Data Transfer Security with Steganography

A major project report submitted in partial fulfillment of the requirement for the award of degree of

Bachelor of Technology

in

Computer Science & Engineering / Information Technology

Submitted by

Shikhar Khandelwal (201441)

Shyamansh Sharma (201251)

Under the guidance & supervision of

Mr. Arvind Kumar, Assistant Professor (Grade-II)

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology,

Waknaghat, Solan - 173234 (India)

Candidate's Declaration

We hereby declare that the work presented in this report entitled **'Data Transfer Security with Steganography'** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science & Engineering / Information Technology** submitted in the Department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology, Waknaghat is an authentic record of my own work carried out over a period from August 2023 to May 2024 under the supervision of **Mr. Arvind Kumar,** (Assistant Professor (Grade-II), Department of Computer Science & Engineering and Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature with Date)
Student Name: Shikhar Khandelwal
Roll No.: 201441

(Student Signature with Date)
Student Name: Shyamansh Sharma
Roll No.: 201251

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature with Date)
Supervisor Name: Mr. Arvind Kumar
Designation: Assistant Professor, (Grade-II)
Department: CSE/IT
Dated:

ACKNOWLEDGEMENT

Firstly, we express our heartiest thanks and gratefulness to almighty God for His divine blessing which made it possible to complete the project work successfully.

We are grateful and wish our profound gratitude to Supervisor **Mr. Arvind Kumar, Assistant Professor (Grade-II)**, Department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat.

Deep Knowledge & keen interest of our supervisor in the field of "**Data Transfer Security with Steganography**" to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, and valuable advice have made it possible to complete this project.

The in-time facilities provided by the Computer Science department throughout the project development are also equally acknowledgeable.

Last but not the least, our sincere thanks to all our teachers and friends who have helped us straightforwardly or in a roundabout way in making this project a win.

Finally, we acknowledge with due respect the constant support and patience of our parents.

Shikhar Khandelwal
201441

Shyamansh Sharma
201251

TABLE OF CONTENT

Content **PageNo.**

Declaration by Candidate ii

Acknowledgment iii

Abstract viii

Chapter 1: INTRODUCTION

1.1 General Introduction..... 1

1.2 Problem Statement. 3

1.3 Objectives.....4

1.4 Significance and Motivation..... 5

1.5 Organization. 7

Chapter 2: LITERATURE SURVEY

2.1 Overview of relevant literature 8

2.2 Key Gaps in literature.....22

Chapter 3: SYSTEM DEVELOPMENT

3.1 Requirements and Analysis 24

3.2 Project Design and Architecture..... 26

3.3 Data Preparation. 30

3.4 Implementation.....33

3.5 Key Challenges..... 44

Chapter 4: Testing

4.1 Testing Strategy.....45
4.2 Test Cases and Outcomes.....46

Chapter-5 Results and Evaluation

5.1 Results.....48

Chapter-6 Conclusions and Future Scope

6.1 Conclusion.....53
6.2 Future Scope.....53

LIST OF FIGURES

S. No	Title	Page No.
1	Project Design	26
2	Image Structure as a Stego Image	27
3	Steganographic concealment process	28
4	Sample Image Used in Steganography	31
5	Optimal Image for Steganography	32
6	Authentication Program using Axios	34
7	Program defining Chat structure and chat engine	35
8	Program defining Chat App Layout	36
9	Program for Encryption function	38
10	Program for Decryption function	40
11	Input form for Image Steganography	46
12	Decrypting form for Stego Image	47
13	Login UI	48
14	Chat Section	49
15	Image Upload Section	50
16	Image Extractor UI	51
17	Image comparison before & after Steganography	51
18	Comparison with histogram	52

LIST OF ABBREVIATIONS

S. No	Title
1	AES: Advanced Encryption Algorithm
2	DES: Data Encryption Standard
3	LSB: Least Significant Bit
4	SIS: Steganography Imaging System
5	UI: User Interface
6	UX: User Experience
7	GIF: Graphics Interchange Format
8	GUI: Graphic User Interface
9	TCP: Transfer Control Protocol
10	IP: Internet Protocol
11	SNR: Signal to Noise Ratio
12	MHC: Maximum Hiding Capacity
13	MSE: Mean Square Error
14	BMP: Bit Map File Form
15	JDK: Java Development Kit
16	PSNR: Peak Signal to Noise Ratio
17	DFrFT: Discrete Fractional Fourier Transforms
18	RGB: Red, Green, Blue

ABSTRACT

Data loss, privacy concerns, and security problems usually follow popular means of communication such as messaging apps. Steganographic and image overlay combine to provide an innovative means of data security in apps. In our project, we solve the problem associated with image cropping as it leads to data loss through two protection layers. As such, the initial image is encrypted with strong encryption algorithms to prevent illegal access. Subsequently, steganography involves hiding of an encrypted image within a larger cover image. Through this approach, vital details may be shielded even when the photo is trimmed. The integrated way of preventing such loss entails an additional protective layer as the original picture will be hidden within the overlying picture. The steganography in data transfer security integration is a complex procedure which involves a number of techniques and methods. Digital images are one of the most widespread mediums for hiding information because they are so prevalent and can store a great deal of data including the most vital, such as spy teams are not likely to even notice them. Procedures such as LSB (Least Significant Bit) substitutions, that substitute the least significant bits of pixel values with data to be hidden, and masking and filtering in the spatial domain are the examples of these techniques that provide hiding information within the image files. Consequently, audio steganography employs the manipulation of sound waves which are virtually unnoticeable to hide the secret data in the sound files, while the text-based steganography manipulates the linguistic elements such as spacing between words, punctuation marks, or word choice to embed the covert messages in the seemingly normal text. Furthermore, the overlay also appears OK, which means that nobody would find any difference. Our project will be user-friendly and implemented on a chat application so that people can easily access it. The users will be able to transmit information through this application, with confidence that no one else is spying on the transmission of the information. Our project assists in making messaging apps more secure by ensuring data integrity and privacy. Thus, one can comfortably communicate thoughts or experiences they have encountered knowing that data integrity and privacy is guaranteed

CHAPTER 1: INTRODUCTION

1.1 Introduction

Communication has changed from the conventional ways to an unhindered interaction across long distances in the current digital era. Nonetheless, digital communication entails ensuring that people's privacy and data is safe. In today's world of interconnectivity in which individuals provide their most confidential data to electronic communication mediums, securing our conversations is critical.
We put forward a novel scheme that combines steganography in text messaging. This revolutionary method lays down a solid foundation for a reliable and safe communication channel where people can communicate confidentially without jeopardizing the message.

The development of our project, however, goes beyond a mere innovation. It clearly reflects our concern for privacy and reliability in messaging. In our project, we have a deep understanding of the problems that face people or an organization due to data breaching and piracy.
This is the way we want our proposed solution to be seen as the flagship of innovation in total integration of data protection. Using steganographic principles, we created a system that integrates secret messages in normal SMS, hiding them from curious eyes. However, this approach surpasses conventional techniques by adding another level of protection that is almost imperceptible.

Our project is vital and not only relates to personal communication. In a market place, which shares all kinds of delicate details, safe channels of communication are crucial. We have a powerful and secure network for businesses that keeps an organization's sensitive information and company information safe.

Essentially, we have built our project based on accessibility and simplicity. Aware that technology must support and not impede, hence our easy-on-use interface to support users who are either techies or non-techies. Our platform is designed to seamlessly integrate with your existing communication routines, making it accessible whether you are an experienced tech fan or just a beginner.
Also, it scales up and can serve an array of communication requirements, from person-to-person to organizations' communications. Such scalability enables our project to efficiently tackle the varying communication needs of individuals and organizations.

Key Points:

- Keeping the content of confidential text messages safe.
- Modern day steganography for encryption.
- Improving data security and privacy in digital communications.

Overall, our project marked an outstanding milestone in the world of secured communication. We have developed a highly effective instrument which can be used by individuals and organizations to guard their private data and confidential information; and all this is achieved by incorporation of steganography within ordinary-text message mode. Our solution has a very simple interface and provides strong scaling capabilities, which could revolutionize how we conduct communications in the twenty-first century.

1.2 Problem Statement

Messaging applications have changed the way we communicate on a regular basis; however, it is often accompanied by a compromise in security. The weakness is a major risk to people, organizations, and governments, especially regarding data safety like military or political functions.

Transmitting sensitive information is critical in military and government communication as it supports decision making, strategic planning and operation success. This critical information, however, is exposed because the existing messaging apps are not sufficient, and it could compromise national security and threaten missions. Without this type of encryption, unauthorized people are able to read messages that should remain secret. As an encrypted message gets attention on the internet and can be easily decoded with the help of cryptanalysis to solve this detect.

1.3 Objectives

These are the objective of developing our project: -

Enhanced Encryption

- Integrate multi-layered encryption: Employ multiple layers of encryption to provide an extra level of security and protection against potential decryption attempts.

Steganography Integration

- Seamlessly embed messages within images: Develop a steganography technique that seamlessly embeds text messages within the inconspicuous layers of images without compromising image quality.
- Optimize image selection for steganography: Identify image formats and characteristics that are most suitable for steganographic embedding, ensuring efficient data hiding and retrieval.
- Evaluate image fidelity: Assess the impact of steganography on image quality to ensure that the embedded messages do not perceptibly alter the original image.

Military and Government Focus

- Tailor security protocols to high-security needs: Adapt security protocols and encryption algorithms to meet the stringent requirements of military and government communication.
- Integrate secure communication protocols: Integrate secure communication protocols, such as IPsec and TLS, to ensure secure data exchange over public networks.

1.4 Significance and Motivation of the Project Work

The modern digitally integrated world where messaging applications are vital for secure and reliable messaging service. These messaging apps are left unguarded as they fail to provide sufficient data protection mechanisms, allowing sensitive data to be exposed to illegal access as well as data breaches. The existence of people, business entities and government departments during such military and government operations, commercial transactions and private conversations is threatened by this risk due to the importance of data integrity and confidentiality.

Our objective in this new project will therefore be to fill this vital hole through development of a new text messenger. Advanced encryption such as steganography provides an unprecedented level of data security. It also offers another form of traditional security which is different from steganography, which is essentially the art of hiding data within apparently harmless materials. encryption methods. Our app embeds highly secret SMS into invisible layers of pictures thus protecting them against intrusion-and-misappropriation.
Our project is important because it provides the much-needed secure and reliable message platforms in diverse areas of the economy.

Our solution offers several compelling benefits that make it a valuable asset in today's data-driven world:

- **Enhanced Data Security**: Our messaging app uses high-end encryption and Stenographic methods to guarantee that information is safe from outsiders and hackers.
- **Protection of Sensitive Information**: In our solution, we securely guard against unauthorized access to individuals' personal details, corporate information, and intellectual property, thus averting such possible liabilities as monetary loss, public relations debacle, and litigation.

- **Compliance with High-Security Standards:** The measures of quality assurance for our- application include those recommended for critical applications like military, government operations.
- **Safeguarding National Security**: Our solution allows for the safe flow of sensitive information in military and government communications vital for making sound decisions, formulating the strategy, and successfully waging war.
- **Empowering Individuals**: The messenger of our application allows people to conduct safe and private talks without divulging their information or secret discussions for other persons to get through them.

Our understanding about these challenges has driven the motivation behind the current project. Data privacy and security is important as it builds trust between individuals, protects business interests and secures nation states. We want to design new approaches towards solving this key challenge while enabling people and organizations to safely interact and share information freely.

Our project goes beyond just ensuring that there is adequate protection for information. This is the major improvement in development of secure communications technologies for protection of varied information. It is believed that our project may revolutionize communications in the current digital era where people are comfortable sharing confidential details through texting and messaging systems.

1.5 Organization of Project Report

The report is organized as follows:

- Chapter 2 outlines the existing related work in the field of Steganography and encryption powered web applications in information security. It further presents the outputs.

