

Fingerprint Recognition System Using Arduino

Ashish Ernest Rahul

Software Engineer, Department of Embedded Technology, Vellore Institute of Technology, Vellore, India

Abstract: Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

We are going to attempt to build a working model of a fingerprint recognition system using Arduino which can be used for authentication.

Keywords: fingerprint recognition

1. Introduction

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges. These are sometimes referred to as "Chanced Impressions".

Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster. Fingerprint analysis, in use since the early 20th century, has led to many crimes being solved.

2. System hardware design

The whole system is composed by following parts: a fingerprint capturing sensor, Arduino microprocessor to run fingerprint recognition programs on it.



Fig. 1. Basic work flow

A. Main processing chip

Arduino is an open-source hardware and software company, project and user community that designs and manufactures single-board micro-controllers and micro-controller kits for building digital devices and interactive objects that can sense and control objects in the physical and digital world. Its products are licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL), permitting the manufacture of Arduino boards and software distribution by anyone. Arduino boards are available commercially in preassembled form or as do-it-yourself (DIY) kits.

Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards or breadboards (shields) and other circuits. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs from personal computers. The micro-controllers are typically programmed using a dialect of features from the programming languages C and C++. In addition to using traditional compiler toolchains, the Arduino project provides an integrated development environment (IDE) based on the Processing language project.

The Arduino project started in 2003 as a program for students at the Interaction Design Institute Ivrea in Ivrea, Italy, aiming to provide a low-cost and easy way for novices and professionals to create devices that interact with their environment using sensors and actuators. Common examples of such devices intended for beginner hobbyists include simple robots, thermostats and motion detectors.

B. Interfaces

Most Arduino boards consist of an Atmel 8-bit AVR micro-controller (ATmega8, ATmega168, ATmega328, ATmega1280, ATmega2560) with varying amounts of flash memory, pins, and features. The 32-bit Arduino Due, based on the Atmel SAM3X8E was introduced in 2012. The boards use single or double-row pins or female headers that facilitate

connections for programming and incorporation into other circuits. These may connect with add-on modules termed shields. Multiple and possibly stacked shields may be individually addressable via an I²C serial bus. Most boards include a 5 V linear regulator and a 16 MHz crystal oscillator or ceramic resonator. Some designs, such as the LilyPad, run at 8 MHz and dispense with the onboard voltage regulator due to specific form-factor restrictions

C. Camera interface

The fingerprint sensor module used in this project is R307 Model which is shown in the Figure 3. This is a finger print sensor module with TTL UART interface for direct connections to the Arduino micro-controller or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. A level converter (like MAX232) is required for interfacing with PC serial port.

Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks

The fingerprint sensor can be wired as below. Do not follow color code of connector provided.

The corner pin is +5V as shown below in red line, then is Ground (GND), Then TXD which goes to MCU's RX-IN, and last pin is RXD which goes to MCU's TX-OUT pin.

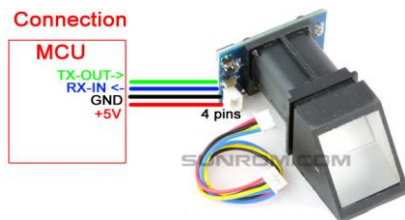


Fig. 2. Finger module

The Fig. 2, shows how to interface the sensor with the Arduino Micro-controller.

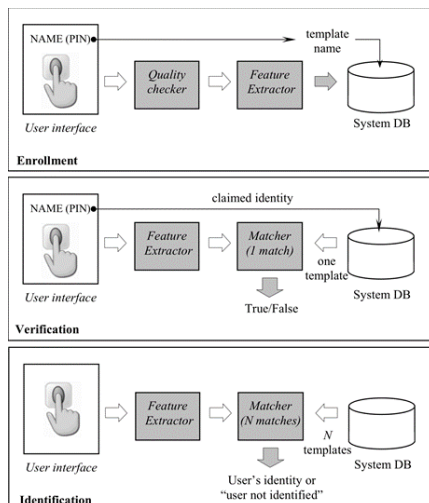


Fig. 3. System block diagram

D. Arduino board

Arduino micro-controllers are pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory. The default bootloader of the Arduino UNO is the optiboot bootloader. Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor–transistor logic (TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header. Other variants, such as the Arduino Mini and the unofficial Boarduino, use a detachable USB-to-serial adapter board or cable, Bluetooth or other methods. When used with traditional micro-controller tools, instead of the Arduino IDE, standard AVR in-system programming (ISP) programming is used.

