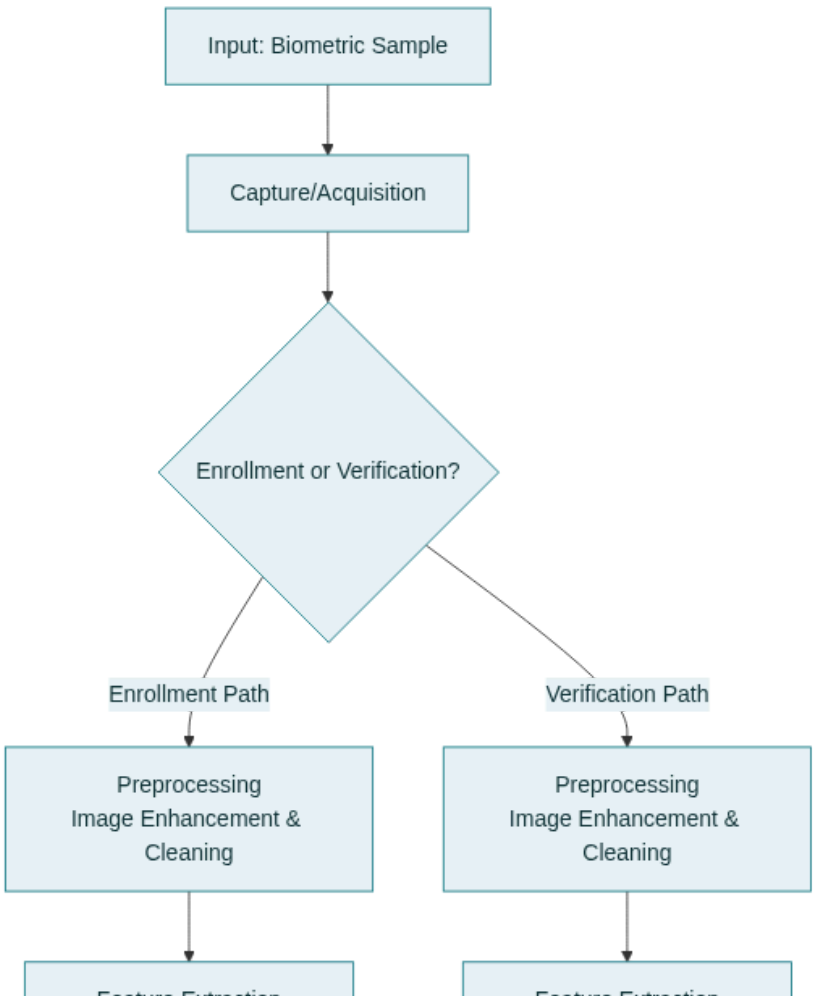
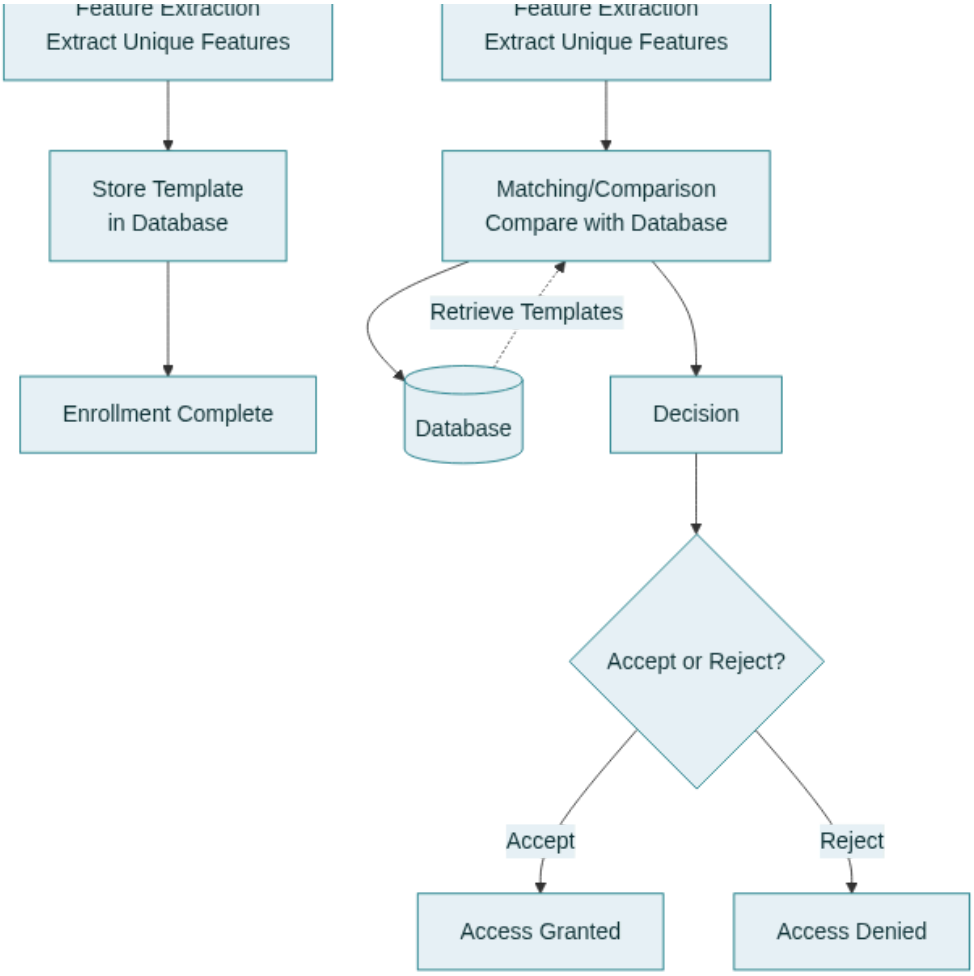
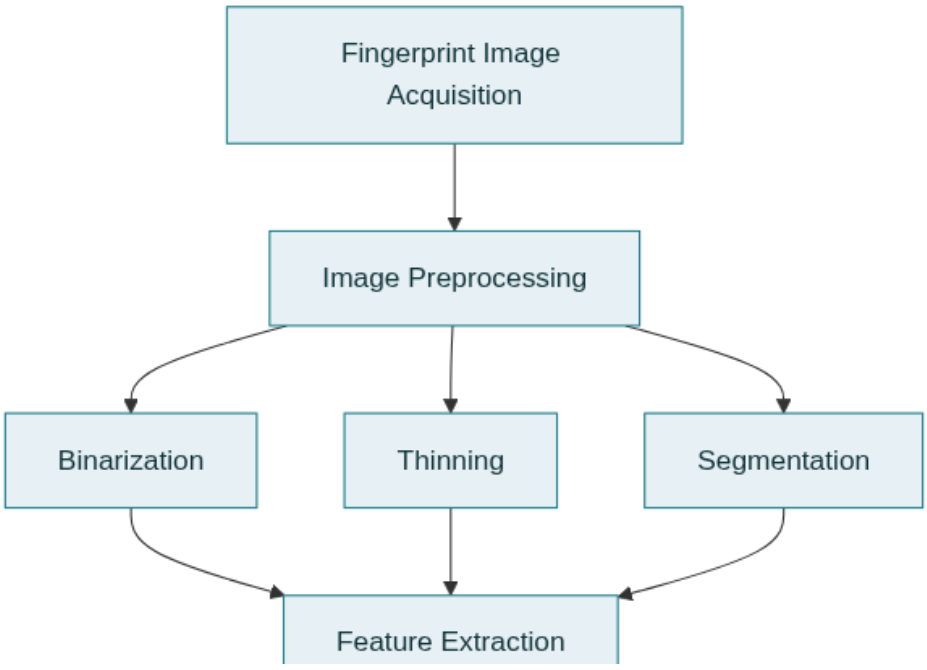
Comprehensive Notes on Biometrics (All Five Units)

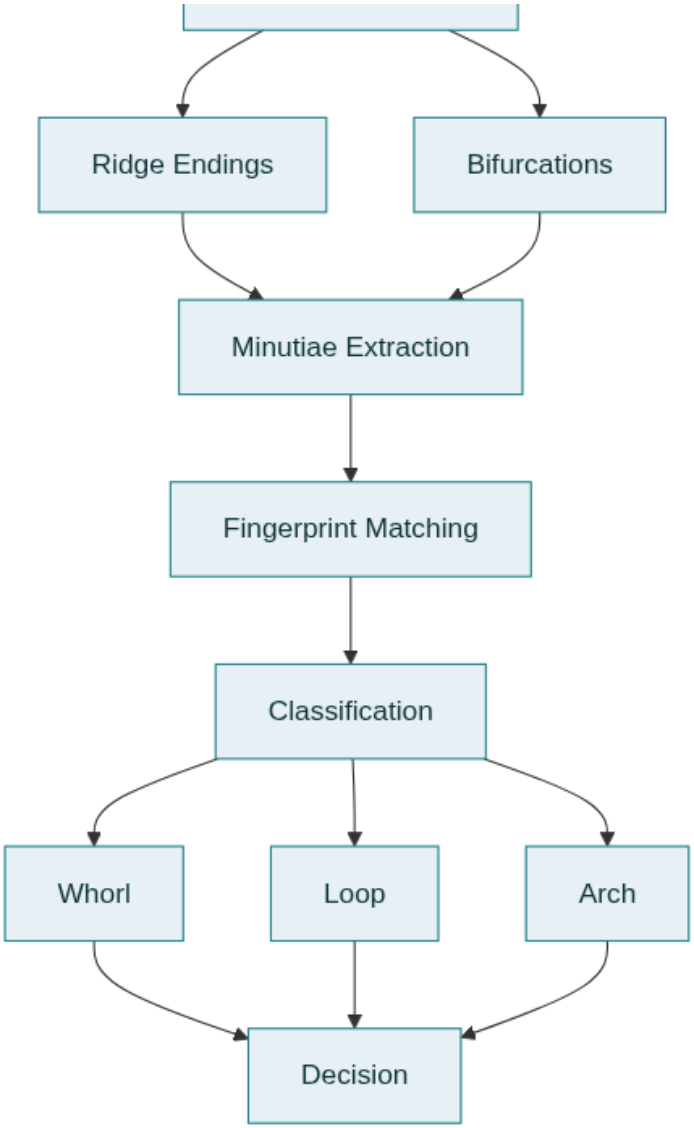
Exam-oriented overview:
The following notes cover all topics listed in your five-unit syllabus in detail, with each subtopic expanded in point form and linked logically to the others. Content is written at B.Sc. Forensic Science level, aligned with concepts used in Indian universities and government documents such as the Aadhaar Act and UIDAI guidance for biometric systems. Flowcharts and diagrams are indicated where they best support understanding; you can redraw them in your notebook using the described structure.[1] [2] [3]


Input: Biometric Sample
Capture/Acquisition
Enrollment or Verification?
Enrollment Path
Verification Path
Preprocessing
Image Enhancement &
Cleaning
Preprocessing
Image Enhancement &
Cleaning

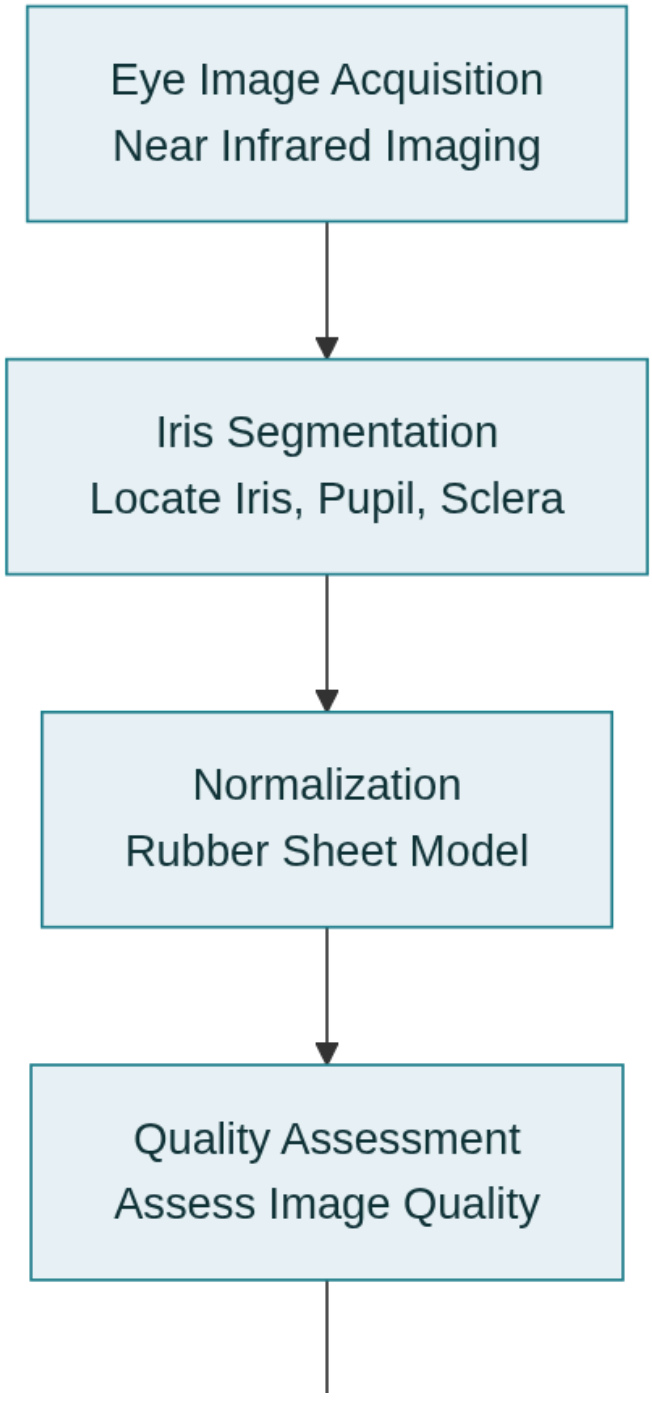

Feature Extraction
Extract Unique Features
Store Template
in Database
Enrollment Complete
Feature Extraction
Extract Unique Features
Matching/Comparison
Compare with Database
Retrieve Templates
Database
Decision
Accept or Reject?
Accept
Reject
Access Granted
Access Denied

