

SECURING IRIS AUTHENTICATION USING STEGANOGRAPHY



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS

JUDUL: SECURING IRIS AUTHENTICATION USING STEGANOGRAPHY

SESI PENGAJIAN: 2016/2017

Saya NUR LIYANA NADHIRAH BINTI MOHD SABRI mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.

Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.

Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.

** 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 PENULIS)

(TANDATANGAN PENYELIA)

Alamat tetap Lot 144, Kg. Gong
Dermin, Binjai, 16150
Kota Bharu, Kelantan.

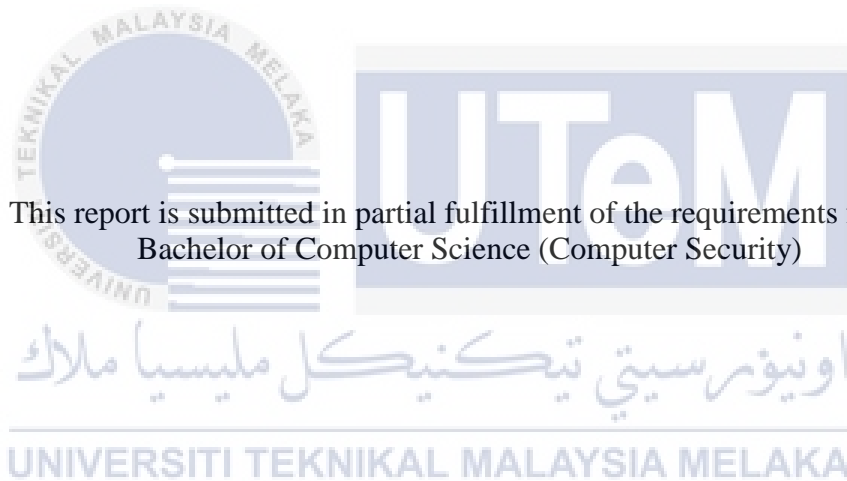
DR. ZAHEERA BT ZAINAL ABIDIN
NAMA PENYELIA

Tarikh:

Tarikh:

SECURING IRIS AUTHENTICATION USING STEGANOGRAPHY

NUR LIYANA NADHIRAH BINTI MOHD SABRI



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2017

DECLARATION

I hereby declare this project entitled
SECURING IRIS AUTHENTICITATION USING STEGANOGRAPHY



Is written by me and is my own effort and there is no part has been plagiarized without citations

STUDENT:

DATE:

(NUR LIYANA NADHIRAH BT MOHD SABRI)

SUPERVISOR:

DATE:

(DR. ZAHEERA BT ZAINAL ABIDIN)

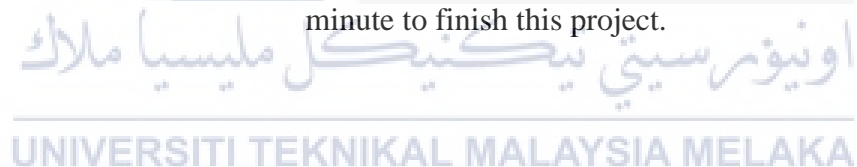
DEDICATION

To my parents, siblings and family, thank you for supporting and love all this time.

To my supervisor, who always help me when in needs and give me guide alongside to finish this project.

To my friends who always cause me trouble, distraction, annoy each other, fight together, jaywalking, and daydream but at the same time help and assist me in finishing this project.

Lastly, to my secret helper, thank you so much for providing me a helping hand at last minute to finish this project.



