YILDIZ TECHNICAL UNIVERSITY
FACULTY OF ELECTRICAL AND ELECTRONICS
COMPUTER ENGINEERING DEPARTMENT

SENIOR PROJECT

Mobile Presence Checker

Project Manager
Prof. Dr. Ahmet Coşkun Sönmez

Project Group
05011038 Uygar ER
05011067 Engin ÖZER

İstanbul

INDEX

1. Image List

1. Foreword

In our daily life there is many methods to provide identity identification. Biometric methods are the most popular of them without any suspect. Iris recognition, face recognition, voice recognition and fingerprint recognition can be given as samples of biometric methods. Nowadays many people began to use fingerprint recognition or face recognition in their laptops to start their sessions. These methods became more closer to us and our daily life. Because biometric methods are the most reliable way to identify the right person. In China since at least 700 AD, fingerprints were used to officially certify contracts. In Europe in 1858, fingerprint use in fighting crime was proposed and was implemented in Germany in 1903.

In this new era that biometric methods are everywhere in our ordinary life, new solutions about identifying the right person, should be done by using this methods. At this point we will develop a system that will check presence reliably and faster than any other methods. Our system will be mobile and use fingerprint recognition to achieve this aim.

We thank to Prof. Dr. Ahmet Coşkun Sönmez who is supporting us and brings us new visions about our project.

2.Summary and Introduction

The system that we will set up, will be basically a mobile presence checker and will have reporting feature. The prototype of this system will be performed on eBox architecture. eBox will provide the mobility and let us to use .NET framework. eBox is a little and mobil computer that have Windows CE operating system on it.

Thanks to the architecture of eBox we will use Visual Studio to make coding and use Windows CE emulator to try our applications. Our system will consist of an LCD screen, numeric keyboard and fingerprint reader and can be possible to produce it in series production.

3.Existing System And Problems

The system that we'll set up, will basically behave like presence checker. In normal scenario instructor checks presence of the students that are in the class. In the midterm instructor makes a calculation about the presence of each student and If it's possible, lets them to take an examination. Else the students that were not exist in the class for an enough time, they are failed.

Checking presence can be done in many way. For example when the student comes into the university campus, a record can be taken by a special reader and control by some applications. But controlling presence of the student that is in the class difficult because of some reasons. One of these reason, a student can register itself before begining of the lesson although he or she is not in the class while instructor giving the lesson. Besides In this scenario since the reader is in public area, a harmfull attack physically or programmaticaly can be done. And also in this situation the reader is fixed and there is no mobility with it.

4.Earlier Solutions And Results

Sample system was put into practice in order to check the presence of school and classes in the China at Hunan University. In this system students must use their fingerprints to get in the classroom. According to manager of the college, checking presence with old methods causes loss of time and also was abused by the students. Because of this, the getting fair results about the checking presence had became difficult. After the new system was taken into use the attendance of lessons increased noteworthy. This shows us that using these kind of systems will help us reasonably.

5.Our Solution To The Problems

Here, comes our offer, to that problem. In our system it is planned that each instructor have a mobile device that will make presence checking process. Since that mobile device will be used supervision of the instructor, harmfull attacks will be prevented easily. Checking presence will be done by using finger print of a student that takes the lesson. The instructor gives the mobile devices to the students and each of them gives their finger prints to the device. Device will make matching and registering process. Afterwards the results can be reported by the

system. So that control and reliability will be provided. These system will also provide saving time, and let fast and flexible operations.

We are planning three roles for this project.

- Administrator
- Instructor
- Students

Administrator have right to manage the system from the super stratum. Administrator can add new instructor to the system, delete existing instructors, update their status, assign new lessons to them and delete existing lessons. Administrator can determine the count of week for a term and date for the first lesson. Administrator also decides for quota of a lesson. The administrator determines a lower limit for a lesson. So that if a student has already used it's nonattendance right, it's not allowed to join the roll call.

Instructors have right to start a new presence checking process. Instructor can report the results of checking presence. If there is enough quota he can add new student or remove existing student. Instructors can update the status for checking presence. If an instructor starts a checking presence process only it can end this process by accepting the result of roll call. The system that we'll set up will get the fingerprint of a student only one time. Then this fingerprint will be used for every lesson. Instructor can leave messages or notes of a visa to the students and students can display it while roll call. Instructor can print results and mail them to the students.

The system that we'll set up will follow these steps in order to make checking presence;

1. Instructor logs in and selects the lesson to start roll call.
2. Instructor starts the application that will make matching process.
3. Students will type their identity numbers and give their fingerprints by using the keyboard, if it is not successful locking mecanism can be worked.
4. The application makes matching process and If the process is successful, shows the message for giving information.

5. After all system will be approved and closed by the instructor.

6. If a problem occurs about checking presence of a student, instructor can make this check process manually.

Our system will also let instructor take new record of a student that is not registered to system. In this scenario, instructor selects the application that wil make registration process. Identity number and fingerprint of a student are taken. Afterwards the instructor confirm the new record.

In order to actualize this project we will use various hardware. First of all, we'll work on the eBox platform which is used for developing mobile applications. eBox is a new platform which is published by Microsoft and using Windows CE operating system on it. Since eBox is a platform that is supported by Microsoft, we will use MS Visual Studio framework 2.0 to develop our application and make coding faster. One of our other hardwares is the LCD screen that will be used to display forms of our application. Selecting applications, listing results and lessons, showing messages of our applications will be done through LCD monitor. In addition to these all, one numeric keyboard will be used to get identity numbers from the machine. Selection will be done by using numeric keyboard in the beginning but afterwards it can be done by using touch screen. (If we use touch screen virtual keyboard can be used.)

