[LIGHT IMAGE ENCRYPTION]

[SYAFI BIN ABD RAZAK]

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: [LIGHT IMAGE ENCRYPTION]

SESI PENGAJIAN: [SESI 2020/2023]

Saya: SYAFI BIN ABD RAZAK

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

( )	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
( )	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
(✓)	TIDAK TERHAD	

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

(TANDATANGAN PELAJAR)

Alamat tetap: NO 8 JALAN EH 19,
TAMAN EVERGREEN HEIGHTS,
83000, BATU PAHAT, JOHOR.

Tarikh: 20.09.2023

(TANDATANGAN PENYELIA)

PM Dr. Nur Azman Abu
Faculty of ICT,
Universiti Teknikal Malaysia Melaka

(NUR AZMAN ABU)

Tarikh: 21.09.2023

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

[LIGHT IMAGE ENCRYPTION]

[SYAFI BIN ABD RAZAK]

This report is submitted in partial fulfillment of the requirements for the Bachelor of [Computer Science (Software Development)] with Honours.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[YEAR OF SUBMISSION]

DECLARATION

I hereby declare that this project report entitled

[LIGHT IMAGE ENCRYPTION]

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : _____ Date : 20.09.2023

([SYAFI BIN ABD RAZAK])

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
UTeM
اونيۏرسيتي تيکنيکل ملسيا ملاک

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of [Computer Science (Software Development)] with Honours.

SUPERVISOR : _____ Date : 21.09.2023

([NUR AZMAN ABU])

PM Dr. Nur Azman Abu
Faculty of ICT,
Universiti Teknikal Malaysia Melaka

DEDICATION

As a tribute to my numerous friends and family members, I am writing my dissertation. To my beloved parents, who have consistently encouraged and motivated me in everything. My gracious managers, thank you for always giving me those brilliant ideas and priceless time to help me finish this year's final project. My friends, who have always encouraged me and provided me with sage advice. I'm grateful. My affection for each of you cannot be quantified in any manner. God's favor be with you.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ACKNOWLEDGEMENTS

I would like to start by expressing my sincere thanks to my supervisor, Pm Dr Nur Azman Bin Abu, who has been my pillar of support and mentor throughout the completion of my thesis. His tolerance and understanding were a huge assistance to me while I worked on this thesis; without them, I would not have been able to finish it. I also want to express my gratitude to my assessor, Dr. Shekh Faisal Bin Abdul Latip, for his evaluation of me and his candid criticism of my research.

Next, I should thank and praise Allah for allowing me to successfully complete this thesis without encountering any mental or physical issues. I'm appreciative of the strength and excitement you've always provided me with so I can finish this thesis.

I also want to express my gratitude to my family, especially my parents Abd Razak Bin Hussin and Misnah Binti Ponamin, for their unfailing support and for giving me the time and space I needed to complete my thesis.

In closing, I want to thank everyone who has supported and encouraged me, especially my friends and fellow students. Because of their enthusiasm to share their knowledge and help, I am more motivated to successfully finish this thesis. By doing so, I would also want to show my thanks to everyone who has ever been into my life because they are all there to teach us something.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ABSTRACT

Light image encryption is one of the encryption techniques that are designed to safeguard digital images efficiently and effectively in environments with constrained resources, such as embedded systems and mobile devices. Since these techniques are tuned for low computational and memory demands, they are perfect for use on devices with limited processing power and storage. Light image encryption techniques typically employ asymmetric key encryption methods, which employ the same key for encryption and decoding. They are designed to provide a high level of security while reducing the computational and memory requirements of the encryption and decryption procedures. Compression techniques are frequently used in conjunction with light image encryption techniques to minimize the size of the image data prior to encryption. The encryption and decryption methods' computational and memory needs can be further decreased as a result, increasing their viability for use in contexts with limited resources. This admittedly document attempts to propose, as concretely as possible, a light image encryption algorithm that is implemented for security. This algorithm offers encryption that will encrypt certain data of an image using AES algorithm. It can be useful in situations where the photographer wants to show pictures of his work to the client before selling the pictures.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ABSTRAK

