WIRELESS FINGERPRINT IMAGES COMMUNICATION

SUHANIF BIN ZAKARIA

This report is submitted in partial fulfillment of the requirements for the award of Bachelor of Electronic Engineering (Industrial Electronics) With Honors.

Faculty of Electronic and Computer Engineering
Universiti Teknikal Malaysia Melaka

April 2009

UNIVERSTI TEKNIKAL MALAYSIA MELAKA
FAKULTI KEJURUTERAAN ELEKTRONIK DAN KEJURUTERAAN KOMPUTER

BORANG PENGESAHAN STATUS LAPORAN
PROJEK SARJANA MUDA II

Tajuk Projek	:	**WIRELESS FINGERPRINT IMAGES COMMUNICATION**
Sesi Pengajian	:	**2008 / 2009**

Saya **SUHANIF BIN ZAKARIA**

mengaku membenarkan Laporan Projek Sarjana Muda ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Laporan adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan laporan 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**	

Disahkan oleh:

_____ (TANDATANGAN PENULIS)

Alamat Tetap: LOT 80, KG SRI PINANG,
DPN KOMPLEKS SUKAN,
16200 TUMPAT,
KELANTAN.

Tarikh: 30 / April / 2009

_____ (COP DAN TANDATANGAN PENYELIA)

Tarikh: 30/ April / 2009

"I hereby declared that this report entitled Wireless Fingerprint Images Transmission is a result of my own work except for the works that have been cited clearly in the references."

Signature : ……...
Student : SUHANIF BIN ZAKARIA
Date : 30 / April / 2009

"I hereby declare that I have read this report and in my opinion this report is sufficient in terms of the scope and quality for the award the Bachelor of Electronic Engineering (Industrial Electronics) With Honors".

Signature : ……

Name : EN AMAT AMIR BIN BASARI

Date : 30 / April / 2009

To my beloved parents, family, fellow friends and supervisor, thanks for all supports in successfully producing this projects.

ACKNOWLEDGEMENTS

In the name of ALLAH SWT, I would to say *'Alhamdullilah'* for the strength and spirit that had given to me in order to make this final year project and also thesis possible as well within the allocated time. I would like to take this opportunity to give my appreciation to all people that kindly contributed to the completion of this project and also thesis. With the cooperation and contributions from all parties, it had made the process of this project become smoothly.

I would like to convey my acknowledgement to my supervisor, Pn. Hanim Binti Abdul Razak who always gives me the guidance. Besides that, I also would like to thanks to Mr. Amat Amir Bin Basari because of his willingness to take over the position as a supervisor. For both of them, I really appreciate for everything that has been done to make this project possible. May ALLAH will always blessing them. I also would to thanks to Faculty of Electronic and Computer Engineering for the provide ness the tools and other things.

Not to be forgotten, to my beloved parents, especially my father that always encourage me to keep patient and work smart so that I can be a successful person. Besides that I also would like to give my appreciation to my sisters and brother and also my relatives who always support me and always encourage me to be a successful person.

ABSTRACT

The main purpose of this project is to build and establish the Wireless Local Area Network for fingerprint images transmission. In order to build the wireless connection, the Dlink DI-624 Wireless 108G Router is used as a receiving device. The protocol 802.11g is applied for this communication. Regarding to this project, the images from Microsoft Fingerprint Reader will be transmitted to the server by using PDA as an interface. The images that send to the server are in real time process, which means that each time the user scans their fingerprint, the images will be transmitted to the server and the server will make the matching process in order to accept or reject the access. This system can be implemented as a time attendance systems. The Microsoft Visual Studio.Net is used to build the Graphical User Interface (GUI) since it provides the Smart Device Application that can be use in order to implement in PDA, while in the server will be installed with database.

