WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Exploring Advanced Techniques in Image Steganography and Date Hiding For Secure Communication

***Venugopal Rohith*[#1], *Sangeetha Varadhan**[2]

[#1]1PG Student Department of Computer Applications,DR. M.G.R. Educational & Research Institute
Chennai,Tamil Nadu,India
[1]rohithv004@gmail.com
*[2] Assitant Professor Department of Computer Applications,DR. M.G.R. Educational & Research Institute
Chennai,Tamil Nadu,India
[2]sangeetha.mca@drmgrdu.ac.in

ABSTRACT :

The evolution of image steganography and data hiding techniques has ushered in a new era of secure communication and information concealment. This paper delves into advanced methodologies that have transformed the landscape of digital watermarking, copyright protection, and covert data transmission. From the rudimentary LSB (Least Significant Bit) substitution to sophisticated machine learning-based approaches, a spectrum of techniques has been explored for embedding information within digital images. The aim is to strike a balance between imperceptibility and robustness against detection, with an emphasis on adaptability, distortion optimization, and hybridization. Furthermore, the paper highlights the challenges posed by modern steganalysis techniques and the imperative for continued innovation to ensure the resilience and efficacy of steganographic systems.

Keywords: Image Steganography, Data Hiding, LSB Substitution, Spread Spectrum, Transform Domain, Adaptive Steganography.

I.INTRODUCTION:

Multimedia data such as image, text, file or video with data encryption.Image steganography is a technique for hiding an image within another image. In image steganography, the cover image is manipulated so that the hidden data is not visible, which does not make it suspicious, as in cryptography.On the contrary, steganizations are used to detect any secret. the message in the image and extract the hidden information[1].

In propose a slightly different approach, taking into account style image as well as internal information and cover image. The generated brace image is converted to the style image given as input. Reveal network is used to decode the secret information created from the stego image. As with the other methods, a VGG-based auto-encoder-decoder architecture is used Arbitrary resizing of the secret data and style image is done by an adaptive example[2].

The channel because all semantic and color information in Cr and Cb channels. Additionally, to reduce the payload by two-thirds, the hidden image is converted to grayscale image format. Y channel of the cover image Haltone secret image is fed to the encoder-decoder network to generate the brace image.The source image is the Y channel combined with Cr and Cb channels to create the cover image brace image in the YCrCb color space. To encode the hidden image, the Y channel de the brace image is fed back to the revealing network to output the grayscale hidden image. Also, two different variants are used for reproductive models - basic and residual models[3].

A combination of encryption and steganography is used where the LSB of the cover image is replaced by the most significant bit of the secret image. A pseudo-random number generator is used to select the pixels and the key is encrypted every time it is rotated. A K-LSB method is proposed, where the k least bits are replaced by a secret message. Stega analysis uses an entropy filter to detect and reveal the secret image[4].

LSB methods are used to hide secret information jokes in videos as well. Videos are sequences of images called video frames. Each video is cut into frames and the binary bits of the secret information are hidden in the LSB of the video frames. The basic form of LSB substitution method and Video uses a combination of Huffman coding and LSB substitution methods. Another interesting approach is to use audio together with video footage to improve concealment[5].

II.LITERATURE SURVEY

According to **Brendan Halloran**.et al., 2019 the secure storage and transmission of secret information has received the undivided attention of many researchers. Techniques for hiding confidential information in undetectable digital media such as video, audio and images are collectively known as steganography.Popularity and availability of digital images among media [6].

According to **Khider Nassif Jassim**.et al., 2019The information we collect may be sensitive, such as information about financial and business developments. Hackers or online thieves try to steal valuable information, ie. credit card numbers. Organizations are looking for secure online channels to move their data efficiently and prevent data theft. One of the most applicable methods that have been developed to protect data transmitted over a network is encryption, which transmits the original data or information in encrypted form[7].

According to **M Mazhar Afzal**.et al., 2020 The word "Steganography" originates from Greece and has been used in various forms for 2500 years, which is the art of hiding confidential information in any digital way so that no one can decipher it. It found practice in various fields such as military, governmental, diplomatic, medical, personal and intelligence services. This survey article sheds light on the basics of image steganography and its various techniques and sub-techniques[8].