- Chapter 3 puts forward the system that is formulated to cater the chat application with steganography to send and receive the message seamlessly. This is where we cover the requirements, project design and implementation along with challenges faced with the explanation of the programs.

- Chapter 4 is all about testing the system for the accuracy and precision of the chat app and the steganography for encryption and decryption discussing the test strategy, test cases and outcomes thus produced.

- Chapter 5 puts forward the analysis of the results in depth and also with content to existing work in the field.

- Finally, Chapter 6 presents the conclusion of the study. It also contains the application contribution with future scope of the project and how we are planning to improve it .

CHAPTER 2: LITERATURE SURVEY

2.1 Overview of Relevant Literature

This article on reference [1] defines image steganography covers a wide range of methods employed and their contribution by several scholars. One of these contributions is Ramadhan JM's paper that introduces new techniques in the field of image steganography. This is the very first time that the DFrFT and the LSB method have been incorporated in this paper. Each of these methods presents a different way of hiding information in digital pictures. Unlike the DFrFT where the transform domain is incorporated to hide data, LSB manipulates the least significant bits of pixel values.

Also noteworthy is the use of a bit-inverted technique in Savita Bhallamudi's work that improves security and image quality found in LSB-based steganography. The LSB algorithm makes the steganography more robust to detection but provides a better visual quality for the cover image increasing the stealthiness and security of the algorithm.

Yet another contribution is by Lee, G. J., who supported Yong's suggested solution for overcoming the complexity challenge in applying various steganographic methods. Yong's approach uses in real time unauthorized picture transmission, hiding verification information data in coefficients of random polynomials. The new approach aims at lowering down this huge computational burden in order to speed up both encoding and decoding of covertly contained information resulting in a highly useful steganography system.

Additionally, the findings of Nagam-Hamid and Ahaya Abid reveal more insights about IWT and security against high frequency wavelets. In their case, they emphasize on the resiliency and security aspects of steganography using IWT. The

use of high-frequency sub-band demonstrates a better ability to conceal the data without being compromised by diverse image processing assaults.

This Research paper concludes with high PSNR values have been detected, effective encryption, but data loss in noisy environments.

The paper [2], highlights important features regarding information security while transferring private details among parties. The paper focuses on the need for combined use of cryptography with steganography to improve overall protection of data during communication. Cryptographic algorithms encode content but reveal it at the same time while steganography hides secret messages inside some other type of media which guarantees invisibility to non-authorized persons.

The paper proposes a new scheme of utilizing crypto steganography that is based on a combination of stenographic techniques and cryptographic algorithms. Such fusion enables the safe hiding of secret data in pictures. It's a way to prevent such malevolent agents from intercepting the communication and discovering the information.

Within the paper, a literature review is undertaken on different forms of steganography with emphasis on color image-based techniques for their vast hiding capacities. The large information content available in image color channels can be used for implementing more voluminous steganographic data. They consider various color spaces and channels, including RGB and YCbCr, for altering pixel values and hiding secret information without drastically reducing the visual quality of the cover picture.

The document summarizes the role that combines cryptography and steganography in protecting information integrity as it moves. This highlights color image-based steganography as an effective way for secretly hiding big chunks of sensitive information in image holders and protecting them from disclosure and illegal usage.

It has an efficient method for data transmission while keeping the data hidden.

Reference paper [3] uses binary message embedded in image pixel, sophisticated way for making information secret. A multi-stage algorithm that starts with compressing data through zip file method and ends to converting into binary codes enables efficient use of memories and hides information in digital images.

The developed Steganography Imaging System (SIS) represents a substantial advancement, featuring an enhanced algorithm. SIS functions as a user-friendly interface allowing seamless uploading of images and text for the embedding and extraction of data within images. Operating on a two-tiered approach, SIS prioritizes reinforcing data confidentiality and ensuring the integrity of concealed information.

The SIS is designed as a significant upgrade of the SIS, with improved algorithms. SIS serves as an easy-to-use point through which one can load texts and pictures into images for the purpose of both data storage and extraction. Using a dual approach, SIS focuses upon maintaining privacy of the hidden information as well as supporting integrity of concealed data.

The strong safety measures to protect secrecy and reliability while compressing and restoring image data ensures that potential data corruption/breach are prevented. Such an approach also highlights the need for sharing data via more than one carrier and prevents leaking or revealing details about the hidden facts.

Taking off from prior studies on digital watermarking, this article focuses on masking signal essence and intercalating information in differing canisters. The built-up algorithm and SIS approach uses binary data hiding and compression that enables secret and accurate transit as well as data protection. It is thus very important in ensuring that confidential information in a digital world is secured.
It has efficient data hiding, minimal image distortion, higher PSNR values.

Reference paper [4] published in 2020 highlights the importance of transmitting confidential information in a safe manner thereby leading to investigation of steganography. The concept centers on the incorporation of hidden information into the carrier channel that holds the message, which can be pictures, video recordings, or music files. For this reason, the primary aim is to make sure that the data remains unnoticed using encrypted messages where the information is controlled through a certain key, which significantly improves the overall methods of transmitting information.:

It has been revealed in this paper a historical overview on Stenography which provides insight into its background, and mentions that it has been used earlier in prisons in order to pass secret messages between prisoners and outside people. Such a historical perspective is a glance at how old this technique is and it has existed and applied for so many years in diverse set ups.

It recognizes the pervasiveness of digital media, specifically images, as the preferred vehicle of stego communication. In recognition of image as a popular means of communicating, they can now be used as hiding places for confidential information. The paper aims to reveal the mathematics behind different steganographic processes that focus on image steganography. Classifying these practices is quite difficult since they have multi sided properties and every strategy involves particular formulas to encode and retrieve hidden data from photographs.

The paper also goes deeper in the mathematics of image steganography methods using different approaches. Such methods are complex to identify as they have several approaches that make it difficult to generate a common standard for categorization.

The paper presents a detailed account of how the techniques, algorithms, and mathematical principles used for hiding data elements in photos work. Such specific investigation points to the importance and difficulty of employing pictures as secret

signs of information transmission into the modern cyber environment, which is currently widespread within the most widely used kinds of Internet communication.

It has a better classification of image steganography techniques, importance in data security.

The article [5] is very detailed as it focuses on securing information, system, environment, society, economy, and state protection. The holistic approach appreciates that security is a multi-faceted concern. There are threats like hardware destruction, theft, unauthorized access, and data sharing – these have wide repercussions wherever you look.

In this regard of assurance of security, Steganography, a way of communicating secretly is discussed in the paper. In contrast with cryptography whose purpose is to protect information so that it can remain confidential, Steganography hides the fact whether there exists a transmission of data. This approach encrypts the messaged into innocent carriers such that it does not draw attention to unwanted listeners.

Additionally, this essay particularly focuses on Crypto-Steganography, which is the synergy of steganography and cryptography that seeks to enhance information security with the combined benefits and weaknesses of each discipline. In other words, this method involves embedding encrypted message in carriers, thus providing an additional layer for shielding information.

To put it simply, there are several categories of Steganography, namely, texts, pictures, sounds, and videos. Focusing mainly on image-based steganography and especially LSB technique. This approach entails modifying the least significant value digits of pixels in a digital image whereby changes made cannot be seen by human eyes.

Using one such technique, LSB, this paper highlights how images may be made to serve as effective carriers of hidden information and thus strengthen the protection of data. In other words, visual data are important and can be vulnerable, and so new ways of hiding and protecting information inside them must be sought. In this paper author Successfully combines cryptography and steganography for data security and image quality evaluation.

The Reference paper [6] works on confidentiality of data in modern digital settings is now a critical element. This is important given that sensitive data moves across electronic networks, and the authors recognize this fact. Deep packet inspection as a new instrument for checking security of messages transmission via the Internet. It enables analysis and inspection of information packages on-the-spot to identify possible risks and communication security failures. Notably, malicious entities may take advantage of the interception nature of transmitted information to access it and distort it.

Using AES encryption and LSB steganography into a single security strategy, proposed is a double- layer approach towards protection of confidential data. The hybrid technique utilizes the strengths of encryption and steganography in order to improve data security.

The first layer entails inserting a hidden text message into an LSB of a digital impression file. In the case of the LSB steganography, there is the use of the inherent redundancy within the digital image files to change the least significant bit of the corresponding pixel values so as to encode the secret message. These changes appear invisible to the human eye with this procedure retaining the photo's overall appearance and protecting the hidden data.

The processed stego image is then encrypted using the AES (advanced encryption standard) algorithm and in combination with a 128-bit encryption key. The use of the AES encryption process strengthens the security of the stego. This is because in order for one to use the AES encryption, he must have the key for the encryption as well as decryption processes. The second layer of encryption is a further measure for safe-guarding the hidden data embedded in the photograph.

The paper has literature review that explains recent steganography methods and data protection practice commonly found in recent studies. The paper outlines some improvements that have been made on LSB and also discusses adaptive LSB schemes

as well as confidential keyed LSB techniques and multi-planar data embedding in RGB components. Still, the review doesn't delve deep into particular strengths and failures at distinct scenes for individual methods.

A crucial aspect of data security known as cryptography is defined as a practice of transforming intelligible information into gibberish data. It emphasizes that cryptography is an established
technology that uses mathematical algorithms to encrypt data when it passes through networks such as the Internet. Nevertheless, it is important to point out that this paper raises a major issue. It highlights how cryptanalysts can analyze ciphertext. In response to this vulnerability, more layers of security are required to strengthen data protection against data interception and other forms of unauthorized access.

The paper introduces steganography which is yet another way of securing communication in times of cryptanalysis. The other approach that is also the complementary one in place of cryptography is steganography which means art and science of hiding a message in another data. Steganography is different from cryptography since it deals with hiding the data within what seems to be a harmless carrier like a picture, an audio file, or even a video. The goal is to camouflage the presence of the encoded information in such a way that third parties will not be able to identify its location and thus prevent them from extracting this secret information.

The authors also examine various steganographic techniques and approaches which can be used in practice. They encompass the concept of hiding secret information into over media that include different algorithms and procedures. For example, image steganography is considered as one of the popular ways because images are widely involved in digital communication. Such a method incorporates data in the pixels of an image utilizing the fact that lots of stuff can fit into pictures without being obvious.

A paper focusing on how these two concepts work side by side towards ensuring the safety of data is provided. Steganography is different from cryptography in that

stenography does not even indicate what information it contains. The amalgamation of these approaches, popularly termed crypto- steganography, is one solid approach that integrates encrypted and secret messaging techniques. This combination is intended for improving data secrecy as it consists of many stages through which only authorized people are allowed to send and receive encrypted information.

The paper, in summary, highlights the ever-expanding area of data security and the necessity of diverse measures to ensure secrecy. The use of cryptography and steganography ensures that data is
protected from being intercepted, analyzed and accessed by unauthorized persons during communication in the digital environment.

It has enhanced data security via combined cryptography and steganography with quality stegoimages.

The authors of [7] propose a two-stage security strategy that couples the AES algorithm and LSB steganography. Steganography employs this redundancy of digital image files. A secret text message is encoded in the first layer with data encoding process of LSB steganography in a digital image file of a picture. ``` The second layer uses the AES algorithm and an encryption key of 128 bits to encrypt the stegoimage, providing additional security.

The literature review of the paper outlines various modern steganography and data security practices and approaches. Existing research has utilized advanced LSB algorithms, adaptive LSB schemes, LSB with confidential key and embedding data into all planes of the RGB component but his research paper lacks in limited evaluation metrics and absence of comparative analysis with existing methods.

The combination of steganography and AES encryption provides a robust and secure method for data protection.

The authors of [8] mention this dichotomy as they explore the way different actors employed steganography for benevolent and malignant ends. Civil rights organizations also engage in Steganography which is a form of hiding a message in order to maintain secrecy and avoid any sort of interference. Notwithstanding, this technique has also been abused by bad actors including terrorists' groups for hiding illicit conversations and acts.

