Photodiode-Based Fingerprint Sensor

Dissanayake D.M.M.L.
Department of Electrial and Electronic Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e21109@eng.pdn.ac.lk

Firdous M.T.
Department of Electrial and Electronic Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e21139@eng.pdn.ac.lk

Samarakoon S.M.O.T.
Department of Electrial and Electronic Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e21345@eng.pdn.ac.lk

I. Introduction

Fingerprint recognition stands out as a leading biometric identification technology due to its reliability, convenience, and rapid authentication capabilities. With advancements from traditional ink-based methods to modern optical, capacitive, and ultrasonic systems, fingerprint sensing has found diverse applications in mobile devices, security systems, and identity verification. This paper introduces a photodiode-based optical fingerprint sensor designed for high precision, speed, and environmental adaptability. The proposed design addresses challenges like contamination sensitivity and resolution limitations, offering a compact, low-power, and scalable solution for biometric systems. The main objectives of the fingerprint sensor are to accurately capture the unique ridge and valley patterns of a fingerprint, ensuring precise detection of the physical structure.

II. Literature review

Biometric identification is the process of recognizing individuals based on their unique physiological or behavioral traits, offering a secure and reliable alternative to traditional methods like passwords or ID cards. The concept of biometrics dates back to the 19th century, with fingerprints being systematically used for identification by Sir Francis Galton in the 1880s. This foundational work led to the development of automated systems in the mid-20th century, with significant advancements in the late 20th and early 21st centuries due to the rise of digital technologies and artificial intelligence.

Modern biometric systems utilize features such as fingerprints, facial structures, iris patterns, and voice characteristics, which are inherently unique to each individual. These systems are now widely adopted in applications ranging from smartphone security and financial transactions to border control and public safety. Despite their advantages, biometric identification systems face challenges, including vulnerabilities to spoofing, environmental factors, and concerns regarding data privacy.

A. Facial recognition

Facial recognition identifies or verifies individuals by analyzing unique facial features. It often uses algorithms to map points like chin shape, creating templates for comparison with stored images in controlled databases, such as for access control. Various technologies exist, including 3-D, vascular and heat-pattern, and skin texture analysis for this. When a person approaches a scanner, their live image is matched to the database, enabling actions like opening doors or logging into networks. This technology, leveraging cameras and AI algorithms like Convolutional Neural Networks (CNNs), offers a contactless solution for tasks like attendance and access control in offices or schools. While highly accurate in controlled settings (over 95%), challenges like lighting, poses, and occlusions (e.g., masks, glasses) can impact performance. Recent AI advancements have improved reliability and efficiency, making it increasingly seamless and effective.[3]

1) Performance Metrics:

- Input Image Resolution: Typically, 224x224 pixels for models like ResNet or MobileNet.
- Response Time: Less than 1 second on modern GPUs for high-quality images.
- Accuracy: Over 98% in controlled environments; around 85-95% in real-world settings.
-

2) Hardware Requirements:

- Cameras with at least 720p resolution for data collection.
- Edge devices like NVIDIA Jetson Nano or cloud-based GPUs for model inference.

Fig. 1

B. Fingerprint Recognition

Fingerprints, ridge and valley patterns on the tip of a human finger, are one of the most important biometric characteristics due to their known uniqueness and persistence properties. Fingerprint-based attendance systems use sensors such as optical or capacitive scanners to capture and analyze the unique ridge and valley patterns of a fingerprint. Optical sensors use light reflection to create high-resolution images, while capacitive sensors detect electrical differences caused by skin contact. These systems are highly accurate, with matching accuracy exceeding 98% under optimal conditions. Their compact design and affordability make them widely popular in personal and organizational use. However, they can be affected by external factors such as dirty, wet, or worn fingerprints, which may reduce performance. Maintenance and regular cleaning of sensors are essential for consistent operation.

1) Performance Metrics:

- Image Resolution: Typically, 500 DPI (dots per inch), as per FBI PIV standards.
- Response Time: Less than 0.5 seconds for image capture and matching.
- Lifetime: Over 1 million touches for robust sensors.

