QR CODE STEGANOGRAPHY FUNCTIONAL SPECIFICATION

By Kieran Carroll

C00241073

2021/2022

Y4 Cybercrime & IT Security

Institute of Technology Carlow

Project Supervisor: James Egan

Abstract

The functional specification document is used to specify the central components of a system. This document identifies project scope which includes the central goal, deliverables, assumptions, and risks. The functionality of the tool is outlined and discussed, while the main users and the technologies that will be used are identified. A use-case diagram is provided to illustrate the systems functionality and the user's interactions with the system. Finally, the metrics that will determine the success of the tool are clearly summarized.

Table of Contents

Abstract 1
Introduction 3
Project Scope 3
Goal 3
Deliverables 3
Assumptions 4
Risks 4
System Functionality 4
Users 5
Tools 5
Libraries 6
Languages 6
Operating systems 6
Use Cases 7
Use Case Diagram 7
Use Case Breakdown 8
FURPS 10
Metrics 11

Introduction

The steganography tool will be developed to utilize QR codes, steganography, and cryptography in conjunction to provide a means of secure and secret communication. The application will be developed as a desktop application with a universal target audience. This tool can be used by anyone who has the intention of hiding data or discreetly and securely communicating online. To successfully implement this application the least significant bit method will be used to embed a message entered by the user into a generated QR code, and the advanced encryption standard (AES) will be used to encrypt and decrypt the message. The application will provide a simple graphical user interface (GUI) that will be used to navigate through the various actions available. The generated QR code will be displayed alongside the resulting stego QR code after the embedding process so that the user can perform visual steganalysis by comparing both QR codes to examine for any discrepancies. There are numerous tools online that can perform steganography, but none that I have come across specifically employ the use of QR codes and AES encryption and decryption, thus this functionality alone sets this project apart from the tools available online.

Project Scope

Goal

The central aim of this project is to construct a tool that provides users with the capability of secretly and securely embedding and extracting a message from a QR code. This document outlines the necessary steps required to achieve this goal and exhibits all scopes of the project.

Deliverables

Through the implementation of this tool, I am aiming to:

- Create a desktop application with a GUI that will allow the user to easily navigate through the application and select the functionality they want.
- Allow the user to generate a QR code and use it embed a message.
- Provide security by using AES to encrypt and decrypt the embedded message.
- Test the systems embedding capacity and robustness.

Assumptions

- I will have the time and technical capability to successfully implement all aspects of the project.

Risks

- Time restrictions might not allow the tool to be fully implemented.
- Technical capability could limit the proficiency of the tool.

System Functionality

There are 6 functions that the tool will provide:

1. QR code generation
2. Entering a message & key
3. Embedding the message
4. Extracting the message
5. Encrypting the message
6. Decrypting the message

The primary functionality of the tool is to provide secrecy by enabling users to generate a QR code, embed a message of their choice into the QR code and then extract that message when needed, this is the steganography portion of the tool. The secondary functionality of the tool is to provide security by encrypting the message the user enters, distributing it all over the QR code and then decrypting that message when needed, this is the encryption portion of the tool. The user will open the tool on their desktop and will be presented with a landing window that welcomes them and explains the purpose of the tool. Two buttons will be displayed on the landing window, one that takes them to the embedding widow and another that takes them to the extraction window.

1. Embedding – In the embedding window the user will be able to perform a few actions. 3 textboxes will be presented, one for entering a key, for entering a message to encode and another for a message to embed. Once a user enters a key and the two messages, they will be able to click a button labelled “embed” which will generate a QR code, encrypt the message using the key and embed the payload into the generated QR code. The message entered that will be encoded will allow for all types of characters to be entered as the alphanumeric mode (max characters 4,269) will be used to encode the QR code. As a result

of the number of characters entered the size of the QR code will vary, the max QR code size is 177x177. The algorithm used for encryption and decryption will be the AES algorithm, while the least significant bit method in steganography will be applied to embed and extract the encrypted message. To embed the payload the least significant bits of the error-correction codewords will be modified to successfully embed the message. The resulting QR code that contains the embedded message will then be displayed in the window. The user will be able to be save the QR code in the image file format of their choice to a folder on their PC by clicking a save button.

2. Extracting – From the embedding window or the welcome window, the user will be able to navigate to the extraction window by clicking on a button. In the extraction window the user will be able to click a button that allows them to browse folders on the PC and select an image of a QR code that they want to extract a message from. Once they select a QR code they will then click a button labelled “extract” which will decode the QR code and extract the encrypted message, they will then have to enter in the same key that was used to encrypt the message which will then decrypt the message, thus revealing the secret message.

