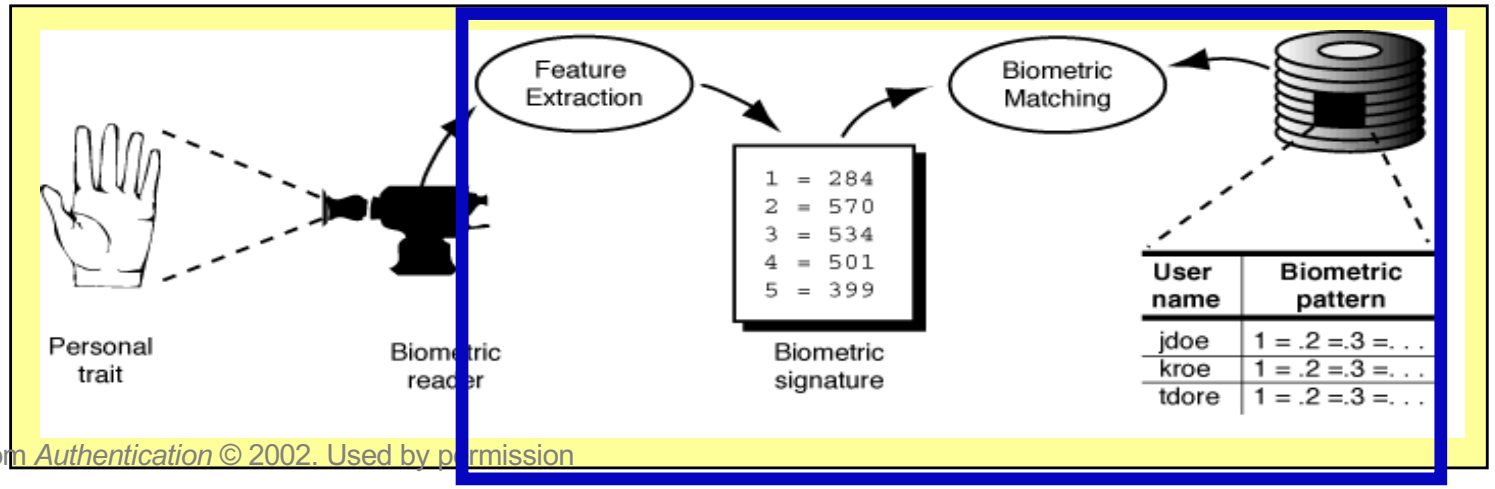
Spoofing,Fingerprint

Michele Nappi

mnappi@unisa.it
089-963334

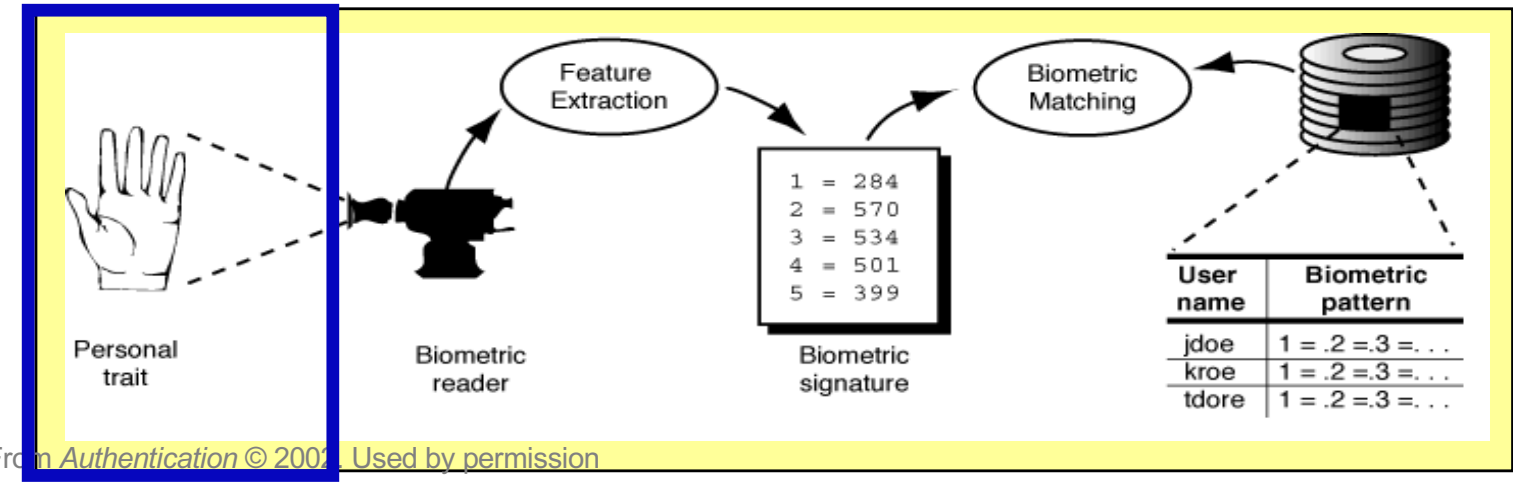
Sicurezza dei Sistemi Biometrici



From *Authentication* © 2002. Used by permission

Digital Spoofing

Physical Spoofing



From *Authentication* © 2002. Used by permission

Sicurezza dei Sistemi Biometrici

Test di violabilità di sistemi biometrici in commercio hanno dimostrato che molti sono vulnerabili a:

- Digital spoofing
  - Attacchi replay: un hacker ruba l'immagine digitalizzata e se ne serve in un'altra occasione
  - Attacchi di manipolazione del valore di soglia tipico di ciascun sistema (obiettivo: aumentare il FAR)
  - Inserimento nel sistema di un "cavallo di Troia" per fornire dati erronei al programma di estrazione dei parametri biometrici dall'immagine scansionata.
  - Alterazione del risultato finale del processo biometrico: l'inserimento e l'analisi dei dati sono corretti, ma il risultato generato dal sistema è alterato
- Physical spoofing
  - Simulazione fisica della biometrica

Sicurezza dei Sistemi Biometrici (cont.)

Cosa succede se vengono rubati i dati biometrici di un individuo?

- La possibilità di utilizzare questa caratteristica biometrica risulta compromessa per sempre:
  - "***I pollici sono solo due. Se qualcuno ruba i tuoi dati biometrici, saranno persi per sempre. Niente potrà ricostituirli***"
- Se qualcuno rubasse le caratteristiche biometriche del nostro volto, della nostra retina o iride sarebbe ancora peggio: non ne abbiamo altre!
- Vulnerabilità dei sistemi biometrici: le implementazioni delle tecniche biometriche sono scarse, non esistono criteri unificati a livello mondiale per la valutazione della sicurezza dei sistemi biometrici.

- Per garantire la sicurezza dei dati biometrici occorre
  - **Adozione di crittosistemi e relativi segreti a tutela del dato biometrico (Strong cryptography and crypto-card based solutions)**
- La memorizzazione del dato biometrico è molto sensibile occorre adottare tecniche per la sua difesa, in quanto una volta rubato il dato non è rigenerabile.

Biometrics at Airports

Country	Programme Name	Airport	Biometrics Technology	Status
Australia	SmartGate	BNE, CNS	Face e-Passport	-Introduced August 2007 -For Australian and New Zealand citizens -Entry only
Austria	ABC System	New terminal : VIE	Face	-Planned pilot
Canada, USA	NEXUS Air	JFK, LAX, ATL, ORD, SFO, MCO, YVR	Iris Smartcard	-Entry only -Operational -For US and CAN citizens, and permanent residents of at least three years
China	e-Channel, APC, AVC	HKG	Fingerprint Smartcard	-Entry and exit -Operational -For citizens and permanent residents
Czech Republic	ABC System	PRG	Face	-Planned Pilot : -Technical study available -Fall 2009 pilot
Dubai	E-Gate	DXB	Fingerprint Smartcard	-Entry only -Operational -available for all travellers with entry permit
Finland	ABC System	HEL Vantaa Airport + Pilot at Vaalima Land Border (Oct. 2009)	Face	-Pilot start: July 2008 - Operational since April 2009

Biometrics at Airports

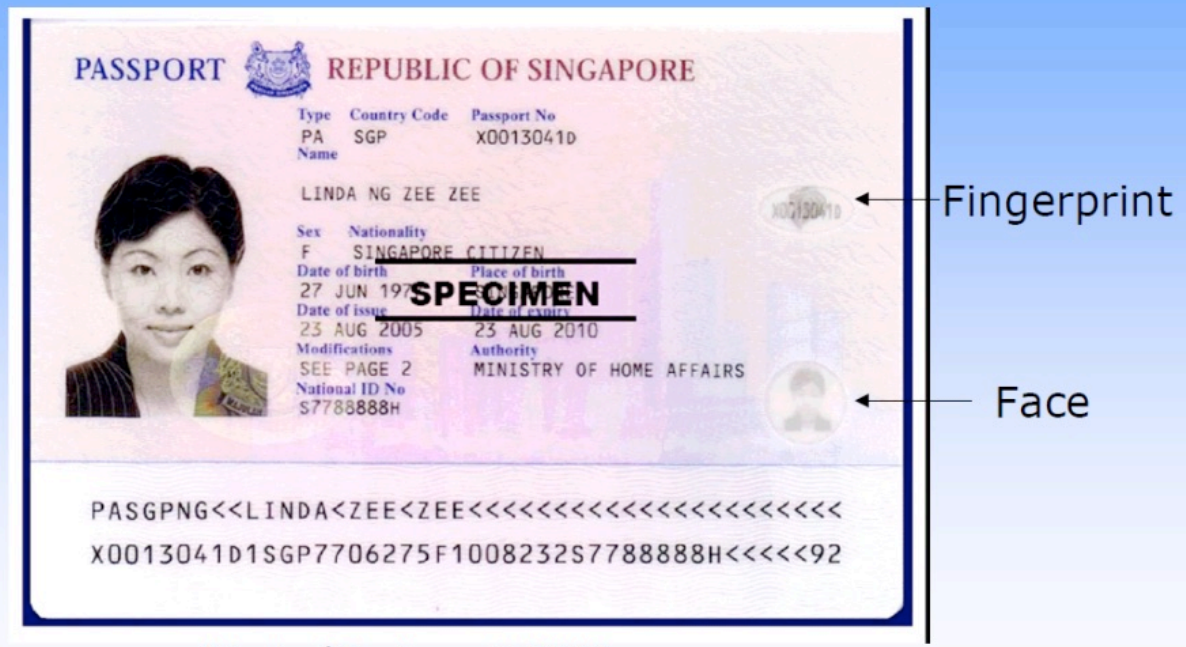
France	PARAFES	CDG	e-Passport Fingerprint	- Pilot since August 2007 - Entry and exit - For EU/ EEA and CH
Germany	ABG	FRA	Databank Iris	- Entry and exit - For EU/ EEA and CH, and permanent residents
Germany	EasyPASS	FRA	e-Passport Face	- Pilot since October 2009 - Entry and exit - For EU/ EEA and CH
Malaysia	Immigration Autogate	KUL, PEN, BKI, MYY, KCH, LGK	Fingerprint e-Passport e-ID (MyKad)	- Introduced August 2000 - Entry and exit - For Malaysian citizens
NL	PRIVIUM	AMS	Iris Smartcard	- Introduced October 2001 - Entry and exit -Targets frequent flyers with an EU nationality
NL	No-Q	AMS	e-Passport Face	- Pilot Q1 2010 - Exit
Portugal	RAPID	LIS, FAO, FNC, OPO Plans to expand to seaports	Face e-Passports	- Introduced May 2007 - For EU/ EEA and CH - Entry and exit
Singapore	(eIACS) enhanced Immigration Automated Clearance System	SIN	Fingerprint Smartcard	- Operational since March 2006 - Entry and exit - For citizens and permanent residents

EBF
EUROPEAN BIOMETRICS FORUM

Biometrics at Airports

Country	Programme Name	Airport	Biometrics Technology	Status
Spain	ABC System	MAD	Face Fingerprint	-Planned pilot -2009 finalizing technical solutions -2010 pilot
Switzerland	Augreko	ZRH	Face e-Passport	-Planned pilot from mid 2010
UK	ABC System	MAN, STN + 10 other airports	Face	-Pilots
UK	IRIS	LHR, LGW, MAN, BHX, STN	Iris Databank	-Operational since January 2006 -For EU/ EEA and CH, permanent residents and Visa holders -Entry only
USA	Global Entry	20 major airports US	Databank Fingerprint	-Entry -Frequent travellers -Operational -For users of NEXUS, citizens of US & CAN, and pre-screened third countries citizens (currently only NL through FLUX)
USA/ NL	FLUX -Alliance	20 major airports US + AMS	US: Databank Fingerprint NL: Iris SmartCard	-Pilot until April 2010 -Combination of existing GlobalEntry and PRIVIUM programmes -Pre-registration & vetting (extensive background checks)

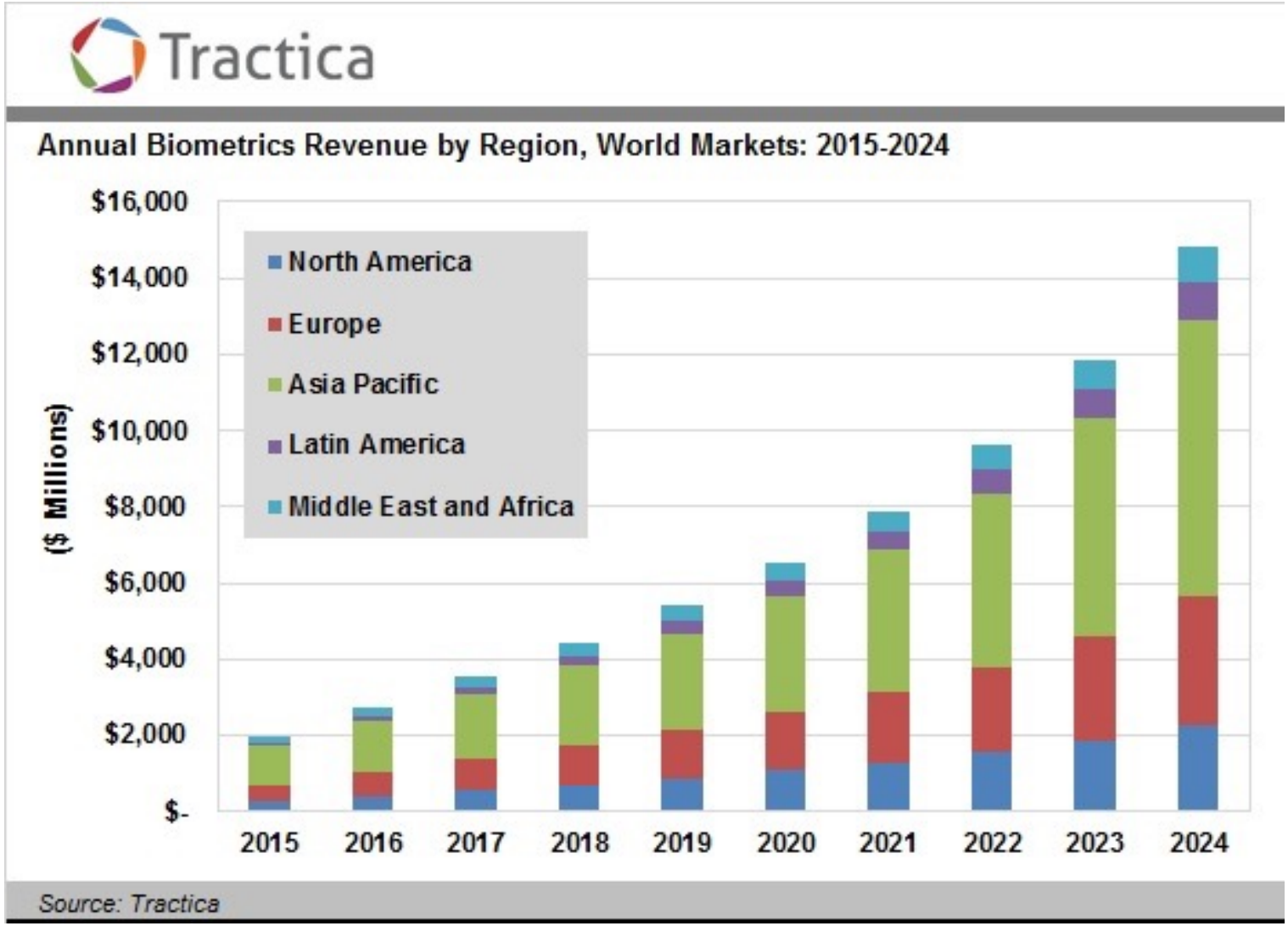
Singapore Biometric Passport



Started in August 2006

Slide by courtesy of Anil K. Jain

Biometric Revenues



Quote di Mercato

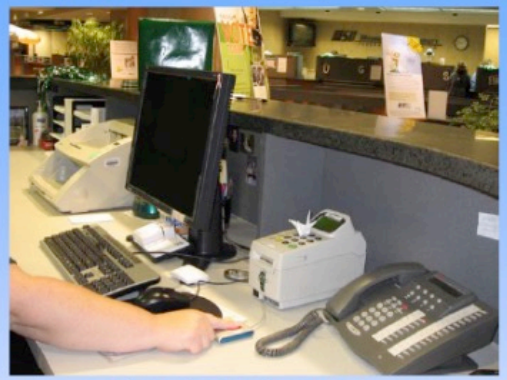
Biometrics	*Vendors*	*Market Share*	*Applications*
Fingerprint	54%	34%	Law enforcement; civil government; enterprise security; medical and financial transactions
Hand Geometry	5%	26%	Time and attendance systems, physical access
Face Recognition	23%	15%	Transaction authentication; picture ID duplication prevention; surveillance
Voice Authentication	10%	11%	Security, V-commerce
Iris Recognition	3%	9%	Banking, access control

