Security System Based On Fingerprint ID for Mobile Phone

A. Saleem, M. Al-Akaidi
School of Engineering & Technology
De Montfort University, Leicester

Abstract

Mobile phone theft has become a major crime problem over the past few years. At present a mobile phone thief can only replace the SIM card of a stolen phone with new one, which is cheap to purchase from any mobile service provider. Traditional security system for mobile phones is based on security code, which can be forgotten, stolen or lost. In this work we propose a new security system for mobile phone, which based on fingerprint ID. We believe that such system will decrease the rate of mobile phone theft significantly.

1 INTRODUCTION

There has been a dramatic rise in the number of the people who own a mobile phone, and in parallel with this there has been a rise in the number of phone thefts.

According to the statistics reported by the Home Office Research Study regarding the mobile phone theft in UK, there was an increase in the percentage of the robberies involving phones – from about 8% in 1998/99 to about 28% in 2000/01. the information clarified in the report show that there were about 470,000 mobile phones stolen in incidents involving householders in 2000. This will underestimate the full number of phones targeted, since they didn't cover incidents against commercial targets, and it excludes those under 16 [2].

The rise in mobile phone theft has brought the issue of phone security system. One of these proposed systems is the Personal Identification Number (PIN), thieves need to know the PIN in order to use the phone illegally. A large number of methods are available to discover a subscriber's PIN. 'Shoulder surfing' is a technique of spying on people when they enter there PINs in public places, either by using cameras or simply by looking over their shoulders. A computer and a sequential number dial-out program are used as well to obtain the PIN. An alternative solution was proposed to solve this problem, in this solution each handset has given a unique number known as International Mobile Equipment Identity (IMEI)[3][4]. Unfortunately, even if the police know the IMEI number of a lost or stolen mobile phone, they can not tell which carrier supplies service to that phone. In order to identify the phone (in UK), they must submit the IMEI number to each of the six mobile phone carriers (Vodafone, O_2, BT, One-one, Orange), which means that if 1000 phones are stolen, the police are required to fill out six thousands separate forms to obtain the relevant identification details, which is obviously not feasible [5].

In this project we have introduced a new security system for mobile phone based on fingerprint ID which is impossible to be forgotten or stolen. This security system will prevent anybody-except the phone owner- not only to access the phone but also to unlock the phone's keys if it is already accessed. Furthermore, our system has the capability to recognize more than one fingerprint and allows more than one authorized users to access the mobile, at the same time it allows the user to access the phone in the case of thumb injuring or cutting, which makes the system more flexible.

In the case of mobile phone stolen, the thief will not be able to unlock the keys in order to use the phone, and even if he/she tries to reboot the phone he can not access the phone as well.

2 WHY FINGERPRINT ID?

Fingerprints are perhaps the primary means of personal identification, although there are many other unique characteristics of an individual that can be used. They include voiceprints, dental impressions, DNA, retinal patterns, and even the shape of the ear lobes. Although these other characteristics are as much unique to the individual as are fingerprints, they lack many advantages which fingerprints have especially for the security systems. Common to the other distinctive attributes, fingerprints are universal and unique. In other words, everyone has them and no two have ever been found to be identical. Fingerprints are also unchangeable [6].

What actually makes a fingerprint unique depends on one main factor. Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern. When an inked imprint of a finger is made, the impression created is of the ridges while the furrows are the un-inked areas between the ridges. Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called ‘minutiae’ are what is most unique to the individual [1].

These features are particular patterns consisting of terminations or bifurcations of the ridges. It is these features that Automated Fingerprint Identification Systems (AFIS) extract and compare for determining a match [1].

3 THE SYSTEM HARDWARE

The hardware design consists of a development kit and fingerprint sensor. The development kit contains cellular Processor, keypad, LCD (16-bit Colour Display), multiple peripheral, debug interfaces. Figure 1 illustrates the block diagram of the system prototype. The cellular microprocessor has an integrated On-Chip Flash memory and an integrated SRAM. The fingerprint sensor has been used is the *Fujitsu MBF300 Fingerprint Sweep Sensor*, which is capacitive based, solid-state fingerprint acquisition device. The MBF300 sensor size is only 4.3mm x 14mm, with a height of only 1.2mm. The reduction in sensor size makes this device ideal for integration into mobile applications such as cellular phones.

