Biometric for Secure Access Control

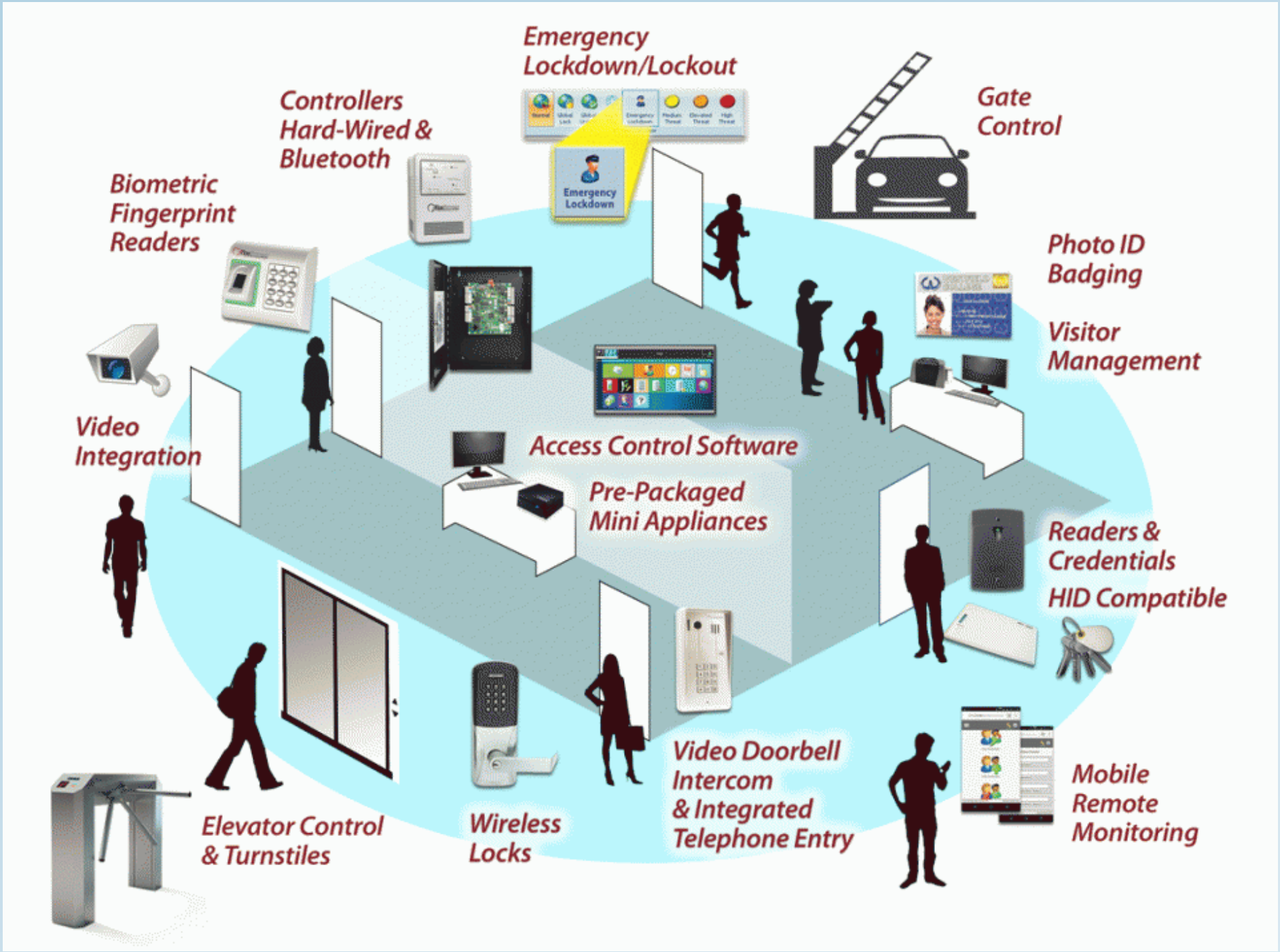
Presenter: Chao-Lung, Chou(周 兆龍)

Department of Computer Science and Information Engineering,
Chung Cheng Institute of Technology, National Defense University

Agenda

- Access control
- Authentication
- Biometric system
- Challenges of biometric access control
- Face anti-spoofing methods
- Conclusions


校園建築
A1 社資中心 (01)
A2 井塘樓 (02)
A3 憩賢樓 (03)
A4 健康中心 (15)
A5 學思樓 (04)
A6 研究大樓 (25)
A7 逸仙樓 (05)
A8 商學院 (26)
A9 中正圖書館 (06)
A10 警衛室 (22)
A11 校友服務中心 (09)
A12 樂活館/自強4舍 (12)
A13 志希樓 (07)
A14 果夫樓 (08)
A15 資訊大樓 (14)
A16 電算中心 (14)
A17 四維堂 (11)
A18 風雨走廊
A19 行政大樓 (16)
A20 風雩樓 (10)
A21 八角亭
A22 集英樓 (17)
A23 新聞館 (18)
A24 大智樓 (19)
A25 大仁樓 (20)
A26 大勇樓 (21)
A27 羅馬廣場
A28 綜合院館 (27)
A29 傳播學院 (31)
A30 楓香步道
A31 道藩樓 (32)
A32 精神堡壘
A33 百年樓 (33)
A34 季陶樓 (34)
A35 藝文中心 (37)
A36 藝中木平台 (37)
A37 國際大樓 (36)
A38 蔣公銅像
A39 國際會館
A40 國際關係中心
A41 研究暨創新育成總中心
運動場所
B1 游泳池 (23)
B2 網球場(山下)
B3 體育館 (24)
B4 攀岩場
B5 籃球場(堤外)
B6 棒球場
B7 網球場(山上)
B8 六期運動場
宿舍
C1 莊敬1-3、9舍 (61-63,67)
C2 莊敬4-8舍 (64-66)
C3 自強10舍 (69)
C4 自強9舍(山居學習中心) (71)
C5 自強5-8舍 (68)
C6 自強1-3舍 (70)
吸菸區
1 憩賢亭 (03)
2 季陶樓前階梯下方 (34)
3 自強5舍旁涼亭 (68)
樂活小舖
B1 影印部
1F 男士理髮部
男女美髮部
鐘錶眼鏡部
體育用品部
H.I.Feeling 早午餐咖啡
2F 心路洗衣部
穆斯林祈禱室
(26) 藍色：教室大樓
(03) 橘色：常去地點
課程教室編碼示意
ex 企業理論 上課教室 26 03 65
26 03 65
A8商學院 (26)
03=3F 大樓樓層
MAP of National Chengchi University
國際關係研究中心 Institute of International Relations
11666臺北市文山區政大里2鄰萬壽路64號
國際會館 International House
台北市文山區秀明路二段112巷17號
大坑溪
濟賢橋
渡賢橋
道南橋
後門口
郵局
電腦&手機部門
伊果咖啡
校內緊急電話
便利商店
學生餐廳
自動提款機
緊急無線電
圖書館
合作社
電梯
吸菸區
政大書城
穆斯林祈禱室

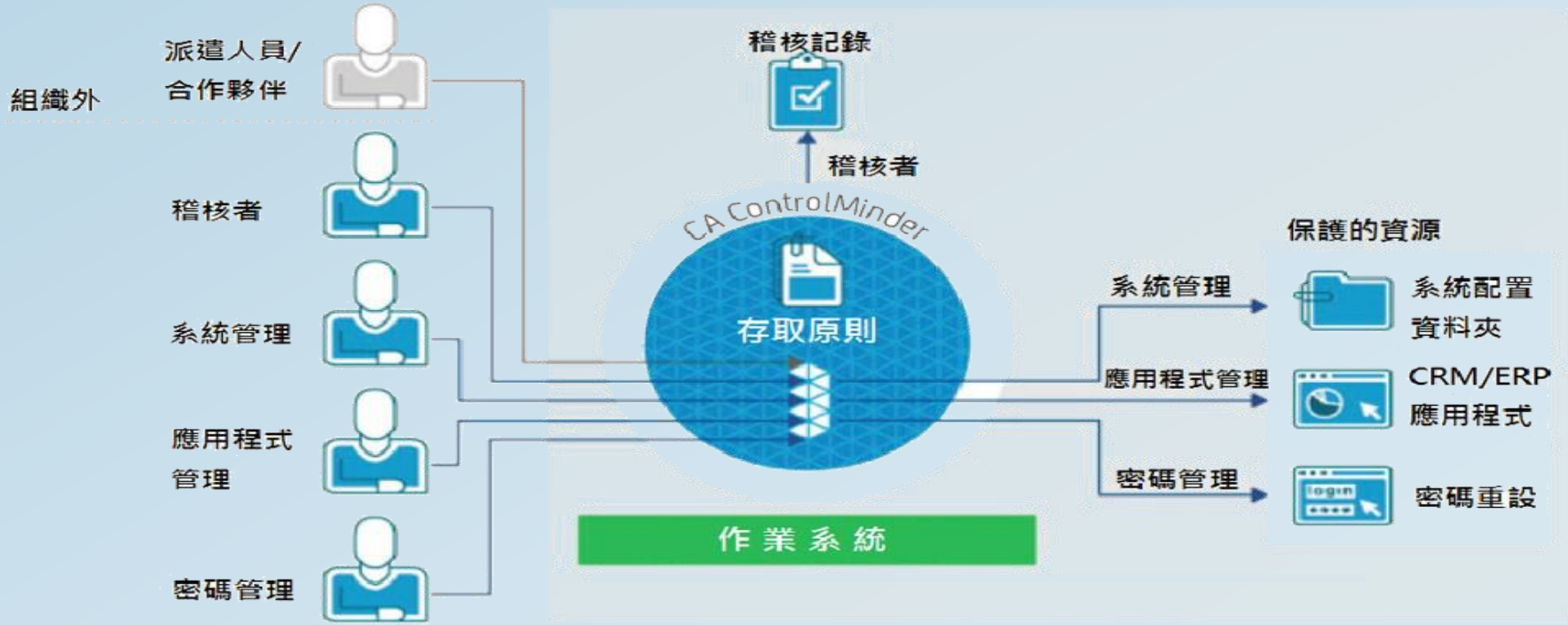

Emergency
Lockdown/Lockout
Controllers
Hard-Wired &
Bluetooth
Gate
Control
Biometric
Fingerprint
Readers
Photo ID
Badging
Visitor
Management
Video
Integration
Access Control Software
Pre-Packaged
Mini Appliances
Readers &
Credentials
HID Compatible
Elevator Control
& Turnstiles
Wireless
Locks
Video Doorbell
Intercom
& Integrated
Telephone Entry
Mobile
Remote
Monitoring
Emergency
Lockdown

Introduction

- **Access control**
  - implements a security ***policy*** that specifies ***who*** or ***what*** may have access to each specific system resources.
  - including ***physical*** and ***logical*** controls.

