Biometric Locker System

Y. L. Lay, H. J. Yang, C. H. Tsai

***Abstract*—Storage locker system is for the temporarily keeping the goods. This study implements a storage locker system with the technique of fingerprint recognition as the way to open and close the lock. The system captures the fingerprint of the locker renter and requires a fingerprint match to reopen the locker door, ensuring that only the renter can open the locker door to remove its contents. This system not only reduces the trouble for customers to bring the key, but also increases the trust and security for customers. The implementation process and system recognition rate for the storage locker system are examined in this study.**

***Index Terms*—fingerprint, locker, recognition**

I. INTRODUCTION

THE explosive growth in computer, telecommunicaitons, fnformation, transformation, and other tenologies has had a major impact on the ways companies bring value to their customers. The technology boom has creasted exciting new ways to learn about and track customers, and to create products and services tailored to individual customers needs.Technology is helping companies to distribute customers' services more efficiently and effectively [1]. Security is a major concern in many facets of life today [2]. Personal security, homeland security, and computer security have dominantly occupied center stage with many people turning to technology to help protect themselves. Biometrics has emerged as one of the most convenient, accurate, and cost-effective forms of security [3].

Fingerprint, voice, signature, hand geometry, face geometry and iris or retinal scans are all in use today. Each different type has its advantages and disadvantages, making each suitable for different types of applications [2]. Among these various technologies, fingerprint biometric systems are generally lower cost and have been in use for many years [4][5], thus they are more mature than other types of biometric systems.

They represent an easy and affordable way for applications to quickly and easily determine the identity of someone looking to access a facility, on-line account or database.

During the past decade, researchers have introduced a variety of technologies for reading real-time (or live scan) fingerprint patterns [6][7][8]. In the 1990s fingerprint scanners were developed using optical imaging, ultrasonics, infrared gauging, mechanical force, temperature, and electrical capacitance to detect the patterns on the surface of the finger and convert those patterns into electrical signals. Today, practical products came to market based on optics, temperature, and electrical capacitance [9][10]. And these products are trying to find their applications such as door access control, time & attendance management, ATM, POS, copy machine, automobile in people's daily life and so on.

Typical locker, usually locked by hardware key, though has been widely used in modern society, commonly suffers for some possible flaws: lost key, unauthorized key copy, etc. The latter means that previous locker user, or renter, could have a chance to steal the coming user's possessions. Specifically, this kind of locker open a possibility of crime as possessions can be deposited by one person while retrieved by different one. This situation could be seen when people try to transport illegal stuff from person to person by a locker rented in the public location. The aforementioned problems come with mechanical locker would be solved when the locker is integrated with biometrics-based authentication function. Since September 11, 2001 the United States government shows great interest in using biometrics for verification the person's identity in the areas of visa and government-issued identification cards. At present, some public locations or buildings, the installation of lockers with built-in biometrics identification is recommended for the help of reducing possibility of illegal movements. The biometrics identification could also show its merits when the fingerprint biometric locker system is used in schools or companies where the users can totally get rid of the burden of carrying key, keyless system so called, and will be allowed to access his locker any time just with a touch of his finger.

Manuscript received July 24, 2011. The author would like to show appreciation that this work was supported by the National Science Council of Taiwan, ROC under Grant No. NSC- 96- 2221- E- 167- 026- MY3.

Yun-Long Lay is with the National Chin-Yi University of Technology Department of Electronic Engineering, Taichung, Taiwan 41170 R.O.C. (Tel: 886-4-2392-4505 ext. 7340; fax: 886-4-2392-6610; e-mail: yllay@ncut.edu.tw).

Hui-Jen Yang is with the National Chin-Yi University of Technology Department of Information Management, Taichung, Taiwan 41170 R.O.C. (Tel: 886-4-2392-4505 ext. 7923; fax: 886-4-2392-3725; e-mail: yanghj@ncut.edu.tw).

Chung_Ho Tsaiis with the National Chin-Yi University of Technology Institute of Electronic Engineering, Taichung, Taiwan 41170 R.O.C. (Tel: 886-4-2392-4505 ext. 7310; fax: 886-4-2392-6610; e-mail chtsai@ncut.edu.tw).

II. Fingerprint Biometric Locker System Implementation

A. Fingerprint

The Fingerprint Biometric Module**,** built around a DSP chip [11], will conduct the feature extraction process as an image was captured by fingerprint sensor and will do match function when verification of the current snapped fingerprint with pre-enrolled template is required. Designed and works as a slave device, the fingerprint module needs external host to dominate the work. One typical selection of the host is microcontroller, as here in this studied system, such as the prevailing 8051 chips. All the commands issued by host and every message sent back from the module are conducted via a widely used RS-232 serial interface following a simple, yet reliable communication protocol.