According to **Omar Elharrouss**.et al., 2021 Image steganography is the process of hiding information, which can be text, image or video, in a cover image. Secret information is hidden so that it is not visible to the human eye. Deep learning technology, which has become a powerful tool in various applications such as image steganography, has recently received more attention. The main purpose of this paper is to explore and discuss the various deep learning methods available in the field of image steganography[9].

According to **Ahmad Zulfakar**.et al., 2024 This article focuses on three steganography methods in the spatial domain: LSB (least significant bit), PVD (pixel value difference), and edge-based data embedding (EBE) methods. A simple experiment was conducted to encode multiple images using these three methods, and LSB distortion measurements using mean square error (MSE) and peak noise ratio (PSNR) were investigated. Although the distortion measurement result of the experiment is considered acceptable for the LSB method, all methods produced a significant difference in file size[10].

III.PROPOSED SYSTEM

In today's digital age, secure communication has become increasingly important to protect sensitive information from unauthorized access and interception. To address this need, we propose a comprehensive system that leverages advanced image steganography and data hiding techniques for secure and covert communication. Our proposed system integrates several innovative approaches to enhance the security, robustness, and stealthiness of hidden messages within digital images.

1. Enhanced LSB (Least Significant Bit) Substitution

Our system will utilize an enhanced LSB substitution technique that incorporates randomization and encryption to embed secret data within the least significant bits of image pixels. By introducing randomness and encryption keys, we aim to increase the security and resilience against detection through statistical analysis.

2. Transform Domain Embedding with Encryption

Our system will employ transform domain techniques, such as Discrete Cosine Transform (DCT) or Wavelet Transform, to embed the secret data in the frequency domain of the image. Additionally, we will encrypt the transformed coefficients using advanced encryption algorithms to enhance the security and prevent unauthorized extraction of the hidden message.

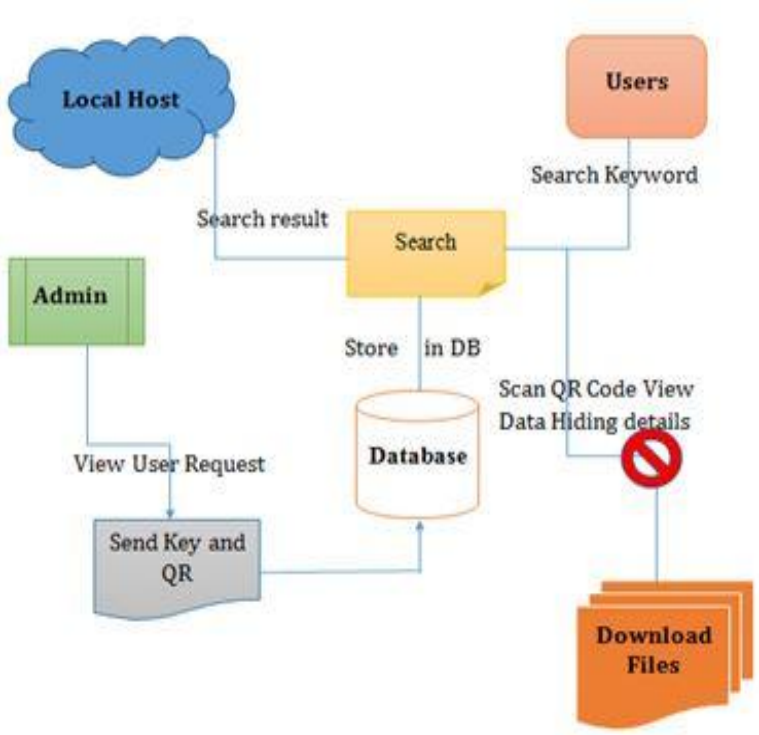
3. Distortion-Optimized Embedding Algorithm

We propose a distortion-optimized embedding algorithm that minimizes the visual distortion caused by embedding the secret data into the cover image. By optimizing the embedding process, our system aims to make the hidden message imperceptible to the human eye while maintaining high security and robustness against attacks.

4. Hybrid Steganographic Approach

Our system will combine multiple steganographic techniques, such as LSB substitution, transform domain embedding, and spread spectrum steganography, in a hybrid approach to leverage their strengths and mitigate their weaknesses. This combination will enhance the overall security, robustness, and stealthiness of the hidden message, making it more challenging to detect and extract.

