

# Fingerprint Identification Using Filter bank Technique

Cong-Anh Hoang<sup>1</sup>, Huu-Vinh Dang<sup>1</sup>

<sup>1</sup> Faculty of Technology and Engineering, Hai phong University, Haiphong, Viet Nam

Date of Submission: 25-03-2025

Date of Acceptance: 05-04-2025

**ABSTRACT:** Fingerprint recognition technology, a branch of biometrics, utilizes unique fingerprint characteristics to verify identity. Evolving from manual fingerprinting methods to digital scanning, this technology is now widely applied in security, finance, healthcare, and mobile devices. Modern fingerprint sensors can scan beneath the epidermal layer, enhancing accuracy and anti-spoofing capabilities. Notably, the Filterbank technique improves fingerprint feature extraction using spatial-frequency filters, optimizing noise resistance and enabling recognition even with low-quality images. With cloud computing integration, this technology continues to advance, offering superior security and exceptional convenience.

**KEYWORD:** Filterbank, Hai Phong University, Fingerprint identification.

## I. INTRODUCTION

Biometric technology utilizes physiological or behavioral characteristics to authenticate personal identity and is considered a highly reliable authentication method. Among biometric modalities, fingerprint recognition has the longest history of application, particularly in forensic science, due to its proven uniqueness and permanence. Fingerprint recognition systems primarily rely on minutiae matching for detailed feature analysis. The rapid advancements in computer science and electronic engineering have significantly reduced the cost of fingerprint recognition systems, expanding their applications beyond forensics to civil sectors such as passports, mobile devices, ATMs, and driver's licenses.[1]

In this study, the author collected a database of 100 fingerprint images for experimentation. The processing steps included histogram equalization and grayscale normalization, fingerprint code (Finger Code) computation, and the application of the FilterBank technique to identify specific fingerprints within the dataset.

## II. FINGERPRINT IDENTIFICATION AND DECODING SYSTEM

### 1. Fingerprint Identification System

The fingerprint recognition system is an advanced biometric solution widely applied in security, access control, and identity verification. The system operates through a sequential processing workflow consisting of the following key steps:

- Data Acquisition: Fingerprint images are captured using specialized sensors or retrieved from a database.

- Image Processing: Image processing algorithms, such as histogram equalization, noise filtering, and contrast enhancement, are applied to optimize input data quality.

- Feature Extraction: The system analyzes and extracts key biometric features, including ridge endings, bifurcation points, ridge frequency, and orientation.

- Matching and Identification: Extracted features are compared with database samples to determine identity or grant access authentication.[2]

The system operates in two primary modes:

- Verification Mode (1:1): A one-to-one comparison between the input fingerprint and a pre-registered sample, requiring prior identity information.

- Identification Mode (1:N): A one-to-many comparison where the input fingerprint is matched against the entire database to determine identity without user-provided information.

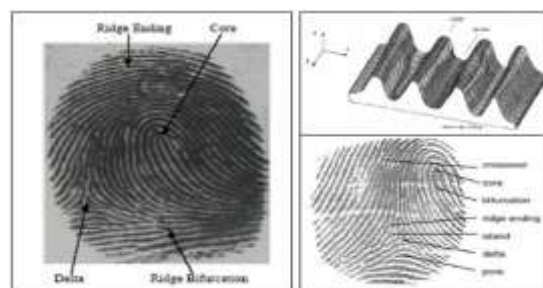


Figure 1. Fingerprint Image

## 2. FINGERPRINT DECODING

Fingerprint patterns are formed by ridges and grooves on the fingertip surface. These ridges typically run parallel but can also create distinct shapes (Figure 1).

When a ridge suddenly terminates, the point is referred to as a "ridge ending"; if a ridge splits into two branches, it is called a "bifurcation point." These ridge endings and bifurcations, collectively known as "minutiae," play a crucial role in fingerprint recognition. A high-quality fingerprint generally contains between 60 and 80 minutiae points, though this number may vary depending on the fingerprint.

Each fingerprint must be analyzed based on its core characteristics. The morphology of the core allows fingerprints to be classified into six types: plain arch (a), tented arch (b), right loop (c), left loop (d), whorl (e), and double loop (f), as illustrated in Figure 2.