The most important hardware is the fingerprint reader. Fingerprint reader will communicate with eBox through USB. We will get scalar results from the fingerprint readers and will use them in our applications.

6.Feasibility

This part consist of feasibility of software and cost, feasibility of hardware and cost, feasibility of time, total cost and legal feasibility parts.

6.1.Feasibility of Software and Cost

Firstly, the biggest requirement is choosing the programming language. Firstly, the programming language that will be used at this project must be so powerful and easy to use for making process quickly. To take software development progress quickly, this condition will be

one of the main issue we will be thinking of while choosing the programming language. In addition, this programming language must have strong libraries for us to use. The other issues that will be thought of is that this language must be up to date and widely used language. This condition helps programmers to get help from other programmers. But, the most important issue that must be taken in account is that, this language must be used under our platform Windows CE x86. Otherwise, software and hardware requirement will rise off. This language should also be chosed from object oriented family to follow up our century's software trend. Also, It will be a very much money and time expense to educate project team with a new language.

For this Project, two programming languages as C++ and Java appears as alternatives. C++ is such as language that has very powerful libraries of C language but also C++ is an object oriented programming language and has exception handling utilities. In addition, developing software in this languages will not cost extra expenses. Project team has members who has knowledge in C++ language. C++ compilers can easily be found free. Although C++ has so many powerful libraries, its library files and binaries changes upon the platform. Java is a platform independent language and has wide spread libraries. The biggest difference between Java and other languages is that Java compiler does not compile the code into machine executable binary. Java compiler compiles the code into Java byte code. This byte code can be executed in every platform that JVM(Java Virtual Machine) installed in. The object oriented programming style in Java is better than C++. C and C++ languages always needs compilers that is designed for specific platform. This causes risk for the speedly growing computer world. But, C++ is a language that game and system programmers still cannot give up with. Our Project team is experienced in both of the languages. But, after all this comparisons for the reason Project will be developed under eBox platform and the need of low-level programming the chosen programming language is C++. But, after putting together Project components and necessary operating system is chosen, last decision in programming language will be taken.

The operating system that will be used in Project is Windows CE because of the reason that host platform is eBox. Windows CE(Compact Edition) is an operating system that is developed for embedded devices. As opposite the general thought, Windows CE is not a Windows desktop family operating system with reduced utilites, it is a desperate operating system. For example to embedded operating systems Windows XP Embedded can be given. But,

candidate operating system Windows CE can not run Windows desktop applications due to platform and framework diffrences. But, by using the correct .net framework version application development at Windows CE is not su much diffrent from developing other desktop applications. Even at mobile phones this applications can be used by just compiling for the right platform at Visual Studio 2005. For this, a free version .net framework 2.0, Windows CE emulator and express edition of Visual C++ can be downloaded from internet.

Windows CE and Windows NT have much resemblances in the mean of utilities. Both of the operating systems can be used under 32-bit operating systems. Windows CE can be used under x86, ARM, MIPS,SH3/4 and power PC and Windows NT can be used under x86 competible platforms.

The software requirements and operating system can freely be obtained.

6.2.Feasibility of Hardware and Cost

1- LapTop (Datron)

- Processor : Intel® Duo 1.83 GHz 2 MB 533 MHz L2 cache memory
- Memory : 2 GB DDR2 667 MHz
- Display Adapter : 160 GB 5400 rpm SATA
- Network Adapter : 10/100 Ethernet Intel Pro/Wireless 2200BG Network

CD-RW/DVD-ROM, 15.1" TFT screen, Turkish keyboard

2- LapTop (Asus)

- Processor : Intel® Duo P8600 2.43 GHz 3 MB 533 MHz L2 cache memory
- Memory : 3 GB DDR2 667 MHz
- Display Adapter : ATI Mobility Radeon HD 3470 VRAM:256 MB
- Network Adapter : 10/100/1000 Mbps Intel Pro/Wireless 2200BG Network

CD-RW/DVD-ROM 15.4” TFT screen, Turkish keyboard

3- eBox-2300

- Processor : Vortex86 (System-on-Chip)(Fanless)
- Memory : Onboard 128MB SDRAM
- VGA : Shared System Memory Area 8MB
- Flash Memory : Support 32MB up to 2GB
- USB : 3 Connectors (USB 1.1) 2x at front, 1x at back
- I/O : RS-232 Port x 2

  RJ-45 Ethernet Connector

  External 6-pin Mini DIN for PS2 keyboard and mouse

  Mini PCI socket x 1

  Enhaced IDE interface, 44-pin box header x 1

This project will be actualized by above mentioned computers. These features for the computer were enough for developing. Necessary research and test processes were done. Datron that has these qualifications costs 789 USD and Asus costs 1280 USD.

The eBox will be provided us by the Yıldız Technical University at no charge.

The mini LCD monitor costs 65 USD.

The mini keyboard costs 15 USD.

The fingerprint reader costs 85 USD.

Total cost of the all hardware components is 2234 USD.