Forensic Identity

- Does Charlie have a criminal record?
- Should John be granted a visa?
- Does Alice already have a driver license?
- Is Mary authorized to enter the facility?
- Can Steve access the website?
- Is Cathy the owner of the bank account?
- We rely on credentials: documents & secrets

Commercial Applications

Meijer supermarket, Okemos



MSU Federal Credit Union, East Lansing

Citibank, Singapore: pay by fingerprints

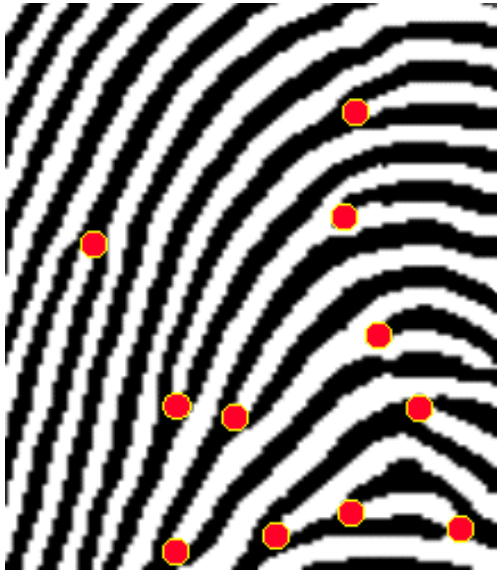
Time & Attendance; Hilton Waterfront Beach Resort

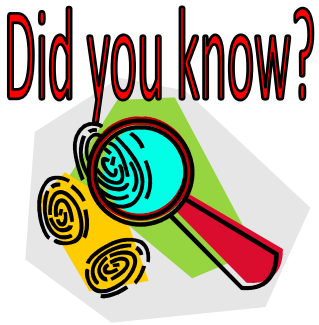
Slide by courtesy of Anil K. Jain

RIDGEOLOGY:

The study of the uniqueness of friction ridge structures and their use for personal identification.[1]

A fingerprint is made of a series of **ridges** and **valleys** on the surface of the finger. The uniqueness of a fingerprint can be determined by the **pattern** of ridges and valleys as well as the **minutiae points** (●), which are points where the ridge structure changes.





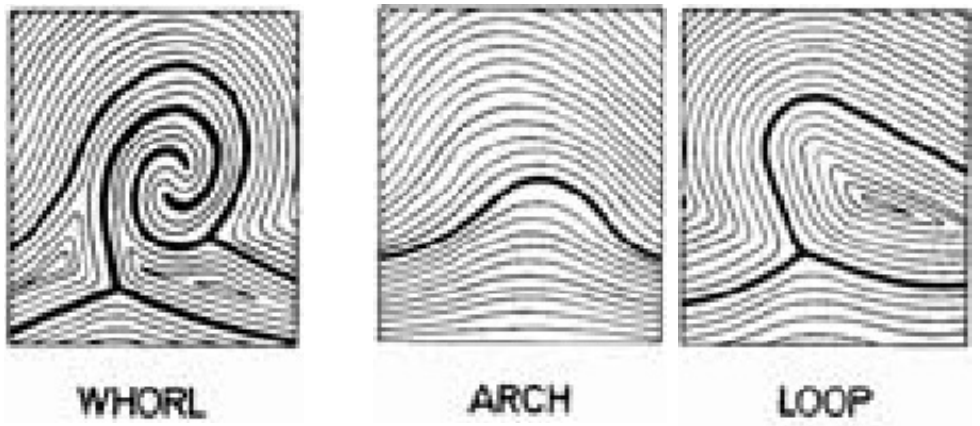
The **koala** is one of the few mammals (other than primates) that has fingerprints. In fact, koala fingerprints are remarkably similar to human fingerprints; even with an electron microscope, it can be quite difficult to distinguish between the two.

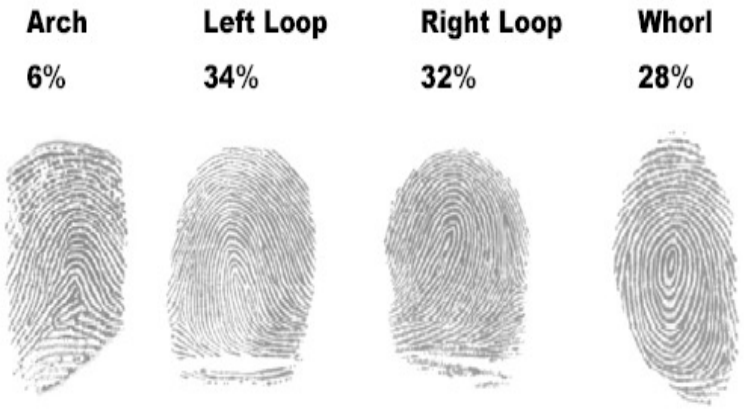
[1] *Introduction to Basic Ridgeology* by David Ashbaugh, May 1999

Image from http://www.cs.usyd.edu.au/~irena/minutia.gif

Fingerprint (cont.)

- Le caratteristiche globali **non sono sufficienti** per il riconoscimento
- Si utilizzano solo per classificare (clastering) le impronte (divisione in classi)

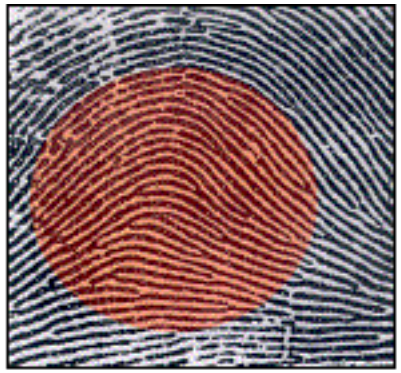




Fingerprints have general ridge patterns that permit them to be systematically classified.

LOOP

In a loop pattern, the ridges enter from either side, re-curve and pass out or tend to pass out the same side they entered.



ARCH

In an arch pattern the ridges enter from one side, make a rise in the center and exit generally on the opposite side.

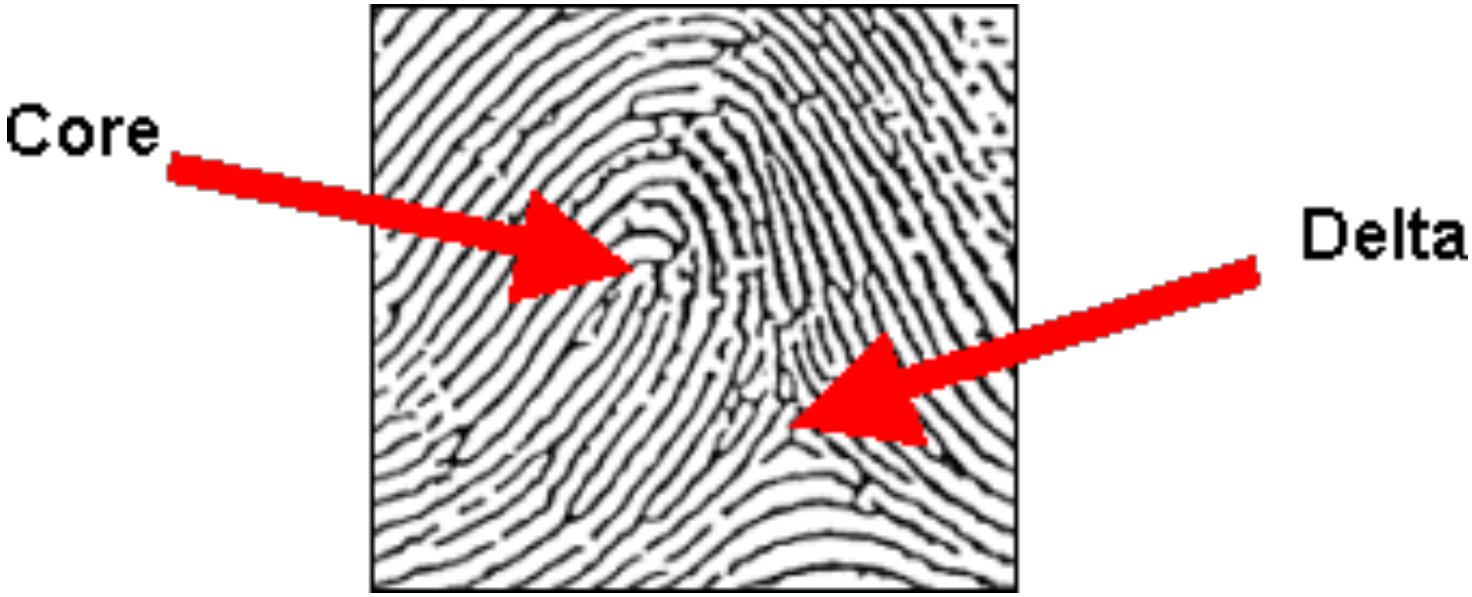
WHORL

In a whorl pattern, the ridges are usually circular.

- All fingerprints are divided into three classes on the basis of their general pattern: **loops**, **arches** and **whorls** (**LAW**).
- Each of the 3 patterns types have focal points which are used for classification.

BASIC PATTERN TYPES

LOOP



There are two focal points: the **Core**, or the center of the loop, and the **delta**. The **Delta** is the area of the pattern where there is a triangulation or a dividing of the ridges. When recording fingerprints, the delta and the area between the delta and the core must be completely recorded.

http://www.fbi.gov/hq/cjisd/takingfps.html

BASIC PATTERN TYPES

ARCH

The **Arch** pattern has **no delta** or **core**; but, it too, must be fully recorded so that its individual characteristics can be readily distinguished.

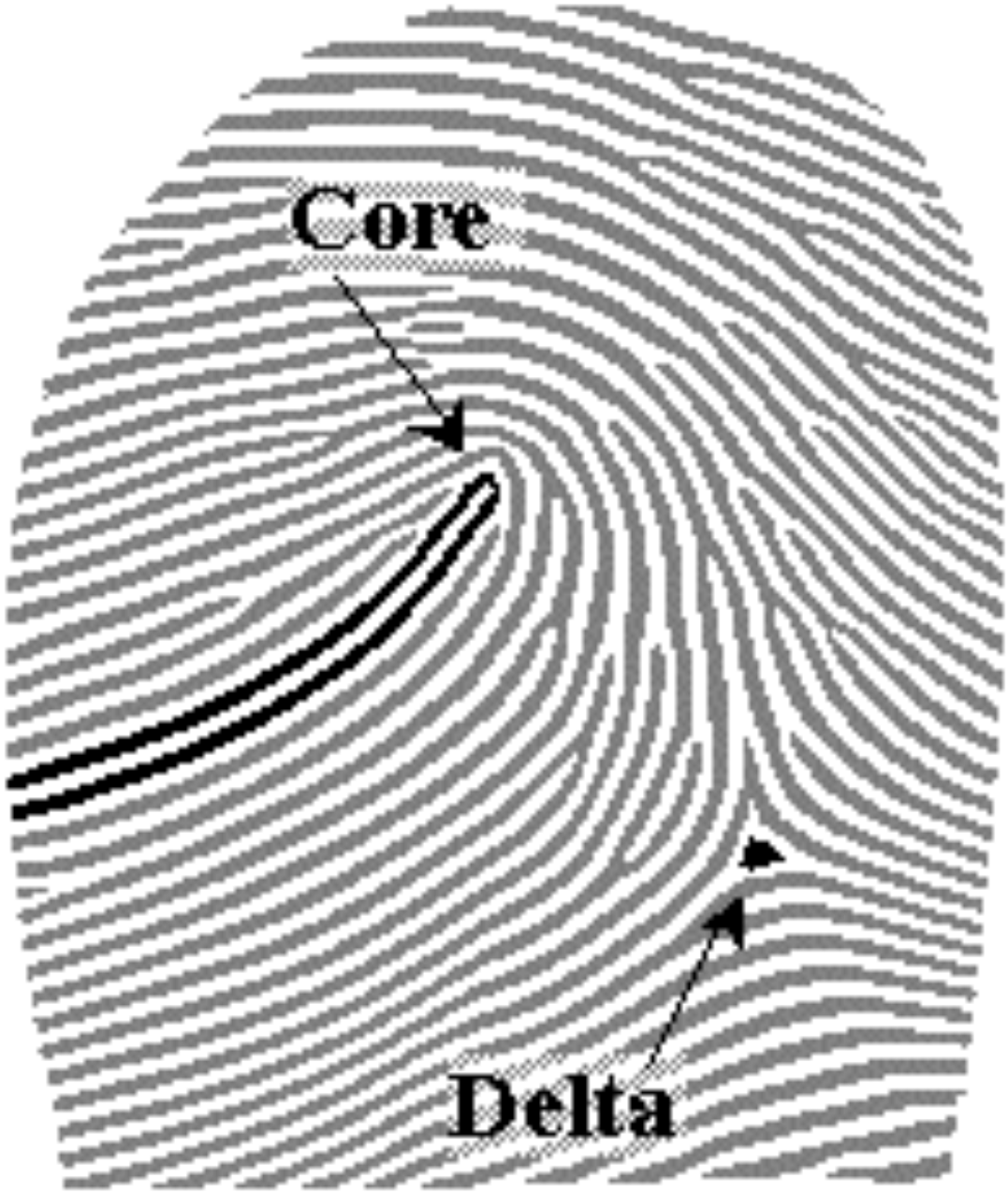
http://www.fbi.gov/hq/cjisd/takingfps.html