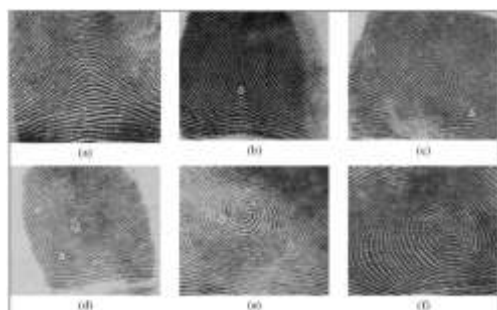


Figure 2. Major Fingerprint Types

### Fingerprint Decoding Methods

- Correlation-Based Method: This approach directly compares the input fingerprint image with the registered template using alignment techniques and evaluates the correlation between the two images.

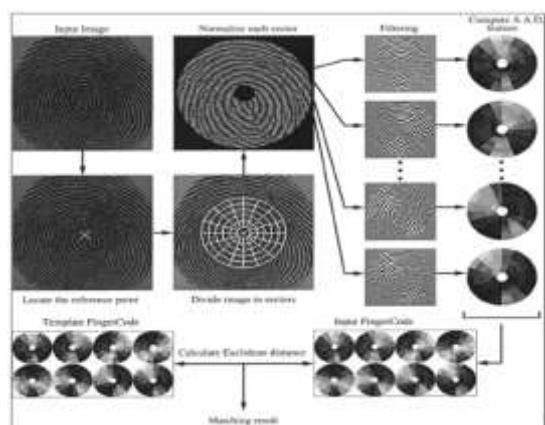


Figure 3. Filterbank Technique Based on Fingerprint Fusion

- Minutiae-Based Method: This method extracts and marks key biometric features such as ridge endings and bifurcation points. Matching is performed by analyzing the spatial relationships and patterns of these minutiae points.

- Filterbank Method:[3] This technique analyzes fingerprints based on spatial frequency, orientation, and phase. It employs filters to extract feature information and performs matching based on the structural patterns in the frequency domain.

## 3. FINGERPRINT RECOGNITION BASED ON FILTERBANK

There are four main steps in the FilterBank-based fingerprint recognition algorithm (Figure 3):

### a. Region of Interest (ROI) Extraction:

- In a fingerprint image, not all regions contain useful information. Some areas may be noisy, blurred, or lack clear fingerprint features (e.g., image edges or regions degraded due to poor scanning).

- The Region of Interest (ROI) in a fingerprint image consists of all areas surrounding key reference points. Each region is computed within specific radius and angle constraints. The boundary delineation of this extracted region follows a honeycomb grid pattern (Figure 4).



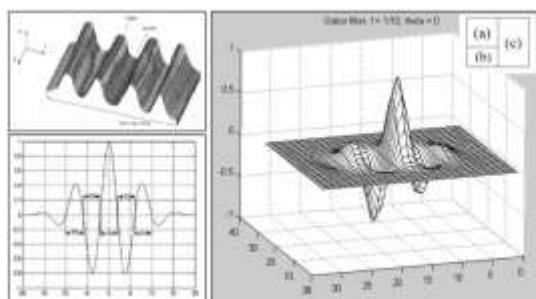
Figure 4. Region of Interest Covered by a Hexagonal Grid

### b. Filtering ROI in Eight Directions Using Gabor Filterbanks

In fingerprint images, ridge and groove patterns form sinusoidal wave structures with unique frequencies and orientations that gradually vary across different regions. Bandpass filters are tuned to suppress noise while preserving fingerprint structures.[4,5]

The Gabor filter (Figure 5), with optimized parameters, is used to analyze and retain

the essential features of ridges and valleys in fingerprint images. By applying Gabor filters in eight different orientations, the system enhances the clarity of ridge structures while reducing distortions and background noise.



**Figure 5. Gabor Filtering.** (a) Ridge and valley structures in the fingerprint image, (b) 1D Gabor filter applied along the x-axis, (c) Gabor filter in the spatial domain.

The Gabor filter exhibits both frequency selectivity and directional selectivity, making it optimized for resolution in both the frequency and spatial domains. Fine details can be interpreted as critical points along the ridgeline structures, which represent the essential information the system aims to capture.[5,6,7]



**Figure 6. Fingerprint Image Enhancement Using Gabor Filter.**

As a result, properly tuning the Gabor filter can effectively suppress noise, preserve ridge structures and valley patterns, and extract directional information from the fingerprint image in a specific orientation..

c. Computing the Average Absolute Deviation (AAD) to Generate the Feature Vector (FingerCode).