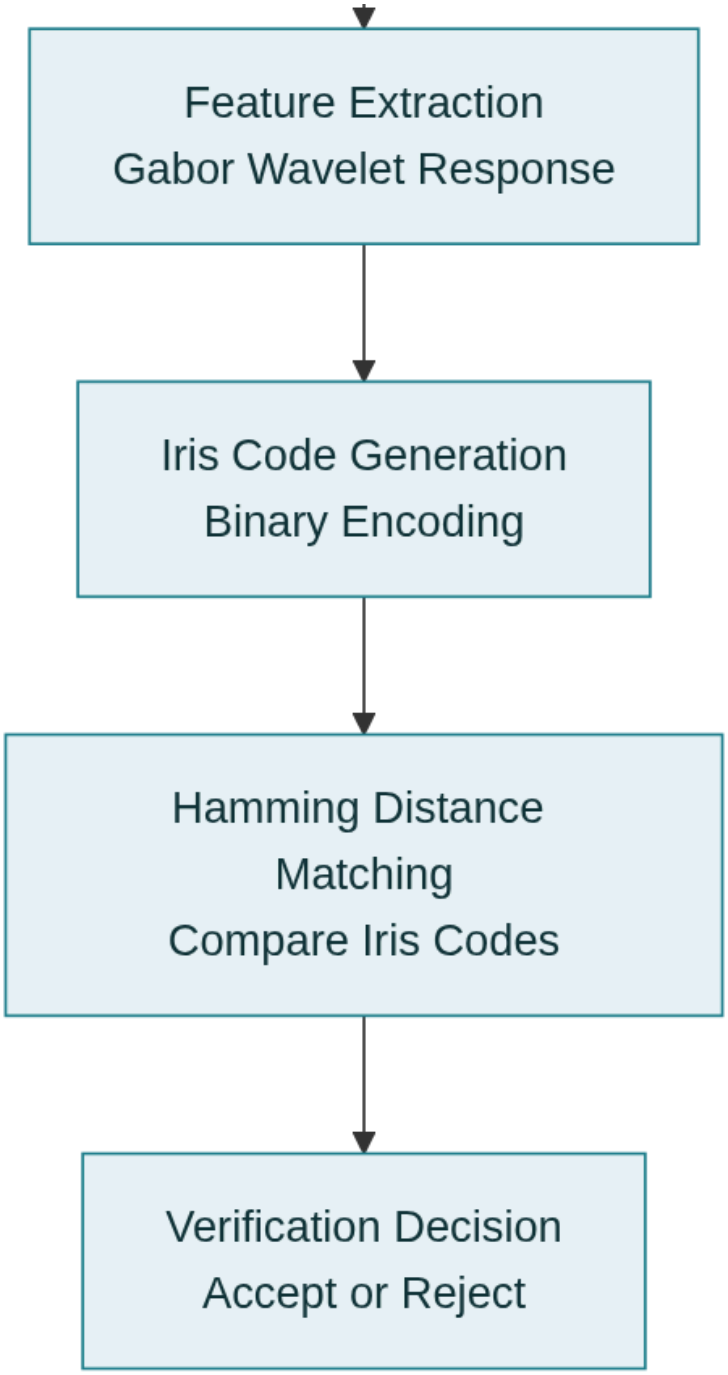
Biometric System Architecture and Process Flow


Fingerprint Image Acquisition
Image Preprocessing
Binarization
Thinning
Segmentation
Feature Extraction

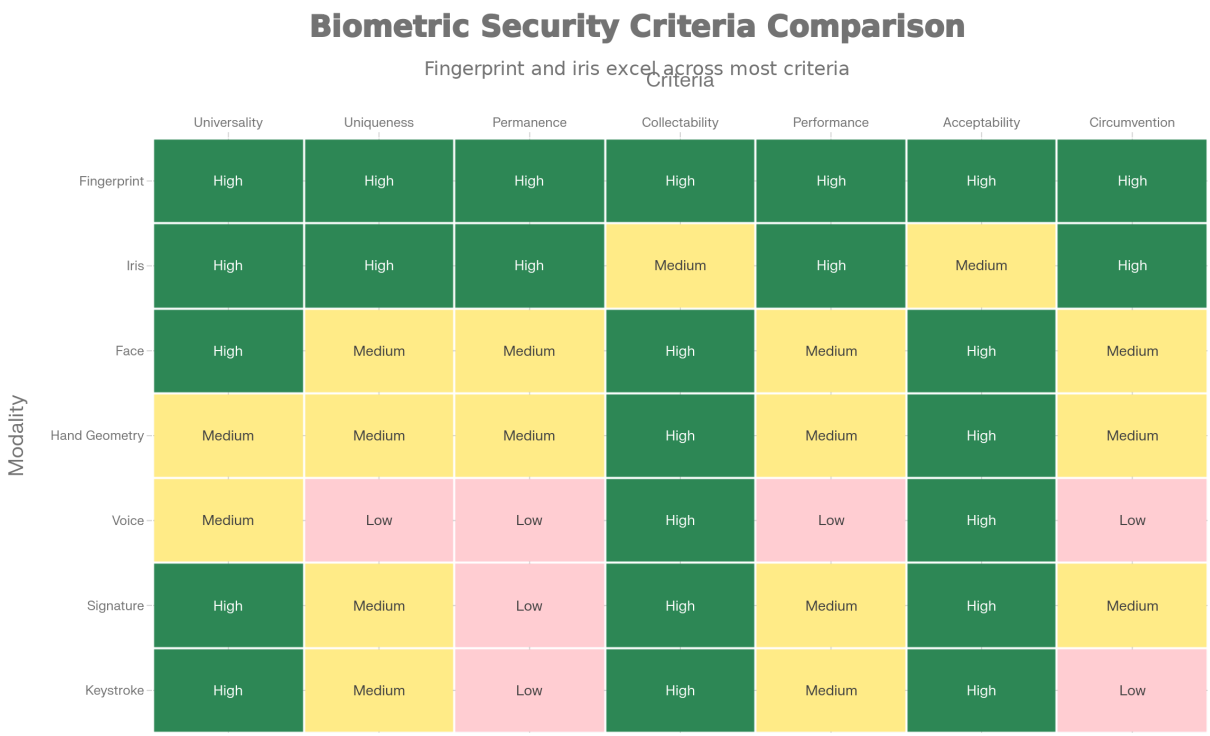

Ridge Endings
Bifurcations
Minutiae Extraction
Fingerprint Matching
Classification
Whorl
Loop
Arch
Decision

Fingerprint Recognition System Processing Pipeline


Eye Image Acquisition
Near Infrared Imaging
Iris Segmentation
Locate Iris, Pupil, Sclera
Normalization
Rubber Sheet Model
Quality Assessment
Assess Image Quality


Feature Extraction
Gabor Wavelet Response
Iris Code Generation
Binary Encoding
Hamming Distance
Matching
Compare Iris Codes
Verification Decision
Accept or Reject

Iris Recognition System Processing Steps



Biometric Modalities Characteristics Comparison Matrix

Unit I – Introduction to Biometrics

1. Biometric Fundamentals

- Biometrics refers to **automated recognition of individuals** based on their physiological or behavioural characteristics (e.g., fingerprint, iris, face, voice, signature).[4] [5] [1]
- Traditional identity methods (passwords, PINs, ID cards) depend on *what you know* or *what you have*, whereas biometrics depends on *what you are* or *how you behave*, making impersonation more difficult.[6] [7] [4]
- A complete biometric system includes:
  - **Sensor**: captures raw biometric data (e.g., fingerprint scanner, NIR iris camera, microphone).[1] [4]
  - **Feature extraction module**: converts raw data into mathematical features (minutiae, texture codes, spectral coefficients).[8] [9]
  - **Database (template storage)**: securely stores enrolled biometric templates for future comparison.[10] [6]
  - **Matcher / Decision module**: compares input features with stored templates and outputs a similarity score or decision.[6] [4]
- Two basic **operation modes**:

- **Verification (1:1)**: confirms a claimed identity by comparing captured sample with that person's template (e.g., Aadhaar authentication).[11] [3]
- **Identification (1:N)**: determines which enrolled person matches the captured sample without a claimed ID (e.g., AFIS search of crime database).[12] [13]

- Performance of biometric systems is measured using:
  - **False Acceptance Rate (FAR)** – probability that an imposter is incorrectly accepted.[4] [1]
  - **False Rejection Rate (FRR)** – probability that a genuine user is incorrectly rejected.[1] [4]
  - **Equal Error Rate (EER)** – operating point where FAR = FRR; lower EER indicates better accuracy.[14] [1]
  - **Receiver Operating Characteristic (ROC)** curve – plots trade-off between FAR and FRR.[15] [14]

Flowchart: Basic Biometric System

- Start → **Biometric sample capture** (sensor) → **Pre-processing** (noise removal, normalization) → **Feature extraction** → **Template generation**.
- Enrollment path: template → **Database storage** under a secure ID.
- Verification path: template → **Matching with enrolled template** → **Decision** (accept/reject) based on threshold score.[6] [1]
- This structure corresponds to the architecture visualised in the first chart.

2. Biometric Technologies and Comparison with Traditional Techniques

- **Physiological biometrics** (based on body structure):
  - Fingerprint, palmprint, hand geometry, iris, retina, facial geometry, finger/palm vein, DNA, ear shape.[5] [1] [16]
- **Behavioural biometrics** (based on actions):
  - Signature dynamics, voice, keystroke rhythm, gait, mouse dynamics.[4] [17] [5]
- **Traditional identification**:
  - Documents (voter ID, PAN, passport), smart cards, passwords and PINs.
  - Vulnerable to loss, theft, sharing, duplication and shoulder-surfing.[6] [7]
- **Advantages of biometrics over traditional methods**:
  - Stronger link between person and credential (cannot easily be shared or forgotten).[18] [4]
  - Convenience: user does not need to remember anything or carry physical tokens.[6] [18]
  - Supports large-scale, real-time authentication (e.g., Aadhaar processes millions of biometric authentications daily).[11] [19]
- **Limitations / risks**:

- Biometric traits are **irrevocable**; once compromised, they cannot be re-issued like a password.[20] [6]
- Potential privacy violations due to mass collection and centralised storage, highlighted in Indian context for Aadhaar.[21] [22] [20]
- Environmental and sensor conditions can affect quality (dry fingers, lighting, background noise).[10] [4]

3. Characteristics of a Good Biometric System

- Biometric traits must satisfy standard properties widely accepted in literature and practice:[4] [1] [2]
  - **Universality** – almost every person should possess the trait (e.g., fingerprints, face).[18] [1]
  - **Uniqueness** – trait should differ sufficiently across individuals; iris and fingerprints are highly unique, even among twins.[9] [18]
  - **Permanence** – trait must be stable over time; iris and fingerprint ridge patterns formed in utero and remain stable with minor ageing changes.[13] [18]
  - **Collectability** – trait must be measurable quantitatively with practical sensors (e.g., fingerprint scanners, iris cameras).[1] [16]
  - **Performance** – system based on the trait must achieve acceptable levels of accuracy, speed, and resource use.[4] [1]
  - **Acceptability** – users must be willing to present the trait; face and fingerprint generally more acceptable than DNA sampling.[23] [1]
  - **Circumvention resistance** – difficulty of spoofing trait using artefacts (e.g., latex fingerprint, high-quality face masks).[1] [4]
- A **good biometric system** also shows:
  - **Robust pre-processing**, handling noise and partial data (e.g., latent fingerprints).[24] [8]
  - **Template protection mechanisms** such as encryption, cancelable biometrics and biometric cryptosystems to protect stored templates.[25] [6]
  - **Compliance with legal and ethical norms**, e.g., Indian regulations treat biometrics as *sensitive personal data* and require strong safeguards.[20] [3]

4. Benefits and Applications of Biometrics

- **Security and access control**: smartphones, laptops, secure facilities, ATMs and e-governance systems rely on biometric authentication for stronger identity proofing.[4] [7]
- **Civil identification and welfare**: India's Aadhaar programme assigns a 12-digit unique identity linked to fingerprint, iris and photograph to support targeted delivery of subsidies, welfare and digital services.[21] [11] [3]

- **Forensic science**: AFIS databases, facial recognition in CCTV, voice comparison and DNA profiling assist in criminal investigations and disaster victim identification.[12] [24] [13]
- **Healthcare and banking**: patient identity management, prescription control, KYC (Know Your Customer) processes and fraud prevention increasingly use biometrics.[26] [20]
- **Advantages for government systems**:
  - Reduced duplicate and fake identities, better targeting of benefits, reduced leakages reported in Aadhaar-linked schemes.[27] [28]