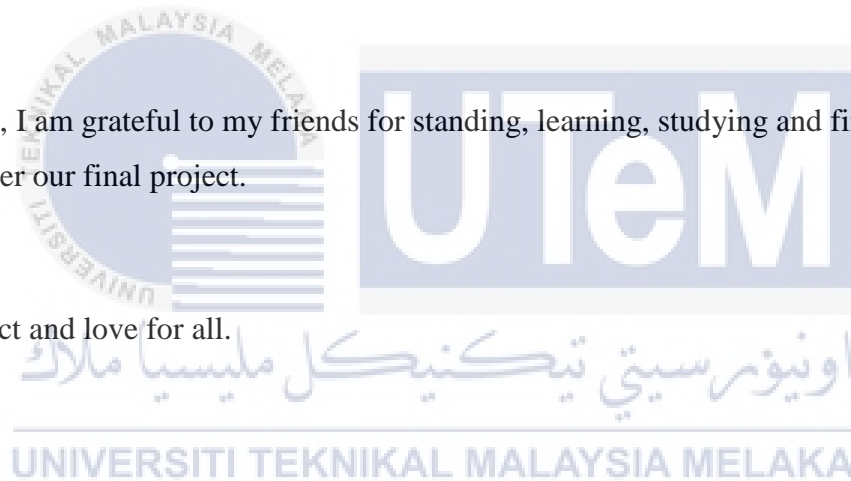
ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor. Dr. Zaheera Bt Zainal Abidin for her advice and support in guiding me throughout the project.

For my family, I would like to say thank you for the greatest support and all sort of love, guidance, respect and advices throughout my years spending and studying in this university.

Lastly, I am grateful to my friends for standing, learning, studying and finishing together our final project.

Respect and love for all.



ABSTRACT

In biometrics security, steganography is highly used for securing biometric data template from unauthorized user at the access control level system. The word steganography in Greek means covered writing and hiding the existence of the message from unauthorized person that indicated the science of secret communication. However, hacking activities still occurred at the biometric point system such as overriding biometric template in database. Therefore, several countermeasures have been review to overcome the hacking activities from happening. Studies on steganography techniques have been identified by viewing on a modification of Least Significant Bits (LSB). The LSB is proposed to iris image which converts hidden images or messages to binary stream and hides into a proper lower bit plane. For hiding secret information, the basic idea is to replace the LSB of the cover image with the bits of the messages to be hidden without destroying the property of the cover image. The LSB-based technique is the most challenging as it is difficult to differentiate between the cover-object and stego-object even though few LSB bits of the cover object are replaced. In addition, LSB used a stego-key while embedding messages inside the cover image. When the cover images are transmitted through transmission channel, white noise is applied to stego images, that reduces the number of bits and also hidden secret data bits which are affected by that auto created noise. By using the key and white noise application, the chance of getting attacked by the attacker is reduced and the embedded information to be transmitted to destination without being detected by the attacker. The experiment shows that the LSB produces a low error rate as few bits are changed, that is 0.0059dB. On the other hand, LSB can be easily combined with other method due to its flexibility feature. The parameters used in the experiments are peak of signal to noise ratio (PSNR) and mean squared error (MSE). Finding has shown a better results of high noise rate compared to before the embedding process. As a conclusion, the study of the project brings a successful outcome and significantly brings impact of higher security towards steganography field and biometrics applications.

TABLE OF CONTENT

CHAPTER	SUBJECT	PAGE
	DECLARATION	i
	DEDICATION	ii
	ACKNOWLEDGEMENT	iii
	ABSTRACT	iv
	TABLE OF CONTENTS	v
	LIST OF TABLES	ix
	LIST OF FIGURES	x
CHAPTER 1	INTRODUCTION	
	1.1 Introduction	1
	1.2 Problem Statement	2
	1.3 Project Question	3
	1.4 Project Objective	4
	1.5 Project Scope	4
	1.6 Project Contribution	5
	1.7 Thesis Organization	6
	1.8 Conclusion	6
CHAPTER II	LITERATURE REVIEW	
	2.1 Introduction	7
	2.1.1 Steganography	7
	2.1.2 Iris Recognition	8
	2.1.2.1 Characteristics of Biometric Technologies	8
	2.2 Related Work	9
	2.2.1 Noise Effect on Image Authentication	11
	2.3 Critical Review of Current Problem	12