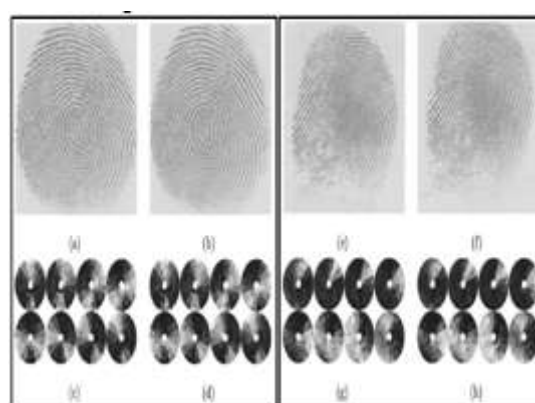
After obtaining eight filtered images, the variance of pixel values is computed within each region to construct the feature vectors, also known as FingerCode, for identification purposes.

A higher variance in a region indicates that the ridge structures are aligned parallel to the applied Gabor filter orientation.

A lower variance suggests that the ridges are orthogonal to the applied Gabor filter direction.

This variance-based analysis helps in encoding the fingerprint's unique texture patterns into a compact feature representation.

Figure 7 illustrates the fingerprint and its corresponding feature vector representation. The grayscale levels within a circular region represent the feature values for that area in the corresponding filtered image.



**Figure 7. Feature Vector.**

Notably, Figures 7(c) and 7(d) appear similar to Figures 7(g) and 7(h); however, the circular regions represent two different fingerprints and exhibit distinct patterns. This distinction highlights the ability of the feature extraction process to capture unique fingerprint characteristics despite similarities in overall structure.

d. Calculating the Euclidean Distance Between Two FingerCodes for Correlation Results

- Once the FingerCodes of two fingerprints are obtained, the algorithm measures their similarity using the Euclidean distance.

- Each fingerprint is represented as a feature vector (FingerCode).

- The Euclidean distance between two vectors is computed using the formula:

$$d = \sqrt{\sum_{i=1}^n (x_i - y_i)^2} \quad \#(1)$$

Trong đó:  $x_i, y_i$ : are the i-th feature values of the two FingerCodes; n is the total number of features.

A smaller distance indicates a higher similarity between the two fingerprints, while a



larger distance suggests a lower match likelihood.[8]

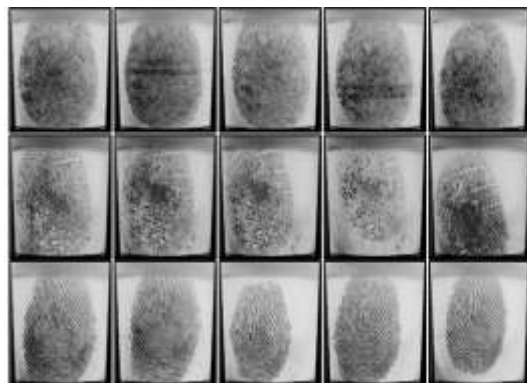


Figure 8. Collected Fingerprint Images.

### III. BUILDING A FINGERPRINT RECOGNITION SYSTEM BASED ON THE FILTERBANK TECHNIQUE

#### 3.1. DATA COLLECTION

The collected fingerprint images vary in quality due to experimental conditions. Some images exhibit high contrast, while others have low contrast or are affected by noise, among other factors (Figure 8).

#### 3.2. IMAGE PREPROCESSING (IMAGE NORMALIZATION)

Due to the discrete nature of variables, the histograms of processed images are not uniform. Histogram equalization enhances image quality by spreading the intensity levels of the input image across the full intensity range.[9]

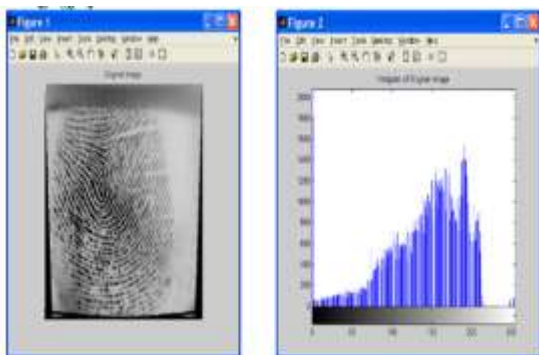


Figure 9. Histogram of the Original Fingerprint.

After applying Histogram Equalization (HE), the results show a significant improvement in mean intensity and contrast in the equalized histogram. These enhancements are also evident in the corresponding comparison histograms.