B. Communication Protocol

The fingerprint module is designed to be a slave device. It works under the control of an external host. The control is implemented by one specific communication protocol over the RS-232 interface. A complete communication protocol consists of the transmitted part and received part (Fig. 1). At the beginning of a control process, the host will send one command to the module. On receiving the command packet, the fingerprint module proceeds with some necessary protocol checks and will return a response message, pertaining the result of command execution, to the controlling host. This completes the whole control sequence and the packets are detailed in the following figures.

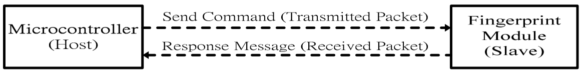
Microcontroller
(Host)
Send Command (Transmitted Packet)
Response Message (Received Packet)
Fingerprint
Module
(Slave)

Fig. 1

Typical scenario of communication between microcontroller and Fingerprint Biometric Module

C. Transmitted Packet Format

The formats of transmitted packet format consist of STX, command, length, parameter data, ETX, and checksum (Fig. 2). STX refers to the start of the packet; the command means the command issued by the microcontroller host; the length means the filed indicates the length in byte of the parameter data; parameter data refers to the data transmitted with the command; ETX refers to the end index of the transmitted packet; checksum refers to the checksum of the all transmitted data for checking of data integrity.

STX	Command	Length	Parameter Data	ETX	Checksum

Fig. 2 The transmitted packet format

D. Received Packet Format

The fields in the received packet format (Fig. 3) are same as transmitted packet format except response message and parameter data. Response Message indicates the execution result of the issued command by fingerprint module; Parameter Data means **t**he data returned by fingerprint module.

STX	Response Message	Length	Parameter Data	ETX	Checksum

Fig. 3 The received packet format

As can be seen in the above figures, a checksum is implemented at the end of each packet to keep integrity of data sending over the wires. Also the length of each transmitted or received packet will vary by the data amount required by each command and message.

E. Multi-Drop Bus (MDB)

In order to collect renting fee, a coin changer and a bill validator are equipped in this system and are controlled by the microcontroller over a Multi-Drop Bus (MDB). MDB is a communication standard, usually found its use in electrically controlled vending machine, and is a serial bus interface configured for Master-Slave operation. This interface communicates with a fixed data rate of 9600 bits/sec and a maximum of 32 slaves can be attached to the system under a master controller. In this fingerprint biometric locker system, two slaves (coin changer and bill validator) have been hooked. Each slave has a predefined address and its own command set. In its operation (Fig. 4), the microcontroller continuously polls each slave and the polled slave takes this chance to report its status in the real operation conditions by ACK (acknowledgement), NAK (non-acknowledgement) or specific data (DAT) to the master such as the amount of money collected by a coin changer. To achieve high reliability of data transmission in the MDB, the CHK (check) byte, which derived from checksum of the transmitted data, is applied. Also, for better system reliability and avoiding electrical interference between master and slaves, a photo-coupler interface (Fig. 5) is implemented on the microcontroller board to connect each devices.

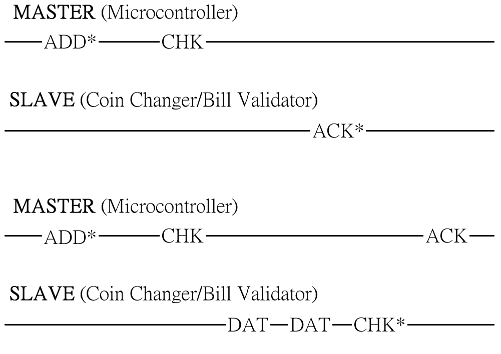

Fig. 4 Some typical transmission processes over MDB

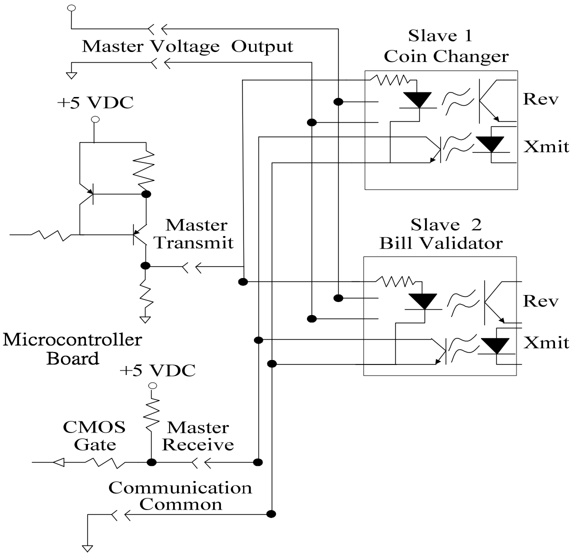

Fig. 5 The photo-coupler interface implemented on the microcontroller board

III. System Architecture and Experiment

The whole fingerprint biometric locker system is composed of user interface, fingerprint processing module, locker control, and fee collecting devices (Fig. 6). Besides, this system will upload management data to a personal computer with a RS232 serial cable. This system starts its service, with the help of guiding messages displayed on the LCD Module, after the press of a "rent" button on the interface keypad by the user. This locker renter will first be asked to put required amount of fee into the coin changer/bill validator to continue whole renting process. A fingerprint image, captured by fingerprint sensor, will be sent to the fingerprint biometric module, and then a template, extracted from this image, is associated with an assigned locker, and recorded in data base for later use in identifying this person at reopening this locker (Fig. 7).