6.2.1.Analyze Of Fingerprint Sensors And Advantages

We will use a fingerprint reader but the type of it is important according to project type and requirements. Every application has different requirements and each type of sensor has its specific advantages and disadvantages. The following criteria can assist in reaching an answer:

- Costs
- Degree of maturity
- Image quality in sub optimal conditions
  - indoor/outdoor

  - personal/public use
  - normal/abnormal fingers
  - dry/moist fingers
- Size
- Sensitivity against vandalism
- Temperature resistance
- Sensitivity against forgery
- ESD (electrostatic discharge) sensitivity

Requirement	**Type of sensor currently best**
• Low costs	Capacitive silicon line sensor
• High level of development	Optical reflexive sensor
• High image quality	Optical reflexive sensor
• Small size	Thermal/capacitive line sensor
• High vandalism protection	Optical transmissive sensor
• High temperature span	Capacitive silicon sensor
• High forgery protection	Optical transmissive sensor
• High ESD strength	Optical reflexive sensor

6.2.2. Analyze Of Area Sensors VS Stripe Sensors

In our project we also thought about sensors type and we analyzed these two type. With area sensors, the finger to be recognized has to be placed on the sensor statically while for merchantable stripe sensors, also known as strip, swipe, or slide sensors, the same finger area has to be moved (swiped) actively over the sensor stripe.

- Since semiconductor stripe sensors need significantly less sensor cells than area sensors, their chip area and hence their price can be correspondingly lower.
- Although state-of-the-art stripe sensors are insensitive to slow, fast, or uneven finger motion, more training is needed than for area sensor to reach familiar low false rejection rates. For that reason, stripe sensors are recommended for applications with regular sensor use.

- Most area sensors allow a faster authentication as stripe sensors, if the whole process is considered.
- Due to their functional principle, stripe sensors are unsusceptible to latent image attacks and thus don't need software countermeasures which may increase false rejection rate.
- Area sensors generally have a lower current consumption than stripe sensors due to their significantly lower reading speed.
- Together with a suitable mechanical finger guide, stripe sensors, in comparison to area sensors, require a higher spoofing effort for attacks based on mechanical fingerprint copies.
- Stripe sensors expect an active cooperation of the user. In certain applications this may reduce the danger of accidental authentications, e.g., by unintentionally touching the sensor.
- Because of their low space requirement, stripe sensors are especially suited to very small devices.
- Stripe sensors are self-cleaning to a higher extent than area sensors.

The decision whether the properties of a sensor type are favorable or unfavorable thus mostly depends on the requirements of a dedicated application. As a result, it cannot be fixed globally. As a rule, one may assume that swipe sensors rather offer security while area sensors tend to ease of use. In this project we selected area sensors to use because of its easy use.

6.3.Feasibility of Time

Technical feasibility and gather required information.....8 days

Gathering required hardware components.....10 days

Arranging data structure.....3 days

Training and practicing about Windows CE, and use of components.....8 days

Software developing in .NET framework.....35 days

Test processes.....4 days

Reporting and preparation to project presentation.....2 days

This project is supposed to be completed in 70 days by two software developer. During these time each developer will work 4 hour in each day. Wages per hour is 5 USD and so total cost for two developer is 2800 USD.

6.4.Total Cost

Workforce Cost : 2800 USD

Hardware Cost : 2234 USD

Software Cost : 0 USD

Total Cost : 4034 USD

6.5.Legal Feasibility

There is no inconvenience for the system that will be developed.

7.Scenario And Work Flow

At this project we developed a software and hardware system that consists of the parts following; Secugen's Hamster Plus fingerprint reader, host computer and a software that manages attendance checking operation. Each part of this project were put together carefully to make sure every piece of them works correctly. Parts of this project is explained here;

- **Host PC:** This is a PC that Mobile Presence Checker software running on. This computer needs some extra functionalities to handle our operation. First of all, Secugen's Hamster Plus device driver software must be installed on this computer. This driver software introduces fingerprint reader device to host computer. And also; fingerprint capture, extracting and matching shared sources (dlls) must be registered to operating system with regsvr system utility. After each of this operations has been completed, the fingerprint reader must be plugged into host computer. Then, system is completed and ready to use.

- **Fingerprint Reader:** After researching for a fingerprint reader running on Windows CE for a long time, researches showed our project team that only convenient fingerprint reader was Secugen's Hamster Plus. Hamster plus is one touch reader (There are two kind of fingerprint scanners. One of them scans user's fingerprint with just one touch. This is called one touch fingerprint scanner. Other type's name is sliding touch fingerprint reader. With this reader user can scan his/her fingerprint image by sliding his/her finger on device up to down). This one touch reader, scans fingerprint images with minimum ratio of error.

- **Mobile Presence Checker:** This software is designed to make attendance checking operation for lessons. As it will be detailed at the following pages, this software manages student information, teacher information, system administrator information, lesson information and student information of all lessons. Main structure was built on fingerprint operations. Roll Call (Attendance Checking) operation, Student, Teacher, Administrator registration is based on fingerprint records. Other information are listed here; Lesson registration, getting students of a lesson, attendance statistics, attendance mailing, attendance export to Excel.

7.1.Work Flow

Mobile Presence Checker has a main workflow which can be made step by step. Each step of this software is designed to rollback operation. The work flow is like this;

- The system comes with an administrator account and its password so that operations will be made.
- After buying the system user can register a new administrator account so that their personal information will be kept on a safe user.

Administrator Scenario – Register Teacher:

- Administrator logs on Mobile Presence Checker with his/her username and password or fingerprint.
- Administrator opens teacher registration window to register a new teacher.
- Administrator fills the required fields with new teacher's id, name, surname and password.
- Administrator gets three fingerprint samples from teacher by using three buttons at the bottom of form.
- Administrator clicks on register button to save teacher.