ABSTRAK

Tujuan utama dalam pembangunan projek ini adalah untuk membina dan melaksanakan Rangkaian Kawasan Tempatan tanpa wayar bagi kegunaan penghantaran imej cap jari. Dalam perlaksanaan hubungan tanpa wayar ini, ‘Router’ dari jenis Dlink DI-624 Wireless 108G digunakan sebagai alat penerima. Selain itu, dalam komunikasi ini, protocol 802.11g digunapakai. Berdasarkan kepada projek ini, imej yang dirakam dari ‘Microsoft Fingerprint Reader’ akan dihantar kepada server dengan menggunakan ‘PDA’ sebagai alat pengantaraan. Imej yang dihantar adalah dalam bentuk masa nyata, yang mana bermaksud, setiap kali para pengguna membuat pengimbasan cap jari, imej tersebut akan dihantar kepada server dan server akan membuat pengecaman sama ada imej cap jari tersebut sama atau tidak dengan imej yang sedia ada di dalam pangkalan data. Sistem ini boleh diaplikasikan untuk sistem masa kehadiran. Perisian Visual Studio.Net digunakan kerana ia dilengkapi dengan Aplikasi Alat Pintar yang membolehkan antaramuka di masukkan ke dalam PDA.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF APPENDIXES

CHAPTER I

INTRODUCTION

1.1 PROJECT OVERVIEW

Nowadays, the fingerprints become an important thing to the security system such as for attendance system, door lock system and even in forensic investigation. This is because each people don’t have the same fingerprint. Besides that, the fingerprints cannot be altered without creating a new unique fingerprint. Even when the skin tissue is injured, the skin that grows back will have the same print.

Fingerprint verification is one of the most reliable personal identification methods in biometrics. With the rapid development of fingerprint verification, a number of its applications have been proposed until now including time attendance system etc. For this project, a wireless fingerprint attendance management system is designed and implemented. This system based biometrics and wireless technique solves the problem of spurious attendance and the trouble of laying the corresponding network by using the Personal Digital Assistant (PDA). It can make the users' attendances more easily and effectively.

1.2 PROJECT OBJECTIVE

The objective of this project to establish the Wireless Local Area Network (WLAN) connection for fingerprint images communication and also developing the Graphical User Interface (GUI) by using VB.NET in order to interface the fingerprint scanner/reader with Personal Digital Assistant (PDA).

1.3 PROBLEM STATEMENT

Basically, by using the previous method, the users have to go to the particular fingerprint scanner/reader which is usually placed at the specific location such as at the main entrance in order to scan for attendances. So, for this method, it will face the problem when there are many users want to scan at the same time. The users must wait and queue to scan the attendance. It is wasting time.

So, this project is discovering in order to solve the problem. By applying the wireless connection for the attendance system, the users might not face the problem anymore. The user can scan the attendance by using their PDA wirelessly. The data will directly send to the server and store into the database. So, it helps user to save their time.

1.4 SCOPE OF WORKS

The scope of the project is to establish the Wireless Local Area Network (WLAN) connection in order to use for transmission of fingerprint images. The process of the transmission consists of transmitting and receiving. For this connection, the protocol IEEE 802.11g has been use. The communication device is between Personal Digital Assistant (PDA) and server. The fingerprint images will be transfer from Personal Digital Assistant (PDA) to server and the server will reply to the Personal Digital Assistant (PDA). The D-Link DI-624 Wireless 108G Router will be use as a receiver.

The Graphical User Interface (GUI) that will develop will be the interface between the Personal Digital Assistant (PDA) and server. The Graphical User Interface (GUI) will be installs into Personal Digital Assistant (PDA) while the server will be setup to centralize the operation and the database that will be creating will be installs into the server. The database will be creating by using Microsoft Access. In the database, it consist the user's information such as fingerprint, name, picture, and etc. So each time user try to access the server by the Personal Digital Assistant (PDA), the server will reply to Personal Digital Assistant (PDA) whether the server accept or reject the user's access due to the information given during the access time.

1.5 SUMMARY OF METHODOLOGY

For this project, there are several researches that have been made such as research in wireless LAN, Fingerprint and Graphical User Interface (GUI). The entire researches are important to each other in order to make this project is possible. The entire data and information was gathered together so that this project was in the right path.

1.6 REPORT STRUCTURES

This report contains five chapters and each chapter briefly describe about this project. For Chapter I, it is describe the introduction of this project. Every element in this chapter such as project overview, project objective, problem statement, scope of works, and summary of methodology is describe in simple explanation.