Introduction

- **Access control**
  - implements a security ***policy*** that specifies ***who*** or ***what*** may have access to each specific system resources.
  - including ***physical*** and ***logical*** controls.

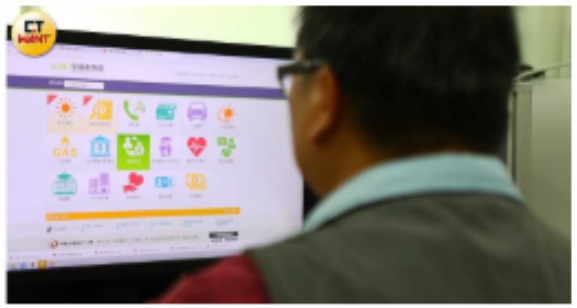


【全國盜領網1】官方繳費平台出包　無密碼免驗證挪用他人存款

為了節省時間，也為了避免在公司、住家與銀行間四處奔波，許多民眾都會透過網路付費平台，繳交例如水費、電費、信用卡費、小孩學費，甚至銀行貸款等生活支出。但由財金資訊公司營運的「全國繳費網」，卻爆出重大資安漏洞，只要有心人掌握了個人身分證字號與銀行帳號，就能在手指與滑鼠間游移，三十秒內無聲無息的讓帳戶存款乾坤大挪移…

2020-05-04 06:32

繼續閱讀



【全國盜領網2】掌握身分證銀行帳號　別人幫你繳房貸

便利民眾繳納各種生活支出的「全國繳費網」，可能已成為詐欺集團犯案的工具。本刊調查，其實今年已有案例，小君（化名）自爆，今年三月間接獲警方通知，銀行存款疑遭盜領，一度還以為是詐騙電話，但刷卡查證後，帳戶裏真的少了五萬元，讓她嚇了一跳。警方深入追查，嫌犯是一名無業的二十六歲賴姓男子，透過他的銀行來往紀錄，發現竟還…

2020-05-04 06:32

繼續閱讀

【全國盜領網3】手機就可登錄操作　存款遭清空都不知道

財金公司營運的「全國繳費網」爆發資安漏洞，本刊記者實測電腦版「全國繳費網」，真的只要掌握別人的身分證字號，就能利用別人的銀行帳號，轉走帳戶裏的錢。而且帳戶款項遭轉出後，也沒有接獲銀行通知，尤其，「全國繳費網」也有手機版，只要登錄就可操作，讓人覺得十分擔憂。本刊記者實測，登入「全國繳費網」後，在繳納信用卡費…

2020-05-04 06:32

繼續閱讀

【全國盜領網4】銀行公會主導創建　涵蓋1800家企業繳費項目

財政部及公、民營金融機構共同出資，籌設的「財金資訊股份有限公司」，原本是財政部於西元一九八四年以任務編組方式，成立的「金融資訊規劃設計小組，到了一九九八年，報奉行政院核定，這才改制為公司組織。「全國繳費網」則是西元二〇〇四年九月由銀行公會主導建置示範性網站，由財金公司負責營運維修，可提供民眾即時網上繳費的跨行…

2020-05-04 06:32 https://www.ctwant.com/search?q=%E7%9B%9C%E9%A0%98

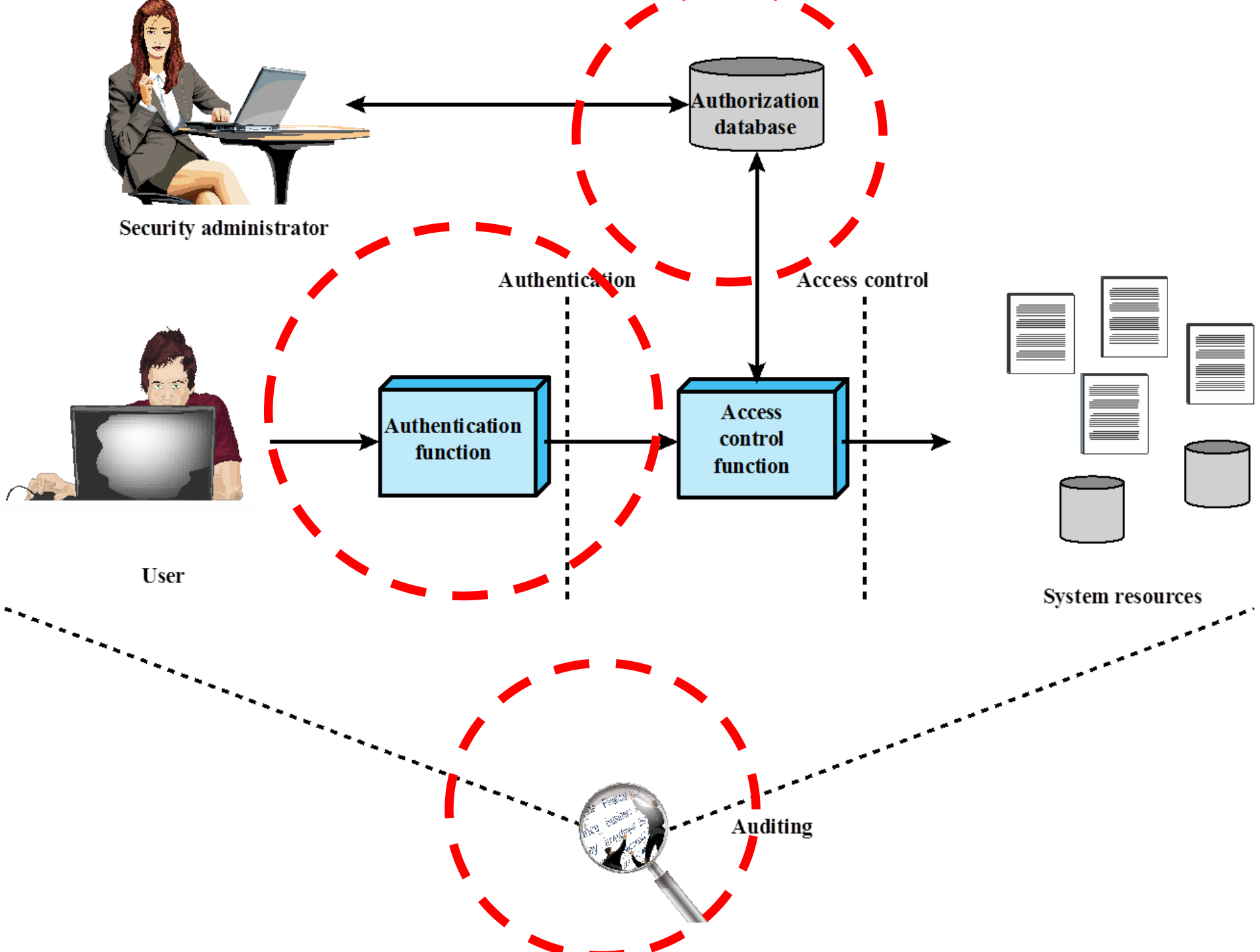
繼續閱讀

Introduction

- **Threats to access control**
  - Gaining physical access
  - Bypassing security
  - Exploiting hardware and software
  - Intercepting communication