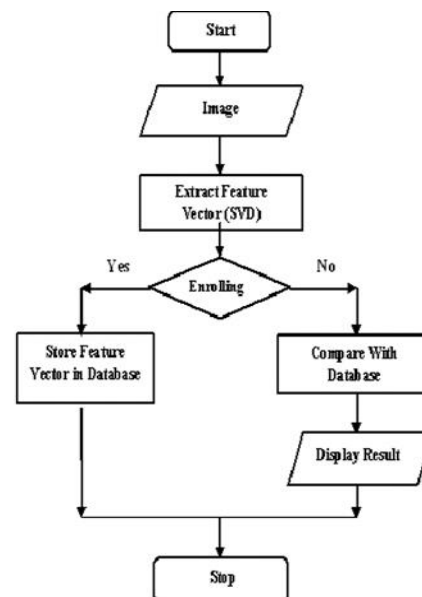


Fig. 4. Block diagram of approach

The Arduino board exposes most of the micro-controller's I/O pins for use by other circuits. The Diecimila, Duemilanove, and current Uno provide 14 digital I/O pins, six of which can produce pulse-width modulated signals, and six analog inputs, which can also be used as six digital I/O pins. These pins are on the top of the board, via female 0.1-inch (2.54 mm) headers. Several plug-in application shields are also commercially available. The Arduino Nano, and Arduino-compatible Bare Bones Board and Boarduino boards may provide male header pins on the underside of the board that can plug into solder-less breadboards.

Many Arduino-compatible and Arduino-derived boards exist. Some are functionally equivalent to an Arduino and can be used interchangeably. Many enhance the basic Arduino by

adding output drivers, often for use in school-level education, to simplify making buggies and small robots. Others are electrically equivalent but change the form factor, sometimes retaining compatibility with shields, sometimes not. Some variants use different processors, of varying compatibility.

3. Working of the project

A. Capture and detection

Fingerprint image acquisition is considered to be the most critical step in an automated fingerprint authentication system, as it determines the final fingerprint image quality, which has a drastic effect on the overall system performance. There are different types of fingerprint readers on the market, but the basic idea behind each is to measure the physical difference between ridges and valleys.

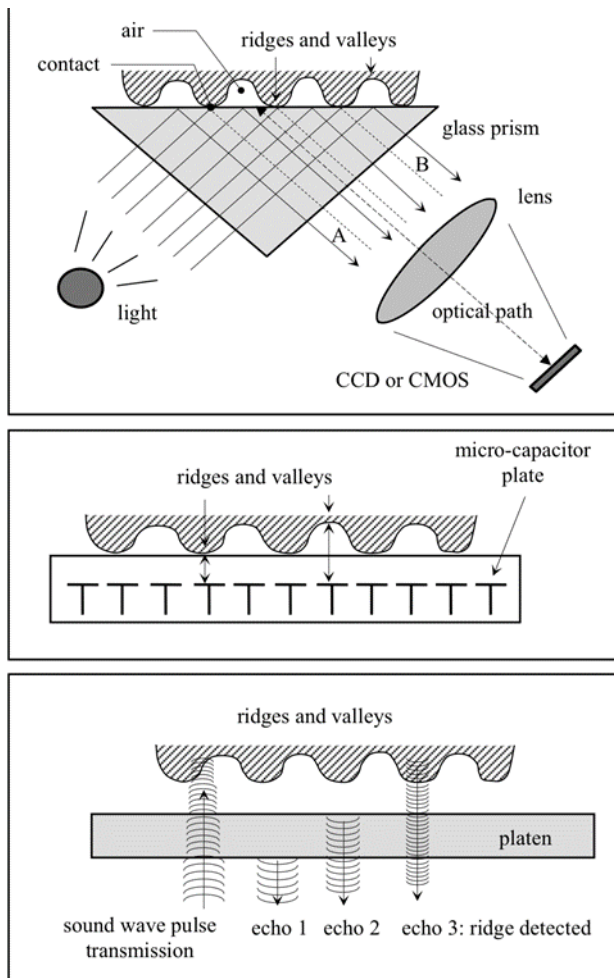


Fig. 5. a) FTIR-based optical fingerprint sensing; b) capacitive sensing; c) the basic principle of the ultrasound technique

All the proposed methods can be grouped into two major families: solid-state fingerprint readers and optical fingerprint readers. The procedure for capturing a fingerprint using a sensor consists of rolling or touching with the finger onto a sensing area, which according to the physical principle in use

