

DATA SECURITY THROUGH QR STEGANOGRAPHY

MINI PROJECT REPORT

*submitted in partial fulfillment of the requirements.
for the award of the degree in*

**BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING**

BY

DHANUSH G (201191101014)

SAKTHIVEL G (201191101050)

SHUVAM PANDAY J (201191101053)



Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY

University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.



**DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING**

APRIL 2023



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of

MR. DHANUSH G Reg.No 201191101014,

MR. SAKTHIVEL K Reg.No 201191101050,

MR. SHUVAM PANDAY J Reg.No 201191101053,

who carried out the mini-project entitled **DATA SECURITY THROUGH QR STEGANOGRAPHY** under our supervision from January 2023 to May 2023

Mini Project Coordinator 1

Mrs.Chinchu Nair
Assistant Professor
Dr.MGR Educational and
Research Institute
Deemed to be University

Mini Project Coordinator 2

Dr.Manikandan
Assistant Professor
Dr.MGR Educational
and Reseach Institute
Deemed to be University

HOD

Dr.S.Geetha
HOD of CSE
Dr.MGR Educational
and Research Institute
Deemed to be University

Submitted for Viva Voce Examination held on

Internal Examiner

External Examiner



DECLARATION

We, MR Dhanush G (201191101014), MR Sakthivel K (201191101050), MR Shuvam Panday J (201191101053), hereby declare that the Mini Project Report entitled **“DATA SECURITY THROUGH QR STEGANOGRAPHY”** is done by us under the guidance of **“Mrs.Chinchu Nair & Dr.Manikandan”** is submitted in partial fulfilment of the requirements for the award of the degree in **Bachelor of Technology in Computer Science and Engineering.**

Date:

Place: CHENNAI

- 1.
- 2.
- 3.

Signature of the Candidates

ACKNOWLEDGEMENT

We would first like to thank our beloved Chancellor Thiru A.C. SHANMUGAM, B.A., B.L. and President Er. A.C.S. Arunkumar, B.Tech., M.B.A., and for all the encouragement and support extended to us during the tenure of this project and also our years of studies in his wonderful University.

We express my heartfelt thanks to our Vice Chancellor Prof. Dr. S. Geethalakshmi in providing all the support of our Mini Project.

We express my heartfelt thanks to our Head of the department, Prof. Dr. S. Geetha, who has been actively involved and very influential from the start till the completion of our project.

Our sincere thanks to our Project Coordinators Mrs. Chinchu Nair & Dr. Manikandan, for their continuous guidance and encouragement throughout this work, which has made the mini project a success.

We would also like to thank all the teaching and non-teaching staffs of Computer Science and Engineering department, for their constant support and the encouragement given to us while we went about to achieving my project goals.



TABLE OF CONTENTS

CHAPTER NAME	TITLE	PAGE NUMBER
	ABSTRACT	1
1	PROJECT SYNOPSIS/ INTRODUCTION	2
2	LITERATURE SERVEY	5
3	SOFTWARE REQUIREMENTS	6
4	SYSTEM DESIGN	8
5	DATABASE DESIGN	10
6	DETAILED DESIGN	12
7	TESTING	14
8	IMPLEMENTATION	17
9	CONCLUSION	24
10	BIBLIOGRAPHY	25



ABSTRACT

QR code steganography is a process of hiding secret information in a QR code image. It enables users to store a larger amount of data than normal in a single QR code image. The secret information can be text, image, audio, or even video. The secret information is hidden in the QR code image in such a way that it can be read and decoded by a suitable reader. The process of QR code steganography involves embedding the secret information into the QR code image and then encrypting it. This makes it difficult for anyone to decode secret information without the right key. QR code steganography uses QR codes as a medium for hiding secret information. It works by embedding the secret information into the QR code image. The secret information is encrypted and stored in the QR code image. The encryption process ensures that the data is secure and is only readable by the intended recipient. The QR code image is then scanned to decode the secret information.

QR code steganography offers several advantages compared to other methods of steganography. It is relatively easy to implement and is relatively secure compared to other methods. Furthermore, it allows users to store large amounts of data in a single QR code image.

CHAPTER-1: PROJECT SYNOPSIS

1. Title of the Project:

Data Security Through QR steganography

2. Objectives of the project:

In this project , we are using a more robust steganography algorithm that can better resist attacks such as image compression and cropping. Here we are using cmyk method to make the qr code colourful to increase the storage.

3. Project Category:

The project category for QR steganography could fall under various categories depending on the scope and complexity of the project. Some possible project categories could be:

- **Cybersecurity**
- **Information Technology**
- **Computer Science**
- **Mathematics**

4. Hardware and software Requirement Specifications:

Hardware requirements:

- **Operating system- Windows7/Windows 10**
- **Processor- Intel dual core**
- **RAM-2GB**
- **Hard Disk- Minimum 50GB**
- **Keyboard, monitor, scanner and mouse**

Software requirements:

- **MySQL Database server**

5. Programming Language:

Front End :

- **HTML,CSS**

Back End:

- **Python**

CHAPTER-1: INTRODUCTION

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. The word steganography is derived from the Greek words *steganos* (meaning hidden or covered) and the Greek root *graph* (meaning to write).

Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content concealed through steganography -- hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

PURPOSE:

The main objective of QR steganography is to hide a secret message within a QR code image in such a way that it is not noticeable to the casual observer. This is achieved by embedding the secret message in the code using various steganographic techniques.

QR codes are a type of two-dimensional barcode that can store a large amount of data, including text, URLs, and other types of information. QR steganography can hide a secret message within the code by manipulating the color, pattern, or size of the individual modules that make up the code. This can be done by replacing certain modules with others that have slightly different colors or patterns, or by using modules that are slightly larger or smaller than normal.

QR steganography can be used for a variety of purposes, such as sending secret messages or hiding sensitive data in plain sight

ADVANTAGES

QR steganography has several advantages over other forms of steganography:

Easy to use: QR codes are commonly used in everyday life, making it easy to hide secret messages in plain sight.

Large storage capacity: QR codes can store more information than traditional barcodes, providing a larger storage capacity for hidden messages.

Difficult to detect: QR codes can be hidden within images, making them difficult to detect by an observer who is not aware of the hidden message.

Secure: QR steganography can provide a high level of security, as the hidden message can only be accessed by those who know the key or algorithm used to encode it.

Cross-platform compatibility: QR codes can be read by almost any modern smartphone or tablet, making them accessible to a wide audience.

Overall, QR steganography can be a simple yet effective way to hide messages in plain sight, providing a secure and efficient way to transmit sensitive information.

DISADVANTAGES

QR steganography, which involves hiding secret information within a QR code, has some disadvantages, including:

Limited storage capacity: QR codes have limited storage capacity, which means that only a small amount of data can be hidden within them. This can be a disadvantage if a large amount of information needs to be hidden.

