer of protection is created that conceals the presence of sensitive information. This approach not only encrypts the data but also hides it in a way that is imperceptible to unauthorized viewers. As a result, this method provides a highly secure and confidential means of protecting data from potential threats and breaches, ensuring that only intended recipients can access and decipher the hidden information [10]. Data Encryption process is shown in Figure 1.

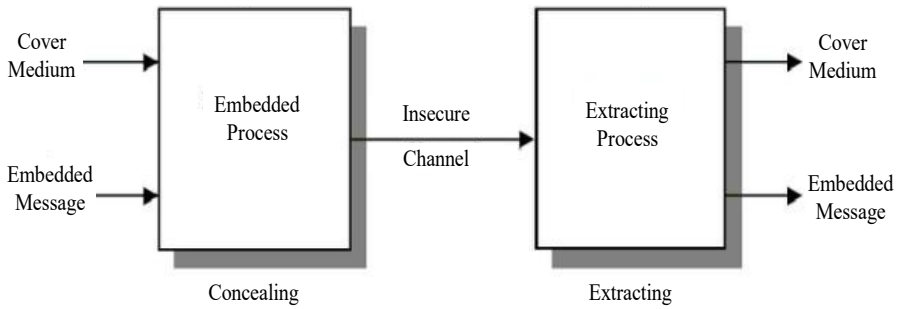

Figure 1. Data Encryption process.

Cloud Storage

Explore the approach to securely storing encrypted data within the reliable and scalable environment of AWS cloud servers. This method leverages AWS's robust infrastructure to ensure data integrity and availability while utilizing advanced encryption techniques to protect sensitive information. By storing data in an encrypted format, it remains secure from unauthorized access both in transit and at rest. AWS's scalable resources provide flexibility to accommodate varying storage needs, ensuring efficient and reliable data management. This approach combines the security of encryption with the dependability of AWS, offering a comprehensive solution for secure cloud storage.

Data Retrieval

The data retrieval process involves decrypting and reconstructing the original data from steganographic encodings. This begins by identifying the digital media containing the hidden data, such as an image, audio file, or video. Using specialized software, the least significant bits or other steganographic markers are extracted from the media. These bits, which were subtly modified to embed the encrypted data, are then reassembled into their original form. The extracted data is subsequently decrypted using the appropriate decryption key, fully restoring the original information. This meticulous process ensures that the hidden data is accurately and securely retrieved, maintaining the integrity and confidentiality of the information.

FLOWCHART

Flow chart of proposed system is shown in Figure 2.

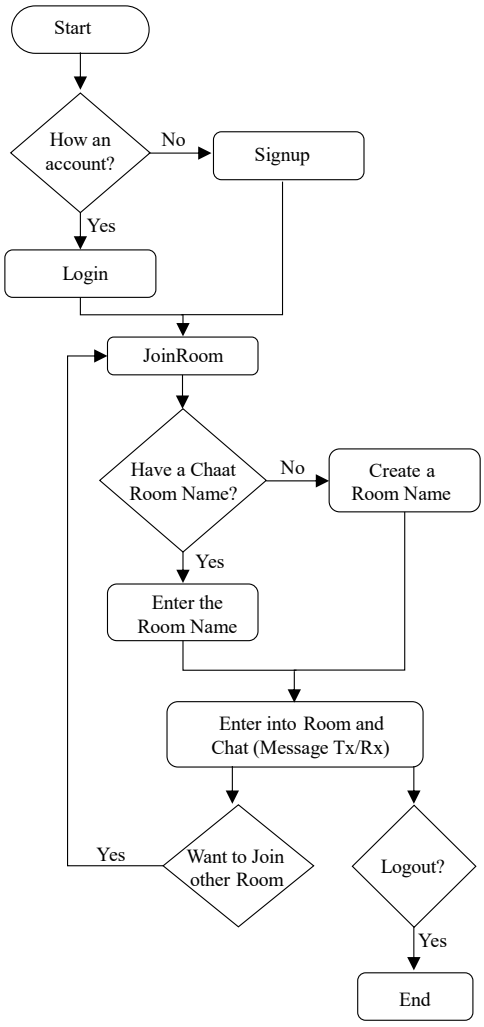

Figure 2. Flow chart of proposed system.