2.4 Proposed Solution	13
2.4.1 Steganography	13
2.4.2 Biometric System	14
2.5 Conclusion	15
CHAPTER III METHODOLOGY	
3.1 Introduction	16
3.2 Least Significant Bit (LSB) Technique	16
3.2.1 Data Embedding	17
3.2.2 Data Extraction	18
3.2.3 Image Encoding Algorithm	19
3.3 Extraction of Hidden Message	19
3.3.1 Message Extraction Algorithm	19
3.4 Iris Authentication	20
3.4.1 Iris Authentication Extraction	20
3.5 Project Milestone	22
3.6 Conclusion	24
CHAPTER IV ANALYSIS AND DESIGN	
4.1 Introduction	25
4.2 Problem Analysis	25
4.3 Performance Analysis	26
4.4 Evaluating on Steganography Technique	27
4.5 Exaggerate on LSB Technique for Color Image	27
4.5.1 Existing LSB Method for Color Image	29
4.5.1.1 8 Bit color Image	29
4.5.1.2 24 Bit color Image	29
4.6 Proposed Approach Architecture	30
4.6.1 Enrollment Process	31
4.6.2 Recognition Process	32
4.7 Conclusion	33
CHAPTER V IMPLEMENTATION	
5.1 Introduction	34

5.2 Software Development Environment Setup	34
5.3 Software Configuration Management	36
5.3.1 Encoding Process	36
5.4 Implementation Status	38
5.4.1 Data Hiding in Iris Template	38
5.4.2 Hiding Iris Code in Digital Image	39
5.5 Expected Result	41
5.6 Conclusion	44
CHAPTER VI	
6.1 Introduction	45
6.2 Test Plan	45
6.2.1 Test Organization	45
6.2.2 Test Environment	46
6.2.3 Test Schedule	46
6.3 Test Strategy	46
6.4 Test Description	47
6.5 Result and Analysis	47
6.5.1 Data Hiding and Image Hiding Simulation	47
6.5.2 Recognition in Database System (Demo Version)	51
6.5.3 Analysis based on PSNR and MSE value	52
6.5.3.1 Brief Summary of Least Significant Bit with Noise (LSB + Noise)	53
6.5.3.2 Brief Summary of Most Significant Bit (MSB)	53
6.5.3.3 Brief Summary of Discrete Cosine Transform (DCT)	54
6.5.2.3 Brief Summary of Discrete Wavelength Transform (DWT)	55
6.6 Analysis and Comparison of LSB Method and Other Methods	55

	6.6.1 The Comparison Graph of Proposed Method and Others Method	56
	6.7 Conclusion	58
CHAPTER VII	7.1 Introduction	59
	7.2 Project Summarization	59
	7.3 Project Contribution	60
	7.4 Project Limitation	60
	7.5 Future Works	60
	7.6 Conclusion	60
	REFERENCES	62
	APPENDIX	64



LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Summary of Problem Statement	3
1.2	Summary of Project Question	4
1.3	Summary of Project Objective	4
1.4	Summary of Project Contribution	5
2.1	Milestones of Project	22
5.1	Comparison of SNR, MSE and PSNR	38
5.2	Actual Least Significant of Random Color Component Bits	40
5.3	Changed Least Significant of Random Color Component Bits	41
6.1	Comparison of PSNR and MSE Value	55
6.2	Graph Comparison for Proposed Method and Others Method	57