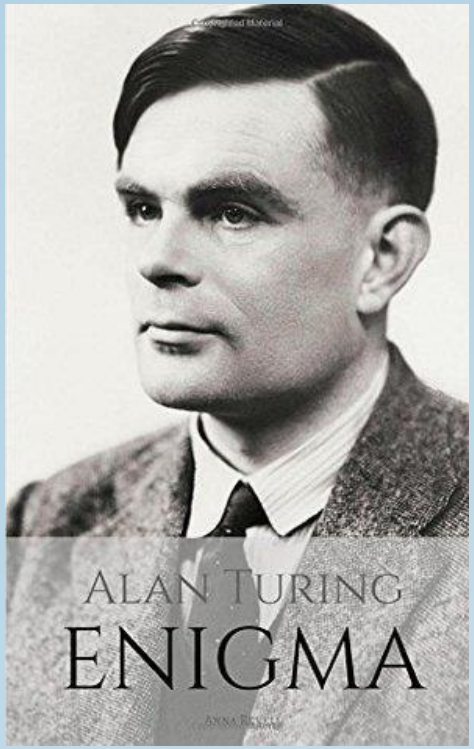
Access control

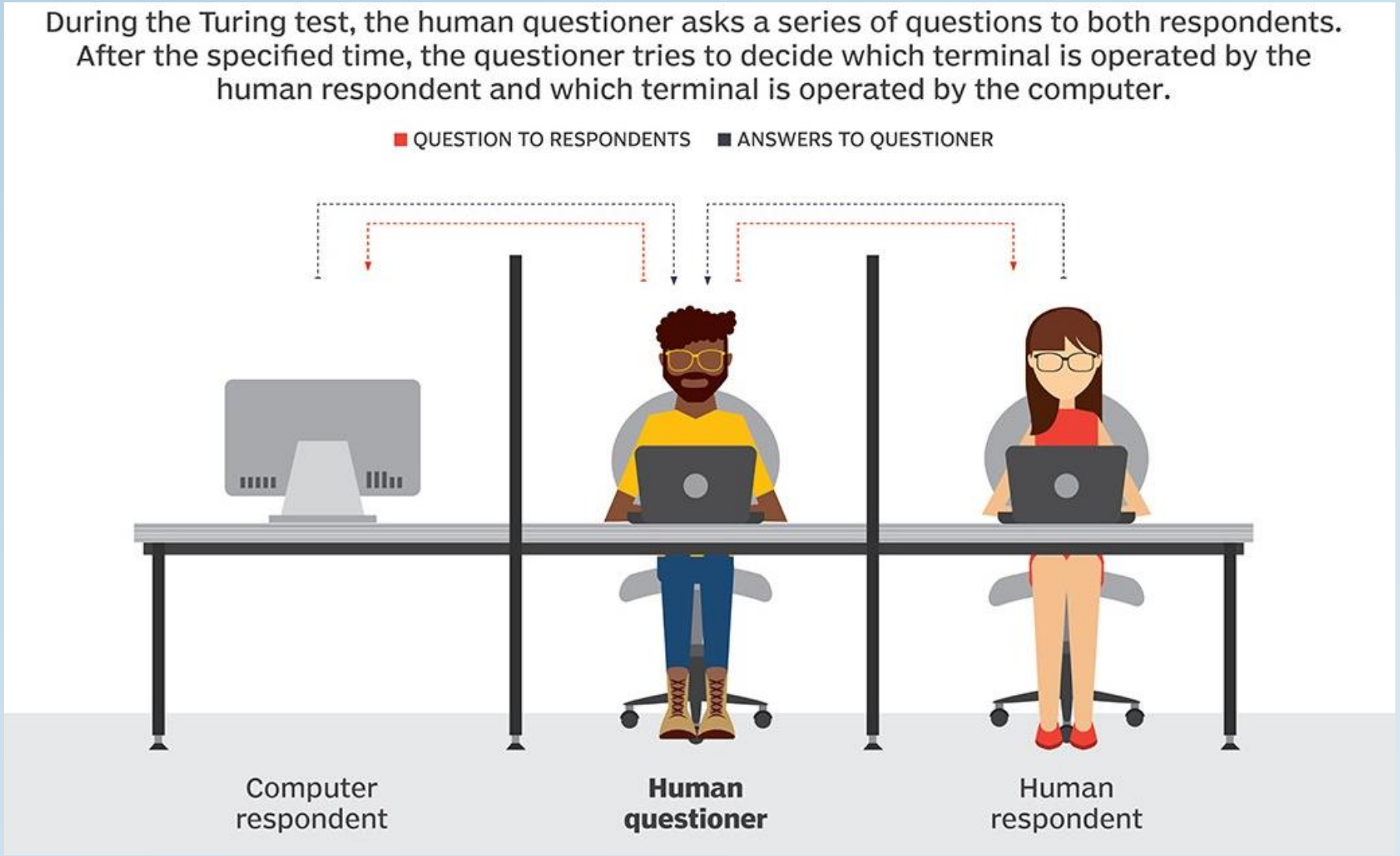
- The **AAA** Protections
  - **Authentication**: Proof of ***identity***. (Who a person is?)
  - **Authorization**: The assignment of ***permissions*** to individuals or roles. (What a person may do?)
  - **Auditing**: What the person actually ***did***.


Authorization database
Security administrator
Authentication
Access control
Authentication function
Access control function
User
System resources
Auditing


THE TRUE ENIGMA
WAS THE MAN WHO CRACKED
THE CODE
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
THE IMITATION GAME

Turing test





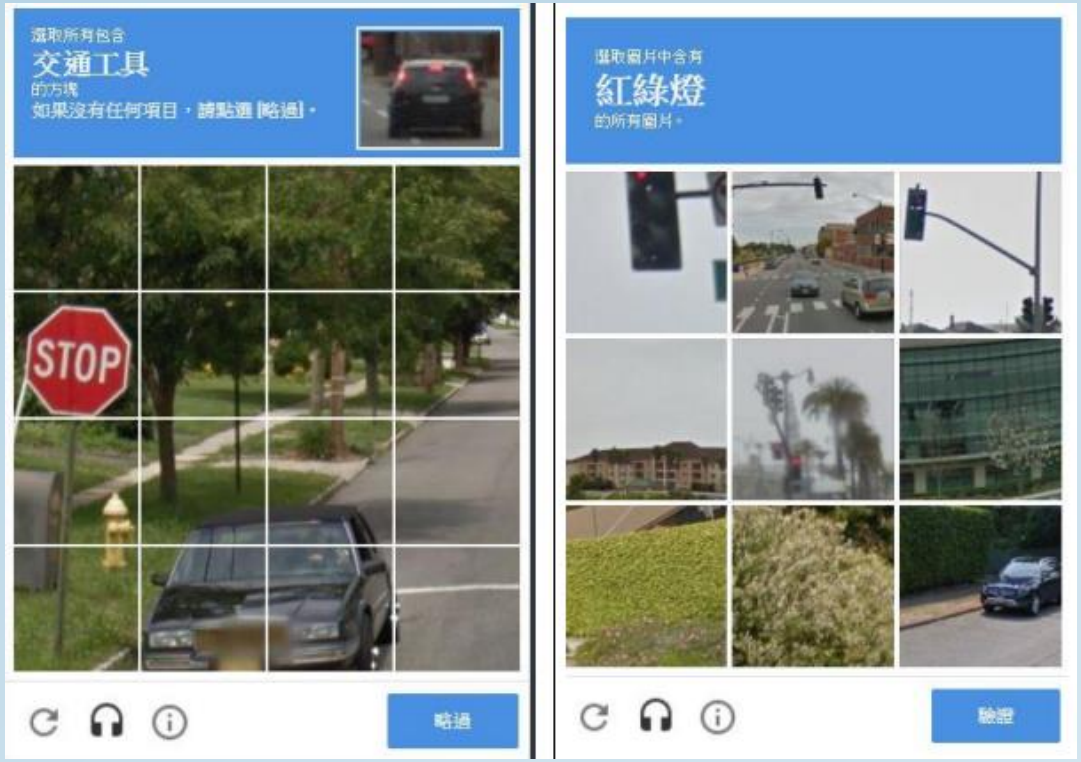
https://searchenterpriseai.techtarget.com/definition/Turing-test

Turing test

- **Imitation game** http://whichfaceisreal.com/index.php

Turing test

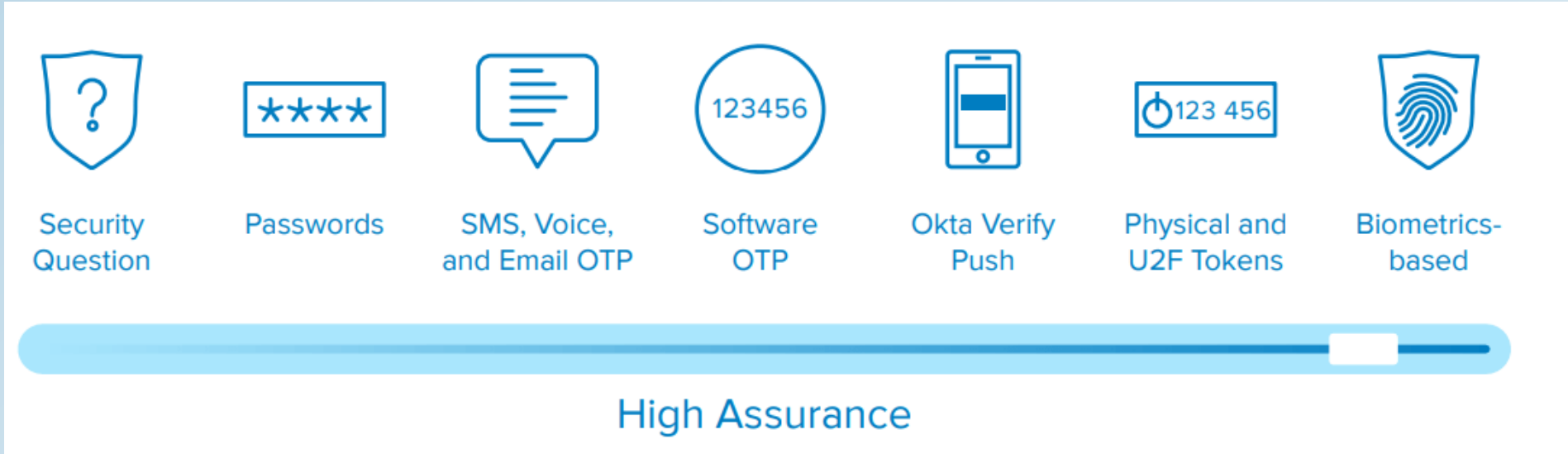
- **CAPTCHA**
  - Completely Automated Public Turing test to tell Computers and Humans Apart



http://www.takming.edu.tw/cc/resources/tech/T070_%E8%AA%8D%E8%AD%98CAPTCHA.pdf

Authentication types

- **Knowledge:** Something you know e.g., password
- **Ownership:** Something you have e.g., badge
- **Location:** Somewhere you are
- **Characteristics:** Something you are e.g., fingerprints
- **Action:** Something you do e.g., walk, keystroke

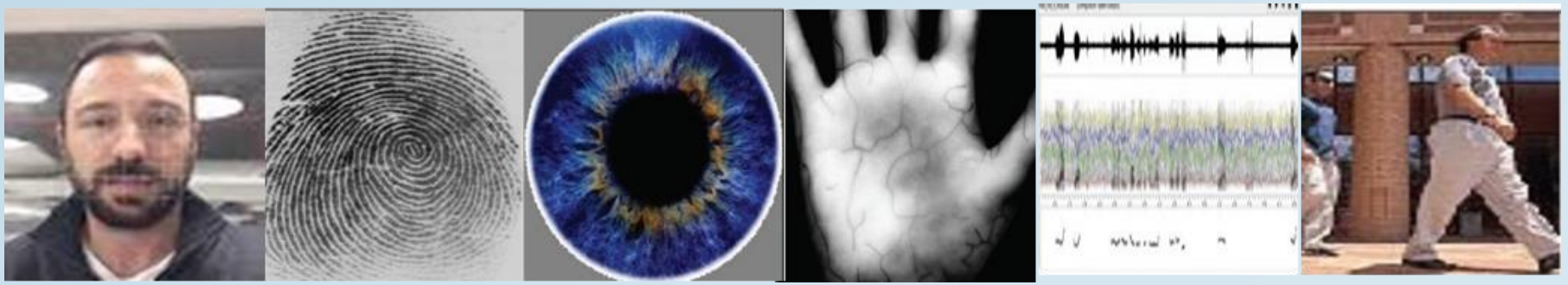


Authentication types

- Single-factor Authentication
  - Only one form of five types authentication
- Two-Factor Authentication(2FA)
  - Combined ***two or more*** types of authentication
  - Provides higher level of security

Biometric basics

- **Biometric** is the automated process of identifying or verifying an individual based upon his or her **physical** or **behavioral** characteristics.
  - Physical properties = something you ***are***
    - **Face, Iris, Fingerprint, Retina, Ear, Palm vein…**
  - Behavioral properties = something you ***do***
    - **Handwrite, Gait, Voice, Keystroke**…



