IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cipher Shield

Steganography Project Using React and Python Libraries

[1]Rina Pawar, [2]Rajashri Chaudhari, [3]Sanskruti Kadam, [4]Siddhi Patil, [5]Dr.Siddharth Kalpagam

[1]Student, [2]Student[3]Student, [4]Student,[5]Associate Professor

[1]Computer Engineering ,

[1]Terna Engineering College, Navi Mumbai, India

Abstract: Steganography, an undercover communication technique, hides sensitive messages within seemingly innocent cover media to avoid detection. This research delves into the importance of steganography in enhancing data security and introduces Steganography Web, a secure platform for honing steganography skills using React and Python. The investigation underscores the significance of carefully selecting cover media and examines various steganographic approaches, particularly focusing on the commonly used Least Significant Bit (LSB) technique. Steganography's security stems from its capacity to challenge potential attackers in distinguishing between original and altered media, thereby maintaining a high level of correlation between them. In essence, steganography serves a vital role in safeguarding communications and safeguarding confidential information within our digitally interconnected society

Index Terms **- Steganography**, **Securecommunication, Steganography, Data privacy, React, Python, Imperceptibility, Encryption formatting.**

I. INTRODUCTION

Steganography Web integrates conventional steganographic methods with contemporary technologies to establish a secure platform for concealing and revealing hidden messages within digital media. Employing React for the frontend and Python for the backend, alongside tools like OpenCV for image processing, the platform delivers robust steganographic communication capabilities. Noteworthy features include face authentication, enhancing security levels. Its modular and scalable architecture facilitates seamless integration of new functionalities. Security protocols are comprehensive, encompassing encryption, access controls, and stringent data protection measures. By amalgamating age-old artistry with cutting-edge technology, Steganography Web furnishes a secure conduit for clandestine communication while emphasizing user- friendliness and confidentiality.

This project comprises three primary components:

1. Image Steganography: This component employs the LSB Algorithm to enable the embedding and extraction of messages within images. Functions like 'encodeMessage' and 'decodeMessage' manipulate the leastsignificant bits of pixel color components, ensuring covert communication.

2. Text Steganography: Utilizing the AES encryption standard, this segment ensures the secure transmission of textual data. User-input text undergoes encryption with a predefined secret key (SECRET PASS), safeguarding sensitive information and ensuring confidentiality during transit and storage.

3. Face Authentication: Augmenting security measures, this feature utilizes facial recognition technology for user authentication. Users register by capturing multiple facial images from varying angles, which are subsequently employed for identity verification during login. This authentication mechanism guarantees that only authorized users gain entry to the platform, thereby enhancing overall security.

II. OVERVIEW OF STEGANOGRAPHY

Steganography conceals confidential messages within innocent carriers to avoid detection, differing from cryptography by hiding the message's existence. Evolving from ancient to digital methods, it operates in digital media like images, audio, or text. Techniques vary, including LSB insertion and text-based methods. Applications include covert communication and copyright protection. Challenges include detection difficulty and misuse risks.

I. Text Steganography

Text steganography hides secret messages within ordinary text to enable covert communication. Unlike cryptography, which encrypts messages, text steganography focuses on concealing the message's existence. Techniques involve subtle text modifications, such as whitespace manipulation or hidden characters. It finds use in espionage, copyright protection, but detection and security risks remain challenging, requiring advanced analysis techniques.

II. Image Steganography

Image steganography conceals secret data within digital images without altering their appearance significantly. Techniques like LSB insertion, spread spectrum, algorithmic, and spatial domain methods are employed for this purpose. It finds applications in covert communication, digital watermarking, and authentication. Challenges include detection difficulty and potential information loss or corruption.

Steganography projects aim to discreetly embed information within various data formats, ensuring imperceptibility and resistance to detection. Challenges include maintaining carrier quality while concealing messages and striking a balance between imperceptibility, capacity, and security. Integration of cryptography, digital signal processing, and information theory principles facilitates this balance, ensuring successful hiding of information while maintaining integrity and resilience against detection.