Administrator Scenario – Lesson Management:

- Administrator logs on Mobile Presence Checker with his/her username and password or fingerprint.
- Administrator opens Lesson Management window to manage lesson informations.
- If administrator wants to search for lessons;
    - Administrator writes Lesson fall information to search lessons. But, if admin wants to get a more specific lesson, s/he can fill in lesson code or (and) teacher code fields. If s/he fills all that fields only one specific lesson will turn back.
    - Searched lessons will be listed at the table below it.
    - If administrator wants to update lesson's information
        - s/he can update the area's value by just clicking and writing the new value. Then only clicking on delete button is enough.
    - If administrator wants to delete lesson's information.
        - s/he can delete information by just clicking the delete button.
    -
- If administrator wants to add a new lesson;
    - s/he must fill in all the fields that is in the insert new lesson box.
    - If there is no lesson with same lesson code, teacher code and fall lesson will be inserted.

Teacher Scenario – Lesson Attendance Management:

- Teacher logs on Mobile Presence Checker with his/her username and password or fingerprint.
- Teacher opens Lesson Attendance Management window to manage his lesson's attendance information.
- Teacher chooses the lesson that he wants to manage attendance information from the combobox at left corner of form.
- Teacher checks students the student that registered to his/her lesson's information. If s/he gets anything wrong, s/he can update students attendance information.
- s/he can delete a student from his/her lesson.
- s/he can add a new student by writing the new student's id at the box locating on right corner of the form.

Teacher Scenario – Roll Call:

- Teacher logs on Mobile Presence Checker with his/her username and password or fingerprint.
- Teacher opens Roll Call window to roll call students at the lesson.
- The teacher chooses the lesson name s/he wants to roll call from the combobox then click on "start roll call" button.
- The teacher leaves devices for students to let them give their attendance.
- First student, writes his/her student number then touches fingerprint sensor when form says "Device is ready".
- First student, leaves device for other students to give their attendance checked.
- Second students does the same thing and so on.

7.2.System Modules

Our system includes following modules.

- **Data Compression:** Data compression module is a module that manages data compression and decompression jobs that is needed for file processing. This module's main purpose is to reduce the size of data that will be stored on disk. And also with this compression process, no raw data will be stored on disk.
- **Data Encryption :** Data Encryption module is a module that manages data encryption and decryption jobs that is needed for file processing. This module's main purpose is to

store all the data in encrypted format so that noone will see and understand raw data by just reading the files under the Data folder at project.

- **Excel File Writer / Reader :** Excel File Writer module is a module that manages data to be send from Mobile Presence Checker to computer in a format that a teacher can easily understand. This module is used at sending user's attendance information to teacher at excel format. Also it does batch student registration job.
- **File Driver:** File driver is Mobile Presence Checker's most detailed class. At this class, all the file operations is handled. At general applications, data operations are made through SQL and a database server. Because of the fact that this project's main purpose is to do fingerprint operations at Windows CE operating system, project team designed a new file system to store, insert, update and delete various kinds of data. While designing this class basic SQL operations are implemented on files. Encryption and compression stuff is also done on this class.
- **Fingerprint :** Fingerprint data is stored as a byte array at system. One student has id, name, surname, fingerprint 1, fingerprint 2 information. So, a class is needed to both store, insert and update student, teacher and administrator information.
- **FreaderProcesses :** This class is intended to do all the fingerprint reader operations including opening device, closing device, capturing image, live capturing image, drawing image to a picturebox, fingerprint matching, verification, fingerprint parameters settings etc.
- **Lesson:** This class's main purpose is to manage lessons' information in many ways. First of all basic select, update, insert and delete operations are made here. In addition to them, attendance setting, full class attendance setting, getting teacher's lessons, getting maximum fall at the system, getting all the lessons at that fall etc.
- **LessonInfo:** This class is intended to manage data of students of a specific lesson. At the constructor of this class we determine the lesson's lesson code, teacher code and lesson fall. All this three parameters are enough for us to determine a lesson uniquely. Each lesson has its own lesson files so that all the students information are kept separately. At this class so many various student and lesson information can be taken at many formats.
- **Login:** Login class is a class that project's login functions are based on such as inserting a new user, deleting user, updating user's information and the most important login control.

- **Tables:** This class produces many kinds of data tables and datagridviews with the data that functions get via arraylist data parameters.

8. Information About Fingerprints And Sensors

Three types of features are available for biometric identification:

- Coarse features (loops, arch, whorls)
- Fine features (minutia)
- Pore structure

Coarse features have strong genotypic contributions and are suited for presorting during an identification with a very large data base. The minutia are predominantly randotypic in nature and cause most of the uniqueness in a fingerprint. Therefore, either directly or indirectly (in picture correlation procedures), almost all fingerprint systems examine minutia. Minutiae are the endings and the branchings of the finger lines. Because these follow a strong random pattern, they are the carriers of "uniqueness". Pore structure is seldom used, due to large fluctuations in the quality of the scanning procedure.

Individual fingers can be damaged permanently (e.g. with rare skin diseases) or temporarily (e.g., dirty or worn down from abrasion), which can hinder or render impossible the recording and analysis of a fingerprint. With good sensors and analysis software, the failure to enroll rate is around 5% for everyone. If office workers are exclusively considered, the failure to enroll rate falls to under 1%. If a wound is not too deep, the finger lines will fully regenerate to their original state. Deep cuts leave line forming scars, and should be recognized as such by good identification algorithms, thereby barely impairing the identification performance. Most systems offer the possibility to record a "substitute finger" in enrollment, so that a fingerprint authentication can still take place during the healing process.