Steganography differs from cryptography as the former hides the fact that the message exists rather than changing it into an unreadable format. The feature has contributed in making matters regarding the information security in this concept very interesting as well as worrisome. Specifically, the main objective of the study is to expand on the concept of steganography by looking at various methods utilized as well as their capabilities and liabilities.

The study meticulously evaluates the efficacy of seven steganography techniques utilized in GIF images to hide vital data. Such procedures revolve around image alteration and color shifting as well as other means of incorporating patterns which blend naturally with the concealed content. The study employs GIF images as hosts, and it attempts to analyze if such steganography techniques can conceal hidden data without affecting the original images much.

This evaluation process thoroughly scrutinizes every steganographic method and its strengths and limitations. In this context, the objective is mainly to examine the strength of these techniques with respect to privacy and detectability through conventional security systems. Additionally, the research explores possible loopholes and weaknesses that might be present in these methods for steganography and may indicate some ways to detect them and to use them against an attacker.
This gives an extensive study on how these methods perform in reality. The researchers decided the best way to do this was by using animated GIF images as the main stealth media during the investigations process. Therefore,

steganography gets analyzed from the perspective of today's approaches toward information security systems. It outlines the potential patterns and artifacts that may be introduced when hiding within images, which could be used for steganalysis.

Reference paper [9] Steganography is also a very old procedure that can be traced back to ancient civilizations like the older Greek community who used manual copies rather than today's digital techniques. Steganography originated as one of the early simple techniques for hiding messages within texts. These included writing of words onto a slave's bald head, which would subsequently regrow, to an even more grotesque form where a hidden secret alphabet was embedded within literature. Another intriguing method where a message was written in milk and heat could reveal it.

With the advancement of the electronic era, steganography has replaced modern machinery after some time. This progress has greatly been due to the introduction of digital signal processing, the existence of the universal internet and mind-blowing computer revolution. As a result, such developments in technology have brought about new sophisticated and diverse techniques of hiding data within the virtual world.

The conversion of digital signal processing has changed how we process, transmit and transform data, as well how we take and watch pictures. This comes with a number of contributions mainly because of the internet that offered a giant platform for steganography growth into larger numbers. Furthermore, the computing capacity is growing fast and advanced steganographic schemes are already applicable on even complicated secret data.

Brief and weighty overview of the Steganography trend in modernity is this article. It is one that follows up on the history of steganography including ancient manuals and contemporary digital strategies. Thus, this discussion paper aims at pointing out significant technological advancements that have altered steganography since the old school days. Various spatial domain-based techniques with distinct advantages and drawbacks.

2.2 Key Gaps

This research paper [1] lacks LSB algorithm explanation, comparative analysis, detailed security measures, and future work suggestions. Lack of explanation LSB algorithms make it a bit difficult to learn LSB algorithms from the paper. In this research paper we found Inaccurate processing of blurry images & lack of advanced steganography exploration and the blurry image processing was a direct giveaway to predict that the .

This research paper [2] we found potential attacks like cropping and histogram equalization. This research paper lacks depth in the steganography methods, security metrics, and implementation justification. Limited comparative analysis and vulnerability consideration.

This research paper [3] we found Limited file format support, zipped file size constraints, lacks advanced steganalysis testing. This research paper lacks in detailed analysis of steganography's robustness, real-world applicability, and comprehensive security evaluation.

This research paper [4] we found difficulty in classifying techniques, focusing mainly on image steganography. Lacks in-depth analysis of specific image steganography techniques, quantitative evaluation, and exploration of emerging challenges in the field.

This research paper [5] explores crypto-steganography for secure data transfer but lacks details on experimental validation and real-world applications. It's Vulnerable to detect, manipulate & attack, as there were no datasets mentioned.

This research paper [6] has a limited diversity in cover images, unclear steganalysis resistance, scalability unaddressed. This research paper has proposed such methods that lower PSNR and MHC values than the existing ones. The proposed method

cannot hide a larger amount of secret data in the cover images while also not maintaining the image quality.

This research paper [7] mentions potential future work, such as enhancing the LSB steganography algorithm. It lacks in limited evaluation metrics and absence of comparative analysis with existing methods.

This research paper [8] does not offer a detailed analysis of the performance or comparative evaluation of the steganography methods used. It lacks out on limited emphasis on practical applications and real-world effectiveness of discussed techniques.

This research paper [9] lacks comparative analysis, depth on ethical implications, steganalysis advancements, and detailed exploration of limitations. Lack of steganalysis details, limited experimental results, and datasets.

CHAPTER 3: SYSTEM DEVELOPMENT

3.1 Requirements and Analysis

3.1.1 Requirements

Software Requirements

- **Firebase**: The messaging application will use Firebase as a backend. Firebase is among the tools with which we shall create our application. It comes with different vital elements namely, authentication, real time data synchronization and storage among others.
- **Vs-code**: One of the tools we would use in developing a messaging app is Vs-code. Since the Vs-code offers many options like syntax highlighting, code completion or debugging, the development process can be advanced.
- **JavaScript**: The messaging application will employ Java Script as the programming language. JavaScript is quite an expressive language that performs the duties of front end and also back-end development.
- **React JS**: The front-end of the messenger application that will use the JavaScript framework is referred to as React JS. ReactJS is an easy, light-weighted framework suitable for building sophisticated and effective apps.

Hardware Requirements

None: The project does not have any specific hardware requirements other than the required hardware specification to run all the required software's and the project.

Additional Requirements

- **Steganography Library**: For this reason, a steganography library will also be required for the implementation of steganography in the messaging application. Many of those libraries include Steg hide and OpenStego.
- **Image Editing Software**: To embed images in a steganography format, image editing software will be required. There are several image editing software options like Adobe Photoshop and Gimp.
- **Testing Framework**: The security of this messaging facility will need a testing framework.

3.2 Project Design and Architecture

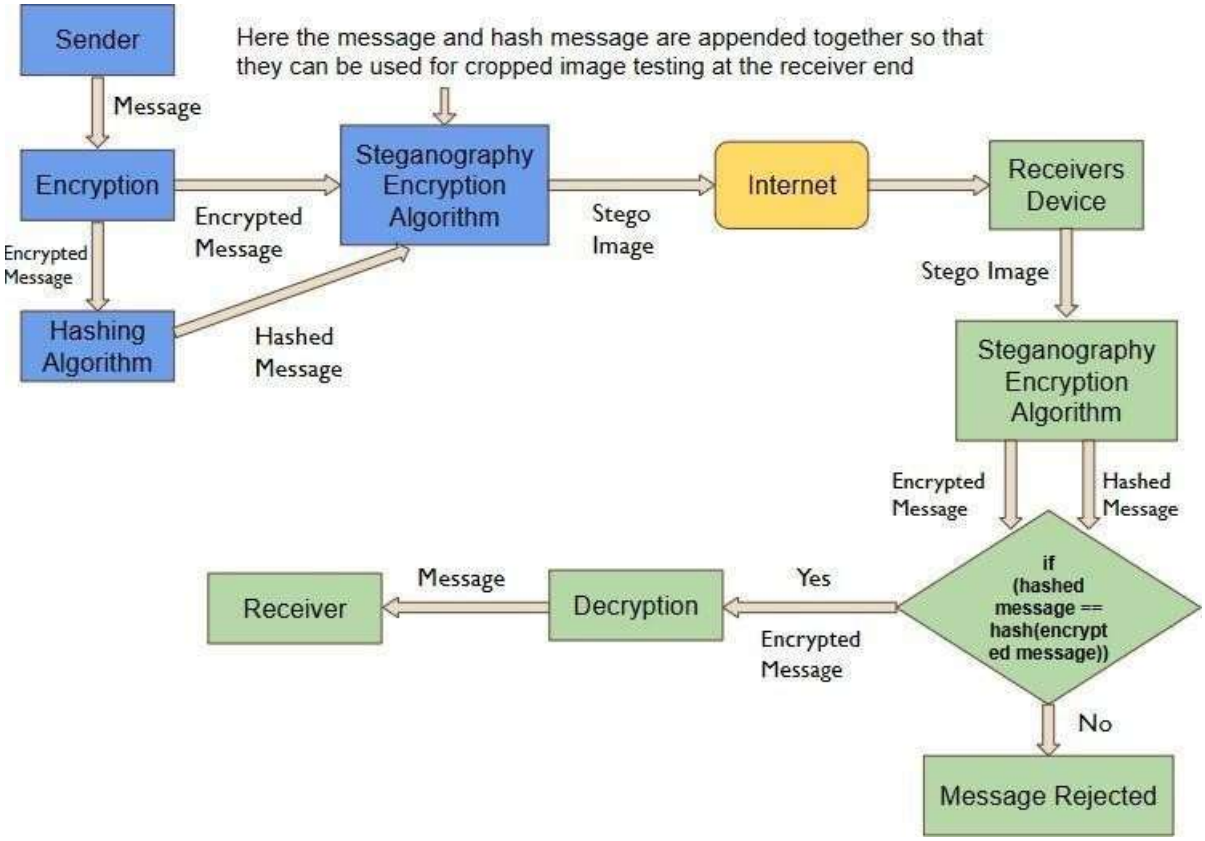


Figure 1 : Project Design

The Figure 1 defines the structure of the program in which the message starts from the sender application and travels to the server where it is encrypted. After the encryption the message is sent to two different functions 1)Hashing Function 2)Steganography Encryption Algorithm. The encrypted message is directly embedded into the stego image and side by side the encrypted message is getting hashed when the encrypted message is embedded a fag is added to the image to differentiated in the hash part and the encrypted message while taking out data from the stego image. After the process of stego image is completed, we end up creating an image encapsulated with the encrypted message, flag and the hashed message. as shown in the figure 2.

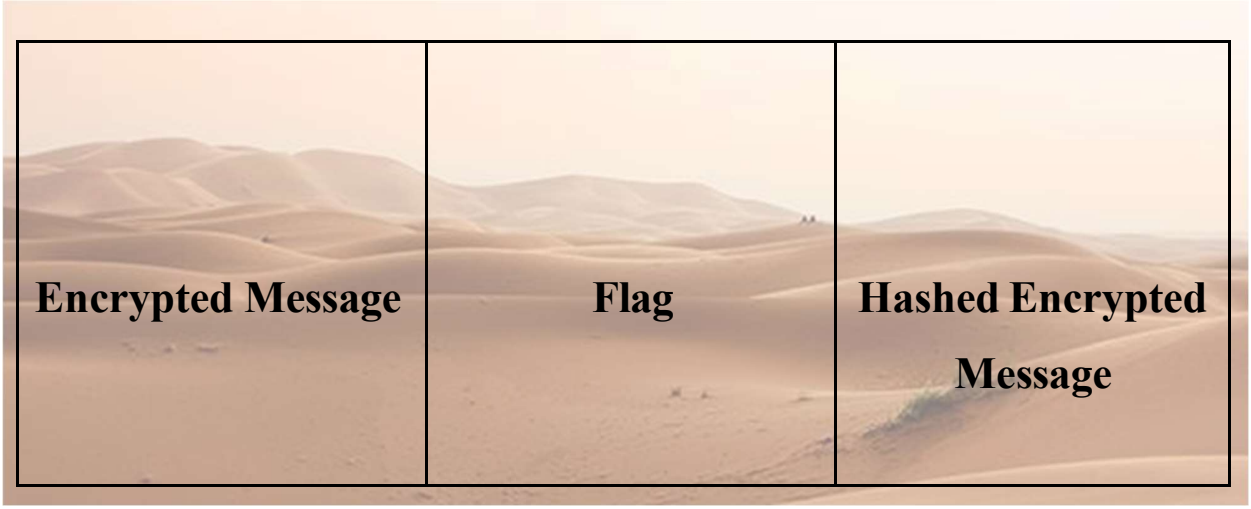


Figure 2 : Image structure after the images are generated the stego image will look like the above figure

After the image is generated, it is transmitted over the internet to the receiver. At the receiver end the stego image is processed through steganalysis where the encapsulated data is extracted from the image with the hashed message, after the message extracted is also hashed and compared to the original hashes message sent by the sender. if the hashed message matches, then the message is accepted and sent to the receiver screen to display, if the message received after hashing does not matches the hashed message received in the stego image then it indicates there is a loss and the message received is tapered cropped or has a packet loss so it is rejected and not displayed to the end user.