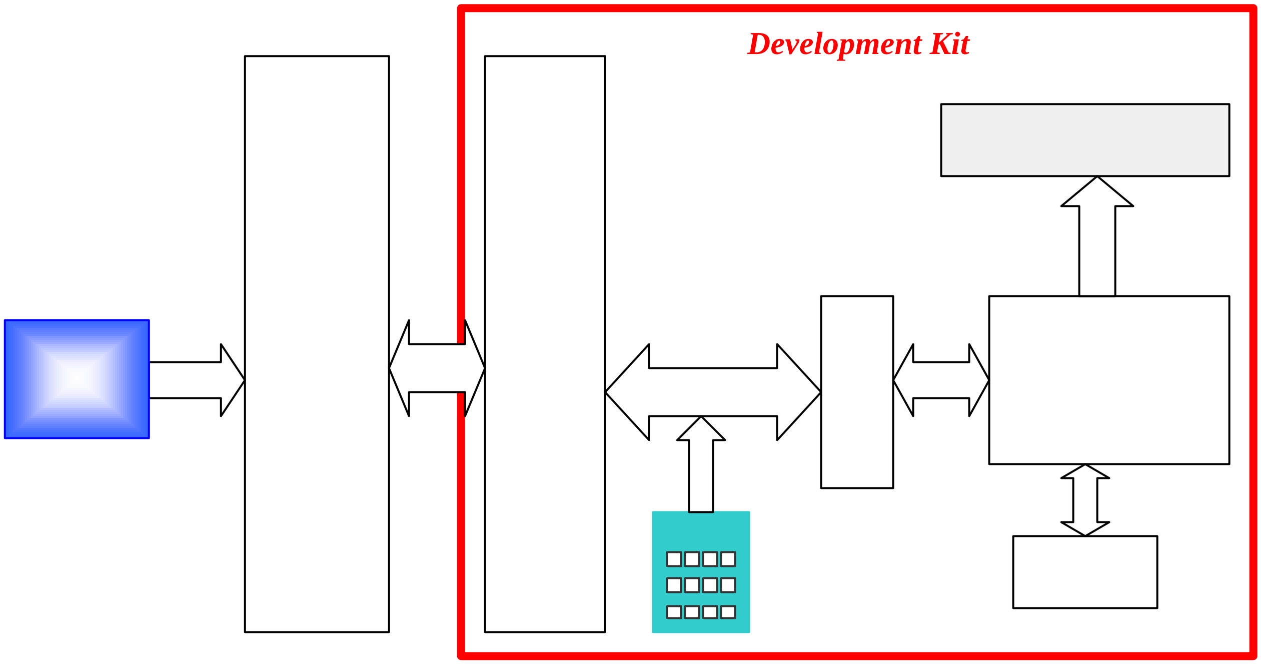

Figure 1: The Prototype Block Diagram

4 THE SYSTEM ALGORITHM

The flow chart shown in Figure 2 explains the algorithm of the system operation. As soon as the user switches on the phone, the security system will not allow him\her to access the phone unless he\she used his \her thumb, if the user does not use the phone for 5 seconds, the system will lock the phone keys automatically.

The system has the capability of check the existence of the thumb every 5 ms, if the thumb exists, the system will scan the existence thumb and compare the scanned image with one of the templates and if the match occurs, then the keys will be unlocked, otherwise the system will wait for 10 ms before restart checking the existence of the thumb again.

