A

PROJECT REPORT ON

**STEGANOGRAPHY OF MESSAGES ENCRYPTED WITH QR CODE**

Submitted in partial fulfilment of the requirement for the

award of the degree of

**BACHELOR OF TECHNOLOGY**

IN

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

BY

**M. SRAVAN KUMAR**

**J. VARUN**

**G. SHRAVAN KUMAR**

**P. NIKHILA**

**22P61A6232**

**22P61A6218**

**22P61A6212**

**22P61A6246**

Under the esteemed guidance of

Mrs. V. Rajyalakshmi

**Asst Professor, Dept. of CSE(CS)**



**Department of Computer Science and Engineering**

**(Cyber Security)**

**VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY**

(Approved by AICTE, Accredited by NBA, NAAC, Permanently Affiliated to JNTUH)

Aushapur (v), Ghatkesar (m), Medchal.dist, TELANGANA-501301

Academic Year 2023-2024



AUSHAPUR (V), GHATKESAR (M), MEDCHAL, DIST-501 301

**Department of Computer Science and Engineering**

**(Cyber Security)**

**CERTIFICATE**

This is to certify that the project entitled **“STEGANOGRAPHY OF MESSAGES ENCRYPTED WITH QR CODE**” is being submitted by M. SRAVAN KUMAR (22P16A6232), J. VARUN (22P16A6218), G.SHRAVAN KUMAR (22P61A6212), P. NIKHILA (22P61A6246), in partial fulfilment of the requirement for the award of the degree of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide work carried out by them under my guidance and supervision during the academic year 2023-2024. The results embodied in this project report have not been submitted to any other University for the award of any degree or diploma.

Internal Guide Head of Department

Mrs. V. Rajyalakshmi Dr. P. Sushma

Asst Professor Department of CSE (CS)

Department of CSE(CS)



**AUSHAPUR (V), GHATKESAR (M), MEDCHAL.DIST-501 301**

**Department of Computer Science and Engineering (Cyber Security)**

**DECLARATION**

We, **M. SRAVAN KUMAR** bearing hall ticket number **22P61A6232, J.VARUN** bearing hall ticket number **22P61A6218, G.SHRAVAN KUMAR** bearing hall ticket number **22P61A6212**, **P.NIKHILA** bearing hall ticket number **22P61A6246** hereby declare that the project report entitled **“STEGANOGRAPHY OF MESSAGES ENCRYPTED WITH QR CODE**” under the guidance of Mrs.V. Rajyalakshmi, Asst Professor, Department of Computer Science and Engineering(Cyber Security), **VBIT**, Hyderabad, is submitted in partial fulfilment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Cyber Security).

This is a record of Bonafide work carried out by us and the results embodied in this project have not been reproduced or copied from any source. The results embodied in this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

**M. SRAVAN KUMAR (22P61A6232)**

**J. VARUN (22P61A6218)**

**G. SHRAVAN KUMAR (22P61A6212)**

**P. NIKHIA (22P61A6246)**

**ACKNOWLEDGEMENT**

First and foremost, we wish to express our gratitude towards the institution **“Vignana Bharathi Institute of Technology”** for fulfilling the most cherished goal of our life to do Bachelor of Technology.

It is great pleasure in expressing deep sense of gratitude to our **Internal guide, Mrs. V. Rajyalakshmi**, Asst Professor, Department of Computer Science and Engineering (Cyber Security) for her valuable guidance and freedom she gave to us.

We also express our sincere thanks to Mrs. V. Rajyalakshmi, Associate Professor, Project Coordinator for his encouragement and support throughout the project.

We are deeply grateful to **Dr. P. Sushma**, **Head of Department, Department of Computer Science and Engineering (Cyber Security)** for granting me the opportunity to conduct this project.

We take immense pleasure in thanking **Dr. P.V.S. Srinivas Principal, Vignana Bharathi Institute of Technology, Ghatkesar** for having permitted us to carry out this project work.

Our utmost thanks also go to all the **FACULTY MEMBERS** and **NON - TEACHING STAFF** of the Department of Computer Science and Engineering (Cyber Security) for their support throughout our project work.

**M. SRAVAN KUMAR (22P61A6232)**

**J. VARUN (22P61A6218)**

**G. SHRAVAN KUMAR (22P61A6212)**

**P. NIKHILA (22P61A6246)**

**ABSTRACT**

This project presents a secure and efficient data-hiding technique by integrating **Elliptic Curve Cryptography (ECC)**, **QR code encoding**, and **Least Significant Bit (LSB) steganography**. The method is designed to enhance secure communication by ensuring both encryption and concealment of messages within digital media, making it suitable for applications such as confidential messaging, watermarking, and digital forensics.

The process begins with the generation of an ECC key pair, leveraging the SECP256R1 curve for strong cryptographic protection. The sender encrypts the message using the ECC public key. ECC is chosen due to its ability to provide high levels of security with relatively small key sizes, making it lightweight and suitable for modern computing environments.

Once encrypted, the ciphertext is **Base64 encoded** to convert it into a textual format, which is then embedded into a **QR code**. QR codes provide a structured and scannable visual format that allows the encrypted message to be efficiently represented as an image.

The generated QR code is then hidden inside a cover image using **LSB steganography**, a technique that embeds data into the least significant bits of an image’s pixel values. This alteration is imperceptible to the human eye, thereby effectively concealing the presence of the message while preserving the visual integrity of the image. The final stego-image is saved and can be transmitted over any communication channel without raising suspicion.

At the receiver’s end, the hidden QR code is extracted from the stego-image using LSB decoding. The extracted QR code is then decoded to retrieve the Base64-encoded encrypted message. Finally, the encrypted data is decrypted using the ECC private key, and the original plaintext message is revealed.

This layered approach combines the strengths of cryptography, encoding, and steganography to provide a secure and covert means of communication. By embedding encrypted QR codes within images, this system ensures not only message confidentiality and integrity but also adds a layer of stealth, making it highly resistant to unauthorized access and visual detection

**VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY**

**Department Computer Science and Engineering**

**(Cyber Security)** **COURSE OUTCOMES**

Course: Real Time Project Class: III B. Tech & II Semester

AY: 2024-2025

**Course Outcomes**

After completing the Projects, the student will be able to:

|  |  |  |
| --- | --- | --- |
| **Code** | **Course Outcomes** | **Taxonomy** |
| **C1** | Identify and state the problem precisely to prepare the abstract | Remember |
| **C2** | Analyze the existing system, and outlining the proposed methodology for effective solution | Analyze |
| **C3** | Use various modern tools for designing applications based on specified requirements | Apply |
| **C4** | Prepare the document of the project as per the guidelines | Create |

**PROGRAM OUTCOMES**

**PO 1: Engineering knowledge:**

Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization for the solution of complex engineering problems.

**PO 2: Problem analysis:**

Identify, formulate, research literature, and analyse complex engineering substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences problems reaching.

**PO 3: Design/Development of Solutions:**

Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and cultural, societal, and environmental considerations.

**PO 4: Conduct investigations of complex problems:**

Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

**PO 5: Modern tool usage:**

Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

**PO 6: The engineer and society:**

Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

**PO 7: Environment and sustainability:**

Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and the need for sustainable development.

**PO 8: Ethics:**

Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

**PO 9: Individual and team work:**

Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

**PO 10: Communication:**

Communicate effectively on complex engineering activities with the engineering community and with the society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

**PO 11: Project management and finance**:

Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

**PO 12: Life-long learning:**

Recognise the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

**PROGRAM SPECIFIC OUTCOMES**

**PSO 1**

Demonstrate expertise in ethical hacking techniques, proficiency in identifying vulnerabilities and potential threats in systems and networks.

**PSO 2**

Showcase mastery in collecting, preserving, and analyzing digital evidence to support legal investigations and cybercrime cases.

**PSO 3**

Exhibit managerial skills and knowledge along with certification in ethical hacking

which is globally recognized to predict future challenges in protecting digital assets of individuals, organizations and society.

**VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY**

**Department Computer Science and Engineering**

**(Cyber Security)** **COs Mapping with PO/PSO**

Project Title: Revealing Cybersecurity Threats: Insights into Internal and External Risks. Name of the Supervisor: Dr. P. Sushma

Batch Details:

|  |  |  |  |
| --- | --- | --- | --- |
| S.NO | Regd.no | Student name | Web Based |
| 1 | 22P61A6232 | M. SRAVAN KUMAR | CYBER SECURITY |
| 2 | 22P61A6218 | J. VARUN | CYBER SECURITY |
| 3 | 22P61A6212 | G. SHRAVAN KUMAR | CYBER SECURITY |
| 4 | 22P61A6246 | P. NIKHILA | CYBER SECURITY |

## Note: Write your domain name in technology field (ex. ML, IOT, BC, Security, Cloud etc)

CO-PO Mapping for Major Project: High-3 Medium -2 Low-1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Program Outcomes** | | | |  |  |  |  |  |  |  |  | **Program Specific Outcomes** | | |
| **Cos-**  **POs** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **1** | **2** | **3** |
| **CO1** | 3 | 3 | 3 | 3 | 3 | 3 |  | 3 | 3 | 3 |  | 3 | 3 |  |  |
| **CO2** | 3 | 3 | 2 | 2 | 3 |  | 3 | 3 | 3 |  |  | 3 | 3 |  |  |
| **CO3** | 3 | 3 | 3 | 3 |  | 3 | 3 | 3 |  | 3 |  | 3 | 3 |  |  |
| **CO4** | 3 | 3 |  |  | 3 | 3 | 3 |  | 3 | 3 |  | 3 | 3 |  |  |
| **CO5** | 3 | 3 | 3 | 3 |  | 3 | 3 | 3 | 3 |  |  | 3 | 3 |  |  |
| **Avg** | **3** | **3** | **2.8** | **2.8** | **3** | **3** | **3** | **3** | **3** | **3** |  | **3** | **3** |  |  |

SUPERVISOR SIGNATURE

**INDEX**

**CONTENT PAGE NUMBER**

**CERTIFICATION**

**ACKNOWLEDGEMENT**

**ABSTRACT**

**CO-OP MAPPING**

**1.INTRODUCTION 01**

MOTIVATION  **02**

OVERVIEW OF EXISTING SYSTEM  **02**

OVERVIEW OF PROPOSED SYSTEM  **04**

PROBLEM DEFINITION  **05**

OBJECTIVE OF PROJECT  **05**

SCOPE OF PROJECT  **06**

**2.LITERATURE SURVEY 07**

**3.SYSTEM ANALYSIS 12**

HARDWARE REQUIREMENTS  **13**

SOFTWARE REQUIREMENTS  **13**

**4.SYSTEM DESIGN 14**

UML DIAGRAMS  **15**

GOALS  **15**

TYPES OF UML DIAGRAMS  **16**

**5.IMPLEMENTATION 20**

SAMPLE CODE

**6.OUTPUT SCREENS 23**

**7.TESTING AND DEBUGGING 28**

**8.CONCLUSION 31**

**9.FUTURE ENHANCEMENTS 33**

**10.REFERENCE 35**

**CHAPTER -01**

**INTRODUCTION**

**1. INTRODUCTION**

In today’s digital era, where vast amounts of sensitive data are exchanged over networks, ensuring secure and covert communication has become more crucial than ever. Traditional encryption methods provide confidentiality, but they may still be susceptible to detection and interception during transmission. To address this challenge, this project proposes a multi-layered security mechanism that combines Elliptic Curve Cryptography (ECC), QR code encoding, and Least Significant Bit (LSB) steganography.

The core idea of the project is to not only encrypt the message but also hide its existence from potential attackers. The use of ECC ensures strong encryption with smaller key sizes compared to traditional algorithms like RSA, providing an efficient and secure cryptographic layer. Once the message is encrypted using ECC, it is converted into a QR code, which helps in structuring and visualizing the data in a compact image format that is easy to embed and retrieve.

To further enhance the confidentiality and stealth of the communication, the QR code is embedded into a cover image using LSB steganography. This technique alters the least significant bits of image pixels to encode the QR code without noticeably changing the appearance of the image. As a result, the encrypted data remains hidden in plain sight, making it less likely to be detected or tampered with during transmission.

The proposed system offers a comprehensive security solution by combining encryption, encoding, and steganography. It ensures the confidentiality, integrity, and concealment of the message, making it suitable for applications such as secure messaging, watermarking, digital forensics, and secure data storage.

This documentation outlines the design, implementation, and working of the system, starting with message encryption and ending with message decryption at the receiver’s end. By leveraging well-established cryptographic and steganographic techniques, this project aims to demonstrate a practical and reliable approach for secure data hiding and transmission in the modern digital landscape.

**1.1 MOTIVATION**

In today's digital world, securing sensitive information is more crucial than ever. Traditional encryption methods protect data but often expose its presence, attracting unwanted attention. To overcome this, our project combines encryption with data hiding. We use **Elliptic Curve Cryptography (ECC)** for strong, efficient encryption. To conceal the encrypted data, we embed it in an image using **Least Significant Bit (LSB) steganography**. A **QR code** acts as an intermediate format for reliable encoding and decoding. This layered technique ensures that both the content and its presence remain protected. Our solution aims to provide secure, discreet communication. It is ideal for applications in cybersecurity, digital forensics, and personal privacy

* + 1. **OVERVIEW OF EXISTING SYSTEM**

This project combines Elliptic Curve Cryptography (ECC), QR code generation, and Least Significant Bit (LSB) steganography to create a secure communication system. The goal is to ensure the confidentiality, integrity, and stealth of messages during transmission, making it ideal for applications such as secure messaging, digital watermarking, and forensics. The system begins with the generation of an ECC public-private key pair. The sender uses the public key to encrypt a plaintext message, ensuring that only the intended recipient, who holds the private key, can decrypt it. The encrypted message is then Base64 encoded, converting it into a text format suitable for encoding into a QR codeA QR code is created from the Base64-encoded message, serving as a compact, scannable representation of the encrypted data. To further secure the message, LSB steganography is applied, embedding the QR code into a cover image, such as a standard JPEG or PNG. This process modifies the image’s least significant bits, which is imperceptible to the human eye, thereby concealing the presence of the QR code and, by extension, the encrypted message. The recipient extracts the hidden QR code from the cover image using LSB decoding. Once the QR code is retrieved, it is decoded to reveal the Base64-encoded encrypted message. The recipient then decrypts the message using their private ECC key, recovering the original plaintext. This multi-layered security approach ensures that the message remains confidential, tamper-proof, and hidden from unauthorized viewers. By combining ECC encryption, QR code encoding, and LSB steganography, the system offers a highly secure and covert method for communicating sensitive information.

**Drawbacks of existing system**

1. Security Issues

* Data Breaches: E-commerce platforms are a popular target for cyberattacks. Without strong encryption and secure protocols, user data (like payment details and personal information) could be vulnerable.
* Weak Authentication: If the authentication mechanisms are weak (e.g., simple passwords or lack of two-factor authentication), unauthorized access to user accounts and the admin panel can occur.
* Payment Gateway Risks: If the payment system is not integrated securely, users' financial information could be exposed to hackers.

2. Performance and Scalability

* Slow Loading Times: With high traffic or large product catalogs, the site can become slow, leading to poor user experience and a potential loss in sales.
* Scalability: As the platform grows (more users, products, and transactions), the system might struggle to handle the increased load unless properly optimized, leading to downtime or performance issues.

3. User Experience (UX) Problems

* Complex Navigation: If the user interface (UI) is cluttered or hard to navigate, it can frustrate users and lead to higher bounce rates.
* Poor Mobile Experience: E-commerce sites that aren’t optimized for mobile can result in a loss of potential customers since a significant amount of traffic comes from mobile devices.
* Inconsistent Checkout Process: A complicated or lengthy checkout process can cause cart abandonment, leading to lost sales.

4. Lack of Personalization

* Generic User Experience: If the platform doesn't offer personalized recommendations or tailored experiences, users might feel disconnected, reducing engagement and sales.
* No Dynamic Content: Offering static content rather than dynamic recommendations based on user behaviour (e.g., recently viewed products, personalized deals) can make the shopping experience less engaging.

5. Maintenance and Updates

* Technical Debt: If the codebase isn’t well-structured or documented, making changes or adding new features can become difficult and time-consuming.
* Infrequent Updates: If the platform isn’t regularly updated, it may become outdated in terms of design, features, and security patches.
* Manual Processes: Admins might rely on manual processes for product management, order fulfilment, or inventory management, which can lead to inefficiencies or errors.