For Chapter II, this chapter is discussing the literature review of the project in overall aspect. Based on this project, the literature review is focused on Wireless Local Area Network (WLAN), Access Point, Personal Digital Assistant (HTC P3600i), Graphical User Interface (GUI – VB.NET), Fingerprint Reader (Microsoft Fingerprint Reader) and also TCP/IP.

For Chapter III, this chapter is describing the project methodology which is focusing on how the data and information are gathered, how the data is being processed and analyzed; besides the flow chart is also briefly discussed. In this chapter also, the factors that had been considered in choosing the method of the system is explain in details. Besides that, the advantages of the method that had been chose are also briefly discussed.

For Chapter IV, this chapter is about results and discussion. Based on this project, the result that determined is more to prototype. So, in this chapter, the prototype which will be the real model is briefly explained. For this chapter, it is also focus on the comparison with the previous research. The process, procedure and implementation are briefly explained in discussion part.

For Chapter V, this chapter is explaining the conclusion and suggestions. The entire project is concluding in this chapter. With the conclusion, the suggestion in order to improvise this project for future had been determined and briefly explained.

CHAPTER II

LITERATURE REVIEW

2.1 WIRELESS LOCAL AREA NETWORK (WLAN)

A wireless LAN or WLAN or wireless local area network is the linking of two or more computers or devices using spread-spectrum or OFDM modulation technology based to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

Wireless computing is a rapidly emerging technology providing users with network connectivity without being tethered off of a wired network. Wireless local area networks (WLANs), like their wired counterparts, are being developed to provide high bandwidth to users in a limited geographical area. WLANs are being studied as an alternative to the high installation and maintenance costs incurred by traditional additions, deletions, and changes experienced in wired LAN infrastructures. Physical and environmental necessity is another driving factor in favor of WLANs. Typically, new building architectures are planned with network connectivity factored into the building requirements.

However, users inhabiting existing buildings may find it infeasible to retrofit existing structures for wired network access. Examples of structures that are very difficult to wire include concrete buildings, trading floors, manufacturing facilities, warehouses, and historical buildings. Lastly, the operational environment may not accommodate a wired network, or the network may be temporary and operational for a very short time, making the installation of a wired network impractical. Examples where this is true include ad hoc networking needs such as conference registration centers, campus classrooms, emergency relief centers, and tactical military environments. Ideally, users of wireless networks will want the same services and capabilities that they have commonly come to expect with wired networks. However, to meet these objectives, the wireless community faces certain challenges and constraints that are not imposed on their wired counterparts.

2.1.1 Frequency Allocation

Operation of a wireless network requires that all users operate on a common frequency band. Frequency bands for particular uses must typically be approved and licensed in each country, which is a time-consuming process due to the high demand for available radio spectrum.

2.1.2 Interference and Reliability

Interference in wireless communications can be caused by simultaneous transmissions (i.e., collisions) by two or more sources sharing the same frequency band. Collisions are typically the result of multiple stations waiting for the channel to become idle and then beginning transmission at the same time. Collisions are also caused by the “hidden terminal” problem, where a station, believing the channel is idle, begins transmission without successfully detecting the presence of a transmission already in progress. Interference is also caused by multipath fading, which is characterized by random amplitude and phase fluctuations at the receiver. The reliability of the communications channel is

typically measured by the average bit error rate (BER). For packetized voice, packet loss rates on the order of 10–2 are generally acceptable; for uncoded data, a BER of 10–5 is regarded as acceptable. Automatic repeat request (ARQ) and forward error correction (FEC) are used to increase reliability.

2.1.3 Security

In a wired network, the transmission medium can be physically secured, and access to the network is easily controlled. A wireless network is more difficult to secure, since the transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance.

2.1.4 Power Consumption

Typically, devices connected to a wired network are powered by the local 110 V commercial power provided in a building. Wireless devices, however, are meant to be portable and/or mobile, and are typically battery powered. Therefore, devices must be designed to be very energy-efficient, resulting in “sleep” modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-offs.

2.1.5 Human Safety

Research is ongoing to determine whether radio frequency (RF) transmissions from radio and cellular phones are linked to human illness. Networks should be designed to minimize the power transmitted by network devices. For infrared (IR) WLAN systems, optical transmitters must be designed to prevent vision impairment.