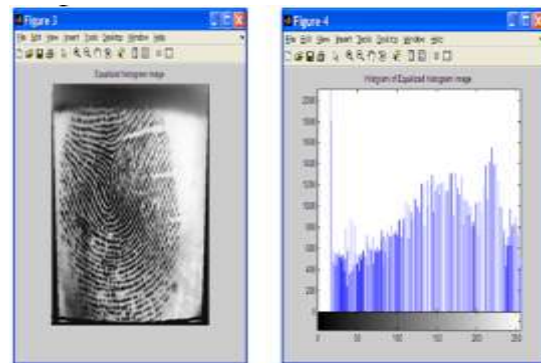


Figure 10. Histogram of the Fingerprint After Equalization.

#### 3.3. DEFINING THE REGION OF INTEREST (ROI)

As mentioned in Section II, the required ROI ratio must incorporate all components within a circular region centered at the reference point. To accurately extract the ROI, the process must:

a. Accurately Identify the Reference Point

**Step 1:** Divide the input fingerprint image into non-overlapping pixel blocks of  $15 \times 15$  pixels to facilitate structured analysis and processing..

**Step 2:** Compute the gradient angles  $\partial_x(i, j)$  and  $\partial_y(i, j)$  at each point  $(i, j)$  using the Sobel operator.

**Step 3:** Estimate the orientation of each block centered at a pixel using the following equations:

$$V_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \partial_x(u, v) \quad \#(2)$$

$$V_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \partial_y(u, v) \quad \#(3)$$

$$O(i, j) = \frac{1}{2} \tan^{-1} \left( \frac{V_x(i, j)}{V_y(i, j)} \right) \quad \#(4)$$

**Step 4:** Smooth the orientation field using a Gaussian filter to reduce noise and enhance continuity in the fingerprint ridge flow.

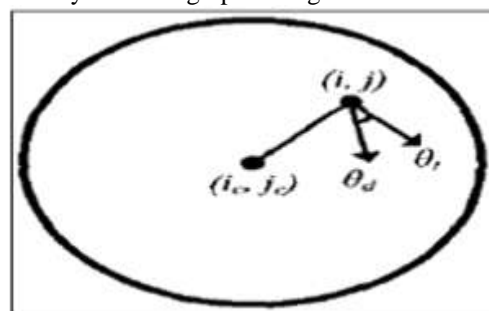


Figure 11. Region S Surrounding the Point  $(i_c, j_c)$

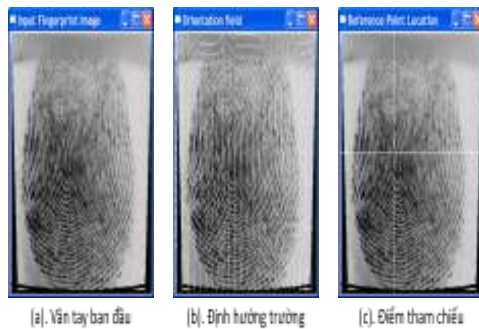
**Step 5:** Initialize a label image (L) with the same dimensions as O. The label image L will be used to mark reference points.

For each pixel  $(i_c, j_c)$  in D, define a surrounding region S around  $(i_c, j_c)$ . Assign corresponding pixel values in L using the following equation:

$$L(i_c, j_c) = \sum_{(i,j) \in S} |\cos(\theta_t(i, j) - \theta_d(i, j))| \quad \#(5)$$

Where:  $\theta_d(i, j)$ : represents the ridge orientation at  $(i, j)$  within S;  $\theta_t(i, j)$ : denotes the perpendicular direction to the line connecting  $(i, j)$  and  $(i_c, j_c)$ .

If  $(i_c, j_c)$  is located at the ridge center,  $\theta_d$  and  $\theta_t$  will exhibit similar values at the highest point within S, resulting in high values in L. Identify the global maximum and secondary peak in L. If a double-loop pattern is detected in the fingerprint image, the midpoint of the connecting line should be designated as the reference point. Otherwise, the maximum value location is assigned as the reference point.



**Figure 12. Reference Position Identification.**

b. Embedding Images in Key Regions

With  $I(x, y)$  representing the grayscale levels at pixel  $(x, y)$  in a fingerprint image of size  $M \times N$  and  $(x_c, y_c)$  denoting the grayscale levels at a specific pixel, the Region of Interest (ROI) is defined as the set of samples computed in the parametric domain  $(r, \theta)$  according to: [10]

$$S_i = \begin{cases} (x, y) \\ b(T_i + 1) \leq r < b(T_i) \\ \theta_i \leq \theta \leq \theta_{i+1}, \\ 1 \leq x \leq N, 1 \leq y \leq M \end{cases} \quad \#(6)$$

with:  $T_i = i/k$ ;  $\theta_i = (i \bmod k) \cdot 2\pi/k$ ;