5. Physiological Biometrics – Overview

- **Fingerprint**:
  - Based on ridge and furrow patterns and minutiae (ridge endings, bifurcations).[24] [29]
  - Very high uniqueness and permanence; widely used in forensic and civil applications.[1] [13]
- **Face**:
  - Uses geometric features, landmark distances and texture descriptors to model facial appearance; easily captured by cameras.[5] [16]
- **Iris**:
  - Uses complex patterns of crypts, furrows and freckles in the coloured ring around pupil; encoded as an iris code using Gabor filters.[18] [9]
- **Retina**:
  - Based on vascular pattern at back of eye, captured using NIR scanning; highly accurate but less acceptable due to invasiveness.[16] [5]
- **Hand geometry and palmprint**:
  - Measure palm shape, finger lengths, or high-resolution palm line textures for identification.[30] [15]
- **Finger/palm vein**:
  - Capture subcutaneous vascular patterns using NIR imaging, offering strong liveness detection.[14] [31]

6. Competing Technologies, Strengths and Weaknesses

- **Fingerprint vs Iris vs Face vs Hand geometry**:
  - Fingerprint: mature tech, cheap, but affected by worn or damaged ridges and contact hygiene issues.[13] [10]
  - Iris: extremely low false match rates but requires specialised cameras and user cooperation (gaze, distance).[18] [9]
  - Face: non-intrusive and can be captured at a distance, but affected by lighting, pose, ageing, masks and spoofing.[5] [16]

- Hand geometry: robust and acceptable but less unique, suitable for small to medium populations.[15] [1]

7. Automated Fingerprint Identification Systems (AFIS)

- AFIS is a **computerised system** for automatic storage, search and matching of fingerprints, widely used in law enforcement and civil identification.[12] [13]
- System components:
  - **Image acquisition modules** – live-scan or ten-print card scanners.[29] [12]
  - **Pre-processing and enhancement** – noise removal, ridge orientation estimation, ridge thinning.[32] [33] [12]
  - **Feature extraction** – core and delta detection, minutiae extraction, pattern type classification (Henry classes).[10] [34]
  - **Database and indexing** – efficient representation to support fast search in large databases.[35] [36]
  - **Matching engine** – uses minutiae matching algorithms with rotation/translation compensation to compute similarity scores.[8] [37]
- AFIS in India:
  - State and central agencies maintain fingerprint bureaus; Aadhaar authentication uses fingerprints too, though separate from criminal AFIS databases.[38] [11] [3]
- Advantages:
  - Fast search over millions of records, aiding latent print identification and background checks.[13] [12]
- Issues:
  - Dependence on image quality, potential false positives/negatives, and need for standardisation across devices and agencies.[39] [13]

Unit II – Fingerprint Biometrics

1. Fingerprint Patterns

- **Fingerprint**: impression of friction ridges on terminal phalanges; forms during foetal development and remains largely unchanged throughout life.[24] [13]
- Classical **pattern types** under Henry system:[29] [34]
  - **Arches** – ridges enter from one side and exit the other without looping; includes plain arch and tented arch.
  - **Loops** – ridges enter from one side, recurve and exit on the same side; require at least one delta and a core; subdivided into ulnar and radial loops.[34] [29]
  - **Whorls** – circular or spiral patterns with at least two deltas; includes plain, central pocket loop, double loop and accidental whorl.[29] [34]

- Pattern frequencies: large datasets show whorls and loops dominate; arches are least common.[39] [13]
- In forensic classification, *core* and *delta* locations and ridge counts between them play key roles in assigning patterns.[36] [29]

2. Fingerprint Features (Global and Local)

- **Global features**:
  - Pattern type (arch/loop/whorl), ridge flow, orientation field and singular points (core, delta).[10] [33]
- **Local features (minutiae)**:
  - Ridge ending, ridge bifurcation, short ridge, lake, crossover, spur, dot and island.[39] [8] [29]
  - Statistical studies show ridge endings and bifurcations constitute >95% of minutiae.[39]
- **Additional features**:
  - Ridge density, pore positions (poroscopy), edgeoscopy, scars and creases provide supplementary individuality for forensic examination.[24] [13]

3. Fingerprint Image Processing

- **Acquisition**:
  - Inked ten-print cards, optical and capacitive live-scan sensors, or latent prints on crime scene objects.[24] [13]
- **Pre-processing steps**:[32] [8] [33]
  - **Segmentation** – isolate fingerprint region from background.
  - **Noise reduction and enhancement** – histogram equalisation, Gabor filtering and FFT-based enhancement to clarify ridge structures.
  - **Binarisation** – convert grayscale image to binary ridges and furrows using adaptive thresholding.
  - **Thinning (skeletonisation)** – reduce ridges to one-pixel width while preserving connectivity to aid minutiae detection.
  - **Orientation and frequency estimation** – compute local ridge directions and spacing for enhancing filters and core/delta detection.

Flowchart: Fingerprint Recognition Pipeline

- Acquire fingerprint → Segment region of interest → Enhance and binarise → Thin ridges → Extract minutiae and core/delta → Classify pattern → Match with database template → Output score and decision.[8] [10] [32]

4. Minutiae Determination

- **Minutiae extraction algorithms** typically follow these steps:[24] [8] [40]
  - Work on thinned binary image; compute **crossing number** for each ridge pixel to identify ridge endings (CN=1) and bifurcations (CN=3).
  - Remove **spurious minutiae** caused by noise, breaks, bridges or spikes using morphological operations (clean, spur, H-break).[8]
  - Use region masks and distance thresholds to eliminate minutiae near image borders or in low-quality areas.[32] [33]
- **Quality control**:
  - Only minutiae inside reliable regions and above minimum separation are kept, improving matching robustness.[32] [8]

5. Fingerprint Matching

- Fundamental assumption: relative configuration of minutiae (type, position, orientation) is highly distinctive and stable for each finger.[39] [37]
- Matching approaches:[8] [10] [37]
  - **Minutiae-based**: align query and template using reference points (core or a selected minutia) and compute correspondences between minutiae pairs; tolerant to limited distortion.
  - **Correlation-based**: compare grayscale or ridge maps by correlation after alignment; sensitive to distortion and misalignment.
  - **Hybrid / feature-based**: combine minutiae with ridge orientation, texture or local structures for improved performance.[10] [33]
- Modern systems use tolerance for translation, rotation and non-linear skin distortion; some use circular or local coordinate systems around core to speed matching.[37] [8]

6. Fingerprint Classification

- Purpose: reduce search space in large databases by indexing fingerprints into classes.[10] [34]
- **Henry classification system**:[29] [34]
  - Ten-finger formula based on presence or absence of whorl patterns in specific fingers, producing a fraction code used to sort records.
- Automated classification:
  - Uses ridge orientation fields, singular point detection and ridge distribution sequences to assign image to Henry classes or extended subclasses.[41] [36] [34]
- Advanced methods employ machine learning (SVMs, CNNs, persistent homology features) for pattern classification and even gender or blood group prediction from fingerprints.[42] [43] [44]

