



# Trends and New Technologies in Biometrics

## 生物辨識的新技術和趨勢

- ✦ 陳慶瀚
- ✦ 中央大學資工系
- ✦ 機器智慧與自動化技術實驗室
- ✦ 2007年5月16日



# Biometrics

Automated verification of a person's identity based on any measurable, robust, distinctive physical characteristic or their behavior.



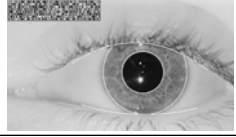



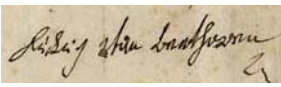


# How does it work?

- ✦ Each person is unique
- ✦ What are the distinguishing traits that make each person unique?
- ✦ How can these traits be measured?
- ✦ How differentiate these distinguishing traits for different people?



# Biometric Modalities

Modality	Example	Invasiveness	"1:many" Accuracy	Vendors	Typical Applications
Fingerprint		Moderate	☆☆☆	~ 80 / 8	Law enforcement, financial, POS
Hand Geometry		Moderate	☆	~ 2	Access control, border control
Iris		Moderate/high	☆☆☆	~ 2	ATMs, access control
Face		Low	☆☆	~ 12	Surveillance, Passports
Voice		Low/Moderate	☆	~ 32	Access control, logon
Keystroke		Moderate	☆	~ 1	Computer Security
Signature		Moderate	☆☆	~ 15	Financial, PocketPC



# Biometrics Technologies

- ✦ Collection of Physiological or Behavioral Data
- ✦ Signal/Image Processing and Feature Extraction
- ✦ Pattern Recognition



# Biometrics Data Collection

- ❖ Comprises input device or sensor that reads the biometric information from the user
- ❖ Converts biometric information into a suitable form for processing by the remainder of the biometric system
- ❖ Examples: video camera, fingerprint scanner, digital tablet, microphone, etc.



# Biometrics Signal processing

- ✦ For feature extraction
- ✦ Receives raw biometric data from the data collection system
- ✦ Transforms the data into the form required by matching subsystem
- ✦ Discriminating features extracted from the raw biometric data
- ✦ Filtering may be applied to remove noise



## Biometrics Feature Matching

- ✦ Receives processed biometric data from signal processing subsystem and biometric template from storage subsystem
- ✦ Measures the similarity of the claimant's sample with the reference template
- ✦ Typical methods: distance metrics, probabilistic measures, neural networks, etc.
- ✦ The result is a number known as match score





# Biometrics Decision system

- Interprets the match score from the matching system
- A threshold is defined. If the score is above the threshold, the user is authenticated. If it is below, the user is rejected
- Typically a binary decision: yes or no
- May require more than one submitted samples to reach a decision: 1 out of N



# Biometrics Storage subsystem

- ⊕ Maintains the templates for enrolled users
- ⊕ One or more templates for each user
- ⊕ The templates may be stored in:
  - ⊠ physically protected storage within the biometric device
  - ⊠ conventional database
  - ⊠ portable tokens, such as a smartcard



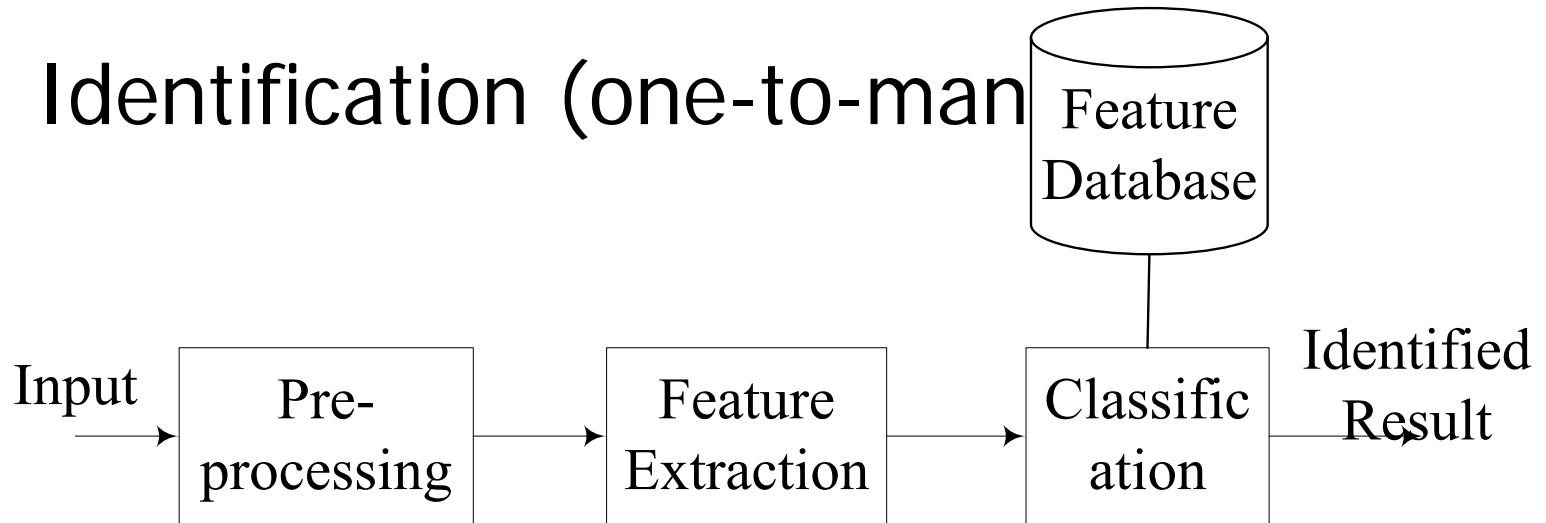
# Biometrics Transmission System

- ✿ Subsystems are logically separate
- ✿ Some subsystems may be physically integrated
- ✿ Usually, there are separate physical entities in a biometric system
- ✿ Biometric data has to be transmitted between the different physical entities
- ✿ Biometric data is vulnerable during transmission

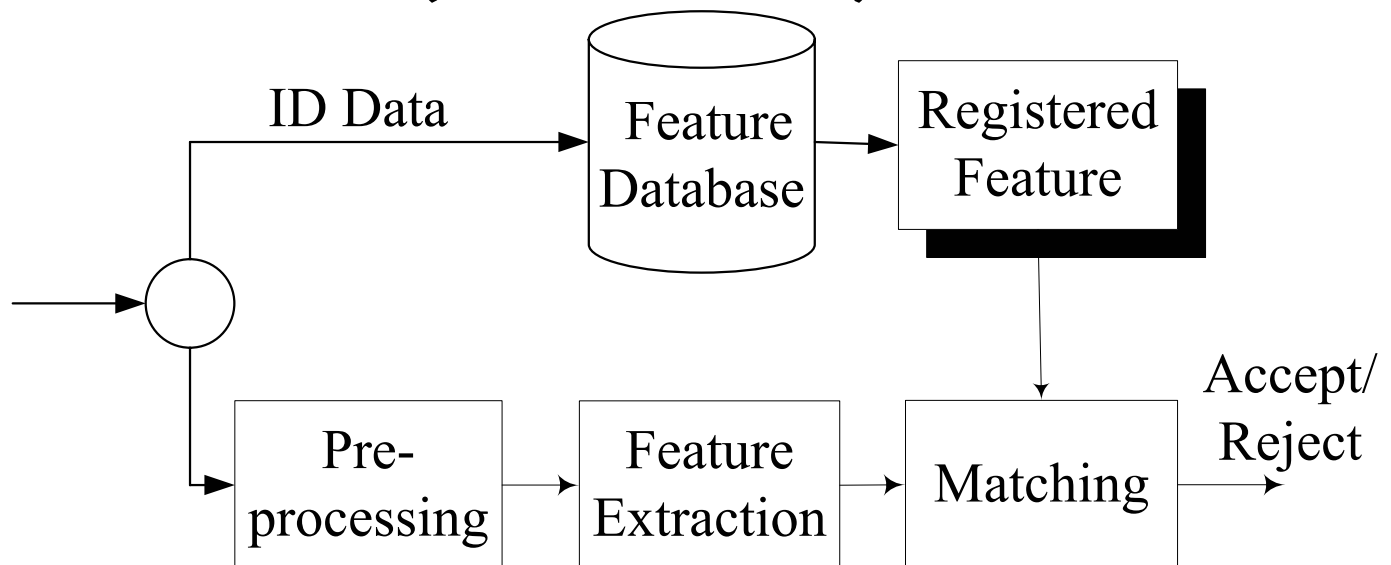


# Two Models in Biometrics

## Identification (one-to-many)



## Verification (one-to-one)





# Two Models in Biometrics

## Identification Systems:

- Who am I?

## Verification Systems:

- Am I who I claim to be?

- More accurate.

- Less expensive.

- Faster.

- More limited in function.

- Requires more effort by user.



# Two Models in Biometrics

- Identification and verification:
  - Finger scan
  - Iris scan
  - Retina scan
  - Facial scan (optical and infrared)
- Verification only:
  - Hand Geometry
  - Voice Print
  - Keystroke Behavior
  - Signature