$$r = \sqrt{(x - x_c)^2 + (y - y_c)^2};$$

$$\theta = \tan^{-1} \left( \frac{y - y_c}{x - x_c} \right);$$

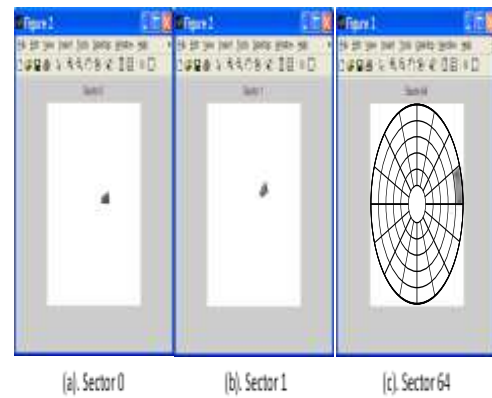
b: The width of each frequency band ( $b = 20$ ).

k: The number of disks per band ( $k = 16$ ).

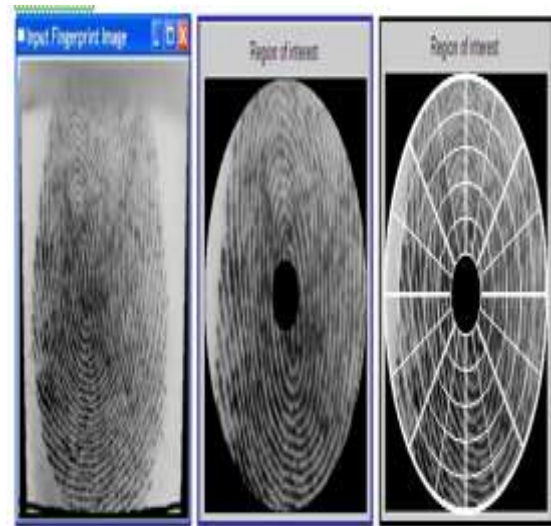
B: The number of bands considered around the reference point for feature extraction ( $B = 5$ ).

$i = 0 \dots (B \times k - 1)$ .

In a fingerprint image scanned at 500 dpi (a standard established by the FBI), a 20-pixel-wide band captures a region encompassing fingerprint ridges and valleys. As a result, this bandwidth is necessary to capture a single minutiae detail in a localized region, facilitating the extraction of distinctive fingerprint features.



**Figure 13. Segmentation of the image into sectors.**



**Figure 14. Image Mosaicking.**

The bands within the same circular region are not used for feature extraction because the ridges surrounding a point in this area exhibit a very high curvature (core), resulting in low coherence.

### 3.4. GABOR FILTERING

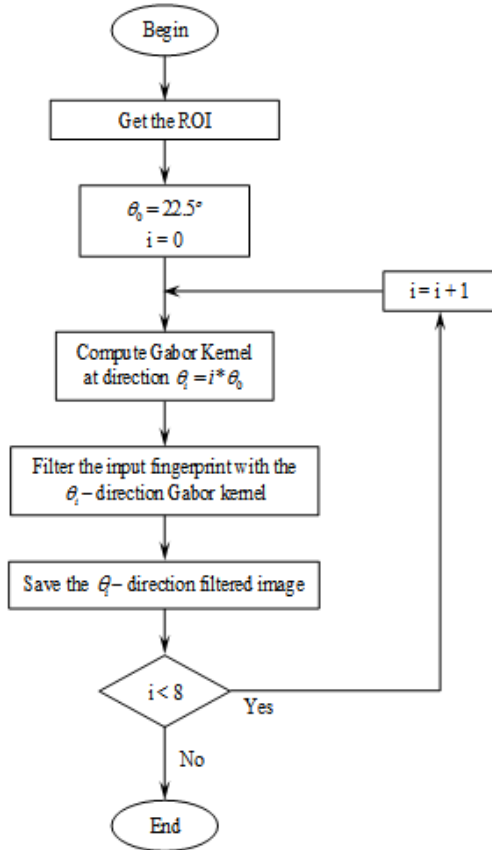


Figure 15. Flowchart of Gabor filter algorithm

The general form of the Gabor filter is as follows:

$$G(x, y, f, \theta) = \exp \left\{ -\frac{1}{2} \left[ \frac{x_{\theta}^2}{\sigma_x^2} + \frac{y_{\theta}^2}{\sigma_y^2} \right] \right\} \cos(2\pi f x_{\theta})$$

$$x_{\theta} = x \cos \theta + y \sin \theta; y_{\theta} = -x \sin \theta + y \cos \theta$$

Where:  $\theta$ : The orientation of the ridge flow along the x-axis;  $f$ : The selected frequency  $x_{\theta}$  in the direction of the ridge flow;  $\sigma_x, \sigma_y$ : The standard deviations of the Gaussian function along the respective axes  $x_{\theta}, y_{\theta}$ . [12]

The frequency is determined based on the average ridge frequency (1/K), where K represents the distance between two consecutive ridges. For fingerprint images scanned at a fixed resolution, the ridge and valley frequency within a specific region falls within a certain range.