(optical, ultrasonic, capacitive or thermal) captures the difference between valleys and ridges. When a finger touches or rolls onto a surface, the elastic skin deforms. The quantity and direction of the pressure applied by the user, the skin conditions and the projection of an irregular 3D object (the finger) onto a 2D flat plane introduce distortions, noise and inconsistencies in the captured fingerprint image. These problems result in inconsistent and non-uniform irregularities in the image. During each acquisition, therefore, the results of the imaging are different and uncontrollable. The representation of the same fingerprint changes every time the finger is placed on the sensor plate, increasing the complexity of any attempt to match fingerprints, impairing the system performance and consequently, limiting the widespread use of this biometric technology.

In order to overcome these problems, as of 2010, non-contact or touchless 3D fingerprint scanners have been developed. Acquiring detailed 3D information, 3D fingerprint scanners take a digital approach to the analog process of pressing or rolling the finger. By modelling the distance between neighboring points, the fingerprint can be imaged at a resolution high enough to record all the necessary detail.

A fingerprint is the reproduction of a fingertip epidermis, produced when a finger is pressed against a smooth surface. The most evident structural characteristic of a fingerprint is a pattern of interleaved ridges and valleys; in a fingerprint image, ridges (also called ridge lines) are dark whereas valleys are bright. Ridges and valleys often run in parallel, sometimes they bifurcate and sometimes they terminate.

B. Fingerprint recognition

Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

1) Patterns

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

- Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- Whorl: Ridges form circularly around a central point on the finger.

Scientists have found that family members often share the

same general fingerprint patterns, leading to the belief that these patterns are inherited.

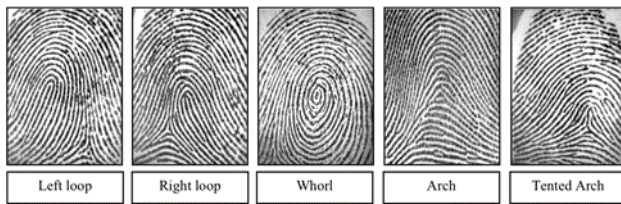


Fig. 6. One fingerprint from each of the five major classes

2) Fingerprint processing

Fingerprint processing has three primary functions: Enrolment, searching and verification. Among these functions, enrolment which captures fingerprint image from the sensor plays an important role. A reason is that the way people put their fingerprints on a mirror to scan can affect to the result in the searching and verifying process. Regarding to verification function, there are several techniques to match fingerprints such as correlation-based matching, minutiae-based matching, ridge feature-based matching and minutiae-based algorithm. However, the most popular algorithm was minutiae based matching algorithm due to its efficiency and accuracy.

3) Minutiae features

The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

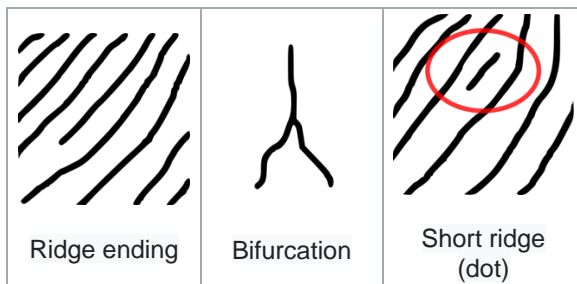


Fig. 7. Features

C. Algorithms

Matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared.

1) Pre-processing

Pre-processing helped enhancing the quality of an image by filtering and removing unnecessary noises. The minutiae based algorithm only worked effectively in 8-bit gray scale fingerprint image. A reason was that an 8-bit gray fingerprint image was a

fundamental base to convert the image to 1-bit image with value 0 for ridges and value 1 for furrows. As a result, the ridges were highlighted with black color while the furrows were highlighted with white colour. This process partly removed some noises in an image and helped enhance the edge detection. Furthermore, there are two more steps to improve the best quality for the input image: minutiae extraction and false minutiae removal. The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges. As a result, the thinned ridges of the fingerprint image are marked with a unique ID so that further operation can be conducted. After the minutiae extraction step, the false minutiae removal was also necessary. The lack of the amount of ink and the cross link among the ridges could cause false minutiae that led to inaccuracy in fingerprint recognition process.

2) Pattern-based (or image-based) algorithms

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images can be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

3) Direct Matching

In this matching, the input and template images are read, the matching is performed by comparing the two images pixel wise.