LIST OF FIGURES

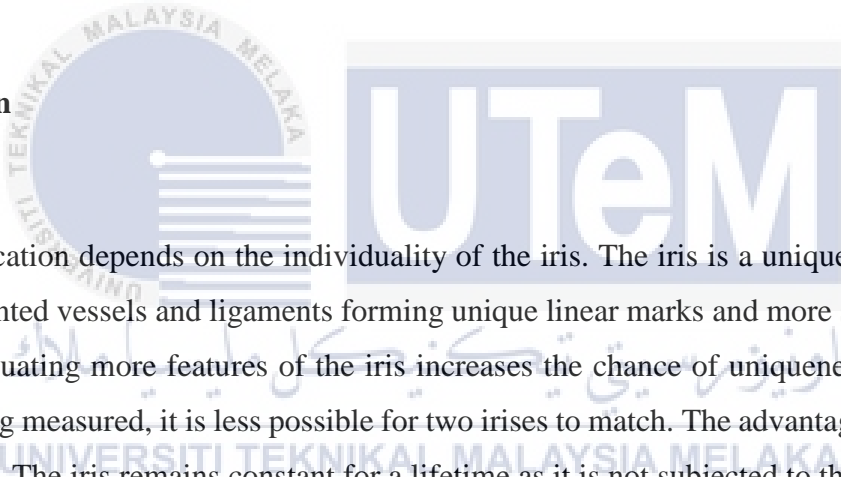
FIGURE	TITLE	PAGE
2.1	Front View of The Human Iris	9
2.2	Steganography Method Uses in Proposed Approach	14
3.1	Iris Authentication Extraction	20
3.2	Hamming Distance Equation	21
3.3	LSB Used in Biometric System	22
4.1	Image Steganography Using LSB Approach	26
4.2	Formula of MSE and PSNR	26
4.3	Proposed Approach for Iris Template Using Steganography	31
5.1	Hiding Data in Iris Template	35
5.2	Secret Message Embedded into Cover Image	36
5.3	Formula of MSE and PSNR	38
5.4	LSB Steganography Used in Proposed Approach	39
5.5	Iris Code to Be Hide (with data hiding)	41
5.6	Cover Image	41
5.7	Stego Image After Hiding Process	42
5.8	Noise Image (error image auto created between cover image and iris template in producing stego image)	42
5.9	Recovered Iris Code from Stego Image	43
5.10	Recovered Message from Stego Image	43
6.1	Flowchart on how the simulation work using MATLAB	47
6.2	MATLAB Terminal Command	48
6.3	Right Click and Evaluate Selection	48
6.4	Data Hiding in an iriscode image	48
6.5	Iriscode With Data Hiding Embedded Within Cover Image Produce a Stego Image	49

6.6	Noise Image (error image auto created between cover image and iris template in producing stego image)	49
6.7	Recovered Iris Code from Stego Image	50
6.8	Recovered Message from Stego Image	50
6.9	SNR, PSNR and MSE value produced	51
6.10	Interface Menu of Database	52
6.11	Cover Image added into Database	52
6.12	Iris Recognition in Database	52
6.13	The Difference Between LSB and MSB	54
6.14	Formula of DCT	55
6.15	A General Formula of DWT	55
6.16	LSB Graph Reading	57
6.17	LSB + Noise Graph Reading	57
6.18	LSB Graph Reading	57
6.19	MSB Graph Reading	57
6.20	LSB Graph Reading	58
6.21	DCT Graph Reading	58
6.22	LSB Graph Reading	58
6.23	DWT Graph Reading	58

CHAPTER 1

INTRODUCTION

1.0 Introduction



Iris authentication depends on the individuality of the iris. The iris is a unique trait, which is composed of pigmented vessels and ligaments forming unique linear marks and more similar features and marks. Evaluating more features of the iris increases the chance of uniqueness. Since more features are being measured, it is less possible for two irises to match. The advantages of using the iris is its stability. The iris remains constant for a lifetime as it is not subjected to the environment, as it is protected by the cornea and aqueous humor. Iris recognition is widely used for security purposes. It provides perfect security because of its ability to eagerly recognize error irises. Iris recognition will be a possible option for any security system in the future. The iris is a circular diaphragm, lies in between the cornea and the lens of our eye. The iris is perforated close to its center by a circular hole known as the pupil. The function of the iris is to manage the quantity of light entering in the pupil, and this is done by the sphincter and the dilators muscle, which adjust the volume of the pupil. The average diameter of the iris is 12.1 mm, and the pupil size can vary from 11% to 81% of the iris diameter. The retina is a thin film of cells at back of the eyeball. The blood vessels of a person's retina also provide a unique pattern. Iris recognition provides the highest precision in recognizing human, because no two irises are same- even not between twins, or even among the left and right eye of the person. The pattern of one's iris is fully formed by