2.1.6 Mobility

Unlike wired terminals, which are static when operating on the network, one of the primary advantages of wireless terminals is freedom of mobility. Therefore, system designs must accommodate handoff between transmission boundaries and route traffic to mobile users.

2.1.7 Throughput

The capacity of WLANs should ideally approach that of their wired counterparts. However, due to physical limitations and limited available bandwidth, WLANs are currently targeted to operate at data rates between 1–20 Mb/s. To support multiple transmissions simultaneously, spread spectrum techniques are frequently employed. Currently, there are two emerging WLAN standards: the European Telecommunications Standards Institute (ETSI) High-Performance European Radio LAN (HIPERLAN) and the IEEE 802.11 WLAN. Both draft standards cover the physical layer and medium access control (MAC) sublayer of the open systems interconnection (OSI) seven-layer reference model.

The HIPERLAN committee has identified the 5.15–5.30 GHz and 17.1–17.2 GHz bands for transmission. The 5 GHz band has been ratified for HIPERLAN use by the Conference of European Postal and Telecommunications Administrations (CEPT). Data rates up to 23.529 Mb/s are projected, and multihop routing, time-bounded services, and power-saving features are expected.

2.2 IEEE 802.11 DRAFT STANDARDS

The IEEE 802.11 draft standard describes mandatory support for a 1 Mb/s WLAN with optional support for a 2 Mb/s data transmission rate. Mandatory support for asynchronous data transfer is specified as well as optional support for distributed time-bounded services (DTBS). Asynchronous data transfer refers to traffic that is relatively insensitive to time delay. Examples of asynchronous data are available bit rate traffic like electronic mail and file transfers. Time-bounded traffic, on the other hand, is traffic that is bounded by specified time delays to achieve an acceptable quality of service (QoS) (e.g., packetized voice and video).

Wireless technologies are encroaching upon the traditional realm of “fixed” or “wired” networks. The most widely adopted wireless networking technology thus far has been the 802.11 networking protocol, which consists of six modulation techniques, the most of common of which are the 802.11a, 802.11b, and 802.11g standard amendments. The price erosion and popularity of 802.11 capable hardware (especially 802.11b/g) has made wireless networks both affordable and easy to deploy in a number of settings, such as offices, homes, and wireless hot spots.

Because of this, 802.11 is currently the most popular and common non-telephony communication protocol available for wireless communication. The 802.11 standard defines a set of protocol requirements for a wireless MAC, or medium access control, which specifies the behavior of data link layer communication between stations in a wireless network. A station is simply a device with wireless capabilities, such as a laptop or PDA with a wireless networking interface. Throughout this paper, we often refer to stations as clients. Most 802.11 networks operate in infrastructure mode (as opposed to ad-hoc mode) and use an access point (AP) to manage all wireless communications; it is this type of network that is the setting for our fingerprinting technique.

A key component of the 802.11 standard is the MAC specification that outlines the function of various communication frames. The MAC coordinates access to the wireless medium between stations and controls transmission of user data into the air via control and management frames. Higher-level protocol data, such as data produced by an application, is carried in data frames.

2.2.1 Architecture

The *basic service set* (BSS) is the fundamental building block of the IEEE 802.11 architecture. A BSS is defined as a group of stations that are under the direct control of a single coordination function (i.e., a DCF or PCF) which is defined below. The geographical area covered by the BSS is known as the *basic service area* (BSA), which is analogous to a cell in a cellular communications network. Conceptually, all stations in a BSS can communicate directly with all other stations in a BSS. However, transmission medium degradations due to multipath fading, or interference from nearby BSSs reusing the same physical-layer characteristics (e.g., frequency and spreading code, or hopping pattern), can cause some stations to appear “hidden” from other stations.

An ad hoc network is a deliberate grouping of stations into a single BSS for the purposes of internetworked communications without the aid of an infrastructure network. Figure 2.2.1.1 is an illustration of an *independent BSS* (IBSS), which is the formal name of an ad hoc network in the IEEE 802.11 standard. Any station can establish a direct communications session with any other station in the BSS, without the requirement of channeling all traffic through a centralized access point (AP).