BASIC PATTERN TYPES

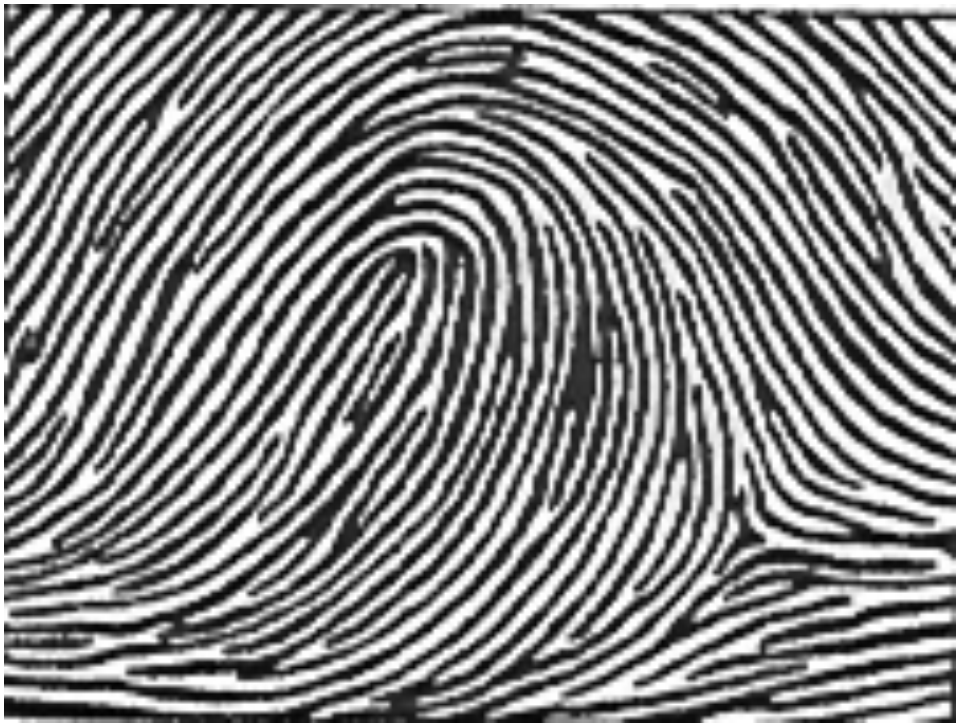
WHORL

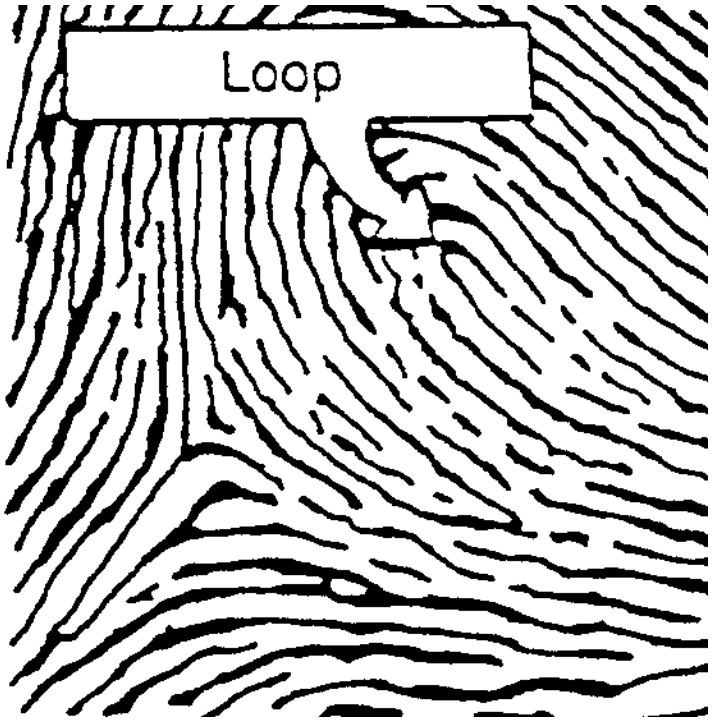
A **Whorl** pattern will have **two or more deltas**. For a whorl pattern, all deltas and the areas between them must be recorded.

http://www.fbi.gov/hq/cjisd/takingfps.html


Core
Delta

Loops (60-65 % of fingerprints)

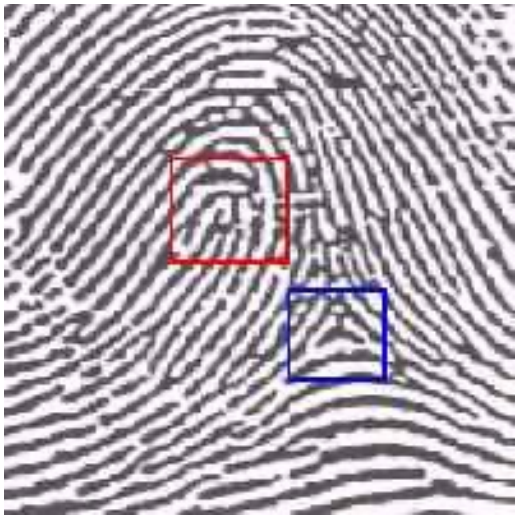




Loop patterns have lines that start on one side of the print, rise toward the center, turn back and leave on the same side from which they started

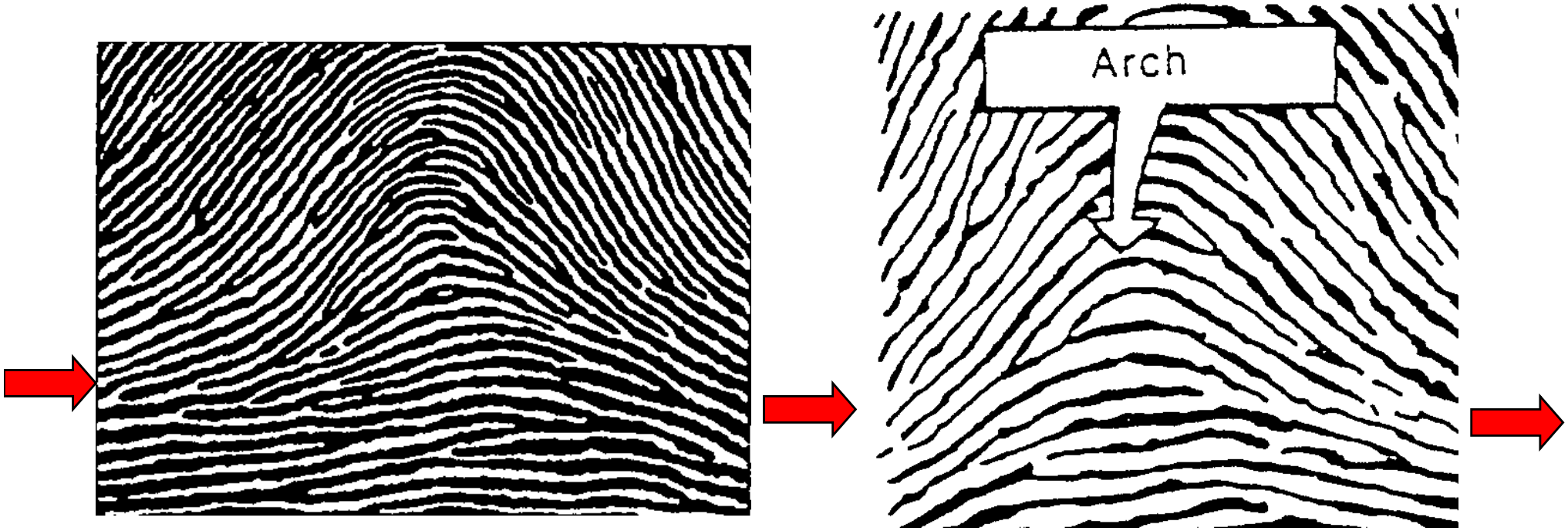
Loops

One **Delta** and **One Core**



Arches (5 % of fingerprints)

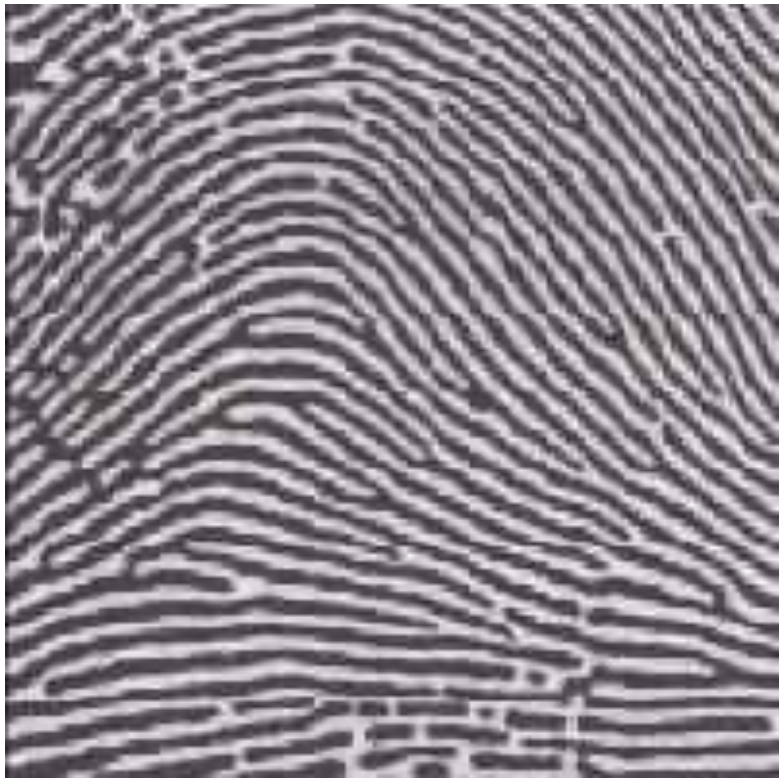
No Delta

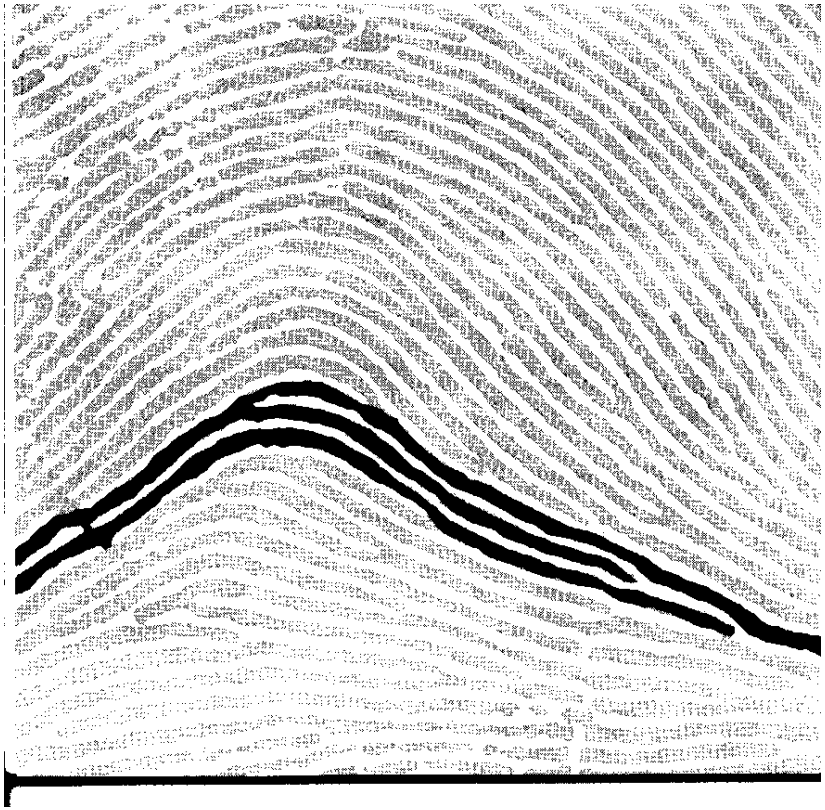


An Arch fingerprint has ridges that enter from one side, rise to a slight bump and exit out the opposite side from which they entered.

Plain Arch

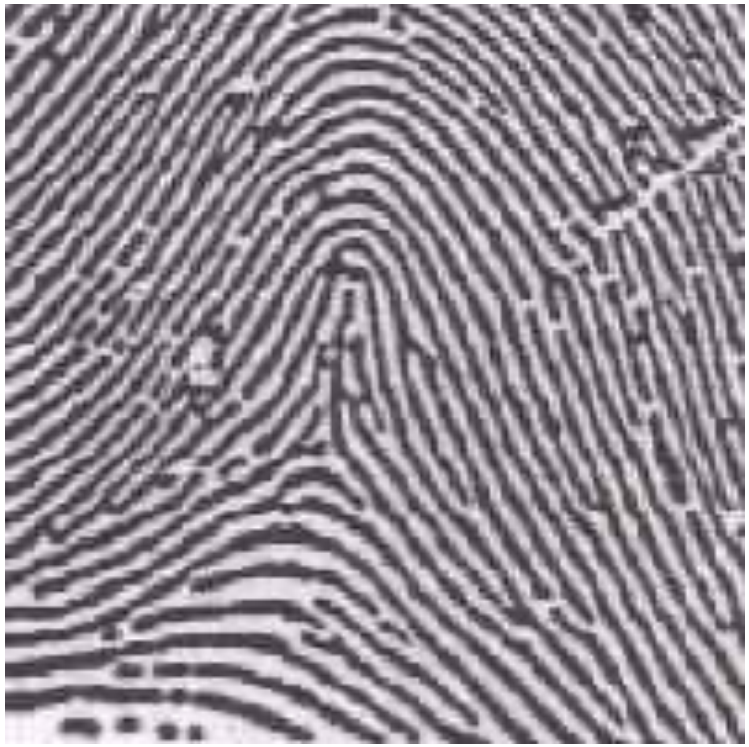
No Delta

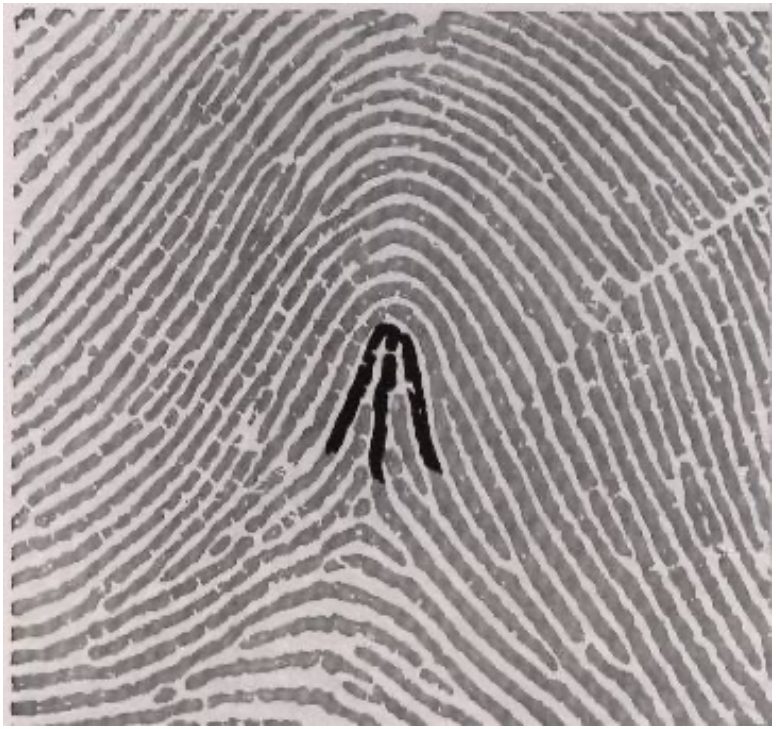




Tented Arch

No Delta

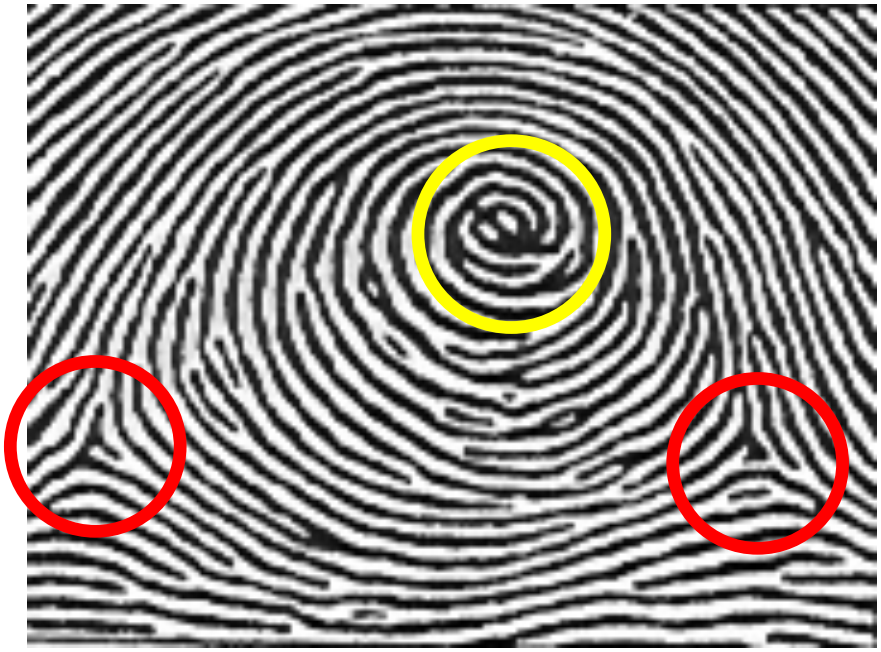


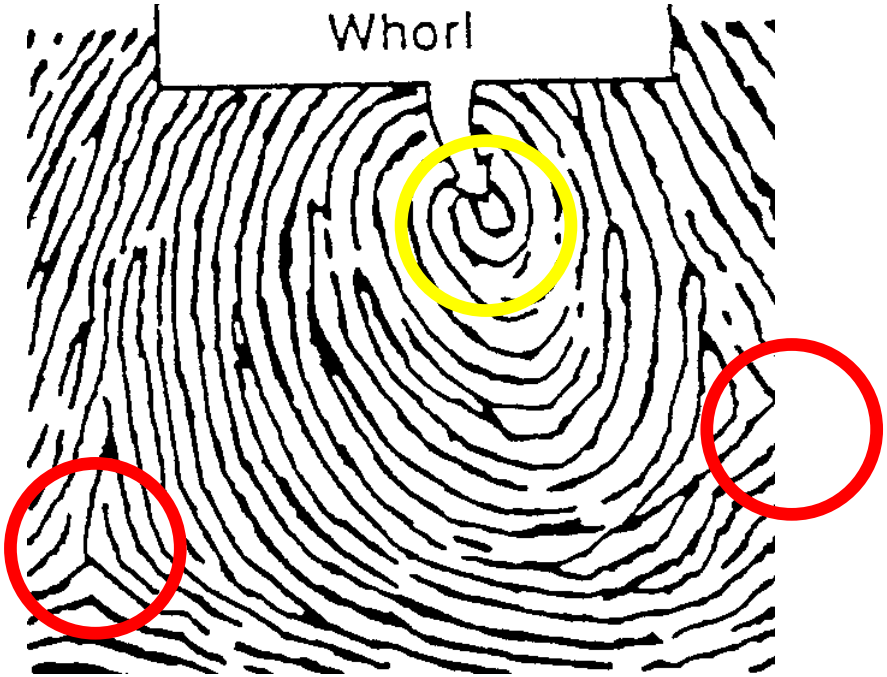


The tented arch is similar to the plain arch EXCEPT that instead of rising smoothly at the center, there is a **sharp spike**, or the ridges meet at an angle that is less than 90 degrees.

Whorls (30-35 % of fingerprints)

At least Two Deltas and One Core

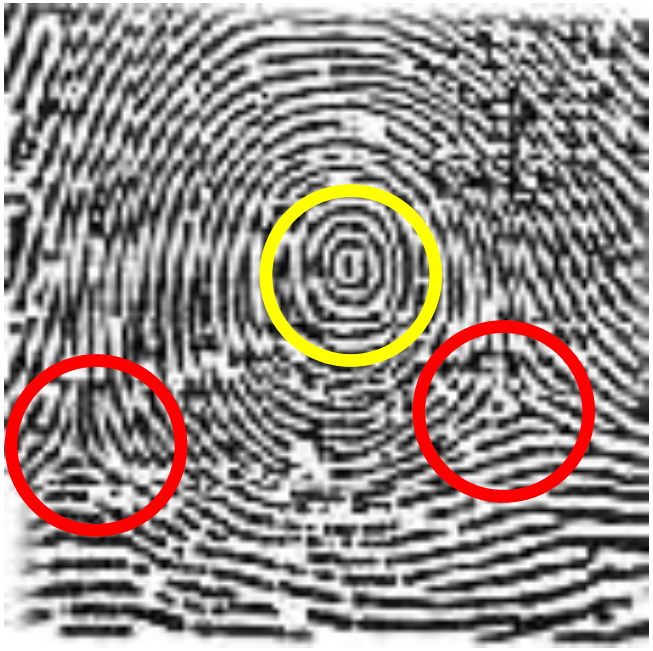


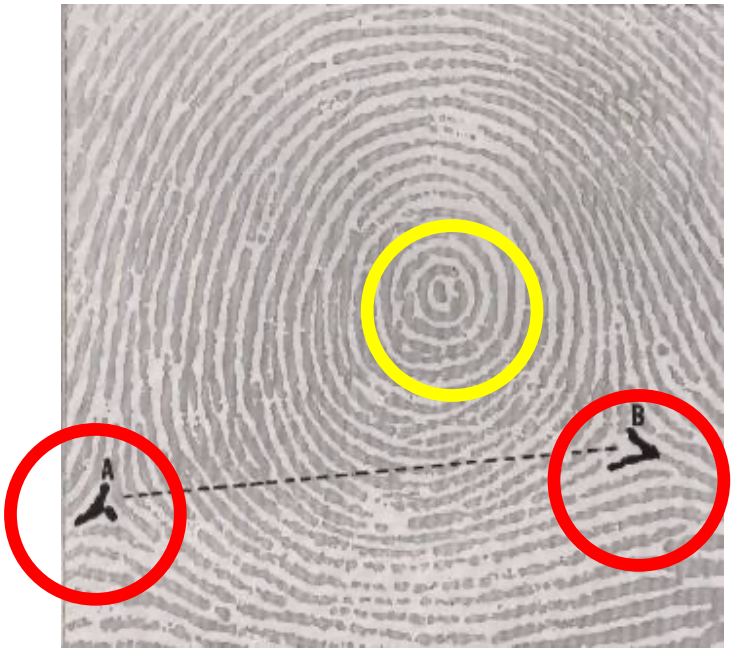


Whorls have at least one ridge that makes (or tends to make) a complete circuit. If a print has more than two deltas, it is most likely an accidental.

Plain Whorl

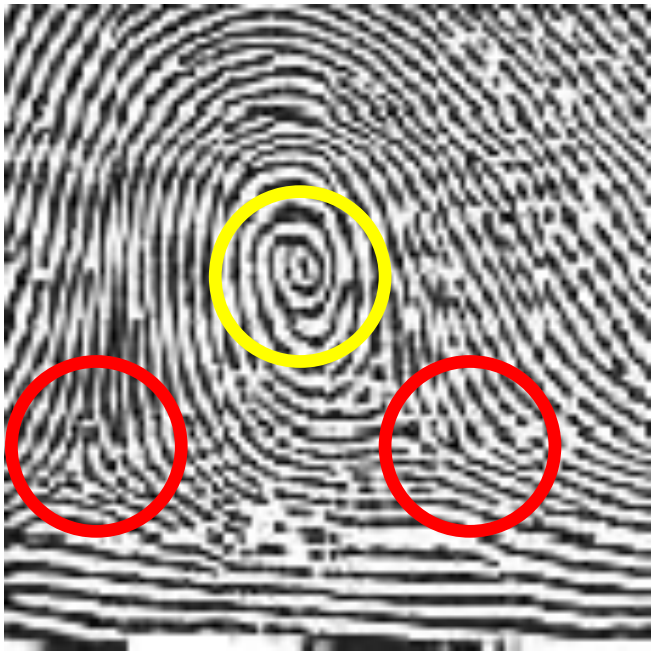
At least Two Deltas and One Core

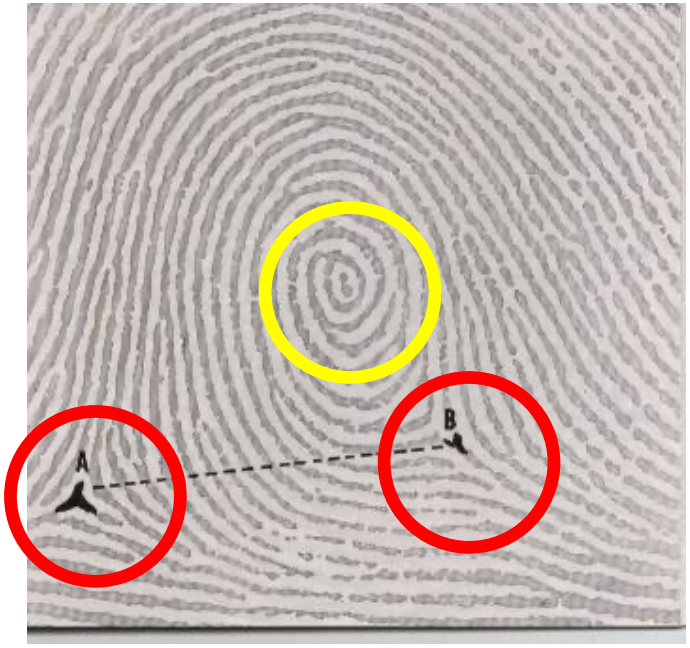




Central Pocket Loop Whorl

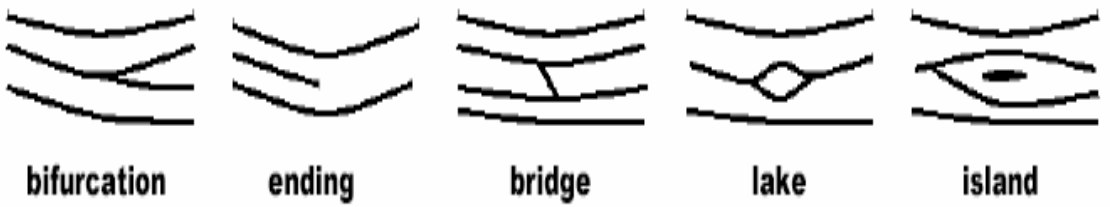
At least Two Deltas and One Core





Fingerprint (cont.)

- Le caratteristiche locali dette minuzie (singolarità) si utilizzano solo per il riconoscimento all'interno della classe prodotta dalle caratteristiche globali




Ridge Ending

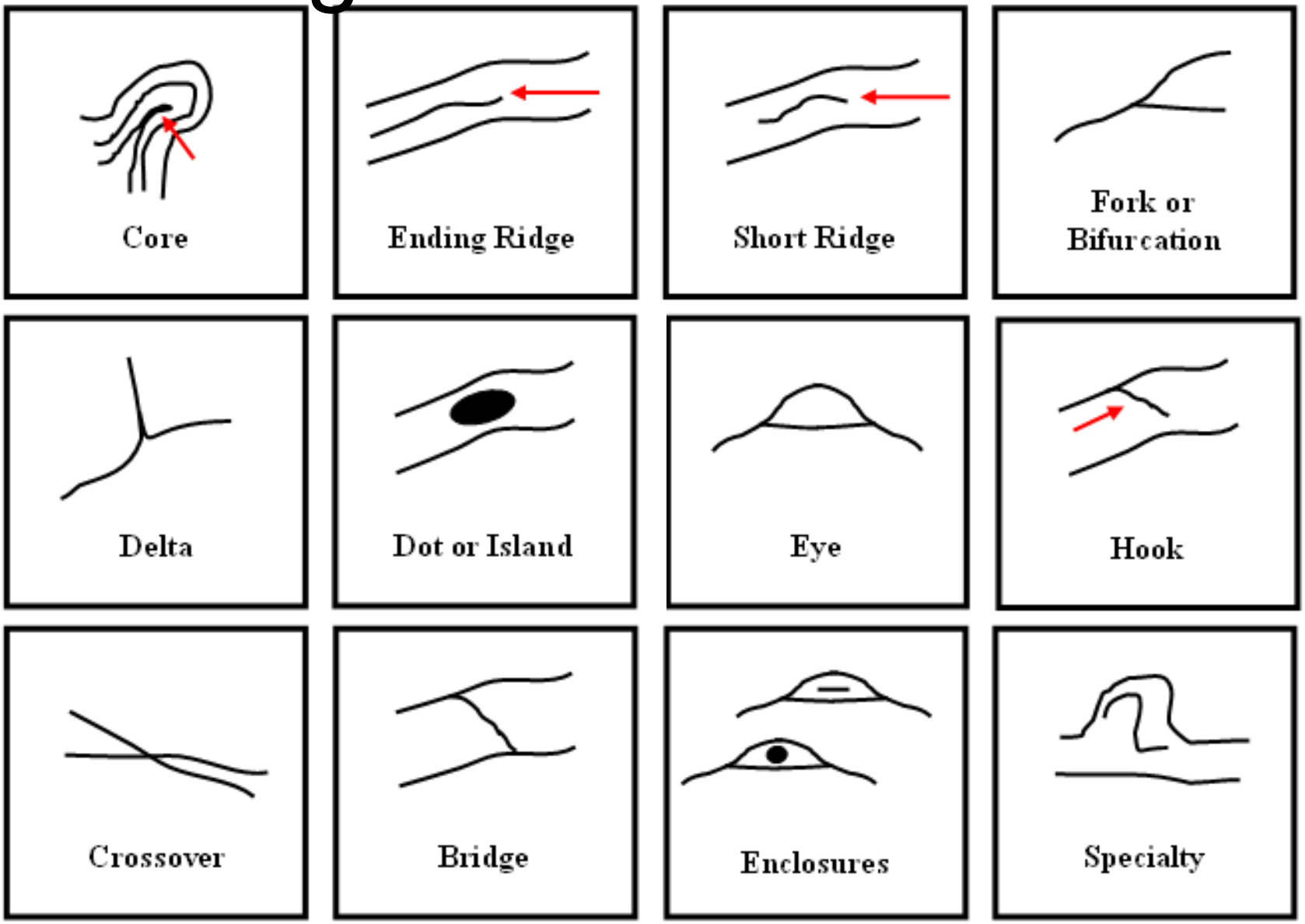

Ridge Bifurcation

Right Loop

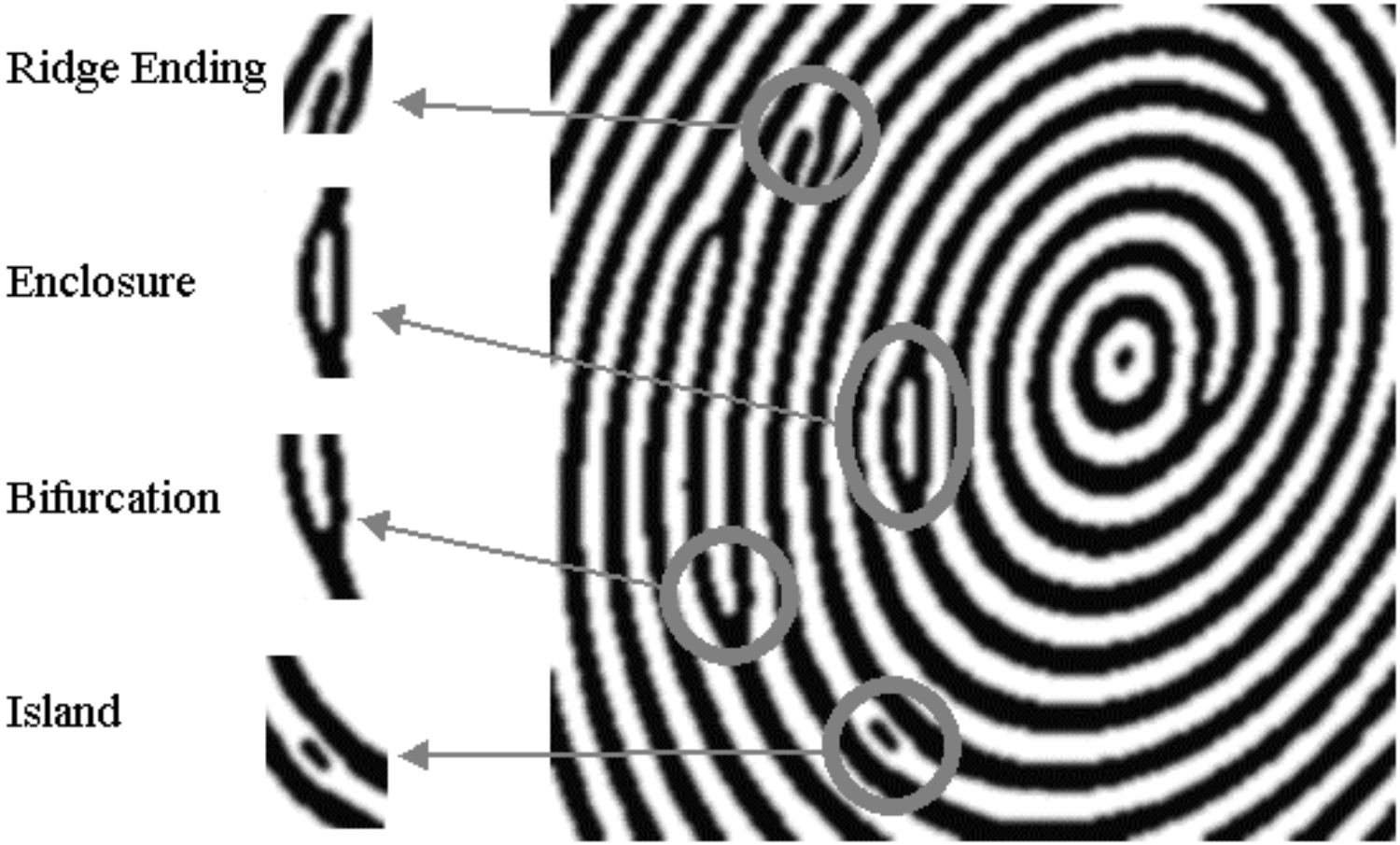
Right Loop with minutiae points

Ridge Characteristics

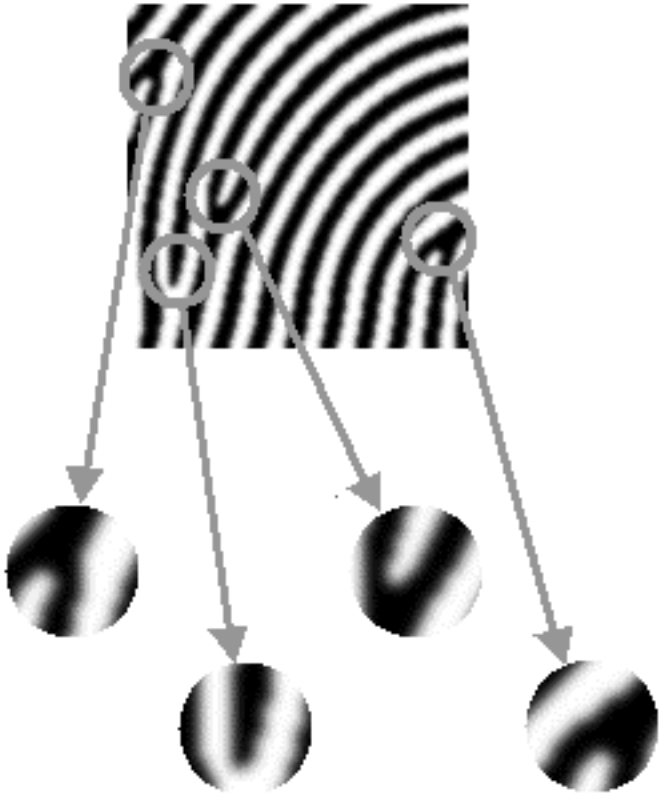
Ridge Characteristics

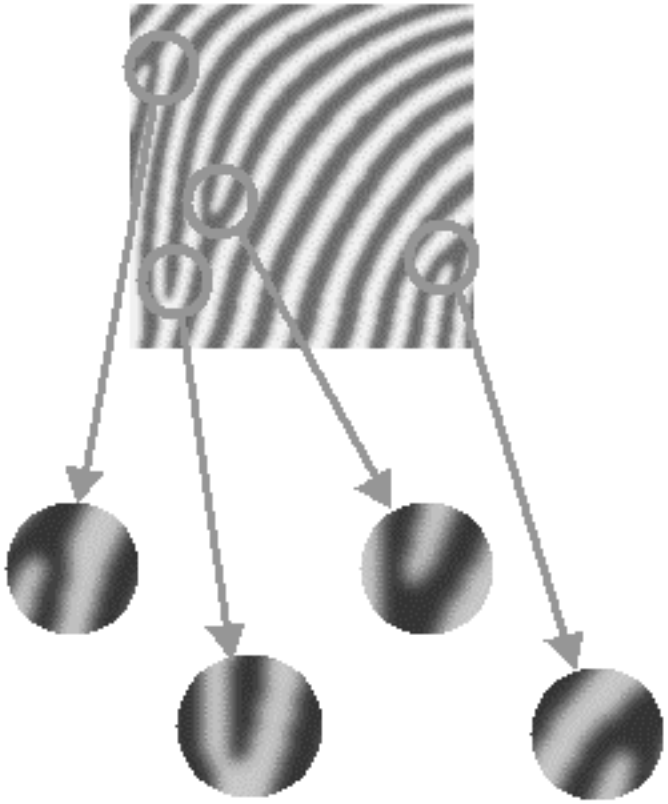


Minutiae



Do these print match?





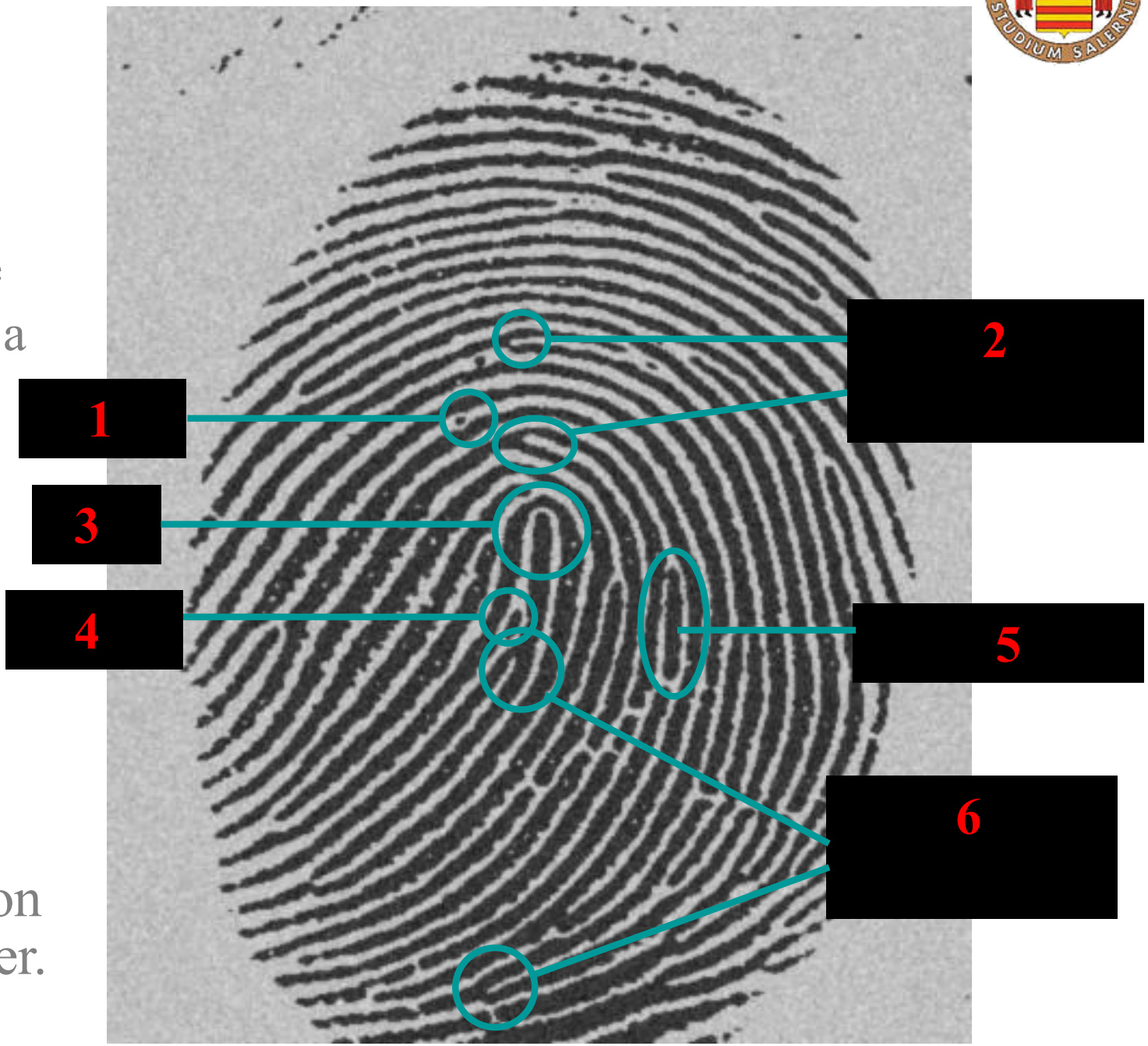
Examples of Ridge Characteristics

http://cnx.org/content/m12574/latest/properties.jpg

How many ridge characteristics can you identify in this fingerprint?

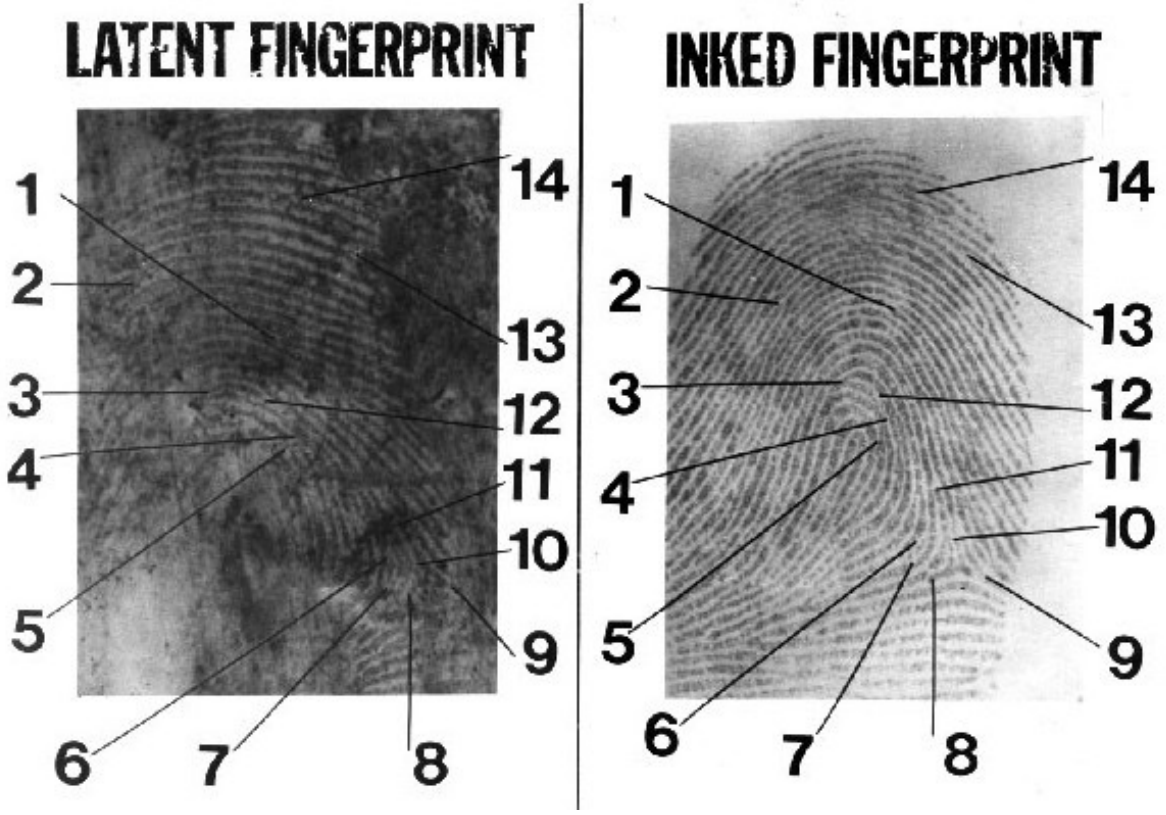
Note: Usually fingerprints from a crime scene are partials and only a small # of ridges are actually recovered from the scene.

There are **as many as 150 minutiae** (ridge characteristics) on the average finger.



http://www.dkfz.de/tbi/projects/bmcv/images/iu_it246_04s_fingerprint1.jpg

Fingerprint error



The above images depict an erroneous identification that was produced by an IAI Certified Latent Print Examiner employed by a small police department in the state of Illinois, US. The examiner had a four year college degree and passed the IAI CLPE certification exam. The Examiner's certification was revoked by the IAI Latent Print Certification Board because of this incorrect identification.

Ridge Characteristics

- IF two prints are said to be the same, they will have to reveal **ridge characteristics** that not only are **identical**, but have the **same relative location** to one another.

Ridge Characteristics

- When comparing prints, **8 to 16** identical ridge characteristics are usually needed to say that a match has occurred

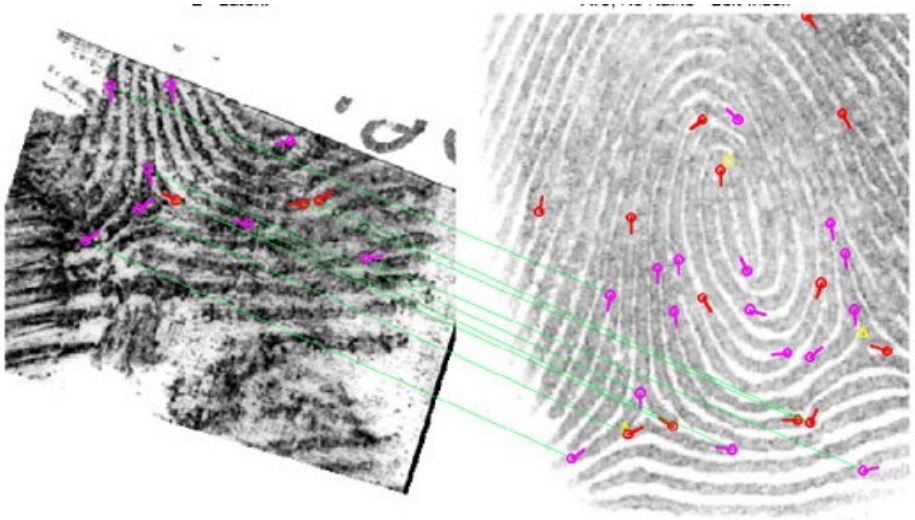
- The fingerprint expert uses his judgment to determine whether or not two ridges match.
  - In a judicial proceeding, an expert must demonstrate a point-by-point comparison in order to prove the identity of an individual.

- No statistical studies have been done to determine how many ridge comparisons are necessary

Fingerprint Identification

When minutiae on two different prints match, these are called points of **similarity** or points of **identification**. At this point there is **no** international standard for the number of points of identification required for a match between two fingerprints. However, the United Kingdom requires a minimum **16 points** while Australia requires **12 points**.

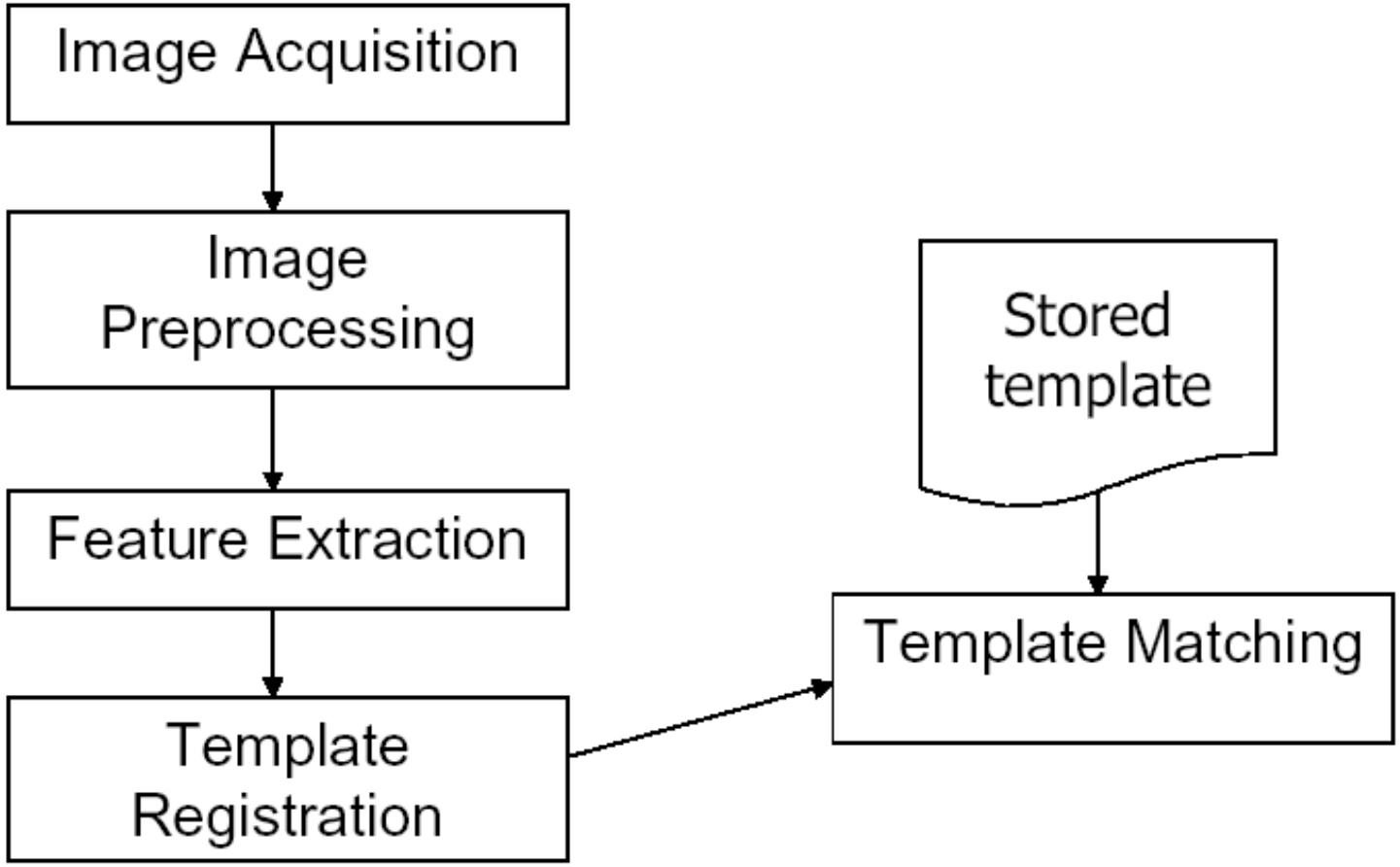
Automated Fingerprint Identification System (AFIS)



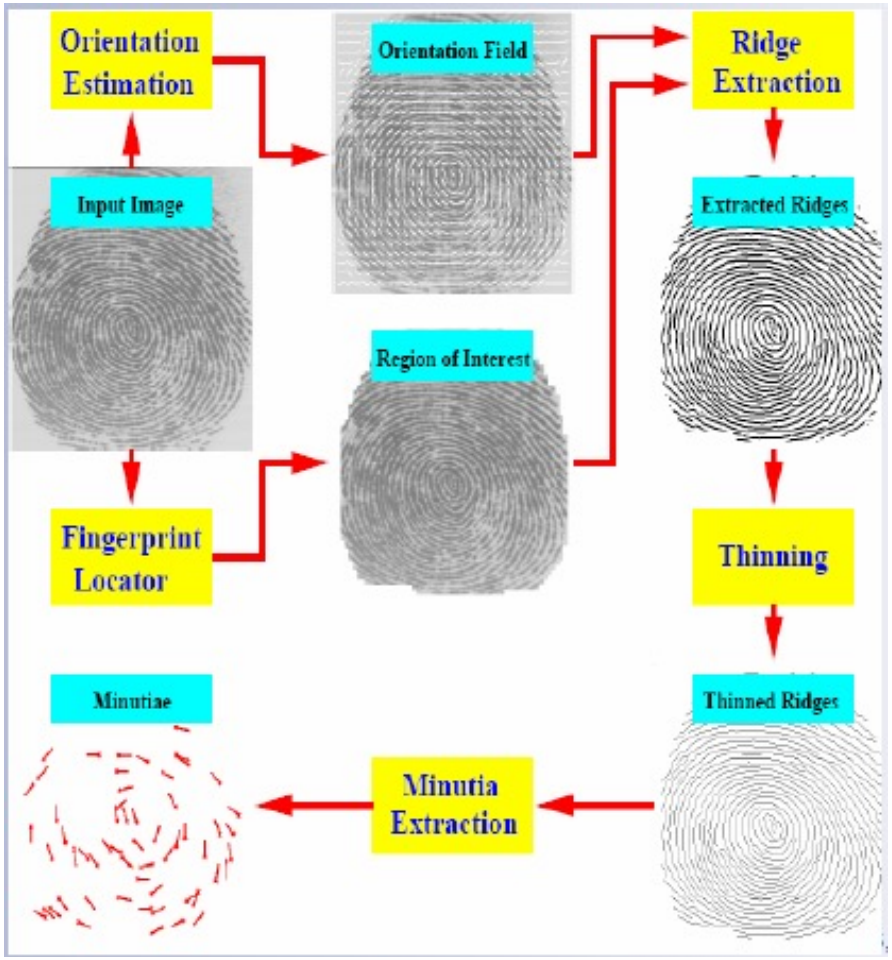
http://www.fdle.state.fl.us/CrimeLab/images/fingerrint%20comparison%20for%20afis.jpg

AFIS is a computerized system capable of reading, classifying, matching, and storing fingerprints for criminal justice agencies. Quality latent fingerprints are entered into the AFIS for a search for possible matches against the state maintained databases for fingerprint records to help establish the identity of unknown deceased persons or suspects in a criminal case.

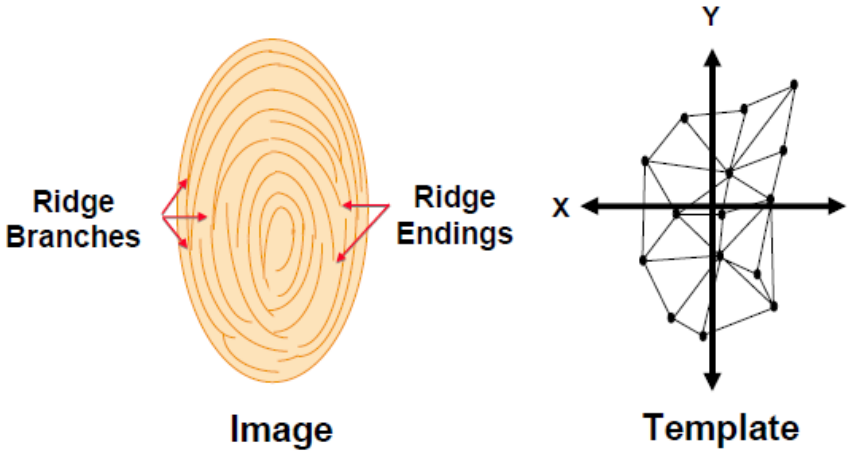
Automatic Verification System



Fingerprint Matching



Fonte: Paolo Lobato Correia



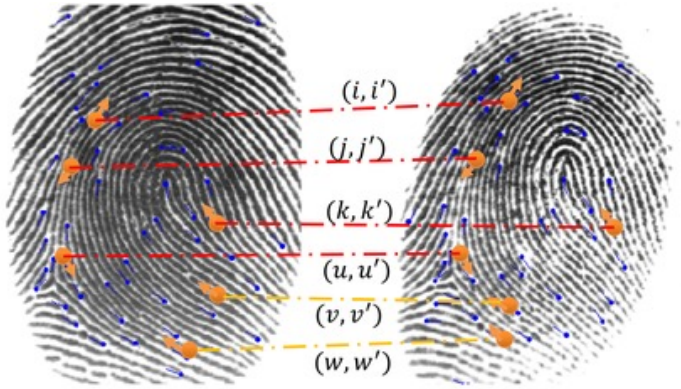
Fonte: IBIA

Feature Enhancement

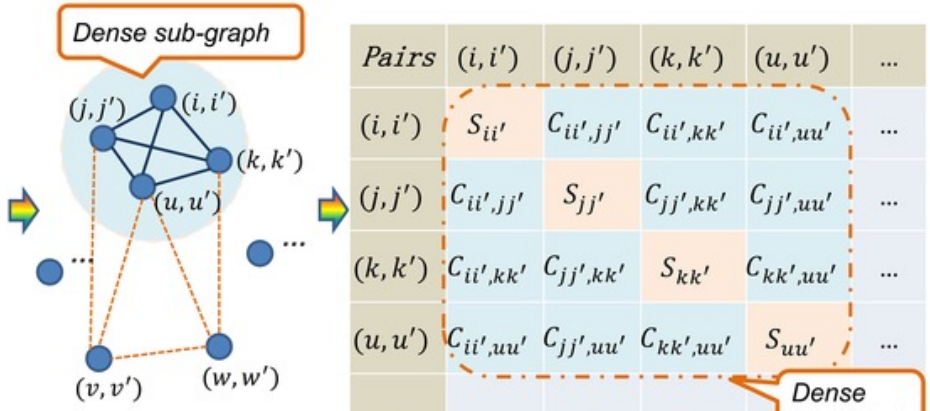
Original

Enhanced

Fingerprint Matching



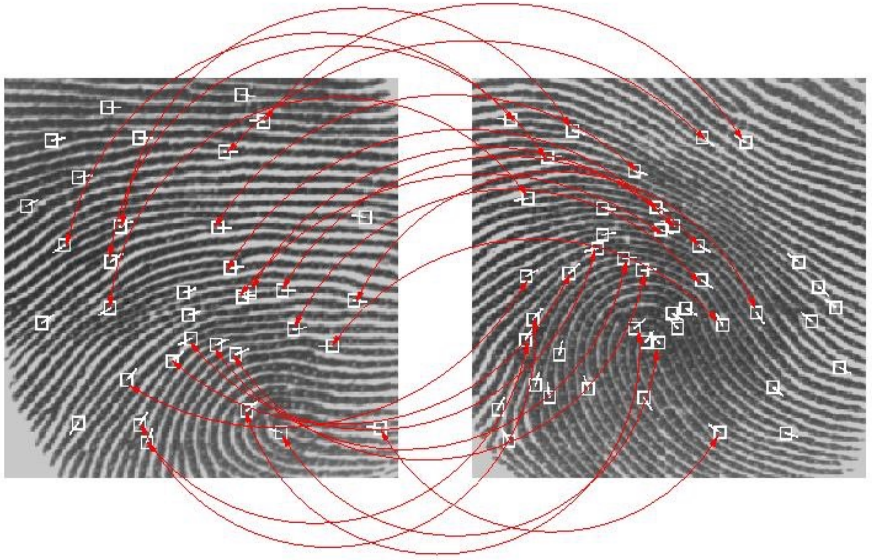
(a) A genuine match example
(Note: fingerprint images are from FVC2004 DB1 27-3 and 27-5)



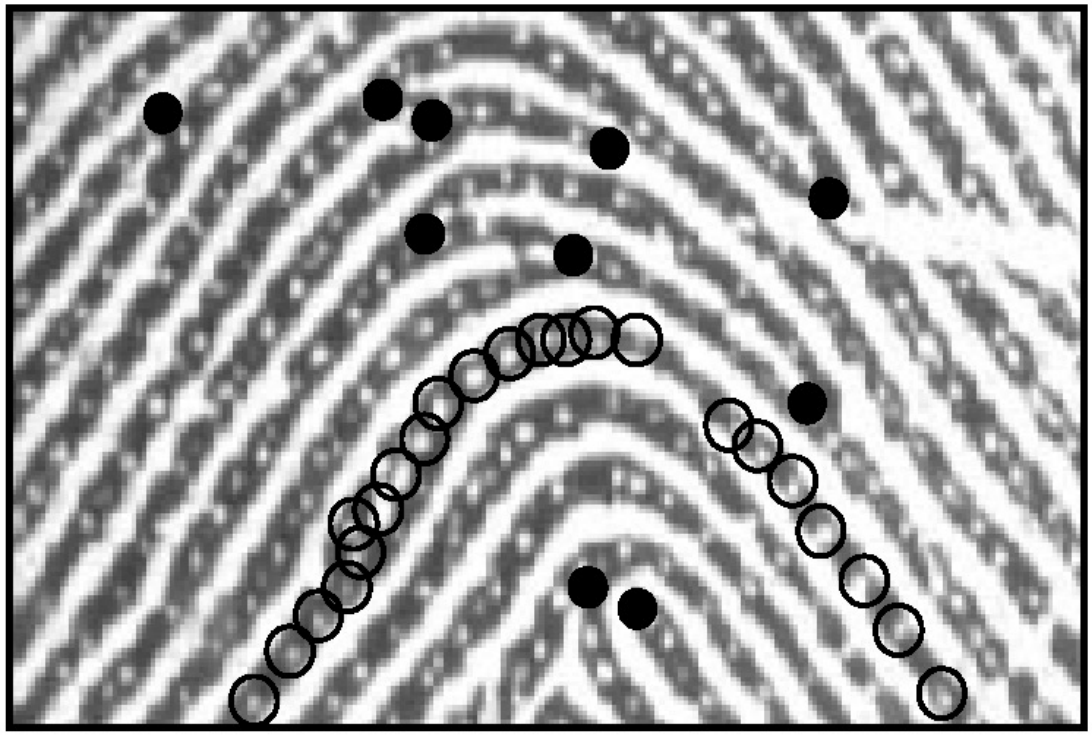
Pairs	(i,i')	(j,j')	(k,k')	(u,u')	...
(i,i')	$S_{ii'}$	$C_{ii',jj'}$	$C_{ii',kk'}$	$C_{ii',uu'}$	...
(j,j')	$C_{ii',jj'}$	$S_{jj'}$	$C_{jj',kk'}$	$C_{jj',uu'}$	...
(k,k')	$C_{ii',kk'}$	$C_{jj',kk'}$	$S_{kk'}$	$C_{kk',uu'}$	...
(u,u')	$C_{ii',uu'}$	$C_{jj',uu'}$	$C_{kk',uu'}$	$S_{uu'}$	...
...	...	...	...	...	...

Dense Sub-Block

(b) The correspondence graph (c) The minutia tensor matrix (*MTM*) T_F



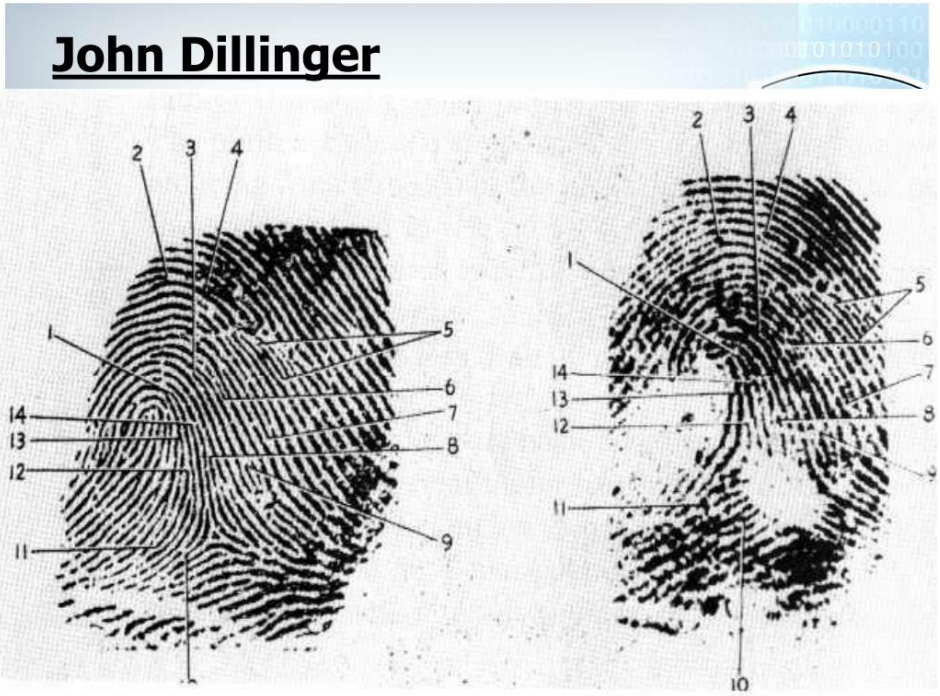
Il Livello Locale e Ultra-Fine



Minutiae (cerchi neri riempiti) evidenziate su una porzione di immagine di impronta digitale,

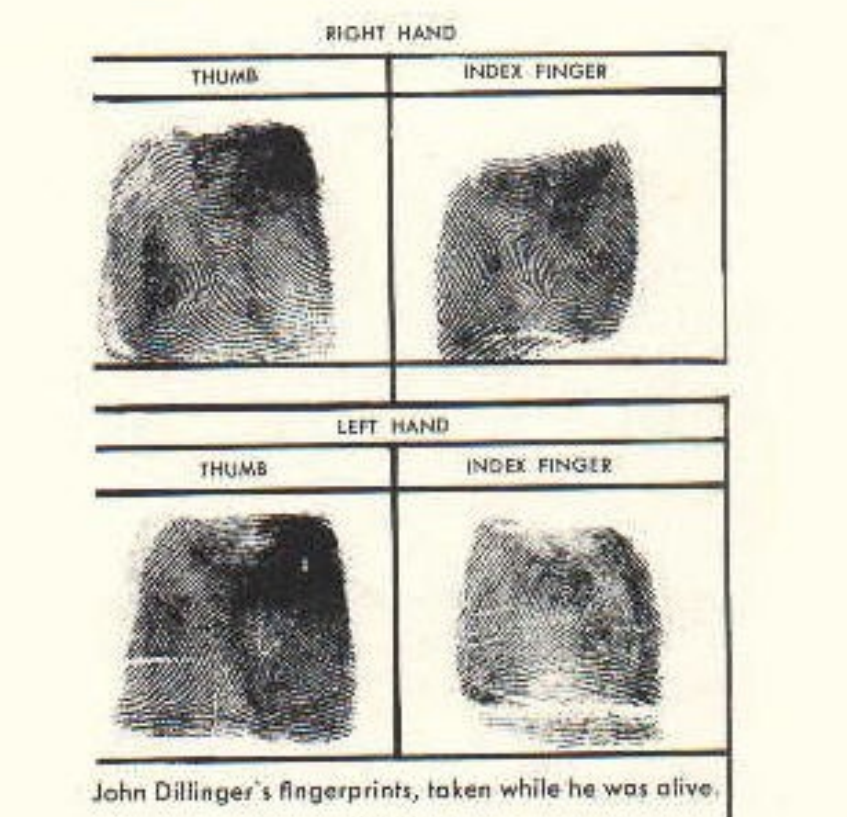
Posizione dei pori per la sudorazione (cerchi neri non riempiti) lungo una singola linea crestale.

Il Caso Dillinger

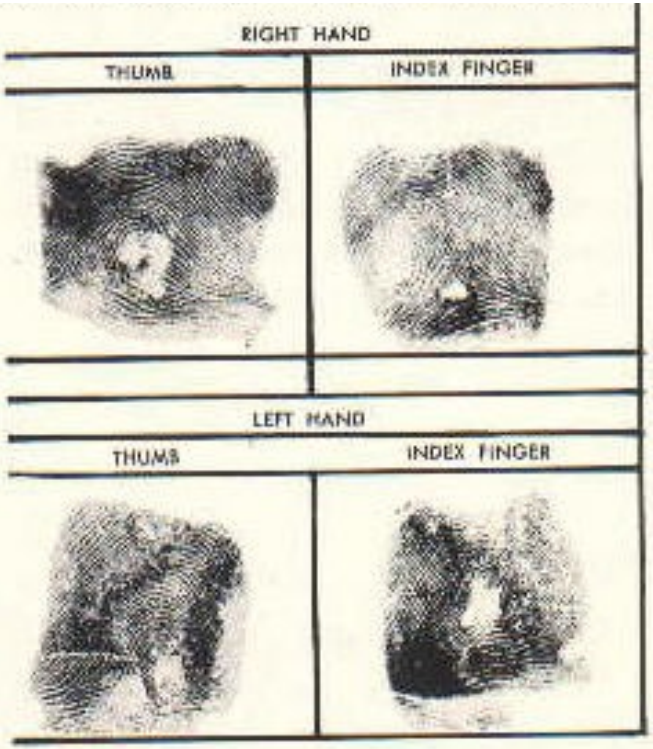


2nd Principle: A fingerprint will remain unchanged during an individual's lifetime

A positive identification of John Dillinger from his fingerprints, even though he had mutilated them



John Dillinger's fingerprints, taken while he was alive.



Dillinger's fingerprints, taken after he was shot and killed, show mutilated tips — his fruitless attempt to thwart identification.

Fingerprint (cont.)

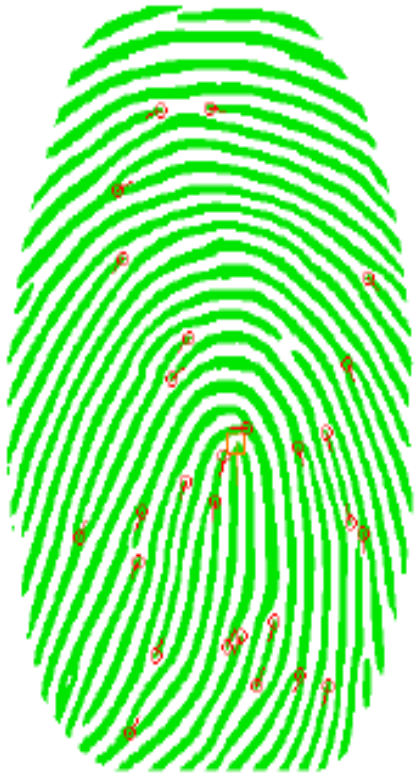
Vantaggi:

- Universalità
- Unicità
- Permanenza (Stabilità)
- Misurabilità
- Accettabilità
- Efficacia
- Acquisizione
  - Attiva e Passiva
  - Basso costo dei sensori

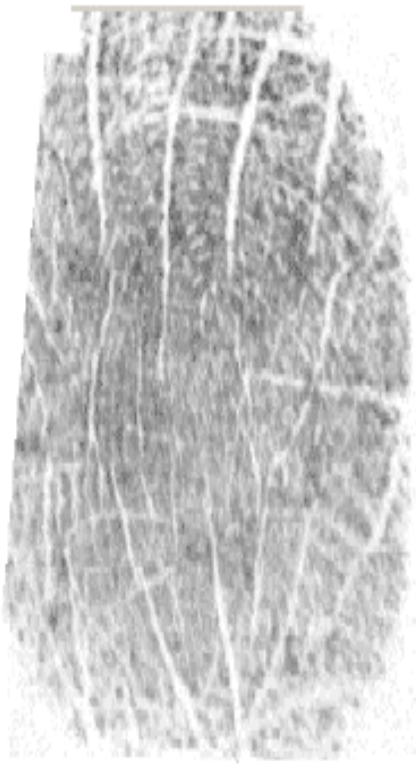
Svantaggi:

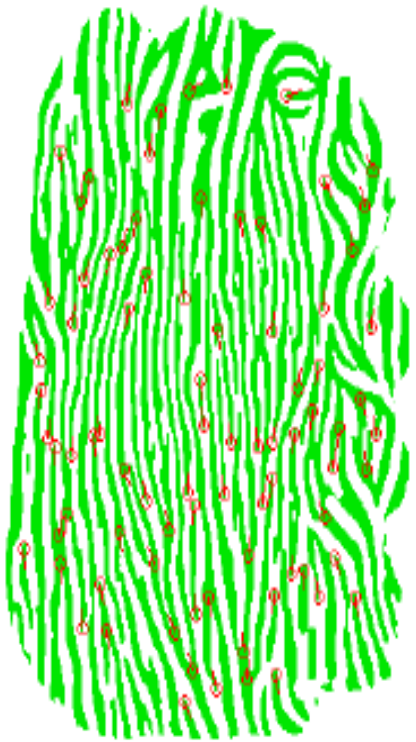
- Efficienza
  - memoria della chiave di ricerca: 256 bytes – 1.2k
    - Risoluzione: 500 dpi
  - Tempo di ricerca
- Stabilità
  - Abrasioni, Rughe…
  - Sporco, Sudore…
  - Disidradazione (over 65)
- Insidia
  - Relativamente facile da duplicare (Physical spoofing)

Fingerprint: Stabilità?



Example image of a 22 year old subject



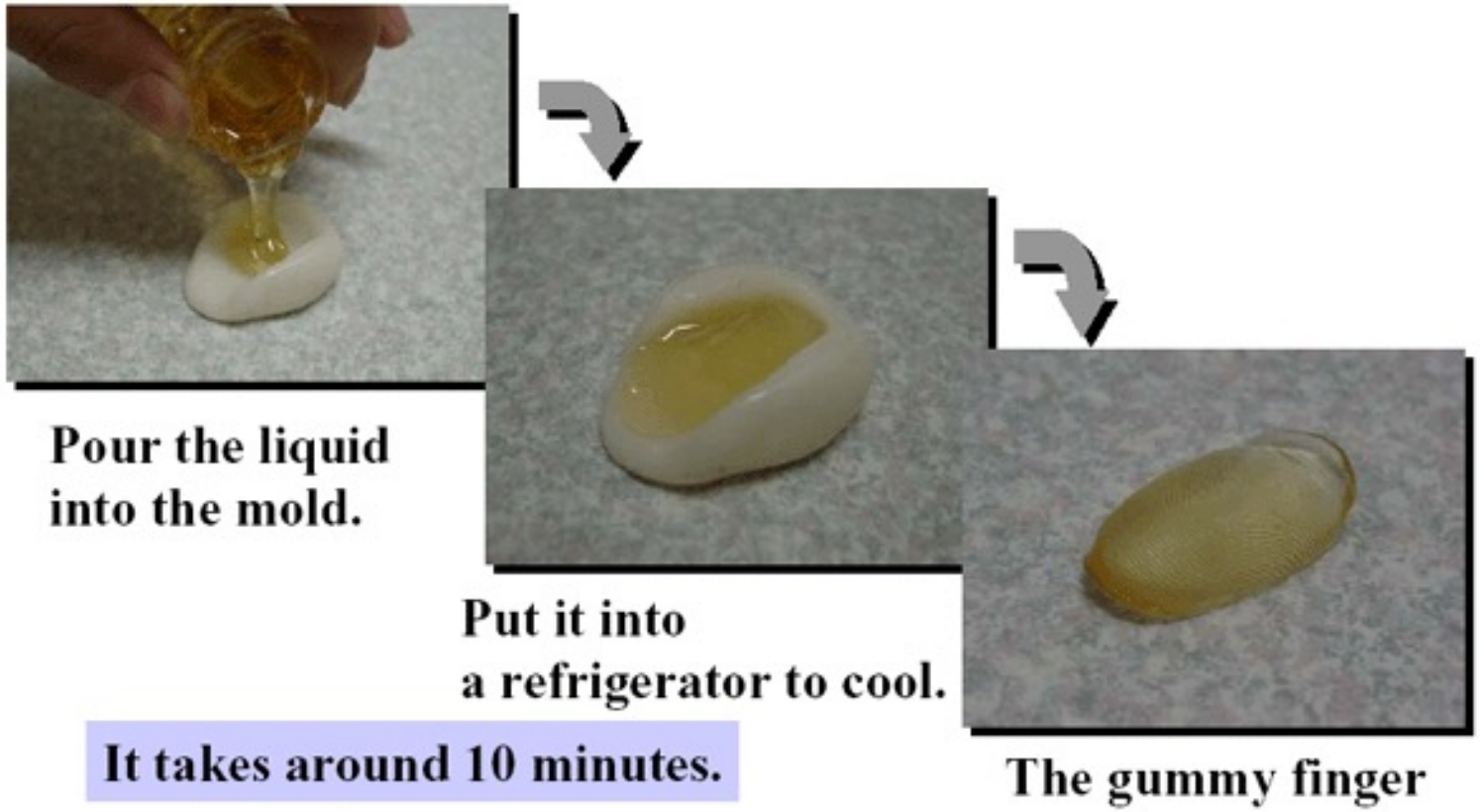


Example image of an 81 year old subject

Physical spoofing: Metodo di Matsumoto

- Only a few dollars' worth of materials

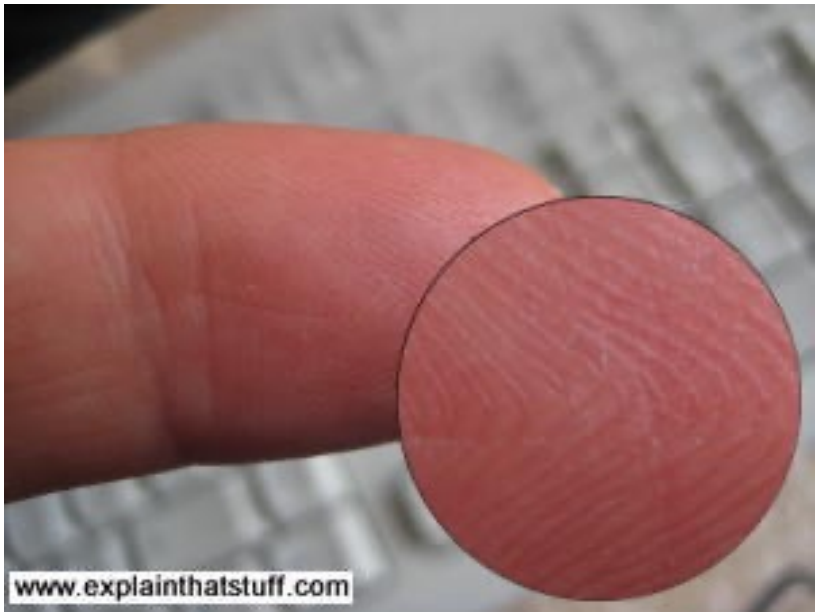
Physical spoofing: Metodo di Matsumoto (cont.)