6. Payment and Inventory Management

* Payment Failures: Integration issues with payment gateways can lead to payment failures or delays, frustrating customers and potentially costing sales.
* Inventory Inaccuracy: If the system doesn’t update product availability in real-time or has flaws in inventory tracking, it could lead to overselling or stockouts, damaging customer trust.

7. Customer Support

* Lack of Efficient Support Channels: Without an integrated customer service solution (live chat, support tickets, etc.), it can be difficult to resolve customer issues in a timely manner.
* Return and Refund Handling: If the platform doesn’t have a clear and smooth process for returns and refunds, it can cause frustration and negatively affect customer satisfaction.

8. Integration Limitations

* Third-Party Integration: The platform may struggle to integrate with third-party services such as shipping providers, analytics tools, and marketing platforms, limiting the scalability of the business.
* Payment Gateway Incompatibility: If the payment gateways are not flexible or compatible with certain currencies or countries, it can limit the platform's global reach.

9. SEO and Marketing Challenges

* Poor Search Engine Optimization (SEO): If the website is not properly optimized for search engines, it will be harder for potential customers to find the site, limiting traffic.
* Ineffective Marketing Integration: If the platform doesn’t allow easy integration with marketing tools or social media, it may be harder to effectively reach and convert new customers.

10. Legal and Regulatory Compliance

* Privacy Concerns: Platforms that don’t comply with data protection regulations like GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act) could face penalties.
* Tax Compliance: Ensuring that taxes are calculated and applied correctly across different regions can be complex and might lead to issues if not properly handled.

**1.1.2 OVERVIEW OF PROPOSED SYSTEM**

The proposed system integrates Elliptic Curve Cryptography (ECC), QR Codes, and Steganography to create a highly secure and efficient data protection solution. ECC is used for strong encryption with smaller key sizes, providing secure data transmission with reduced computational overhead. The encrypted data is then encoded into a QR code, facilitating portable and convenient storage and transfer. QR codes also ensure data integrity by embedding cryptographic hashes or digital signatures for verification.

Steganography adds a layer of concealment by embedding the QR code (containing the encrypted message) within an innocuous medium, such as an image, ensuring that the data remains hidden from unauthorized users. This multi-layered approach increases security by making the encrypted data difficult to detect and intercept.

The system's workflow includes encrypting data with ECC, generating a QR code for the encrypted data, embedding it within a digital medium via steganography, and then transmitting or storing the image. Upon reception, the QR code is extracted, and the encrypted message is decrypted using the ECC key.

The integration of these techniques offers a robust security framework, combining encryption, data integrity checks, and covert data transfer. This system is ideal for scenarios requiring high confidentiality, such as secure document sharing or private communication. It ensures that data remains protected from unauthorized access while maintaining efficiency and ease of use.

**Advantages of proposed system**

* **Strong Security**: Using Elliptic Curve Cryptography (ECC), the system provides robust encryption with smaller key sizes, ensuring high security without excessive computational cost. ECC is highly resistant to attacks, making it ideal for secure communication.
* **Low Computational Overhead**: ECC's efficiency means it can be deployed in resource-constrained environments (like mobile devices or IoT systems) without significantly impacting performance, unlike traditional encryption methods like RSA.
* **Data Integrity**: QR codes can store cryptographic hashes or digital signatures, allowing for easy verification of the integrity of the encrypted data. This ensures the data has not been tampered with during transmission.
* **Covert Data Transmission**: Steganography hides the encrypted message within an image or other medium, making it harder for unauthorized parties to detect the presence of sensitive information, thus providing a covert channel for secure communication.
* **Portability**: QR codes provide a convenient and portable way to store and share encrypted data, which can easily be scanned by mobile devices or QR code readers. This makes the system user-friendly and accessible for various scenarios.
* **Multi-Layered Security**: Combining ECC, QR codes, and steganography creates a multi-layered security approach. Even if one layer is compromised, the others provide additional protection, significantly reducing the risk of data breaches.
* **Ease of Use**: The integration of QR codes makes data transfer simple and intuitive. Users can scan the code to quickly access the encrypted data without needing specialized software or technical expertise.
* **Resistance to Interception**: The use of steganography ensures that even if the transmission is intercepted, the encrypted message remains concealed within an innocuous-looking medium, reducing the likelihood of detection by malicious actors.
* **Scalability**: The system is adaptable to a wide range of applications, from secure personal communication to enterprise-level data protection, making it suitable for various industries and use cases.
* **Privacy Protection**: The combined approach protects not just the content of the data but also its existence, ensuring that sensitive information remains confidential throughout the transfer process.
* **Efficient Resource Usage**: ECC's efficiency, paired with the compactness of QR codes, ensures minimal storage and transmission costs, making it ideal for applications where bandwidth and storage are limited.
* **Flexibility**: The system can be customized to fit different types of data, including text, images, and other file formats, expanding its applicability in diverse contexts.

* 1. **PROBLEM DEFINITION**

The project aims to solve the problem of securely transmitting sensitive data in a resource-efficient and covert manner. Using **Elliptic Curve Cryptography (ECC)**, it ensures strong encryption with minimal computational overhead. **Steganography** is employed to conceal the encrypted data within innocuous files, such as images, preventing detection by unauthorized parties. **QR Codes** are used to store and transfer the encrypted data, enabling easy access and portability. The system also incorporates data integrity verification through cryptographic hashes or digital signatures. This multi-layered approach enhances data security, prevents unauthorized access, and ensures confidentiality and authenticity. The solution is designed to be efficient, user-friendly, and resilient against cyber threats.

* 1. **OBJECTIVE OF PROJECT**

The objective of this project is to create a secure, efficient, and covert system for transmitting sensitive data. By integrating Elliptic Curve Cryptography (ECC), the project aims to provide strong encryption with minimal computational overhead, ensuring the security of sensitive information in resource-constrained environments. The system will employ steganography to conceal the encrypted data within innocuous files, such as images or audio, preventing detection by unauthorized users or attackers. This additional layer of security will make it difficult for attackers to identify or access the encrypted data, even if the transmission is intercepted.

The project also incorporates QR Codes to store and transfer the encrypted data, offering a portable and easily scannable method for secure data exchange. This approach simplifies the process for end users while maintaining high levels of security. To further enhance the system, cryptographic hashes or digital signatures will be embedded within the QR codes to ensure data integrity, allowing recipients to verify that the data has not been tampered with during transmission.

In essence, the project aims to combine ECC, steganography, and QR codes to create a multi-layered security system that protects both the content and the existence of sensitive data. The objective is to provide a comprehensive solution that enables secure communication, protects privacy, and ensures data integrity in diverse environments, from personal to enterprise-level use cases. This system is designed to be user-friendly and effective in combating modern security threats, such as unauthorized access and interception.

* 1. **SCOPE OF PROJECT**

The scope of this project is to develop a secure communication system by integrating Elliptic Curve Cryptography (ECC), QR code encoding, and Least Significant Bit (LSB) steganography. The main goal is to hide encrypted messages within digital images, ensuring both confidentiality and stealth. The project begins by using ECC for encrypting the message. ECC is chosen because it provides strong encryption with smaller key sizes, making it efficient and suitable for modern systems. Once the message is encrypted, it is converted into Base64 and then embedded into a QR code. This QR code serves as a compact, portable way to store the encrypted data.

Next, the QR code is concealed within an image using the LSB steganography technique. This method involves altering the least significant bits of the image’s pixel values, making the hidden data invisible to the naked eye. The final stego-image can be transmitted securely over any communication channel, with no visual indication of the hidden message. On the receiver’s side, the QR code is extracted from the stego-image using LSB decoding. After extracting the QR code, it is scanned and decoded to retrieve the Base64-encoded encrypted message. This message is then decrypted using the ECC private key to reveal the original plaintext message.

The system can be used for various applications such as confidential messaging, digital watermarking, and digital forensics. The secure transmission and hiding of sensitive data in this way ensures the message is both private and imperceptible to unauthorized parties. The design focuses on creating a user-friendly interface for encryption and decryption processes, making the system lightweight, covert, and efficient, even for low-resource environments. This integrated approach combining ECC, QR codes, and LSB steganography offers a reliable and secure way to communicate, hiding encrypted data within images in a manner that ensures both security and privacy.

**CHAPTER 02**

**LITERATURE SURVEY**

**2. LITERATURE SURVEY**

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. In this paper, we present a QR code as a secret message to increase the embedding capacity and information security of the image steganography. we use quick response (QR)code. QR codes generated by our proposed system can carry its ordinary message in addition to the payload and with the use of LSB(Least significant Bit) method .If anyone can read the message, but the payload can only be obtained using a secret key. The message and the payload are unrelated; i.e. any message can be generated regardless of the payload and vice versa. We can take advantage of that by generating HMAC-XTEA algorithm, Hash based Message Authentication code (MAC) which involves a cryptographic hash functions and a secret key. So, if message that gives misleading information to the adversary. we test the proposed system and show that the generated QR code is (valid) i.e. indistinguishable from an ordinary QR code which makes it look innocent and less susceptible.

Data is very much insecure in this internet dominating world now these days. Steganography is technique to hide data in given medium without suspicious of it. So, in this paper one method of data has been discussed in digital images. One image format in which each pixel is represented using 8-bit binary number whose range come from zero to 255. So gray scale image maximum having 256 colors in each pixel. LSB hiding technique uses LSB of 8-bit number representing a pixel. This LSB change due to data hiding causes less change in pixel value which is not detectable through human visual system. For measuring the effectiveness of LSB technique many mathematical parameters can be used like peak signal to noise ratio, mean square error and many others.

Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. In this paper we propose an advanced system of encrypted data embedded into an image file using random LSB insertion method in which the secret data are spread out among the image data in a seemingly random manner. This is achieved using a secret key. It combined both feature of steganography and cryptography. To enhance security level that. It also provides integrity and message authentication using MAC algorithm.

Steganography is considered the first line of defense in information security as it hides a secret message (payload) inside an innocent looking file (container) to transfer the payload under the adversary’s nose without noticing it. Steganographic systems only use the container to hide the payload. In this paper, we present a steganographic system that uses the container not only to hide the payload, but also to give misleading information to the adversary. To achieve this goal, we use quick response (QR) code as a container. QR codes generated by our proposed system can carry its ordinary message in addition to the payload. Anyone can read the message, but the payload can only be obtained using a secret key. The message and the payload are unrelated; i.e. any message can be generated regardless of the payload and vise versa. We can take advantage of that by generating a message that gives misleading information to the adversary. We test the proposed system and show that the generated QR code is (valid) i.e indistinguishable from an ordinary QR code which makes it look innocent and less susceptible to an adversary’s attack. Moreover, it is space-efficient, has an acceptable level of noise immunity and is prone to steganalysis attacks.

In the public communication channels, security is broadly increased because of the exchange of sensitive information. For each transmission of data security is highly demanded. The Major goal of this paper is to provide secure communication between authorized people. In the audio steganography technique, data is hidden within the audio signal, the audio signal can be modified in imperceptible manner. Secret text or audio information can be hidden in host message. The host message should contain the same characteristics before the steganography and after the steganography. In existing method, each audio sample converted into bits and then the textual information is embedded in it. In embedding process, the data is inserted sequence. In proposing system each audio sample is converted into its ASCII values and selected data also converted into ASCII values, then it is converted into the binary values. According to the random number generation position of the audio file and data is selected. Data can be inserted in randomly. This paper secret data is concealed with the audio file. The limitation of this method is an audio file must be in WAV type only.

**CHAPTER 03**

**SYSTEM ANALYSIS**

**OPERATING REQUIREMENTS**

**Software Requirements**

* **Operating System:** Windows, Linux, or macOS
* **Python Version:** Python 3.7+

**Hardware Requirements**

* **Processor:** Intel i3 or equivalent (minimum)
* **RAM:** 4GB (minimum), 8GB+ recommended
* **Storage:** At least 100MB for image and QR code storage
* **Camera/Scanner (Optional):** For scanning QR codes from printed images

**CHAPTER 04**

**SYSTEM DESIGN**

**SYSTEM DESIGN**

**4.1 UML DIAGRAMS**

UML stands for Unified Modelling Language. UML is a standardized general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta- model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modelling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems. The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

**GOALS**

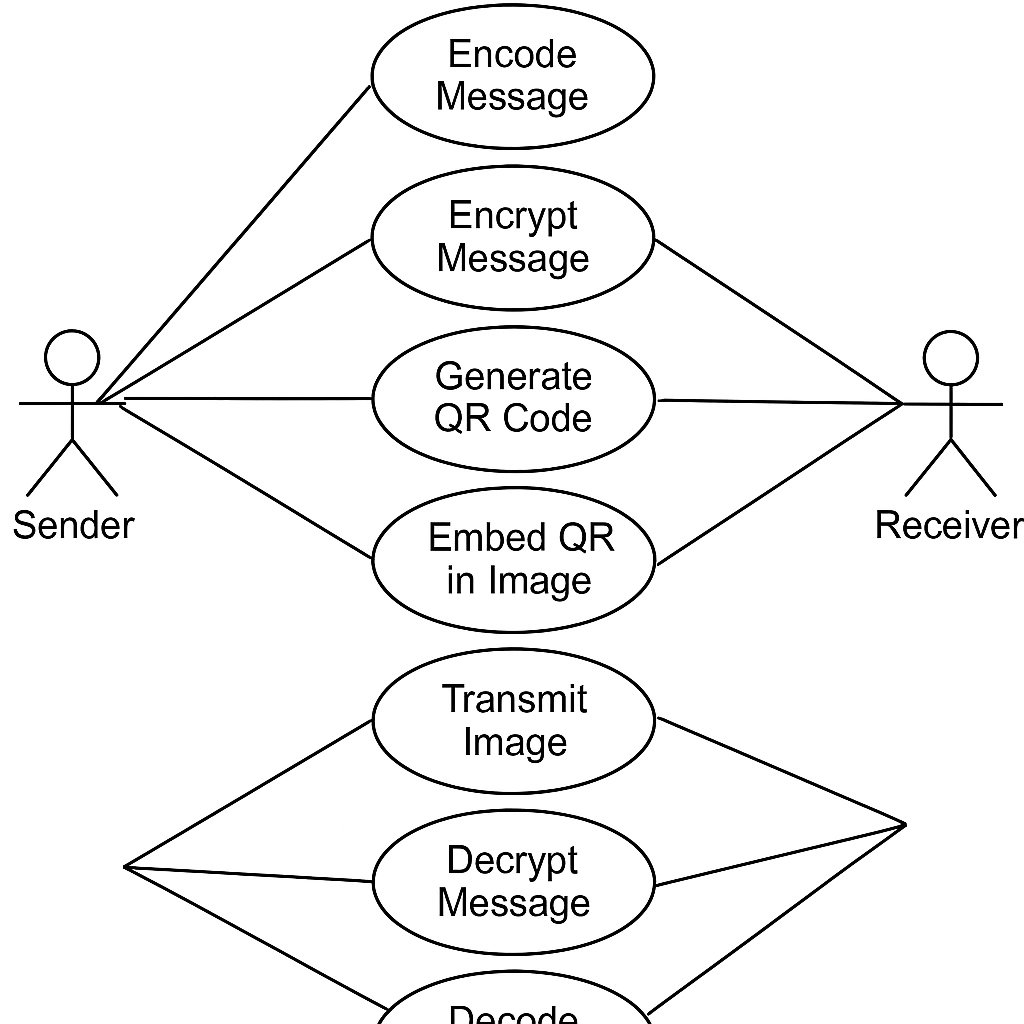
The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

## **TYPES OF UML DIAGRAM**

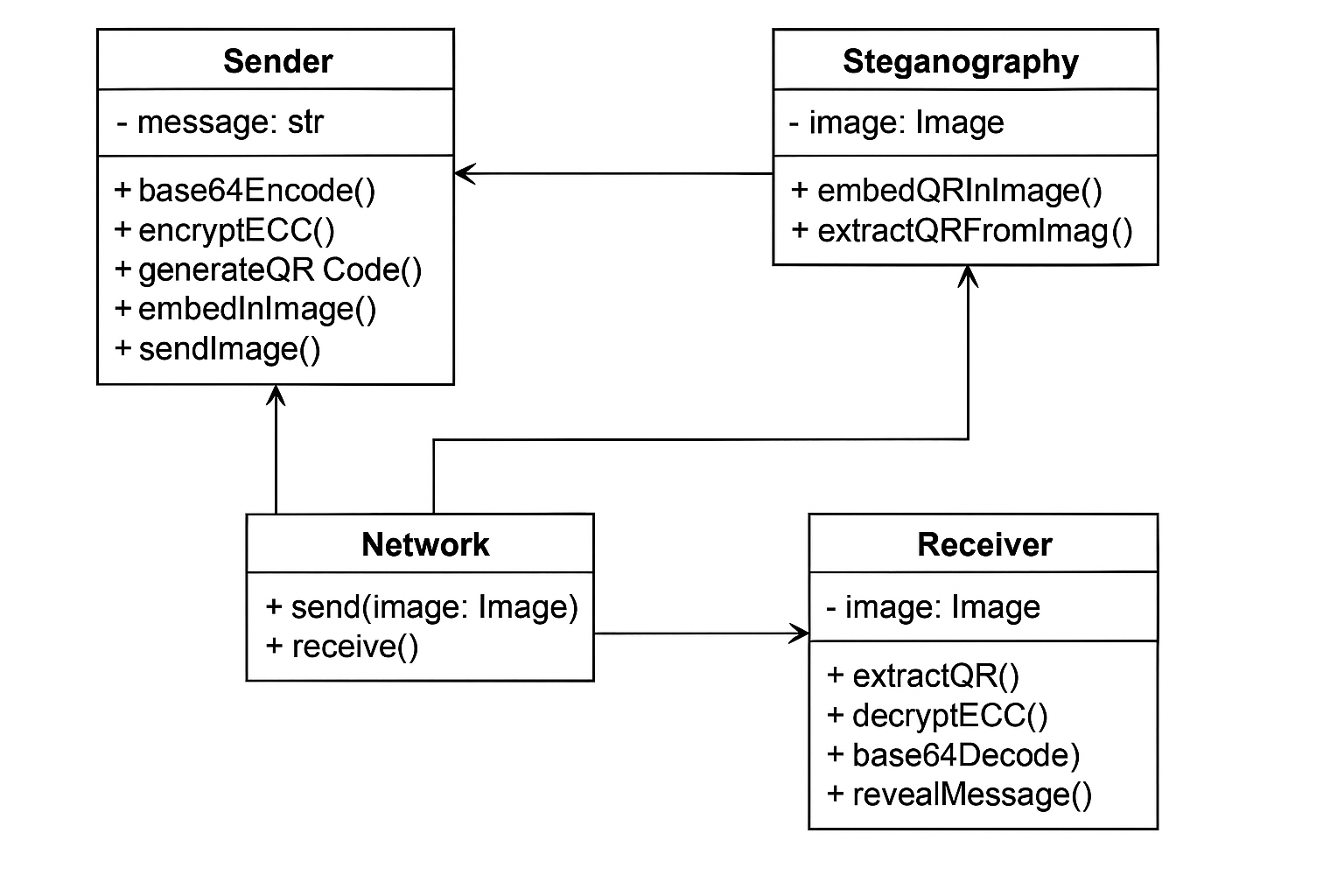
Each UML diagram is designed to let developers and customers view a software system from a different perspective and in varying degrees of abstraction. UML diagrams commonly created in visual modelling tools include:

**A. USE CASE DIAGRAM**

Display the relationship among actors and Use Cases. A use case is a set of scenarios that describing an interaction between a user and a system. A use case diagram displays the relationship among actors and use cases. The two main components of a use case diagram are use cases and actors.

**Fig 1 Use case diagram:steganography of encrypted messages with qr code**

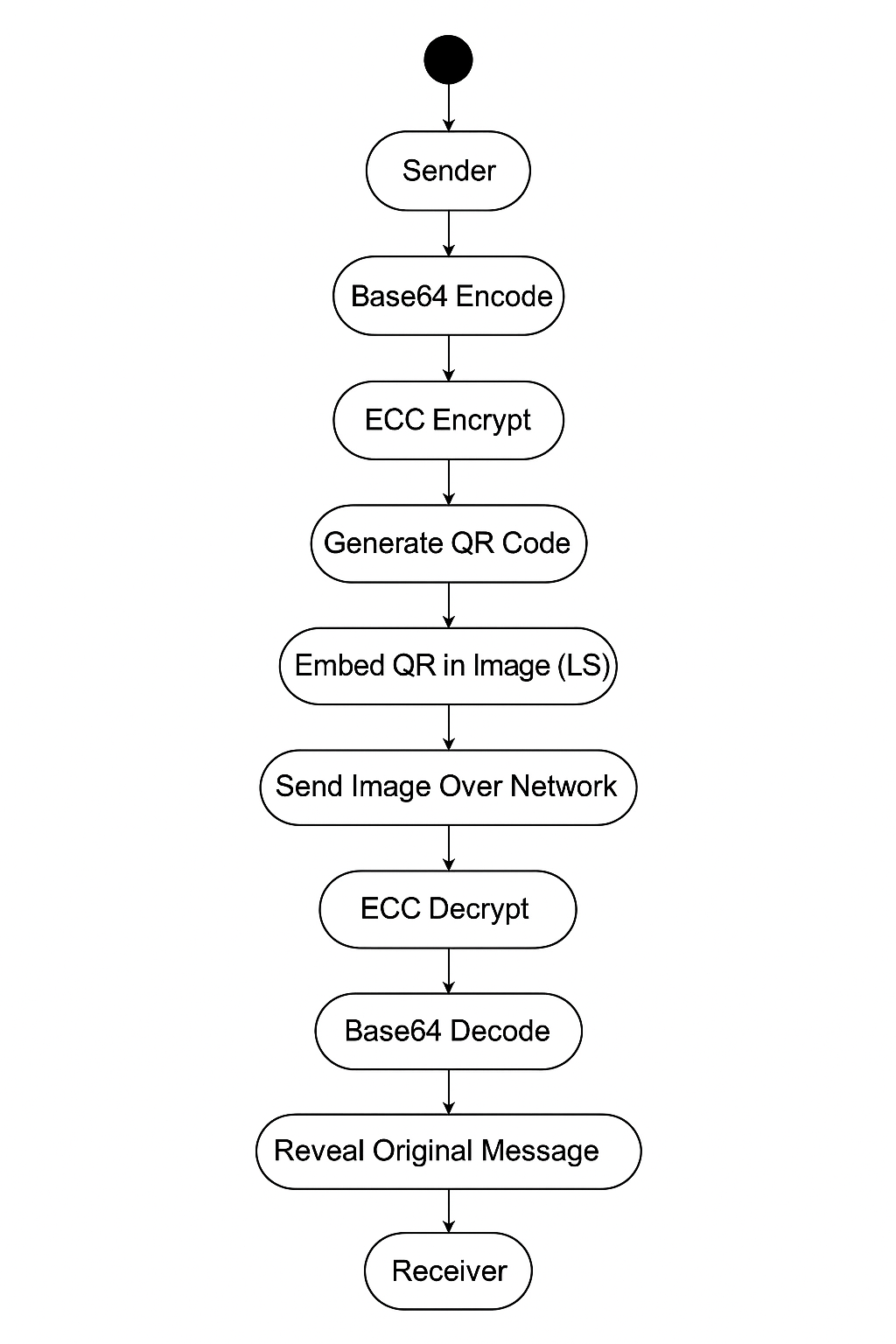
**B.CLASS DIAGRAM**

 Class diagrams are widely used to describe the types of objects in a system and their relationships. Class diagrams model class structure and contents using design elements such as classes, packages and objects. Class diagrams describe three different perspectives when designing a system, conceptual, specification, and implementation. These perspectives become evident as the diagram is created and help solidify the design. One of the core purposes of class diagrams is to help conceptualize, specify, and implement the design of a system. They serve as a bridge between abstract, high-level design concepts and the tangible implementation details. Class diagrams are instrumental in conveying the system's blueprint and ensuring that all parties involved have a shared understanding of its architecture. The essential components of a class within a class diagram consist of its "name," "attributes," and "operations." The "name" serves as a unique identifier for the class and often reflects the real-world entity it models. "Attributes" define the properties or characteristics of objects belonging to the class, encapsulating their state. "Operations" specify the methods or functions that can be invoked on objects of the class, effectively defining their behaviours and functionality.

# fig 2 class diagram: steganography of encrypted messages with qr code

**C.ACTIVITY DIAGRAM**

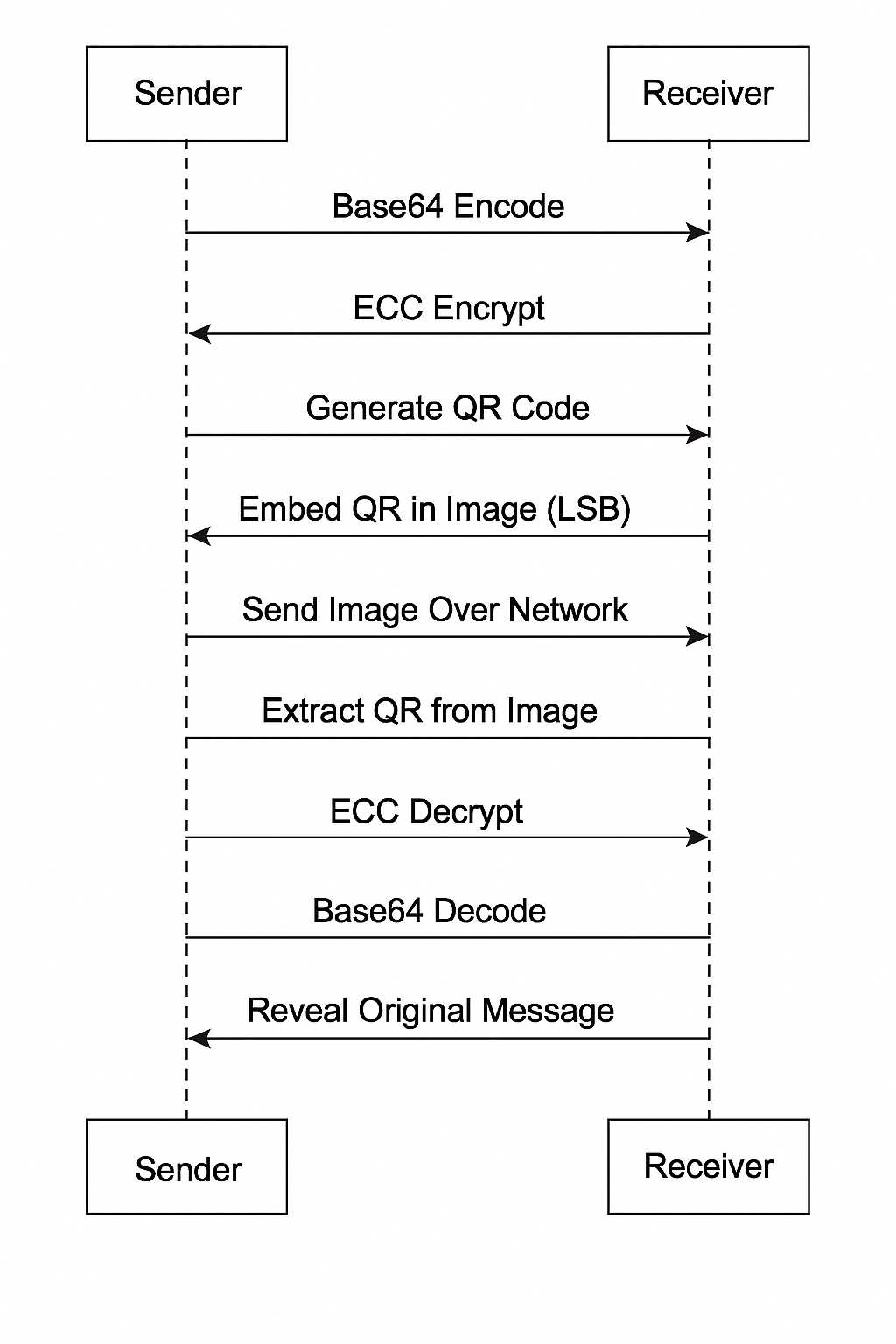
An activity diagram is a behavioural diagram i.e. it depicts the behaviour of a system. An activity diagram portrays the control flow from a start point to a finish point showing the various decision paths that exist while the activity is being executed. Activity Diagrams describe how activities are coordinated to provide a service which can be at different levels of abstraction. Typically, an event needs to be achieved by some operations, particularly where the operation is intended to achieve a number of different things that require coordination, or how the events in a single use case relate to one another, in particular, use cases where activities may overlap and require coordination.



**fig 3 Activity diagram : steganography of encrypted messages with qr code**

**D.SEQUENCE DIAGRAM:**

The sequence diagram illustrates the interaction between a User, a User Terminal, and a Database through various actions related to student information management. It starts with the User logging in via the User Terminal, which sends a request to the Database for user confirmation, followed by a confirmation response back to the User Terminal. When the User registers a student, the User Terminal sends this request to the Database, which registers the student and sends back a confirmation of successful registration.To view student information, the User requests this via the User Terminal, which forwards the request to the Database. The Database retrieves the information and sends it back through the User Terminal to the User. For updating student information, the User makes a request, and the User Terminal updates the information in the Database, which then confirms the update and sends a successful update message back. When deleting student information, the User initiates the request, the User Terminal sends the deletion request to the Database, which processes the deletion and confirms success. Finally, when the User logs out, the User Terminal validates this with the Database, which sends back a successful logout message. This sequence ensures the proper flow of requests and responses between the User, User Terminal, and Database for managing student information.



**Fig.4 Activity diagram of Student Management System**

**CHAPTER 05**

**IMPLEMENTATION**

**IMPLEMENTATION**

**Explanation:**

**These modules are used for the following purposes:**

**1.**[Tkinter](https://sodocumentation.net/tkinter) – To create the GUI.

1. **SQLite3** – To connect the program to the database and store information in it.
2. **TkCalender** – To get the user to enter a date.

**4.Tkinter.messagebox** – To show a display box, displaying some information or an error.

1. **Tkinter.ttk** – To create the tree where all the information will be displayed.

**Initializing the GUI Window**

We have initialized the GUI Window by creating the object of TK() as the main. Set the title of the window, The geometry is the size of the window.

**Creating the color variables:** Creating the background and foreground color variables. **Creating the StringVar and IntVar variables:** Stores the name, email, gender, contact, and stream you entered in the form.

**Place the components in the main window**

We are creating the main frame where we are labeling the window with the title “Student Management System”. We are also creating 2 frames into that i.e left\_frame and right frame specifying the color, width, and height of the frame.