8.1. Types of Fingerprints

All fingerprint sensors try to generate a digital picture of the finger surface. This picture normally has a pixel resolution of 500 DPI (Dot Per Inch). The picture generation can be different for every type of sensor.

Static Capacitive Sensor Type 1

Here, one electrode is responsible for each pixel and measures the capacity compared to the neighbor electrode/pixel (inter pixel measurement). The capacity, in turn, is dependent on the dielectric. If a pixel is on a groove (i.e. air), the capacity is substantially smaller than on a finger line (ridge). In this case, the dielectric is water, which is distinguished by a very high dielectric constant. The measurement of capacity is static in the sense that charging happens with fixed charge units and then voltage is measured. Practical systems are always a mix of type 1 and type 2.

Static Capacitive Sensor Type 2

Also here one electrode per pixel is used, but the capacity is measured between pixel and ground, whereby the conductivity of the fingers does not play an insignificant role. The capacity measurement is in principle the same as in type 1. Practical systems are always a mix between type 1 and type 2.

Dynamic Capacitive Sensor

Here the capacity is measured by AC voltage. Inter pixel and pixel to ground measures can also be used here.

Luminescent Capacitive Sensor

An electroluminescent foil with a transparent back electrode uses the finger at its front side as counter electrode. At the points where the finger ridges touch the foil surface, the field strength is largest, and, as a result, the light emission brightest. That way a glowing image of the ridge structure develops at the back side of the foil. This image may be acquired by a image sensor chip.

Optical Reflexive Sensor

The finger lies on a prism surface for example. Where the finger ridges touch the glass, a total reflection of light inside of the glass is disturbed. This will supply a picture of the finger lines to a camera chip.

Optical Scattering Sensor

Similar to the optical reflexive sensor the finger touches one surface of the prism. However, due to a changed light guidance and camera chip placement only the light scattered by the contacting finger ridges is received by the camera while all other light is absorbed by passing through the glass surface instead of being totally reflected. This way, a, inverse image with bright finger ridges and dark valleys is created.

Optical Transmissive Sensors with fiber optical plate

Here a suitable light source illuminates through the finger. The finger lies directly on a fiber optical plate, which, in turn is directly connected to a camera chip. The fiber optical plate ensures that the finger does not touch the camera chip, nevertheless the light arrives at the camera chip without losing focus.

Optical Contactless Sensor

The finger surface is directly acquired by a camera chip. The fingerprint area needs no contact to a plate.

Acoustic (Ultrasound) Sensors

Here a picture of the finger surface on the glass is recorded by very high frequency ultrasound (e.g., 50 MHz).

Pressure Sensitive Sensors

With pressure sensors, the pressure per pixel of the finger is measured.

Thermal Line Sensors

With these sensors, the finger is moved linearly over a narrow array of thermal sensors, similar to sensors for opening automatic doors on a larger scale. The thermal sensors register temperature differences over time, which vary between the finger lines and grooves.

Capacitive and Optical Line Sensors

These sensor arrays work similar to thermal line sensors. Instead of temperature differences of time, the single sensors cells measure the capacity or the light, respectively, to build the image.

8.2. The Uniqueness Of The Fingerprint

This is a working hypothesis which in the mathematical sense is difficult (if not impossible) to prove. The opposite is more provable, namely finding two identical fingers. Until now, no two fingerprints from different fingers have been found which are identical. This holds true even for identical twins, between right and left fingers and can be anticipated also for clones.

In a scientific sense, the term uniqueness has to be replaced by the probability to find two identical fingerprints from different fingers. This probability may be determined empirically by comparing all fingerprints of a forensic data base against each other. For example, if such a collection contains 100 million fingerprints, a probability of nearly 10^{-14} should be provable (due to inter-dependencies this probability is assumed to be higher but should lie below 10^{-6}). However, such a large trial has not yet been undertaken until today. Furthermore, the probability for misnaming fingerprints (fingerprints from the same person/finger are filed under different names) is supposed to be much higher. This experience is well known from experiments with much smaller collections. As a result, the outcome of such a trial may become quite questionable.

8.3.Applications Used With Fingerprint Authentication

This project is just an implementation of a scenario which was thought for student attendance. But besides this, there can be some alternative implementations of this. Following areas can be given example for fingerprint authentication.

- PC access.
- PC network access (internet, intranet)
- Access to rooms (key replacement).
- Safety on weapons: no access for children and other unauthorized users.
- Mobile phones: network access, theft protection, mobile financial transactions.

- ID: company pass, personal identification, club ID.
- Credit cards, bank cards, EC cards.
- Automobile: Seats, mirrors, temperature, and other personal settings .
- Automation of hotels (e.g., check-in and room access).
- Company vending machines (soft drinks) .
- Participation in sporting events.
- Memberships (discotheques, tanning salons, slot machines, video stores).
- Personal access to patient records.
- By governmental departments to track compatriots

8.4.Suitable Finger For Fingerprint Recognition

In principle, every finger is suitable to give prints for authentication purposes. However, there are differences between the 10 fingers, which are expressed in different performance for FAR (False Acceptance Rate), FRR(False Rejection Rates) and FTE(Failure to Enroll). These differences are based on:

- Different finger qualities (use, moisture)
- Different sizes
- Different ergonomics (e.g., systems ergonomically optimized for the thumb are only usable by other fingers with contortion)

Whereby the type of sensor also reacts in specific ways to these differences. In most cases one can assume that the **index finger** obtains the best performance regarding FAR and FRR.

9. Fingerprint Recognition Algorithm

Automatic and reliable extraction of minutiae from fingerprint images is a critical step in fingerprint matching. The quality of input fingerprint images plays an important role in the performance of automatic identification and verification algorithms.

Fingerprint based identification has been one of the most successful biometric techniques used for personal identification. Each individual has unique fingerprints. A fingerprint is the pattern of ridges and valleys on the finger tip. A fingerprint is thus defined by the uniqueness of the local ridge characteristics and their relationships. Minutiae points are these local ridge characteristics that occur either at a ridge ending or a ridge bifurcation. A ridge ending is defined as the point where the ridge ends abruptly and the ridge bifurcation is the point where the ridge splits into two or more branches. Automatic minutiae detection becomes a difficult task in low quality fingerprint images where noise and contrast deficiency result in pixel configurations similar to that of minutiae. This must be taken in account while developing applications on fingerprint recognition issue.

Whole steps of extraction algorithm is like following;

1. Pre-Processing
2. Minutiae extraction
3. Post-Processing

The figure shown deals with the first step called pre-processing and gives an insight into the process that has been followed for the enhancement of the input fingerprint image.

The next step deals with the extraction of minutiae. In the third step called post-processing, false minutiae are deleted from the set of obtained minutiae and hence the actual minutiae required for fingerprint matching are obtained. The following section gives the description of the steps followed in this project for the extraction of the actual minutiae.

9.1. Description of The Algorithm

9.1.1.Pre-Processing

1. The input image is segmented from the background which ensures the removal of noise. For this, the whole image is divided into blocks of size 16×16 and the variance of each block is computed. The variance is then compared with the threshold value. If the variance of a block is

less than the threshold value, then it is deleted from the original figure. This process is carried out for the whole image. The image obtained from the above step is then normalized to get the desired variance of the given image. The normalized image is given by where denotes the gray-level value at pixel (i, j), M and VAR denote the estimated mean and variance of respectively and denotes the normalized gray-level value at pixel (i, j) and are the desired mean and variance values respectively.

2. The estimation of the orientation of the image is then carried out as the next step. The whole image is divided into blocks of size 16×16 and the local orientation in the figure is computed by where θ(i, j) is the least square estimate of the local ridge orientation at the block centered at pixel (i, j).

3. The angles between the blocks are then smoothened by passing the image through a low pass filter.

4. The following method is adopted for the calculation of the frequency of the local blocks. X-signatures of each block are computed along the direction perpendicular to the orientation angle in each block. The window used for this purpose is of size 16×32. The frequency is then computed by the distance between the peaks obtained in the X-signatures.

In general, the frequency of image constitutes has a certain frequency for the hole image and hence the above step can be omitted if the global frequency of the given figure is known.

5. As the next step, each block is filtered along the direction of the orientation angle using the value of the frequency obtained for each block. A Gabor filter is used for this process and a suitable value of local variances is taken for carrying out the process of filtering. A Gabor filter takes care of both the frequency components as well as the spatial coordinates. The inputs required to create a Gabor mask are frequency, orientation angle and variances along x and y directions. Filtering is done for each block using the local orientation angle and frequency. Pre-processing of the image is completed by the steps as mentioned and the enhanced image is obtained.

9.1.2. Minutiae Extraction

The next step after enhancement of the image is the extraction of minutiae. The enhanced image is binarised first in this step. The skeleton of the image is then formed. The minutiae points are then extracted by the following method. The binary image is thinned as a result of which a ridge is only one pixel wide. The minutiae points are thus those which have a pixel value of one (ridge ending) as their neighbor or more than two ones (ridge bifurcations) in their neighborhood. This ends the process of extraction of minutiae points.

9.1.3. Post-Processing

The minutiae points obtained in the above step may contain many spurious minutiae. This may occur due to the presence of ridge breaks in the given figure itself which could not be improved even after enhancement. This results in false minutiae points which need to be removed. These unwanted minutiae points are removed in the post-processing stage. False minutiae points will be obtained at the borders as the image ends abruptly. These are deleted using the segmented mask. As a first step, a segmented mask is created. This is created during segmentation carried out in the stage of pre-processing and contains ones in the blocks which have higher variance than the threshold and zeros for the blocks having lower variance. This segmented mask contains all ones in the regions where the image is located and all zeros at the other places.

To know if a minutiae point is valid or not, a local window of size 11×11 is taken in the segmented mask at the location of the minutiae point and the total sum of the window is computed. If the sum is lesser than 121, then the point is invalid as it would be on the borders. If the sum is 121, it means that the point is not on the border and hence it has to be preserved. Thus, minutiae at the borders are removed preserving only those inside the figure. For the deletion of minutiae inside the figure which would occur due to ridge breaks, a window of size 11×11 is taken around each minutiae point keeping it at the centre of the window and then is checked for any other minutiae that lie in the block. If other minutiae exist in that block, all the minutiae in the block are deleted. Thus, the minutiae points resulting from ridge breaks are eliminated. Though this process helps in removing false minutiae, it also poses a risk of eliminating closely placed minutiae points even though they are real.