Susceptible to detection: QR codes can be easily scanned and analyzed using various tools, making it easier for anyone to detect if a message is hidden within them. This means that QR steganography may not be the most secure way to hide sensitive information.

Quality degradation: When information is hidden within a QR code, it can cause the image quality to degrade, making it difficult to scan the QR code accurately. This can lead to errors and make the hidden message difficult to decode.

Limited usage: QR codes are not universally supported, and some devices may not be as effective as a means of transmitting hidden messages.

Overall, QR steganography can be useful for hiding small amounts of information, but it may not be the best option for securing large amounts of sensitive data.

CHAPTER-2 : LITERATURE SURVEY

Steganography of Encrypted Messages Inside Valid QR Codes

<https://ieeexplore.ieee.org/document/8985346>

Research and Development of QR Code Steganography Based on JSteg Algorithm in DCT Domain

<https://ieeexplore.ieee.org/document/9278285>

Steganography of Encrypted Messages Inside Valid QR Codes.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8985346>

CHAPTER -3 : SOFTWARE REQUIREMENT SPECIFICATIONS

Introduction:

QR Steganography is a software tool that enables users to hide information within QR codes. The software will allow users to input a message or data, which will then be encoded into a QR code image. The encoded information can only be accessed by scanning the QR code using a QR code scanner. The purpose of this Software Requirements Specification (SRS) document is to describe the functional and non-functional requirements for the QR Steganography software.

FUNCTIONAL REQUIREMENT:

User Interface:

The software should have an intuitive and user-friendly interface that allows users to easily input the message or data they want to encode.

Encoding:

The software should be able to take input data from the user and encode it into a QR code image.

Decoding:

The software should be able to decode the information hidden within a QR code image and display it to the user.

Security:

The software should implement security measures to prevent unauthorized access to the encoded information.

Image Generation:

The software should generate QR code images that are easily readable by any QR code scanner.

Error Correction:

The software should include error correction mechanisms that enable the QR code image to be read even if the image is partially damaged or distorted.

NON-FUNCTIONAL REQUIREMENT:

Performance:

The software should be able to encode and decode information quickly and efficiently.

Portability:

The software should be able to run on multiple platforms, including Windows, macOS, and Linux.

Security:

The software should ensure the confidentiality and integrity of the encoded information, such that only authorized users can access it.

Reliability:

The software should be reliable and error-free, with minimal crashes or unexpected behavior.

Compatibility:

The software should be compatible with a wide range of QR code scanners.

User Documentation:

The software should include comprehensive user documentation that explains how to use the software and its features.

Conclusion:

The QR Steganography software will be a valuable tool for anyone who needs to transmit information in a secure and discreet manner. By implementing the functional and non-functional requirements outlined in this document, the software will be reliable, efficient, and easy to use.

CHAPTER-4 : SYSTEM DESIGN

Introduction:

QR steganography is the practice of hiding information within a QR code without affecting its functionality. Here is a high-level system design for QR steganography:

Encoding: The first step is to encode the information you want to hide into a binary stream. This information could be text, an image, a video, or any other type of data.

QR Code Generation: The next step is to generate a QR code using a library such as QRcode or Zxing. This QR code will serve as the carrier for the hidden data.

QR Code Modification: After generating the QR code, the next step is to modify the QR code to embed the hidden data. This can be done in a few ways:

Substitution: In this method, specific pixels within the QR code are replaced with pixels that represent the hidden data. This technique is useful for hiding small amounts of data.

LSB Substitution: In this method, the least significant bit of each pixel in the QR code is replaced with a bit of the hidden data. This technique is useful for hiding larger amounts of data.

Reed-Solomon Coding: In this method, the hidden data is encoded using Reed-Solomon coding, and the resulting code is embedded within the error correction codewords of the QR code. This technique is useful for hiding large amounts of data and providing robustness to errors.

Decoding: To decode the hidden data from the modified QR code, you will need to reverse the process used for embedding the data. This involves:

- **Extracting the modified pixels from the QR code**
- **Reversing the embedding process to extract the hidden data**
- **Decoding the binary stream back into the original data format (e.g. text, image, video, etc.)**

Some additional considerations when designing a QR steganography system include:

Security: Depending on the sensitivity of the hidden data, you may need to use encryption to protect it from unauthorized access.

Capacity: The amount of data that can be hidden within a QR code depends on the size of the code, the level of error correction used, and the embedding technique employed. You will need to choose an appropriate technique that balances data capacity with robustness to errors.

Performance: The time required for encoding and decoding will depend on the complexity of the embedding technique and the size of the hidden data. You may need to optimize your implementation to ensure reasonable performance.

CHAPTER-5 : DATABASE DESIGN

QR steganography is the process of hiding secret information within a QR code, which is a two-dimensional barcode. To design a database for QR steganography, you need to consider the following entities:

User: This entity stores the user's information, such as name, email address, and password.

QR code: This entity stores the QR code's information, such as the image file, size, and content.

Secret message: This entity stores the secret message that is hidden within the QR code. It could include the message content, encryption algorithm used, and the key.

Access logs: This entity stores the access logs of the QR code. It could include the timestamp of when the code was accessed, the IP address, and the user who accessed it.

Here is a sample database schema for QR steganography:

User

- UserID (Primary Key)
- Name
- Email
- Password

QRCode

- QRCodeID (Primary Key)
- Image
- Size
- Content

SecretMessage

- **SecretMessageID (Primary Key)**
- **MessageContent**
- **EncryptionAlgorithm**
- **Key**

AccessLogs

- **AccessLogID (Primary Key)**
- **QRCodeID (Foreign Key)**
- **UserID (Foreign Key)**
- **Timestamp**
- **IPAddress**

In this schema, the User entity has a one-to-many relationship with the Access Logs entity, as each user can access multiple QR codes, and each QR code can be accessed by multiple users. Similarly, the QR Code entity has a one-to-one relationship with the Secret Message entity, as each QR code can have only one secret message hidden within it.

This database schema can be further optimized and customized based on the specific requirements of your QR steganography application.

CHAPTER-6: DETAILED DESIGN

Designing a detent mechanism for QR steganography would require careful consideration of the security requirements and the user experience. Here is a possible design:

1. Mechanism:

- **The detent mechanism could be a physical button or switch that is activated when the QR code is scanned with a specific app or device.**
- **The detent mechanism would be connected to a microcontroller that would trigger an action, such as displaying a message or performing a specific function, when the detent is activated.**

2. App or device:

- **The app or device used to scan the QR code and activate the detent mechanism would need to be secure and trusted, to prevent unauthorized access to the hidden data within the code.**
- **The app or device would also need to be designed to detect the presence of the detent mechanism and trigger the appropriate action when it is activated.**

3. Security considerations:

- **The detent mechanism should be designed to prevent tampering or bypassing, such as by using a physical seal or lock to prevent unauthorized access to the mechanism.**
- **The microcontroller used to trigger the action should be securely programmed and stored to prevent unauthorized access or modification.**
- **The app or device used to scan the QR code should be designed to prevent reverse engineering or tampering, and to encrypt the data transmitted between the app or device and the QR code.**

4. User experience:

- **The detent mechanism should be designed to be easy to use and understand, to prevent user error or confusion.**
- **The app or device used to scan the QR code should provide clear instructions or feedback to the user when the detent is activated, to prevent confusion or uncertainty about what action has been triggered.**
- **The detent mechanism and the associated action should be designed to be appropriate for the context in which the QR code is being used, to prevent inappropriate or unintended consequences.**

CHAPTER-7: TESTING

QR code steganography is a method of hiding secret information within a QR code image without changing its appearance. To test for the presence of steganography in a QR code, you can use various steganalysis tools that can detect any alterations or modifications made to the QR code image.