eleven months of age and remains the similar till death. Iris technology is correct because it uses more than 241 points of reference, in iris pattern, as a basis for match.

Meanwhile, an image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap. An image map is a file containing information that associates different locations on a specified image with hypertext links. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element). Greyscale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit les and use the RGB color model, also known as true color. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color is represented by 8 bits. Thus, in one given pixel, there can be 256 different quantities of red, green and blue.

1.2 Problem Statement

Biometrics work well only if the verifier can verify two things, the biometric came from the genuine person at the time of verification and the biometric matches the master biometric on file. However, a variety of problems hinder the ability to verify the above things such as:

- i. Noise in acquired data – Noisy biometric data caused by defective sensors, defective physical characteristics and unfavorable ambient conditions. This causes the data to be incorrectly matched or incorrectly rejected.
- ii. Intra-class variations – The data acquired during authentication may be different from the data used to generate the template during enrollment, affecting the matching process.
- iii. Distinctiveness – Every biometric trait has an upper bound in terms of its discrimination capabilities.
- iv. Non-universality – A subset of the users not possessing a particular biometric.

The above-mentioned problems form the basis for many types of attacks against biometric systems. One of many problem mentioned above, the most common problem is overriding

biometric template in database. Besides that, the copyright crime is a serious issue been mentioned nowadays and hacking activities that interrupted main point of system security. Thus, may be lead to causes biometric system become insecure and vulnerability to those who use it.

PS	Problem Statement
PS1	Copyright stealing is a common issue nowadays
PS2	Overriding biometric template in database
PS3	Hacking activities that interrupted main point of system security

Table 1.1: Summary of Problem Statement

1.3 Project Question

In modern era data is heavily gaining importance as information is dependent on the raw facts for example data. The exchange of information is required to share resources among the distributed users which may be separated by locations. While transferring the data among the users the confidentiality and privacy should be maintained. To meet these requirements the technique Steganography can be used. In this technique we use different mediums to hide the data that are text, images, audio, video and etc.

From the perspective of this project, how can we secure data information to be delivered to a safe destination without being attacked by others? Therefore, the digitally shared data between the users should be converted to some unreadable format which will not be tampered by the intruders. Steganography approach used in this project secure the biometric system and prevent hacker from gaining a data information in the iris database.

PS	PQ	Project Question
PS1	PQ1	How can we secure data information to be delivered to a safe destination without being attacked by others?
PS2	PQ2	How can steganography technique avoid the overriding template in database?
PS3	PQ3	How can proposed project being used to prevent hacking activities?

Table 1.2: Summary of Project Question

1.4 Project Objective

The objective of this project is to compare and enhanced common security features offers by devices. Also to improve the security technology include in access account by user and to find the efficiency in using iris recognition as security feature. However, this project is believed to achieve the following objective:

PS	PQ	PO	Problem Objective
PS	PQ	PO1	To propose a modification of the existing LSB approach.
		PO2	To securing the secret information within the image file using LSB approach.
		PO3	To evaluate the proposed approach with the LSB approach.

Table 1 3: Summary of Project Objective

1.5 Project Scope

This project focus mainly on securing iris authentication using steganography. The scope involve the technique, method and system used to perform the development of this project such as:

- i. Existing Iris template: To hide secret data.
- ii. Cover image: To hide iris template.
- iii. Stego-image: Produced after perform the hiding data in MATLAB.