Users

The user of a system can be defined as the individual who interacts with the system to achieve a certain outcome. There will be two types of users that can interact with the system.

1. The first is a user that intends to encrypt and embed a message into a QR code.
2. The second is a user that intends to extract and decrypt a message from a QR code.

Technologies

Tools

- **Eclipse IDE** – Eclipse is an integrated development environment that is used for developing application in Java and other languages.
- **Window builder** – This is a popular Java GUI designer that is directly built into the Eclipse IDE as a plug-in. It provides an easy-to-use interface that allows for the creation of simple to complex windows. This plugin will be used to create the GUI for the tool.

Libraries

- **ZXing library –** This is an open-source image processing library applied in Java, that has the capability of creating 1D/2D barcodes. In this project it is used for generating and reading QR codes.
- **Bouncy Castle –** A popular java library that provides cryptographic algorithms. Since I will be using AES for encryption and decryption, I will require this library.

Languages

- **Java** – The java language will be used to create the application as I am familiar with the language and some of the libraries and plugins that I can use to develop the desktop application.

Operating systems

- **Windows –** The application will be created on the windows 10 operating system as it is the most popular operating system and is the one that I am most familiar with.

Use Cases

Use Case Diagram

A use case diagram is used to display a high-level overview of the systems functions. The diagram also identifies the various actors and the interactions that they have with the system. The user of the system will be able to enter a message, enter a key, save a QR code and upload a QR code. Through the course of the development of the system some the functions and the order that they are in may be modified.