7. Matching Policies and Decision Making

- **Threshold-based policies**:
  - System calculates similarity score S; if S ≥ threshold T, identity is accepted; otherwise rejected.[4] [1]
  - Lowering T reduces FRR but increases FAR; policy depends on application (e.g., AFIS search vs mobile unlock).
- **Security policies**:
  - Multi-factor authentication (biometric + PIN or token) to mitigate spoofing and template compromise.[25] [6] [45]
  - Audit logs and multi-expert review in forensic AFIS to avoid wrongful identification.[39] [24]

Unit III – Fundamentals of Image Processing & Digital Image Representation

1. Digital Image Representation

- An image is represented as a 2D function $f(x, y)$, where **x, y** denote spatial coordinates and **f** denotes intensity (grey level) at that point.[46] [47]
- In digital form, the image is sampled into a grid of pixels; each pixel intensity is quantised into discrete levels (e.g., 8-bit = 256 levels).[47]
- Colour images often use RGB model, storing separate channels for red, green and blue components.[47]

2. Fundamental Steps in Digital Image Processing

- Common pipeline used in biometric systems and general vision tasks:[48] [47]
  - **Image acquisition**: converting physical scene via sensor and digitiser into a digital image.
  - **Pre-processing**: denoising, contrast enhancement and correction of illumination using spatial or frequency domain filters.
  - **Segmentation**: partitioning image into meaningful regions or objects (e.g., separating fingerprint from background).[49] [47]
  - **Feature extraction**: computing descriptors such as edges, corners, textures, shapes.
  - **Classification / recognition**: assigning labels based on extracted features (e.g., fingerprint class, iris identity).

3. Image Enhancement – Spatial Domain Methods

- Spatial domain operations directly manipulate pixel intensities:[48] [50] [46]
  - **Point operations**: contrast stretching, brightness adjustment, gamma correction.
  - **Histogram processing**:
    - **Histogram equalisation** redistributes grey levels to improve global contrast, especially in low-contrast images; widely used in fingerprint and iris enhancement.[32] [50]
  - **Spatial filtering**:
    - **Smoothing (low-pass filtering)** with mean or Gaussian filters reduces noise but blurs edges.[46] [49]
    - **Sharpening (high-pass filtering)** using Laplacian or unsharp masking emphasises edges and fine details.[49] [46]

4. Image Enhancement – Frequency Domain Methods

- Frequency domain processing uses discrete Fourier transform (DFT) to represent images as sums of sinusoids of different spatial frequencies.[46] [47]
- Steps:[51] [46]
  - Apply DFT to convert image from spatial domain to frequency domain.
  - Multiply frequency representation by a filter $H(u, v)$ to attenuate or emphasise certain frequencies (e.g., low-pass to remove noise, high-pass to sharpen).
  - Apply inverse DFT to obtain processed image back in spatial domain.[47] [46]
- Common filters:
  - **Ideal, Butterworth, Gaussian low-pass or high-pass filters** for smoothing or edge enhancement.[48] [46]
- Frequency domain methods are powerful for global operations like periodic noise removal and precise control of spatial detail.[50] [51]

5. Image Segmentation

- Goal: partition image into regions corresponding to objects of interest (e.g., foreground vs background, iris region vs sclera).[49] [47]
- **Thresholding**:
  - Global thresholding chooses single threshold T based on histogram; pixels with grey level > T assigned to one class, others to another; simple and fast.[47] [49]
  - Local/adaptive thresholding uses varying thresholds for different regions to handle non-uniform illumination.[49]
- **Histogram techniques**:

- Analysing peaks and valleys in intensity histogram to select thresholds; histogram equalisation can also aid segmentation.[50] [49]

- **Region-based methods**:
  - Region growing and splitting/merging based on similarity criteria (mean intensity, variance).[49]
- **Edge-based methods**:
  - Detect edges using gradient or Laplacian operators and link them to form region boundaries.[52] [49]

6. Edge Detection

- Edges correspond to locations with strong intensity changes and often indicate object boundaries.[49] [52]
- **Gradient-based operators**:
  - **Sobel, Prewitt, Roberts, Scharr** compute approximate first derivative in x and y directions.[52] [49]
  - Gradient magnitude $G = \sqrt{G_x^2 + G_y^2}$ is thresholded to locate edges.[52]
- **Canny edge detector**:
  - Multi-stage algorithm: Gaussian smoothing → gradient computation → non-maximum suppression → double thresholding and edge tracking by hysteresis; provides thin and well-connected edges.[52]
- **Laplacian and Laplacian of Gaussian (LoG)**:
  - Use second derivative to find zero-crossings corresponding to edges; sensitive to noise but good for precise localisation.[46] [52]

7. Gradient-Based Segmentation and Boundary Tracking

- **Gradient-based segmentation**:
  - Uses edge maps obtained from gradient operators and groups them into closed contours representing object boundaries.[49] [52]
- **Boundary tracking**:
  - Starting from a detected boundary pixel, algorithms follow connected edge pixels to trace object outline; used in region measurement and feature extraction.[49]
- **Laplacian edge detection**:
  - Can be used in conjunction with thresholding and region-growing to obtain accurate segmentation of fingerprints and iris boundaries.[52] [49]

Unit IV – Iris Biometrics

1. Iris System Architecture, Definitions and Notations

- **Iris**: coloured annular region between pupil and sclera, with complex patterns (crypts, furrows, freckles) formed during gestation and stable over lifetime.[18] [9]
- **Iris recognition system** components:[53] [9]
  - NIR camera for eye image acquisition.
  - Segmentation module to detect pupil, iris boundaries and occlusions (eyelids, eyelashes).
  - Normalisation module implementing **rubber-sheet model** to map circular iris region to dimension-fixed rectangular strip.[9]
  - Feature extraction and **iris code** generation using 2D Gabor wavelets or other filters.[53] [9]
  - Matching module computing **Hamming distance** between iris codes and making decision.

2. Iris Recognition and Iris Location

- **Image acquisition**:
  - Use of **near-infrared illumination** enhances iris texture while reducing reflections and pupil dilation variability.[18] [9]
- **Iris location (segmentation)**:
  - Goal is to find inner (pupil) and outer (limbus) boundaries and mask occlusions.[9]
  - Techniques include edge detection + circular Hough transform, active contours and deep learning segmentation networks.[53] [9]
- Accurate segmentation is critical; errors directly degrade recognition performance.[53] [9]

3. Normalisation (Coordinate System and Head Tilting Problem)

- **Rubber sheet model**:
  - Maps iris from polar coordinates (radius r, angle θ) to rectangular coordinates to compensate for pupil dilation and size variations.[9]
- **Coordinate system**:
  - Often uses pupil centre as origin and normalises radial distance to unit interval; angular direction remains 0 to 2π.[9]
- **Head tilting and eye rotation**:
  - During matching, several rotated versions of iris code are compared to handle head tilt and rotation of eye around line of sight.[53] [9]