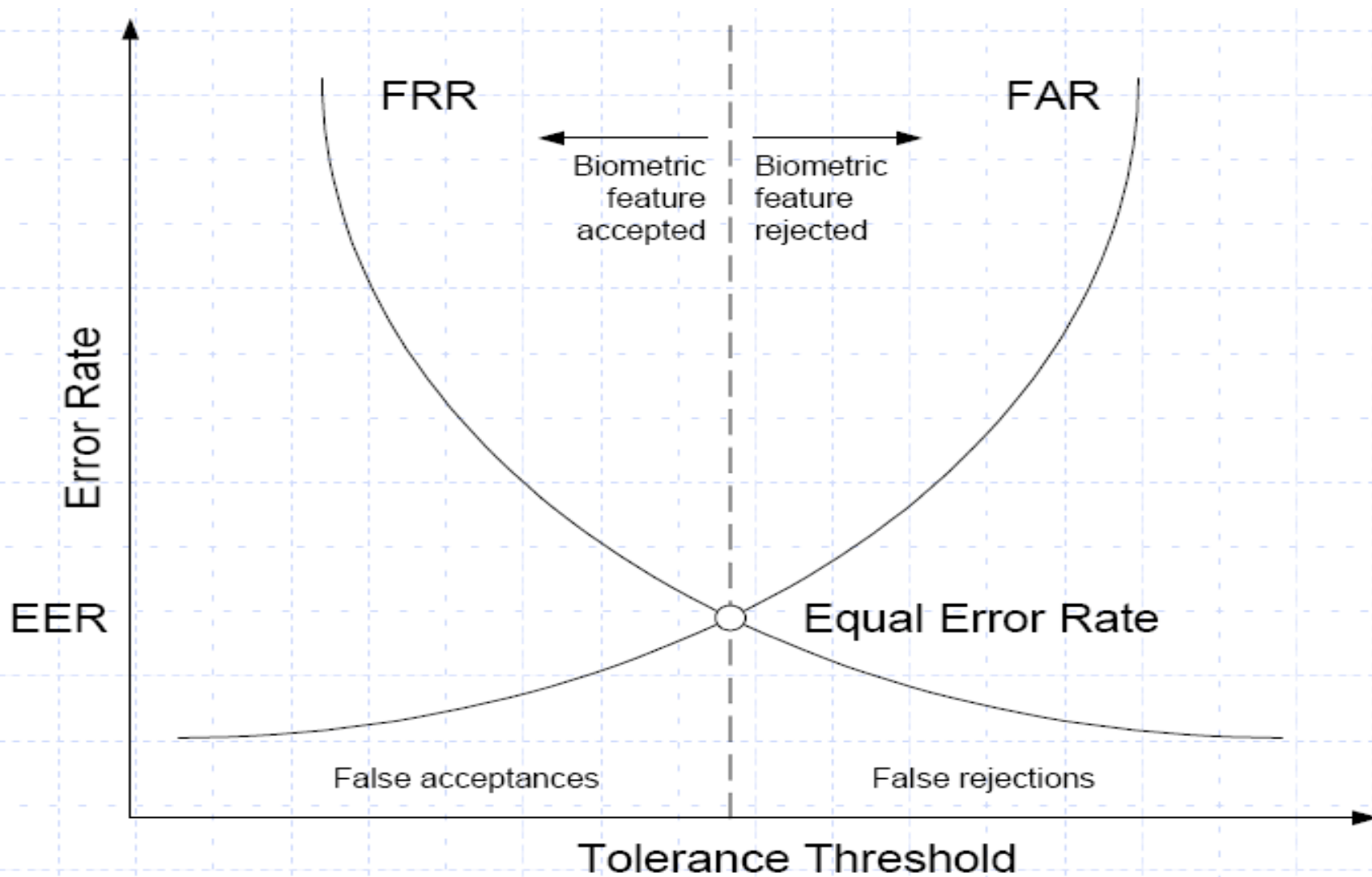


# Performance Evaluation

- ❖ False Acceptance Rate (FAR): Percentage of an impostor being accepted as a genuine individual.
- ❖ False Rejection Rate (FRR): Percentage of a genuine individual being rejected as an impostor.
- ❖ Equal Error Rate (EER): Point where  $FAR = FRR$
- ❖ Failure to Enroll Rate (FTER): Percentage of failures to enroll of the total number of enrollment attempts.



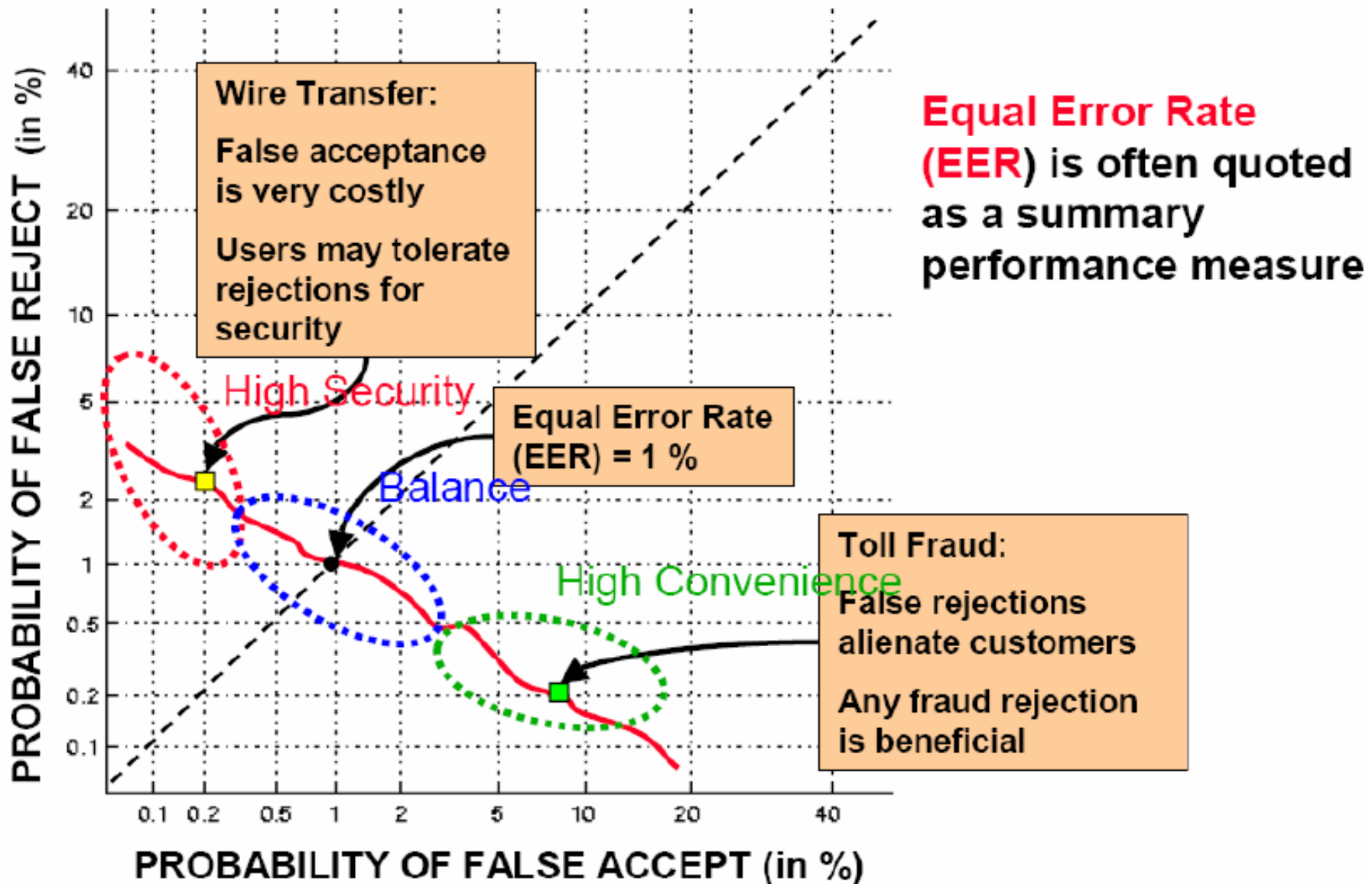
# Performance Evaluation







# Operating Point

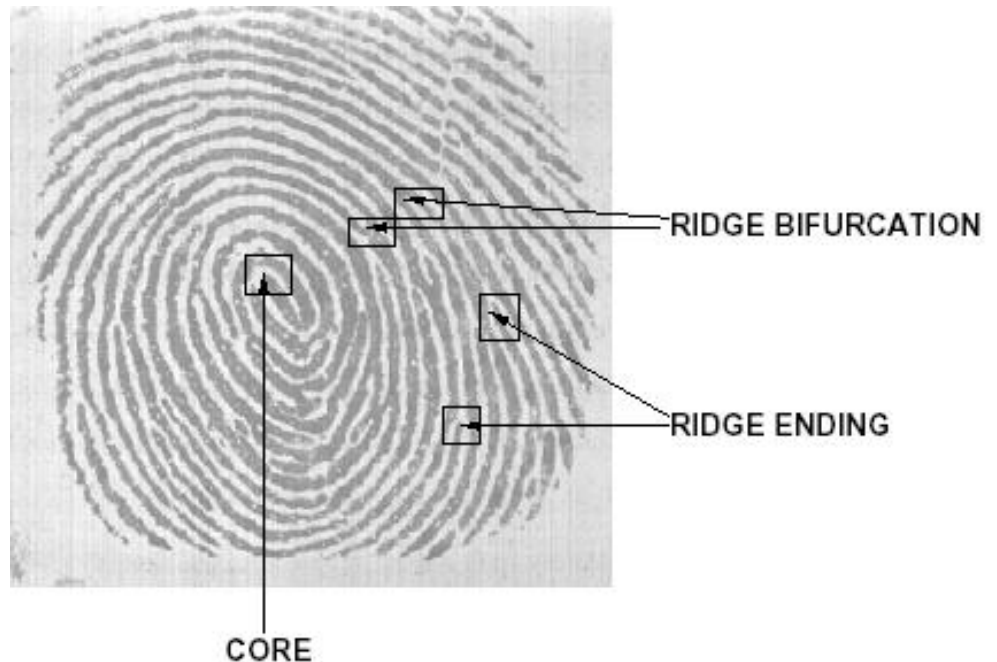




# Fingerprint Biometrics

- ❁ Finger scan: Measures unique characteristics in a fingerprint (minutiae)

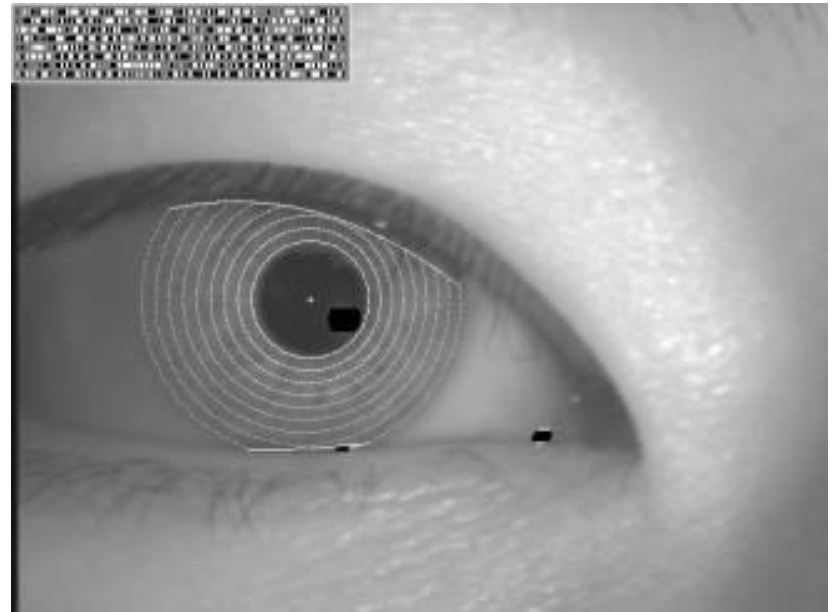
- ❁ Crossover
- ❁ Core
- ❁ Bifurcations
- ❁ Ridge ending
- ❁ Island
- ❁ Delta
- ❁ Pore





# Iris Biometrics

- ✦ Iris scan: Measures unique characteristics of the iris
  - ❑ Ridges (rings)
  - ❑ Furrows
  - ❑ Straitions (freckles)





# Retina Biometrics

- Retina scan: Measures unique characteristics of the retina.
  - Blood vessel patterns
  - Vein patterns



retinal scan

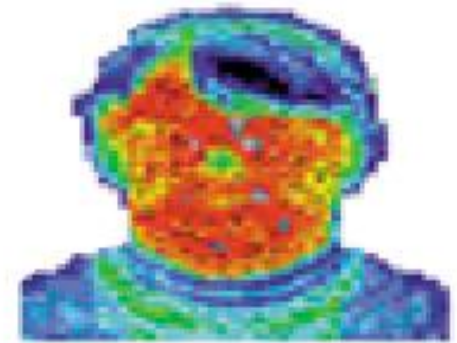


# Face Biometrics

- ❖ Facial scan: Uses off-the-shelf camera to measure the following facial features:
  - ❖ Distance between the eyes.
  - ❖ Distance between the eyes and nose ridge.
  - ❖ Angle of a cheek.
  - ❖ Slope of the nose.
  - ❖ Facial Temperatures.



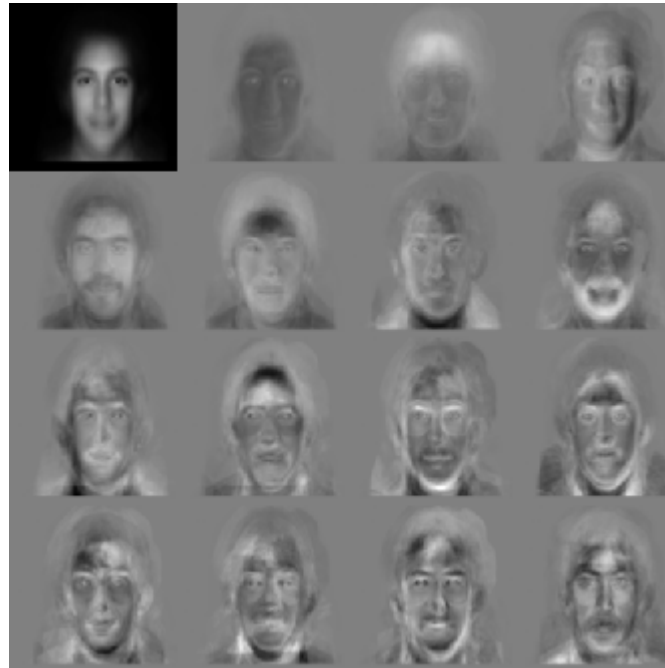
face

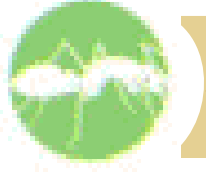


facial thermogram



# Face Biometrics





# Signature Biometrics

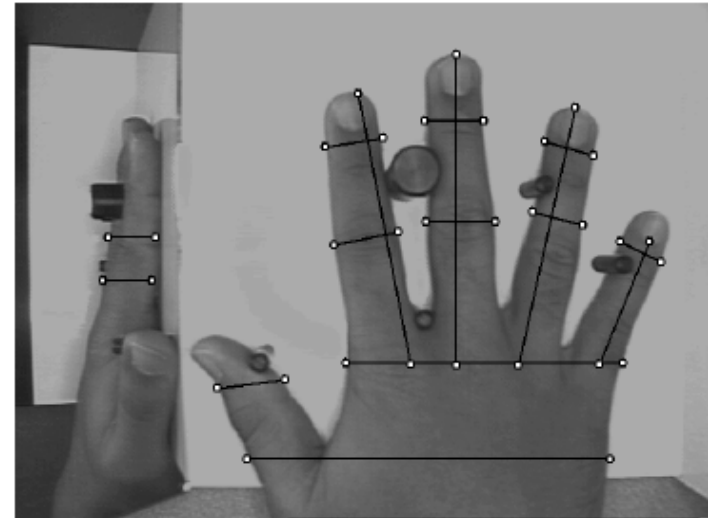
- ✦ Signature scan: Measures speed, pressure, stroke order an image of signature.
- ▣ Non-repudiation

signature



# Hand geometry

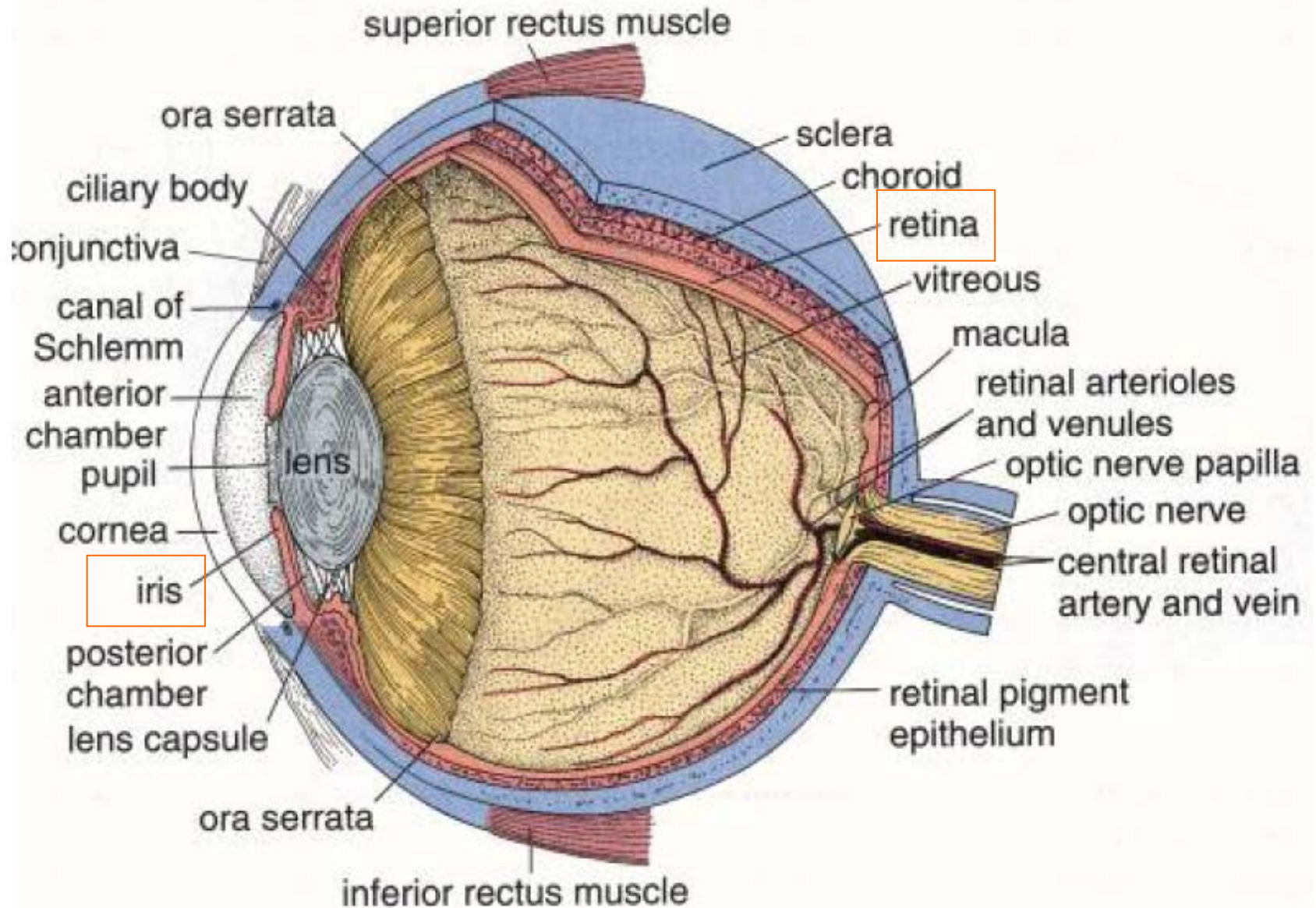
- ✦ Features: dimensions and shape of the hand, fingers, and knuckles as well as their relative locations
- ✦ Two images taken, one from the top and one from the side





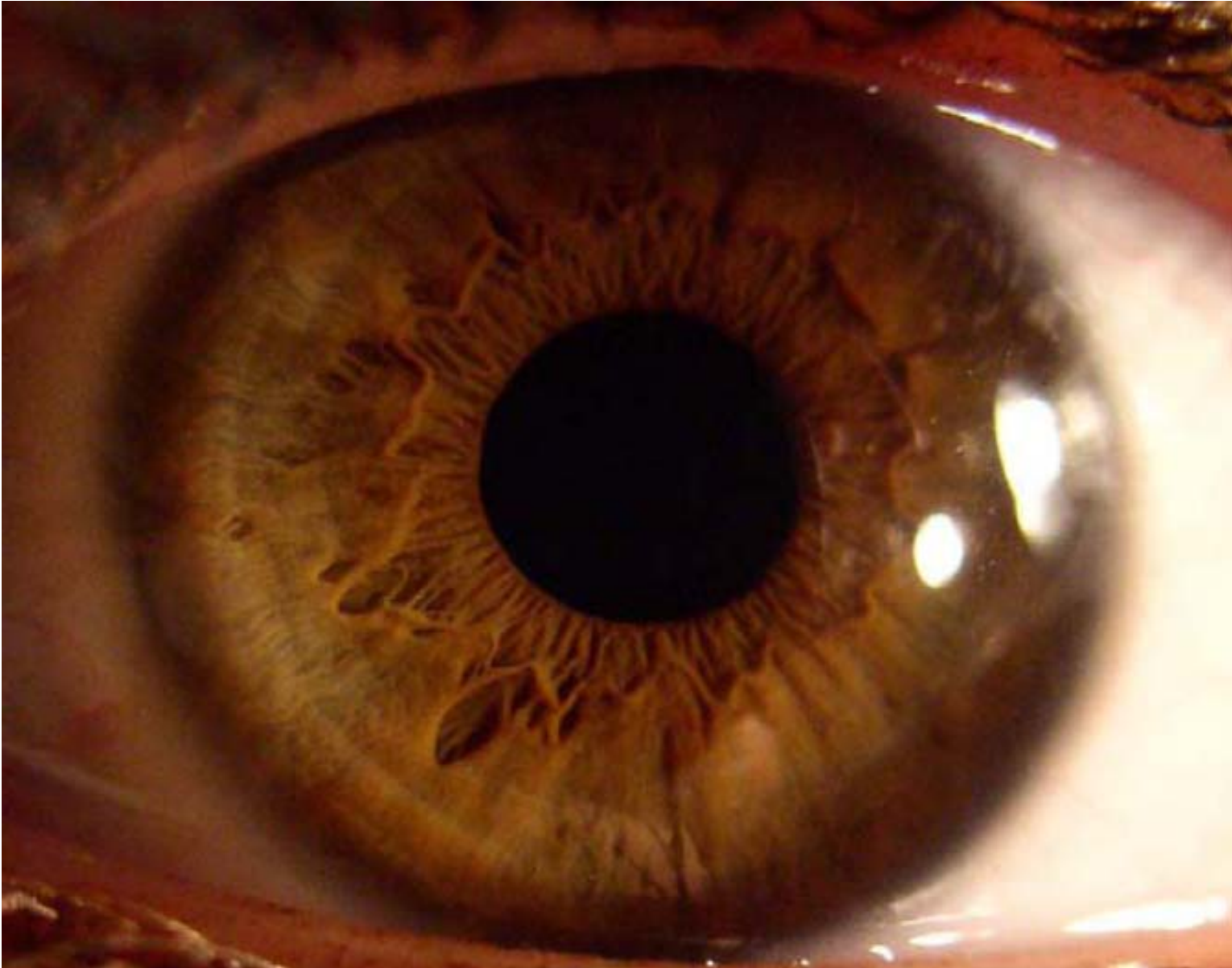


# Eye Biometrics





# Iris Biometrics





# KeyStrobe Biometrics

Measures the time between strokes and duration of key pressed.