- iv. MATLAB: To perform simulation of encoding, decoding and Least Significant Bit (LSB) technique.

1.6 Project Contribution

There is no security system that is completely foolproof. Every system is breakable with an appropriate amount of time and money. Therefore, an innovation on securing the iris authentication needs to produce. The approach of securing iris is designed with the integration of steganography into the biometric system. The importance of steganography has been apprehended against cryptography and information hiding due to capabilities, security services and performance. Steganography is emphasis on avoiding detection and possibilities of largest hidden message meanwhile watermarking is robust, emphasis on avoiding distortion of cover file and a small amount of hidden message. The comparison of previous implementations and future model promise a successful achievement. The contribution of this study is to modify an existing steganography method and evaluate iris model for protecting the biometric system against imposter attack, making the iris biometric system more secure with the implementation of steganography.

PS	PQ	PO	PC	Project Contribution
PS	PQ	PO1	PC3	Proposed a modification of the existing LSB approach
		PO2	PC2	Proposed a securing the secret information within the image file using LSB approach.
		PO3	PC1	Proposed an evaluating steganography approach with the LSB method.

Table 1 4: Summary of Project Contribution

1.7 Thesis Organization

Chapter 1: **Introduction**

This chapter give an introduction of iris recognition and steganography technique that will be use in this project.

Chapter 2: **Literature Review**

Explain more on project title, related work, proposed solution and previous work for securing iris authentication using steganography.

Chapter 3: **Project Methodology**

Discuss on methodology that will be use in this project which are Least Significant Bit (LSB) use to hiding data in iris template.

Chapter 4: **Analysis and Design**

Discuss on analysis project technique and design use in this project.

Chapter 5: **Implementation**

Explain details on implementation of the project and system development.

Chapter 6: **Testing**

Discuss on system testing trial or error that had been performed when running the system development program.

Chapter 7: **Conclusion**

Summarization of project and what objective had been achieved on this project. Also, the contribution and future work for this project.

1.7 Conclusion

This chapter briefly explain on project title, objective, problem statement, project questions, contribution and chapter summarization. The next chapter will review more about technique and method used to perform this project.

CHAPTER 2

LITERATURE REVIEW

2.1. Introduction

2.1.1 Steganography

Image steganography plays crucial role in digital processing. Image processing mainly focus to conceal a file, message, image or video. According to (Roy, 2016)The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Thus, cryptography is the practice of protecting the contents of a message alone, whereas steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Any digital image is comprised of pixels of different size of matrices, various Image steganography algorithms have been developed.

Ever since the technology have taken over the world, the internet become one of the most crucial factors of information technology and communication has been the security of information. Cryptography was known as a technique to secure the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. However, it is not enough to keep the contents of a message secret, the necessary to keep the existence of the message secret may become handy. The technique used to implement this is called, steganography. Steganography is the art and science of invisible communication. This is

accomplished through hiding information in other information, thus hiding the existence of the communicated information (Roy, 2016).

The word steganography is derived from the Greek words “*stegos*” meaning “cover” and “*grafia*” meaning “writing” defining it as “covered writing”. For image steganography, the information is hidden exclusively in images. While, for image processing is one of the significant area of multimedia applications and it is known. Thus, these applications can be found almost everywhere in the modern world. Because of that, there are rapid increasing in number of people working with images which means, that demand for image processing tools also grows.

2.1.2 Iris Recognition

Biometric utilize physical traits (gait and voice recognition) or behavioral characteristics (iris, retina, thumbprint and face) for a reliable identity of authentication. The usage of iris biometric technology and application has increased tremendously for its user friendliness, performance, permanence, accuracy and uniqueness. There are many systems and machines use biometric in daily activities for instance, attendance system, withdrawing money from ATM and thumbprint to switch on laptop. In fact, in biometric, human is the key to access systems. Biometrics data is powerful and useful to the system; however, they have no keys. The biometric data is easy to steal or leading to identity theft and not secured. The more a biometric data is used, the less secret it would be (Zainal Abidin, Manaf, & Shibghatullah, 2011).