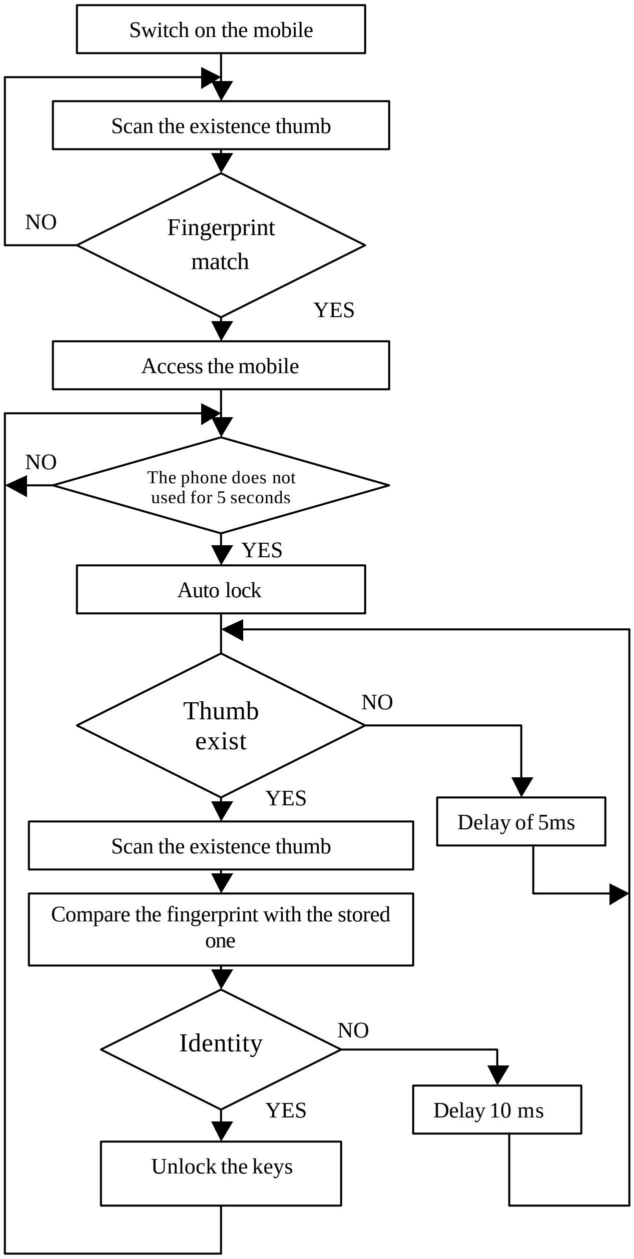

Figure 2: The Flow Chart of the Security System Algorithm

5 IMPLEMENTATION

The proposed security algorithm and design is adaptive with all mobile phone models due to the size of the fingerprint sensor, the low power consumption (˜ 70 mW) and the low cost. Different models of mobile phones with the proposed security system are shown in Figure 3.

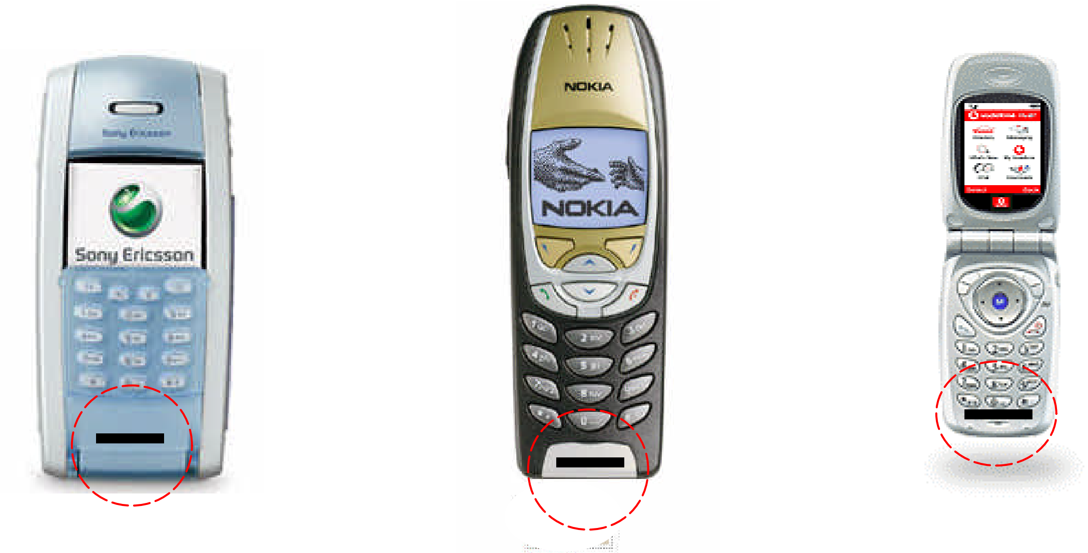

Figure 3: The Security System in Different Mobile Phone Models

6 CONCLUSIONS

The security system algorithm has been tested on a development kit which contains all the primary components of the real mobile phone handset, and it worked properly. The performance and the reliability of this system depend mainly on the performance of the fingerprint identification and verification algorithm. Therefore, the main task in the future is to enhance the performance of the fingerprint identification and verification algorithm which will affect the overall system performance accordingly.

7 REFERENCES

[1] “*FINGERPRINT RECOGNITION THROUGH CIRCULAR SAMPLING*” http://www.cis.rit.edu/research/thesis/bs/1999 /chang/thesis.html

[2] “*MOBIL PHONE THEFT*”, Home Office Research Study 235, Development and Statistics Directorate, 2001

[3] ”*INTERNATIONAL MOBILE STATION EQUIPMENT IDENTITIES (IMEI)*”, 3rd Generation Partnership Project, 3GPP TS 22.016, V3.3.0 (2002-06).

[4] “*ANTIONAL ACTION TO TACKLE MOBILE PHONE THEFT, UK*”, United Kingdom Project Example-Robbery.

[5] “*MEDIA RELEASE: PROBLEM OF MOBILE PHONE THEFT*”, http://www.lawlink.nsw.gov.au/boscar1.nsf/pages/media110401.

[6] “*FINGERPRINT RECOGNITION*” from http://www.ieee.org/ organizations/eab/recollege/faraday/worksheets/ dw/pre_fr.doc