UNIVERSITI TEKNOLOGI MARA

SECURING QUICK RESPONSE (QR) CODE USING STEGANOGRAPHY

MUHAMMAD DANIAL BIN MOHD ALWI

BACHELOR OF COMPUTER SCIENCES (HONS.)
DATA COMMUNICATION AND NETWORK

JULY 2021

ACKNOWLEDGEMENT

Foremost, I most thankful to Allah s.w.t for providing me with the good mental and physical to work in completing this final year project report.

I would like to express my sincere appreciation and gratitude to my supervisor, Professor Jasni Mohamad Zain for her patience, insightful comments and unceasing ideas that have helped me at all the times in my research and writing the final year report. Her immense expertise and experience in Security has enable me to successfully finish this report.

I also wish to express my deepest gratitude to my CSP650 lecturer Dr Zolidah Kasiran for guiding and gave helpful information on the completion of the final report. Finally, sincere thanks to my family and my fellow friends that keep supporting and motivating me towards completion of the final year report. May Allah Bless our lives with loved ones.

ABSTRACT

Quick Response (QR) codes are two-dimensional standardized tags that can be utilized to store little amounts of information effectively. In all fields of life, they are increasingly used, particularly with the large distribution of smart phones used as QR code scanners. While there are several benefits to QR codes that make them very common, there are many security problems and risks associated with them. Running malicious code, stealing sensitive information from users, and violating their privacy and identity theft are some typical security risks that a user might face in the background while just reading the QR code in the foreground. This paper implements a security system for QR codes that guarantees security concerns for both users and generators.

In this work, Steganography is implemented in images with a view to improving both images' security and quality. The algorithm used here is LSB (Least Significant Bit). This is one of the most effective ways to hide the message. It allows transfer of messages from one place to another in a secure way. However, retrieval of hiding messages has become possible to the third person in the modern age. The message is stored in the image based on the message storage block. A major issue is the possibility of another person obtaining stored messages as previous methods partially hid them. I have enhancing the QR-code steganography method by using LSB technique in RGB images and QR-code data input image pattern. An LSB method is presented in this paper to hide the message clearly within the secure transfer.

Keywords: Quick Response, QR Code, Security, Steganography, Secure

TABLE OF CONTENTS

CONTENT **PAGE**

CHAPTER 1

INTRODUCTION

1.1. Background of Study

A Quick Response (QR) code are commonly used as a shortcut to the internet resources. QR code has growing faster in the social interaction technology. Nowadays, QR codes can be mostly everywhere such as magazines, mobile application, website, billboards, and others. Usually, a user will use their smartphones camera to directly capture the QR code which directs them to the website. The simplicity of creating and distributing the QR codes has attract many individuals, businesses, and fraudster where the fraudster seeking to direct people to phishing websites. Any company or individual can create QR codes by using simple Web-based generators that encode any text into its unique QR code representation. The non-human readable nature of the QR data has proof for the trust of Web resource being access.

The purpose of steganography is the practice of hiding private and sensitive information from a someone that users do not trusted. Steganography can be performed by converting it bits of useless or bot used data into regular computer files such as graphic, sound, text, and HTML with bits of different of invisible information. The hidden information can be in plain text, cipher text or even images.

In 2017, steganography techniques have been applied to the protection of biometric data. In this project also they stated that steganography can be applied using two approaches which are reversible and irreversible. A reversible technique allows for a full recovery of the original carrier file even when after extortion of the hidden information. Meanwhile, an irreversible