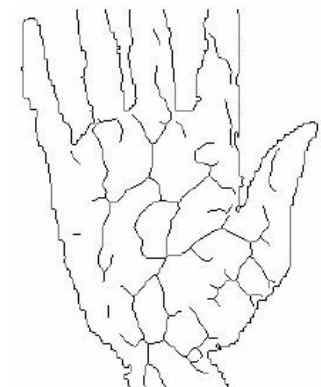


	ASCII	$t_{i.up}(a,w)$	$t_{i.down}(a,w)$
1	Shift	2.684	2.804
2	G	2.754	2.804
3	E	3.034	3.135
4	O	3.225	3.335
5	R	3.405	3.495
6	G	3.565	3.605
7	E	3.675	3.746

Key-in the password : “GEORGE”

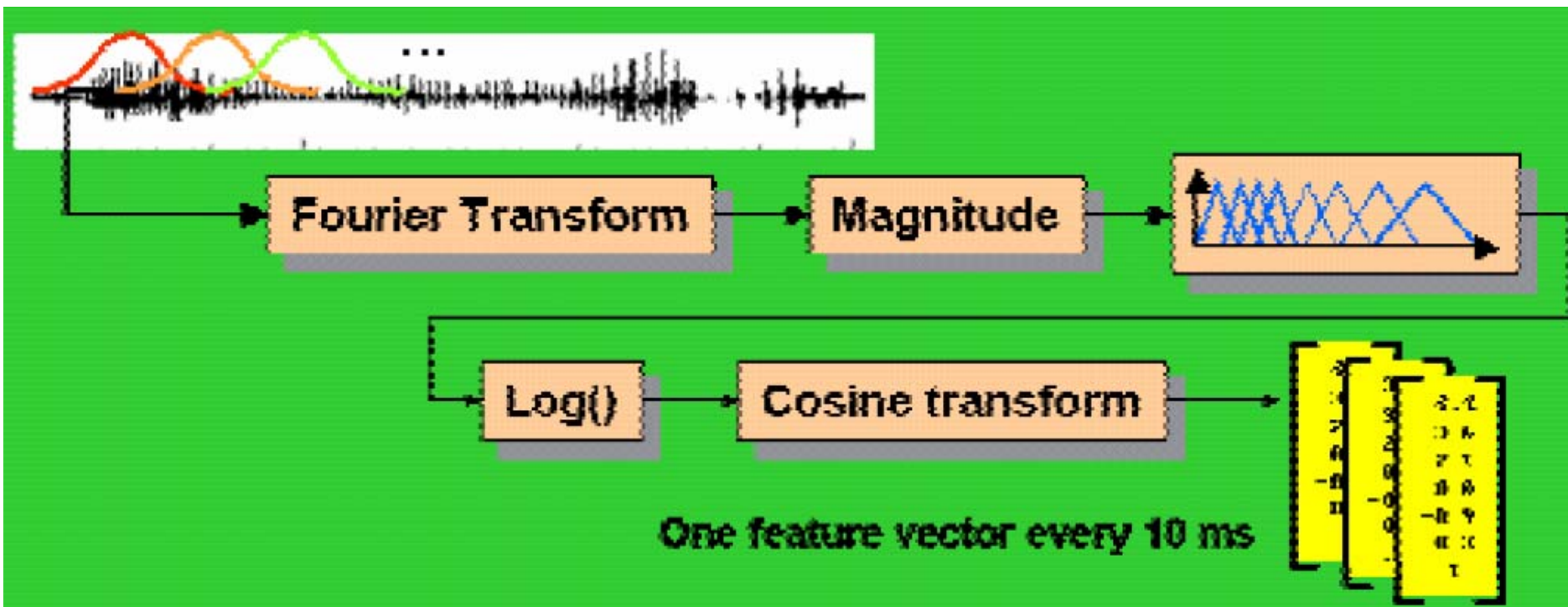
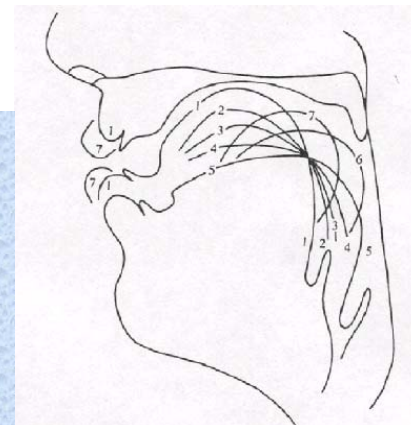