EXPERIMENTAL RESULTS (Images obtained in each step carried out)

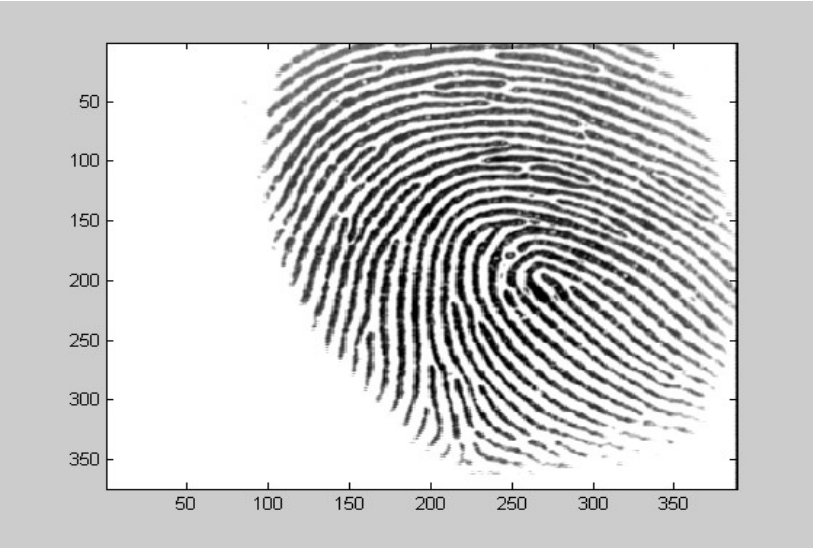

Image 9.1. Original Fingerprint Image

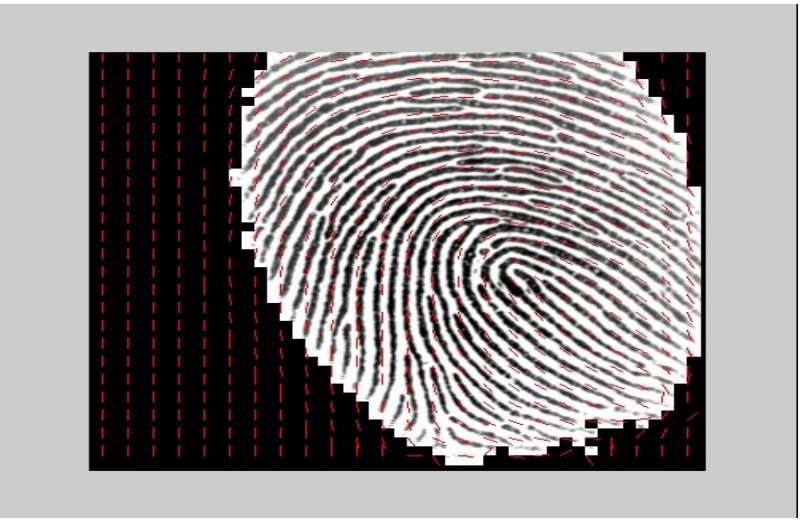

Image 9.2. Segmented Image along with the orientation field

Image 9.3. Normalized Image

Image 9.4. Gradient along x – direction

Image 9.5. Gradient along y – direction

Image 9.6. Enhanced Image after Gabor Filtering

Image 9.7. Binary Output

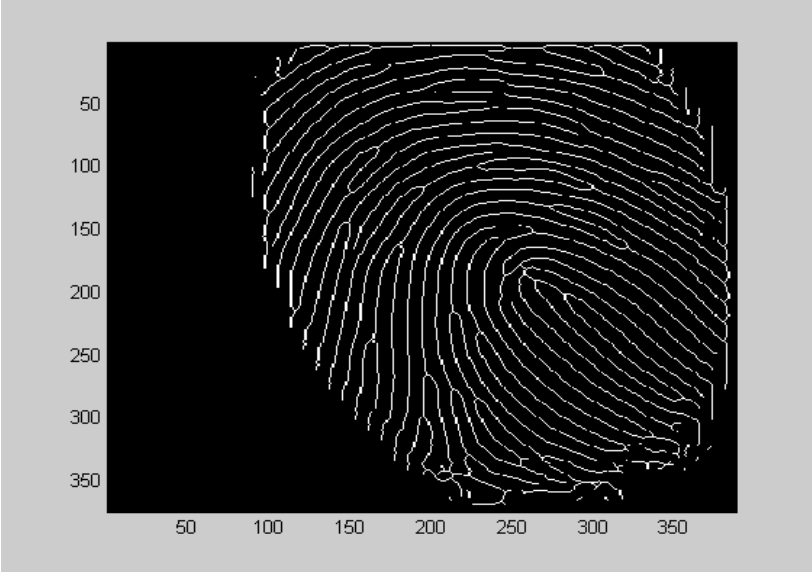

Image 9.8. Thinned Binary Output

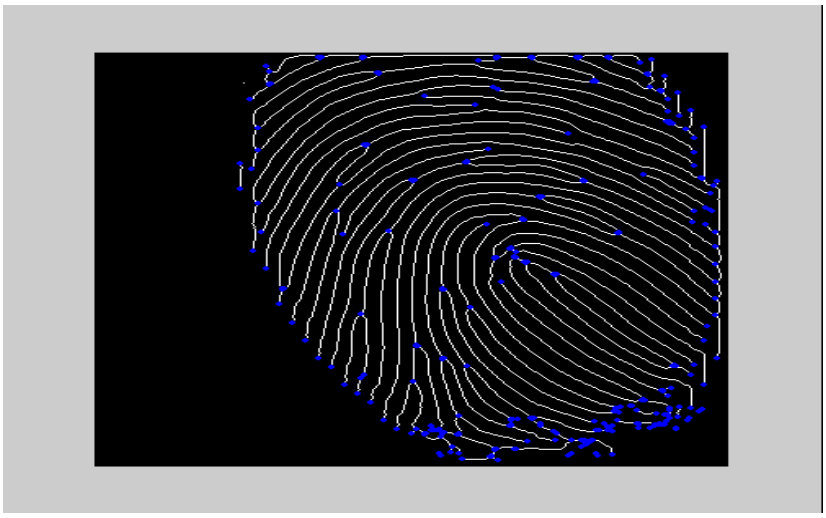

Image 9.9. Thinned Binary along with all the minutiae

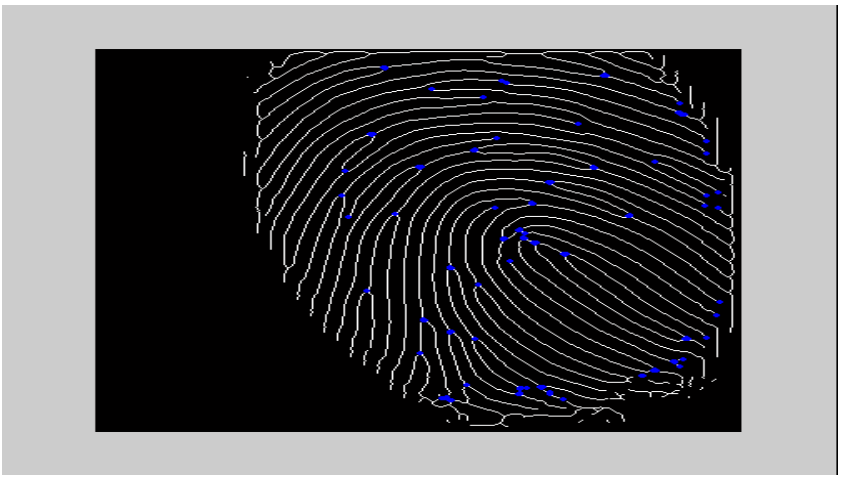

Image 9.10. Minutiae obtained after deleting spurious minutiae at the borders

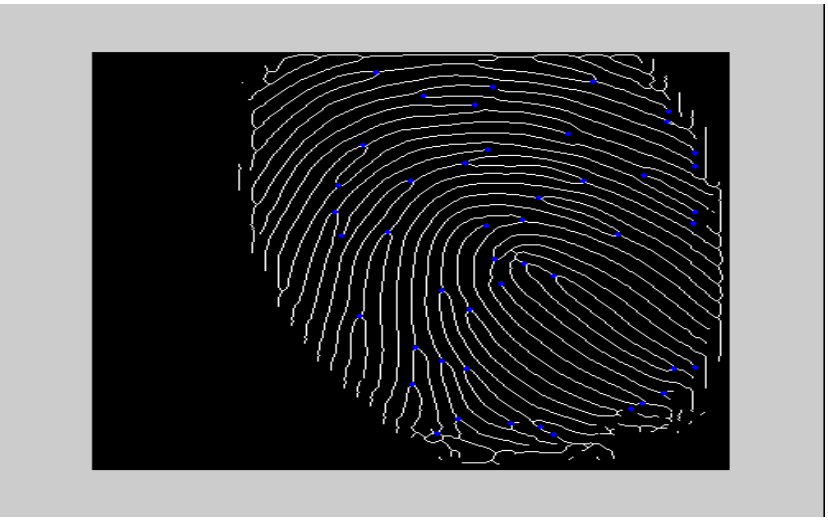

Image 9.11. Final extracted Minutiae after applying the windowing technique

9.2. Conclusions of the Algorithm

The main benefit of this algorithm is its fast running speed. It improves the verification performance too. The algorithm identifies the unrecoverable corrupted areas in the fingerprint and removes them from further processing. This is an important aspect of the algorithm as the presence of these areas would prove to be extremely harmful for the extraction of minutiae points. It helps in removing the spurious minutiae too which may also prove to be harmful in matching fingerprints correctly.

10.Conclusion