**Placing components in the left frame**

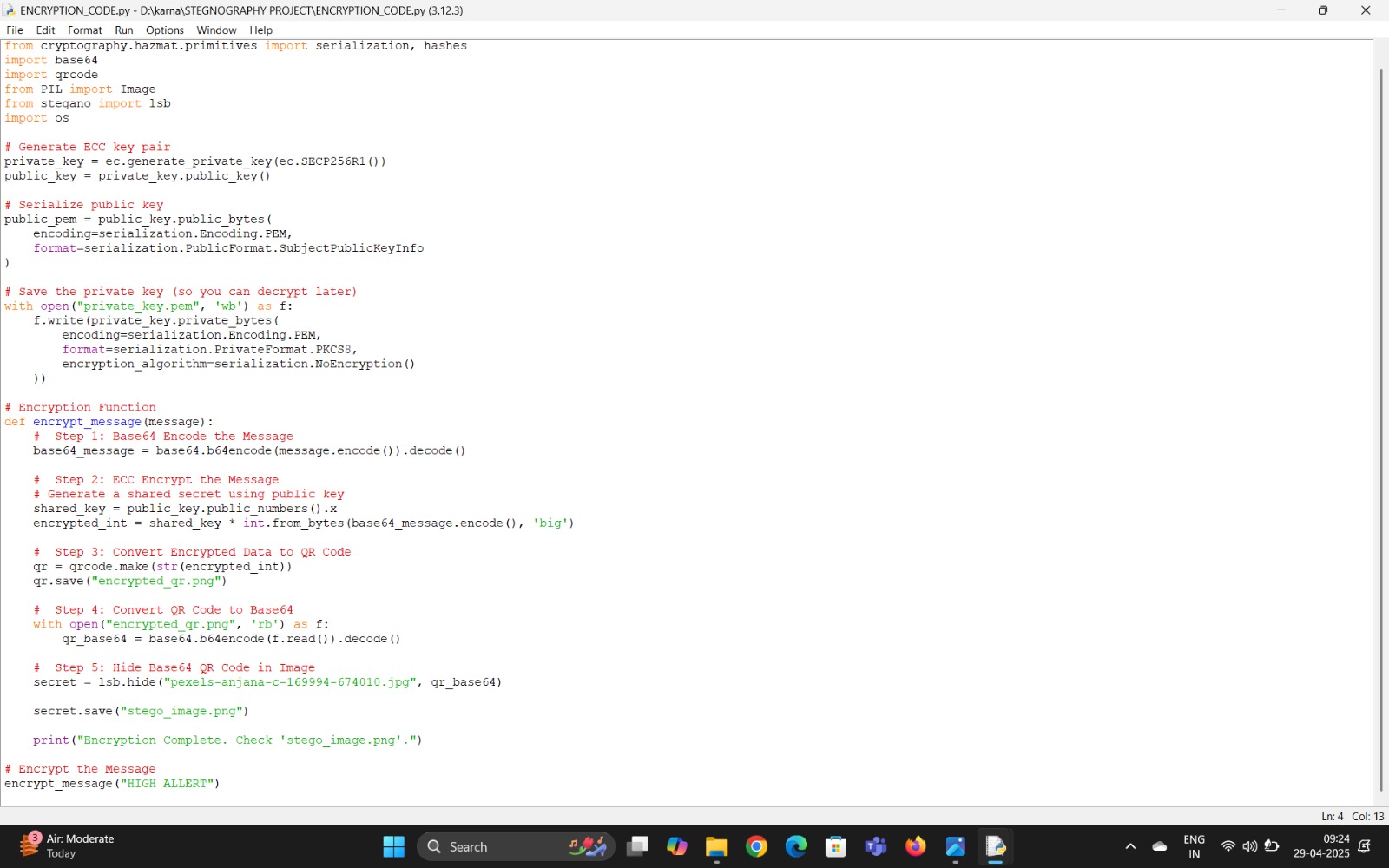
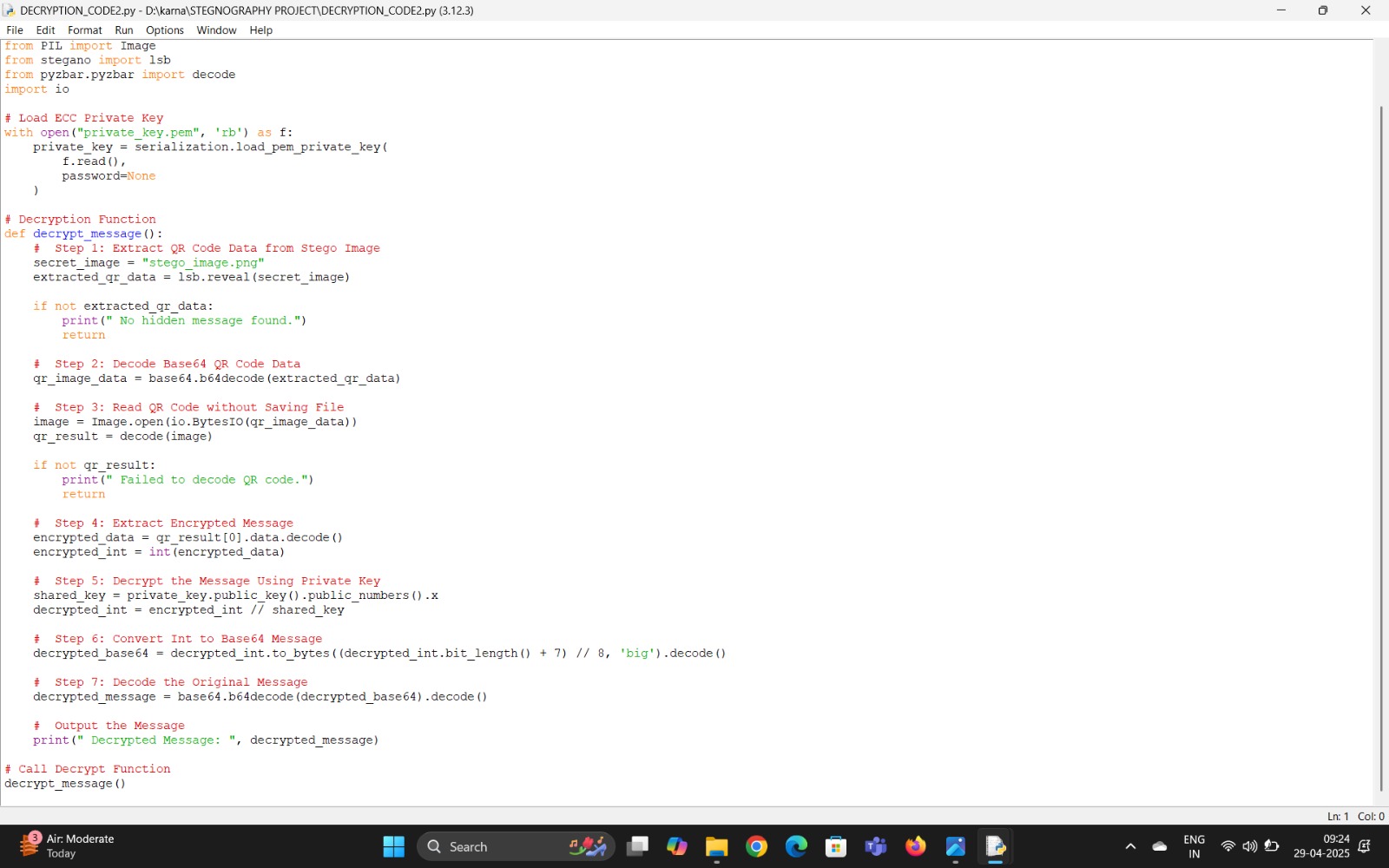
Here we are placing the components like name, contact number, email address, gender, date of birth, and Stream The label function is used for labelling the components and provides formatting. Entry function is used for entering the text. Option Menu provides the dropdown list. The Button label is used for the data entry we provided.

**Placing components in the Right frame**

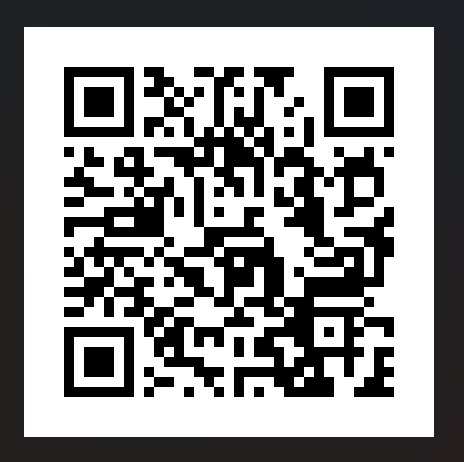
The right frame displays the data that we have entered, deleted, reset, or modified. We have provided the scrollbar to scroll the details horizontally and vertically.

**CHAPTER 06**

**OUTPUT SCREENS**



****



**CHAPTER 07**

**TESTING**

**AND**

**DEBUGGING**

**TESTING AND DEBUGGING**

Testing and debugging for the **Steganography of Encrypted Messages with QR Code** project are essential phases to ensure secure, accurate, and robust data hiding and recovery. These processes validate the encryption integrity, QR code reliability, and steganographic accuracy.

**Testing:**

1. **Unit Testing**:  
   Verifies individual components such as ECC encryption/decryption, QR code generation and scanning, and image steganography (embedding and extraction).
2. **Integration Testing**:  
   Checks how modules like encryption, QR code generation, and steganography work together in sequence to ensure the end-to-end flow is consistent and reliable.
3. **System Testing**:  
   Evaluates the entire system from inputting a message to retrieving the original message from the image, ensuring all steps (encryption → QR generation → embedding → extraction → decryption) work as intended.
4. **Performance Testing**:  
   Assesses how the system performs with varying message lengths, image resolutions, and formats to ensure efficiency and responsiveness.
5. **Security Testing**:  
   Ensures that encrypted messages cannot be decrypted without the correct ECC private key, and that stego-images do not reveal sensitive data if intercepted.
6. **User Acceptance Testing (UAT)**:  
   Engages end users to test the system’s ease of use, interface clarity, and the reliability of message hiding and recovery in realistic usage scenarios.