The process that an image undergoes can be easily visualized as shown below:

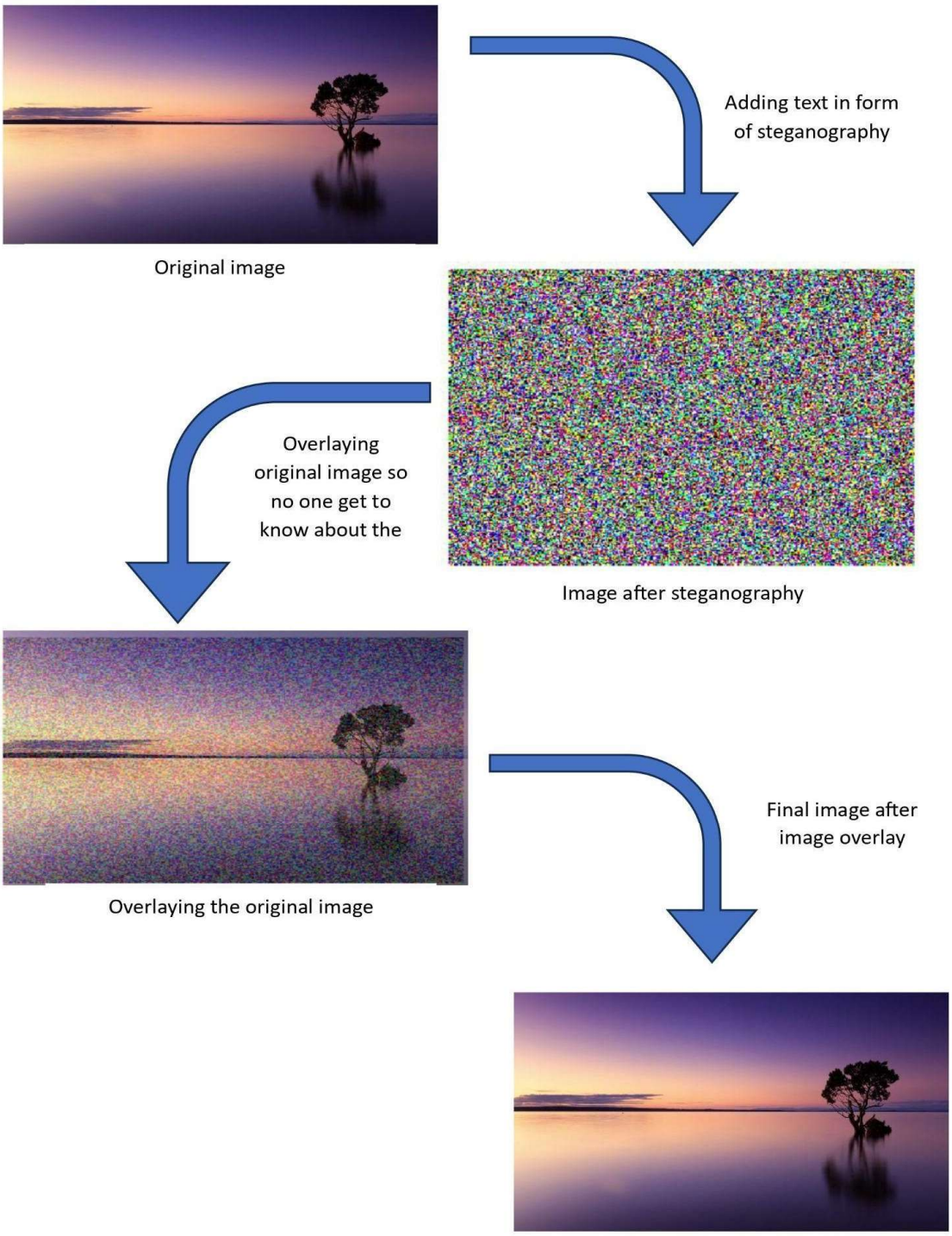


Figure 3 : Steganographic Concealment Process

Steganographic Concealment Process as shown in above figure 3

Step 1: **Steganography**

The original image undergoes steganography, wherein hidden information is embedded within it. This process may involve altering pixel values or image features to encode the desired data.

Step 2: **Overlaying**

The distorted image resulting from steganography is taken, and the original image is overlaid onto it. This overlaying process serves to conceal the steganographic alterations by using the original image as a cover.

Step 3: **Final Image Generation**

The composite image is generated, which includes both the original image and the distorted version with the hidden information. This final image appears visually similar to the original, making it difficult for observers to detect any hidden data.

This technique of overlaying the original image onto a steganographic altered version enhances the concealment of hidden information, ensuring that the presence of steganography is difficult to discern upon visual inspection.

3.3 Data Preparation

Preparation of data is one of the most important stages in creating our steganography-guided message application. This process entails collecting and preparing images that will bear secret codes. Achieving a successful performance, as well as having a strong steganographic algorithm depends on the quality as well as diversity of an image dataset.

We took a multi-pronged strategy involving picture taking in our project. Our imagery database was huge and we were able to include different types of image traits such as resolution, texture, and color depth. Diversity was done with an intention of making the steganographic algorithm capable of working in different image modes and having good quality outputs.

Additionally, we ventured into an organized photo tour across the university grounds so as to make our undertaking more relevant and real. The images ranged across various scenes, objects and textures that contributed more to the image set.\
After acquisition, the pictures were subjected to a thorough pre-processing phase that ensured uniformity in terms of suitability for use with the steganography algorithm. This process involved:

3.3.1 Image Resizing: Each image was carefully resized to a predetermined resolution for the sake of consistency and ease in incorporation of hidden content into the pictures.

3.3.2 Image Format Conversion: The images were carefully converted into a single image format like JPEG or PNG that matches up with the steganographic algorithms.

3.3.3 Image Noise Reduction: An advanced noise reduction technique was employed on images that had very much noise which enabled improvement of image quality as well as eliminating any possible interference to the embedded messages.

The processed images were well arranged in the data set after all that enabled easy referral during the process of steganography. Furthermore, this organization enabled thorough assessment of the steganographic algorithm working for all images and features.

Therefore, by carefully assembling and structuring our collection of pictures, we established firm underpinnings for our stenography-inclined message app to seamlessly hide and reclaim confidential data without disturbing picture quality. The process of preparing this information allowed creating an effective, reliable communication mechanism.

The figure 4 below is the example of the images generated and used in the process of stenography in the chat app: -

Figure 4 : This desert image is used as the bass image in the secure chat application

There are also images that shows great result for avoiding the and can be used to avoid the image distortion due to its deep colored image quality and contrast as shown in figure 5 below:

Figure 5 : Example of another image optimal for steganography

3.4 Implementation

For our current project, we use only one steganographic image for transmitting and receiving data. However, the project can use several random pictures from a directory which will make it secure. The current use of the LSB (least significant bit) algorithm, a common tool for creating a steganographic message, is very popular.

The program currently has multiple components subcomponents and the functions but the important components are : -

- Chat.js
- Decrypt.js
- Encrypt.js
- ChatFeed.jsx
- Loginform.jsx

All the above-mentioned components are explained below with the help of the programs.

Loginform.jsx

Our project starts with a login page which is programmed as an authentication to the chat app so only authorized persons that have their id and passwords saved in chatengine.io can only access the app.

This code below in figure 6 is a simple authentication script running inside of a react modal component. Upon submission of the form, it enables users to enter in their login details (username and password) and then tries to confirm these details against the

Chat Engine API. If the given credentials are valid, then it saves them into the browser's local storage for possible session persistence.

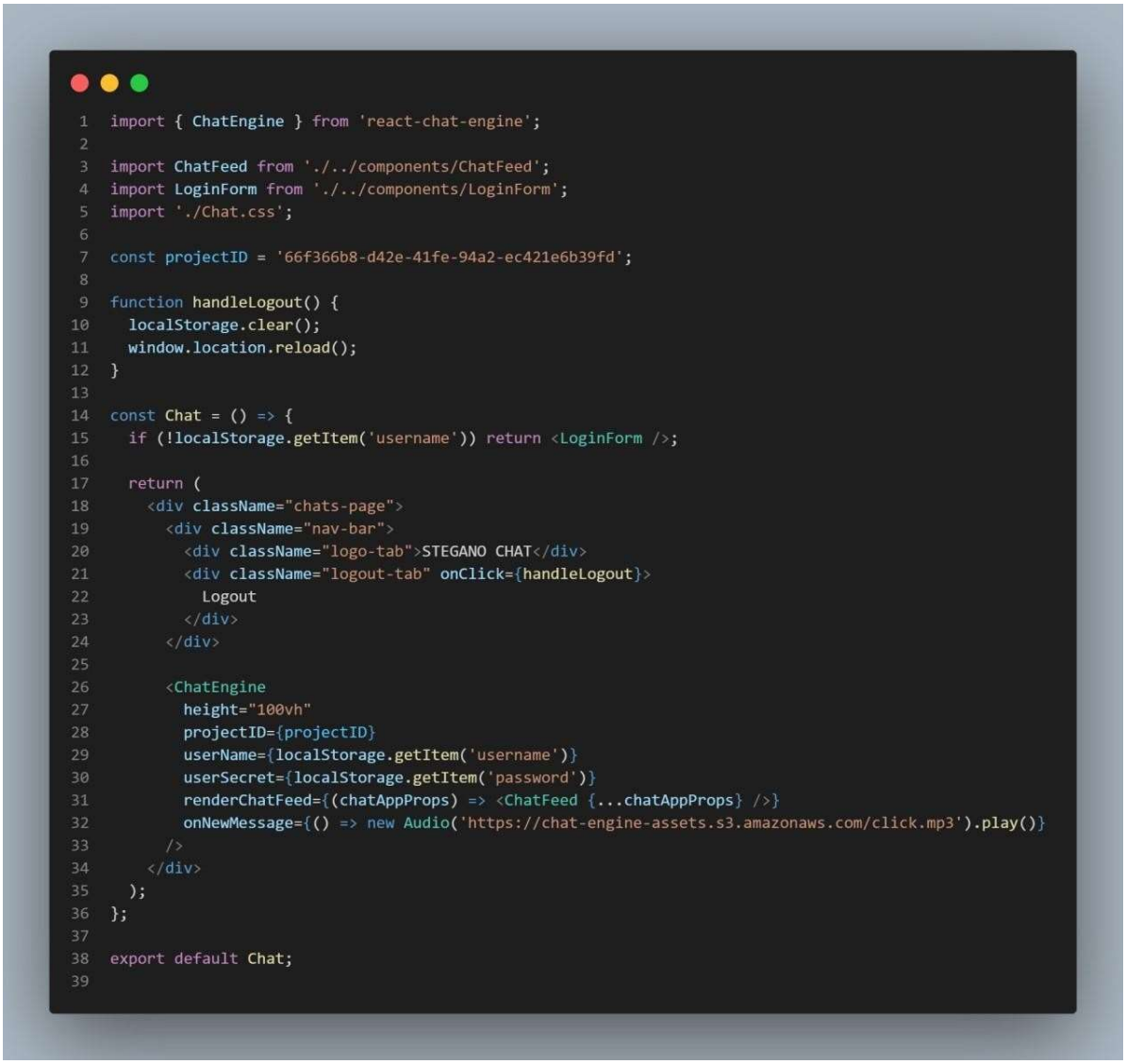
```
const projectID = '66f366b8-d42e-41fe-94a2-ec421e6b39fd';

const Modal = () => {
  const [username, setUsername] = useState('');
  const [password, setPassword] = useState('');
  const [error, setError] = useState('');

  const handleSubmit = async (e) => {
    e.preventDefault();

    const authObject = { 'Project-ID': projectID, 'User-Name': username, 'User-Secret': password };

    try {
      await axios.get('https://api.chatengine.io/chats', { headers: authObject });

      localStorage.setItem('username', username);
      localStorage.setItem('password', password);

      window.location.reload();
      setError('');
    } catch (err) {
      setError('Oops, incorrect credentials.');
    }
  };
```

Figure 6 : authentication program using axios

Chat.js

Then if the authentication is passed successfully and it is verified that the person is authorized to enter the chat, then the program loads the chat component for which the program is given.