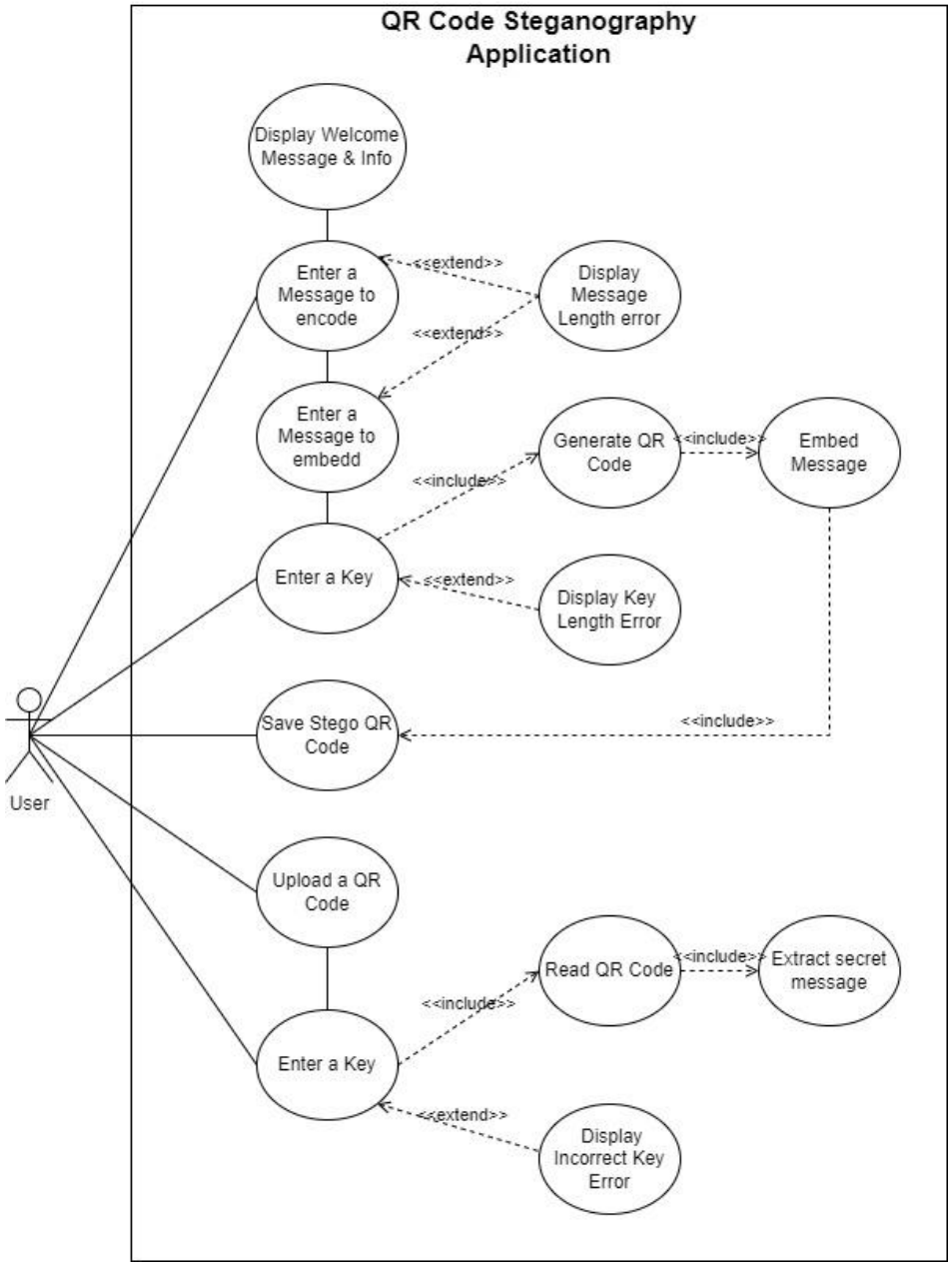

Fig. 1 - Use Case Diagram of the QR Code Steganography Application

Use Case Breakdown

1. Action: Enter a message (to encode & embed)

Actors	User
Preconditions	The user has opened the embedding window in the application.
Steps	• The user launches the application on their desktop. • The user navigates to the embedding window. • The user enters a message of a valid length.
Expected Result	The user can enter a key.

2. Action: Enter a key (embedding window)

Actors	User
Preconditions	The user has opened the embedding window in the application.
Steps	• The user launches the application on their desktop. • The user navigates to the embedding window. • The user enters a key of a valid length.
Expected Result	The user can embed and encrypt a message.

3. Action: Save Stego QR Code

Actors	User
Preconditions	The user has generated a QR code with an embedded encrypted message in the embedding window.
Steps	• The user launches the application on their desktop. • The user navigates to the embedding window. • The user enters a message of a valid length. • The user enters a key of valid length. • The user saves the QR Code to their PC.
Expected Result	A user can save the stego QR code to any folder on their PC.

4. Action: Upload a QR Code

Actors	User
Preconditions	The user has opened the extraction window and has a QR code on their PC that they want to extract a message from.
Steps	• The user launches the application on their desktop. • The user navigates to the extraction window. • The user uploads a QR code.
Expected Result	A QR code is uploaded from the user's PC into the application.

5. **Action: Enter a key (extraction window)**

Actors	User
Preconditions	The user has opened the embedding window in the application.
Steps	• The user launches the application on their desktop. • The user navigates to the extraction window. • The user enters the same key that was used to encrypt the message.
Expected Result	The user can extract and decrypt a message.

FURPS

The FURPS model is used to identify the projects functional and non-functional aspects of a project and outlines the requirements of the project with the client's needs in mind. The initial FURPS model was developed by Robert Gardy and employee of HP. The acronym stands for:

1. Functionality – The central functionality of the tool is to provide a medium for secure and secret data hiding by using steganography, cryptography and QR codes. The user will be able to secretly store data in a QR code by using this tool. The use case diagram displayed in this document fully outlines the core functionality that this tool would provide and displays how a user would interact with the system.

2. Usability – The tool will be user friendly with an interface that is easily navigable. The application will provide an accessible means to embed or extract data from a QR code with no prior knowledge of the steganography or proficient IT skills required.

3. Reliability – The application will not require an internet connection to use therefore it should function as is without consideration of uptime or downtime. Subsequent updates of the application can be issued without harbouring the initial tool. Any errors that could occur would arise from incorrect user input and such an occurrence should result in the user being notified directly with no direct impact of the applications performance.

3. Performance – Traversing through the applications various functions should be fluid and fast. The applications reaction time to user input should be quick and efficient. The application itself will not require a significant amount of resource on the user's device to perform the embedding and extraction functionality. However, its noted that embedding and extracting could take some time to compute although this should not be overly long.

4. Supportability – The application is intended to be developed exclusively as a windows application. Therefore, any user using this operating system will be able to install and use this tool.

Metrics

The project will be considered successful if the following aspects are implemented:

- ✓ A functional desktop application with a simple GUI is provided that allows the user easily to navigate between windows and interact with the system.
- ✓ The user can enter a message of their choice and embed it into a generated QR code.
- ✓ The user can encrypt and decrypt their message using a key of their choice.
- ✓ The ability to save the generated QR code to the user's PC is provided.
- ✓ The ability to upload a QR code from the user's desktop is provided.