ARCHITECTURE DIAGRAM



EXPLANATION

The architecture diagram represents a secure communication system designed to facilitate encrypted and covert messaging between users. The system comprises several key components, each serving a specific function to ensure the confidentiality, integrity.

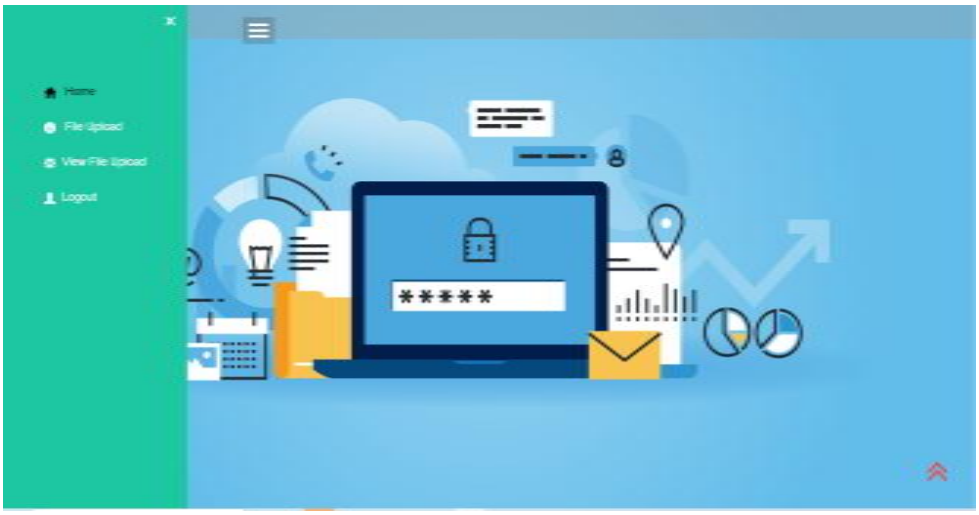
COMPONENTS

- **User Interface (UI)**: The UI component serves as the primary interaction point for users, allowing them to compose, send, and receive messages securely. It provides a user-friendly interface with features like message composition, contact management, and message history.
- **Encryption Module:** The Encryption Module is responsible for encrypting the outgoing messages using advanced cryptographic algorithms and keys. It ensures that the messages remain confidential and tamper-proof during transmission.
- **Decryption Module:** The Decryption Module handles the decryption of incoming messages using the corresponding decryption keys. It verifies the integrity of the received messages and decrypts them for display to the intended recipient.
- **Data Storage:** The Data Storage component stores the encrypted messages, decryption keys, user profiles, and other essential data securely. It employs robust security measures like encryption-at-rest and access control to protect the stored information from unauthorized access.

COMMUNICATION CHANNEL

The Communication Channel facilitates the secure transmission of messages between users. It leverages secure protocols like TLS/SSL to encrypt the data in transit and ensures the integrity and authenticity of the communication.

IV.RESULTS AND DISCUSSION



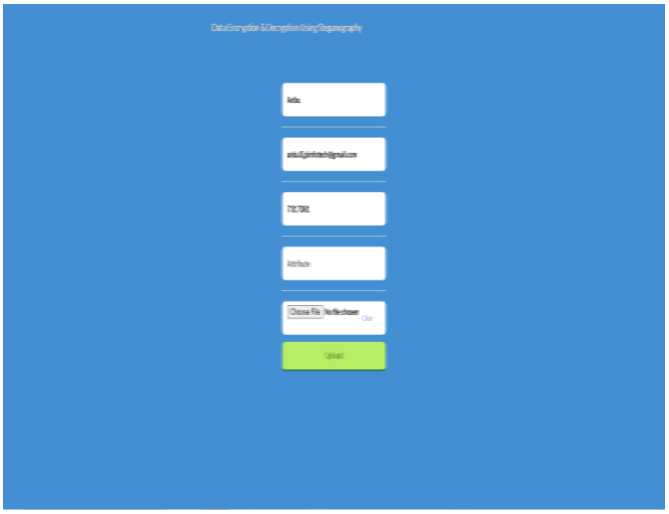


FIG.1 Home Page File Upload Page

a)The Home Page serves as the main landing page for the web application, providing users with an overview of the application's features, services, and offerings.

b)The File Upload Page allows users to upload files, documents, or media content to the web application securely. It provides a user-friendly interface with options to select files from local storage, drag and drop functionality, and progress indicators to track the upload process.