The Chat-Engine component that comes with the react-chat-engine library forms part of the main section of the component. The specification defines objects such as the project ID, credentials obtained from the local storage, and a custom function that renders the chat feed called renderChatFeed which uses the object named "ChatFeed". It also has the event handler which initiates a sound alarm when new messages arrive. As shown in the snippet of figure 7.



```
import { ChatEngine } from 'react-chat-engine';

import ChatFeed from './../components/ChatFeed';
import LoginForm from './../components/LoginForm';
import './Chat.css';

const projectID = '66f366b8-d42e-41fe-94a2-ec421e6b39fd';

function handleLogout() {
  localStorage.clear();
  window.location.reload();
}

const Chat = () => {
  if (!localStorage.getItem('username')) return <LoginForm />;

  return (
    <div className="chats-page">
      <div className="nav-bar">
        <div className="logo-tab">STEGANO CHAT</div>
        <div className="logout-tab" onClick={handleLogout}>
          Logout
        </div>
      </div>

      <ChatEngine
        height="100vh"
        projectID={projectID}
        userName={localStorage.getItem('username')}
        userSecret={localStorage.getItem('password')}
        renderChatFeed={(chatAppProps) => <ChatFeed {...chatAppProps} />}
        onNewMessage={() => new Audio('https://chat-engine-assets.s3.amazonaws.com/click.mp3').play()}
      />
    </div>
  );
};

export default Chat;
```

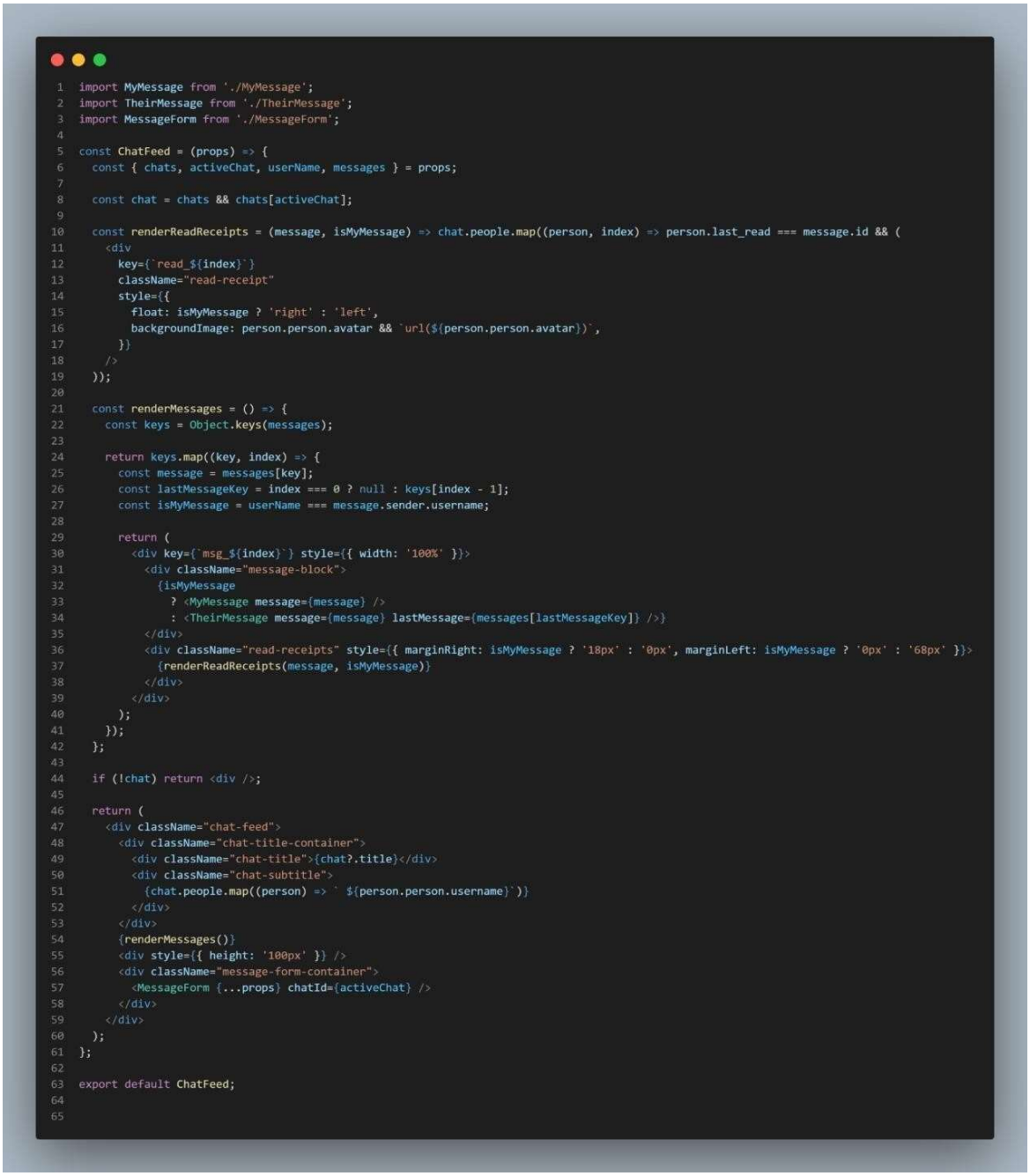
Figure 7: Program defining the chat app where the chat engine is loaded and rest of chat components are initialized.

This figure 6 above is a chat code that utilizes the react-chat-engine library for setting up. The process starts by verifying whether some name already exists in local storage before displaying the sign-in box. The app will then display an interface of a chat and log in successfully.

The Chat component sets up a layout structure with a navigation bar, showing “APP Name” (“stegno chat”) and a logout button that clears local storage and refreshes the page when clicked.

This component not only loads the react-chat-engine but also loads the ChatFeed.jsx component. Which is the actual design structure and the functioning of the application.

ChatFeed.jsx



```jsx
import MyMessage from './MyMessage';
import TheirMessage from './TheirMessage';
import MessageForm from './MessageForm';

const ChatFeed = (props) => {
  const { chats, activeChat, userName, messages } = props;

  const chat = chats && chats[activeChat];

  const renderReadReceipts = (message, isMyMessage) => chat.people.map((person, index) => person.last_read === message.id && (
    <div
      key={`read_${index}`}
      className="read-receipt"
      style={{
        float: isMyMessage ? 'right' : 'left',
        backgroundImage: person.person.avatar && `url(${person.person.avatar})`,
      }}
    />
  ));

  const renderMessages = () => {
    const keys = Object.keys(messages);

    return keys.map((key, index) => {
      const message = messages[key];
      const lastMessageKey = index === 0 ? null : keys[index - 1];
      const isMyMessage = userName === message.sender.username;

      return (
        <div key={`msg_${index}`} style={{ width: '100%' }}>
          <div className="message-block">
            {isMyMessage
              ? <MyMessage message={message} />
              : <TheirMessage message={message} lastMessage={messages[lastMessageKey]} />}
          </div>
          <div className="read-receipts" style={{ marginRight: isMyMessage ? '18px' : '0px', marginLeft: isMyMessage ? '0px' : '68px' }}>
            {renderReadReceipts(message, isMyMessage)}
          </div>
        </div>
      );
    });
  };

  if (!chat) return <div />;

  return (
    <div className="chat-feed">
      <div className="chat-title-container">
        <div className="chat-title">{chat?.title}</div>
        <div className="chat-subtitle">
          {chat.people.map((person) => ` ${person.person.username}`)}
        </div>
      </div>
      {renderMessages()}
      <div style={{ height: '100px' }} />
      <div className="message-form-container">
        <MessageForm {...props} chatId={activeChat} />
      </div>
    </div>
  );
};

export default ChatFeed;
```

figure 8: Program defining the chat layout structure.

Deep in the heart of the program, this portrayal of the code governs the chats that are involved in it. This is an important element that enables one to view the chat, render the messages, and be able to interact with the gadget. Dynamic, since only messages come out of passed props which consist of active chat details, user credential, and message data. In addition, it draws a clear boundary between an owner's messages and those that are not hers. It also has an option called "read receipt," which informs you when another person reads your messages. This interface consists of important chat details like usernames and titles. Furthermore, it contains a users' message input form such that individuals are allowed to join in and add on the discussion being made. This code ensures chat through the conditional checks, and therefore makes chat a useful feature of the application.
After this the program ends up at the situation where the user is trying to implement the function of the project steganography encryption.

Encrypt.js

This is a piece of React code known as Encrypt, which can be used in a web application for conducting steganalysis. It is a crucial element that facilitates image and text manipulation, an operation used to hide data into images via 'steganography' library. This one utilizes functionalities for reading and encoding the file with predominant usage of SMS into pictures. The 'read URL' and 'fileDropEncode' functions, powered by the FileReader API, retrieve the image information which is shown in the interface of this application. Importantly, 'encodeTextIntoimage' and 'encode Dropped Image' functions are vital in encoding text messages into the chosen image. The first set of functions checks whether image data is available as well as verifies that the text message has been entered prior to actual encoding. On successful execution, the encrypted image is shown in the interfaces uncovering implanted information. The 'Encrypt' is one of the most important part of Steganography that allows messages embedding into images and makes secure communication channels through the software.

```
import React from "react";
import steg from "../steganography";

class Encrypt extends React.Component {
  state = {
    dataImageURI: "",
    decodedSecret: " ",
    decodingError: false,
  };

  readURL(input_file) {
    let reader = new FileReader();
    reader.onload = (e) => {
      this.setState({
        dataImageURI: e.target.result,
      });
      document.querySelector("#rawcodeimg").src = e.target.result;
    };
    reader.readAsDataURL(input_file[0]);
  }

  encodeTextIntoImage() {
    if (
      this.state.dataImageURI &&
      document.querySelector("#secret").value.length
    ) {
      document.querySelector("#encodeimg").src = steg.encode(
        document.querySelector("#secret").value,
        this.state.dataImageURI
      );
    }
  }

  fileDropEncode(input_file) {
    let reader = new FileReader();
    reader.onload = (e) => {
      this.setState({
        dataImageURI: e.target.result,
      });
      document.querySelector("#rawcodeimg").src = e.target.result;
    };
    reader.readAsDataURL(input_file[0]);
  }

  encodeDroppedImage() {
    if (
      this.state.dataImageURI &&
      document.querySelector("#secret").value.length
    ) {
      document.querySelector("#encodeimg").src = steg.encode(
        document.querySelector("#secret").value,
        this.state.dataImageURI
      );
    }
  }



  cleanString = (input) => {
    var output = "";
    for (var i = 0; i < input.length; i++) {
      if (input.charCodeAt(i) <= 127) {
        output += input.charAt(i);
      }
    }
    return output;
  };
```

figure 9: Program defining the function encrypting the image with the data.

The react component shown in the figure 9 denoted Encrypt is integrated to provide a web-based steganographic encrypted platform. It allows the masking of information through image processing and uploading capabilities on this user interface. A well-defined layout also presents users with a button dedicated for uploading photo image files. The secret information is entered in a field that is called 'Secret Information.' A 'Encrypt' button initiates this hiding mechanism through scrambling of the typed text within the uploaded picture. The 'original image' and 'hidden info image' show the uploaded image and the resulting encoded image. Users can see how an image has been changed during the encryption process, pictorially speaking. Events such as uploading files, image generation and manipulation are embedded in the code as well. An interactive interphase named 'Encrypt' provides users with convenient opportunities to hide the text inside the pictures without any leaks.

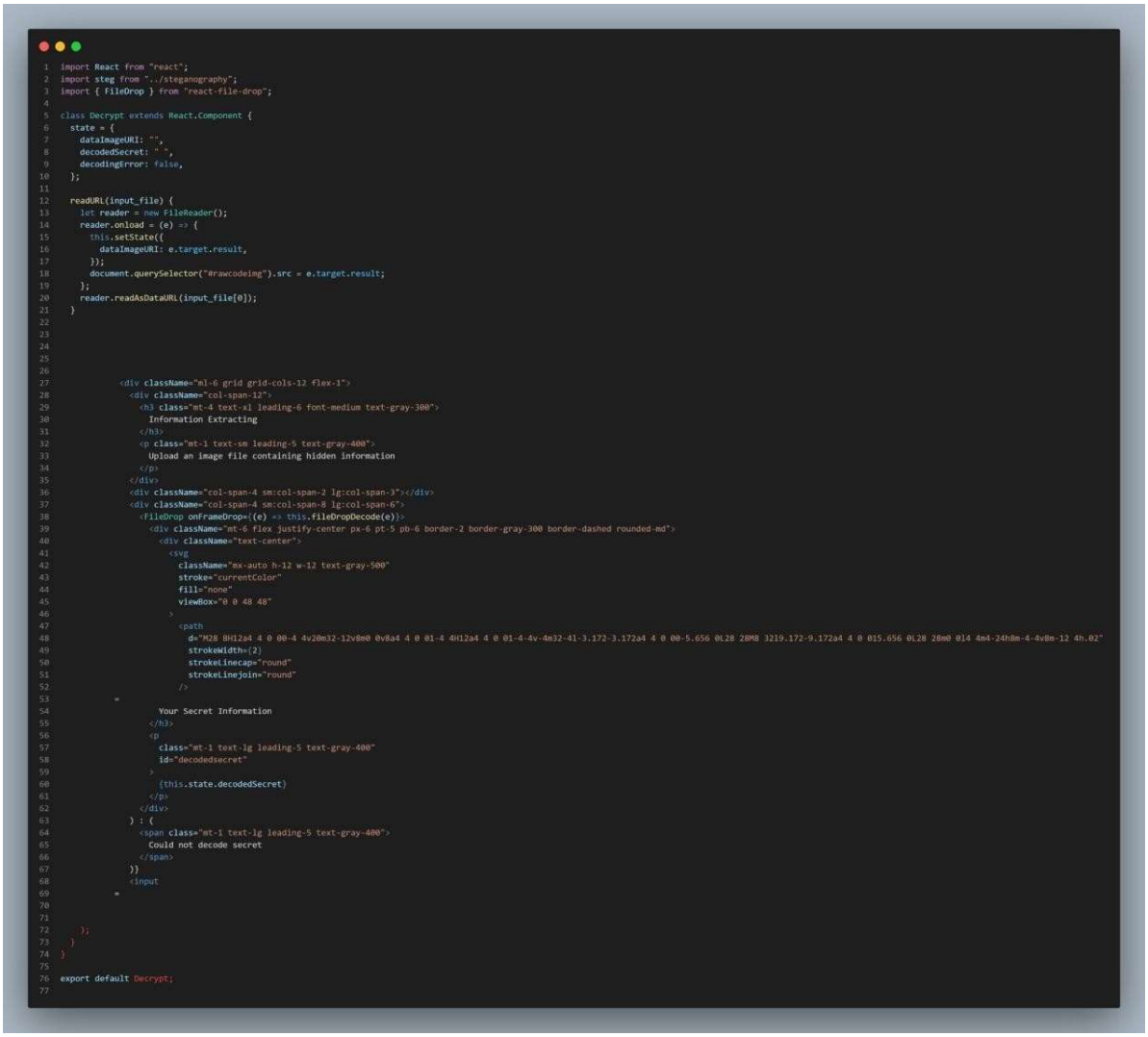
Decrypt.js

A complex 'Decrypt' react component includes means of unveiling an information encoded in pictures with the use of data hiding technique. An intuitive user interface is the last of this component which enables users to discover information that is hidden in images. It operates in state-based mode allowing for automatic transferring both extracted data and displayed errors immediately after getting decoded.

The 'readURL' function utilizes the FileReader API to transform the uploaded picture file into a data URL as part of its implementation process. Visualization of the image happens at almost real-time while 'dataImageURI' triggers decoding processes initially.

On dropping of a file the 'fileDropDecode' method responds by starting the 'decodeDroppedImage' function that decodes the data hidden in the file on the specified area. This makes user experience interactive and enables users to key in photos for decoding purposes through this other more dynamic option and a part of

program is visible below in Figure 10:



```
import React from "react";
import steg from "../steganography";
import { FileDrop } from "react-file-drop";

class Decrypt extends React.Component {
 state = {
   dataImageURI: "",
   decodedSecret: " ",
   decodingError: false,
 };

 readURL(input_file) {
   let reader = new FileReader();
   reader.onload = (e) => {
     this.setState({
       dataImageURI: e.target.result,
     });
     document.querySelector("#rawcodeimg").src = e.target.result;
   };
   reader.readAsDataURL(input_file[0]);
 }




          <div className="ml-6 grid grid-cols-12 flex-1">
            <div className="col-span-12">
              <h3 class="mt-4 text-xl leading-6 font-medium text-gray-300">
                Information Extracting
              </h3>
              <p class="mt-1 text-sm leading-5 text-gray-400">
                Upload an image file containing hidden information
              </p>
            </div>
            <div className="col-span-4 sm:col-span-2 lg:col-span-3"></div>
            <div className="col-span-4 sm:col-span-8 lg:col-span-6">
              <FileDrop onFrameDrop={(e) => this.fileDropDecode(e)}>
                <div className="mt-6 flex justify-center px-6 pt-5 pb-6 border-2 border-gray-300 border-dashed rounded-md">
                  <div className="text-center">
                    <svg
                      className="mx-auto h-12 w-12 text-gray-500"
                      stroke="currentColor"
                      fill="none"
                      viewBox="0 0 48 48"
                    >
                      <path
                        d="M28 8H12a4 4 0 00-4 4v20m32-12v8m0 0v8a4 4 0 01-4 4H12a4 4 0 01-4-4v-4m32-4l-3.172-3.172a4 4 0 00-5.656 0L28 28M8 32l9.172-9.172a4 4 0 015.656 0L28 28m0 0l4 4m4-24h8m-4-4v8m-12 4h.02"
                        strokeWidth={2}
                        strokeLinecap="round"
                        strokeLinejoin="round"
                      />
                    "
                      Your Secret Information
                    </h3>
                    <p
                      class="mt-1 text-lg leading-5 text-gray-400"
                      id="decodedsecret"
                    >
                      {this.state.decodedSecret}
                    </p>
                  </div>
                ) : (
                  <span class="mt-1 text-lg leading-5 text-gray-400">
                    Could not decode secret
                  </span>
                )}
                <input
              "


    );
  }
}

export default Decrypt;
```

figure 10: Program defining the function decrypting the image with the data.

Crucial in unraveling/decoding the information contained in the specified image file is a function christened ‘decodeDroppedImage’ whose matching partner is the ‘decodeImage’ strategy. Using the steganography library, these functions extract the hidden data from the data of an image and store it in the appropriate way to the applications current state. The ‘cleanString’ utility cleanses the extracted string, removing any non-ASCII characters in order to have the end result be comprehensible for the user.

The ‘Decrypt’ element develops a visually attractive and friendly user interface. This gives a friendly area where users can upload images into it or even easily drag and drop of files onto a target area
specified. The intuitive interactive model which encourages simplicity facilitates user-friendliness and accessibility.

On completing the ‘decrypt’ function, the user’s UI will display all the stolen information thus making it transparent for use. It also delicately resolves decoding errors, notifying users on failed efforts but making sure that such experience remains useful and reliable.

The ‘Decrypt’ React component is an advanced yet convenient set of tools helping users unlock hidden information in some images on a straight path with great interfaces.

3.4.2 Algorithm Used for Implementation

LSB algorithm, also known as one of the most popular techniques used in steganography. In this method, one changes the value of the least significant bit of every pixel to represent the binary information which is embedded into the picture. These variations are generally undetectable to the human eye, which has lower sensitivity to changes in the least significant bits of the pixels than any of the digital cameras. Therefore, it becomes possible for the embedded information to be “hidden” in the picture.

Formula

The formula for embedding data using the LSB algorithm is as follows: Data bit + original image pixel value = new image pixel value.
For instance, if the initial pixel value was 1010 in a binary form and the next bit was one, the new pixel value would be 1011.

Steganography

The encrypted data is masked using steganographic algorithms by hiding it in images. The technique conceals the delicate data into something obvious hence hard to detect.

Image Overlay

This project involves image overlay so that the source image with hidden information is superimposed on a bigger picture. This is the second protective barrier that ensures the safety of data during an image crop process.

Double Encryption

With this technique, a double layer of encryption is applied which enhances security as such makes it difficult for intruders to read off the data.

Hashing Algorithms

Data integrity is ensured with hashing algorithms like MD5 and SHA for error detection. The unique fingerprints enable confirmation that the data is indeed unaltered upon reception.

Impact

Hence by careful placement of the images we set a strong foundation of safe retries on the photo messenger which did not affect picture clarity. The development of such information developed a working and trusted message platform. These methods can ensure safety of the transmitted data especially when security of such type of data can never be compromised. Double encryption and steganography provide protection for confidential information whereas integrity checks of data through the use of image overlays and hashing algorithms ensures integrity and prevents tampering with it. These strategies combined result in an all-encompassing security approach for data communication.

3.5 Key Challenges

1. **Balancing Security and Image Integrity:** Steganography hides messages in the image; it may result in minor but clear changes and distortions in the image may be visible on images. Preserving the image quality is also as important as keeping the message secure in the image

2. **Data Embedding Capacity:** Steganography can only hide a limited amount of data in the image so the amount of data stored should be kept in check so only important data is sent and there is no extra or unrequired data is sent.

3. **To Ensure Resistance, Stegana Research:** Steganalysis focuses on finding hidden information in images. Enhancing the steganography algorithm allows us to avoid steganography and maintain data security.

4. **Effective. Several sets of Photographs**: By distributing data in different ways using images, we improve its security significantly.

5. **Managing and Protecting Encryption keys:** Implementation of dual encryption requires robust key management techniques to prevent unauthorized entities from tampering with or compromising encryption keys and secure methods of manufacture, storage on, and distribution play a role in this.

CHAPTER 4: TESTING

4.1 Testing Strategy

The testing scope encompasses all major components of the application, including:

1. **Steganography Algorithm:** Steganography, that is, quality measurement associated with hiding a message unaltered as far as image quality goes.

2. **Encryption Mechanisms:** The ability to avoid brute forcing and reverse engineering while using encryption which is too strong.

3. **Image Selection and Management:** Evaluate how various groups of images can be used as carriers of information, ensure data authenticity, and prevent manipulation.

4. **Key Management:** Secure key life cycle management – authenticated strong key management for generation, storage, and delivery that will guard against unauthorized access and alterations.

5. **Communication Protocol:** With respect to the communication protocol it means securing the information authenticity of the system and making sure that other persons cannot intercept the information they are transmitting to each other.

6. **User Interface:** Usability of the UI, navigation, and interactions with obvious feedback elements, for instance.

4.2 Test Cases and Outcomes

Test Results:

Encryption Performance:

Encrypted messages were seamlessly embedded within images without affecting image integrity. As it is visible in the Figure 11 that the testing message has been embedded with the hidden message and we have received the output image with the hidden message.