The presence checking system that we offer will be first in the world and make this process automatically. If we consider the available systems to realize that process, using mobile finger print reader for checking presence will be more useful than any others. Our system will have the features of mobility, reusability, using in various scenarios (like in conference halls and in meeting places), high security and reliability. If it can be possible to produce it in series production, we believe that it will find wide usage area in many sectors.

11.Sources

1-) www.embeddedpc.net

2-) www.secugen.com

3-) http://msdn.microsoft.com/en-us

4-) http://dotnet.sys-con.com

5-) http://blogs.msdn.com/mikehall/

6-) http://whitepapers.zdnet.com/abstract.aspx

7-) http://en.wikipedia.org/wiki/Wiki

8-) FINGERPRINT IMAGE ENHANCEMENT AND MINUTIAE EXTRACTION
NIMITHA CHAMA
Dept. of Electrical & Computer Engineering
Clemson University

12.Resumes

Name Surname	:	Uygar ER
Birth Date	:	01.07.1987
Birthplace	:	İzmir
High School	:	2001 - 2005 Buca Anadolu Lisesi
Internships	:	Bıçakçılar Tıbbi Cihazlar A.Ş. - İstanbul - (5 week)
		SmartSoft Information Technologies – İstanbul – (8 week)

Name Surname	:	Engin ÖZER
Birth Date	:	16.11.1987
Birthplace	:	İstanbul
High School	:	2001 - 2005 Hüseyin Avni Sözen Anadolu Lisesi
Internships	:	Türk Telekom - İstanbul - (4 week)
		Can Elektronik – İstanbul – (4 week)
		Garanti Teknoloji - İstanbul – (6 week)