**Debugging:**

1. **Identifying Issues**:  
   Uses exception handling, logs, and intermediate output files to detect problems in encryption, QR code generation, or image embedding.
2. **Isolating Problems**:  
   Reproduces issues step-by-step, such as verifying if the encrypted data is valid, if the QR is readable, or if the embedded image retains quality.
3. **Fixing Bugs**:  
   Applies code corrections to ensure the ECC encryption logic, QR encoding/decoding, and steganography algorithms perform without errors or data loss.
4. **Testing Fixes**:  
   Confirms the reliability of fixes by retesting individual modules and the entire workflow, checking both typical and edge cases.
5. **Documentation**:  
   Maintains a log of identified bugs, solutions applied, and test results to support future maintenance and avoid similar issues.

By thoroughly testing and debugging the system across all components, the project ensures high security, data integrity, and reliability in securely transmitting hidden messages using ECC and QR code-based

**CHAPTER 08**

**CONCLUSION**

**conclusion**

In an era where digital security is of paramount importance, our project successfully demonstrates a multi-layered approach to secure communication by integrating **Elliptic Curve Cryptography (ECC)**, **QR code encoding**, and **Least Significant Bit (LSB) steganography**. By combining strong encryption, data encoding, and covert embedding techniques, we offer a solution that not only protects the content of sensitive information but also hides its existence from unauthorized users.

The use of ECC ensures robust encryption with smaller key sizes, making the system lightweight, highly secure, and suitable even for resource-constrained environments. Unlike traditional encryption methods, ECC provides comparable levels of security with much lower computational overhead, thereby making it an ideal choice for modern secure communication systems. The encrypted message, once generated, is encoded into a QR code, ensuring a structured and scannable format that simplifies storage, retrieval, and transmission.

To further enhance security, the generated QR code is embedded into a cover image using LSB steganography. This technique effectively conceals the encrypted data without causing noticeable alterations to the visual quality of the image. Thus, it provides an additional layer of stealth, significantly reducing the chances of interception and detection by attackers. The transmission of stego-images allows confidential communication to occur seamlessly, appearing as harmless image sharing.

At the receiver's end, the process is efficiently reversed — the QR code is extracted, decoded, and the message is decrypted using the private ECC key. This ensures that only the intended recipient, who possesses the correct decryption key, can access the original plaintext message. The system's design thus guarantees **confidentiality**, **integrity**, and **authentication** of the communicated information.

Our project demonstrates the practical application of cryptographic and steganographic principles in securing digital communication. It highlights how multi-layered security measures can provide a resilient defense against modern cyber threats, addressing challenges not just of encryption but also of data concealment and integrity verification.

In addition, the system offers high usability through QR code scanning and minimal computational requirements, making it accessible to a wide range of users and adaptable to various domains such as **secure messaging**, **digital watermarking**, **digital forensics**, and **private data storage**.

By successfully merging ECC, QR encoding, and LSB steganography, the project presents a novel, effective, and scalable solution for secure and covert communication in today’s increasingly interconnected and threat-prone digital world. It paves the way for future enhancements, such as the incorporation of advanced steganographic techniques, support for different media formats, and stronger integrity verification methods.

Thus, this project not only meets its initial objectives but also opens new possibilities for further research and development in the field of secure, covert communication systems.

**CHAPTER 09**

**FUTURE ENHANCEMENT**

**9.FUTURE ENHANCEMENT**

In the future, this project can be significantly expanded to improve security, robustness, and usability. Currently, Least Significant Bit (LSB) steganography is used, but more advanced techniques like Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) steganography could be integrated to make the hidden data even more resistant to image processing attacks such as compression or resizing. Additionally, instead of limiting the hiding process to static images, future versions could allow embedding encrypted data into videos, audio files, or documents like PDFs, making detection even more difficult. The reliability of data extraction could also be enhanced by using stronger error correction techniques during QR code generation. On the encryption side, while Elliptic Curve Cryptography (ECC) provides strong security, it could be combined with symmetric algorithms like AES (Advanced Encryption Standard) to create a hybrid encryption model for even greater protection. To further ensure message authenticity and integrity, digital signatures and cryptographic hash functions such as SHA-256 could be incorporated. From a usability perspective, building a user-friendly mobile or desktop application with an intuitive graphical interface would make the system accessible even to non-technical users. Finally, integrating cloud storage options would allow users to securely store and share stego-images across different platforms, adding flexibility and convenience. These enhancements would make the system more secure, resilient, scalable, and easier to use for real-world applications.

Looking forward, there are several promising directions to further enhance this project. Although the current implementation uses LSB (Least Significant Bit) steganography for hiding encrypted messages inside images, future versions could adopt more sophisticated methods like Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), or even Deep Learning-based steganography techniques. These methods would make the hidden data more robust against common image processing operations such as compression, resizing, and filtering, thus providing stronger resistance to steganalysis attacks. Additionally, instead of restricting the hidden data to QR codes alone, future work could explore hiding different types of files such as text documents, images, audio, and even video files. This would greatly broaden the system’s usability.

From the security standpoint, while Elliptic Curve Cryptography (ECC) already offers strong encryption with lower computational costs, combining ECC with symmetric key encryption like AES (Advanced Encryption Standard) could create a hybrid model. This would not only make encryption faster for larger data but also enhance overall security. Implementing advanced authentication techniques like digital signatures and cryptographic hash algorithms (e.g., SHA-256 or SHA-3) could ensure the authenticity and integrity of the message, providing users with an additional layer of trust.

Another major enhancement could be the development of a complete software solution with a modern, intuitive user interface (UI) — possibly as a cross-platform mobile or desktop application. Features like drag-and-drop image selection, real-time preview of QR codes, customizable encryption options, and automatic key generation could significantly improve user experience. Additionally, machine learning models could be trained to automatically choose the optimal steganography method based on the type and size of the cover medium.

Integration with cloud technologies could allow users to store stego-images securely in the cloud or share them via secure links, adding remote access and collaboration features. Blockchain technology could also be explored for maintaining a tamper-proof record of hidden communications, especially in sensitive applications like digital contracts, secure voting, or confidential communications.

Furthermore, to promote scalability and efficiency, batch processing capabilities could be added, enabling users to encrypt and embed multiple messages at once. Real-time steganalysis defense systems could also be incorporated to alert users if the cover medium becomes vulnerable to potential attacks.

Overall, these future enhancements aim not just to improve security and robustness, but also to make the system more practical, versatile, and user-friendly for real-world deployment across industries such as cybersecurity, military communication, digital rights management, and personal privacy protection.

**CHAPTER 10**

**REFERENCES**

**10.REFERENCES**

1. Mrs. D Betteena Sheryl Fernando “Steganography of messages encrypted with QR Code”

[International Journal of Computer Science Engineering and Information Technology](https://www.researchgate.net/journal/International-Journal-of-Computer-Science-Engineering-and-Information-Technology-2231-3117?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIiwicHJldmlvdXNQYWdlIjoiX2RpcmVjdCJ9fQ) in the year

2021 march.

1. Mr. Arun Kumar Singh “Steganography in Digital Images USinf LSB” Journal of Xidian University in the year 2020 september.
2. Mr. Deepak Singla “Data security and integrity using data hiding” [International Journal of Computer Science Engineering and Information Technology](https://www.researchgate.net/journal/International-Journal-of-Computer-Science-Engineering-and-Information-Technology-2231-3117?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIiwicHJldmlvdXNQYWdlIjoiX2RpcmVjdCJ9fQ) in the year 2020 february.
3. Mr. Osama Faragallah “Steagnography of encrypted messages” [International Journal of Computer Science Engineering and Information Technology](https://www.researchgate.net/journal/International-Journal-of-Computer-Science-Engineering-and-Information-Technology-2231-3117?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIiwicHJldmlvdXNQYWdlIjoiX2RpcmVjdCJ9fQ) in the year 2020 february.
4. Mr. Balasubramani Ramaswamy “A Secure Data Transmission using Audio Steganography Based on Randomized LSB Technique” in the year 2017
5. Mr. Mohammad Soltani “A New Secure Hybrid Algorithm for QR-Code Images Encryption and Steganography” [APTIKOM Journal on Computer Science and Information Technologies](https://www.researchgate.net/journal/APTIKOM-Journal-on-Computer-Science-and-Information-Technologies-2528-2425?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIiwicHJldmlvdXNQYWdlIjoiX2RpcmVjdCJ9fQ) in the year 2017 july.