# Contactless palm vein recognition System



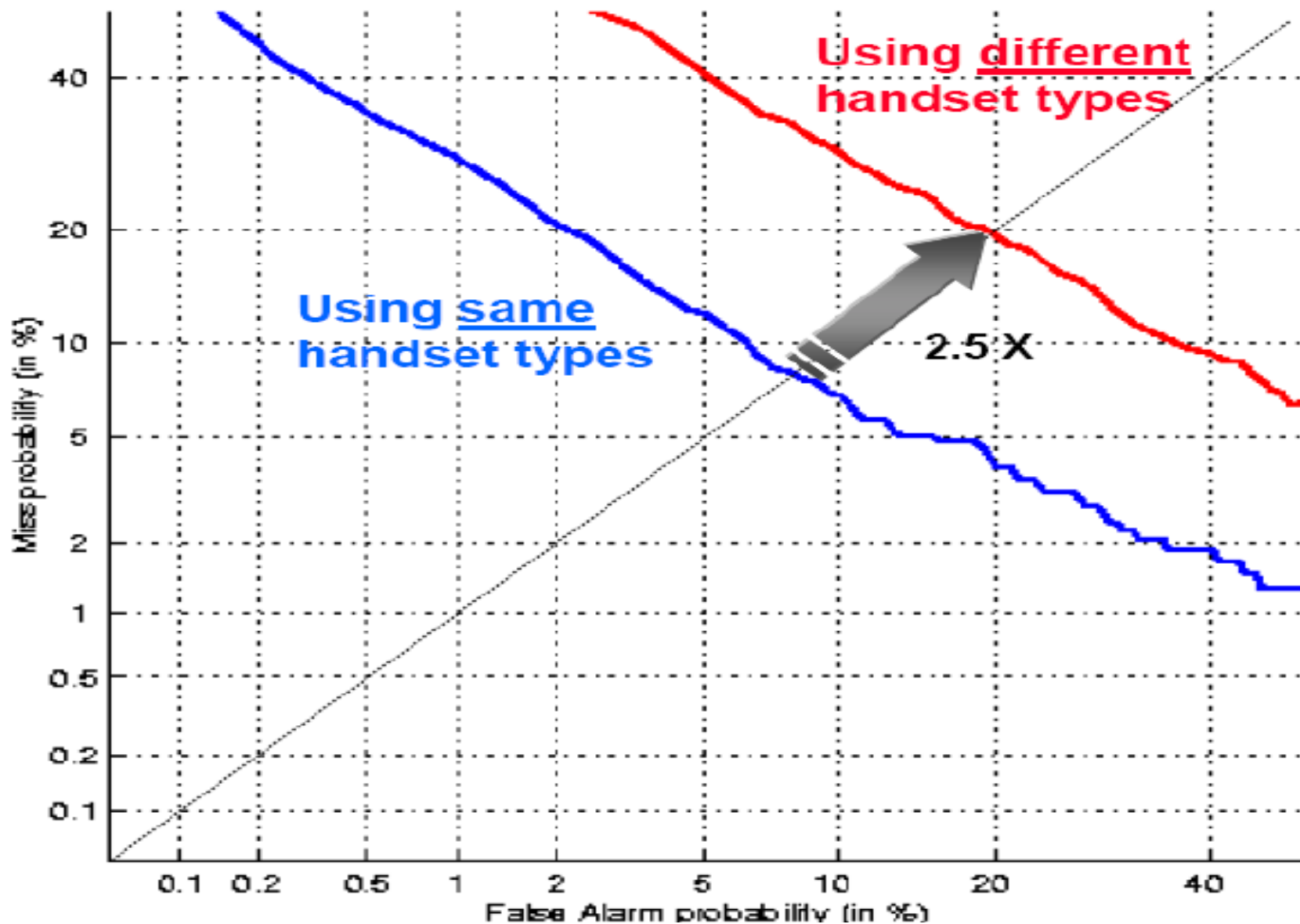


# Voiceprint Biometrics



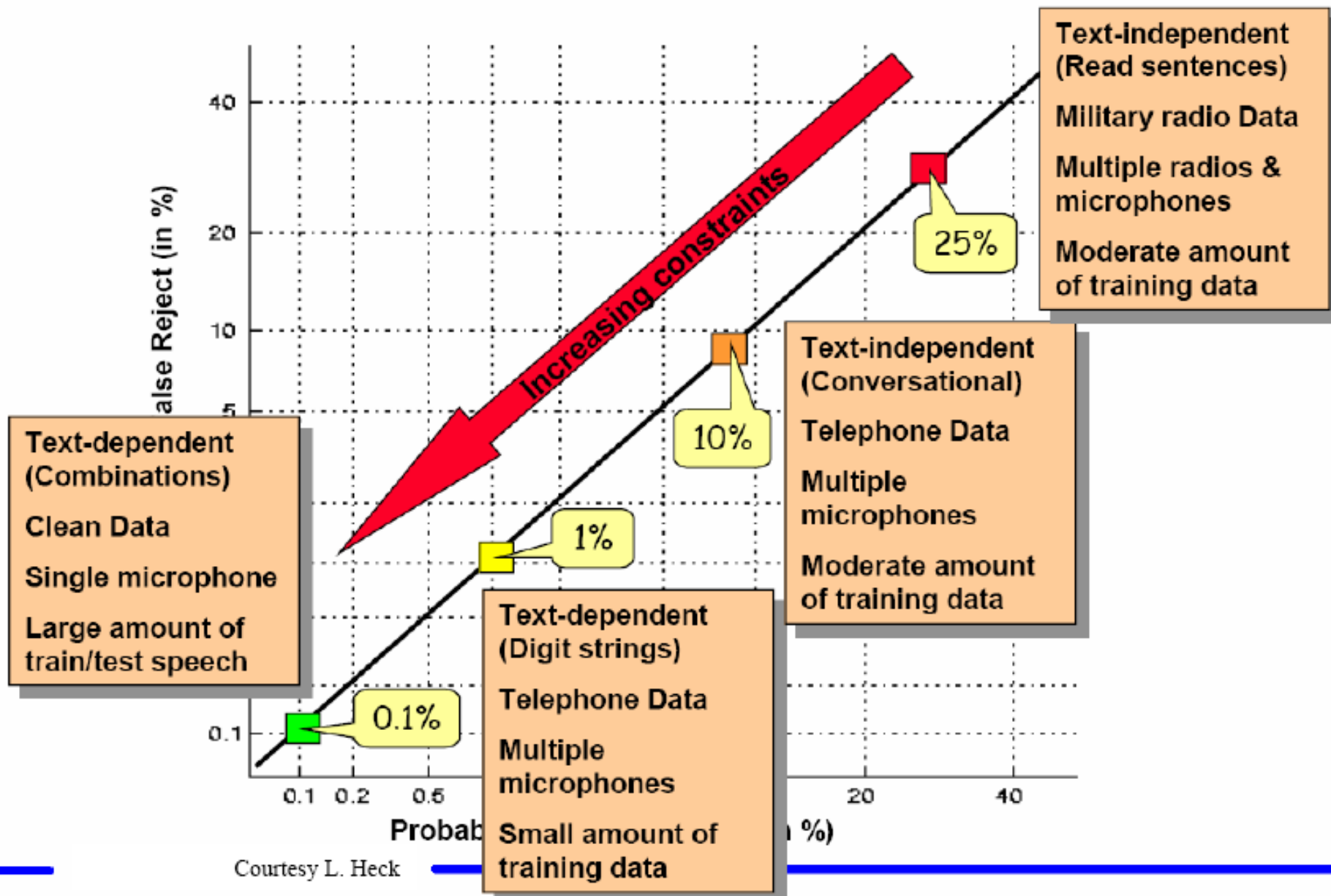


# Handset Effect for Voice Authentication





# Constraints for Voice Authentication





# Factors in Voice Authentication

## Speaker

- Voice quality
- Pitch
- Gender
- Dialect

## Speaking style

- Stress/Emotion
- Speaking rate
- Lombard effect

## Channel

- Distortion
- Noise
- Echoes
- Dropouts

## Noise

- Microphone
- Background noise
- Reverberations



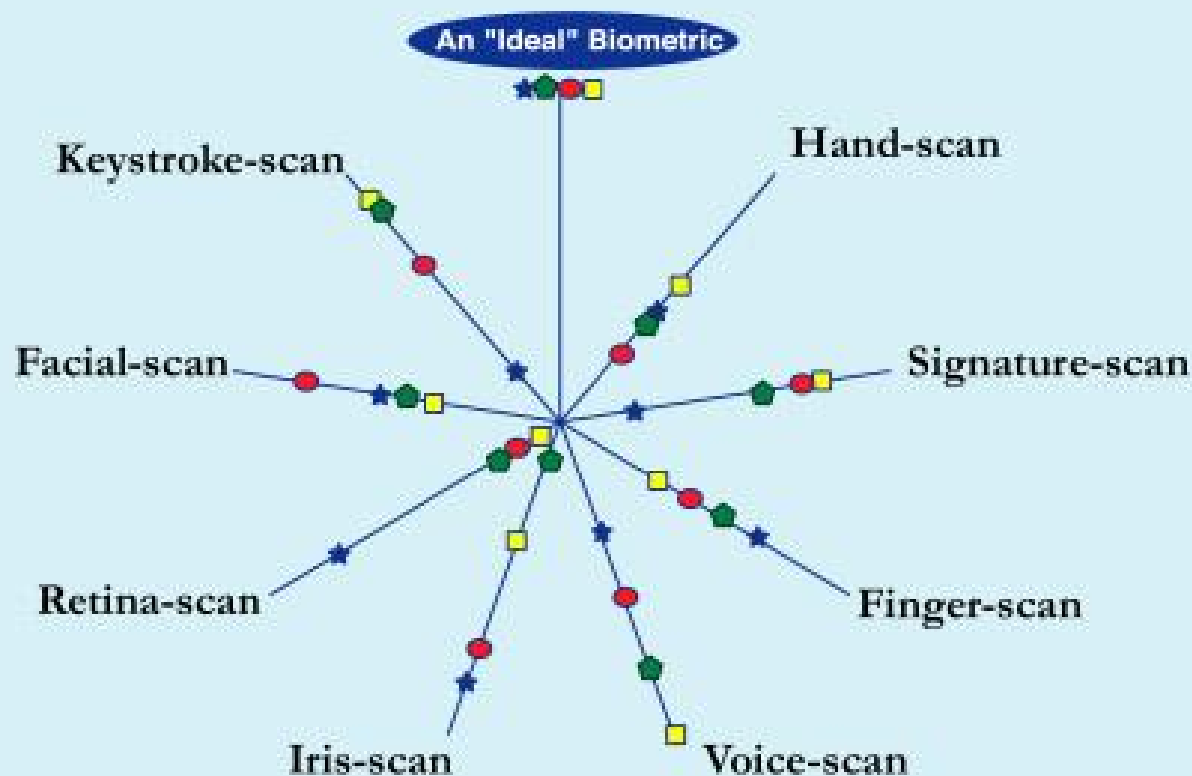


# Comparisons between Bio-Scan

## International·Biometric·Group

Research Consulting Integration

### Zephyr™ Analysis



© 1997-2002 International Biometric Group

■ Intrusiveness    ★ Distinctiveness    ● Cost    ● Effort



# Security Considerations



## Concerns

- Informational privacy concerns
- Personal privacy concerns
- cultural or religious beliefs



## BioPrivacy

- Limited system scope and access
- Limited storage of biometric data
- Security Tools: Encryption
- secure communication



