UNIVERSITI TEKNOLOGI MARA

DATA HIDING MOBILE APPLICATION BY USING ENCRYPTION AND DECRYPTION

NUHA BAKIZAH BINTI MOHD ASRI

BACHELOR OF COMPUTER SCIENCE (HONS.) NETCENTRIC COMPUTING

AUGUST 2021

ABSTRACT

The phenomenal growth of e-commerce applications in the World Wide Web requires the need to increase the security of data communications over the Internet, especially for highly sensitive document transfer. The main for this techniques which was encryption and decryption were introduced and developed to provide security to these applications. The importance of data security in today's world cannot be overemphasized. Numerous data security and hiding algorithms have been developed in the last decade. Online attacks have increased to a large extent nowadays and the most common attack among them is data abuse . It is therefore very important that users recognize the fake website and avoid falling prey to it. In this paper, we have proposed a new encryption and decryption system to solve the lack of data hiding problem. Encryption and decryption are used for image-based authentication here. Encode is mainly achieved by changing the message into other code that any third-party will not understand, one with the database of the user and one with the database of the server. And it is only by uploading the image that the original image can be retrieved.

Keywords : Encryption algorithm, Authentication, Decryption.

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, my special thanks goes to my supervisor, Dr. Fakharani Hani bt. Mohd Ali for her constant support and invaluable guidance during this work. I am grateful to her for offering me an opportunity to work under her. This thesis work would not have been possible without her constant help and support.

I would like to thank Dr. Siti Arpah binti Ahmad, my Co-Advisor for her support throughout my course work and for her advising throughout my course of study.

Special appreciation also goes to my beloved parents I would like to dedicate this thesis to my parents who are the first teachers of my life. Without their encouragement, love and support, I would not have been able to reach this stage of my life. I am forever indebted to them for the sacrifices they made to help to achieve this success.

TABLE OF CONTENTS

CONTENT **PAGE**

CHAPTER 1

INTRODUCTION

In the presence of third parties, cryptography(Buchanan, 2017) is the favored method for safe communication. It is about building and evaluating protocols that transcend the adversary's control and that apply to different aspects of information security, such as confidentiality of data, honesty of data, authentication and non-repudiation. This technique has many applications in computer science and other related fields: used to secure e-mail addresses, information on credit cards, corporate data, etc.

Nowadays, thanks to the stunningly fast advancement of the computer and network technology, people can easily send or receive secret information in various forms to or from almost any remotest part of the world through the Internet within seconds. In fact, at this specific point of time, there may be loads of classified information distributed and shared on the Internet. However, huge secret messages will run a high risk of leaking out when they are transmitted or shared through any public communication channel. A significant area of study, therefore, is how to achieve secure secret communication. All the social networking websites are threatened by the cyber criminals, who attack the social networking platform and breach the privacy of the users(Milton Joe & Ramakrishan, 2018).

In its purest form cryptography is a mathematical panacea of wonder and excitement(Dougherty, 2016). For as long as the calculations to reverse the cryptographic algorithm take longer than the valuable lifetime of the data it protects, it may be considered secure(Dougherty, 2016). Traditionally, a private message can be encrypted into any ciphertext by using a cryptographic technique such as DES or RSA, which seems entirely pointless before it is sent out through the network. Although modern cryptographic systems provide the secret information transmitted and shared on the network with a reasonably high degree of protection, the presence of secret information as ciphertexts easily attracts the attention of hackers as if it