Here are some methods you can use to test for QR code steganography:

- **Visual inspection:** You can visually inspect the QR code image for any signs of manipulation or tampering. Look for any inconsistencies in the pattern or color of the QR code image.
- **Steganalysis tools:** There are several steganalysis tools available online that can help detect steganography in QR codes. Some popular tools include StegExpose, StegDetect, and Outguess.
- **QR code decoders:** You can use QR code decoding software to decode the QR code and check if any hidden information is present. If the decoded data contains any extra characters or symbols that are not part of the original message, it may be an indication of steganography.
- **Statistical analysis:** You can perform a statistical analysis of the QR code image to detect any irregularities. For example, the distribution of the pixels in the image may indicate the presence of steganography.

It is important to note that while these methods can help detect steganography in QR codes, they may not be foolproof. Some steganography techniques are designed to be undetectable by steganalysis tools, and may require more advanced techniques to detect

Use Case Diagram:

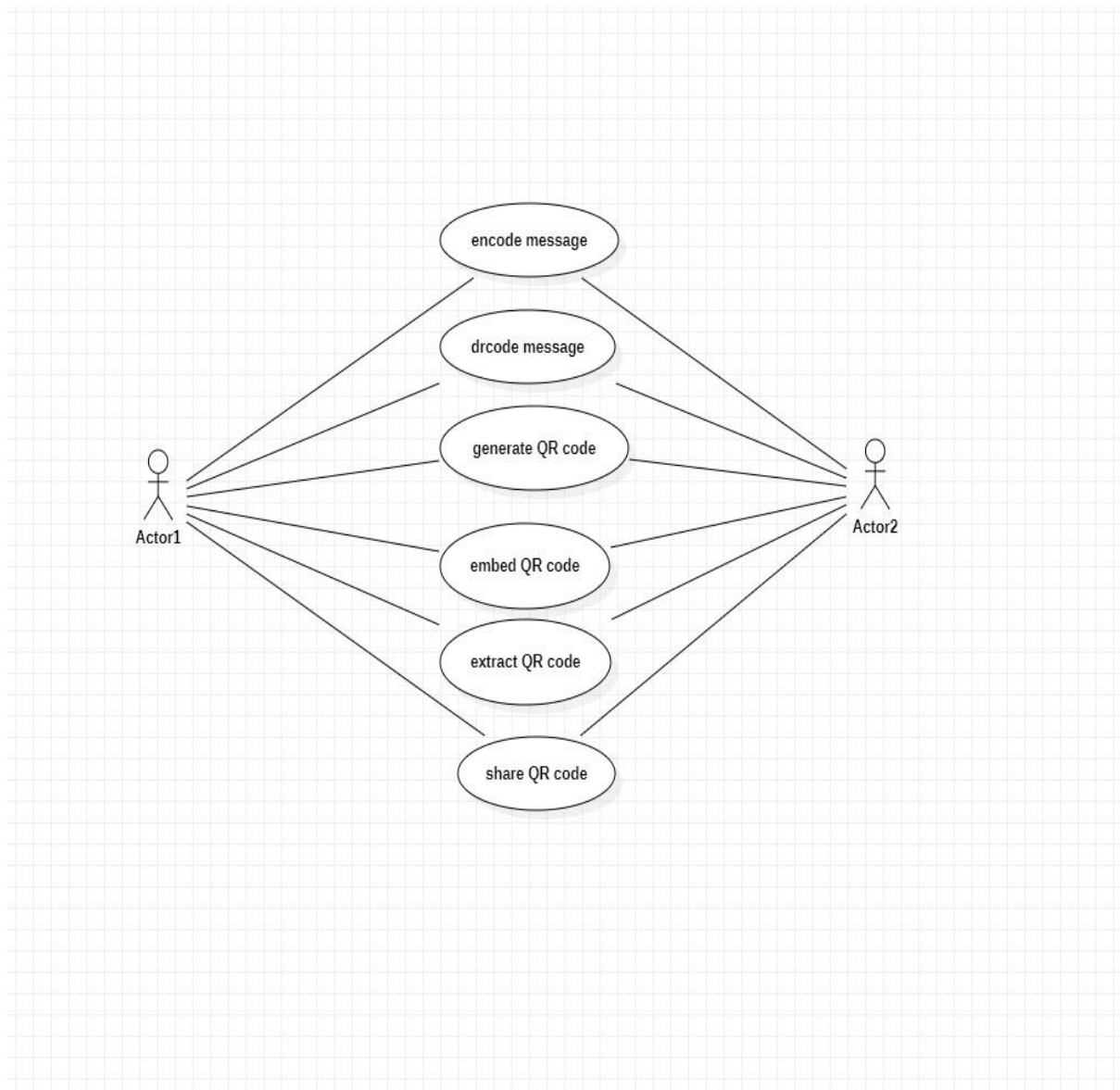


Figure:6.1

Sequence Diagram:

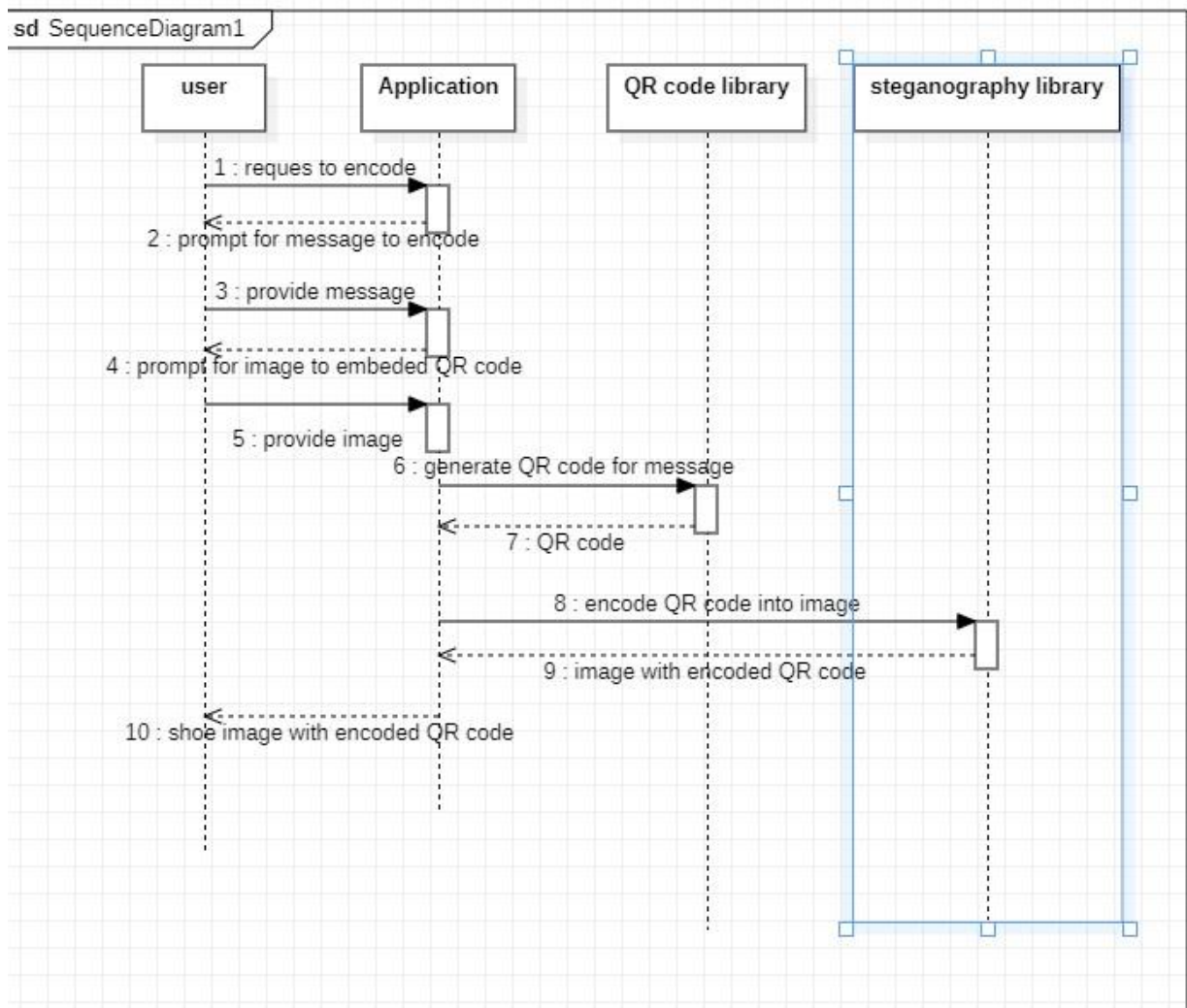
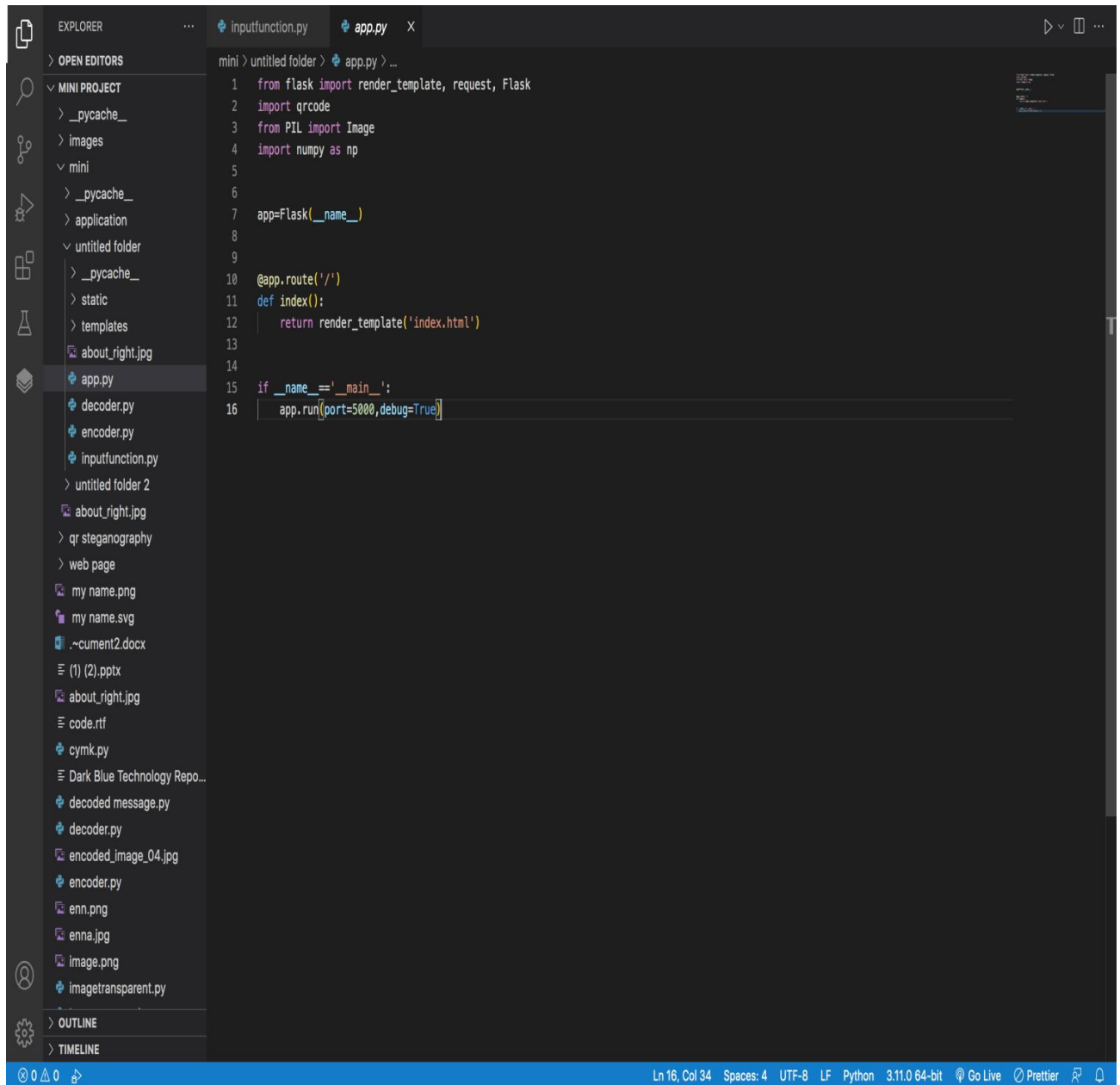


Figure:6.2

CHAPTER-8: IMPLEMENTATION AND RESULT

SAMPLE CODE:

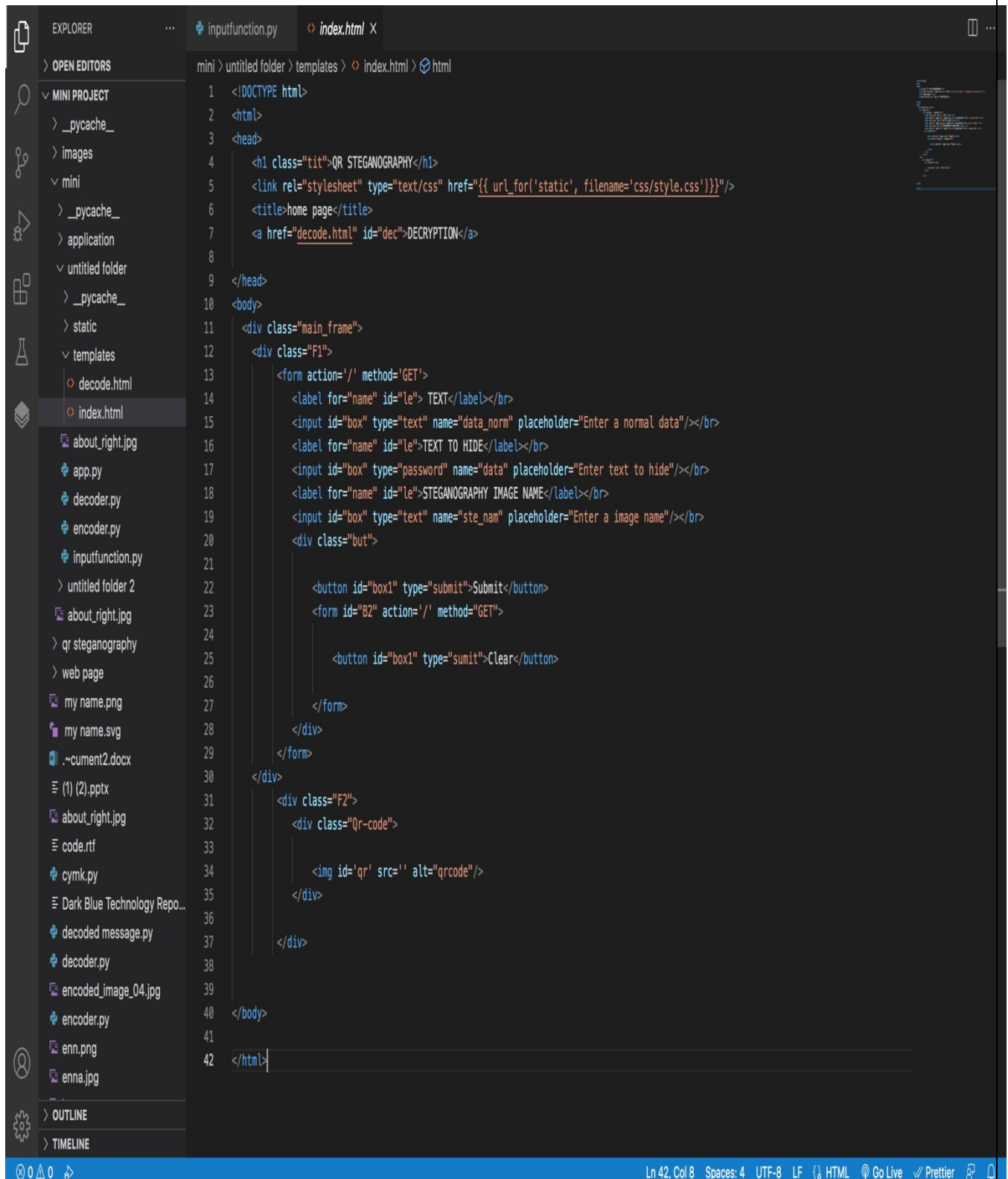
App.py



```
1 from flask import render_template, request, Flask
2 import qrcode
3 from PIL import Image
4 import numpy as np
5
6
7 app=Flask(__name__)
8
9
10 @app.route('/')
11 def index():
12     return render_template('index.html')
13
14
15 if __name__=='__main__':
16     app.run(port=5000,debug=True)
```