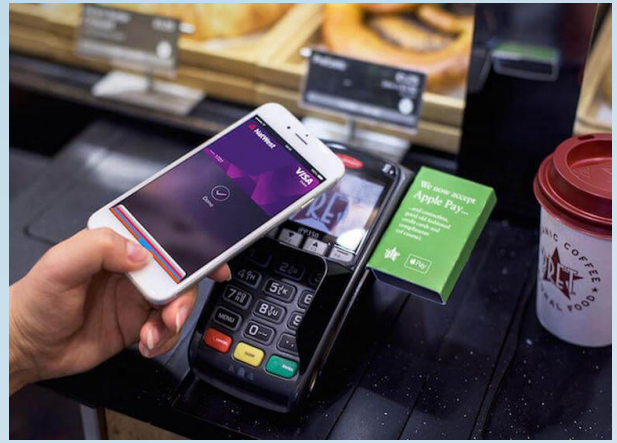
Biometric basics

- Biometric features:

Biometrics applications

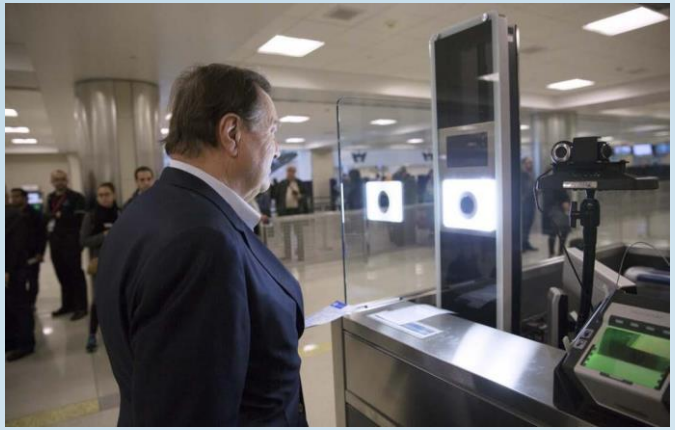
Access Control

Banking



Mobile Payment

Military

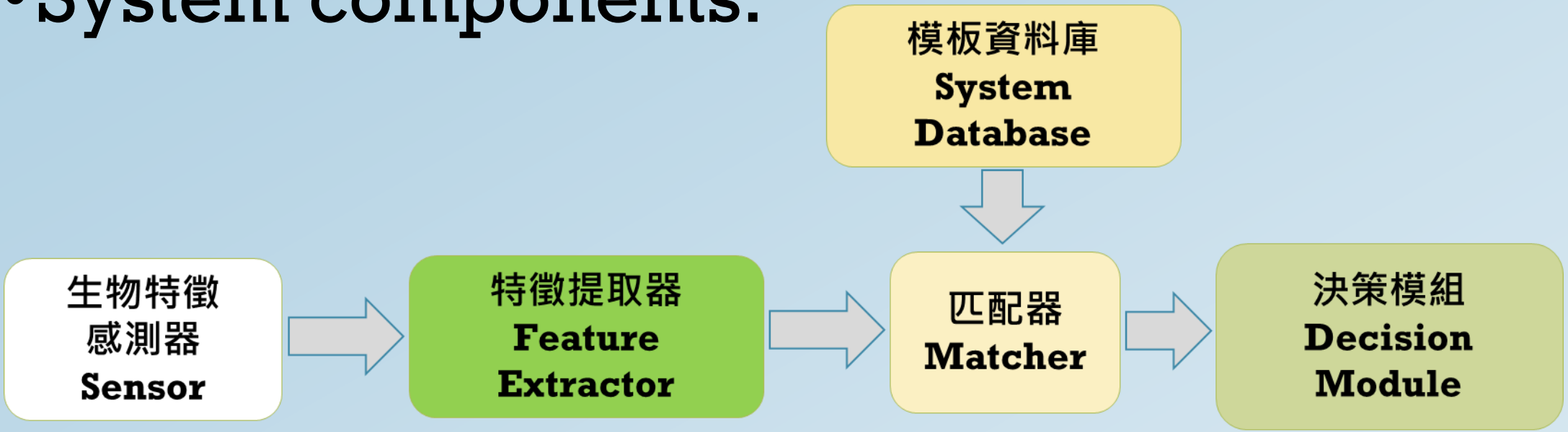


Border control

Law Enforcement

Biometrics system

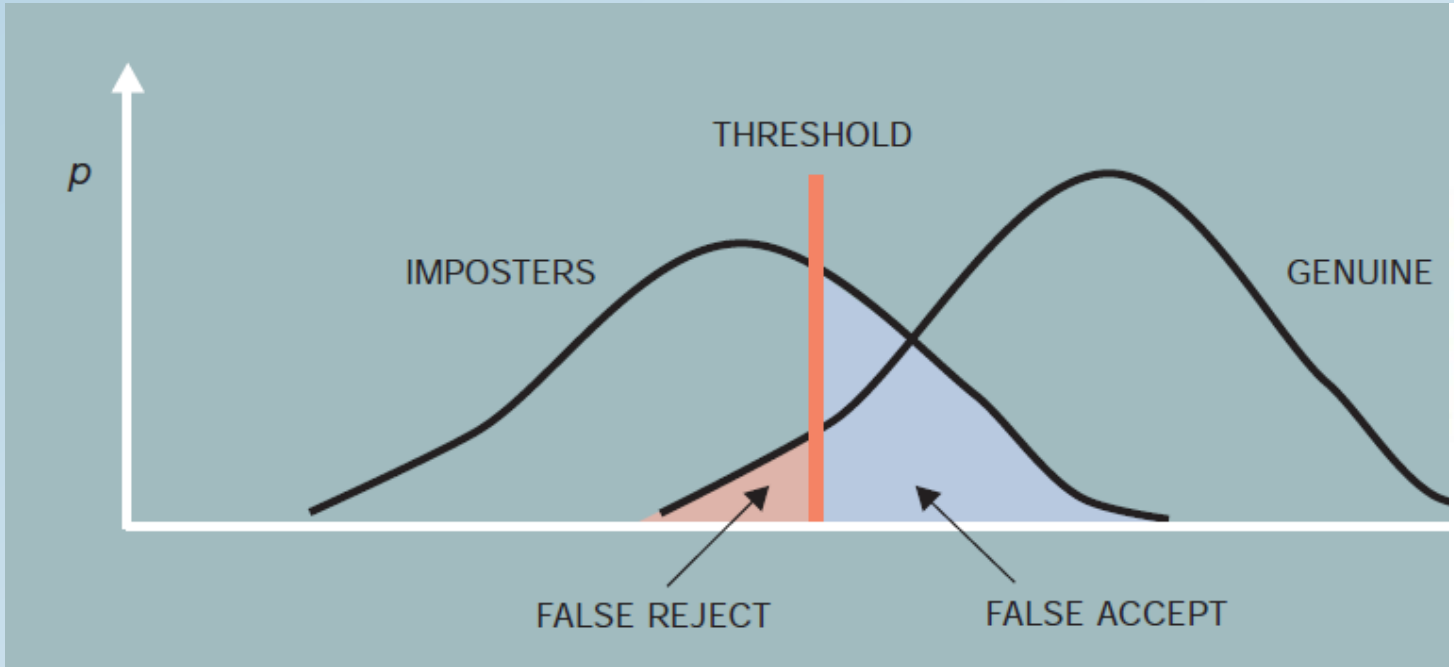
- System components:

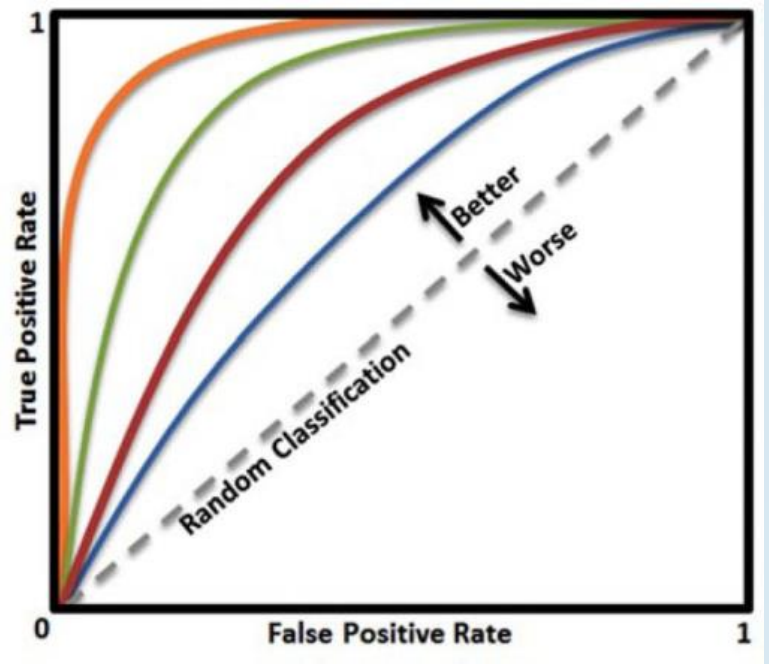


- **Enrollment**
- **Identification (1-to-many)**
- **Verification (1-to-1)**

Biometrics system

- System Evaluation
  - ROC (Receiver Operating Characteristic) curve: plotting by two errors FAR against FRR with the decision threshold as the free variable.





Biometrics system comparison

Biometric	Accuracy	Reliability	Errors
Fingerprint	Very High	High	Dirt, dryness
Face	High	Medium	Hair, glasses, age
Hand Geometry	High	Medium	Hand injury
Iris	Very High	High	Poor lighting
Retinal	Very High	High	Glasses
Voice	Medium	Low	Noise, colds
Signature	Medium	Low	Changing signatures

Accuracy: How well can the specific biometric is able to tell individual apart.
Reliability: How dependable the specific biometric is for recognition purposes.