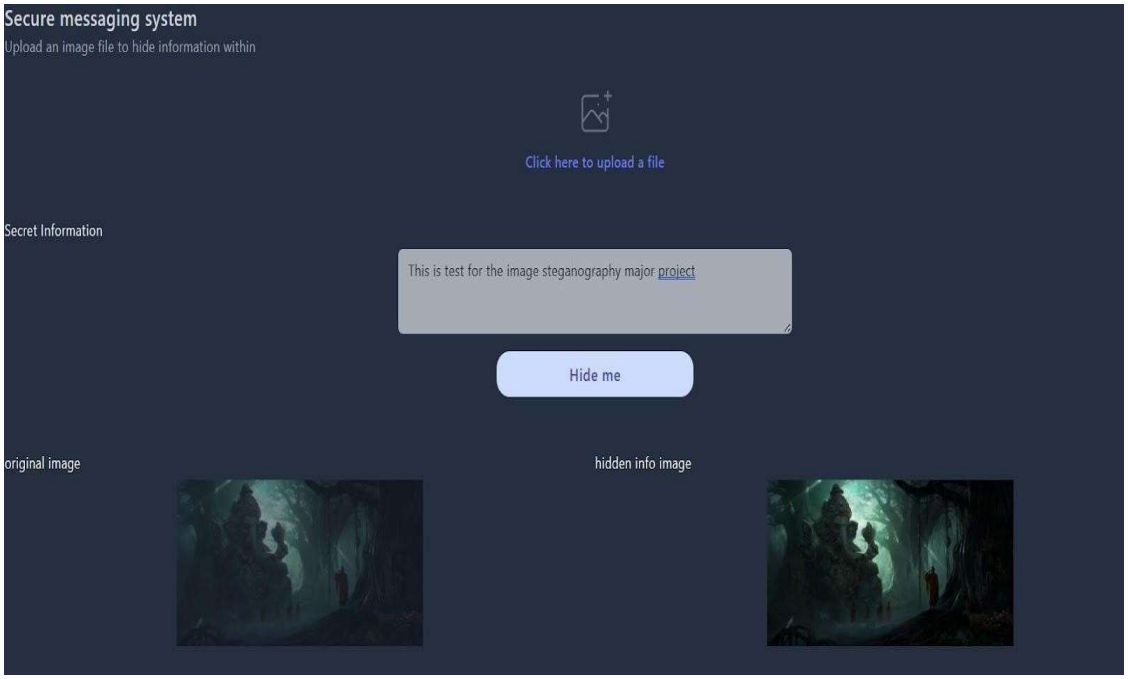


Figure 11: Output of the testing of the stenographic program

Decryption Accuracy:

Extracted hidden messages accurately matched the original input as shown in

the figure 12 and has easily decrypted the message the was hidden while the testing of encryption

Figure 12: Testing of Information Extraction

Security Assessment:

Encryption methods utilized robust algorithms ensuring message confidentiality and No security vulnerabilities or weaknesses detected during testing.

Usability Evaluation:

User interface was straightforward and easy to navigate and we were able to effectively hide and retrieve messages without complications and was not able to directly send steganography images to the person and use a more manual approach which was not a seamless way of performing the action.

The steganography chat app exhibited excellent performance across all testing criteria. It successfully encrypted and decrypted messages while maintaining a high level of security. The user-friendly interface ensures a seamless experience for users without compromising on the app's functionality or security.

CHAPTER 5: RESULTS & EVALUATION

+We were finally able to complete the Chat application based on the Steganography technique which basically means it's a messaging system for secure secret transmission, with privacy protection features. It is powered by Image Steganography.

The project currently uses a user input image for the purpose of sending and receiving data with the help of steganography. The project has scope of using multiple images in a random manner from a database making it more secure and the process of the image working on multiple images which can be given by the user makes it more secure as the images are always random.

The program for the steganography is using the LSB algorithm which is the most used algorithm for most of the steganography applications.

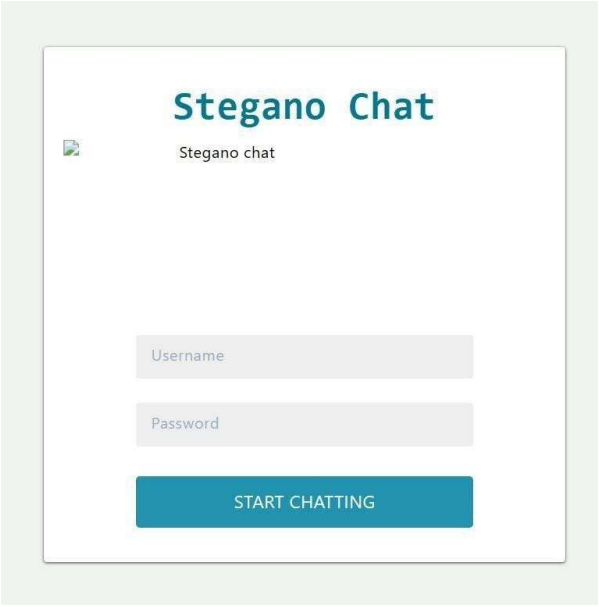


Figure 13 Login UI

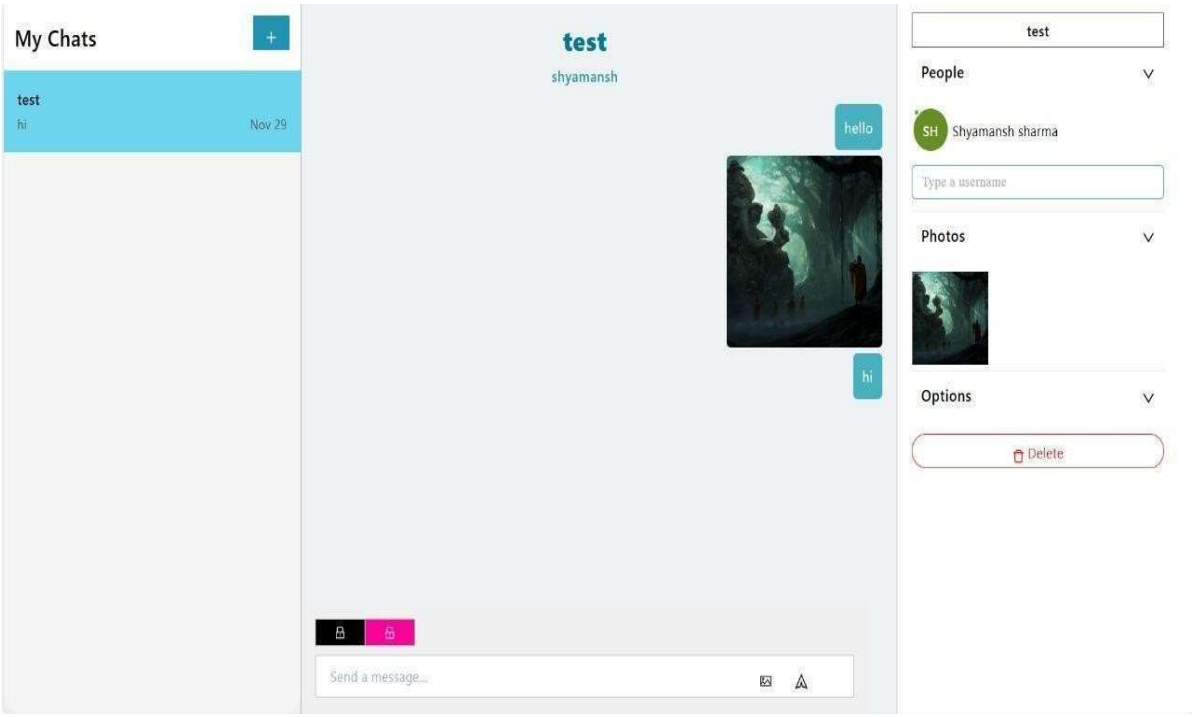


Figure 14:Chat Section

The figure 14 shows the chat section area where both sender and receiver will exchange their thoughts and behind their thoughts whatever images, both sender and receiver want to send to each other will be embedded

This figure 15 UI depicts an area where we will be uploading images you want to hide from attackers.

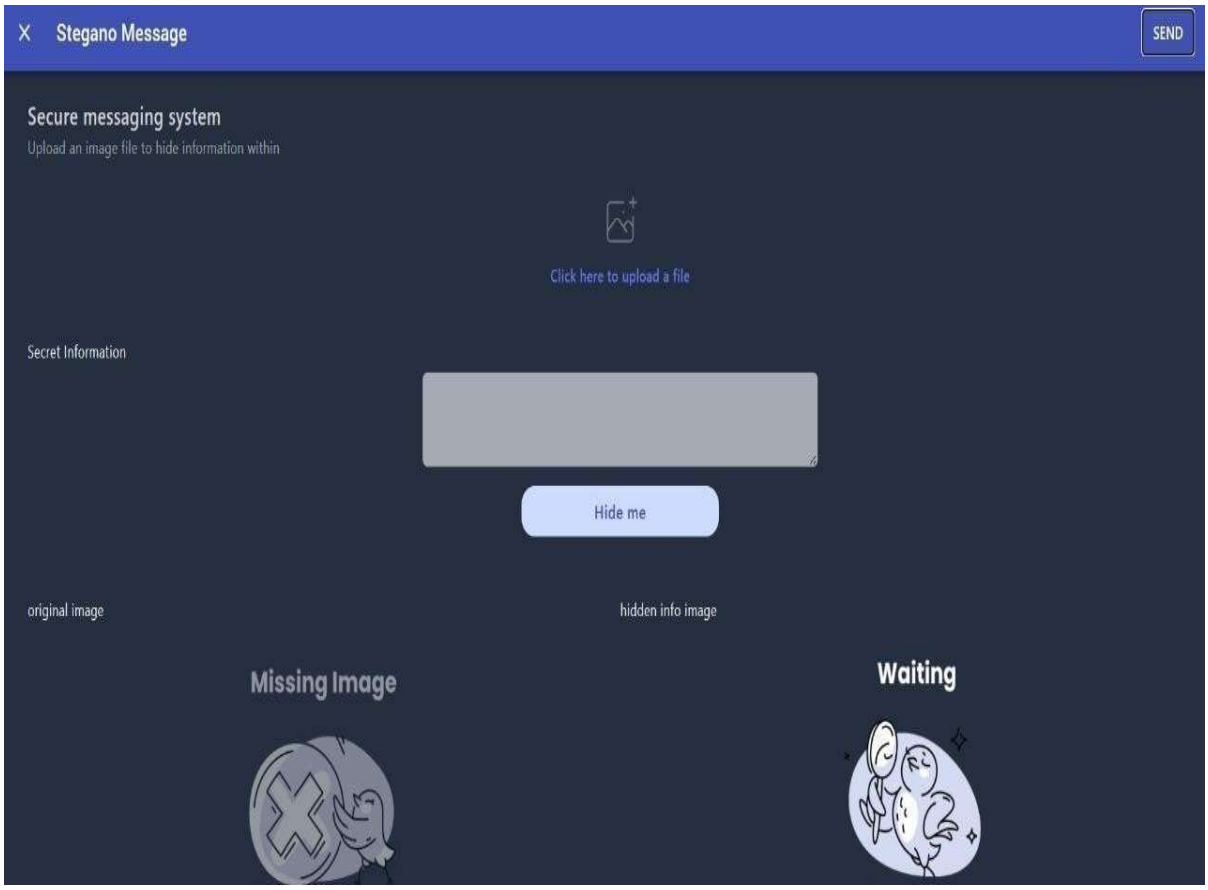


Figure 15 Image Upload section

The figure 16 depicts the decoder section where sender and receiver both can extract each other's information which they receive from the stego images.