Figure:7.1

Index.html



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <h1 class="tit">QR STEGANOGRAPHY</h1>
5   <link rel="stylesheet" type="text/css" href="{{ url_for('static', filename='css/style.css')}}"/>
6   <title>home page</title>
7   <a href="decode.html" id="dec">DECRYPTION</a>
8
9 </head>
10 <body>
11   <div class="main_frame">
12     <div class="F1">
13       <form action="/" method="GET">
14         <label for="name" id="le"> TEXT</label><br>
15         <input id="box" type="text" name="data_norm" placeholder="Enter a normal data"/><br>
16         <label for="name" id="le">TEXT TO HIDE</label><br>
17         <input id="box" type="password" name="data" placeholder="Enter text to hide"/><br>
18         <label for="name" id="le">STEGANOGRAPHY IMAGE NAME</label><br>
19         <input id="box" type="text" name="ste_nam" placeholder="Enter a image name"/><br>
20         <div class="but">
21
22           <button id="box1" type="submit">Submit</button>
23           <form id="B2" action="/" method="GET">
24
25             <button id="box1" type="sumit">Clear</button>
26
27           </form>
28         </div>
29       </form>
30     </div>
31     <div class="F2">
32       <div class="Qr-code">
33
34         <img id="qr" src="" alt="qrcode"/>
35       </div>
36     </div>
37   </div>
38
39 </body>
40
41
42 </html>
```

figure:7.2

Decoder.py

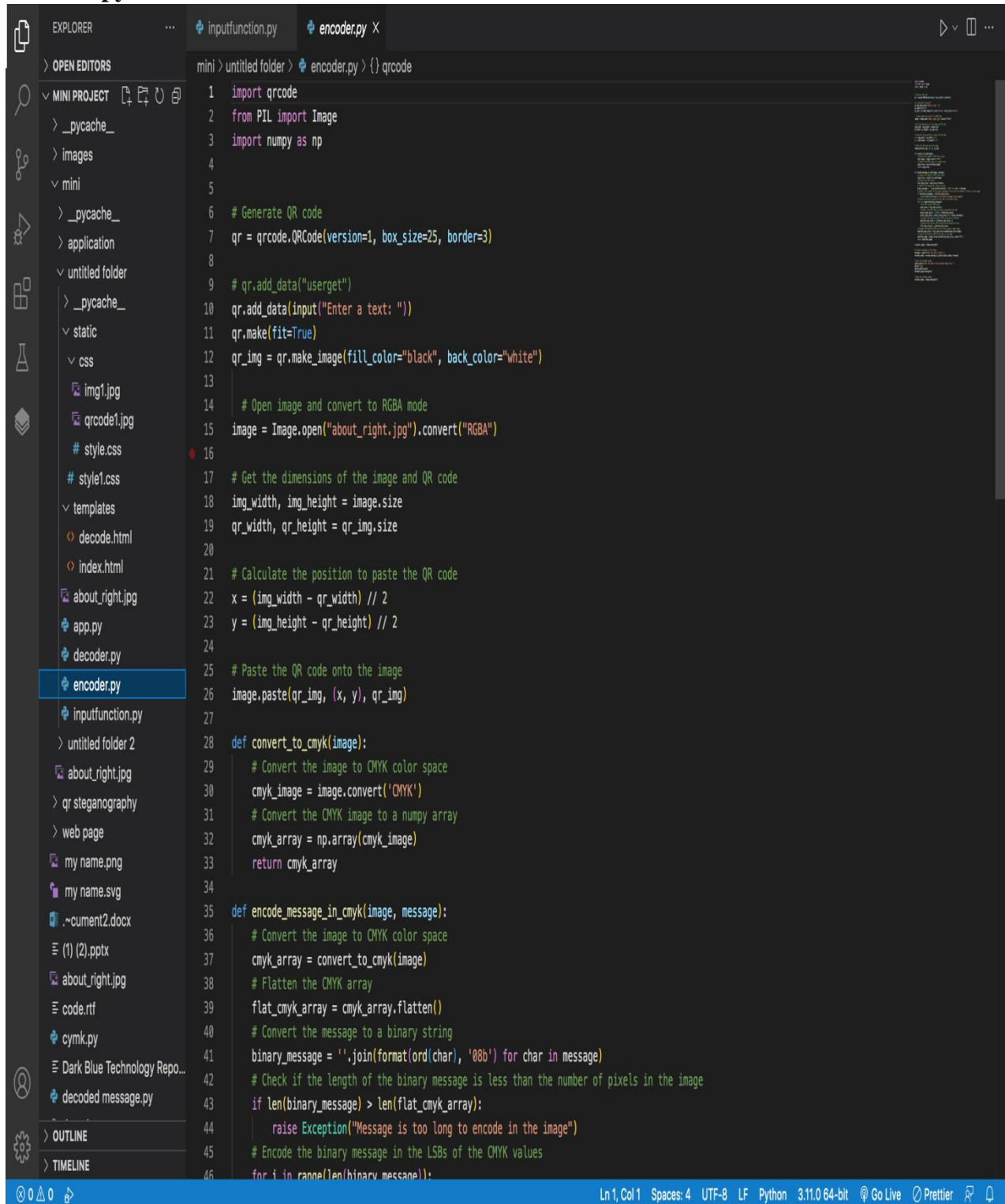


figure:7.2

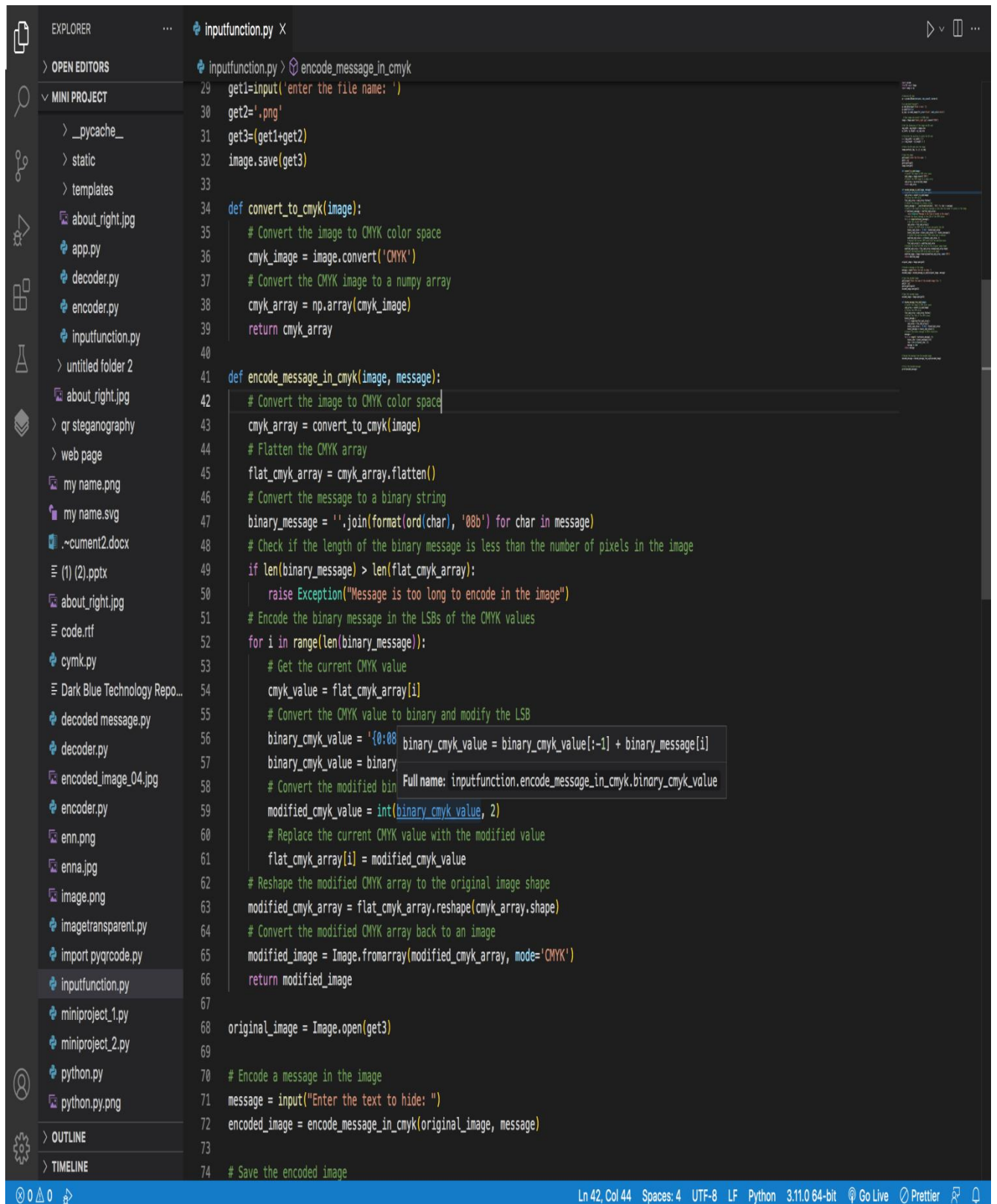


figure:7.3

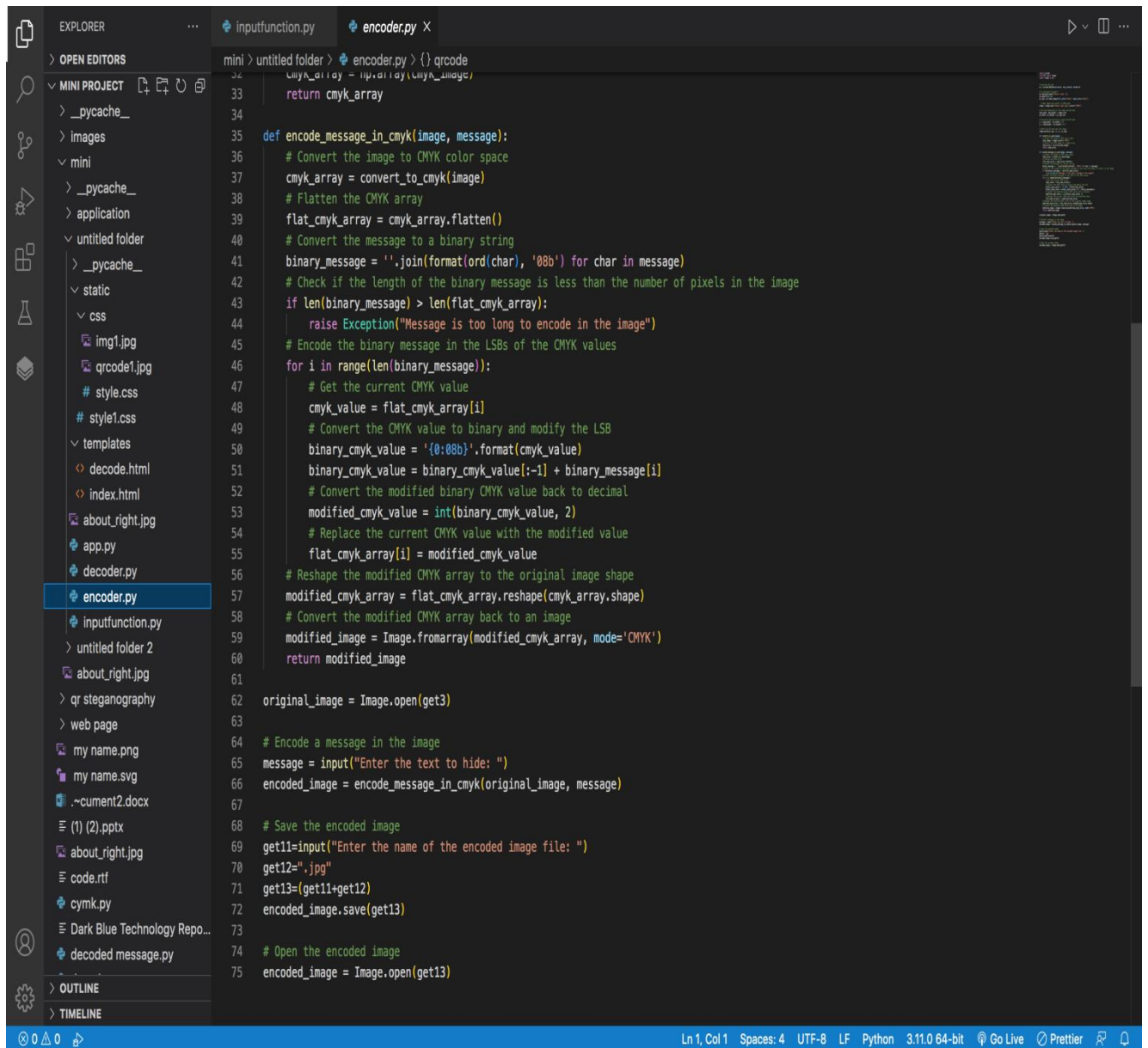


figure:7.4

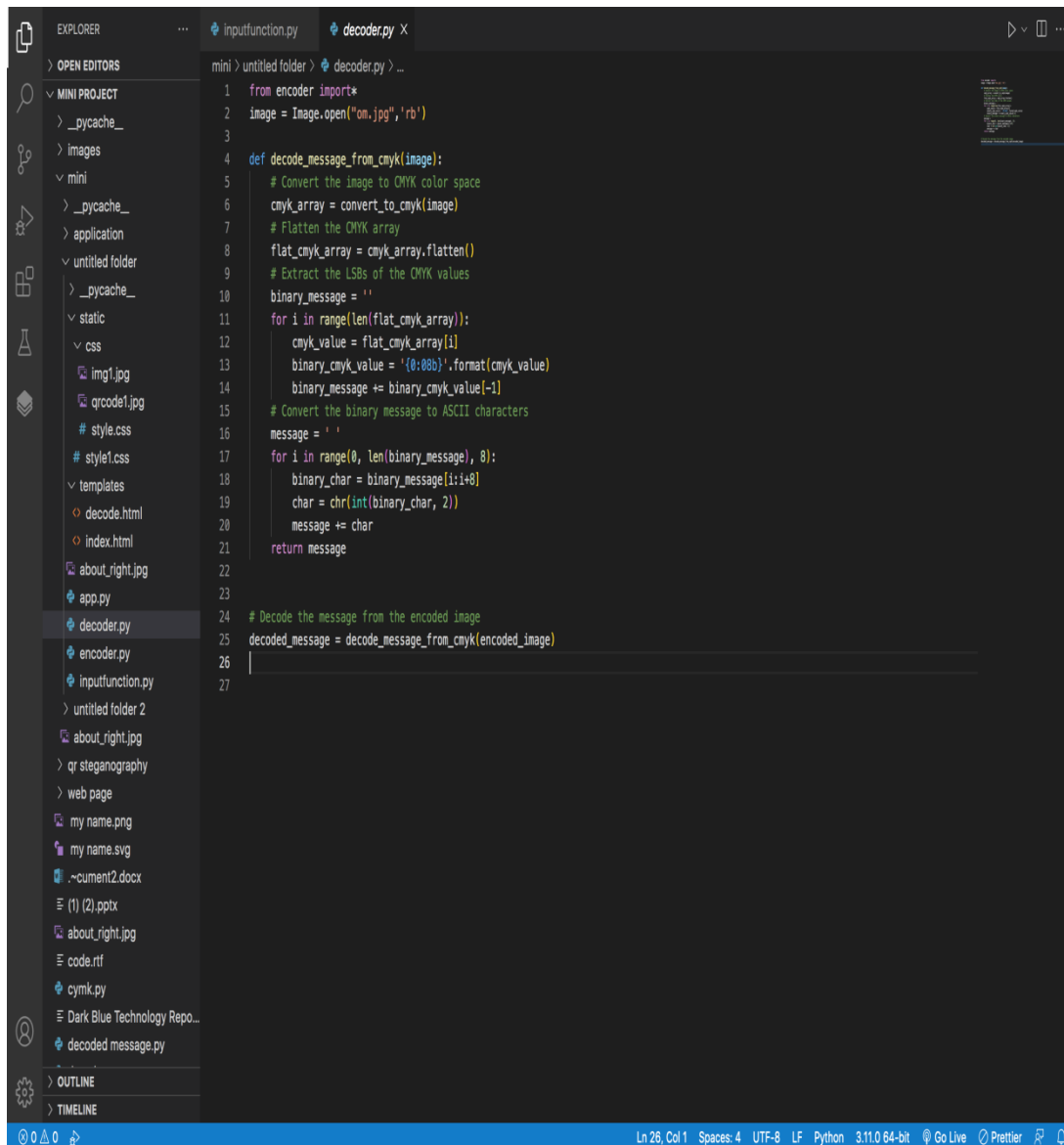


Figure:7.5

FRONT-END :

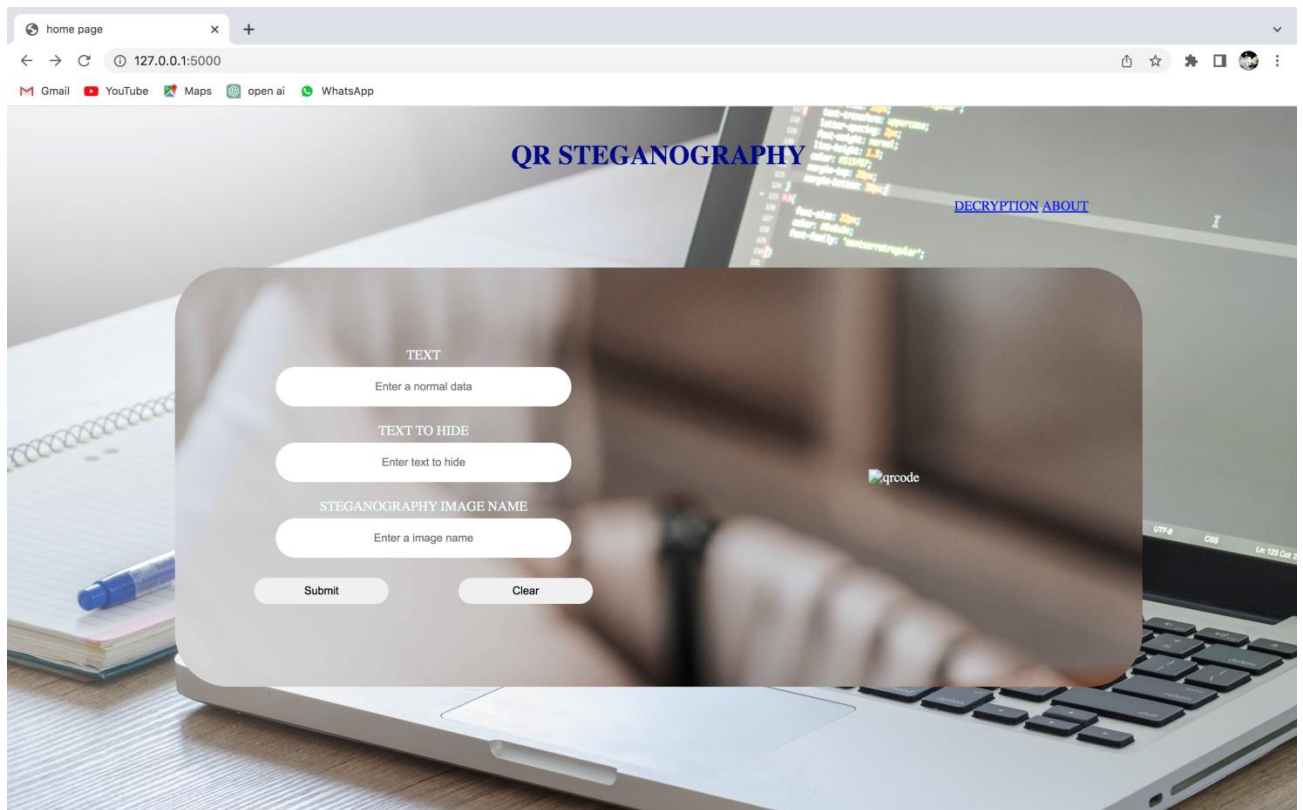


Figure:8.1

SAMPLE OUTPUT:



Figure:8.2