4. Iris Code, Feature Extraction and Texture Energy Feature

- **Feature extraction**:
  - Apply 2D Gabor wavelets or Log-Gabor filters to normalised iris image to capture local frequency and orientation information of iris texture.[9]
- **Iris code**:
  - Quantise filter responses into binary bits (e.g., sign of real and imaginary parts), forming a compact code (typically 2048 bits).[9]
- **Texture energy features**:
  - Additional descriptors based on local energy of filtered responses or texture statistics (e.g., Local Binary Patterns, wavelet coefficients) can be used in classification.[53] [9]

5. Doubly Dimensional Projection and Iris Code Comparison

- Some methods apply **dimensionality reduction / projection** on feature vectors in both spatial and frequency domains to compact representation while preserving discriminative power.[53] [9]
- **Matching using Hamming Distance**:
  - Fraction of mismatched bits between two iris codes (after shifting to handle rotation).
  - Genuine matches produce low Hamming distances (e.g., <0.3), whereas different irises cluster around 0.45–0.5; threshold chosen between these values.[9]

Unit V – Behavioural Biometrics

1. Overview of Behavioural Biometrics

- Behavioural biometrics model **patterns in human actions** over time rather than anatomy, capturing how a person signs, speaks or types.[4] [5]
- Major modalities:
  - **Signature dynamics** – shape and timing of written signature.
  - **Keystroke dynamics** – typing rhythm and key press patterns.[17]
  - **Voice biometrics** – speaker recognition based on speech features.[54] [5]
  - **Gait, mouse dynamics, touchscreen gestures** – patterns of movement and interaction.[55] [4]
- Advantages:
  - Often require no special hardware (e.g., keystroke uses existing keyboard).[17]
  - Can enable continuous authentication in background (e.g., keystroke or mouse dynamics).[17]
- Drawbacks:

- Higher variability due to mood, health, environment and device differences; lower permanence than physiological traits.[4] [17]

2. Signature-scan (Signature Recognition)

- **Static vs dynamic signatures**:
  - Static: uses scanned image of written signature; features include shape, size, stroke direction inferred from skeletonisation.
  - Dynamic/online: captures time sequence of pen coordinates, pressure and velocity using stylus or digitiser.[2]
- **System components**:[5] [2]
  - Acquisition device (tablet, signature pad).
  - Pre-processing (noise removal, normalisation of position and scale).
  - Feature extraction – global shape descriptors, stroke order, timing, pressure profiles.
  - Matching using dynamic time warping, hidden Markov models or distance measures.
- Strengths:
  - Social and legal acceptance; used extensively in banking and document authentication.[2]
- Weaknesses:
  - Susceptible to skilled forgeries; intra-class variability significant; affects permanence and performance.[4] [2]

3. Keystroke Dynamics

- Keystroke dynamics treat **typing pattern as a biometric signature**.[17]
- Features commonly used:[17]
  - **Dwell time** – duration of pressing a key.
  - **Flight time / latency** – time between successive key events.
  - **Intervals between key release and press**, typing speed, use of Shift/CapsLock, error corrections and navigation key usage.
- Systems work in:
  - **Static mode** – authentication at login by analysing fixed text.
  - **Continuous mode** – monitor typing throughout session for anomaly detection.[17]
- Advantages:
  - Requires no extra hardware; low deployment cost; unobtrusive.[17]
- Limitations:
  - Sensitive to keyboard type and posture; health conditions and stress affect typing; may have higher FRR.[17]

4. Voice Recognition

- **Speaker recognition** (who is speaking) vs **speech recognition** (what is being said).[54] [5]
- Voice biometrics capture features like Mel-frequency cepstral coefficients (MFCCs), pitch, formants and prosody.[54]
- Systems often use MFCCs + statistical models (GMM, i-vectors, deep neural networks) to represent speaker characteristics.[4] [54]
- Strengths:
  - Natural and convenient for phone-based authentication; widely deployed in call-centre KYC.
- Weaknesses:
  - Affected by background noise, channel variability, health (sore throat), and vulnerable to replay and synthesis attacks unless liveness checks used.[4] [54]

5. Privacy, Standards and Need for Regulation

- Behavioural biometrics collect **continuous activity data**, raising privacy concerns about profiling and surveillance.[56] [20]
- In Indian context:
  - IT (Sensitive Personal Data) Rules and Aadhaar Act recognise biometrics as sensitive and mandate security safeguards like encryption and restricted use.[20] [3]
  - Emerging Digital Personal Data Protection Act aims to strengthen consent and purpose limitation, though experts argue for stricter rules specifically for biometrics.[57] [20]
- Standards:
  - International bodies such as ISO/IEC produce standards for biometric data interchange, quality and performance testing; many Indian systems adopt these through BIS and UIDAI guidelines.[1] [20]

6. Designing Privacy-Preserving and Sympathetic Biometric Systems

- **Template protection**:
  - Cancelable biometrics – apply repeatable but non-invertible transformations to features; compromised templates can be reissued.[58] [59]
  - Biometric cryptosystems – combine biometrics with cryptography to derive secure keys without exposing raw templates.[25] [6]
- **Sympathetic / user-centric design**:
  - Minimise data collected (data minimisation) and store templates locally on user device where possible.

    - Provide transparency and control to users about usage, retention and sharing of biometric data.[56] [20]
    - Implement strong security controls – mandatory encryption, secure devices, liveness detection, audit trails.[20] [25]
- For India, scholars highlight need for a **distinct category for biometric data** under data protection law with higher safeguards, given irrevocability and misuse risks.[57] [20]

Conclusion

- The five units together provide a comprehensive understanding of **biometric science and technology**, covering theoretical foundations, signal-processing techniques and practical modalities used in India and globally.[4] [5] [1]
- Fingerprint and iris modalities, supported by robust image processing pipelines and AFIS-like systems, form the backbone of high-confidence identity systems such as law-enforcement databases and Aadhaar.[12] [13] [9] [3]
- Behavioural biometrics like signature, keystroke and voice offer additional factors for multi-modal and continuous authentication but need careful handling due to higher variability and privacy implications.[54] [2] [17]
- Across all modalities, **scientific accuracy, standardisation and legal compliance** are critical, especially in Indian context where biometrics underpin large-scale governance and welfare schemes; adherence to recognised characteristics of good biometric traits, rigorous testing of FAR/FRR/EER, and strong data protection frameworks are essential for trustworthy deployment.[1] [11] [20]

⁂

1. https://www.sciencedirect.com/topics/computer-science/biometric-characteristic
2. https://egyankosh.ac.in/bitstream/123456789/89053/1/Unit-4.pdf
3. https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf
4. https://arxiv.org/pdf/2311.13416.pdf
5. http://thesai.org/Downloads/Volume13No4/Paper_91-A_Comprehensive_Overview_on_Biometric_Authentication_Systems.pdf
6. http://arxiv.org/pdf/1305.4832.pdf
7. http://arxiv.org/pdf/2004.04911.pdf
8. https://arxiv.org/pdf/1812.03385.pdf
9. https://world.org/blog/engineering/iris-recognition-inference-system
10. https://computingonline.net/computing/article/download/741/702
11. https://arxiv.org/pdf/2007.09409.pdf
12. https://www.ijraset.com/research-paper/automated-fingerprint-identification-system
13. https://www.ijraset.com/best-journal/dactylography-the-scientific-study-of-fingerprint
14. https://www.mdpi.com/1424-8220/23/24/9706
15. https://www.mdpi.com/1424-8220/23/7/3653