Real-Time Data Sharing Platform

The Real-Time Data Sharing Platform enables secure and covert sharing of the steganographed data. This platform: Stores the steganographed data in a secure repository Enables real-time sharing of data through various channels (e.g., messaging, streaming, or peer-to-peer networks) Extracts the secret data from the cover objects Decrypts the data (if encrypted) Analyzes and processes the shared data in real-time Manages user access, authentication, and authorization Provides a user-friendly interface for interacting with the platform

Steganography Module

The Steganography Module is responsible for hiding secret data within cover objects (such as images, audio, or text). This module: Receives data from various sources as shown in Figure 3 Embeds the data into cover objects using steganographic algorithms Produces steganographed data that appears innocent and unsuspecting

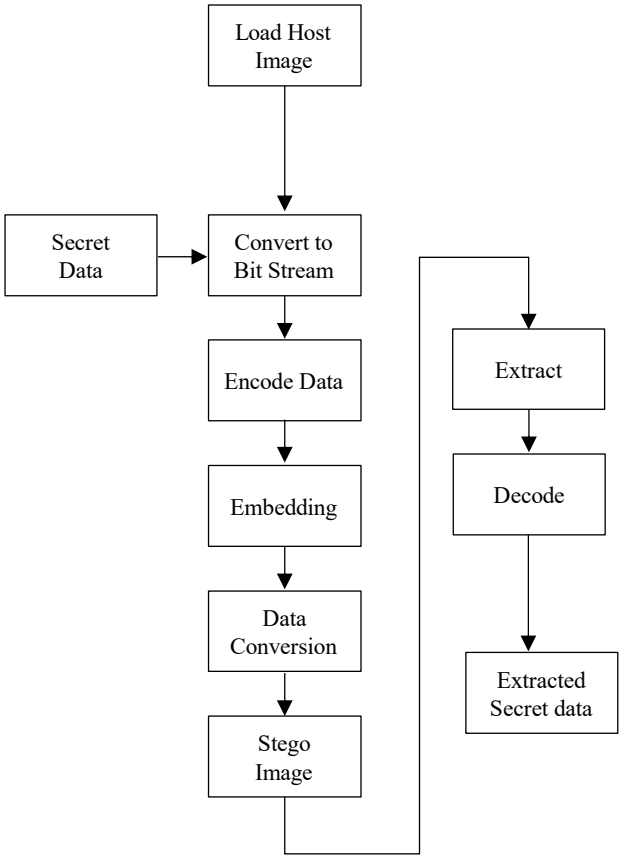

Figure 3. Data receive process of stenography module.

RESULTS

This novel communication solution enhances privacy and security by combining steganography techniques with a peer-to-peer (P2P) architecture. This decentralized approach eliminates reliance on centralized servers, thereby reducing vulnerabilities and improving fault tolerance. The platform enables direct user communication, ensuring real-time data sharing with a user-friendly interface built in TypeScript.

1. *Login Page:* Login Page window is shown in Figure 4.
2. *Chating Page:* Chating Page window is shown in Figure 5**.**

Steganography: Stenography window is shown in Figure 6.