2) Hardware Requirement

- Optical or capacitive sensors (e.g., CrossMatch or SecuGen).
- Low-power microcontrollers (e.g., ARM Cortex-M series) for local matching.

Fig. 2 - CrossMatch Fingerprint Scanner

C. Iris Recognition

Iris recognition systems use Near-Infrared (NIR) cameras to capture the highly detailed and unique patterns of an individual's iris. The iris is translated into a digital code because it is distinctive. Since age spots and discoloration on the iris are likely, a black and white image is used.[4] The history of iris recognition technology dates back to the mid-20th century, but its practical application began in the late 1980s and early 1990s. The concept of using the iris for biometric identification was first proposed by ophthalmologist Leonard Flom and engineer Aran Safir in the 1960s. However, it wasn't until the 1980s that significant advancements in computer vision and image processing enabled the development of practical iris recognition systems. Today, iris recognition technology continues to evolve, with ongoing advancements in hardware and software contributing to its improved accuracy, speed, and reliability. These patterns are analyzed using algorithms like Gabor filters, enabling an accuracy level with an Equal Error Rate (EER) below 0.1%, making it one of the most precise biometric methods. Ideal for high-security attendance systems in industries or institutions requiring stringent accuracy, iris recognition is resistant to environmental variables like lighting or age-related changes. However, the need for specialized hardware and a stable image capture process may pose usability challenges in fast-paced or casual settings.

1) Performance Metrics:

- Wavelength Range: 850 nm is common for most iris scanners.
- Resolution: 640x480 pixels or higher for detailed iris images.
- Response Time: 0.5-2 seconds, depending on environmental conditions.
- Accuracy: Equal Error Rate (EER) below 0.1%, making it one of the most precise modalities.

2) Hardware Requirements:

- Specialized NIR cameras (e.g., Iris ID or IriTech).
- Infrared LEDs for uniform illumination.

Fig. 3 - Iris ID iCAM TD100A Iris Scanner

D. Comparison

TABLE 1

Feature	Facial Recognition	Fingerprint Recognition	Iris Recognition
Accuracy	Medium to High (85-99%)	High (95-99%)	Very High (98-99.9%)
Recognition Time	Less than 1 second	Less than 0.5 seconds	1 to 2 seconds
Environmental Factors	Affected by lighting, pose, and expression variations	Minimal impact, but dirt or wet fingers can interfere	Minimal, except for occlusions (e.g., glasses, eyelashes)
Security Level	Medium	High	Very High
Ease of Use	Very easy (no contact needed)	Easy (contact required)	Moderate (requires proper positioning)
Hardware Cost	Moderate to High	Low to Moderate	High
Data Storage Size	Moderate (Facial templates)	Small (Fingerprint templates)	Moderate to Large (Iris patterns)
Resistance to Spoofing	Low to Medium (vulnerable to photos, masks)	Medium to High (vulnerable to high-quality molds)	High (difficult to replicate iris patterns)
Application Areas	Mobile phones, surveillance, access control	Attendance systems, banking, access control	Border control, high-security facilities
User Acceptance	High (widely used and familiar)	High (familiar and non-intrusive)	Moderate (considered invasive by some users)

E. Principle of Operation

1) Convolutional Neural Networks (CNNs) – Facial Recognition

The system starts by feeding facial images from a dataset into a convolutional neural network (CNN), which extracts features through multiple layers (conv1 to conv5). These convolutional layers capture hierarchical information, starting with basic patterns like edges and progressing to complex facial features, while pooling layers (pool1 and pool3) reduce the spatial dimensions to retain essential details. Simultaneously, SIFT (Scale-Invariant Feature Transform) is applied to the images, beginning with the construction of the Difference of Gaussians to detect key points. These key points are then refined by identifying their precise locations, scales, and orientations. Using these key points, SIFT and RITF eigenvectors are calculated to extract robust, transformation-invariant features. Finally, the features extracted by the CNN and SIFT are fused into a single, comprehensive feature vector, which is passed through fully connected layers for classification. This hybrid approach enhances facial recognition by combining CNN's automated feature learning with the robustness of SIFT's key point-based features.[1]