CHAPTER-9: CONCLUSION

In conclusion, QR steganography is a technique for hiding secret data within a QR code image. It enables secure communication, data storage, and transfer in a covert manner. The LSB method is a commonly used technique in QR steganography where the least significant bits of the QR code pixel values are replaced with the bits of the secret data. QR steganography has a wide range of applications in various fields such as security, information hiding, and cryptography. Despite its benefits, QR steganography is not foolproof as the embedded data can be extracted by advanced steganalysis techniques. Hence, it is important to use strong encryption methods to ensure the confidentiality and privacy of the hidden data.

CHAPTER-10:BIBLIOGRAPHY

- [1] Ali, A., Khan, I., & Tariq, R. (2019). QR code steganography for secure communication: A review. *International Journal of Advanced Computer Science and Applications*, 10(10), 89-96.
- [2] Hu, X., & Jiang, Y. (2018). QR code steganography based on matrix encoding. *Journal of Physics: Conference Series*, 1069(1), 012061.
- [3] Singh, S. P., Kumar, P., & Rajak, B. K. (2017). QR code steganography based secure communication. *International Journal of Computer Applications*, 166(2), 1-4.
- [4] Yadav, P., & Singh, V. (2020). A comparative study of QR code steganography techniques. *International Journal of Emerging Trends & Technology in Computer Science*, 9(3), 64-70.
- [5] Zhang, J., Chen, Z., & Li, J. (2019). A novel QR code steganography algorithm based on group theory. *Symmetry*, 11(11), 1423.
- [6] Kshirsagar, N., & Kulkarni, R. (2018). QR code steganography with RSA encryption. *International Journal of Computer Science and Mobile Computing*, 7(4), 200-206.