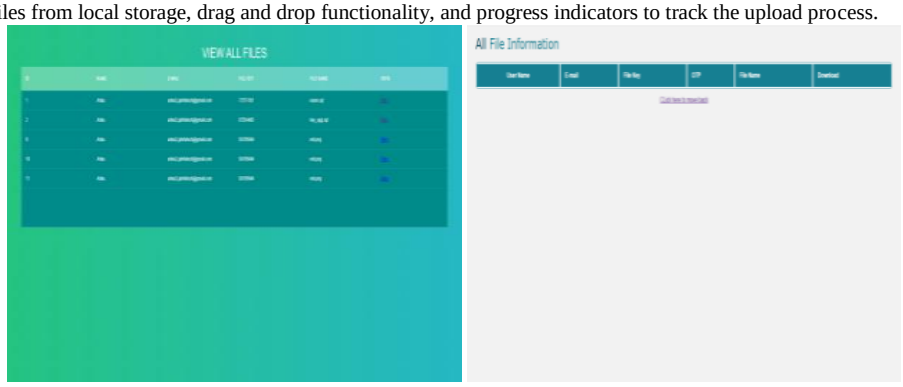


FIG.2User Data Center View Uploaded

a)The User Data Center serves as a centralized hub where users can manage, organize, and view their uploaded files, documents, and media content. It offers features like file categorization, sorting options, search functionality, and access control settings to help users maintain their data efficiently.

b) The View Uploaded Page displays a detailed list or grid view of the files, documents, or media content uploaded by the user. It provides options to preview, download, share, and manage individual files, along with additional metadata and information related to each upload.

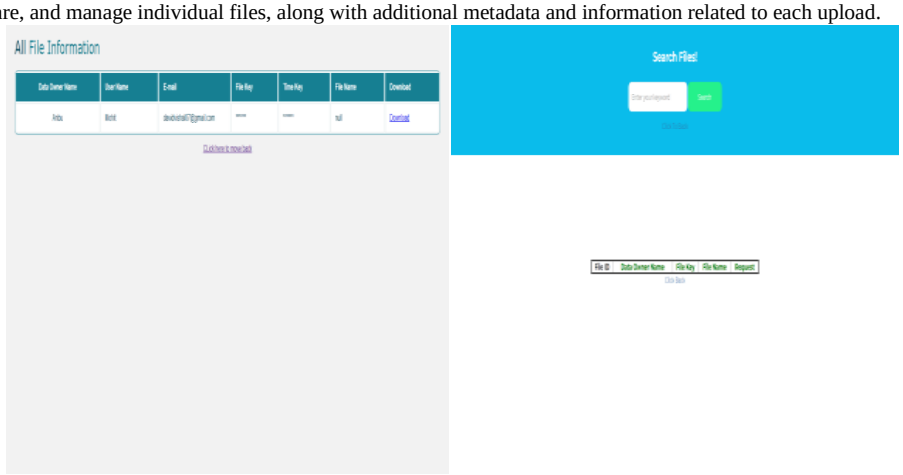


FIG.3User Search Page User Inbox Page

a) The User Search Page allows users to search for specific files, documents, or media content within their uploaded data using keywords, filters, and advanced search options.

b) The User Inbox Page displays a list of messages, notifications, alerts, or updates received by the user within the application. It provides options to view, reply, delete, and manage individual messages, along with filters and sorting options to organize the inbox content effectively.