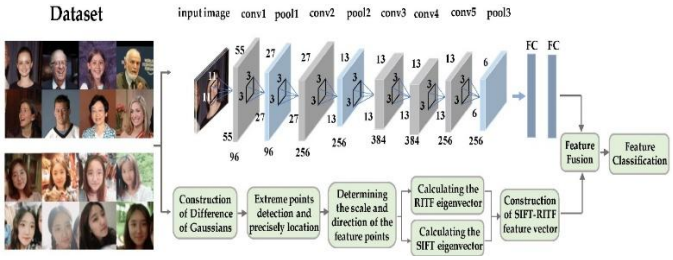

Fig. 4 - The schematic diagram of SR-CNN model, combining the rotation-invariant texture feature (RITF) vector, the scale-invariant feature transform (SIFT) vector, and the convolution neural network (CNN).

2) Optical – Fingerprint Recognition

Friction ridges on palms and fingertips form unique patterns that leave latent fingerprints due to oils, moisture, and dead cells. Optical fingerprint sensors capture these patterns by illuminating the fingertip placed on a glass surface with an LED. Light reflects differently depending on whether it contacts fingerprint ridges or valleys. Ridges, which touch the glass, reflect more light directly to a CMOS or CCD image sensor, while valleys, which do not touch, scatter light and appear darker. This contrast generates a detailed fingerprint image. Advanced models enhance this process with Total Internal Reflection (TIR) techniques, where ridges and valleys interact differently with light due to variations in reflective indices, causing Frustrated Total Internal Reflection (FTIR). The captured high-contrast image is processed to extract unique ridge and valley patterns for authentication.

Fingerprint scanners perform two processes: enrollment and matching. During enrollment, the fingerprint is scanned, confirmed, and stored as a predefined template in the scanner's flash memory. Matching involves comparing a new scan to stored templates. In 1:1 matching, the scan is compared to a specific fingerprint ID, while in 1: N matching, it is compared against all stored templates. Advanced sensors may also include anti-spoofing measures to ensure accuracy and security.[2]

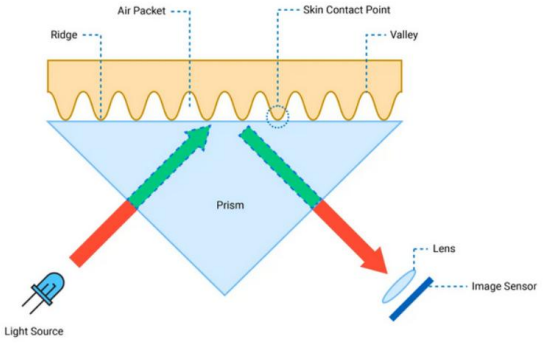

Fig. 5

3) Near-Infrared (NIR) – Iris Recognition

Near-Infrared (NIR) iris recognition utilizes near-infrared light to capture detailed images of a person's iris, the textured, colored ring around the pupil. The NIR light, typically emitted by LEDs, minimizes glare and penetrates the cornea to highlight the intricate patterns of the iris, which are unique to each individual. A specialized camera records the high-resolution image. Image preprocessing techniques remove noise caused by eyelashes, reflections, and shadows, which is then processed to extract distinctive features such as furrows, rings, and crypts. These features are encoded into a biometric template for comparison against stored templates, A common metric is the Hamming Distance, which measures the number of differing bits between two binary templates. A lower Hamming Distance indicates a closer match, ensuring secure and accurate authentication. NIR illumination makes iris recognition effective even in low-light conditions or for individuals with dark-colored irises.