III. NEED OF THE PROBLEM

The need for steganography arises from its vital role in concealing information within various data formats, serving multiple purposes. Steganography plays a crucial role in safeguarding privacy by allowing sensitive data to be hidden, facilitating covert communication, and securing intellectual property through techniques like digital watermarking. Moreover, it ensures data integrity, assists in secure government communication, aids in user authentication, and complicates digital forensics efforts. In essence, the necessity for steganography lies in its indispensable contribution to privacy protection, communication security, intellectual property safeguarding, and cybersecurity enhancement.

IV. PROBLEM STATEMENT

The project addresses the need for covert communication and secure data transmission, especially when confidentiality is crucial. Traditional encryption methods can be detected and decrypted, making them insufficient. Steganography offers a solution by hiding information within harmless carrier files. However, effectively implementing steganographic techniques faces challenges like maintaining carrier quality and ensuring security. The project aims to develop techniques to overcome these challenges, providing a reliable means of embedding and extracting information covertly across different formats while ensuring integrity and confidentiality.

V. OBJECTIVES

We are dedicated to advancing steganography through research, technological innovation, and community engagement. Ourfocus includes exploring new libraries like OpenCV, advocating for interoperable standards, educating users about steganography's capabilities and risks, and fostering a collaborative community. Through these efforts, we aim to enhance data security and promote responsible steganographic usage.

VI. ALGORITHM

Initially, users must register by providing their chosen username and password. Subsequently, the website will capture a photo of their face for authentication purposes. Upon successful registration, users can proceed to log in. If the entered credentials are accurate, the user will be logged in; otherwise, access will be denied. Once logged in, the main page will be presented, offering two options: text steganography and image steganography. Users must select one of these options and proceed with the encryption process.

The Least Significant Bit (LSB) algorithm is a method used in steganography, which involves hiding messages or information within non-secret data. The method we choose for data encryption is the Least Significant Bit (LSB) . The LSB algorithm achieves this by replacing the least significant bit of each byte in an image with a bit from the message to be hidden. Since the least significant bit contributes the least to the overall value of the byte, altering it slightly is less likely to significantly affect the quality of the image to the human eye.

How the LSB algorithm works:

1. Select an Image: Choose an image to serve as the carrier for the hidden message.
2. Encode the Message: Convert the message to be concealed into binary format. Typically, this is done by converting each character into its binary representation.
3. Embedding the Message: Replace the least significant bit of each pixel in the carrier image with one bit of the binary message. The message bits are embedded sequentially into the pixels of the carrier image, usually starting from the top- left corner and moving across rows.
4. Store Message Length: It's common practice to store the length of the message in the first few pixels to aid extraction later.
5. Save the Image: Save the modified image containing the hidden message.
6. Decoding the Message: To extract the hidden message, extract the LSBs of each pixel in the encoded image and concatenate them to reconstruct the binary message. The length of the message is often retrieved from the first few pixels.

It's important to note that while the LSB algorithm is relatively simple and offers some level of security, it is vulnerable to various attacks such as statistical analysis, which can reveal the presence of hidden data. Additionally, compression algorithms or certain image transformations can distort or destroy the hidden message.

Algorithm for Image Steganography (Least Significant Bit - LSB)

1. Message Length Conversion: Begin by converting the message length into binary and concatenate it with the binary representation of the message.
2. Variable Initialization: Start by initializing an array named "history" to track modified locations in the image colours. Use the variable "pos" to iterate through message bits.
3. Iterating Through Message Bits: Enter a loop to process each message bit.
4. Determining Next Modification Location: Call the "getNextLocation" function to determine the next location in the image colours to be modified. This function should return a valid index within the colours array range.
5. Setting LSB of Colour Component: Set the least significant bit (LSB) of the colour component at the chosen location to the current message bit.
6. Advancing to Next Colour Component: Increment the location (loc) until reaching the next colour component.
7. Setting Alpha Channel: Set the alpha channel (transparency) of the colour component to 255.
8. Advancing to Next Message Bit: Increment the position variable to move to the next bit in the message.

