**LITERATURE REVIEW**

**Introduction to Biometric Identification**

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.

**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]

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

**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.

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



CrossMatch Fingerprint Scann

**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 systemsToday, 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.

* **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.
* **Hardware Requirements**:
  + Specialized NIR cameras (e.g., Iris ID or IriTech).
  + Infrared LEDs for uniform illumination.



Iris ID iCAM TD100A Iris Scanner

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 keypoints. These keypoints are then refined by identifying their precise locations, scales, and orientations. Using these keypoints, 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 keypoint-based features.[1]

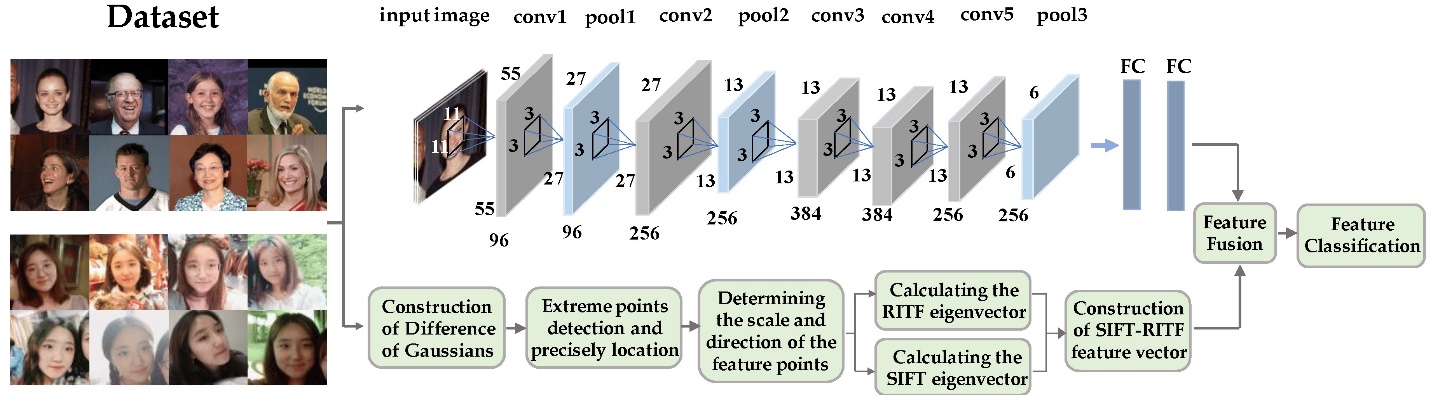
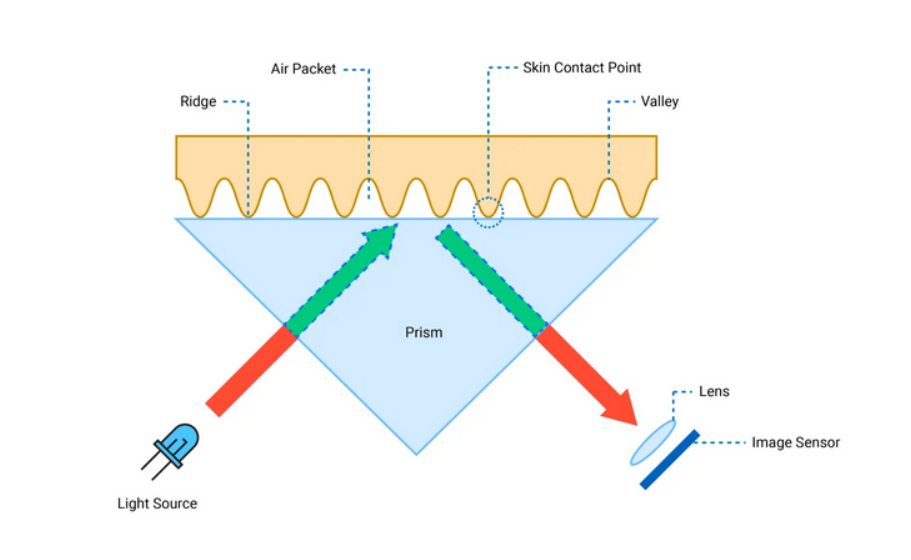


Figure 1. The schematic diagram of SR-CNN model, combining the rotation-invariant texture feature (RITF) vector, the scale-invariant feature transform (SIFT) vector, and the convolution neural network (CNN).

#### **2. Optical – Fingerprint Recognition**

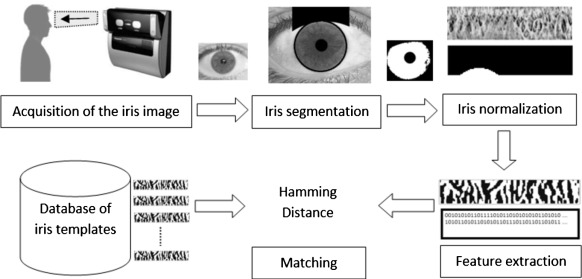
Friction ridges on palms and fingertips form unique patterns that leave latent fingerprints due to oils, moisture, and dead cells. Optical fingerprint sensors capture these patterns by illuminating the fingertip placed on a glass surface with an LED. Light reflects differently depending on whether it 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]



#### **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.

‌

**Comparison**

| **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) |

1)<https://www.mdpi.com/1424-8220/18/12/4237>

2)<https://www.engineersgarage.com/arduino-adafruit-r30x-r307-fingerprint-scanner/>

3)<https://swiftlane.com/blog/how-facial-recognition-works/>

4)<https://www.sciencedirect.com/topics/computer-science/iris-recognition-system>

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |