Biometrics and Cryptography -- Finger Biometric

CPSC 4600/5600 Biometric and Cryptography

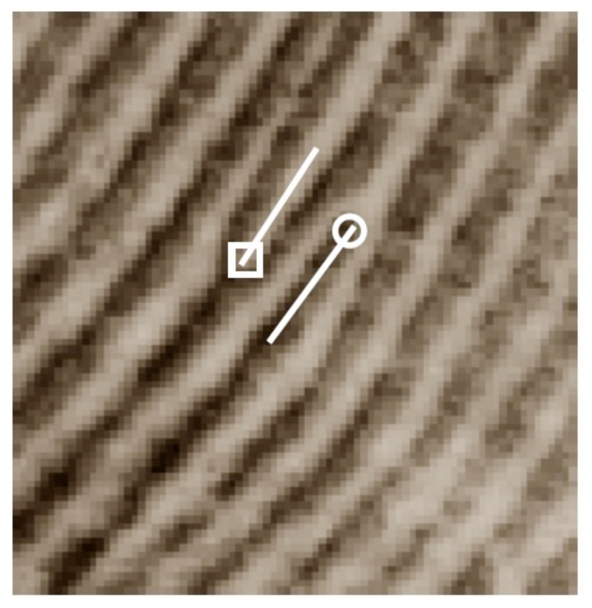
University of Tennessee at Chattanooga

Fingerprint Identification

- Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications.
- Fingerprinting was first created by Dr. Henry Fault, a British surgeon.
- Everyone is known to have unique, immutable fingerprints.
- A fingerprint is made of a series of ridges and valleys on the surface of the finger.

Fingerprint Identification

- The uniqueness of a fingerprint can be determined by the pattern of ridges and valleys as well as the minutiae points.
- Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

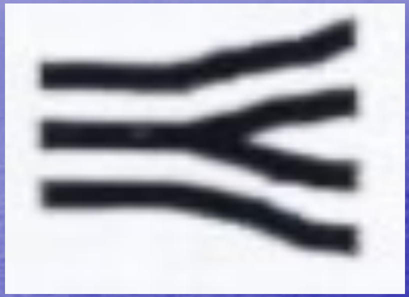


Fingerprint Readers

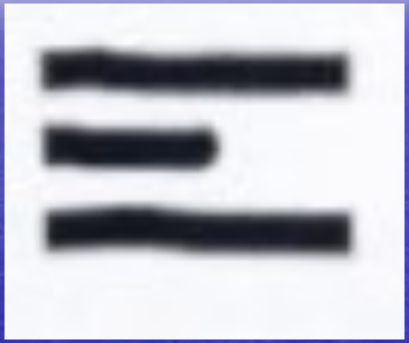
Fingerprint Basics

- A fingerprint has many identification and classification basics

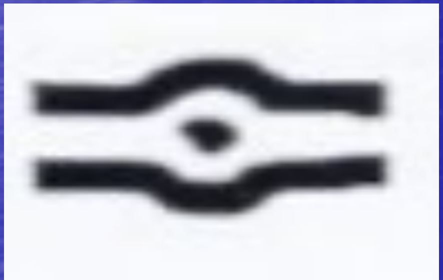
Fingerprint Basics (minutiae)



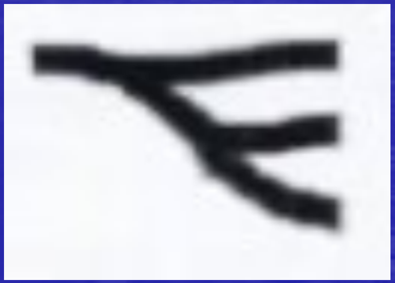
Bifurcation



Ridge ending

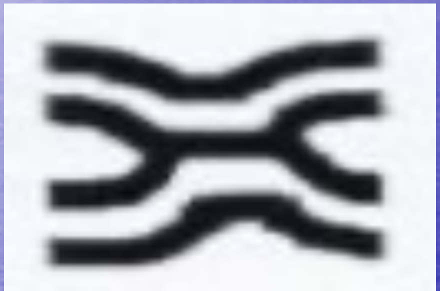


dot

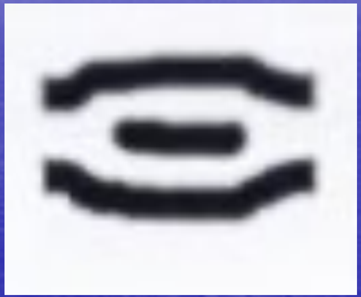


Double bifurcation

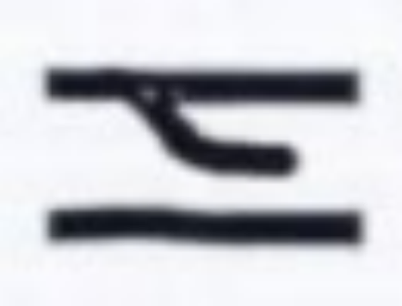
Fingerprint Basics (minutiae)



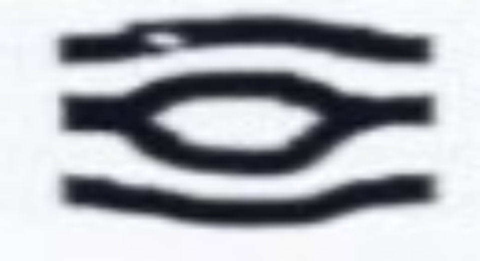
Opposed bifurcation



Island (short ridge)

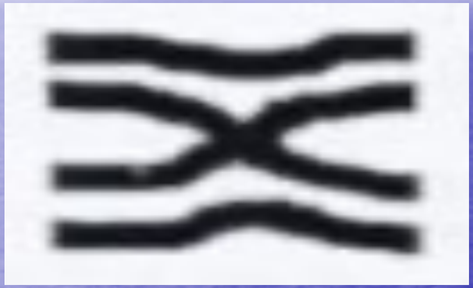


Hook (spur)

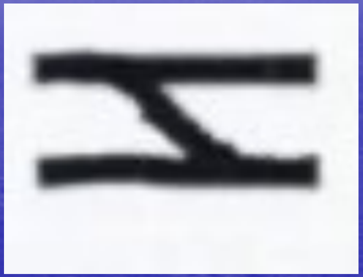


Lake (enclosure)

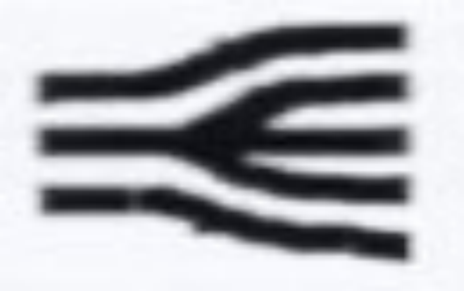
Fingerprint Basics (minutiae)



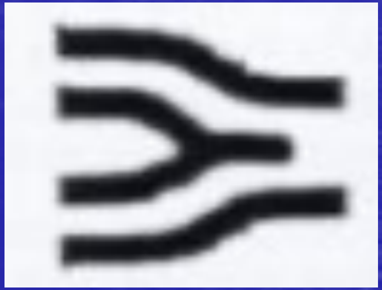
Ridge crossing



Bridge



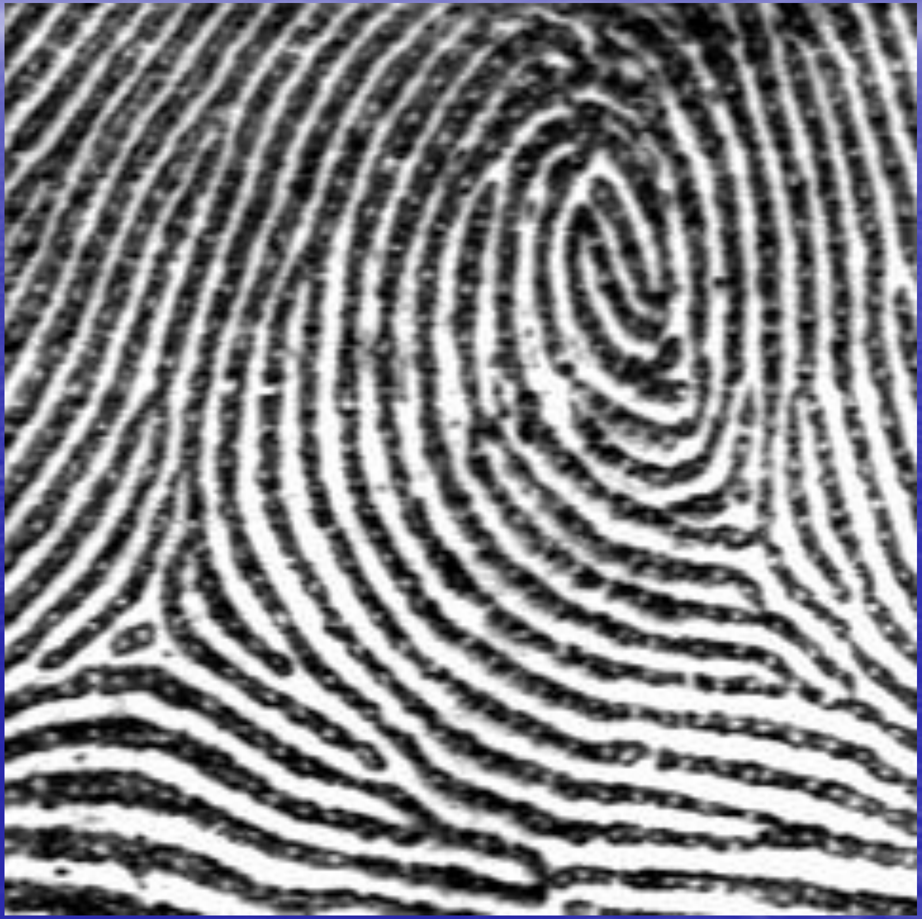
trifurcation



Opposed bifurcation/ridge ending)

Fingerprint Basics

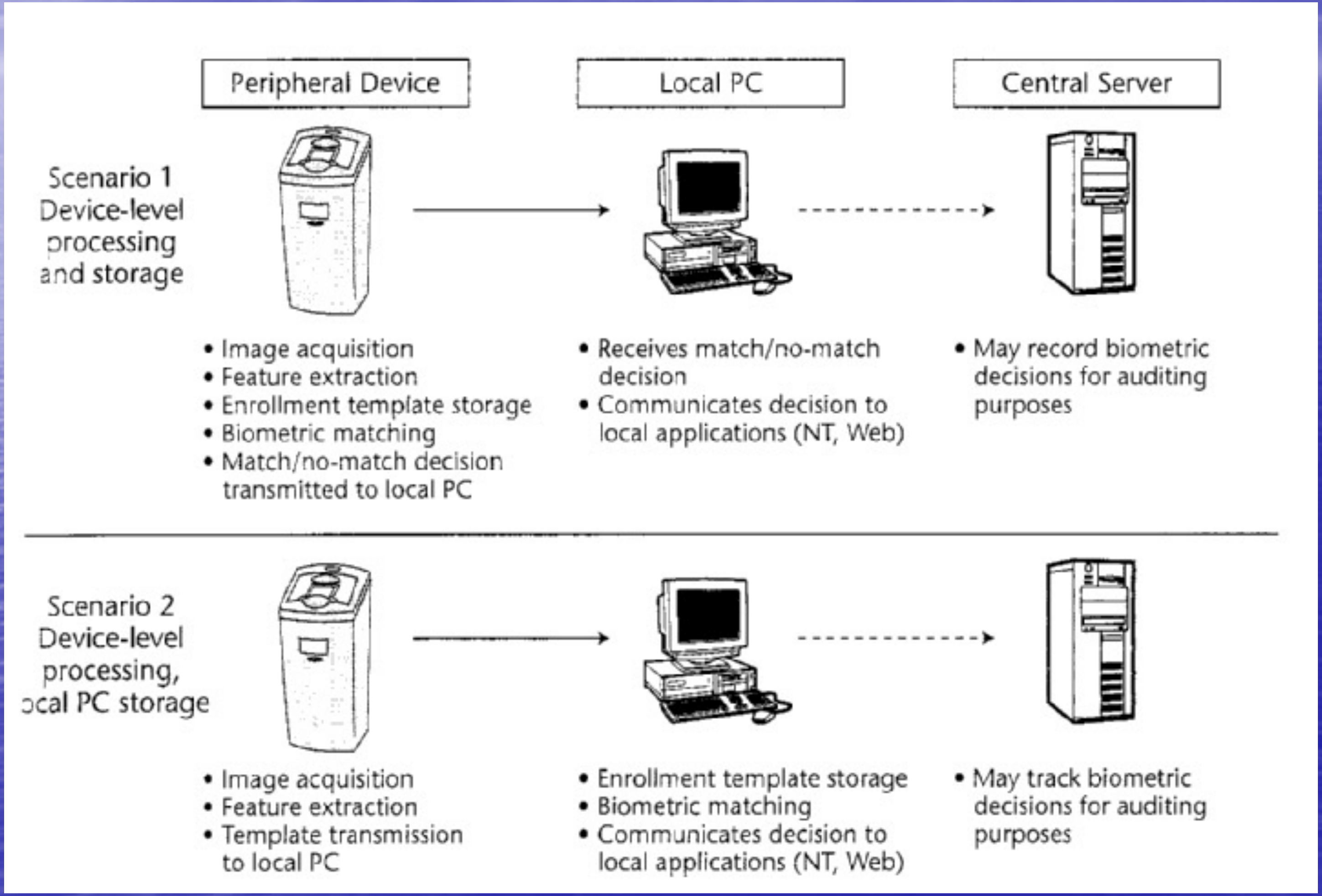
- How many different ridge characteristics can you see?



Fingerprint Identifications

- A single rolled fingerprint may have as many as 100 or more identification points that can be used for identification purposes.
- There is no exact size requirement as the number of points found on a fingerprint impression depend on the location of the print.
- As an example the area immediately surrounding a delta will probably contain more points per square millimeter than the area near the tip of the finger which tends to not have that many points.

Schematic – data storage and processing in finger-scan systems



Scenario 1
Device-level
processing
and storage

- Image acquisition
- Feature extraction
- Enrollment template storage
- Biometric matching
- Match/no-match decision transmitted to local PC

- Receives match/no-match decision
- Communicates decision to local applications (NT, Web)

- May record biometric decisions for auditing purposes

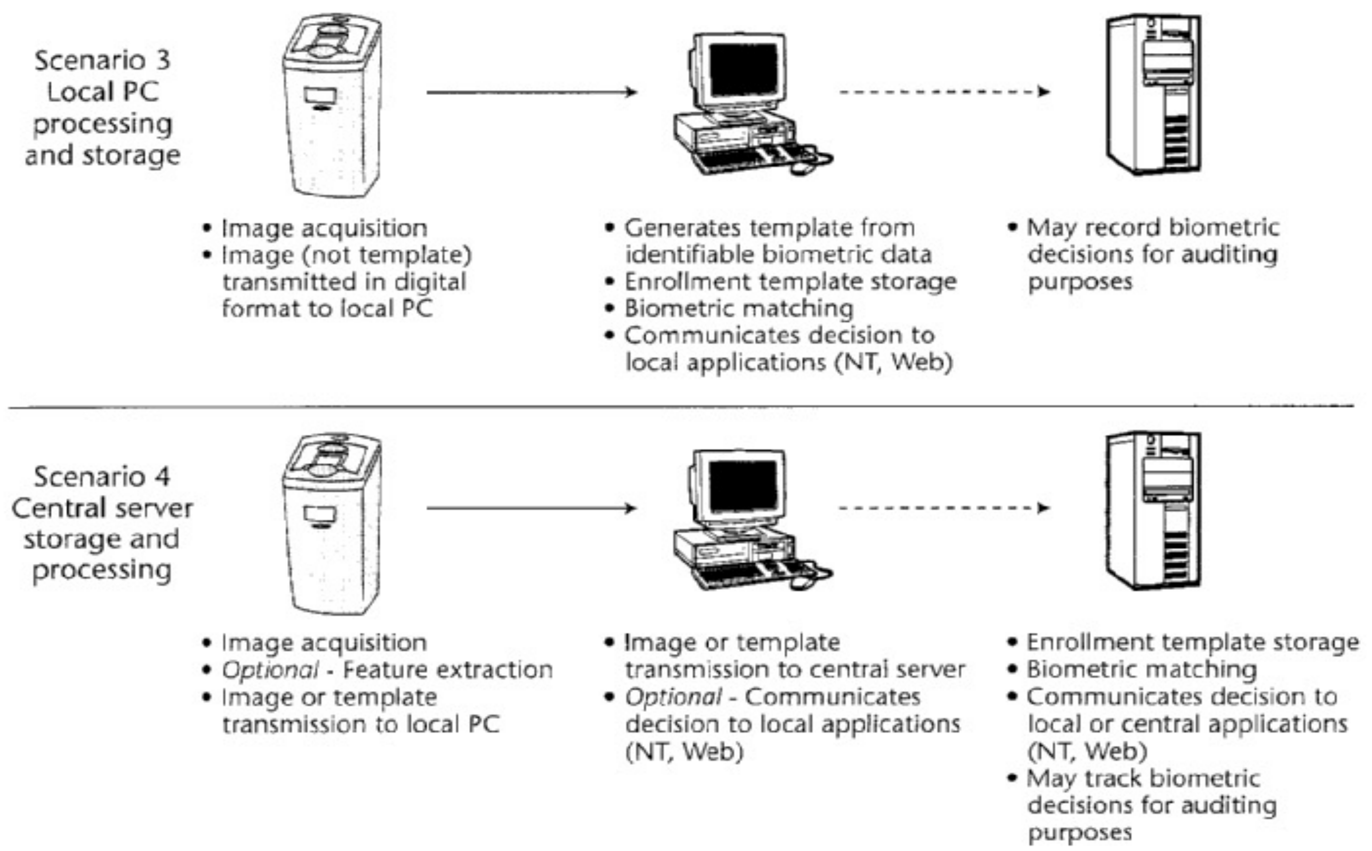
Scenario 2
Device-level
processing,
ocal PC storage

- Image acquisition
- Feature extraction
- Template transmission to local PC

- Enrollment template storage
- Biometric matching
- Communicates decision to local applications (NT, Web)

- May track biometric decisions for auditing purposes

Schematic – data storage and processing in finger-scan systems



Scenario 3
Local PC
processing
and storage

- Image acquisition
- Image (not template) transmitted in digital format to local PC

- Generates template from identifiable biometric data
- Enrollment template storage
- Biometric matching
- Communicates decision to local applications (NT, Web)

- May record biometric decisions for auditing purposes

Scenario 4
Central server
storage and
processing

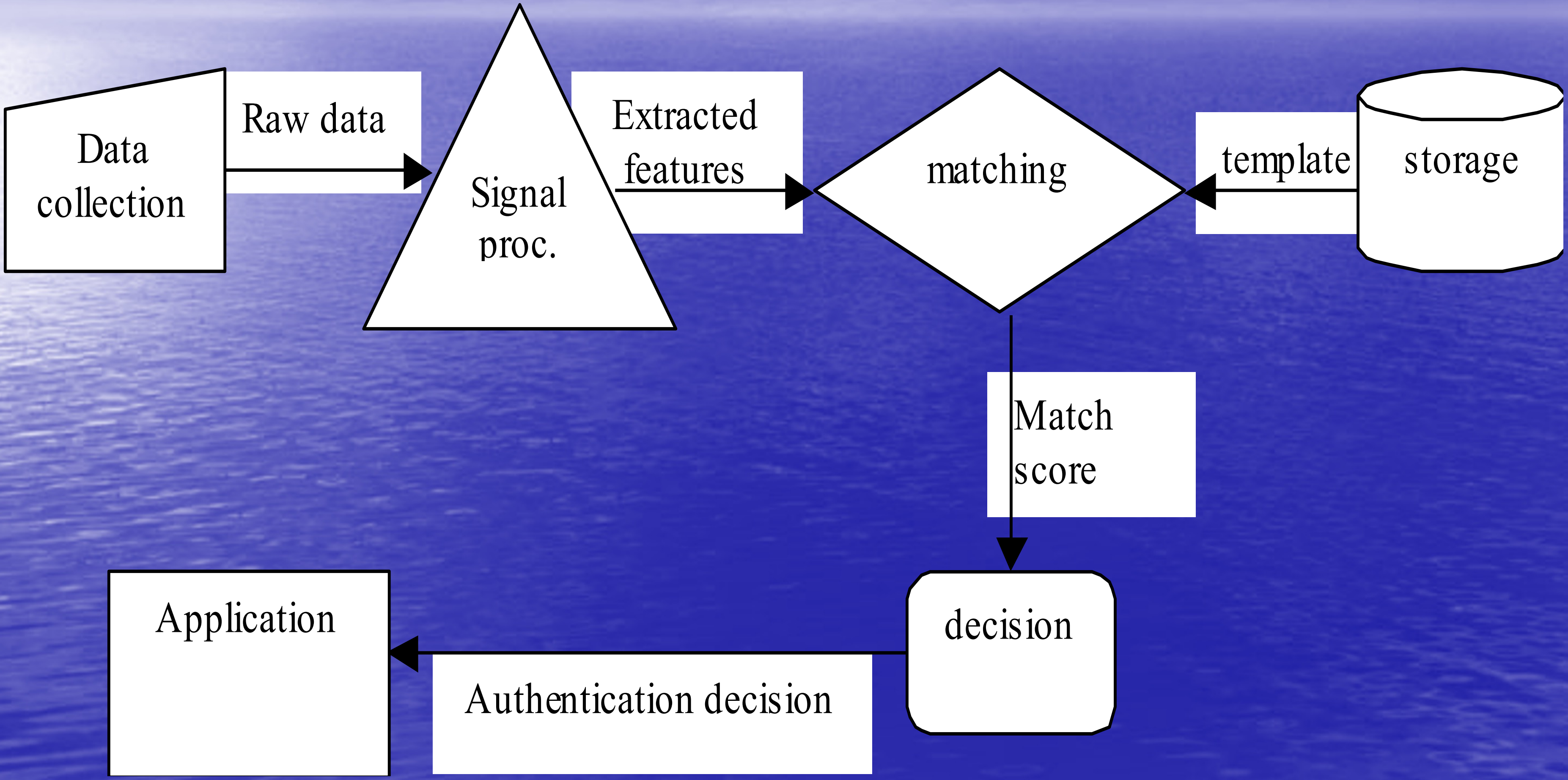
- Image acquisition
- *Optional* - Feature extraction
- Image or template transmission to local PC

- Image or template transmission to central server
- *Optional* - Communicates decision to local applications (NT, Web)

- Enrollment template storage
- Biometric matching
- Communicates decision to local or central applications (NT, Web)
- May track biometric decisions for auditing purposes

Figure 4.3 Schematic—data storage and processing in finger-scan systems.

General Model for Fingerprint Authentication



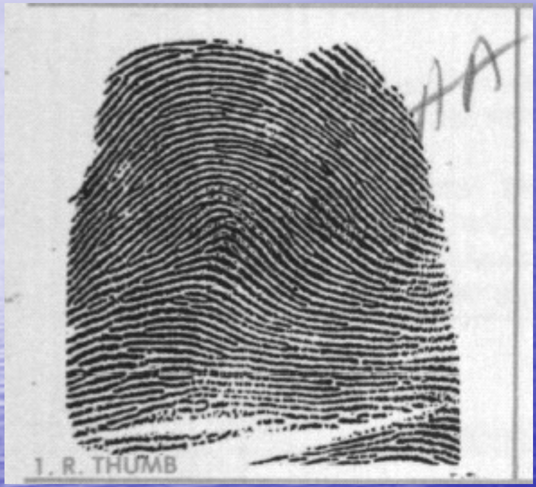
Fingerprint Classification

- Large volumes of fingerprints are collected and stored everyday in applications such as forensics, access control, and driver license registration.
- An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database (FBI database contains approximately 70 million fingerprints!).
- Classifying these fingerprints can reduce the search time and computational complexity, so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.

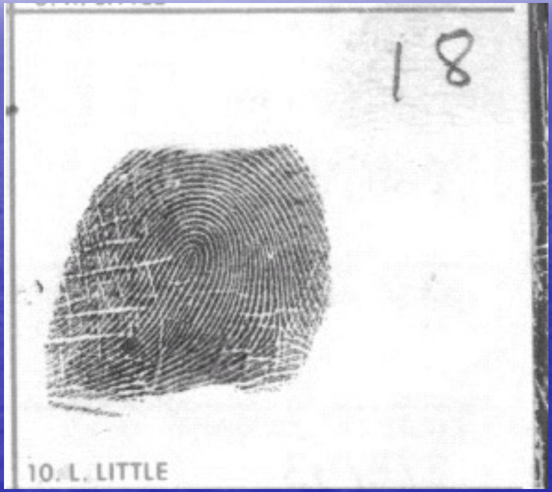
Fingerprint Classification

- Some fingerprint identification systems use manual classification followed by automatic minutiae matching;
- Automating the classification process would improve its speed and cost-effectiveness.
- PCASYS is to build a prototype classifier that separates fingerprints into basic pattern-level classes known as *arch*, *left loop*, *right loop*, *scar*, *tented arch*, and *whorl*.

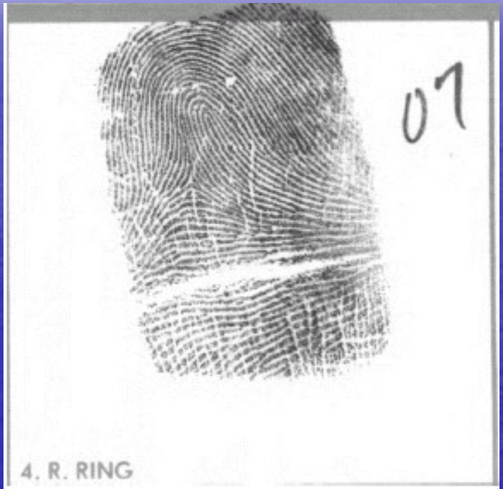
Fingerprint Classification



Arch

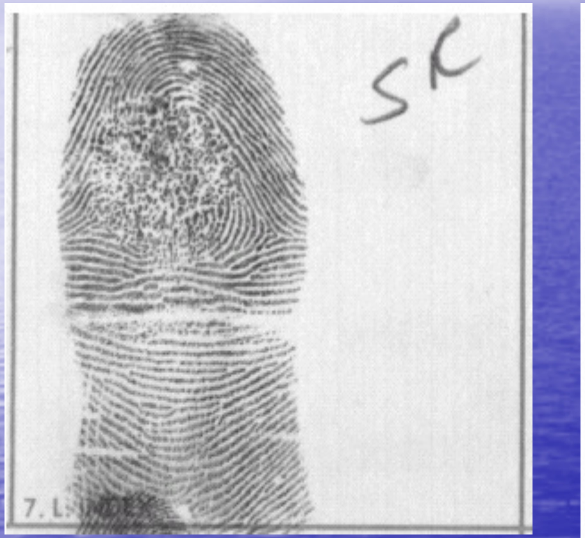


Left loop

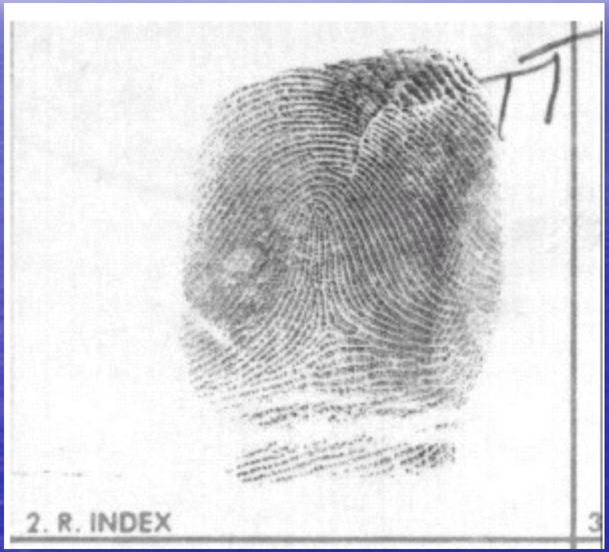


Right loop

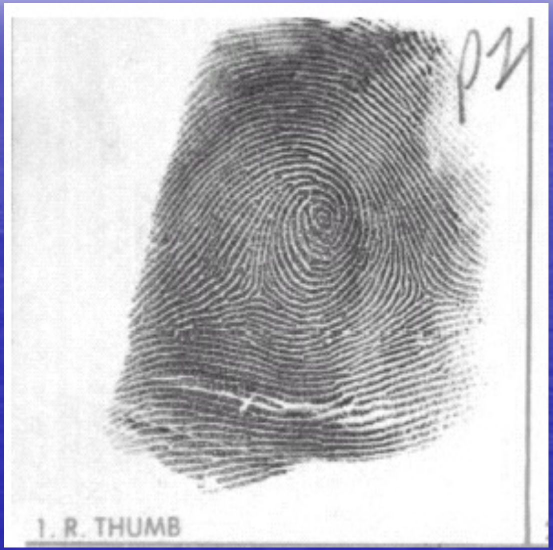
Fingerprint Classification



Scar



Tented arch



Whorl

Fingerprint Classification

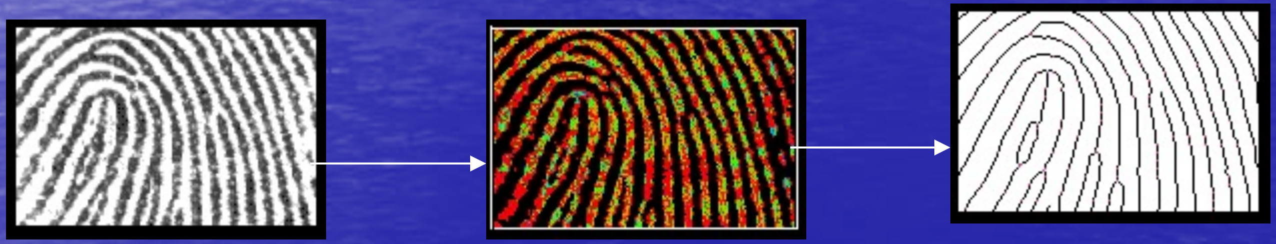
- The loop is by far the most common type of fingerprints.
- The human population has fingerprints in the following percentages:
  - Loop – 65%
  - Whorl -- 30%
  - Arch -- 5%

Minutiae Detection

- Human fingerprints are unique to each person, certifying the person's identity.
- Because straightforward matching between the unknown and known fingerprint patterns is highly sensitive to errors (e.g. various noises, damaged fingerprint areas, or the finger being placed in different areas of fingerprint scanner window and with different orientation angles, finger deformation during the scanning procedure etc.).
- Modern techniques focus on extracting minutiae points (points where capillary lines have branches or ends) from the fingerprint image, and check matching between the sets of fingerprint features.

Minutiae Detection -- Preprocessing

- **Image Processing**
  - Capture the fingerprint images and process them through a series of image processing algorithms to obtain a clear unambiguous skeletal image of the original gray tone impression, clarifying smudged areas, removing extraneous artifacts and healing most scars, cuts and breaks.



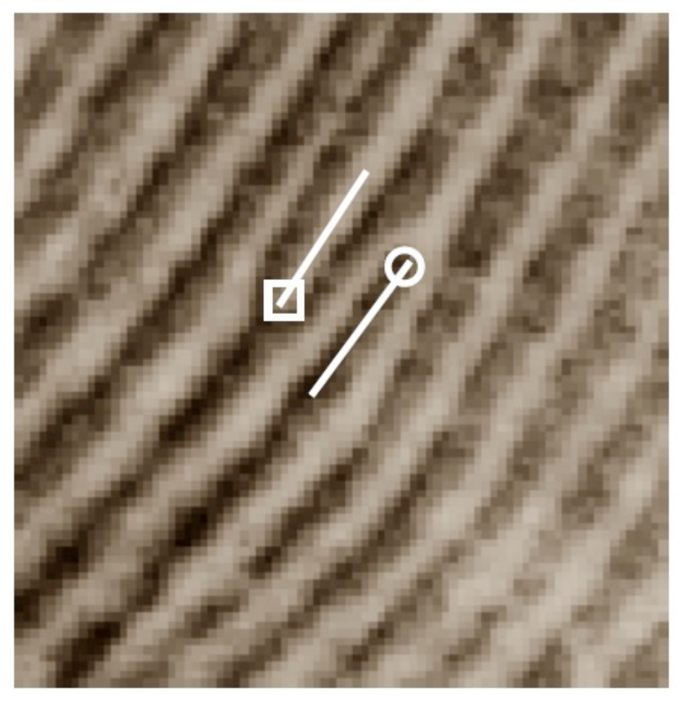
Original image

Undesirable features marked

Final image

Minutiae Detection

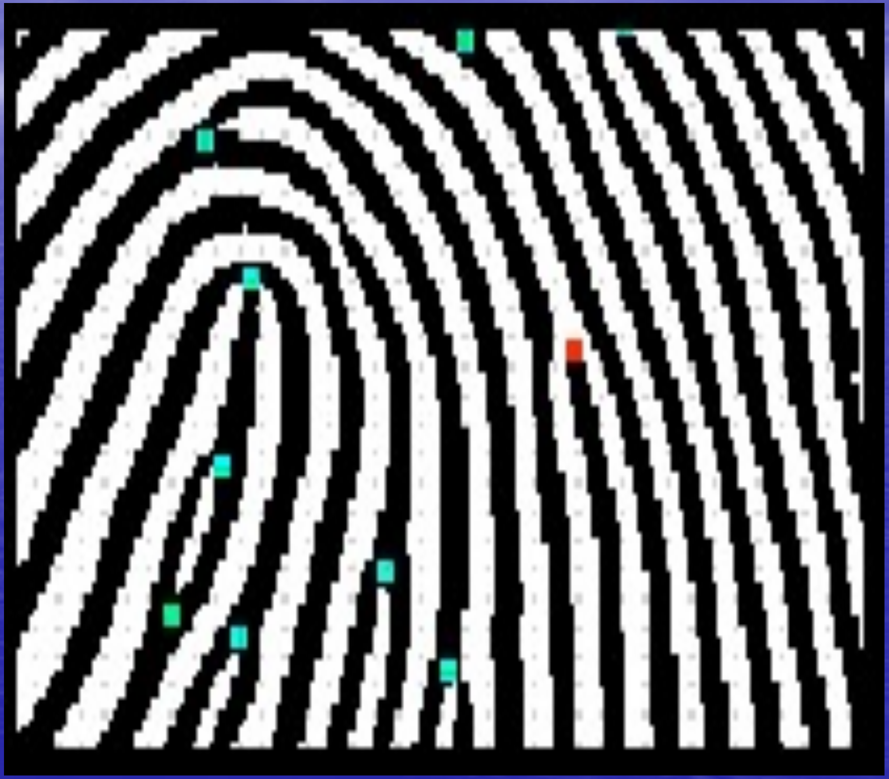
- Two fingerprints have been compared using discrete features called minutiae.
- These features include points in a finger's friction skin where ridges end (called a *ridge ending*) or split (called a ridge *bifurcation*).
- There are on the order of 100 minutiae on a tenprint.



Minutiae: bifurcation (square marker) and ridge ending (circle marker).

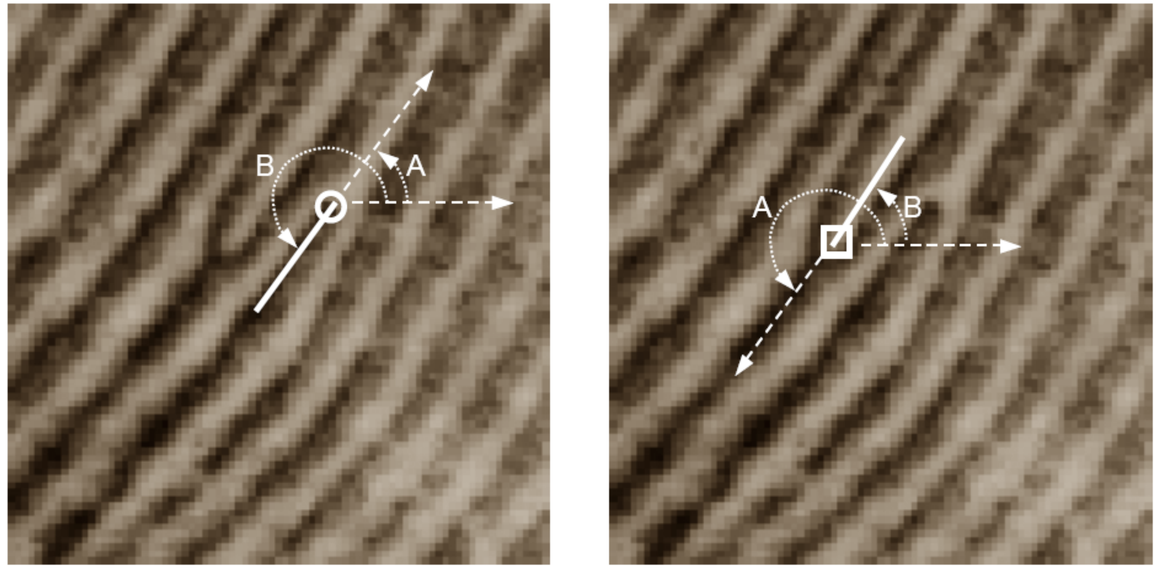
Minutiae Detection

- **Feature Detection for Matching**
  Ridge ends and bifurcations (minutiae) within the skeletal image are identified and encoded, providing critical placement, orientation and linkage information for the fingerprint matching process.



Minutiae Detection

- The location of each minutia is represented by a coordinate location within the fingerprint's image from an origin in the bottom left corner of the image.
- Minutiae orientation is represented in degrees, with zero degrees pointing horizontal and to the right, and increasing degrees proceeding counter-clockwise.

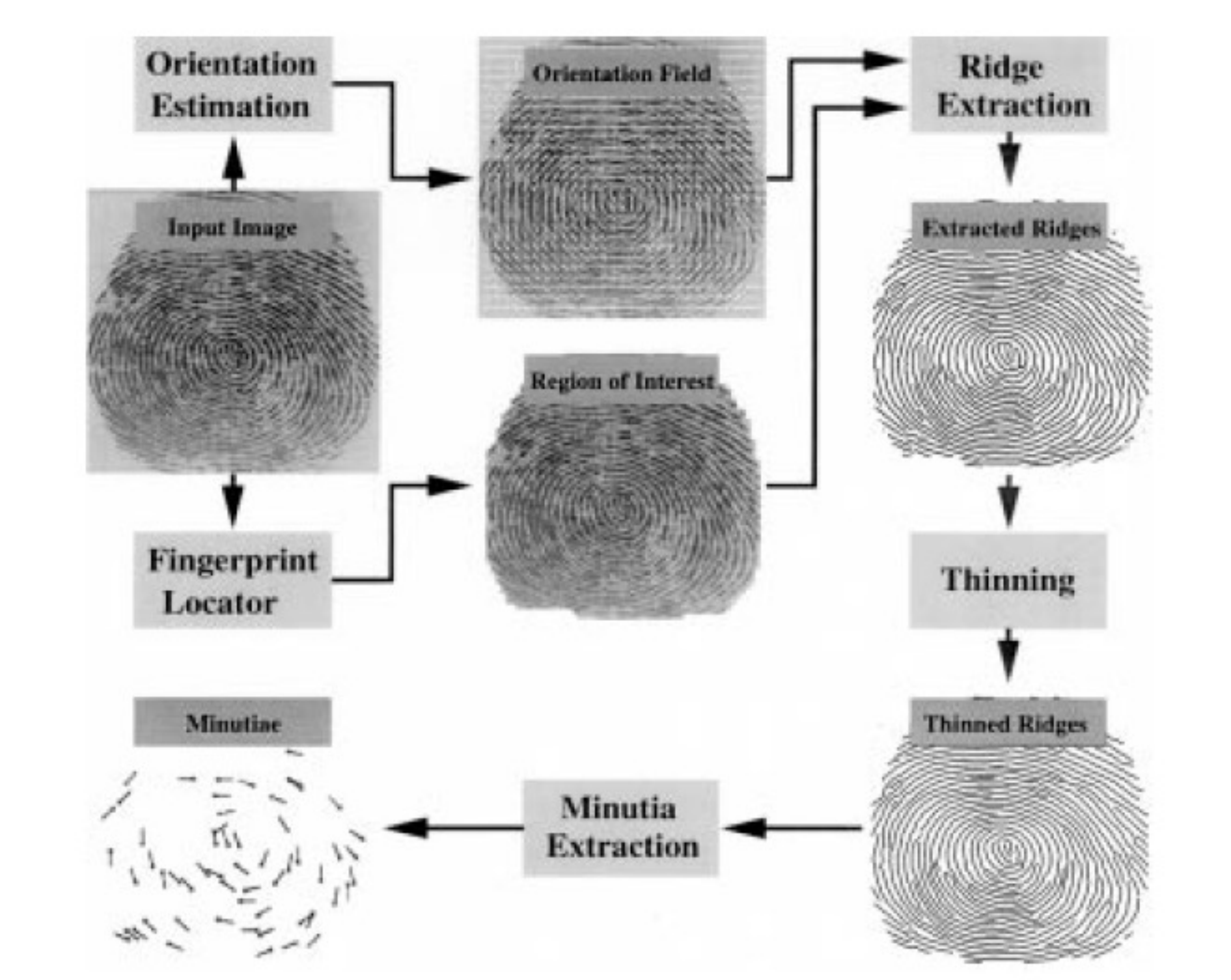


A. standard angle, B. FBI/IAFIS angle

Minutiae Detection

- A good reliable fingerprint processing technique requires sophisticated algorithms for reliable processing of the fingerprint image:
  - noise elimination,
  - minutiae extraction,
  - rotation and translation-tolerant fingerprint matching.
- At the same time, the algorithms must be as fast as possible for comfortable use in applications with large number of users. It must also be able to fit into a microchip.

Minutiae Detection – Extraction Process

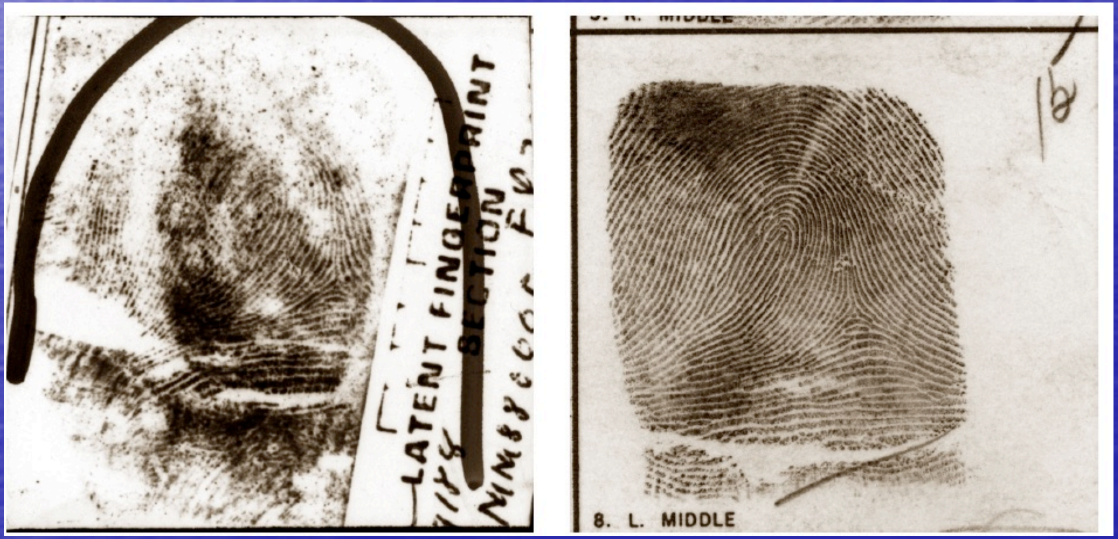


Latent Fingerprints

- In addition to tenprints, there is a smaller population of fingerprints also important to the FBI.
- These are fingerprints captured at crime scenes that can be used as evidence in solving criminal cases.
- Unlike tenprints, which have been captured in a relatively controlled environment for the expressed purpose of identification, crime scene fingerprints are by nature incidentally left behind.
- They are often invisible to the eye without some type of chemical processing or dusting.
- It is for this reason that they have been traditionally called *latent* fingerprints.

Latent Fingerprints

- Typically, only a portion of the finger is present in the latent, the surface on which the latent was imprinted is unpredictable, and the clarity of friction skin details are often blurred or occluded.
- All this leads to fingerprints of significantly lesser quality than typical tenprints.
- While there are 100 minutiae on a tenprint, there may be only a dozen on a latent.



Latent Fingerprints

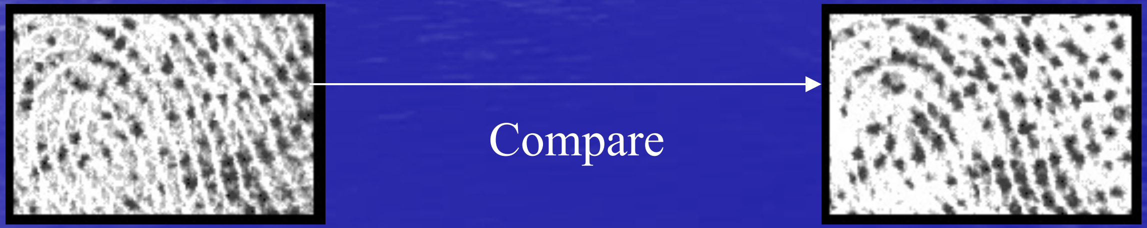
- Due to the poor conditions of latent fingerprints, today's fingerprint technology operates poorly when presented a latent fingerprint image. It is extremely difficult for the automated system to accurately classify latent fingerprints and reliably locate the minutiae in the image.
- Consequently, human fingerprint experts, called latent examiners, must analyze and manually mark up each latent fingerprint in preparation for matching.

Latent Fingerprints

- FBI and NIST collaboratively developed a specialized workstation called the Universal Latent Workstation (ULW).
- FBI has chosen to distribute the ULW freely upon request.

Fingerprint Matching

- The fingerprint matcher compares data from the input search print against all appropriate records in the database to determine if a probable match exists.
- Minutiae relationships, one to another are compared. Not as locations within an X-Y co-ordinate framework, but as linked relationships within a global context.



Compare

Live image

Stored image

Fingerprint Matching

- Each template comprises a multiplicity of information chunks, every information chunk representing a minutia and comprising a site, a minutia slant and a neighborhood.
- Each site is represented by two coordinates. [l = (x,y)]
- The neighborhood comprises of positional parameters with respect to a chosen minutia for a predetermined figure of neighbor minutiae. In single embodiment, a neighborhood border is drown about the chosen minutia and neighbor minutiae are chosen from the enclosed region. [theta]
- A live template is compared to a stored measured template chunk-by-chunk. A chunk from the template is loaded in a random access memory (RAM).

Fingerprint Matching

- The site, minutia slant and neighborhood of the reference information chunk are compared with the site, minutia slant and neighborhood of the stored template (latent) information chunk by information chunk.
- The neighborhoods are compared by comparing every positional argument. If every positional parameters match, the neighbors match. If a predetermined figure of neighbor matches is met, the neighborhoods match.
- If the matching rate of all information chunks is equivalent to or superior to the predetermined information chunk rate, the live template matches the stored (latent) template.

Characteristics of Fingerprint Technology

- Biometric (Fingerprint) Strengths
  - Finger tip most mature measure
  - Accepted reliability
  - High quality images
  - Small physical size
  - Low cost
  - Low False Acceptance Rate (FAR)
  - Small template (less than 500 bytes)

Characteristics of Fingerprint Technology

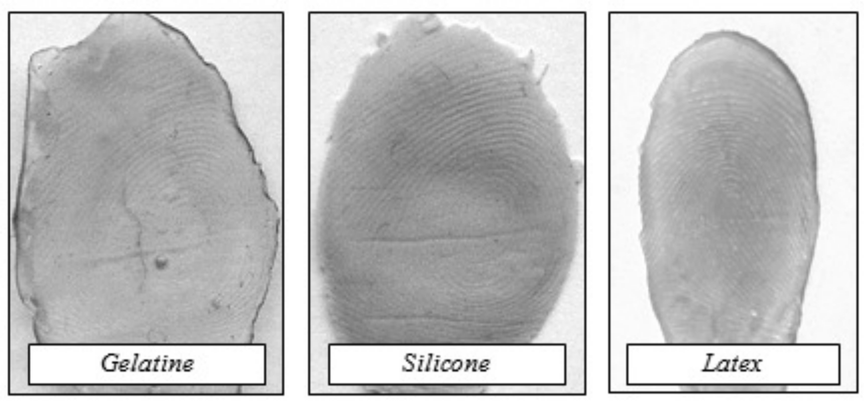
- Biometric (Fingerprint weaknesses)
  - Requires careful enrollment
  - Potential high False Reject Rate (FRR) due to:
    - Pressing too hard, scarring, misalignment, dirt
  - Vendor incompatibility
  - Cultural issues
    - Physical contact requirement a negative in Japan
    - Perceived privacy issues with North America

Fake Finger Detection

- As any other authentication technique, fingerprint recognition is not totally spoof-proof.
- The main potential threats for fingerprint-based systems are:
  - attacking the communication channels, including replay attacks on the channel between the sensor and the rest of the system;
  - attacking specific software modules (e.g. replacing the feature extractor or the matcher with a Trojan horse);
  - attacking the database of enrolled templates;
  - presenting fake fingers to the sensor.

Fake Finger Detection

- The feasibility of the last type of attack has been reported by some researchers: they showed that it is actually possible to spoof some fingerprint recognition systems with well-made fake fingertips, created with the collaboration of the fingerprint owner or from a latent fingerprint: in the latter case the procedure is more difficult but still possible.



Fake Finger Detection

- Based on the analysis of skin distortion.
  - The user is required to move his finger while pressing it against the scanner surface, thus deliberately exaggerating the skin distortion.
  - When a real finger moves on a scanner surface, it produces a significant amount of distortion, which can be observed to be quite different from that produced by fake fingers.
  - Usually fake fingers are more rigid than skin, then the distortion is definitely lower; even if highly elastic materials are used, it seems very difficult to precisely emulate the specific way a real finger is distorted, because the behavior is related to the way the external skin is anchored to the underlying derma and influenced by the position and shape of the finger bone.
- Based on odor analysis.
  - Electronic noses are used with the aim of detecting the odor of those materials that are typically used to create fake fingers (e.g. silicone or gelatin).

Advance of Fingerprint Technology

- As fingerprint technology matures, variations in the technology also increase including:
  - Optical – finger is scanned on a platen (glass, plastic or coasted glass/plastic).
  - Silicon – uses a silicon chip to read the capacitance value of the fingerprint.
  - Ultrasound – requires a large scanning device. It is appealing because it can better permeate dirt.

Change of Fingerprint data

- The matching accuracy of a biometrics-based authentication system relies on the stability (permanence) of the biometric data associated with an individual over time.
- In reality, however, the biometric data acquired from an individual is susceptible to changes introduced due to improper interaction with the sensor (e.g., partial fingerprints, change in pose during face-image acquisition), modifications in sensor characteristics (e.g., optical vs. solid-state fingerprint sensor), variations in environmental factors (e.g., dry weather resulting in faint fingerprints) and temporary alterations in the biometric trait itself (e.g., cuts/scars on fingerprints).

Change of Fingerprint data

- In other words, the biometric measurements tend to have a large intra-class variability.
- Thus, it is possible for the stored template data to be significantly different from those obtained during authentication, resulting in an inferior performance (higher false rejects) of the biometric system.

Evaluation of Fingerprint Technology

- There are two categories of fingerprint matching techniques: minutiae-based and correlation based.
  - Minutiae-based techniques first find minutiae points and then map their relative placement on the finger.
  - The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach.

Evaluation of Fingerprint Technology

- Minutiae-based processing has problems including:
  - In real life you would have impressions made at separate times and subject to different pressure distortions.
  - On the average, many of these images are relatively clean and clear, however, in many of the actually crime scenes, prints are anything but clear.
  - There are cases where it is not easy to have a core pattern and a delta but only a latent that could be a fingertip, palm or even foot impression
  - The method does not take into account the global pattern of ridges and furrows.

Evaluation of Fingerprint Technology

- Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns.
- Local ridge structures can not be completely characterized by minutiae.
- The solution is to find an alternate representation of fingerprints which captures more local information and yields a fixed length code for the fingerprint.

Evaluation of Fingerprint Technology

- Correlation-based processing has its own problems including:
  - Correlation-based techniques require the precise location of a registration point
  - It is also affected by image translation and rotation.

Hands-On Lab of Finger Biometric

1. Download and install NIST Fingerprint Image Software 2
2. Test and Demo Command PCASYS, MINDTCT, NFIQ and BOZORTH3
3. PCASYS (PACSYSX) and MINDTCT are available in NIST Biometric Image Software.
4. You may need Perforce to download NBIS software.