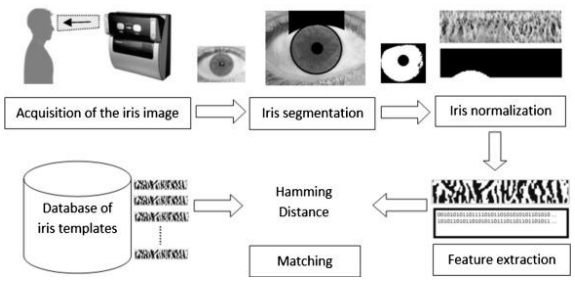

Fig. 6

III. Methods

A. Direct Reflection with Photodiode Array

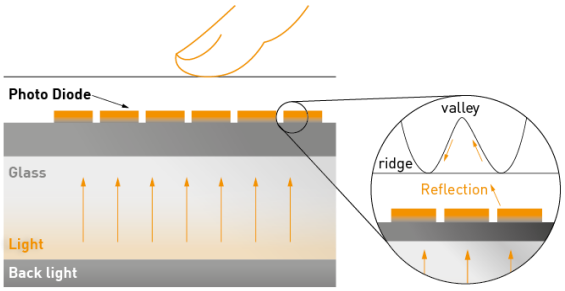

Fig. 7

Direct reflection fingerprint sensors use a photodiode array to take a picture of a fingerprint. Photodiodes are light-sensitive semiconductors that generate an electrical current when exposed to light. The finger is illuminated by a light source, and the distinctive ridge and valley pattern of the fingerprint reflects different intensities of light. Ridges reflect more light while the valleys reflect less or scatter light. The photodiode array then measures this reflected light and produces a 2D array of intensity values. Each value in the array represents the light intensity at a specific point, measured by a photodiode. Also, amplifiers are used to amplify the weak signals produced by photodiodes to obtain more precise patterns. This 2D data from photodiodes are then converted to grayscale image by mapping the intensity values from the photodiodes to pixel values in an image. Key elements, like ridge patterns and minute details, are then extracted from the collected image for comparison and identification.

1) Advantages :

- Smaller in size and possess a greater resolution.
- Photodiodes consume very little power, making them suitable for portable or battery-operated devices.

2) Challenges :

- The finger must come into complete contact with the surface in order to interfere with the light source.
- Photodiodes are susceptible to noise from ambient light, electromagnetic interference, and variability in light source intensity.
- The system's effectiveness depends on the consistent alignment of the photodiode array and the finger.

B. Optical Fiber Sensor

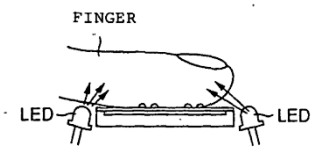

Fig. 2

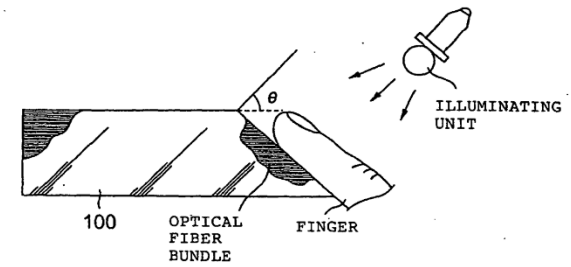

Fig. 8

This fingerprint sensing technique uses a Fiber Optic Plate (FOP) which involves in placing a finger on the upper surface of the FOP while illuminating it at an angle with diffused light. The Fiber Optic Plate (FOP) consists of array of optical fibers. The ridges of the finger make direct contact with the FOP, while the valleys remain separated by an air gap. As a result, the ridges scatter the light, preventing it from reaching the CCD or CMOS sensor beneath the FOP. In contrast, near the valleys, the light undergoes total internal reflection at the FOP-air boundary and is transmitted to the CCD/CMOS sensor [5,9].