Biometrics system

- **Concerns of biometrics:**
  - **Performance**
  - **Accuracy**
    - FAR/FRR
  - **Acceptability**
    - Intrusive / non-intrusive / physical harm
  - **Cost**
  - **Can not be used with certain groups**
    - Disabilities

Biometrics system

- 倒垃圾也要"刷臉"!宛如1人1支監視器 "臉部辨識"遍布全中國｜【國際大現場】20190712｜三立新聞台
  https://www.youtube.com/watch?v=x6FMNx33kzY

- 快遞櫃「刷臉取件」已被小學生破解 其他刷臉系統可靠嗎？｜20191102慧眼看天下第75集-透視兩岸
  https://www.youtube.com/watch?v=k0F6O8G3vPg&t=47s

Samsung Galaxy S10 臉部辨識易破解，建議以指紋辨識為主

Samsung Galaxy S10 這款風雲新旗艦取消了前幾代所配有的虹膜辨識解鎖功能，導入新的聲波螢幕指紋辨識技術，並保留其臉部辨識解鎖、圖形解鎖等功能，其所搭載的 2D 臉部解鎖功能中的加快辨識功能由於只需拿起手機對準前鏡頭就能解鎖的方便性讓許多人愛用，不過官方也明確標示開啟加快辨識可能會降低安全性，國外已經有多個案例表明確有其事。

https://www.kocpc.com.tw/archives/247859

首先國外知名 YouTube 開箱頻道 Unbox Therapy 在近日所上架的影片中，使用另一部手機播放自己頻道上的影片，並將螢幕對準手機前鏡頭，就能以臉部辨識成功令手機解鎖，即使它的手機螢幕上有指紋、灰塵等，S10 的臉部解鎖似乎無法偵測出這些干擾。

義大利科技網站 Smart World 也成功以靜態的圖片成功騙過 Galaxy S10 的臉部辨識器，成功將手機解鎖。

騙過登機、支付系統！AI新創用擬真面具和照片，破解臉部辨識技術

2019.12.16 by Dylan Yeh

- 人工智慧新創公司Kneron以擬真面具及照片分別騙過了支付系統及中國與荷蘭機場的身份辨識系統

Source: https://www.bnext.com.tw/article/55917/airport-store-facial-recognition-systems-fooled

Biometrics system

- **Challenges of biometrics:**
  - **Privacy** (acceptability)
    - **Identity theft**
    - Data protection
    - Data sharing
  - **Security** (circumvention)
    - **Spoofing**
    - Biometrics cannot be changed

內政部數位身分證最新時程出爐！ 明年7月開始全面換發

內政部換發數位身分證最新時程曝光，初步規畫在明年1月開始在澎湖縣、新竹市及部分新北市試辦數位身分證，明年7月開始全面換發。

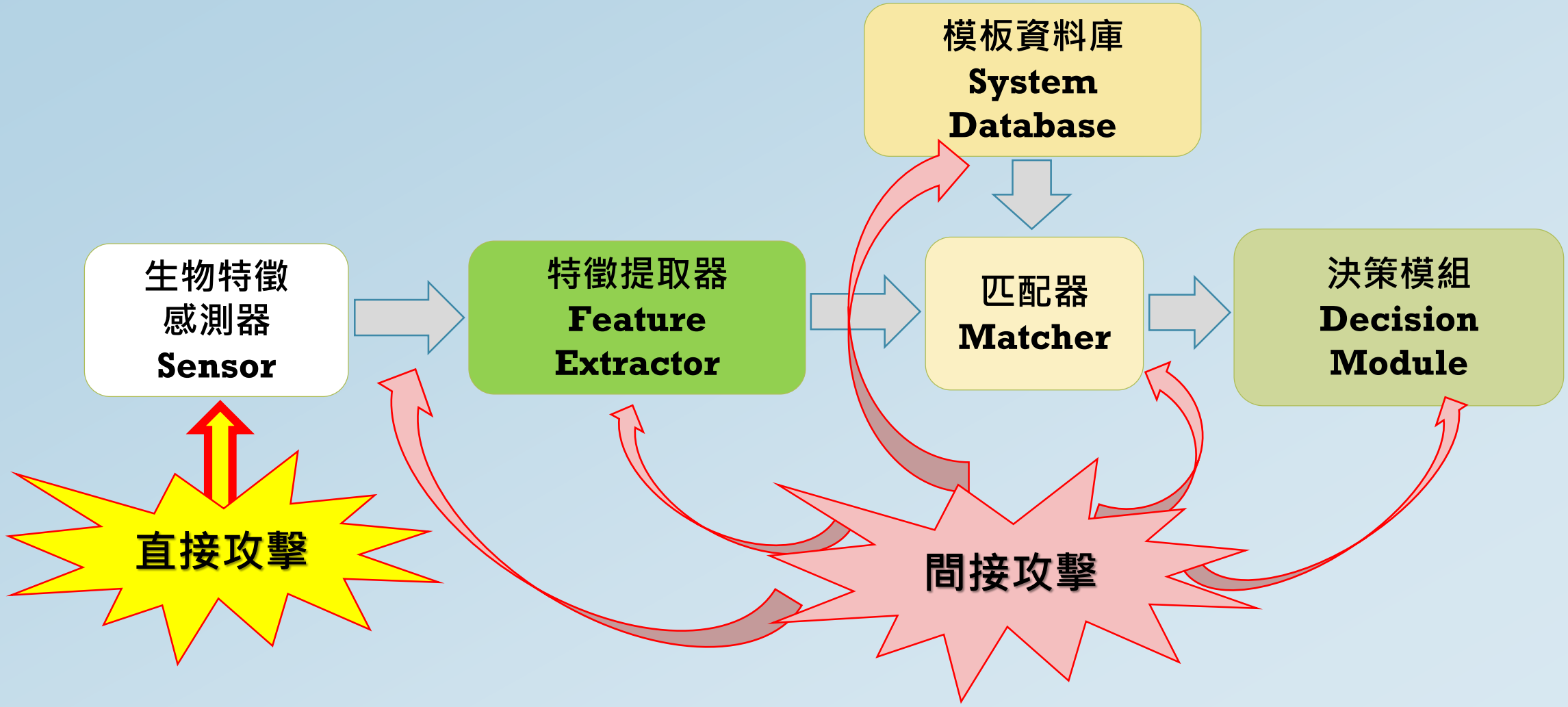
文/ 蘇文彬 | 2020-10-05 發表

讚 6.2 萬 按讚加入iThome粉絲團 讚 118 分享

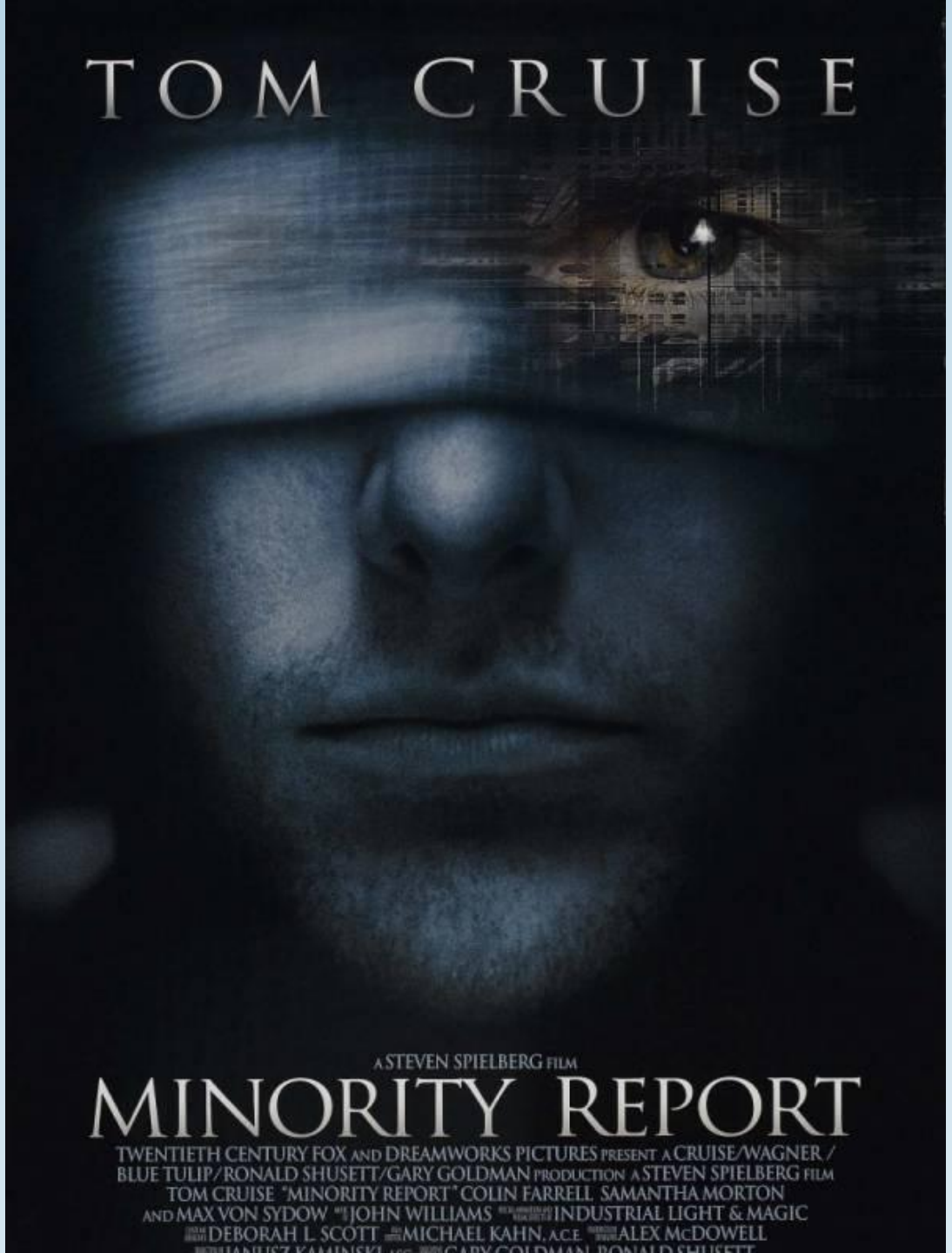
未來換發的數位身分識別證將採用PC晶片卡，卡面記載姓名、出生日期等5項資料。

source: https://www.ithome.com.tw/news/140353

Biometric system vulnerabilities




BLU-RAY™ + DIGITAL HD
MISSION: IMPOSSIBLE
THE 5 MOVIE COLLECTION
TOM CRUISE
MISSION: IMPOSSIBLE
ROGUE NATION
TOM CRUISE
MISSION: IMPOSSIBLE
TOM CRUISE
M:I-2
TOM CRUISE
M:I-III
TOM CRUISE
MISSION: IMPOSSIBLE
GHOST PROTOCOL


TOM CRUISE
A STEVEN SPIELBERG FILM
MINORITY REPORT
TWENTIETH CENTURY FOX AND DREAMWORKS PICTURES PRESENT A CRUISE/WAGNER /
BLUE TULIP/RONALD SHUSETT/GARY GOLDMAN PRODUCTION A STEVEN SPIELBERG FILM
TOM CRUISE "MINORITY REPORT" COLIN FARRELL SAMANTHA MORTON
AND MAX VON SYDOW JOHN WILLIAMS INDUSTRIAL LIGHT & MAGIC
DEBORAH L. SCOTT MICHAEL KAHN, A.C.E. ALEX McDOWELL

Types of presentation attacks

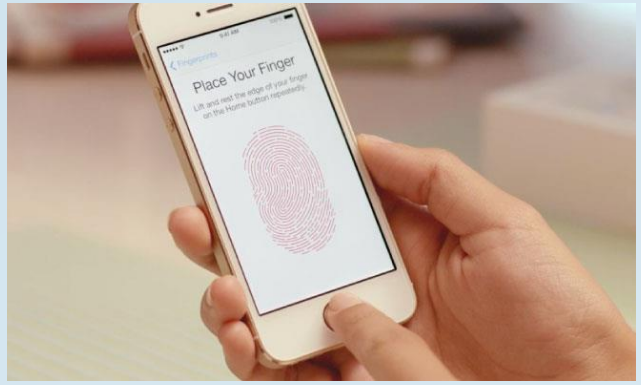
- **Face** presentation attacks
  - Photograph
  - Video
  - 3D mask
  - Makeup
  - Plastic surgery
- Ex:
  - Samsung S8/S10
  - https://www.ettoday.net/news/20190108/1350903.htm

Types of presentation attacks

- **Iris** presentation attacks
  - Photograph
  - Video
  - Artificial eyeball
  - Contact lens
  - Real eye

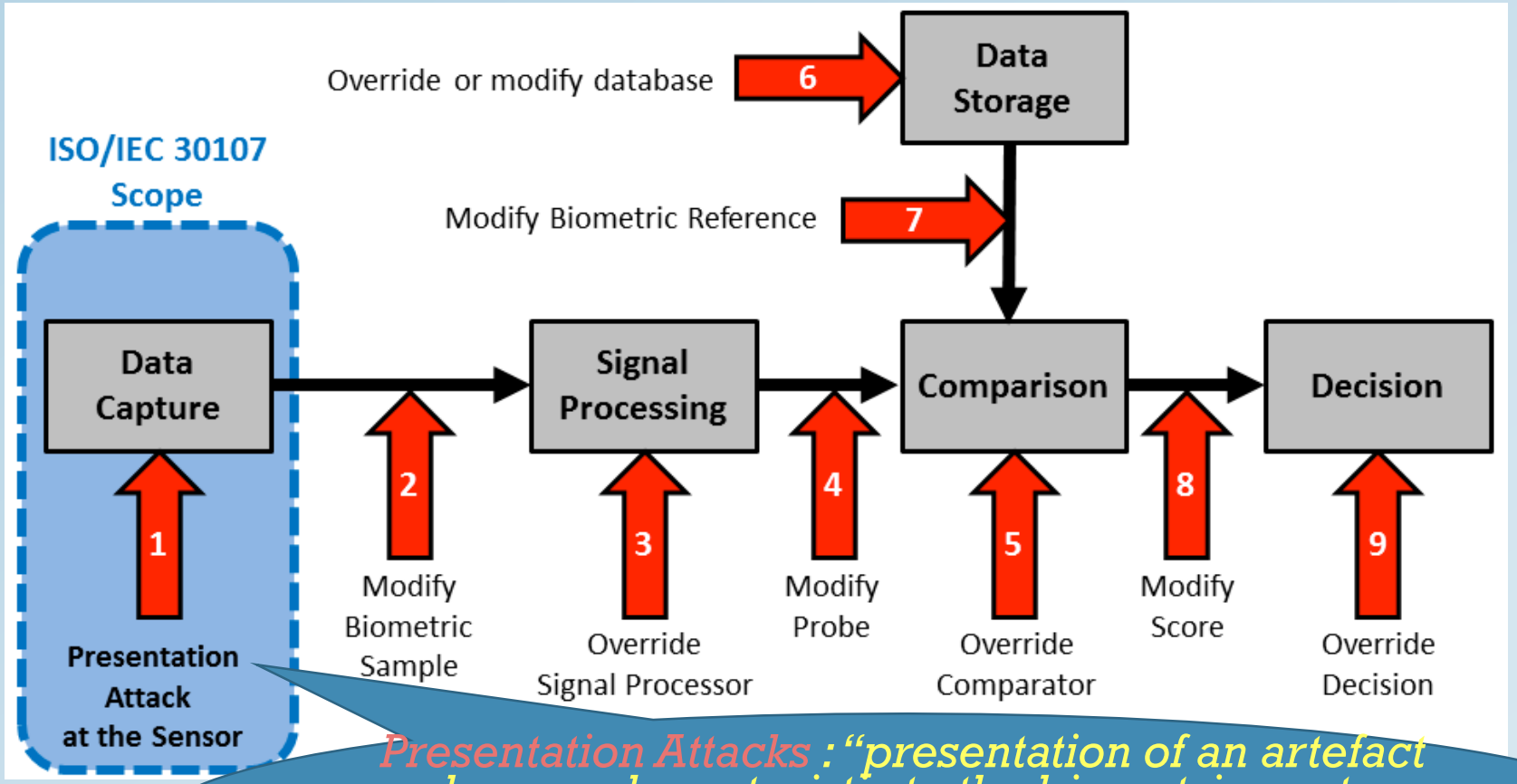
Types of presentation attacks

- **Fingerprint** presentation attacks
  - 2D fake fingerprint
  - 3D fake fingerprint
  - Cadaver fingerprint
  - Reverse-engineered fingerprint image
- Ex:
  - iPhone 5S Touch ID



Biometrics system security

- ISO/IEC 30107 Presentation Attack Detection (PAD)



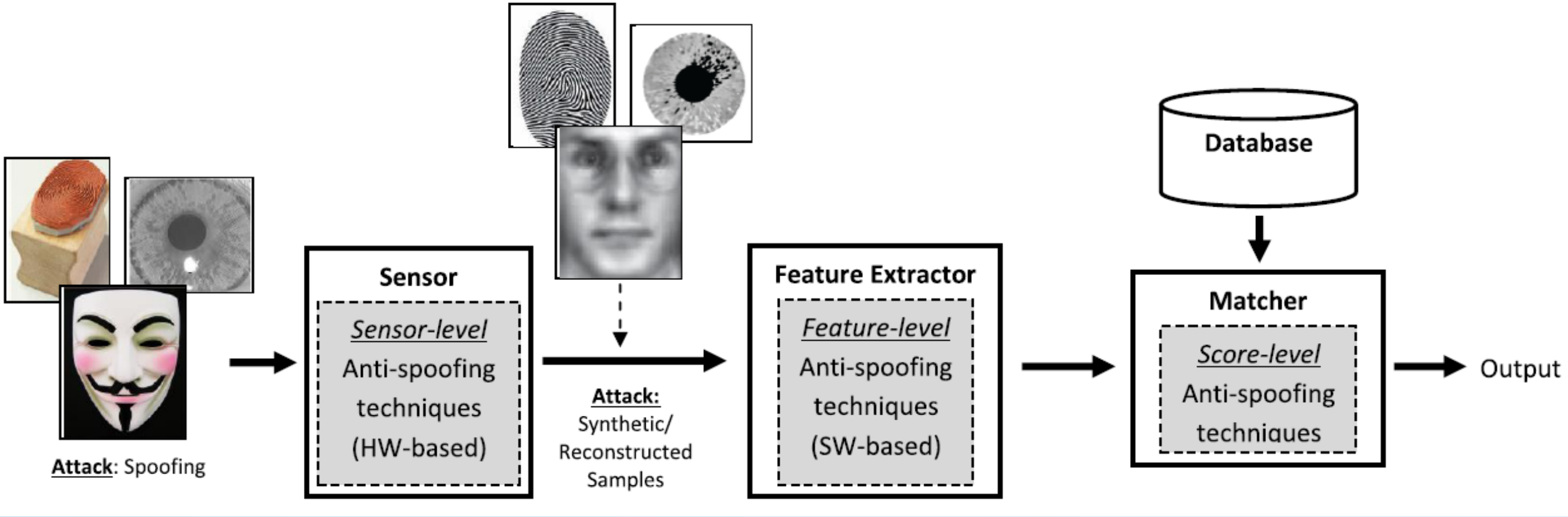
*Presentation Attacks : "presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could **interfere** with the intended policy of the biometric system."*

Biometrics system security

- **PAD** commonly known as **liveness detection** or **anti-spoofing.**
- The goal of PAD is to determine if the biometric being captured is an *actual* measurement from the authorized, ***live*** person who is present at the time of capture.