4) Minutiae Based Matching

This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Most common minutiae matching algorithms consider each minutia as a triplet $m = \{x, y, \theta\}$ that indicates the x, y minutia location coordinates and the minutia angle θ :

$$\mathbf{T} = \{\mathbf{m}_1, \mathbf{m}_2, \dots, \mathbf{m}_m\}, \quad \mathbf{m}_i = \{x_i, y_i, \theta_i\}, \quad i = 1..m$$

$$\mathbf{I} = \{\mathbf{m}'_1, \mathbf{m}'_2, \dots, \mathbf{m}'_n\}, \quad \mathbf{m}'_j = \{x'_j, y'_j, \theta'_j\}, \quad j = 1..n$$

where m and n denote the number of minutiae in \mathbf{T} and \mathbf{I} , respectively. A minutia m'_j in \mathbf{I} and a minutia m_i in \mathbf{T} are considered "matching," if the spatial distance (sd) between them is smaller than a given tolerance r_0 and the direction difference (dd) between them is smaller than an angular tolerance θ_0 :

$$sd(\mathbf{m}'_j, \mathbf{m}_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0,$$

$$dd(\mathbf{m}'_j, \mathbf{m}_i) = \min(|\theta'_j - \theta_i|, 360^\circ - |\theta'_j - \theta_i|) \leq \theta_0.$$

The tolerance boxes (or hyper-spheres) defined by r_0 and θ_0 are necessary to compensate for the unavoidable errors made by

feature extraction algorithms and to account for the small plastic distortions that cause the minutiae positions to change.

Aligning the two fingerprints is a mandatory step in order to maximise the number of matching minutiae. Correctly aligning two fingerprints certainly requires displacement (in x and y) and rotation (θ) to be recovered, and likely involves other geometrical transformations like scale and specific distortion-tolerant geometrical transformations. Let $map(\cdot)$ be the function that maps a minutia m'_j (from I) into m''_j according to a given geometrical transformation; for example, by considering a j displacement of $[\Delta x, \Delta y]$ and a counterclockwise rotation θ around the origin:

$$map_{\Delta x, \Delta y, \theta}(m'_j = \{x'_j, y'_j, \theta'_j\}) = m''_j = \{x''_j, y''_j, \theta'_j + \theta\}, \quad \text{where}$$

$$\begin{bmatrix} x''_j \\ y''_j \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x'_j \\ y'_j \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}.$$

Let $mm(\cdot)$ be an indicator function that returns 1 in the case where the minutiae m''_j and m_i match according to the previous equations:

$$mm(m''_j, m_i) = \begin{cases} 1 & sd(m''_j, m_i) \leq r_0 \quad \text{and} \quad dd(m''_j, m_i) \leq \theta_0 \\ 0 & \text{otherwise.} \end{cases}$$

Then, the matching problem can be formulated as:

$$\text{maximize}_{\Delta x, \Delta y, \theta, P} \sum_{i=1}^m mm(map_{\Delta x, \Delta y, \theta}(m'_{P(i)}), m_i),$$

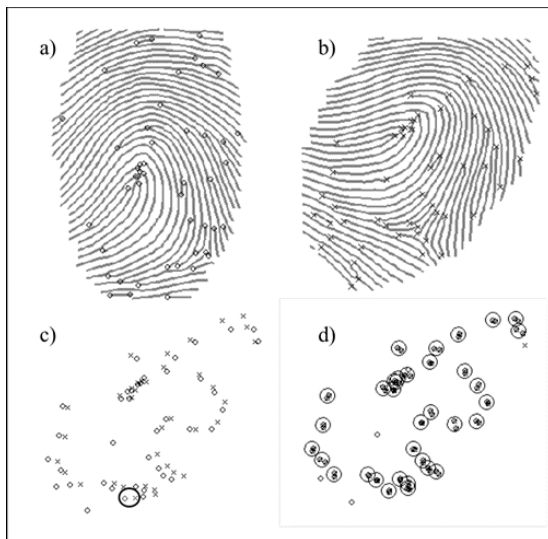


Fig. 8. Minutiae matching by the Chang et al. approach. Figures a) and b) show the minutiae extracted from the template and the input fingerprint, respectively; c) the minutiae are coarsely superimposed and the principal pair is marked with an ellipse; d) each circle denotes a pair of minutiae as mated by the algorithm

where $P(i)$ is an unknown function that determines the pairing between I and T minutiae; in particular, each minutia has either exactly one mate in the other fingerprint or has no mate at all:

1. $P(i) = j$ indicates that the mate of the m_i in T is the

minutia m'_j in I;

2. $P(i) = \text{null}$ indicates that minutia m_i in T has no mate in I;
3. A minutia m'_j in I, such that $\forall i=1..m, P(i) \neq j$ has no mate in T;
4. $\forall i=1..m, k=1..m, i \neq k \Rightarrow P(i) \neq P(k)$ or $P(i) = P(k) = \text{null}$ (this requires that each minutia in I is associated with a maximum of one minutia in T)

5) Ratio of Relational Distance Matching

The methodology is to obtain the common minutiae point set (minutiae points present in both the base and the input image). The prime purpose of this phase is to find the number of common minutiae points available in a pair of fingerprint images. Given two fingerprint images with 'N1' and 'N2' identified minutiae points respectively (where N1 need not be equal to N2), this phase outputs the 'M' common minutiae points, which would be available in both the images. Effectively, if N1 represents the set of minutiae points in image 1 and N2 represents the set of minutiae points in image 2, M would be the intersection of N1 and N2 ($M = N1 \cap N2$). There is a new term called the 'M (i) - tuple' to represent information about a minutiae that would identify it uniquely among the set of all minutiae. The M (i) - tuples of a pair of minutiae can be compared/matched to find if they both are the same or not. When two images with identified minutiae points are given as input, the algorithm considers one image to be the base image (BM) and the other image to be the input image (IM). Either of them can be BM or IM and vice versa.

6) M(I) - Tuples in base image (BM):

For each minutiae $i = 1$ to $N1$, the 5 nearest minutiae points are found. This is done by calculating the Euclidean Distances from the 'i'th minutiae point to all the other minutiae points in the set N (BM) and noting down the 5 nearest minutiae points with respect to Euclidean Distances. If i_1, i_2, i_3, i_4 and i_5 are the 5 nearest minutiae points of i , then we calculate M (i) - tuple in the following way: (a) Calculate distances $i - i_1, i - i_2, i - i_3, i - i_4$, and $i - i_5$. Note that distance ' $i - i_N$ ' means the Euclidean Distance between the points i and i_N . So here, distance $i - i_1$ means the Euclidean distance between minutiae point i and i_1 and so on. (b) Find the following 10 ratios $(i - i_1) : (i - i_2), (i - i_1) : (i - i_3), (i - i_1) : (i - i_4), (i - i_1) : (i - i_5), (i - i_2) : (i - i_3), (i - i_2) : (i - i_4), (i - i_2) : (i - i_5), (i - i_3) : (i - i_4), (i - i_3) : (i - i_5), (i - i_4) : (i - i_5)$. Based on this procedure the algorithm finds the match between two fingerprint images.

4. Fingerprint sensors

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, MEMS. This is an overview of some

of the more commonly used fingerprint sensor technologies.

Optical

Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized type of digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) which captures a visual image of the fingerprint. A scratched or dirty touch surface can cause a bad image of the fingerprint. A disadvantage of this type of sensor is the fact that the imaging capabilities are affected by the quality of skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it is possible for an individual to erode the outer layer of skin on the fingertips to the point where the fingerprint is no longer visible. It can also be easily fooled by an image of a fingerprint if not coupled with a "live finger" detector. However, unlike capacitive sensors, this sensor technology is not susceptible to electrostatic discharge damage. Fingerprints can be read from a distance.

A. Ultrasonic

Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint. Unlike optical imaging, ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint. This eliminates the need for clean, undamaged epidermal skin and a clean sensing surface. LeEco became the first company to introduce this in Smartphone.

B. Capacitance

Capacitance sensors use principles associated with capacitance in order to form fingerprint images. In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric. Apple's Touch ID uses a capacitance fingerprint sensor.

C. Passive capacitance

A passive capacitance sensor use the principle outlined above to form an image of the fingerprint patterns on the dermal layer of skin. Each sensor pixel is used to measure the capacitance at that point of the array. The capacitance varies between the ridges and valleys of the fingerprint due to the fact that the volume between the dermal layer and sensing element in valleys contains an air gap. The dielectric constant of the epidermis and the area of the sensing element are known values.

The measured capacitance values are then used to distinguish between fingerprint ridges and valleys.