The characteristics of the database play a crucial role in selecting the parameters for the Gabor filter. After examining the collected database, I selected the parameter settings:  $\{f = \frac{1}{8}; \sigma_x = 3.0, \sigma_y = 4.0\}$  to implement Gabor filters in the spatial domain with a specified kernel size. Figure 16 illustrates that the Gabor kernel exhibits the same spatial frequency as in the fingerprint image.

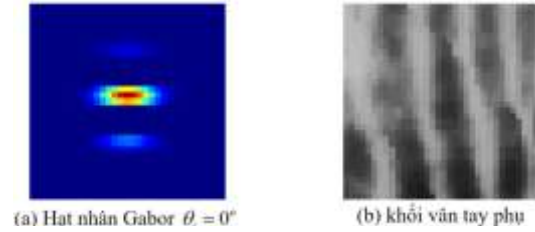


Figure 16. Gabor Kernel.

With four orientations, it is possible to capture the entire fingerprint image, while eight orientations are required to capture the eight reference point values in the designated regions.

$$\theta \in \{0^{\circ}, 22.5^{\circ}, 45^{\circ}, 67.5^{\circ}, 90^{\circ}, 112.5^{\circ}, 135^{\circ}, 157.5^{\circ}\}$$

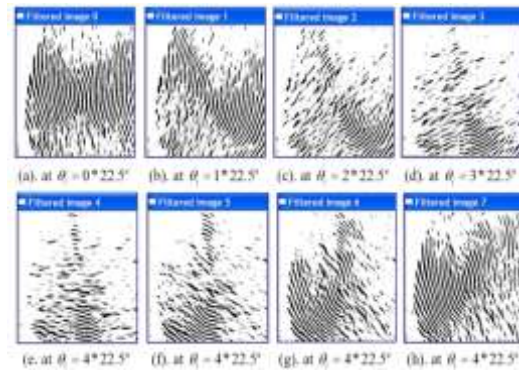


Figure 17. Fingerprint Image Filtering in 8 Directions Using Gabor Filter.

Reconstruct the fingerprint from the filtered images to enhance the fingerprint to the highest possible image quality.

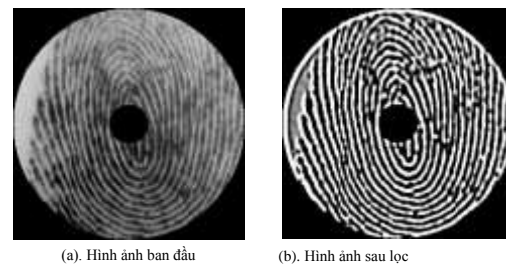


Figure 18. Fingerprint Image Reconstruction Using 8-Direction Gabor Filter.

### 3.5. FEATURE VECTOR

With  $F_{i\theta}(x, y)$  là  $\theta$  - direction Filter the image for sector  $S_i$ . Now, for all  $\forall_i \in \{0^{\circ}, 22.5^{\circ}, 45^{\circ}, 67.5^{\circ}, 90^{\circ}, 112.5^{\circ}, 135^{\circ}, 157.5^{\circ}\}$ , the absolute deviation from the mean gray value (AAD) is defined as:

$$\forall_{i\theta} = \frac{1}{n_i} \left( \sum |F_{i\theta}(x, y) - P_{i\theta}| \right) \quad (7)$$



where:  $n_i$ : is the number of pixels in  $S_i$ ;  $P_{i0}$ : is the pixel value of  $F_{i0}(x, y)$  in sector  $S_i$ .

The image filtering process enhances the boundary between ridge and valley structures, creating a clear distinction between pixel values and the mean value. As a result, a high AAD is observed in the ridge-valley structure. The disk in Figure 19(b) illustrates the AAD values in different subregions, represented by varying shades of gray. Darker areas correspond to lower AAD values.