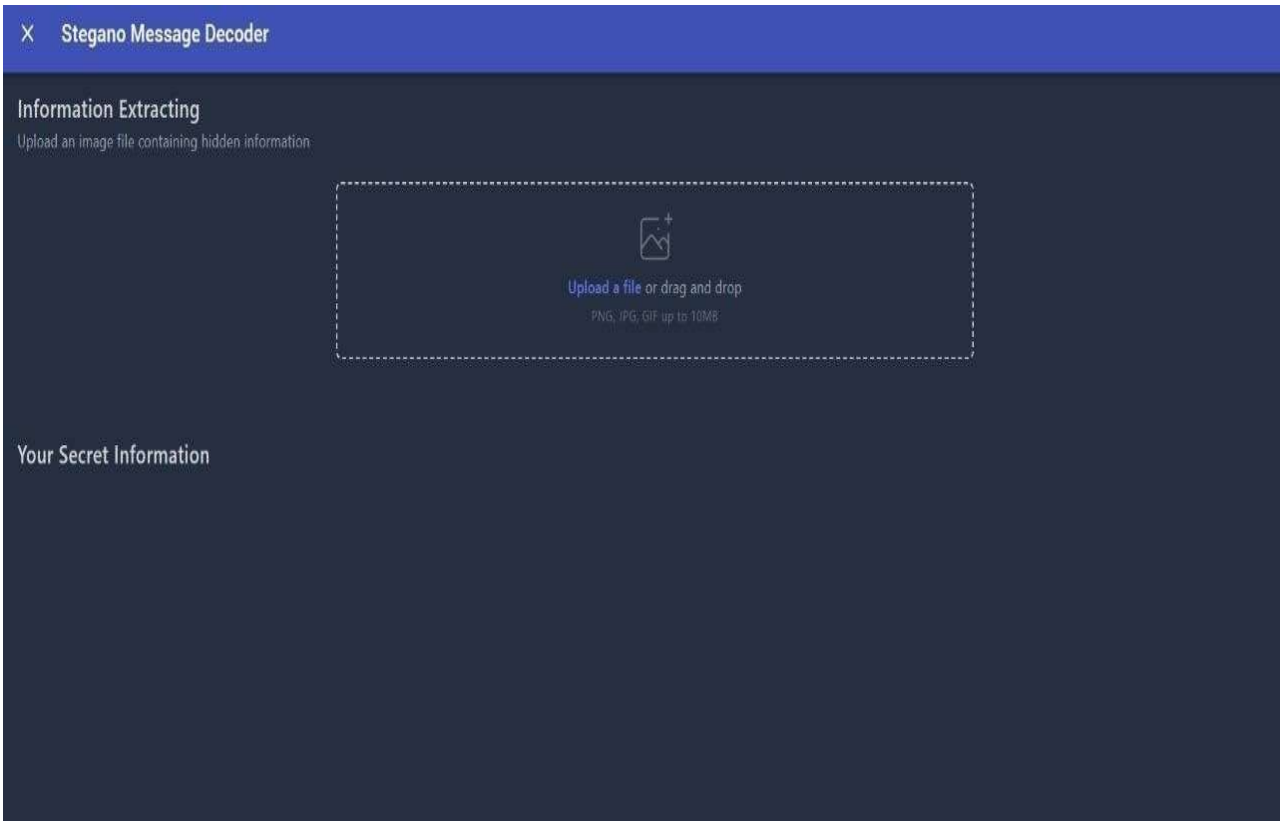


Figure 16 Image Extractor UI

The images generated by the program also went under the process of the Steganographic Concealment meaning the image finally generated will be similar looking to the original images making it almost impossible to figure out that the image went under the steganography process. as shown in image below.

Figure 17 Images before and after the steganography

The image on the right-hand side is the original and the left image is the final image after the process.

Below is the comparison of the given histograms of the two images respectively which are given in order of original image above and the steganographic image as the second histogram below it is for the image after steganography.

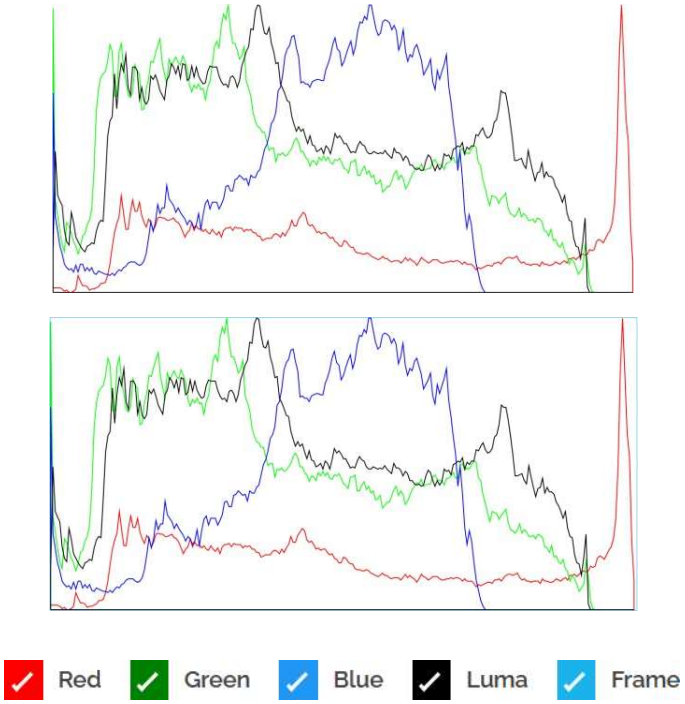


Figure 18 Images histogram comparison

Above histograms prove that the cover image is working as per the expectation and normal steganography testers and human eye would be unable to detect that the images have undergone the process of the steganography.

CHAPTER 6: CONCLUSION & FUTURE SCOPE

6.1 : Conclusion

This project proposes a robust and secure steganography technique. It provides an efficient way of transmitting data in media files without exposing its existence. This project involves low cost and is reliable. This approach needs to be examined against steganography attacks such as cropping and histogram equalization. this steganography technique is reliable and reliable, the best method to ensure confidential data transmission in media files with no loss of speed. With such cost-effectiveness, this project becomes more accessible and usable for many applications. The solution must be tested rigorously with potential attacks such as cropping and histogram equalization.

Continuous R&D is needed to enhance the technique's flexibility as well as resistance to current stenographic threats. As this method grows in maturity, reliability, affordability, and safety highlight why it could be significant for secret communication in various digital contexts.

6.2 : Future Work

The future work lies in Enhancement of Steganographic techniques, improve encryption methods and create an attractive UI design to make it more user friendly and increase the performance optimization. Furthermore, more studies on robustness for emerging detection algorithms should be undertaken. Investigating alternative concealment techniques, including adaptive encapsulation schemes and variable payload alterations, can help increase the robustness of the hidden information. Working closely with cybersecurity experts, including on-going threat tracking will be critical. At the same time, the need for quantum secure refinements on encryption algorithms is crucial in maintaining longevity. Additionally, user-centric design improvement like easy interface and integrations with famous platforms will increase

its adoption by many people. Continuous performance optimization by algorithmic refinement maintains effectiveness of covert communication and encompasses the dynamic nature of modern information security. Also making the cover image technology more effective will be our target so that the stego images may also pass the strict lever checking for the stego images.

REFERENCES

[1.] S. Sravani and R. Ranjith, "Image Steganography for Confidential Data Communication," in 12th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2021.

[2.] Niveditha Shetty. "Steganography for Secure Data Transmission." International Journal of Computational Intelligence Research, vol. 13, no. 10, pp. 2289-2295, 2017.

[3.] R. Ibrahim and T. S. Kuan, "Steganography Algorithm to Hide Secret Message inside an Image," Computer Technology and Application 2 (2021), pp. 102-108, 2011.

[**4.]** S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques," in Proceedings of the IEEE International Conference on Advanced Computer Science and Electronics Information (ICASEI), 2020, pp. 870-875.

[5.] K. C. Nunna and R. Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography, IEEE,2017

[6.] Marwa E Saleh, Abdelmgeid A. Aly and Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques", IJACSA, vol 7, no.6, 2016

[7.] S. Singh and V. K. Attri, "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", *International Journal of Signal Processing Image Processing and Pattern Recognition*, vol. 8, no. 5, 2019.

[8.] K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods", *Multimedia Tools and Applications*, vol. 30, no. 1, pp. 55-88, July 200

[9.] Saha, Babloo, and Shuchi Sharma. "Steganographic techniques of data hiding using digital images." *Defence Science Journal* 62.1 (2012): 11-18.

[10.] R. Shree and D. Swami, "Hybrid Secure Data Transfer Scheme Using Cryptography and Steganography," pp. 166-176,

[11.] M. I. Khalil. Image steganography: Hiding short messages within digital images. JCS&T, Vol.11, No. 2. pp 68-73.

[12.] Billiam A. An Introduction to Steganography and its uses. 2014. Available from: http://null- byte.wonderhowto.com/how-to/introduction-steganography-its-uses-0155310/.

[13.] Vipul Shanna and Madhusudan (2015), "Two New Approaches for Image Steganography Using Cryptography" IEEE Int. Conf. Image Information Processing.

[14.] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[15.] R. Ibrahim and T.S. Kuan, Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings
of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010,
pp. 144-148.

[16.] R. Chandramouli and N. Memon, “Analysis of LSB based Image Steganography Techniques”, Proceeding of IEEE International Conference on Image Processing, (2001) October 7-10, Thessaloniki, Greece.

[17.] N. A. Al-Otaibi and A. A. Gutub, “2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers”, Lecture Notes on Information Theory, vol. 2, no. 2, (2014).

[18.] F. A.P. Petitcolas, R. J. Anderson, and M. G. Kuhn,” Information Hiding – A Survey”, Proceedings of the IEEE, special issue on protection of mutimedia contens, July 1999, pp 1062- 1078.

[19.] T. Morkel, J.H.P. eloff and M.S. Olivier “An overview of image Steganography” information and computer security architecture (icsa) research group.

[20.] N. F. Johnson and Stefan C. Katzen Beisser, “Information hiding techniques for steganography and digital watermarking”, Artech House 2000, ISBN 1-58053-035-4, pp 67-71.

[21.] Zhang, X., & Yan, Z. (2010). Data security and authentication using steganography. International Journal of Computer Science and Information Technologies, 2(3), 153-160.

[22.] Zaidan, A. A., & Al-Jubouri, M. (2015). Secure data transfer over the internet using image crypto-steganography. ResearchGate.

[23.] Verma, A., & Sengar, S. (2016). Secure data transfer over the internet using image steganography. Nevon Projects.

[24.] Ren, Honge; Chang, Chunwu & Zhang, Jian. Reversible image hiding algorithm based on pixels difference, In the IEEE International Conference on Automation & Logistics, ICAL '09, Shenyang, 2009, pp. 847-850.

[25.] Younes, Mohammed Ali Bani & Jantan, A. A new steganography approach for image encryption exchange by using the least significant bit insertion. Inter J Comp Sci Network Security, 2008, 8(6), 247-254.

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: ……

Type of Document (Tick): | **PhD Thesis** | **M.Tech Dissertation/ Report** | **B.Tech Project Report** | **Paper** |

Name:_____ **Department:**_____ **Enrolment No** _____

Contact No._____ **E-mail.**_____

Name of the Supervisor: _____

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): _____

_____

_____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages =
- Total No. of Preliminary pages =
- Total No. of pages accommodate bibliography/references =

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at…… (%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

(Signature of Guide/Supervisor) **Signature of HOD**

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

<table>
<tr><th>Copy Received on</th><th>Excluded</th><th>Similarity Index (%)</th><th colspan="2">Generated Plagiarism Report Details (Title, Abstract & Chapters)</th></tr>
<tr><td rowspan="2"></td><td rowspan="4">• All Preliminary Pages
• Bibliography/Images/Quotes
• 14 Words String</td><td rowspan="2"></td><td>Word Counts</td><td></td></tr>
<tr><td rowspan="2">Report Generated on</td><td>Character Counts</td><td></td></tr>
<tr><td rowspan="2"></td><td>Submission ID</td><td>Total Pages Scanned</td><td></td></tr>
<tr><td></td><td>File Size</td><td></td></tr>
</table>

Checked by
Name & Signature **Librarian**

……

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com