Algorithm for Face Authentication Using Local Binary Patterns Histograms (LBPH)

1. Image Pre-processing: Convert the image to grayscale if it's in colour .
2. Dividing Image into Cells: Divide the pre-processed image into a grid of cells.
3. Computing Local Binary Patterns (LBP): For each cell in the grid, compute the Local Binary Pattern.
4. Generating Histograms: After computing the LBP code for each cell, generate a histogram for each cell.
5. Concatenating Histograms: Concatenate the histograms from all cells to create a feature vector representing the entire image.
6. Evaluation and Refinement: Evaluate the performance of the LBPH-based system on a separate test dataset and refine as necessary.

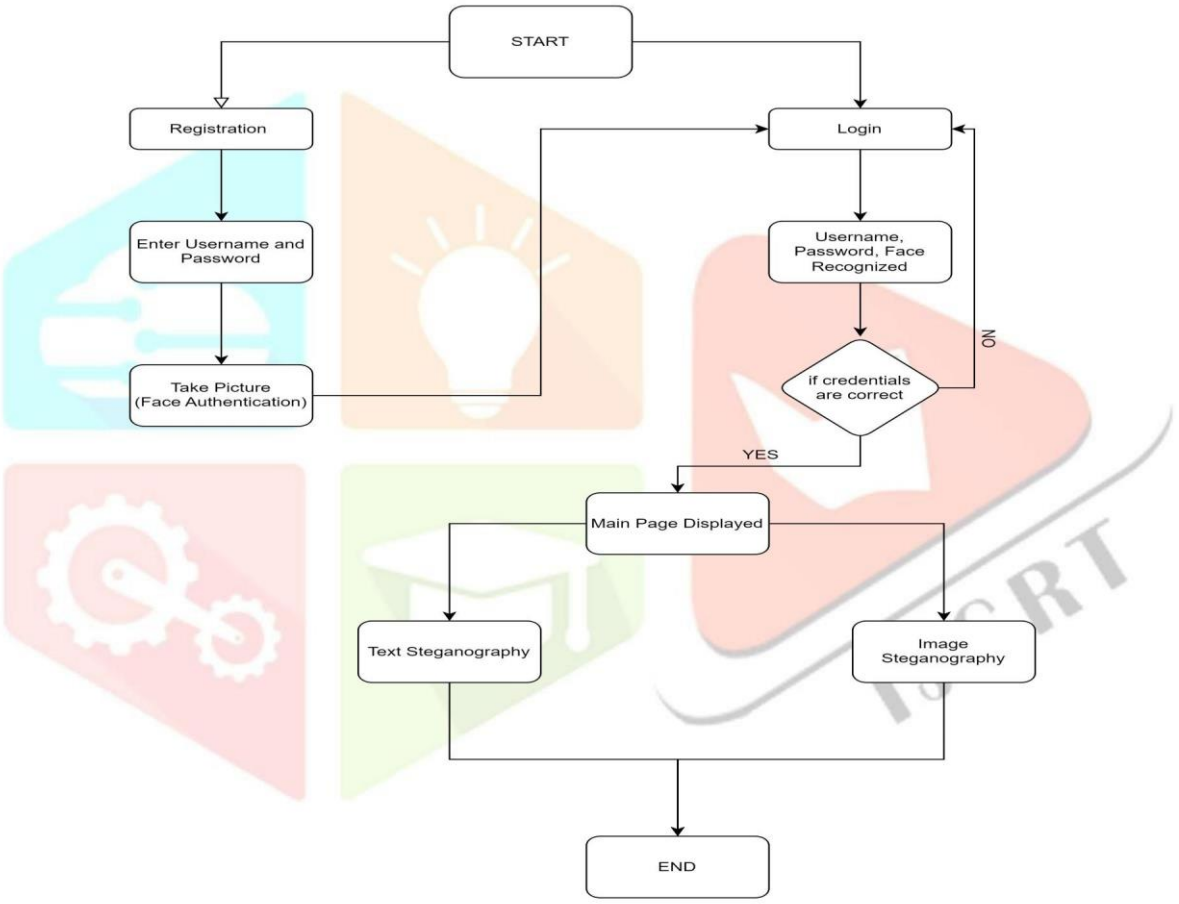

Figure 1 : Flowchart

VII. CONCLUSION

In our steganography project, our primary objective was to advance the field of data concealment and secure communication. Our focus was on improving the imperceptibility, data capacity, and security of steganography techniques across various media formats. Throughout our project, we achieved significant progress in these crucial areas.

Our developed techniques empower users to seamlessly embed and extract data within images and text documents with exceptional discretion and efficiency. By enhancing the imperceptibility of these methods, we ensure that the concealed information remains undetectable to human senses, thereby safeguarding the secrecy of communication. Furthermore, a substantial portion of our efforts was dedicated to bolstering the security of these techniques to effectively withstand steganalysis attempts. By enhancing their robustness and resilience, we ensure that the concealed information remains secure from unauthorized access or detection.In addition to technical advancements, we prioritized ethical and legal considerations throughout our project. We emphasized the responsible and legitimate use of steganography, while also addressing privacy and security concerns. It's essential that technology serves the greater good while adhering to legal and ethical principles. In conclusion, our project endeavours to make positive contributions to the field of steganography by advancing its capabilities, facilitating the safe transmission of concealed information, and promoting ethical and legal practices in its application. We firmly believe in upholding the principles of legality and ethics in all our technological endeavours.