You can place the “gummy finger” over your real finger. Observers aren’t likely to detect it when you use it on a fingerprint reader.

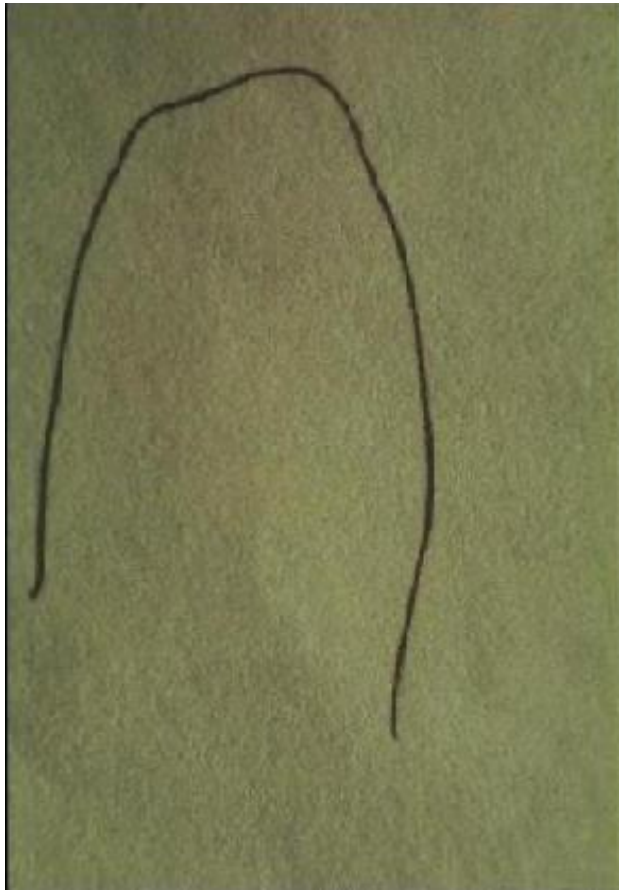
Ultraviolet Light

- RUVIS – Reflected Ultraviolet Imaging System



Ultraviolet Light

Ultraviolet Light



Fingerprint Powders

Gray – Aluminum Powder

Black – Carbon (charcoal)

White – Talc

Dusting for Fingerprints

Fingerprint Powders

Magnetic sensitive

Fingerprint Powders

Fluorescent

Other Methods

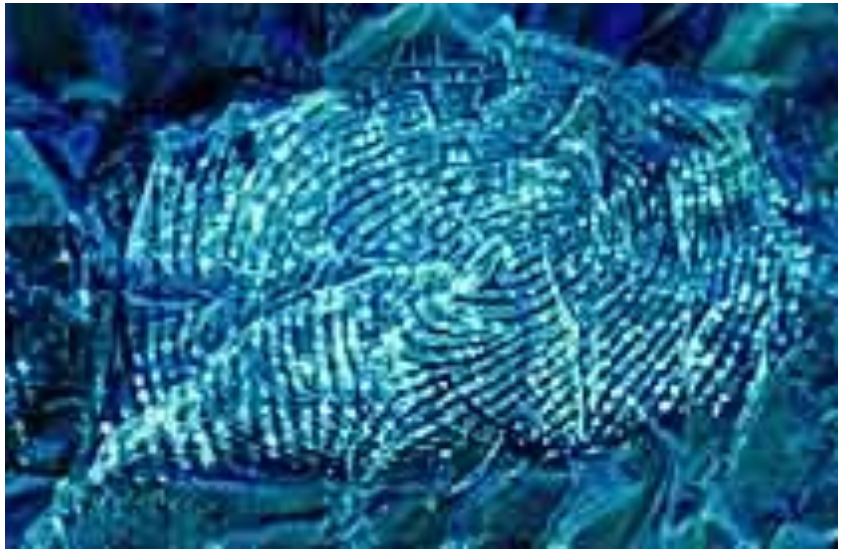
Iodine fuming

Other Methods

Ninhydrin

Other Methods

Cyanoacrylate – Super Glue® fuming



Lifting Fingerprints

Lifting Fingerprints

Tecnologie per la Digitalizzazione delle Impronte Digitali

I sensori di impronte digitali possono utilizzare le seguenti tecnologie:

• ***FTIR Frustrated Total Internal Reflection (Ottica)***, in grado di rilevare le immagini di creste e vallate con due diversi livelli di messa a fuoco;

• ***Capacitiva (dispositivi mobili)***, basata sul rilevamento delle microvariazioni di capacità (accumulo di carica elettrica) originate dalla struttura tridimensionale del polpastrello;

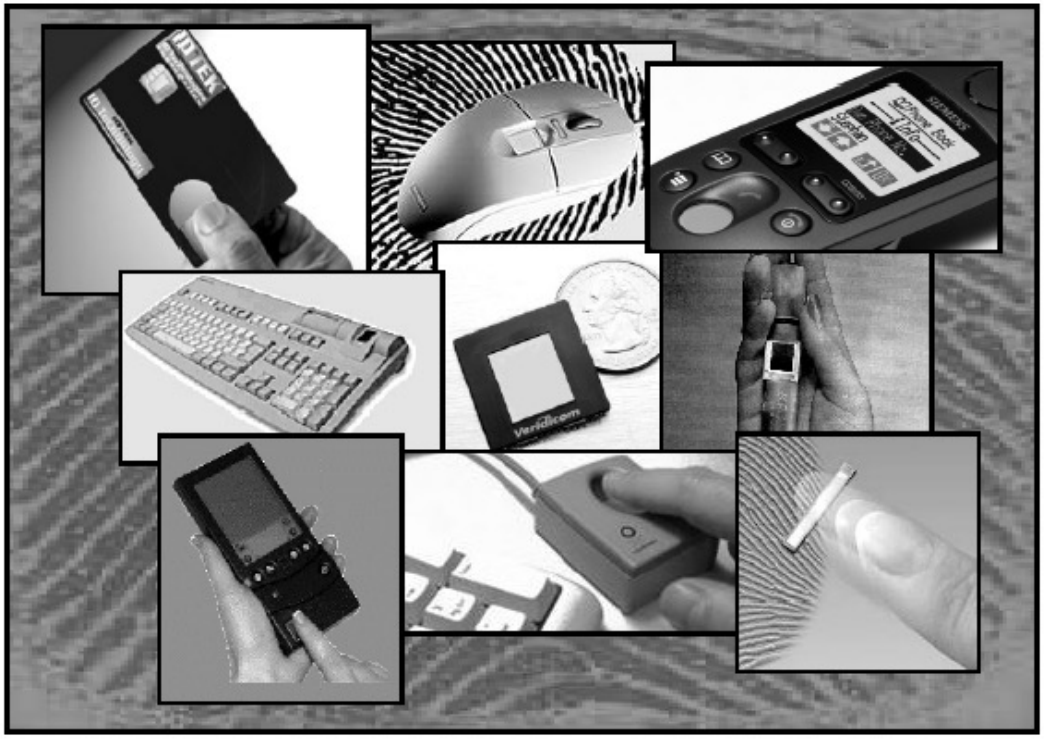
• ***Piezoelettrica***, basata sul rilevamento dell'impronta tramite materiali in grado di convertire la variazione di pressione locale in una differenza di potenziale elettrico;

• ***Termica,*** basata sull'utilizzo di sensori termici in grado di rilevare l'immagine del polpastrello non in lunghezze d'onda visibili ma nella gamma dell'infrarosso.

Digitalizzazione delle Impronte Digitali

I principali parametri che caratterizzano l'immagine digitale delle impronte sono:

- la ***risoluzione***
- l'***area di acquisizione***
- il ***contrasto***
- la ***distorsione geometrica***



Caratteristiche di uno Scanner di Impronte Digitali (1)

Le principali caratteristiche di uno scanner di impronte digitali dipendono dallo specifico sensore utilizzato che a sua volta determina le caratteristiche dell'immagine risultante quali:

• *Dpi* (Dot per inch ovvero punti per pollice) ovvero una misura del risoluzione di scansione espressa come densità di punti per unità di misura;

•*Area utile di acquisizione*, ovvero le dimensioni della superficie sensibile che influenzano il numero di caratteristiche distintive acquisite, ma anche l'accuratezza: sensori con aree più piccole hanno costi inferiori ma anche precisione inferiore in termini di riconoscimento che può essere parzialmente compensata con appositi algoritmi di *mosaicking* per la ricomposizione dell'impronta da un set di immagini più piccole e parzialmente sovrapposte;

Caratteristiche di uno Scanner di Impronte Digitali (2)

• Gamma dinamica, ovvero il numero di livelli di grigio quantizzati dallo scanner che si traduce in una maggiore o minore precisione nella rappresentazione dei dettagli.

Il tipo di sensore condiziona anche le dimensioni, il costo e la durata del dispositivo. Ulteriori importanti caratteristiche vanno considerate nella scelta dello scanner ideale per un certo tipo di applicazione:

• Fps (frames per second): questo valore indica il numero di immagini che lo scanner può acquisire ed inviare all'host in un secondo. Frame rate elevati consentono una maggiore tolleranza verso movimenti involontari del dito rispetto al sensore, rendendo così meno problematica l'interazione con lo scanner e consentendo in alcuni casi anche un preview del risultato dell'acquisizione.

Caratteristiche di uno Scanner di Impronte Digitali (3)

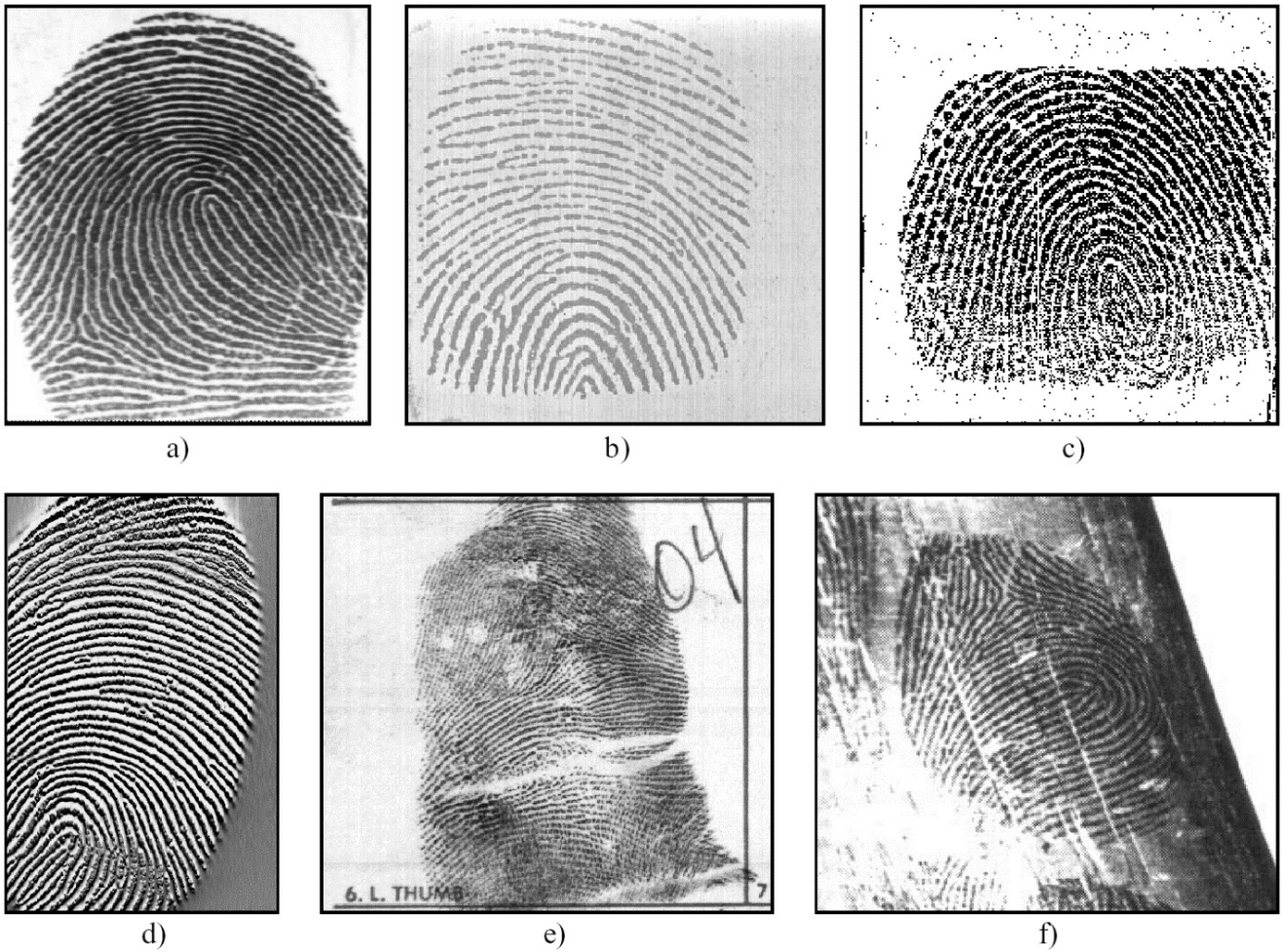
• *Rilevamento automatico della presenza del dito*: Alcuni scanners sono in grado di determinare automaticamente la presenza del dito sul sensore, liberando l'host da un continuo polling del dispositivo e consentendo di attivare la procedura di acquisizione non appena c'è un contatto fisico con l'utente;

•*Test di vitalità:* Rilevazione dei parametri vitali quali battito cardiaco, pressione arteriosa e temperatura;

• *Crittografia*: alcuni dispositivi di scansione delle impronte digitali sono dotati di algoritmi crittografici avanzati allo scopo di ridurre le probabilità di un attacco al canale di comunicazione con l'host;

• *Sistemi operativi supportati*: la compatibilità con più sistemi operativi compresi quelli di tipo open-source può essere un importante aspetto nella selezione di uno scanner in funzione del tipo di applicazione e dell'infrastruttura informatica a cui esso deve essere connesso.

Tecnologie per la Digitalizzazione delle Impronte Digitali (1)



Immagini di impronte digitali prodotte da: a) scanner ottico live-scan; b) scanner capacitivo live-scan; c) scanner piezoelettrico live-scan; d) scanner termico live-scan; e) impressione tramite inchiostro off-line; f) impronta digitale latente.

Risultati Acquisizione a Confronto

Immagini dell'impronta digitale appartenente allo stesso dito acquisito in condizioni ideali con i seguenti scanner commerciali visualizzate con proporzioni reali:

a) Biometrika FX2000,

b) Digital Persona UareU2000,

c) Identix DFR200,

d) Ethentica TactilSense T-FPM,

e) ST Microelectronics TouchChip,

f) Veridicom FPS110,

g) Atmel FingerChip AT77C101B,

h) Authentec AES4000.