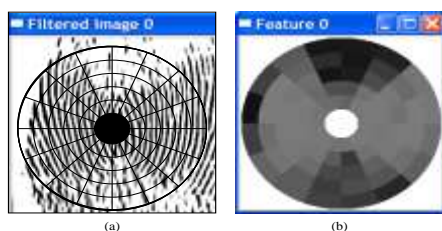


Figure 19. Feature Vector



Figure 20. Feature Vector of Filtered Fingerprint Image f011

Corresponding to the eight filtered images, a total of 640 values (derived from filtering eight images with 80 components) are extracted as feature vectors or the FingerCode for each fingerprint of interest.

The FingerCode images below contain eight characteristic disks, with each disk representing a single filtered image. Figures 20 and 21 display FingerCodes extracted from two different fingerprint images taken from the same user, as do Figures 22 and 23. The sets of disks appear almost identical when the fingerprints are taken from the same user, whereas the reference disks for two different users are significantly different.

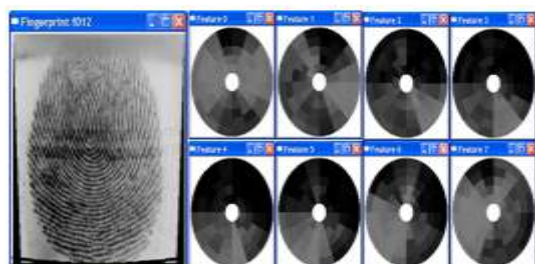


Figure 21. Feature Vector of Filtered Fingerprint Image f012

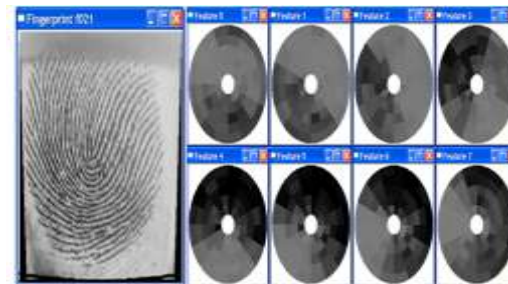


Figure 22. Feature Vector of Filtered Fingerprint Image f021

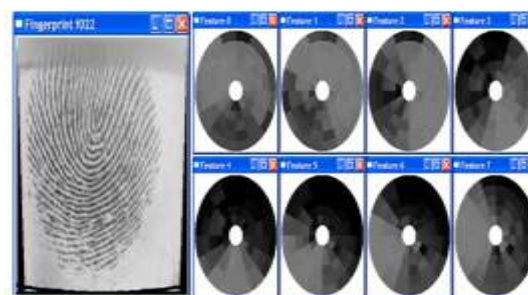


Figure 23. Feature Vector of Filtered Fingerprint Image f022

### 3.6. FILTERBANK-BASED COMPARISON

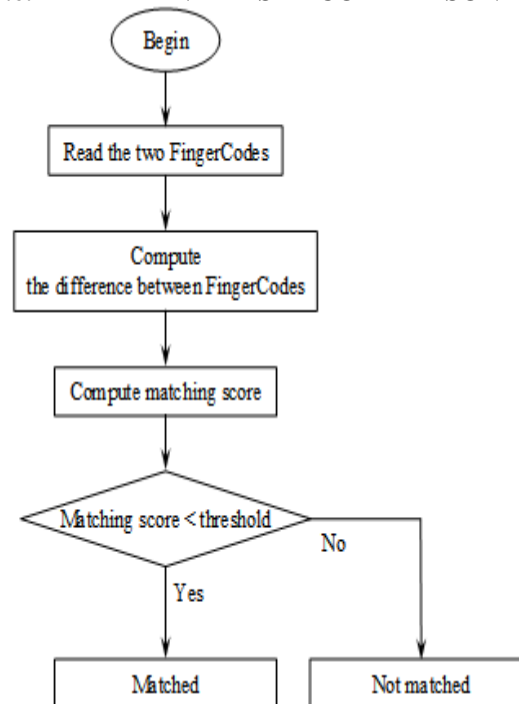


Figure 24. Comparison Algorithm

The difference is calculated using the Euclidean distance between two FingerCodes:

$$d_{\text{Eucl}} = \|V - C\|^2 \#(8)$$

where: V is the FingerCode of the input fingerprint,  
C is the FingerCode of the fingerprint being compared.



Figure 25. Comparison with Sample 12.2



Figure 26. Comparison with Sample 28.9

### 3.7. ACHIEVED RESULTS

#### a. Template Configuration Mode



Figure 27. User Interface for Template Configuration Mode



Figure 28. Fingerprint Saving

The "Get" button will trigger the "Open" dialog, allowing the user to select the required fingerprint (BMP file) from the collected database (Figure 28).