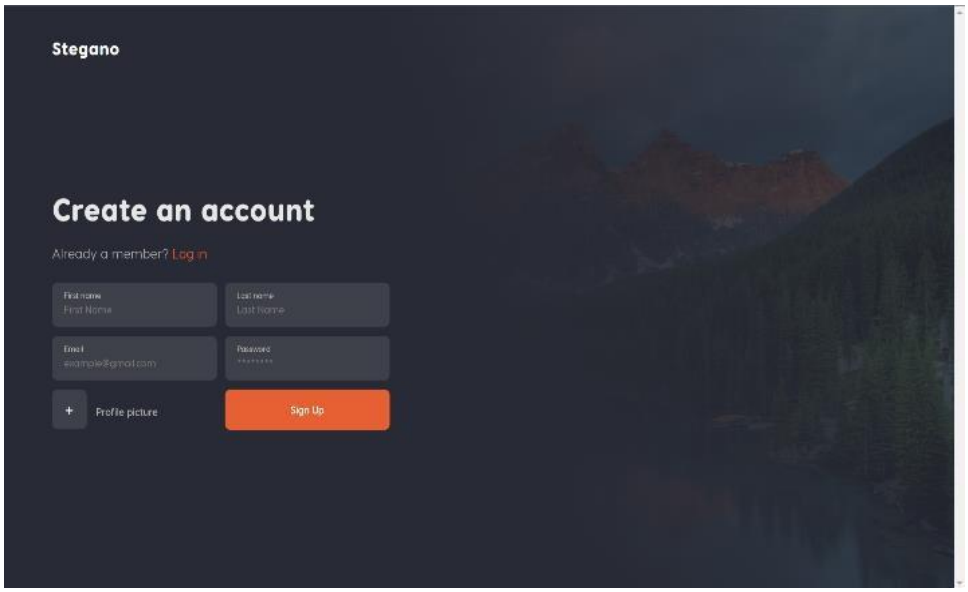

Figure 4. Login Page.

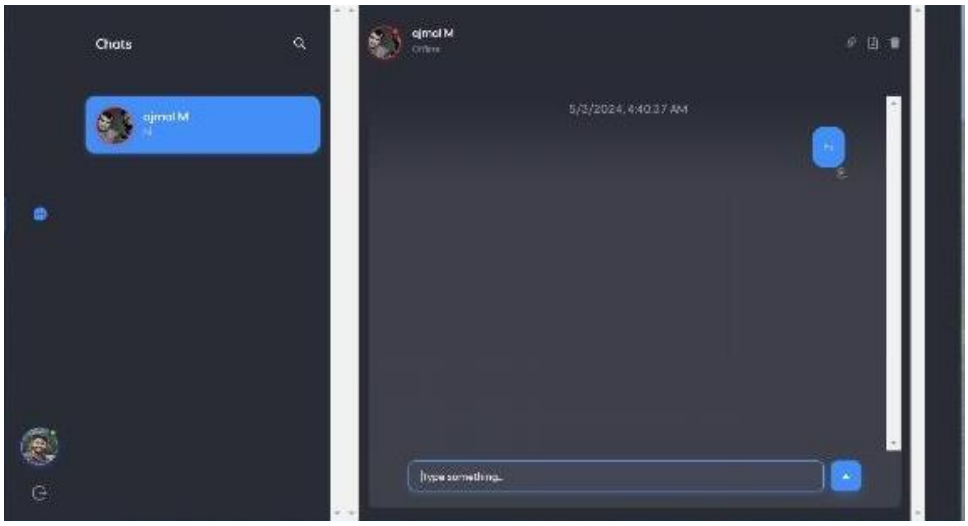

Figure 5. Chating Page.

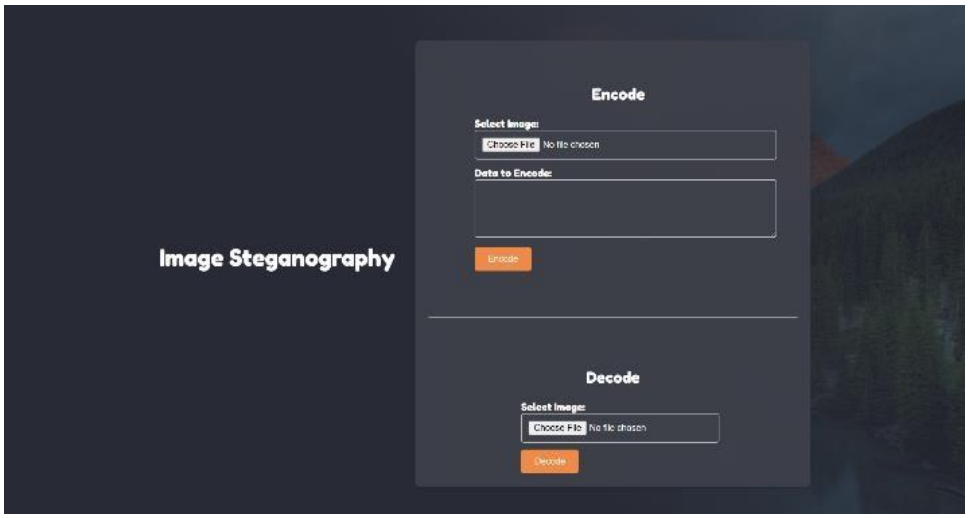

Figure 6. Steganography.

CONCLUSION

Vault Fortify represents a significant advancement in secure digital communication, combining the strengths of peer-to-peer (P2P) architecture and image steganography. By eliminating reliance on centralized servers, Vault Fortify ensures that user data is not vulnerable to centralized breaches or unauthorized access. The P2P model allows for direct communication between users, enhancing both security and privacy. This decentralized approach not only safeguards data integrity but also boosts efficiency, making the application resilient against attacks and ensuring that sensitive information remains protected during transmission.

REFERENCES

1. Kaur S, Bansal S, Bansal RK. Image steganography for securing secret data using hybrid hiding model. Multimedia Tools and Applications. 2021 Feb;80:7749-69.
2. Sarwar MI, Iqbal MW, Alyas T, Namoun A, Alrehaili A, Tufail A, Tabassum N. Data vaults for blockchain-empowered accounting information systems. IEEE Access. 2021 Aug 24;9:117306-24.
3. Seth B, Dalal S, Le DN, Jaglan V, Dahiya N, Agrawal A, Sharma MM, Prakash D, Verma KD. Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. Computers, Materials & Continua. 2021 Apr 1;67(1).
4. Gupta I, Singh AK, Lee CN, Buyya R. Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. IEEE Access. 2022 Jul 4;10:71247-77.
5. Taha MS, Mohd Rahim MS, Lafta SA, Hashim MM, Alzuabidi HM. Combination of steganography and cryptography: A short survey. InIOP conference series: materials science and engineering 2019 May 1 (Vol. 518, No. 5, p. 052003). IOP Publishing.
6. AA AEL-L, Abd-El-Atty B, Venegas-Andraca SE (2019) A novel image steganography technique based on quantum substitution boxes. Opt Laser Technol 116:92–102.https://doi.org/10.1016/j.optlastec.2019.03.005
7. Abd El-Latif AA, Abd-El-Atty B, Elseuofi S, Khalifa HS, Alghamdi AS, Polat K, Amin M. Secret images transfer in cloud system based on investigating quantum walks in steganography approaches. Physica A: Statistical Mechanics and its Applications. 2020 Mar 1;541:123687.https://doi.org/10.1016/j.physa.2019.123687
8. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Diss. University of Buckingham. http://bear.buckingham. ac.uk/id/eprint/149
9. Kadhim IJ, Premaratne P, Vial PJ. Improved image steganography based on super-pixel and coefficient-plane-selection. Signal Processing. 2020 Jun 1;171:107481.
10. Malathi P, Gireeshkumar T. Relating the embedding efficiency of LSB steganography techniques in spatial and transform domains. Procedia Computer Science. 2016 Jan 1;93:878-85.
11. Makhdoom I, Abolhasan M, Lipman J, Piccardi M, Franklin D. PrivySeC: A secure and privacy-compliant distributed framework for personal data sharing in IoT ecosystems. Blockchain: Research and Applications. 2024 Jul 9:100220.
12. Oliveira J, Santin A, Viegas E, Horchulhack P. A Non-interactive One-Time Password-Based Method to Enhance the Vault Security. InInternational Conference on Advanced Information Networking and Applications 2024 Apr 9 (pp. 201-213). Cham: Springer Nature Switzerland.
13. Yeshwantrao SA, Satpute KC, Patil TH, Shinde SB. EVAULT IN BLOCKCHAIN TO STORE AND MANAGE LEGALRECORDS.