# Consumer Fingerprint Product





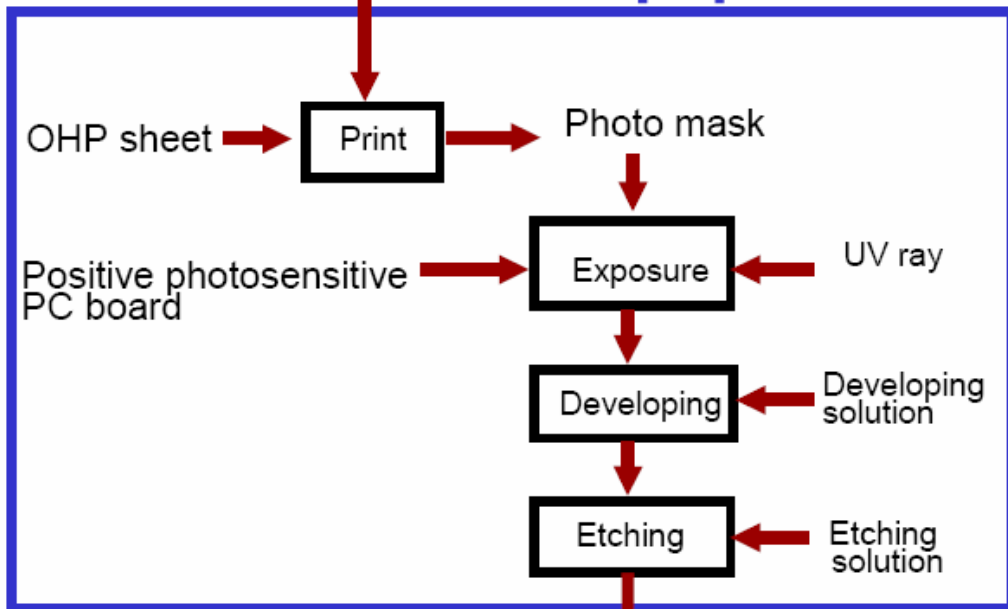
# Fingerprint Spoofing

Tsutomu Matsumoto, University of Yokohama, 2002

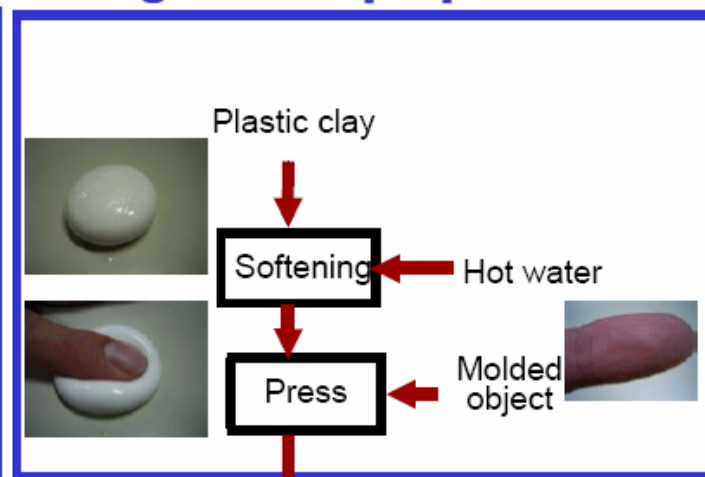
Reference Fingerprint Pattern Image



## Flat artificial finger mold preparation



## Three-dimensional artificial finger mold preparation



Flat artificial fingerprint mold

3D artificial fingerprint mold

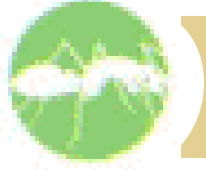
Gelatin sol or silicone rubber

Solidification

Artificial finger

## Artificial finger preparation





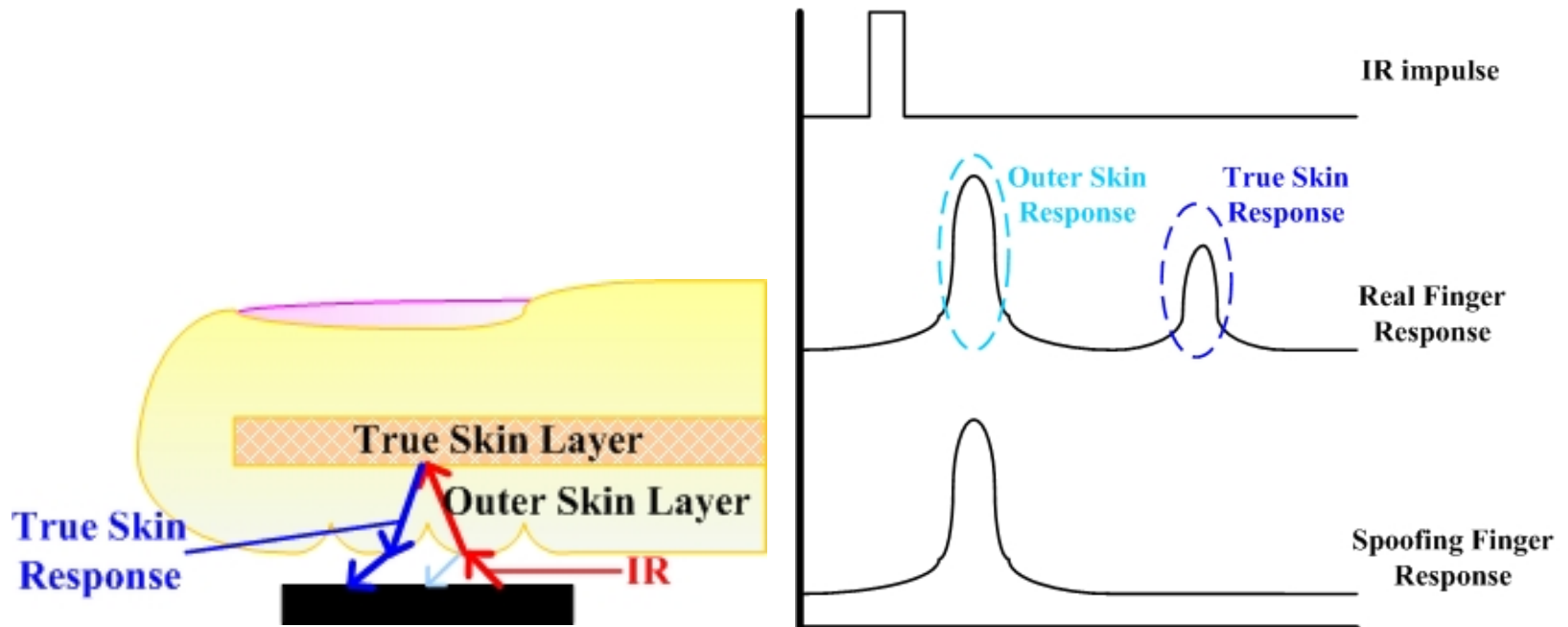
# Fingerprint Spoofing



Tsutomu Matsumoto, University of Yokohama

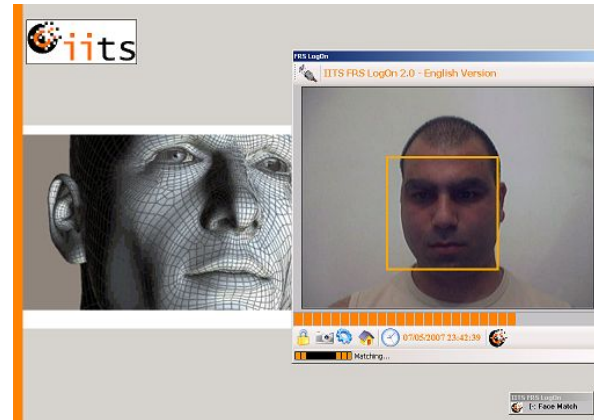


# Anti-Spoofing Example





# Face Biometric Product





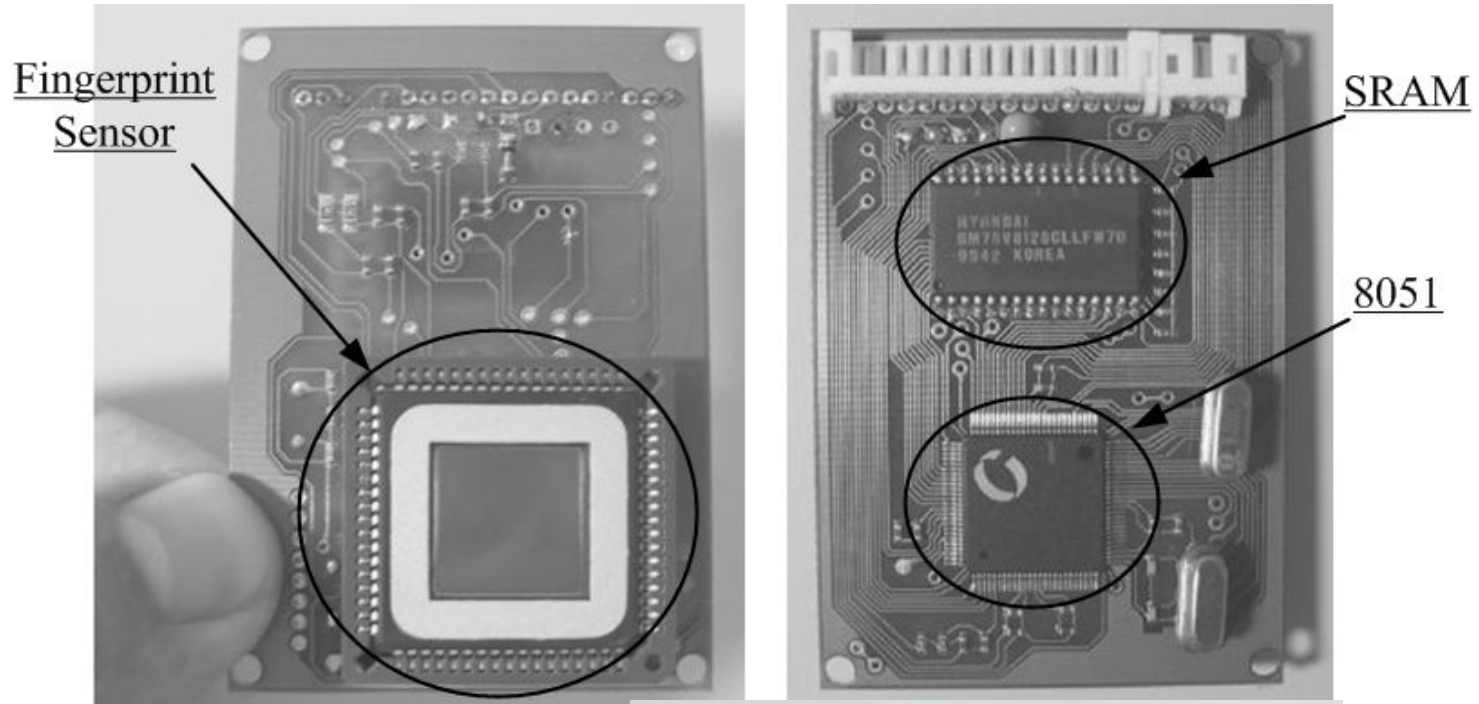
## Embedded Biometric System at MIAT Lab

- ✿ 精簡嵌入式指紋辨識系統
- ✿ 渾沌加密與保密通訊ASIC
- ✿ 具保密通信功能的指紋遙控器
- ✿ DSP嵌入式指紋辨識系統



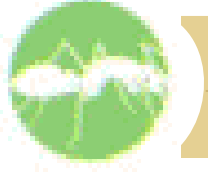


## 精簡嵌入式指紋身份識別系統

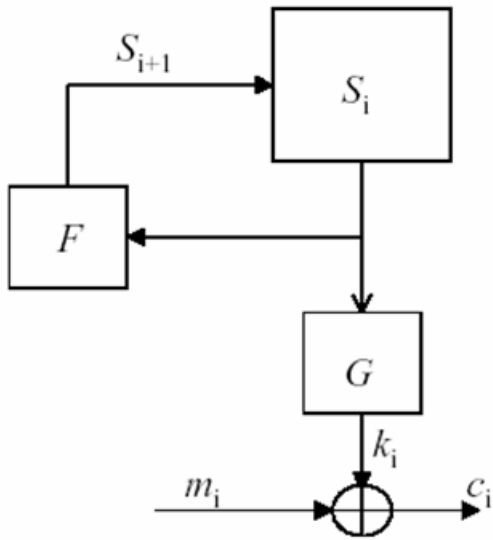
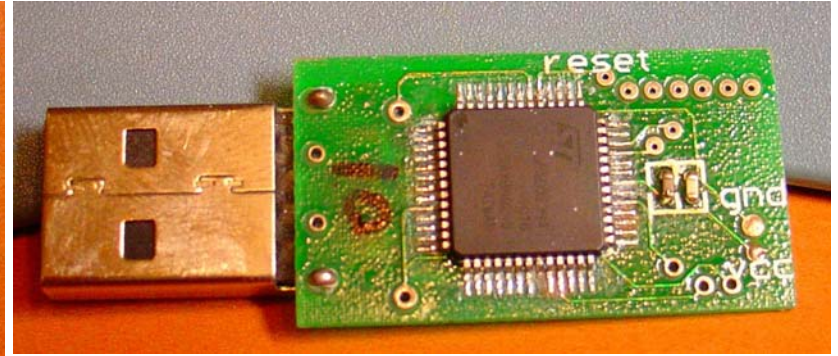
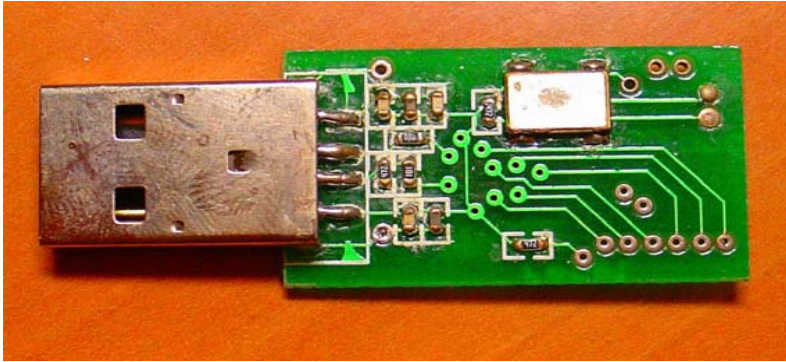


**25MHz 8051**  
**12 Kbytes ROM**  
**35 Kbytes RAM**  
**EER=4.5%**





## 渾沌加密與保密通訊ASIC



Gate Counts:

~ 70,000

Speed:

41.6MB/s at 130MHZ (EP1C20F324C7)應用  
MP3/MPEG-4即時解密撥放器；

加解密隨身碟；

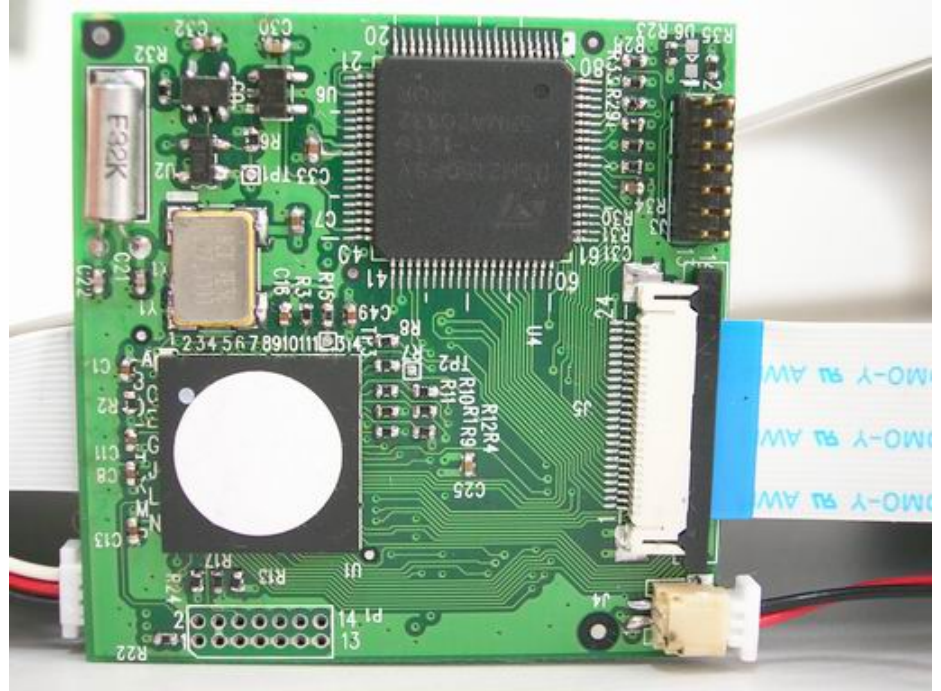
無線網路保密通訊；

串流視訊加解密；

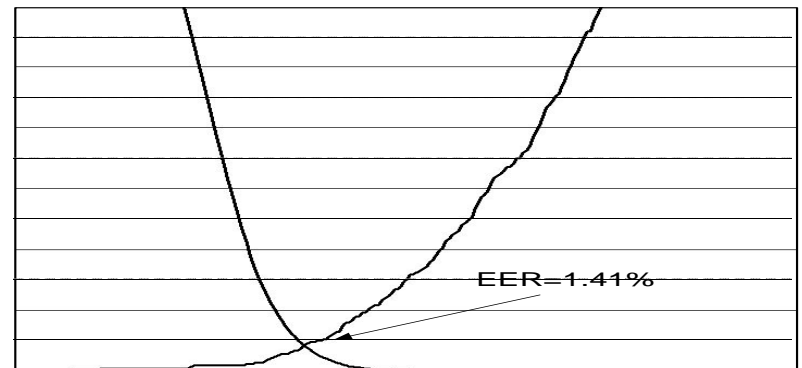
FPGA 電路保密裝置



## DSP嵌入式指紋辨識系統

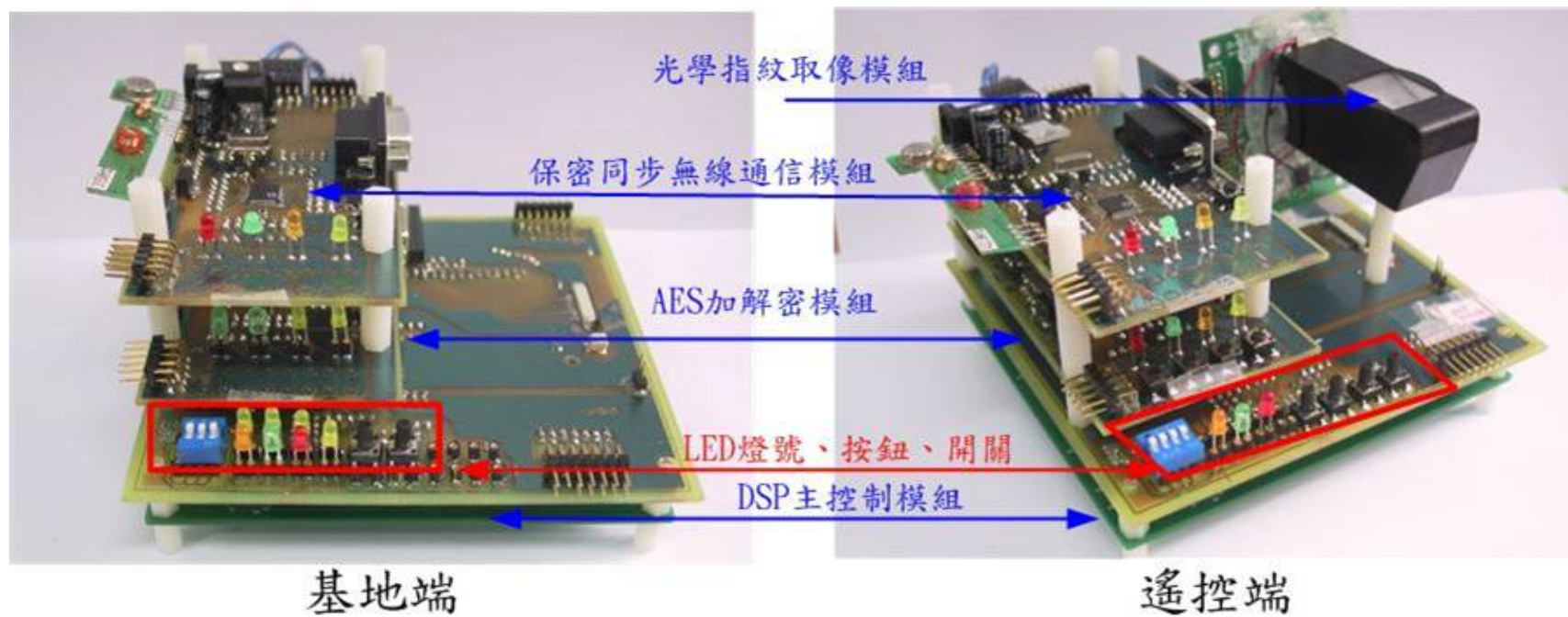


54x13=702枚指紋測試，EER=1.41%  
辨識一枚指紋平均時間小於0.5秒。  
Code Memory:33KBytes  
Data Memory:169KBytes  
Flash Memory: 480 bytes/指紋註冊特徵  
指紋特徵比對速度：800枚/sec



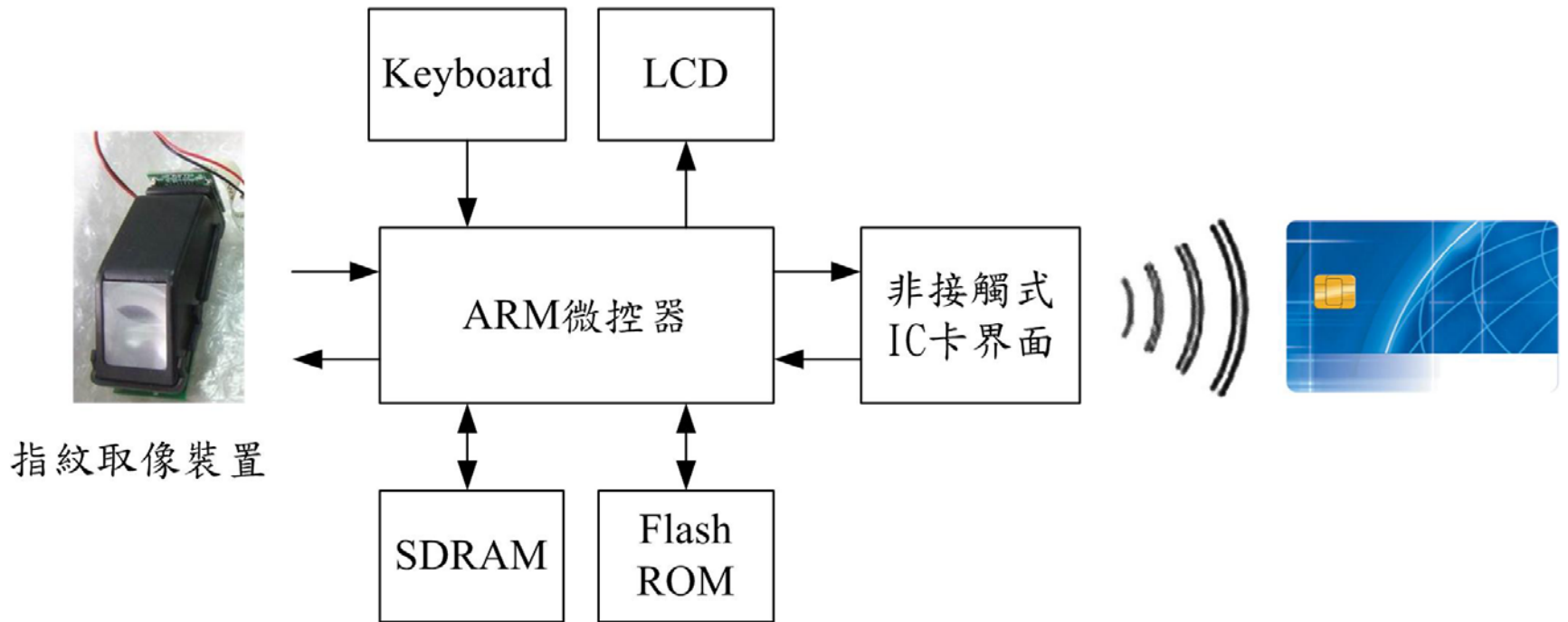


## 具保密通信功能的指紋遙控器





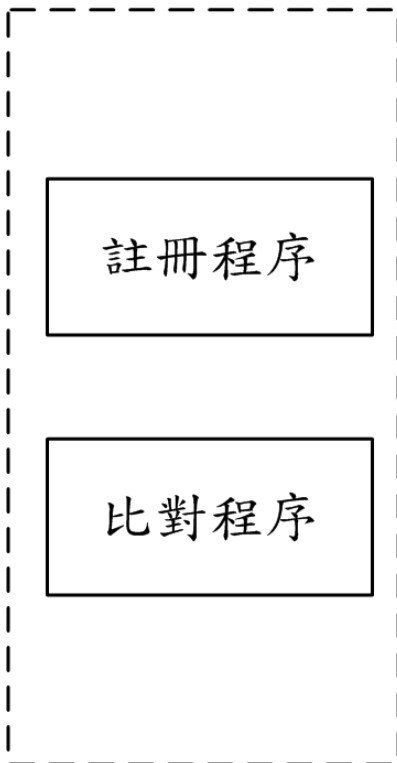
## 非接觸式智慧卡指紋身份識別系統(硬體架構)



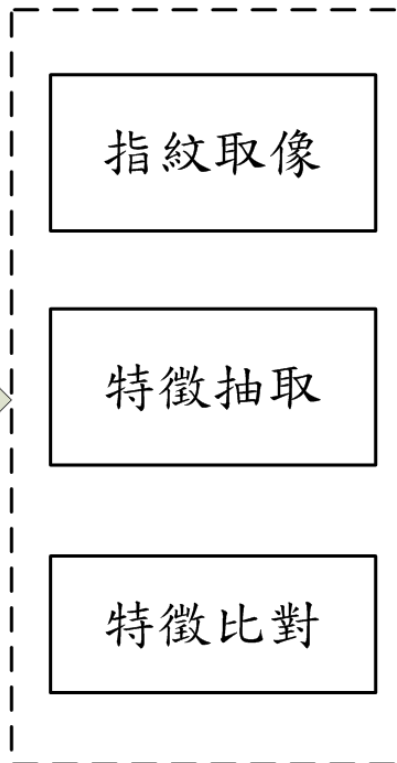


## 非接觸式智慧卡指紋身份識別系統(軟體架構)

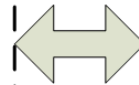
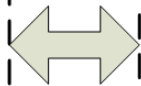
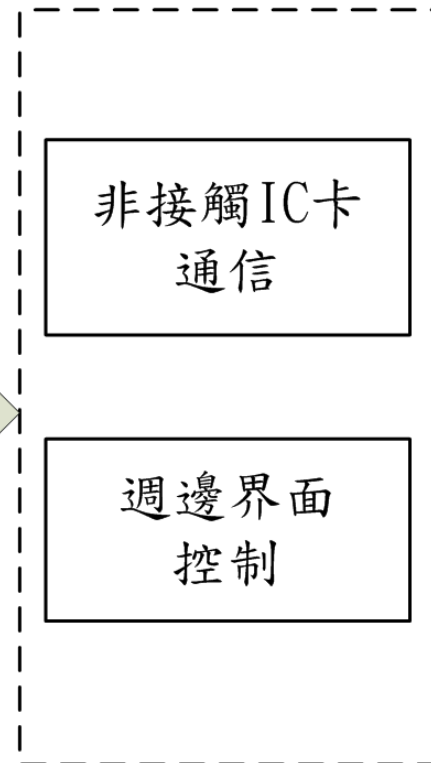
### 身份認證模組