2.1.2.1 Characteristics of biometric Technologies

- 1) Universality - something that each person has.
- 2) Uniqueness - something that separates this very person from others. This means that not all characters can be suitable for biometrics.
- 3) Permanence - biometric measurement should be constant over time for each person.

- 4) Measurability (collectability) - it should be easy to measure, should not demand too much time and cost.
- 5) Performance - speed, accuracy and robustness
- 6) Acceptability - how well people accept biometrics
- 7) Circumvention - how easy it is to fool the system.

According to (Ayoub & Nori, 2013) The Human iris is a thin circular anatomical structure in the eye. The iris's function is to control the diameter and size of the pupils and hence it controls the amount of light that progresses to the retina. To control the amount of light entering the eye, the muscles associated with the iris (sphincter and dilator) either expand or contract the center aperture of the iris known as the pupil.

The iris consists of two layers: the pigmented front fibro vascular called as stroma and beneath it is the pigmented epithelial cells. The stroma is connected to the sphincter muscle which is responsible for the contraction of the pupil and to the set of dilator muscles, responsible for the enlargement of the pupil which it does by pulling the iris radially. The iris is divided into two basic regions: the pupillary zone, whose edges form the boundary of the pupil and the ciliary zone which constitutes the rest of the iris.

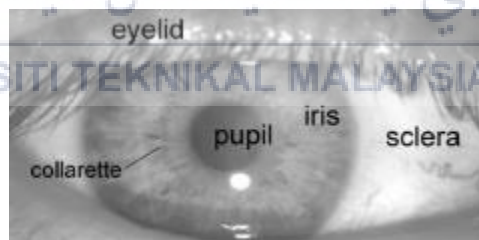


Figure 2.1: Front view of the human iris

2.2. Related Work/Previous Work

Sending encrypted message frequently will draw the attention of third parties, i.e. crackers and hackers, perhaps causing attempts and revealing the original message. Information hiding is a general term encompassing many sub disciplines. Steganography known as an ancient art of hiding information in ways a message is hidden in an innocent – looking cover media, so that will not arouse an eavesdropper's suspicion (Talee & Mohammed, 2014). The objective is to propose a

modification of the existing least significant bit (LSB) approach. Therefore in this chapter, according to (Talee & Mohammed, 2014) steganography replaces bits in image, sound and text file with secret data instead of protecting data the way cryptography does. Steganography conceals the existence of the data.

Capacity, security and robustness are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the ability of an eavesdropper to point the hidden information easily. Robustness is concerned with the resist ant probability of modifying or destroying the unseen data. The main function is to transmit a message through some innocuous carrier, for example, text, image, audio and video over a communication channel.

There are many technique about data hiding, but for this project we use a simple steganography approach which is LSB approach to securing the information encrypted within the image file. Therefore, a simple and well known method to further the approach is directly hiding secret data into the LSB of each pixel in an image. Then, based on the LSB technique, an algorithm for 24-bit color image is developed improves the stego-image quality of color image. In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the secret message. LSB Steganography can be classified by two methods LSB replacement and LSB matching. The terminology LSB replacement or LSB matching was firstly discussed by T. Sharp. First is LSB replacement which is simplest of the LSB steganography techniques. LSB replacement steganography replace the last bits of cover image with each bits of the message that needs to be hidden. Algorithm for LSB Based embedding and extracting process is given as-:

A LSB-based Embedding Algorithm

Input -: cover C

for $i = 1$ to Length(c), do

$S_j \leftarrow C_j$

for $i = 1$ to Length (m), do

Compute index j_i where to store the i^{th} message bit of m

$S_{j_i} \leftarrow \text{LSB}(C_{j_i}) = m_i$