D. Active capacitance

Active capacitance sensors use a charging cycle to apply a voltage to the skin before measurement takes place. The application of voltage charges the effective capacitor. The electric field between the finger and sensor follows the pattern of the ridges in the dermal skin layer. On the discharge cycle, the voltage across the dermal layer and sensing element is compared against a reference voltage in order to calculate the capacitance. The distance values are then calculated mathematically, and used to form an image of the fingerprint. Active capacitance sensors measure the ridge patterns of the dermal layer like the ultrasonic method. Again, this eliminates the need for clean, undamaged epidermal skin and a clean sensing surface.

5. Fingerprint sensor in electronic devices

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezo resistive, ultrasonic, piezoelectric, MEMS. This is an overview of some of the more commonly used fingerprint sensor technologies.

6. Results

This example shows how to automatically detect a fingerprint using feature extraction. The approach in this example can register and recognize a fingerprint even when a person tilts his or her finger, or presses lightly or vigorously against the scanner.

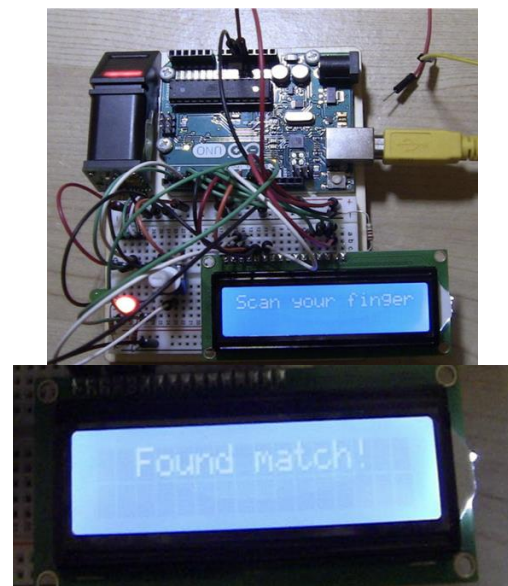


Fig. 9. Fingerprint detected

7. Future applications

Recent developments in fingerprint scanners have focused on reducing both their cost and size. Although lower cost and size are essential to enable a wide deployment of the technology in civilian applications, some of these developments have been made at the expense of fingerprint image quality (e.g., dpi resolution, etc.). It is very likely that while the market will continue to drive down scanner prices, it will also require higher-quality products at the same time. Manufacturers will continue to innovate low-cost small-size scanner designs, but they will also take care that their products deliver high quality-images of large areas of the finger.

Robust extraction of fingerprint feature remains a challenging problem, especially in poor quality fingerprints. Development of fingerprint-specific image processing techniques is necessary in order to solve some of the outstanding problems. For example, explicitly measuring (and restoring or masking) noise such as creases, cuts, dryness, smudginess, and the like will be helpful in reducing feature extraction errors. Algorithms that can extract discriminative non-minutiae-based features in fingerprint images and integrate them with the available features and matching strategies will improve fingerprint matching accuracy. New (perhaps, model-based) methods for computation (or restoration) of the orientation image in very low-quality images is also desirable to reduce feature extraction errors.

Most of the fingerprint matching approaches introduced in the last four decades are minutiae-based, but recently

correlation-based techniques are receiving renewed interest. New texture-based methods have been proposed and the integration of approaches relying on different features seems to be the most promising way to significantly improve the accuracy of fingerprint recognition systems.

8. Conclusion

It's a progress of realizing embedded image capturing system. We describe our design method in this paper. Based on these methods, we design the experimental prototype of the embedded fingerprint capturing and recognition system with Arduino system. This system is smaller, lighter and with lower power consumption. Because of the open source code, it is freer to do software development on Linux. Experimental results show that it's an effective method of using Raspberry Pi board to actualise embedded image capturing system.

References

- [1] D. Ashok Kumar, T. Ummal Sariba Begum, "A Comparative Study On Fingerprint Matching Algorithms For EVM", JCSA Journal Of Science And Education Publishing, Vol. 1, Issue 4, April 2013.
- [2] [G. Senthilkumar, K. Gopalakrishnan and V. Sathish Kumar, "A Tutorial on Fingerprint Recognition", Biometric Sytem Laboratory. <http://bias.csr.unibo.it/research/biolab>.
- [3] "Fingerprint And Forensic Science", https://en.wikipedia.org/wiki/Fingerprint#Capture_and_detection
- [4] wiki/Fingerprint#Capture_and_detection
- [5] Łukasz WIĘCŁAW "A minutiae-based matching algorithms in fingerprint recognition systems", Journal of Medical Informatics & Technologies, vol. 13, 2009.