VIII. IMPLEMENTATION AND RESULTS

Figure 2

Login Page

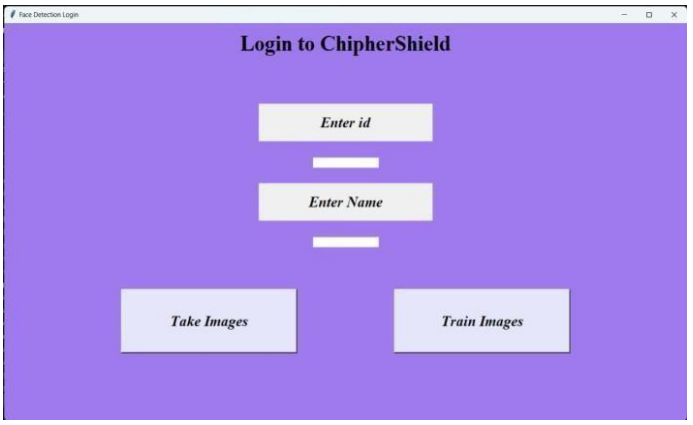

Figure 3

Registration Page

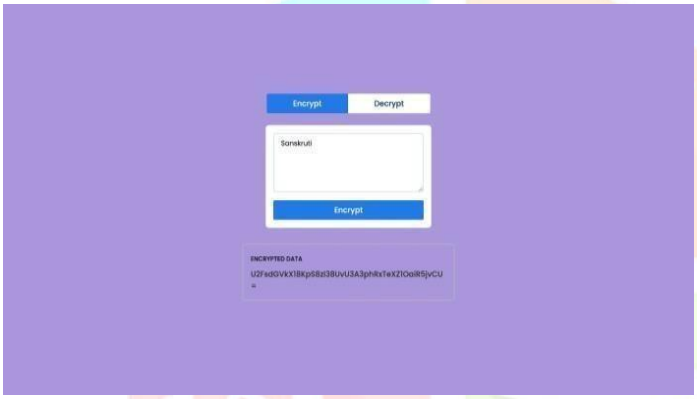

Figure 4

Text Encryption

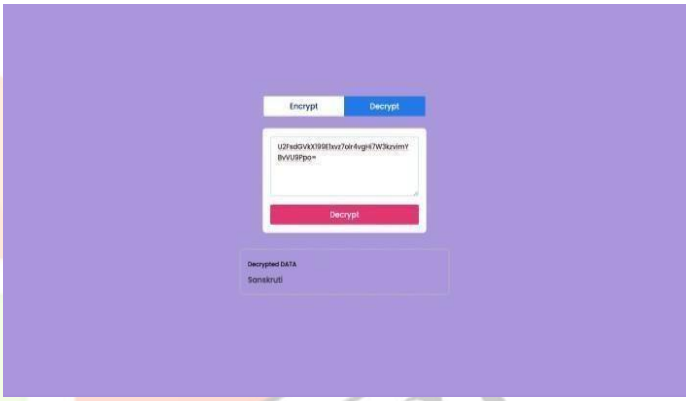

Figure 5

Text Decryption

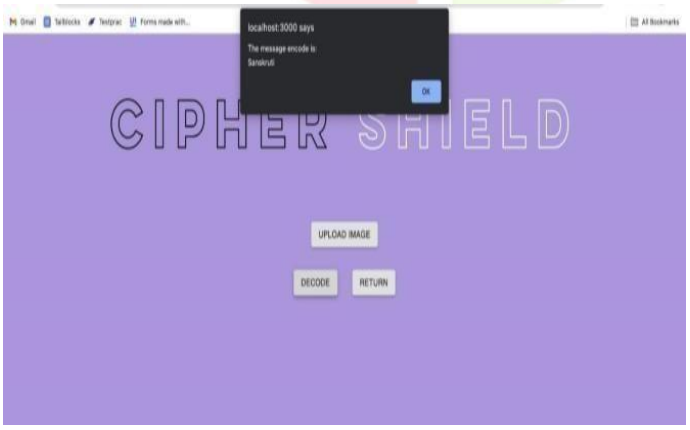

Figure 6

Image Encryption

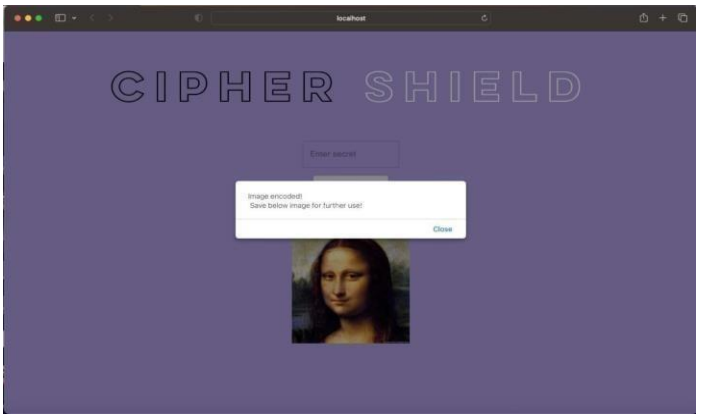

Figure 7

Image Decryption

IX. REFERENCES

[1] Ritweek Raj, Ayush Gupta, Prof. Siva Shanmugam, "Image Steganography Using CNN ," School of Computer Science and Engineering Vellore Institute of Technology , Vellore , Tamil Nadu , May 22, 2023.

[2] Osama Fouad Abdel Wahab , Ashraf A. M. Khalaf Aziza I. Hussein And Hesham F. A. Hamed , "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques", vol. 9, March 2021.

[3] Eshraq Hureib Andan Guthub , "Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography", University of Umin Al-Qura, University of Umm Al-Qura, Makkah, Saudi Arabia, VOL.20 No.8, August 2020.

[4] Xintao duan Kai jia Baoxia li Daidou guo En zhangand Chuan qin "Reversible Image Steganography Scheme Based on a U-Net Structure",College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China , School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, Chin