Penyulitan imej ringan ialah salah satu teknik penyulitan yang direka untuk melindungi imej digital dengan cekap dan berkesan dalam persekitaran dengan sumber terhad, seperti sistem terbenam dan peranti mudah alih. Memandangkan teknik ini ditala untuk permintaan pengiraan dan memori yang rendah, ia sesuai untuk digunakan pada peranti dengan kuasa pemprosesan dan storan terhad. Teknik penyulitan imej ringan biasanya menggunakan kaedah penyulitan kunci asimetri, yang menggunakan kunci yang sama untuk penyulitan dan penyahkodan. Ia direka untuk menyediakan tahap keselamatan yang tinggi sambil mengurangkan keperluan pengiraan dan ingatan bagi prosedur penyulitan dan penyahsulitan. Teknik pemampatan kerap digunakan bersama-sama dengan teknik penyulitan imej ringan untuk meminimumkan saiz data imej sebelum penyulitan. Keperluan pengiraan dan memori kaedah penyulitan dan penyahsulitan boleh dikurangkan lagi akibatnya, meningkatkan daya majunya untuk digunakan dalam konteks dengan sumber terhad. Dokumen ini diakui cuba untuk mencadangkan, sekonkret yang mungkin, algoritma penyulitan imej ringan yang dilaksanakan untuk keselamatan. Algoritma ini menawarkan penyulitan yang akan menyulitkan data tertentu imej menggunakan algoritma AES. Ia boleh berguna dalam situasi di mana jurugambar ingin menunjukkan gambar hasil kerjanya kepada pelanggan sebelum menjual gambar tersebut.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

TABLE OF CONTENTS

PAGE

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF TABLES

PAGE

UTeM
اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF FIGURES

PAGE

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF ABBREVIATIONS

AES	**-**	**Advanced Encryption Standard**
ABE	**-**	**Absolute Error**
MSE	**-**	**Mean Square Error**
SSIM	**-**	**Structural Similarity Index Measurement**
PSNR	**-**	**Peak Signal to Noise Ratio**
DCT	**-**	**Discrete Cosine Transform**
DWT	**-**	**Discrete Wavelet Transform**

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF ATTACHMENTS

Page

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 1: INTRODUCTION

1.1 Introduction

With the rapid development and popularization of computer-network and multimedia technology, the protection of digital images is an essential requirement for safeguarding the confidentiality and privacy of people in general. Due to widespread use of multimedia data and despite widespread threats and attacks in communication systems, security of this data is necessary. Multimedia encryption challenges originate from two realities.

Although classic cryptography provides better encryption and decryption algorithms for one-dimensional data streams, the special properties of digital images, including large data volume, high redundancy, and strong correlation, between adjacent pixels make traditional block ciphers less efficient when processing image data. Therefore, a light image encryption algorithm is introduced. The image information encryption scheme based on chaos uses the random noise characteristics of a chaotic time series to encrypt the image data. Its main operational steps include image pixel diffusion and pixel position confusion. An efficient pixel-level image encryption algorithm was presented, which enhanced the connection between position shuffling of pixels and the changes to gray values as compared to the traditional permutation-diffusion architecture (Ye et al, 2018)

Meanwhile, to address the insensitivity of traditional permutation and diffusion operations to pure image changes, a light bit-level confusion and cascade cross circular diffusion was proposed, which diffuses a small change in the plane image to the whole image with fewer rounds to enhance the security of the cryptographic system and reduce computational redundancy in the traditional architecture (Zhang et al, 2012)

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

This light image encryption algorithm was not to fully encrypt the image but to encrypt some of the data of the image so that people can still see the image but in lower quality. This will help us to prevent unauthorized use of the image.

1.2 Project Problem Statement

Nowadays, many existing light image encryption algorithms fully encrypt the image so that people do not see the real image unless the image is decrypted. The main reason behind this is due to unauthorized use of the image for own purposes without paying to the owner of the image. The conventional encryption algorithm is inadequate for encryption and has a high computational cost. Asymmetric encryption algorithms demand more complex calculations than symmetric encryption algorithms, which represent the image as a vector of real values. The vector is rather long due to the high sampling coefficients of the image.

Image encryption is a heavy processing. It is a challenge to use it on a regular basis. Light image encryption has the capability to encrypt the image in short time and require less computational capacity.

The summary of problem statement for this research is shown at table 1.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Table 1.1 Summary of Problem Statement

PS	Problem Statement
PS1	Traditional encryption algorithm is computationally demanding.
PS2	Existing light image encryption algorithm will fully encrypt an image without any pre display.
PS3	Current light image encryption algorithm encrypts all data without distinguishing their quality contribution to an image.

1.3 Research Question

The research question for this project was derived from the problem statement in Para 1.2. The summary of research question as shown in Table 1.2

Table 1.2 Summary of Research Questions

Research Problem	Research Question
1.	How to encrypt only a certain data of the image?
2.	What is the light image encryption used to encrypt a certain data of the image?

1.4 Research Objective

Based on the Research Problem as in Para 1.1 and Research Question in Para 1.2, the objective in the project as derived in Table 1.3

Table 1.3 Summary of Research Objective

Research Problem	Research Question	Research Objective
1.	How to encrypt only a certain data of the image?	i. To thoroughly study and gain a comprehensive understanding of the present situation and progress in the field of light image encryption. ii. To propose a light image encryption algorithm that only encrypt a certain quality data of the image, for security purposes.
2.	What is the light image encryption used to encrypt a certain data of the image?	i. To evaluate the effectiveness of light image encryption algorithm that has low computational requirements

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.5 Project Scope

The scopes of this project are:

i. This project will ensure the algorithm works with various image formats and the image should be visible to people while some of the image data is encrypted.

ii. The light image encryption algorithm will be developed specifically tailored for images that is computationally efficient and does not add significant overhead to the image data.

iii. This project will evaluate the performance of the encryption algorithm, based on metrics such as ABE, PSNR, SSIM and MSE of the encrypted image.

1.6 Project Contribution

This project is important for any organization that wants to prevent unauthorized use of the image. This project also can be used or improved by any research to establish a good light image encryption algorithm that does not fully encrypt the image using different methods. The benefits of this project are providing high security while minimizing computational overhead which is also encrypting some of the image data to ensure that the image will not be used without the owner's consent.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.7 Summary of Chapter

Chapter 1: Introduction

This chapter discuss about introduction of the project and project background. In this chapter also include problem statement, research question, research objectives, scopes, project contribution, summary of chapter and conclusion.

Chapter 2: Literature Review

This chapter includes reviews of terminology relating to the project issue based on related studies, a critical analysis of present challenges, and potential remedies.

Chapter 3: Project Methodology

This chapter explains the flow or approach needed to complete this project, as well as how the analysis is developed.

Chapter 4: Analysis and Design

This chapter covers the project's design, including logical and physical design, system architecture, and any other designs relevant to the project.

Chapter 5: Implementation

This chapter describes the project's execution in depth, including how the project is carried out and how the final product is generated.

Chapter 6: Testing and Analysis

This chapter deals with the project's testing and validation on the dataset in order to acquire the outcome. This chapter will also provide a general overview of the findings and their outcomes.

Chapter 7: Project Conclusion

The project's end and debate are addressed in the last chapter. This chapter will also include a summary of the conclusion.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.8 Conclusion

As a conclusion in chapter 1, the purpose of this chapter is to focus on project introduction and project background to discuss about problem statement, research question, research objectives, scopes of the project, project contribution, summary, and conclusion. This project is built to develop a light image encryption algorithm that will only encrypt certain data of the image.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Based on the previous studies, the research has been assessed and analyzed into the current project. The main element in this project is developing a light image encryption that only encrypts certain data of the image. The algorithm used for light image encryption is the AES algorithm. The main concept is to only encrypt a certain image's data so that people still can see the image. Therefore, this chapter provides an overview of light image encryption, its core technologies, and its different types. Furthermore, this chapter will highlight some critical reviews of existing works and their proposed solution.

2.2 Digital Images

A digital image is a two-dimensional (2D) vector that contains pixels whose values are between 0 and 255. An image can be represented by any geometric shapes (circles/curves/lines) using these numbers. According to Youssef Elbably (2022), digital images are images that use pixels. Pixels are a finite number for digital image's unit of measurement which any computer can understand.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2.3 2-D Image Representation

A digital image is essentially a form of image made up of pixels. Each pixel is placed in a rectangle pattern and has a finite size and finite intensity to display the image. The four different approaches to representing digital images are pixel-based representation, block-based representation, region-based representations, and hierarchical representations (Youssef Elbably, 2022).

1. Pixel-Based Representation

A digital image that is made up of a grid of individual pixels, each of which represents a different color or shade, is referred to as pixel-based representation, also

known as raster graphics. It is frequently used for digital pictures, scanned images, and computer-generated graphics. It is ideal for depicting intricate patterns, natural settings, and other complex images with precise detail.

2. Block-Based Representation

Digital photos and films are divided into smaller rectangular blocks and then represented using the block-based representation technique. The image or video is then more effectively represented once these blocks have been compressed using techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform. Common image and video compression formats like JPEG and MPEG use block-based representation. Several computer vision applications, including object detection, tracking, and recognition, have also employed it.

3. Region-Based Representation

A way of displaying an image by breaking it up into different regions or segments, each of which represents a different object or portion of the image, is known as region-based representation. Applications for computer vision and image processing frequently employ this kind of representation. When performing tasks like object identification, where the objective is to recognize and localize certain items inside an image, region-based representation is especially helpful.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

4. Hierarchical-Based Representation

The phrase "hierarchical-based representation in images" refers to the use of many levels of abstraction to depict a picture. It requires segmenting an image into several progressively smaller and simpler sub-regions or features, each of which captures a unique portion of the image. This technique has been heavily employed in applications for computer vision and image processing, such as object detection, picture segmentation, and image classification.

2.4 Light Image Encryption

Light image encryption is the process of encrypting digital photos with methods that are designed to be computationally efficient and use comparatively few computer resources. Light image encryption uses the fewest amount of computer resources and memory possible to safeguard the confidentiality and integrity of the image data. According to Manish Gupta et al. (2020), light image encryption is a less complex algorithm that uses 64-bit block cipher and 64-bit key for image encryption, which requires a smaller number of rounds and memory. Light image encryption also contains less memory for the code size. Light image encryption uses 64-bit plain text and requires an 80-bit key to encrypt the image.

Many techniques are used for light image encryption, including symmetric key encryption algorithms that use the same key for both encryption and decryption. These methods can provide a high level of security while reducing the computational and memory requirements of the encryption and decryption procedures. One approach to light image encryption is based on cipher stream that is used by Saeed Bahrami et al, (2012) in his research. Stream ciphers are built using a pseudorandom key sequence that is used to encrypt image data.

اونيۏرسيتي تيکنيکل ملسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Another approach is used by Rupesh Kumar Sinha et al (2020), which the encryption is based on Rubik's Cube algorithm. In Rubik's Cube algorithm, the original image is scrambled using two secret keys that were generated using logistic function and shift register method. After that, with XOR operator, rows and columns of the scrambled image are again mixed using various means.

Finally, chaotic based is used for light image encryption by Jannatul Ferdush et al. (2021). Based on Jannatul Ferdush et al., the chaotic map is an evolution function that displays the chaotic behavior in terms of continuous-time or discrete-time parameters. First, the Arnold map is applied to the raw image. Then, the parameters for the logistic map are selected. The image decryption is performed in a reverse way.