1) Advantages :

- Reduces the thickness of the sensor arrangement.
- Optical fiber sensors can work with different light sources, enabling better performance in various environmental conditions

2) Challenges :

- High manufacturing cost due to the optical fibers.
- Optical fiber sensors can work with different light sources, enabling better performance in various environmental conditions

C. Capacitive

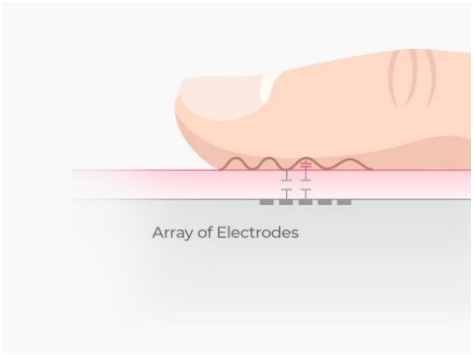

Fig. 9

Capacitive fingerprint sensors use a two-dimensional array of micro-capacitor plates integrated into a single chip. The skin of the finger acts as the opposing plate for each micro-capacitor[9]. When a finger is placed on the sensor's surface, small electrical charges are generated between the surface of the finger and the micro-capacitor plates. While these sensors offer a compact design with a smaller imaging area, size, and resolution, they tend to be more expensive than optical sensors of comparable size and image quality due to the cost of the capacitive components[5].

$$Capacitance(C) = \frac{ka}{d}$$

$$\frac{dQ}{dt} = c\frac{dV}{dt}$$

In this system, dQ/dt represents the change in charge over time, and dv/dt denotes the change in voltage over time. The capacitance C varies with the distance d, while constants k and a remain fixed. Since the charge Q can be preset by charging the capacitor to a known value, any change in C, caused by the distance of ridges (closer) or valleys (farther) from the capacitor plate, will result in a corresponding change in the capacitor voltage v[6]. By measuring the voltage output changes over time at each capacitor in the sensor array, a fingerprint image can be generated.

1) Advantages :

- Composed of smaller imaging area, size and resolution.
- Possess the ability of adjusting some electrical parameters to deal with non-ideal skin conditions (wet and dry fingers).

2) Challenges :

- With the long term use, sensor surface becomes dirty and a parasitic capacitance is formed between the dirt and the plate. As a result the sensed capacitance will increase.

D. Thermal

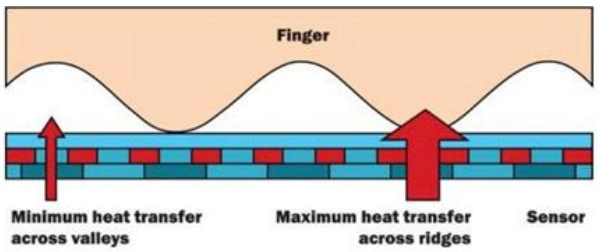

Fig. 10

The silicon die used in thermal fingerprint sensors is made up of pixels formed of pyroelectric material, which is extremely sensitive to temperature changes [5]. These sensors measure the heat transfer from the sensor to the fingerprint after scanning the surface of the finger.

The fingerprint's ridges, which come into direct touch with the sensor, remove heat faster than the air-insulated valleys. The sensor can produce a fingerprint pattern because of the discernible temperature difference between ridges and valleys caused by this disparity in heat flow [7]. The matching signal is produced when a finger is put on the sensor, causing a discernible change in temperature. The sensors are typically maintained at a high temperature by electrically heating them up [9]

1) Advantages :

- Can adapt to a thick protective coating because the heat can easily propagate through the coating.
- Not sensitive to electrostatic discharge.

2) Challenges:

- Typically consume more power than other technologies.
- Less accurate in environments where the temperature difference is not that high between the ridges and the valleys.