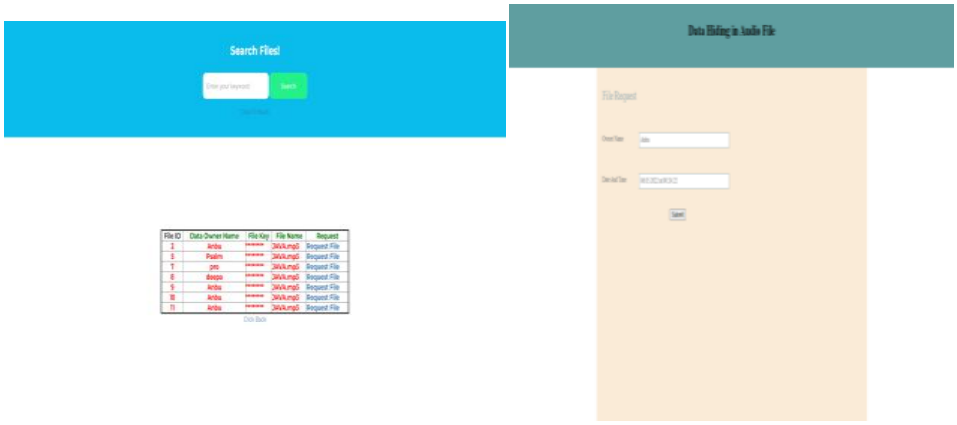


FIG.4 Search Request User Search Result

a) The Search Request functionality enables users to submit search queries or requests for specific information, files, or content within the application.
b) The User Search Result Page displays the outcomes or findings of the user's search request, showcasing a list of relevant files, documents, or content matching the search criteria. It presents the search results in a structured format with options to preview, download, share, and manage individual items.

V.CONCLUSION

In conclusion, the realm of image steganography and data hiding has witnessed remarkable advancements, paving the way for enhanced security and confidentiality in digital communications. While techniques like LSB substitution and spread spectrum steganography have laid the foundation, the integration of transform domain methods, adaptive strategies, and machine learning algorithms has elevated the sophistication and resilience of steganographic systems. However, the perpetual arms race with steganalysis techniques underscores the need for continuous research and innovation. As the digital landscape evolves, it is paramount to develop and refine techniques that not only conceal information effectively but also withstand rigorous detection attempts. Embracing hybrid approaches, distortion optimization, and dynamic key-based strategies can further fortify the security posture of steganographic solutions, ensuring their relevance and efficacy in safeguarding sensitive information in an increasingly interconnected world.

REFERENCES :

[1].H. Shi, X.-Y. Zhang, S. Wang, G. Fu, and J. Tang, ‘‘Synchronized detection and recovery of steganographic messages with adversarial learning,’’ in Proc. Int. Conf. Comput. Sci. Cham, Switzerland: Springer, 2019, pp. 31–43.
[2].Z. Wang, N. Gao, X. Wang, J. Xiang, and G. Liu, ‘‘STNet : A style transformation network for deep image steganography,’’ in Proc. Int. Conf. Neural Inf. Process. Cham, Switzerland: Springer, 2019, pp. 3–14.
[3].R. Zhang, S. Dong, and J. Liu, ‘‘Invisible steganography via generative adversarial networks,’’ Multimedia Tools Appl., vol. 78, no.7, pp. 8559–8575, Apr. 2019.
4. O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, ‘‘An image steganography approach based on k-least significant bits (k-LSB),’’ in Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT), Feb. 2020, pp. 131–135.
[5].M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. Srikanth, and M. Reddy, ‘‘Digital video steganography using LSB technique,’’ Red, vol. 100111, Apr. 2020, Art. no. 11001001.
[6].Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, Brendan Halloran 2019, Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research Neurocomputing 335, 299-326, 2019.
[7].Khider Nassif Jassim, Ahmed Khudhur Nsaif, Asama Kuder Nseaf, Bagus Priambodo, Emil Naf’an, Mardhiah Masril, Inge Handriani, Zico Pratama Putra 2019, Hybrid cryptography and steganography method to embed encrypted text message within image, Journal of Physics: Conference Series 1339 (1), 012061, 2019.
[8].Farooq Nabi, M Mazhar Afzal 2020,Image Steganography: Critical Findings through Some Novel Techniques, International Journal of Innovative Technology and Exploring Engineering 9 (5), 878-890, 2020.
[9].Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane 2021, Image steganography: A review of the recent advances IEEE access 9, 23409-23423, 2021.
[10].Ahmad Zulfakar Abd Aziz, Muhammad Fitri Mohd Sultan, Nurul Liyana Mohamad Zulkufli 2024, Image Steganography:: Comparative Analysis of their Techniques, Complexity and Enhancements, International Journal on Perceptive and Cognitive Computing 10 (1), 59-70, 2024.