Journal of Computing Technologies and Creative Content
Volume 2, Number 1, Nov 2017. Page 78-81.

Biometrics Security for Secured Login Access by Using Random Fingerprint Recognition Technique

Amirul Mukminin Bin Muhamad Yasin
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
1016 Jalan Sultan Ismail,
50250 Kuala Lumpur.
amirul.yasin@s.unikl.edu.my

Dr Rita Zaharah Wan Chik
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
1016 Jalan Sultan Ismail,
50250 Kuala Lumpur.
ritazaharah@unikl.edu.my

***Abstract*—**Fingerprint recognition system has been implemented for a long time in the security system. The fingerprint is one of the ways to identify a person's identity because every person has a unique thumbprint. Normally a person used a thumbprint for authentication, but it is not secured anymore nowadays because a thumbprint is way too easy for some people to copy. The objective of this research to study about fingerprint recognition in the authentication system, to develop biometric security by using random fingerprint recognition technique and to test the usability of random fingerprint recognition technique. The random fingerprint recognition technique will be developed using a Microsoft Visual Studio 2015 Enterprise (via VB.net programming), Microsoft Access and device Adafruit Optical Fingerprint Sensor. This system is to produce a new level of security that can enhance fingerprint authentication by using random fingerprint recognition technique. The benefit for the company that using this system could control the workplace from an outsider or prevent trespassers from accessing the system.

Keywords—Random Fingerprint, Fingerprint Recognition, Biometric, Rapid Application Development (RAD)

1. INTRODUCTION

Biometrics refers to human characteristics that identify individuals based on the anatomical (e.g. fingerprint) or behavioral (e.g. voice) characteristics (Anil jain, 1996). Biometrics have received increasing attention from researchers in recent years. Biometric-based authentication systems are more efficient than traditional authentication systems such as token- or knowledge-based information; which can be forgotten, stolen or lost (Sano et al., 2006). They are more user friendly and convenient as there is no need to remember or carry any extra information. Thus, it is "one of the best ways to link a user to a claimed identity. Of the range of biometric modalities (i.e. iris, fingerprint, hand vein, face and voice), fingerprints have been the most widely used in authentication systems due to their uniqueness, immutability and convenience" (Sano et al., 2006). Although fingerprint-based authentication systems have several advantages over traditional authentication systems, they also "suffer several drawbacks when they are used for remote authentication" (KRatha et al., 2007). Fake fingerprint images can be constructed easily using several spoofing approaches to accessing a system.

2. LITERATURE REVIEW

2.1 Introduction

Background of the project explained in this chapter based on the previous research on same topic and mechanical writings. It been discussed and compare to each other in order to get an overview understanding of this project really means".

2.2 Minutiae Based Fingering Matching

This efficient method is invariant to rotation, translation and distortion effects of fingerprint patterns. Eckert et al., (2005) stated that its algorithm uses a compact description of minutiae features in fingerprints and is separated from a prior feature extraction. The process consists of three major steps. First step finding pairs of possible corresponding minutiae on both fingerprint patterns. Second step combine these pairs to valid tuples of four minutiae each which containing two minutiae from each fingerprint. Finally matching the pattern. The proposed method has inexpensive computation and low and scalable memory requirements. In this method, a reference minutia is chosen from the fingerprint template and the query fingerprint. When the two sets of minutia are matched, reference minutia pair is aligned coordinately and directionally. The matching score of the remaining minutiae is evaluated then. This method guarantees the satisfaction in alignments of regions adjacent to the reference minutiae. However, the regions alignments which are far away from the reference minutiae produce outcomes that are not reliable (Amira Saleh et al., 2011).

2.3 Model of Fingerprint Recognition Using Minute Score Matching

There are several equations of model of fingerprint recognition using minutia score matching (FRMSM) which is a false matching ratio, false non-matching ration and matching score. All of the methods will be discussed in the following.

False Matching Ratio

It is the probability that the system will decided to allow access to an (FMR) imposter is given an (Equation 2.1) (Ravi et al., 2009):

$$FMR = \frac{FalseMatches}{Imposter\ \ Attempts}$$

(2.1)

False Non-Matching Ratio

It is the probability that the system denies access to an approved user. The formula for this probability is given as following (Equation 2.2).

$$FMR = \frac{FalseNonMatches}{Enroll\ \ Attempts}$$

(2.2)

Matching Score

It is used to calculate the matching score between the input and template data is given as follows (Equation2.3).

$$Matching\ \ score = \frac{Matching\ \ Minutiae}{Max\ \ (NT, NI)}$$

(2.3)

Where,

NT = the total number of minutiae in the template.

NI = the total number of input matrices.

3. METHODOLOGY

The initiation phase is the first phase to start the project. It is also considered as the proposal phase. First, need to define the project objective,

problem statement, scope and proposed system. Finally submit the proposal before moved to the research phase.The research phase is done to gather important information for the project. Research on the article, journals and related projects are very important for the literature review.

