UNIVERSITI TEKNOLOGI MARA

IMAGE ENCRYPTION AND DECRYPTION USING 3D-AES BLOCK CIPHER ALGORITHM

ENGKU MARYAM SYAHDINA BINTI ENGKU SAFRUDDIN

Thesis submitted in fulfilment of the requirement for Bachelor Of Computer Science (Hons.) Multimedia Computing

Faculty of Computer and Mathematical Sciences

January 2018

ACKNOWLEDGEMENT

In the name of Allah, The Most Gracious and The Most Merciful

First of all, I would like to express my gratitude to Allah S.W.T, The Almighty for giving me strength and patients in completing this project in the given time. A special thanks to my dedicated supervisor, Dr Suriyani binti Ariffin for her guidance and recommendations from the beginning until the end of this project. All her kindness for helping me in many ways during this research will not be forgotten. All the moral support given throughput the completion of this thesis and all the guidelines she taught.

I owe my loving thanks to my parents who have been my supporter and listener through ups and down throughput completing this project. Without their encouragement and wise advices, it would have been impossible for me to finish my thesis. Lastly, I offer my regard and blessings to all those who supported me in any aspects during the completion of the project.

Thank you

ABSTRACT

Cryptography is the way of storing and transmitting data by convert the information into unreadable cipher for security which only intended sender and receiver only could access. The transformation of original data to cipher data is called encryption, while the reverse is called decryption. The basic advanced encryption standard is still not satisfying to achieve the security goals. Whether the key is not so strong or the time needed for processing is slow. In order to ensure the image data is secure/ protected and encryption time is low, it is very timely to conduct a research on image encryption and decryption using 3D-AES block cipher algorithm. The aim of this study were to conduct a research on how to identify the implementation of security analysis of image using 3D-AES block cipher algorithm. Subsequent to this, this project focus on how to measure the security analysis on randomness test of image. The result of this project is the characteristics of 3D-AES is very high in security and this algorithm is resistance to all identified attacks, the system effectiveness and accuracies of the process. Testing algorithm will compute number of bit errors and bit error rate by comparing encryption and decryption. Total average for bit error rate of 30 images is 0.59233. Average above 0.5 prove that the level of security encryption and decryption is very high and secure.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Project Background

Nowadays, images are generated in many fields, such as in military, government sector and many more. Data security is widely used to ensure the level of security of image information transmission in networks. It is becomes the main role in daily communication through networks (Padate & Patel,2014).

Various techniques of encryption have been developed to make sure the data integrity which the information cannot be altered by the attacker and to improve the speed of encryption and decryption speed. Confidential image data must be protect from being accessed using different technique.

Unfortunately, not all encryption and decryption technique could implemented and compatible with different format and different size of image. According to Chai (2016), to avoid transmission increasing, the size of the convert data cannot be larger size than the original data.

Gujar (2014) said that the requirements to achieve is secrecy, integrity and non-reproduction of exchanged information has made the transmission data through networks become the most important thing to have in communication channel.

According to my reading through related articles and searching the information through internet, there is no such image encryption and decryption using 3D-Aes block cipher algorithm is yet been discovered by anybody. Meantime, I found one article written by Ariffin (2013) about SMS encryption using 3D-AES block cipher algorithm. She had made a test on 3D-AES performance and the result from her research is satisfying. It show that the 3D-Aes has low encryption time when using a big data.