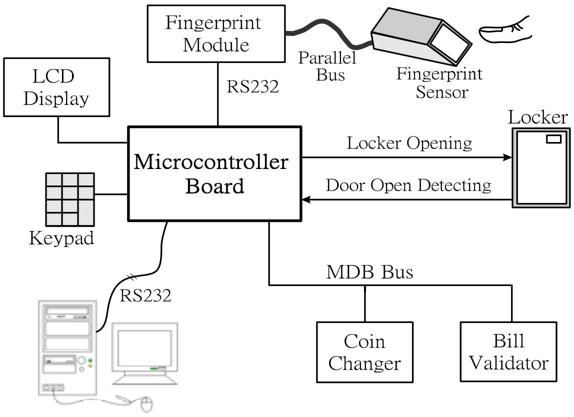

Fig.6 The fingerprint biometric locker system

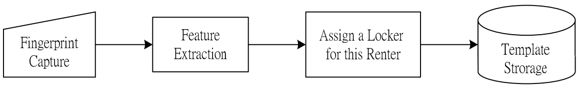

Fig. 7 The enrolling (renting) process

Some time later, when the person wants to get back his possessions, he will touch the keypad's "retrieve" button and follow procedures, briefed on LCD Module, such as scanning his fingerprint and waiting a little while for system to verify this newly acquired fingerprint image with the template enrolled formerly (Fig. 8). By snapping the fingerprint of the locker renter during the renting process and requiring a fingerprint match to reopen the locker door, this system will ensure that only the renter can open the locker to remove its contents.

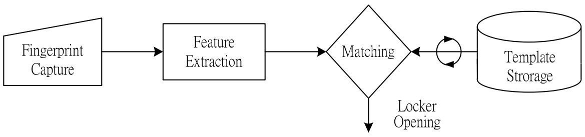

Fig. 8 The identification (retrieve) process

The data, regarding locker usage, fingerprint data and revenue statistics, collected on the microcontroller board will be accessed by a personal computer through a RS232 link (Fig. 8). And further data analysis can be conducted on the PC.

IV. Conclusion

This storage locker system currently has a computer connecting 32 storage cabins. Each storage cabin has a fingerprint recognition and bill counting system. From two month's laboratory testing, the recognition rate of this system is 96%, which matches the need of business application. In the near future, this system will set up in the commercial institution for field test. The usability of this system may investigate for advanced study.

Acknowledgments

This work was supported by the National Science Council of Taiwan, ROC under Grant No. NSC- 96- 2221-E- 167- 026- MY3.

References

[1] Gary Armstrong, Philip Kolter, and Geoffrey da Silva, Marketing: an introduction an Asian Perspective, Prentice Hall, 7th Ed. Singapore, (2005).
[2] Paul Rosenzweig, Alane Kochems, and Ari Schwartz, "Biometric Technologies: Security, Legal, and Policy Implications", Legal Memorandum, pp. 1-6, (2004).
[3] N. K. Ratha J. H. Connell R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM SYSTEMS JOURNAL, VOL 40, NO 3, pp. 614-634, (2001).

[4] Identification Resources,
http :// www.findbiometrics.com

[5] Resource Center,
http://www.bio-key.com

[6] David D. Hwang, Ingrid Verbauwhede, "Design of Portable Biometric Authenticators—Energy, Performance, and Security Tradeoffs", IEEE Transactions on Consumer Electronics, pp. 1222-1231, (2004).

[7] Dale R. Setlak, "Advances in Biometric Fingerprint Technology are Driving Rapid Adoption in Consumer Marketplace" AuthenTec Corp.

[8] "FINGERPRINT AUTHENTICATION TECHNICAL WHITE PAPER", Fidelica Microsystems, Inc.

[9] "Biometric User Authentication Fingerprint Sensor Product Evaluation Summary", Version 1.03, pp. 1-26, Intel Corp, (2005).

[10] Peter Bishop, "Atmel's FingerChip™ Technology for Biometric Security", Atmel Corp, (2002).

[11] FCP301 fingerprint module,
http://www.startek.com.tw