- [7] Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbolology QR Code, ISO/IEC 18004, 2000.
- [8] Denso-Wave Inc., QR code standardization, 2003 [Online]. Available: <http://www.qrcode.com/en/index.html>
- [9] Lin, Pei-Yu. "Distributed secret sharing approach with cheater prevention based on QR code." *IEEE Transactions on Industrial Informatics* 12, no. 1 (2016): 384-392.
- [10] Dey, Somdip, Kalyan Mondal, Joyshree Nath, and Asoke Nath. "Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA QR algorithm." *International Journal of Modern Education and Computer Science* 4, no. 6 (2012): 59.
- [11] Chung, Chin-Ho, Wen-Yuan Chen, and Ching-Ming Tu. "Image hidden technique using QR-barcode." In *Intelligent Information Hiding and Multimedia Signal Processing*, 2009. IHH-MSP'09. Fifth International Conference on, pp. 522-525. IEEE, 2009.

[12] Chen, Wen-Yuan, and Jing-Wein Wang. "Nested image steganography scheme using QR-barcode technique." *Optical Engineering* 48, no. 5 (2009): 057004

[13] Gao, Meifeng, and Bing Sun. "Blind watermark algorithm based on QR barcode." In *Foundations of Intelligent Systems*, pp. 457-462. Springer, Berlin, Heidelberg, 2011.

[14] Sharma, Shweta, and Vikas Sejwar. "Implementation of QR Code Based Secure System for Information Sharing Using Matlab." In *Computational Intelligence and Communication Networks (CICN), 2016 8th International Conference on*, pp. 294-297. IEEE, 2016.

[15] K.S.Seethalakshmi, "Use of Visual Cryptography and Neural Networks to Enhance Security in Image Steganography", *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p-ISSN: 2278-8727.