First make research about authentication history, similar project, advantage and disadvantage, technique and method use. In the planning phase, need to determine the project activities to make sure that all the works could be done within the time period. Then we will determine the hardware and software to be used. The software that will require in the process of developing the project is Microsoft Visual Studio, which is licensed software to develop the coding. The hardware that will be used is a PC with a Windows 10 as the operating system and that will be a platform to run the application. Also, determine the project layout diagram and then estimate the budget and cost. Finally, identify project backup counter how we should handle the problem situation if anything happens during doing the works.

In this phase, will focus on gathering the information from a journal and white paper regarding the similar projects. The information consists of hardware and software requirement, testing environment and also budget and costing will involve on this phase. The development defines the models, their interfaces and behavior. The platform of this project is requiring pc or laptop. This project is creating an application and this will provide an interface for the user. The table below will list the entire software and hardware requirement and function in this system.

In the development phase, the prototype was developed and refine that the prototype meets the project requirement. Also, demonstrate the prototype to fulfil the requirement. Finally, make a review and change the prototype if there any change in requirement. A Visual Basic.Net was also built to interface between the end user and command line application. The application will be tested upon completion to check for flaws or any configuration error. Then the application will test the whole system such as the encoding and decoding process. The system will be refining if there should be any improvement.

After complete system, which has passed the test phase then implement the application. In this phase the requirement that needs to develop the prototype into the real application and apply the code by using visual basic language. It will focus on developing the code for every function for encode and decode. Besides that, it also needs to ensure that the application which is being built using the latest compiler versions with built-in compiler protection. This application will then undergo a real-life purpose and will be tested from time to time for better performance or any errors. Lastly conclude the result of the system. The last step is to prepare a report base on the result of the testing phase and the implementation phase.

4. RESULT

This fact turns the fingerprint biometric valuable for proposed on the security service. The system is unpredictable because of random fingerprint generator. The user no need to remember the password and prevent the access card from exposed to theft.

Figure 2.1: Result of System

Figure 2.1 show the result of system when the device on the child start far away from the device on parent. The latitude and longitude location will check on google maps.

Table 2.1: Enrollment process on fingerprint sensor with the system

Test Case: 2 **Project**: Biometrics Security for Secured Login Access by Using Random Fingerprint Recognition Technique **Test case:** Enrollment of fingerprint image data in the system **Executing Date**: September 2016		
Description: This testing is to show the enrollment process of first authentication method to be used in the system.		
Pre-condition: Adafruid fingerprint sensor, Arduino and visual basic has been installed.		
No.	**1**	**2**
Action	The system show the image and instruct user to place fingerprint with blinking red box.	Repeat the same step to enroll 5 fingerprint start form thumbprint
Expected outcome	The fingerprint scanner detect fingerprint and capture the image of fingerprint	All five-fingerprint successful enroll.
(Pass/Fail)		

Table 2.1 shows the test case 2 that is enrollment process on fingerprint sensor with the system that capturing image for enrollment process is well-function and well-integrated with the system.

Table 2.2: Security Testing Test Case

Test Case: 3 **Project**: Biometrics Security for Secured Login Access by Using Random Fingerprint Recognition Technique **Test case:** Security testing **Executing Date**: September 2016		
Description: This testing is to test the secure of the system		
Pre-condition: Adafruit Industries fingerprint sensor, Arduino and visual basic has been installed.		
No.	**1**	**2**
Action	Use some fingerprint that not enroll yet into the system.	Use another fingerprint that not follow the red blink.
Expected outcome	The system show message "invalid fingerprint".	The system show message "invalid fingerprint".
Test outcome	The system decline the login process and start new session.	The system decline the login process and start new session.
Result (Pass/Fail)	Pass	Pass

The table 2.2 shows the security testing, the conclusion is the system just only can accept the fingerprint that has been registered.

5. Conclusion

The system stored the five fingerprints of authorized users in the database but two fingerprints randomly selected by the system and the authorized user need to put the selected fingerprint on the fingerprint scanner. This technique will make attacker hard to predict finger that system needs. Design and develop a 2-layer security for authentication system which is two random fingerprint authentications that selected by system.

6. Acknowledgments.

I would like to thank my Project Supervisor Dr. Rita Zaharah Wan Chik for allowing me to commence this project and giving me the encouragement and helped at all time of research and writing of this report. Without her persistent help, this project is impossible to complete. I would also like to thank Madam Norsuhaili Bt Seid, Head of Section Information System, lecturers of UniKL MIIT for their supports and guidance throughout this projec..

7. References

Jain, A., Bolle, R., & Pankanti, S. (2006). Biometrics: personal identification innetworked society (Vol. 479). Springer Science & Business Media.

Ravi, J., K, B. R., & Venugopal, K. R. (2009). Fingerprint Recognition Using Minutia Score Matching. International Journal of Engineering Scienc and Technology, Vol.1,no.2, pp. 35-42.

Sahari, F. B. (2010). Digital Signal Processing in Biometrics (Iris Recognition).Universiti Kuala Lumpur British Malaysia Institute.

Saini, R., & Rana, N. (2014). Comparison of Various Biometric Methods. International Journal of Advances in Science and Technology (IJAST), Vol 2.