16. https://www.fraud.com/post/biometric-facial-recognition
17. https://www.aratek.co/news/keystroke-dynamics-as-behavioral-biometrics
18. https://pmc.ncbi.nlm.nih.gov/articles/PMC1298996/
19. http://arxiv.org/pdf/1510.04160.pdf
20. https://www.azbpartners.com/bank/biometric-data-regulation-in-india-legal-landscape-and-risks/
21. https://www.tandfonline.com/doi/full/10.1080/00856401.2019.1595343
22. http://link.springer.com/10.1007/978-981-13-9282-5_38
23. https://pmc.ncbi.nlm.nih.gov/articles/PMC11396455/
24. http://www.ijiris.com/volumes/Vol10/iss-03/42.APIS10121.pdf
25. https://ieeexplore.ieee.org/document/10471316/
26. https://www.ejsss.net.in/uploads/172/15884_pdf.pdf
27. https://www.semanticscholar.org/paper/bc4016f5e271f6f79550670a3c0ee82b242c2238
28. https://www.ssrn.com/abstract=3045235
29. https://www.crime-scene-investigator.net/fbiscienceoffingerprints.html
30. http://eudl.eu/doi/10.4108/eai.7-6-2021.2308682
31. https://ieeexplore.ieee.org/document/10345976/
32. https://ieeexplore.ieee.org/document/11139728/
33. http://telkomnika.uad.ac.id/index.php/TELKOMNIKA/article/view/3112
34. https://www.cse.msu.edu/~cse802/Papers/802_FPClassification.pdf
35. https://eejournal.ktu.lt/index.php/elt/article/download/8026/4032
36. https://www.mdpi.com/1099-4300/21/8/786/pdf
37. https://www.sciencedirect.com/science/article/abs/pii/S003132030500302X
38. https://ieeexplore.ieee.org/document/10201789/
39. https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.70216
40. https://zenodo.org/record/4070910/files/30 17Jun17 5Jan 13969-31444-1-ED (Edit A).pdf
41. https://www.ejece.org/index.php/ejece/article/download/235/140
42. http://www.inderscience.com/link.php?id=74080
43. https://ijsrem.com/download/pattern-recognition-technique-for-prediction-of-blood-group-using-fingerprint/
44. https://arxiv.org/pdf/1711.09158.pdf
45. https://arxiv.org/ftp/arxiv/papers/1210/1210.0829.pdf
46. https://www.uomustansiriyah.edu.iq/media/lectures/6/6_2022_04_15!03_04_27_PM.pdf
47. https://www.geeksforgeeks.org/electronics-engineering/fundamental-steps-in-digital-image-processing/
48. https://restpublisher.com/wp-content/uploads/2025/07/Advancements-in-Image-Enhancement-Comparing-Spatial-and-Frequency-Domain-Methods-Using-COPRAS-Analysis.pdf
49. https://www.ijera.com/papers/Vol7_issue8/Part-1/C0708011016.pdf
50. https://isjem.com/download/advanced-image-enhancement-techniques-for-improved-visual-quality/
51. https://arxiv.org/pdf/1811.02423.pdf

52. https://blog.roboflow.com/edge-detection/
53. https://ieeexplore.ieee.org/document/9872994/
54. http://jsju.org/index.php/journal/article/view/448
55. http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJISMD.2021010103
56. http://arxiv.org/pdf/2411.17321.pdf
57. https://eelet.org.uk/index.php/journal/article/view/2307
58. https://onlinelibrary.wiley.com/doi/10.1002/spy2.198
59. https://opg.optica.org/abstract.cfm?URI=oe-30-21-37816
60. Screenshot-2025-12-19-162855.jpg
61. https://bayanebartar.org/file-dl/library/IELTS2/IELTS-Writing-Maximiser.pdf
62. https://egyankosh.ac.in/bitstream/123456789/67262/1/Block-3.pdf
63. https://www.vssut.ac.in/lecture_notes/lecture1428551142.pdf
64. https://ginasthma.org/wp-content/uploads/2024/05/GINA-2024-Strategy-Report-24_05_22_WMS.pdf
65. https://edustud.nic.in/edu/SupportMaterial202324/10/10_english_eng_sm_2024.pdf
66. https://cdnbbsr.s3waas.gov.in/s35938b4d054136e5d59ada6ec9c295d7a/uploads/2025/03/2025031399.pdf
67. https://ieeexplore.ieee.org/document/10698773/
68. https://www.semanticscholar.org/paper/d36be4afddb7c1bbc31b5487cffed753e8ab2d1c
69. http://koreascience.or.kr/journal/view.jsp?kj=PJJNBT&py=2003&vnc=v13n5&sp=545
70. https://ieeexplore.ieee.org/document/8528832/
71. https://www.semanticscholar.org/paper/c106bac1bf877cd5273c4360b3055ce5af7d090b
72. https://aapm.onlinelibrary.wiley.com/doi/10.1118/1.595331
73. http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.970163
74. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/13217/3036157/Quantum-methods-of-image-analysis-and-processing-in-the-frequency/10.1117/12.3036157.full
75. https://ieeexplore.ieee.org/document/10363410/
76. https://ieeexplore.ieee.org/document/10296866/
77. https://ieeexplore.ieee.org/document/10613925/
78. https://ieeexplore.ieee.org/document/9849109/
79. https://arxiv.org/html/2410.22837v1
80. http://arxiv.org/pdf/1811.07945.pdf
81. http://arxiv.org/pdf/2103.02370.pdf
82. https://openresearchlibrary.org/ext/api/media/5157e32c-8ef1-4a7c-9bf0-0e750b3c8b16/assets/external_content.pdf
83. https://arxiv.org/html/2405.01992
84. https://pmc.ncbi.nlm.nih.gov/articles/PMC3862150/
85. http://arxiv.org/pdf/2312.10604.pdf
86. https://www.tandfonline.com/doi/full/10.1080/17530350.2023.2216220
87. https://dl.acm.org/doi/10.1145/3025453.3025910

88. https://www.atlantis-press.com/article/125960849
89. https://www.ijfmr.com/papers/2023/6/8997.pdf
90. https://www.ijfmr.com/papers/2023/3/2905.pdf
91. http://arxiv.org/pdf/1806.04410.pdf
92. http://telkomnika.uad.ac.id/index.php/TELKOMNIKA/article/download/24231/11499
93. https://jfds.org/index.php/jfds/article/download/585/488
94. http://ijarcs.info/index.php/Ijarcs/article/download/4196/3845