#### b. User Interface



Figure 29. User Interface

When starting the experiment, the user is required to provide their username and select their representative fingerprint stored in the database. If the username already exists with the presented fingerprint, the program will allow the user to continue their work within the system (Figure 28.a). Otherwise, the program will reject the process (Figure 30.b).



Figure 30. Fingerprint Image Verification Mode



There are 20 users in the system, and 71 fingerprint images are used for matching purposes. To establish the accuracy of the fingerprint comparison method, each fingerprint image corresponding to a user is matched against all 71 fingerprint images in the database. For the collected database, a total of 1,420 comparisons were performed. Each image in the database undergoes one genuine comparison. As a result, the verification mode conducts 71 genuine comparisons and 1,349 impostor comparisons.

#### IV. CONCLUSION

The technique is applied at both local and global levels. Each fingerprint is filtered through eight orientations using the Gabor filter. A fixed-length FingerCode is extracted from the input fingerprint. The FingerCode is compact, requiring only 640 bytes. During the matching phase, the Euclidean distance between FingerCodes is computed for comparison.

The fingerprint recognition method based on the FilterBank technique enhances fingerprint image quality by utilizing histogram equalization and normalization before applying the Gabor filter. The optimal parameters for the Gabor filter are selected to ensure effective filtering. Additionally, fingerprint filtering is performed in square blocks to preserve the ridge and valley structures within the region of interest (ROI).

#### REFERENCES

- [1]. Abdelmonem A. Saleh and Reza R. Adhami (2001). Curvature-based Matching Approach for Automatic Fingerprint Identification. IEEE, 0-7803-6661-1/01
- [2]. Anil Jain and Sharath Pankanti (2000). Fingerprint Classification and Matching. CiteSeer.
- [3]. Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharath Pankanti (2000). Filterbank-Based Fingerprint Matching. IEEE Transactions on Image Processing, Vol. 9, No. 5.
- [4]. Jianwei Yang, Lifeng Liu, Tianzi Jiang and Yong Fan (2003). A modified Gabor filter design method for fingerprint image enhancement. Elsevier, Pattern Recognition Letters 24, 1805-1817.
- [5]. Kaoru UCHIDA (2005). Fingerprint Identification. NEC Journal of Advanced Technology, Vol.2, No.1.
- [6]. Muhammad Umer Munir and Dr. Muhammad Younas Javed (2004). Fingerprint Matching using Gabor Filters. National Conference on Emerging Technologies.
- [7]. Nasir Rehan and Khalid Rashid (2004). Multi-matcher Based Fingerprint Identification System. Journal of Applied Sciences 4 (4), 611-618, ISSN 1607-8926.
- [8]. Prof. Jana Dittmann (2004). Biometrics Concept. Claus Vielhauer - Vorlesung Biometrik SS.
- [9]. Mian Qin (October 2005). A Fast and Low Cost SIMD Architecture for Fingerprint Image Enhancement. MSc THESIS.
- [10]. Vutipong Areekul, Ukrit Watchareeruetai, Kittiwat Suppasriwasuth, Saward Tantaratana (2005). Separable Gabor Filter Realization for Fast Fingerprint Enhancement. IEEE, 0-7803-9134-9/05.
- [11]. Lifeng Sha, Feng Zhao and Xiaou Tang (2003). Improved Fingercode for Filteband-based Fingerprint Matching. IEEE, 0-7803-7750-8/03.
- [12]. Shlomo Greenberg, Mayer Aladjem, Daniel Kogan and Itshak Dimitrov (2000). Fingerprint Image Enhancement using Filtering Techniques. Real-Time Imaging, ISSN:1077-2014, 227 – 236.
- [13]. Neil Yager and Adnan Amin (2004). Fingerprint Verification Based on Minutiae Features: a Review. Pattern Anal Applic, 7: 94-113.
- [14]. Lin Hong, Yifei Wan and Anil Jain (1998). Fingerprint Image Enhancement: Algorithm and Performance Evaluation. IEEE, Vol. 20 No. 8, 777 – 789.
- [15]. Thomas P. Weldon and William E. Higgins (2006). The Design of Multiple Gabor Filters for Segmenting Multiple Textures. IEEE, Vol. 20 No. 5.
- [16]. Sharat Chikkerur, Alexander N. Cartwright and Venu Govindaraju (2006). K-plet and CBFS: A Graph based Fingerprint Representation and Matching Algorithm. International Conference on Biometrics