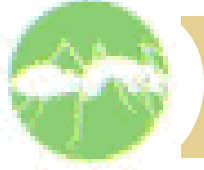


### 指紋辨識模組

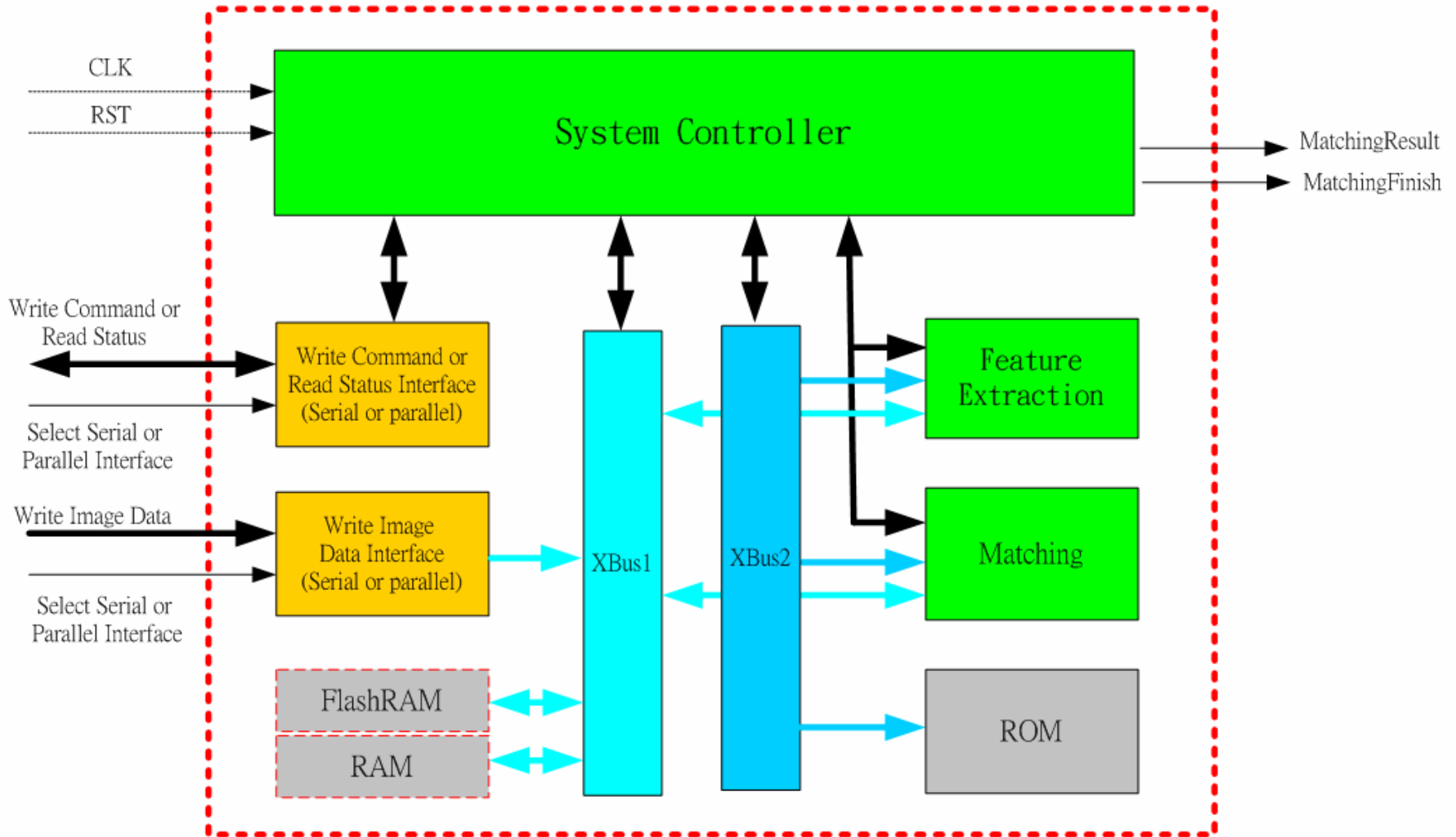


### 界面通信模組





# 指紋辨識系統晶片架構





## 指紋特徵比對晶片

FLEX10KE:EPF10K130EQ240-3

Clock period : 40 ns

Frequency : 25Mhz

工作時間 : 0.82ms ~ 33ms

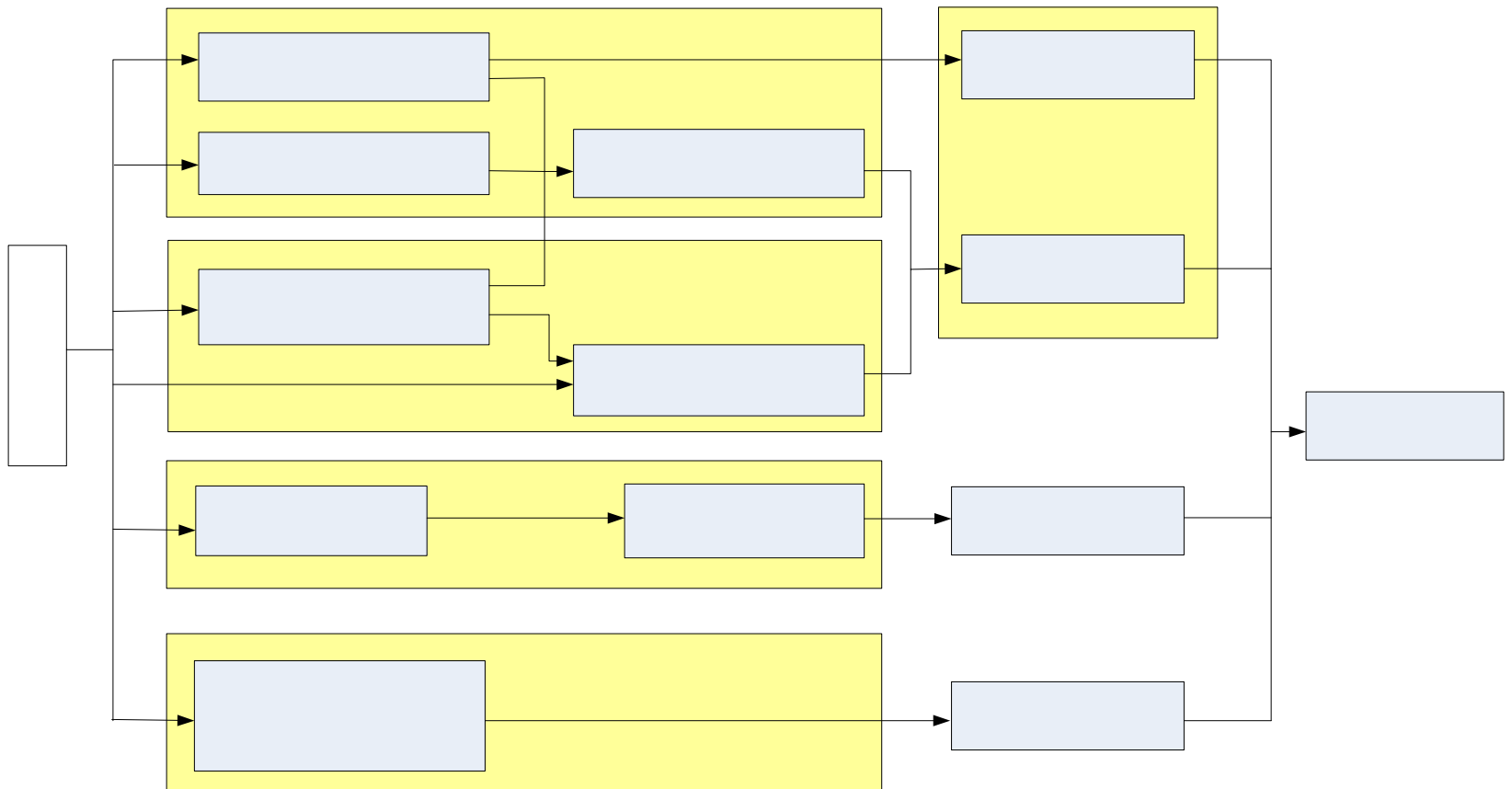
使用資源 :

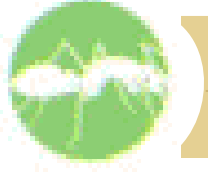
- ✚ Total I/O pins used: 83/180 ( 47%)
- ✚ Total logic cells used: 1545/6656 ( 23%)
- ✚ Total EABs used: 15/16 ( 93%)



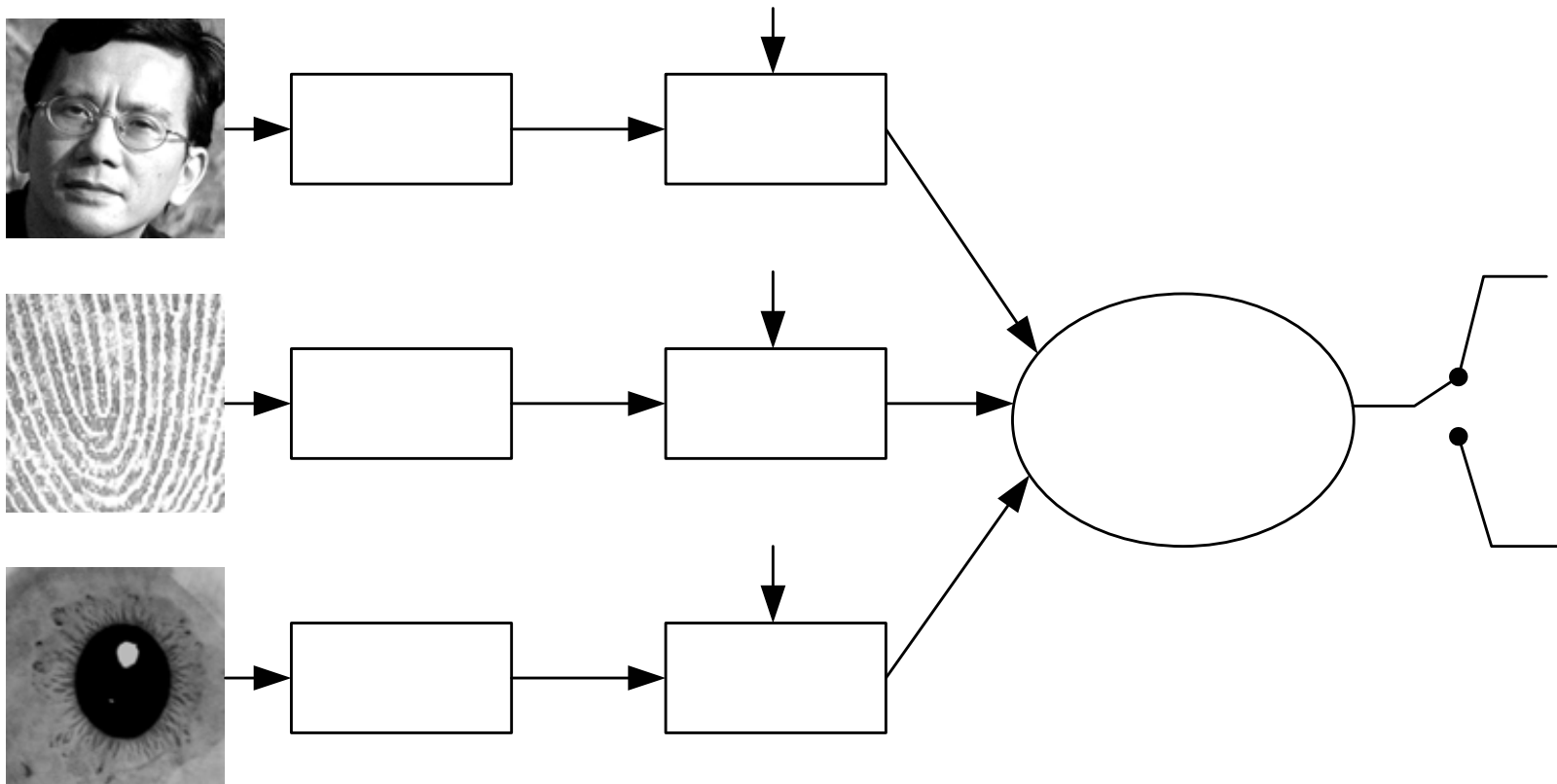


# MIAT 第三代指紋辨識技術





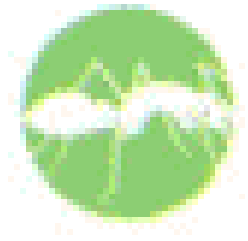
# Multi-modal Biometrics





# Multi-modal Biometrics

	Single Biometrics (Face)	Single Biometrics (Iris)	Multimodal Biometrics (Face+Iris)
Best EER	3.59%	0.7%	0.01%
Average EER	4.77%	1.87%	0.64%



*Fin*