E. Ultrasonic

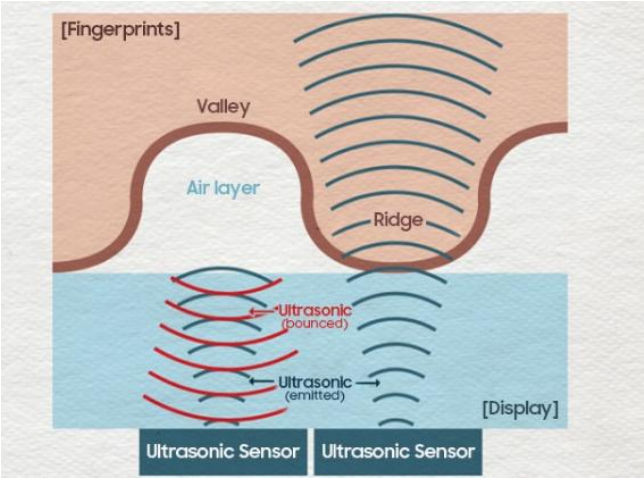

Fig. 11

A biometric authentication feature known as an ultrasonic fingerprint sensor builds a three-dimensional (3D) model of a user's fingerprint using sound waves. When a finger is put on the sensor, an inaudible ultrasonic pulse is released. The fingerprint's ridges and valleys reflect sound waves, and the sensor records the echo to provide a three-dimensional mode[8]. When these echo back to be received by the receiving transducer, they form a unique print composed of ridges and sweat pores from the dermis. The reflection is then converted into digital format by the microprocessor and stored as a template for future comparison.

1) Advantages :

- Ultrasonic recognition technology is unaffected by surface clutter and can penetrate the dead skin layer to reflect the fingerprint pattern.
- Can obtain information from within the tissue.

2) Disadvantages :

- Mechanical parts are quite expensive.
- Takes more time to acquire an image.

IV. Specifications

1. Resolution: 250 DPI (Dots Per Inch)

Justification: A lower resolution is sufficient for general attendance purposes, where extreme precision is not required. This also reduces cost and processing power requirements.

2. Scanning Area: 0.8 cm x 0.8 cm
Justification: A smaller scanning area captures enough of the fingerprint for basic identification, making the sensor more compact and affordable.

3. Sensor Type: Basic Photodiode Array

Justification: A simple and cost-effective photodiode array can capture the contrast between ridges and valleys for basic fingerprint patterns, suitable for a university environment.

4. Light Source: Single Infrared LED

Justification: A single infrared LED provides adequate illumination for capturing fingerprints while minimizing costs and power consumption.

References

[1] Y.-X. Yang, C. Wen, K. Xie, F.-Q. Wen, G.-Q. Sheng, and X.-G. Tang, "Face Recognition Using the SR-CNN Model," *Sensors*, vol. 18, no. 12, p. 4237, Dec. 2018, doi: https://doi.org/10.3390/s18124237.

[2] N. Agnihotri, "How to enroll and match fingerprint templates with Adafruit and R30X fingerprint scanner," *Engineers Garage*. https://www.engineersgarage.com/arduino-adafruit-r30x-r307-fingerprint-scanner/

[3] "How Facial Recognition Works: Everything You Need to Know," *swiftlane.com*.https://swiftlane.com/blog/how-facial-recognition-works/

[4] "iris recognition system - an overview | ScienceDirect Topics," *www.sciencedirect.com.* https://www.sciencedirect.com/topics/computer-science/iris-recognition-system

[5] S. Memon, M. Sepasian, and W. Balachandran, "Review of finger sensing technologies," in *IEEE INMIC 2008: 12th IEEE International Multitopic Conference - Conference Proceedings*, 2008, pp. 226–231. doi: 10.1109/INMIC.2008.4777740.

[6] J.-M. Nam, S.-M. Jung, and M.-K. Lee, "Design and implementation of a capacitive fingerprint sensor circuit in CMOS technology," Sensors and Actuators A: Physical, vol. 135, no. 1, pp. 283–291, Mar. 2007, doi: https://doi.org/10.1016/j.sna.2006.07.009.

[7] A. Ross and A. Jain, "Biometric Sensor Interoperability: A Case Study in Fingerprints," Biometric Authentication, pp. 134–145, 2004, doi: https://doi.org/10.1007/978-3-540-25976-3_13.

[8] Y. Yu, Q. Niu, L. Xiaoshi, J. Xue, W. Liu, and D. Lin, "A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications," *Micromachines (Basel)*, vol. 14, no. 6, pp. 1253–1253, Jun. 2023, doi: https://doi.org/10.3390/mi14061253.

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London: Springer London, 2009. doi: https://doi.org/10.1007/978-1-84882-254-2.