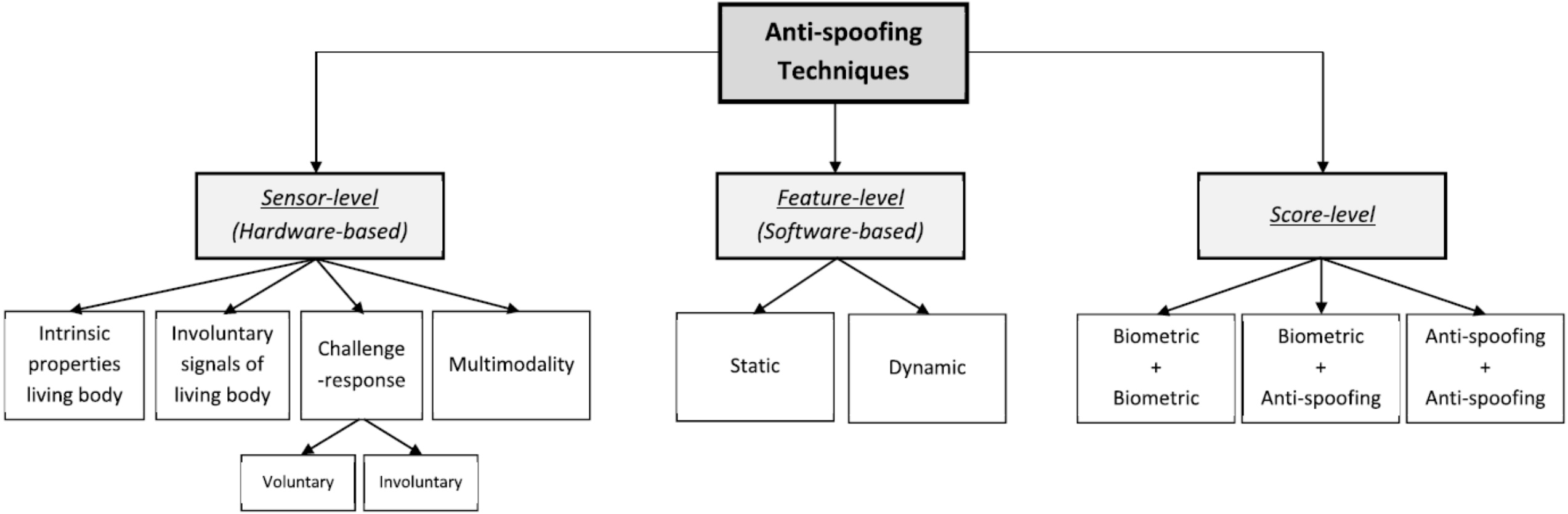
Biometrics system security

- An anti-spoofing biometric system



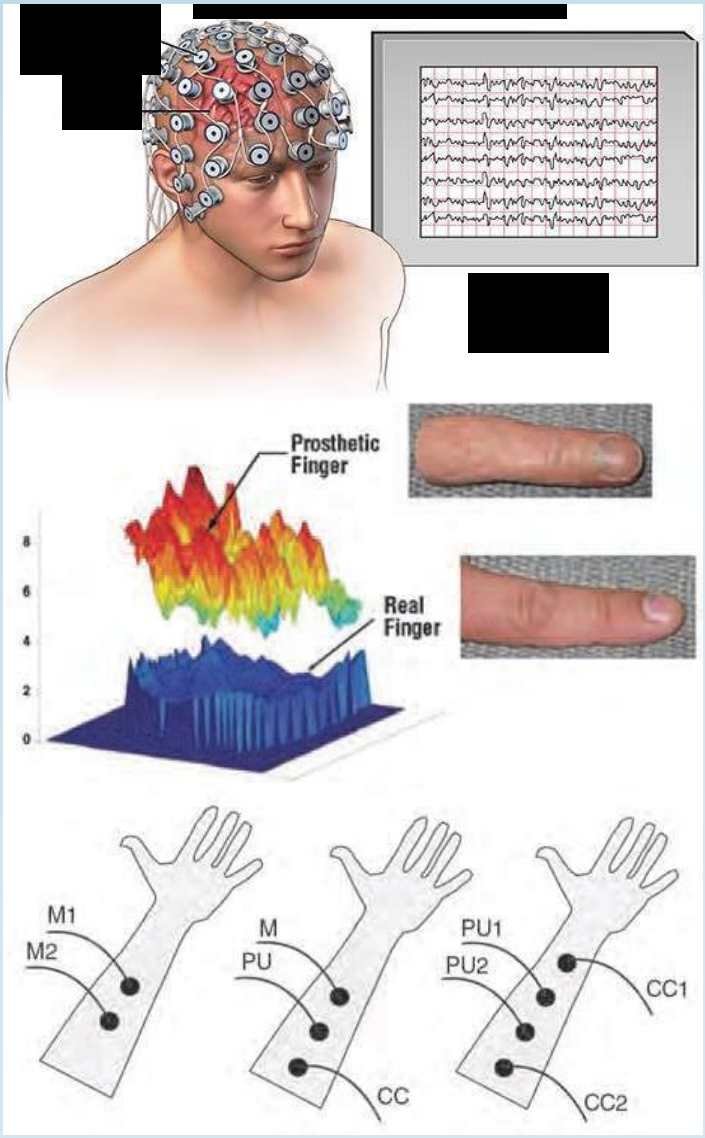
Biometrics system security

- An anti-spoofing biometric system



Presentation attack detection

- Hardware-based
  - Pulse measurement
  - Temperature measurement
  - Skin resistance detection
  - Blood pressure
  - Infrared & ultraviolet light

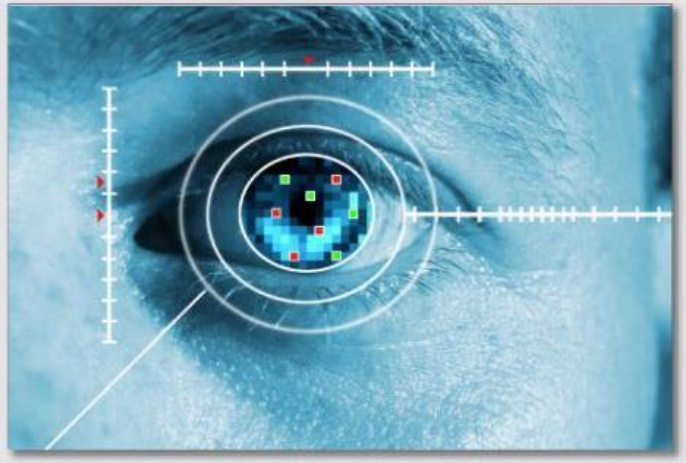
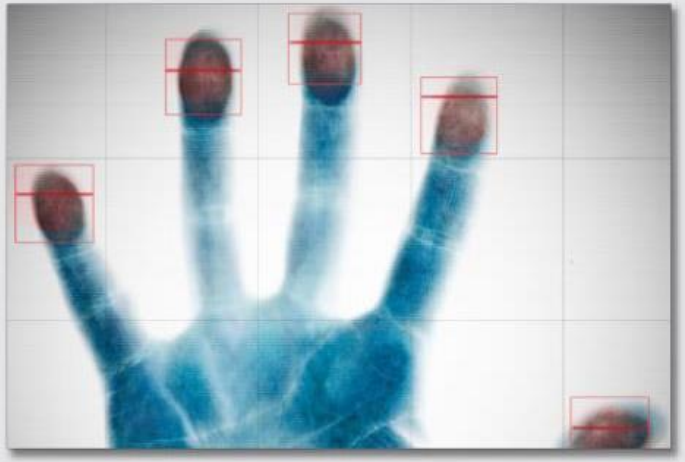


Presentation attack detection

- Software-based
  - Static
    - Only one instance of the biometric trait
    - Ex: photo
  - Dynamic
    - A sequence of samples captured over time
    - Ex: video

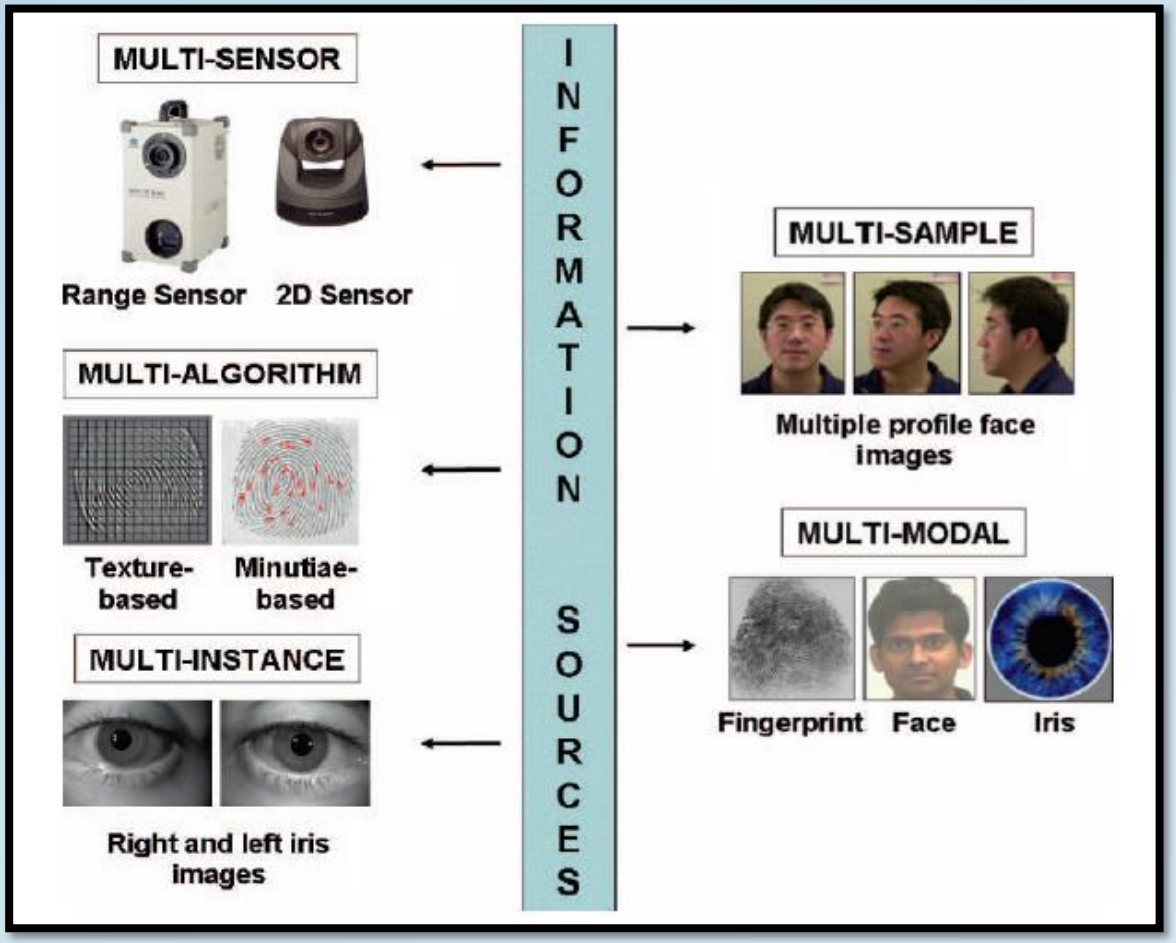
Presentation attack detection

- Fusion-based
  - A combination of multiple pieces of the biometric traits.
  - Hardware-based + Software-based
  - Multimodal biometrics


Multimodal Biometrics

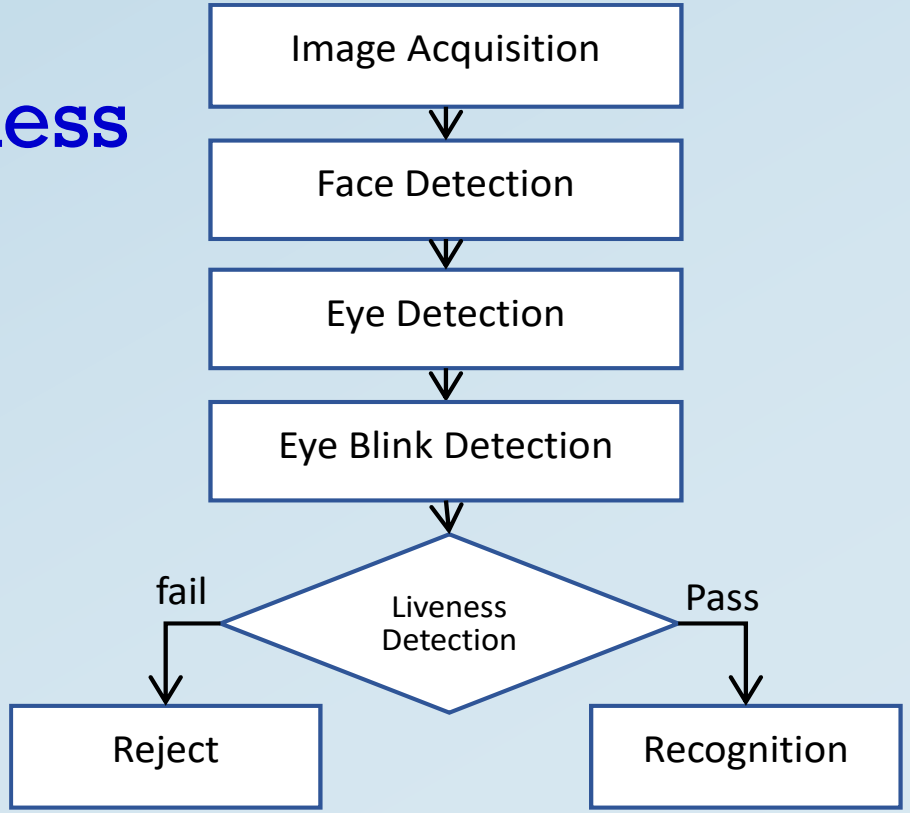
- Multimodal Biometrics:
  - Multiple sensors
  - Multiple algorithms
  - Multiple instances
  - Multiple samples
  - Multiple biometrics



Ross A., Nandakumar K., Jain A. K., Handbook of Multibiometrics, Springer, New York, USA, 2006.

PAD Example#1

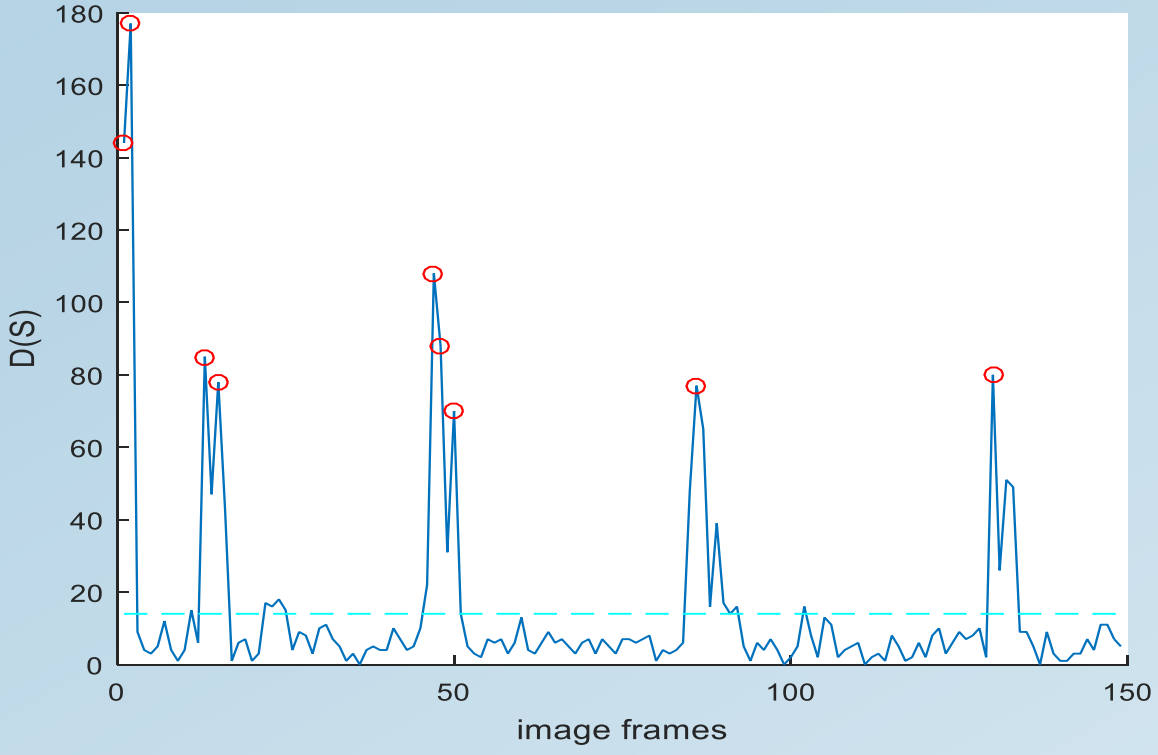
- Blink detection:
  - A healthy human blinks once every 4 to 6 seconds in a minute.
  - Based on the ratio of eye openness
  - Resist to photo attack



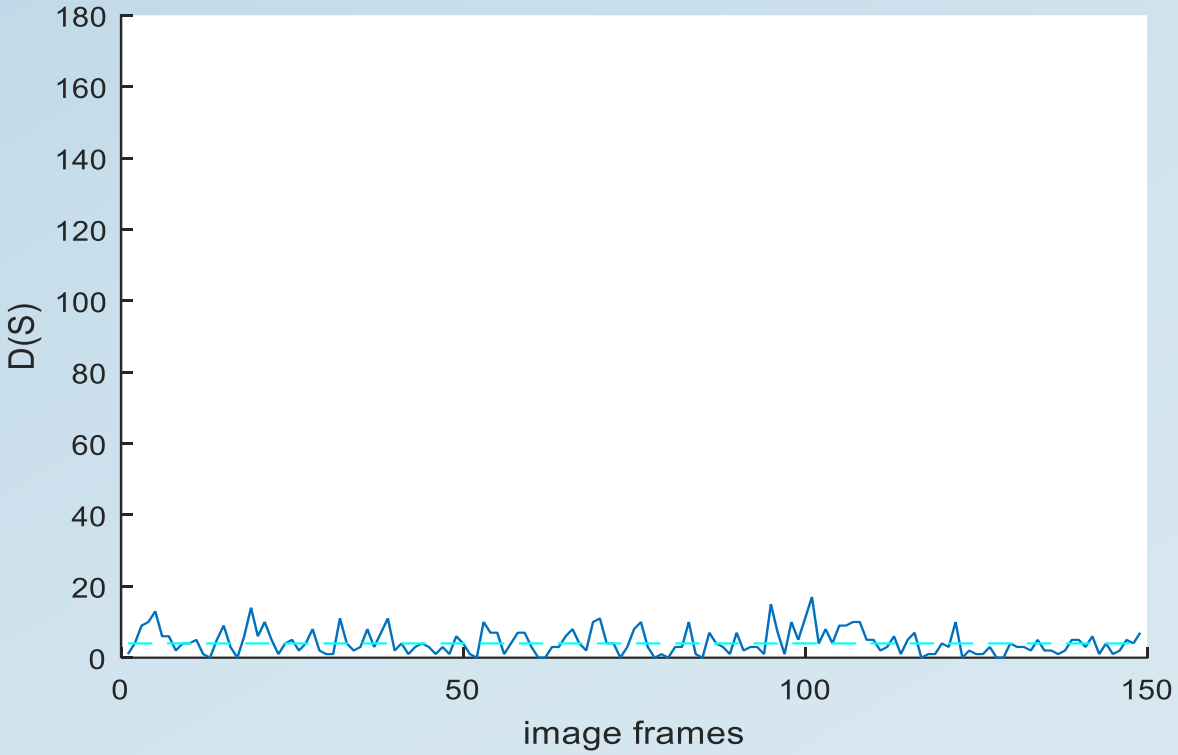
PAD Example#1

- Blink detection:

Live

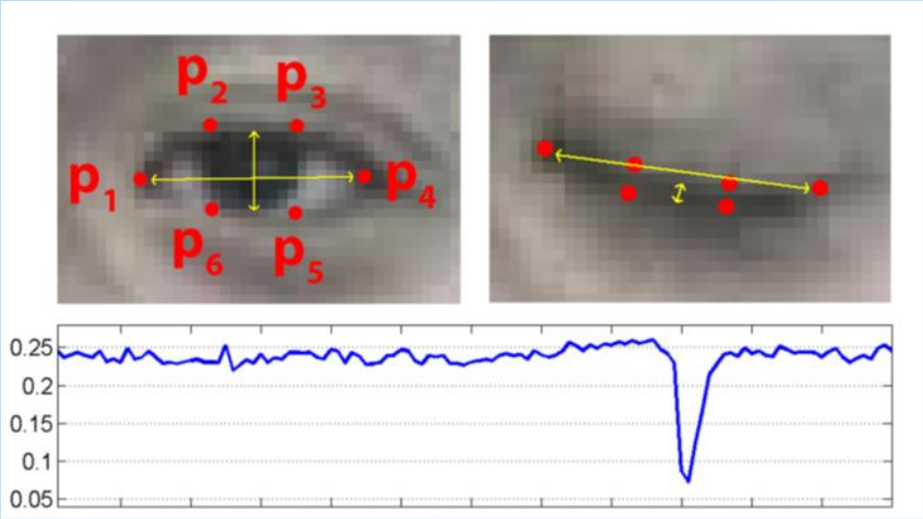


Spoofed



PAD Example#2

- Facial dynamics:
  - Resist to photo attack
  - Based on eye aspect ratio (EAR) & mouth aspect ratio (MAR)
  - Machine Learning



Kazemi V., Sullivan J., "One Millisecond Face Alignment with An Ensemble of Regression Trees," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp.1867-1874, 2014.

PAD Example#2

- Facial dynamics:

靜態

攻擊者所持的偽冒照片在感測器前保持**靜止**不動

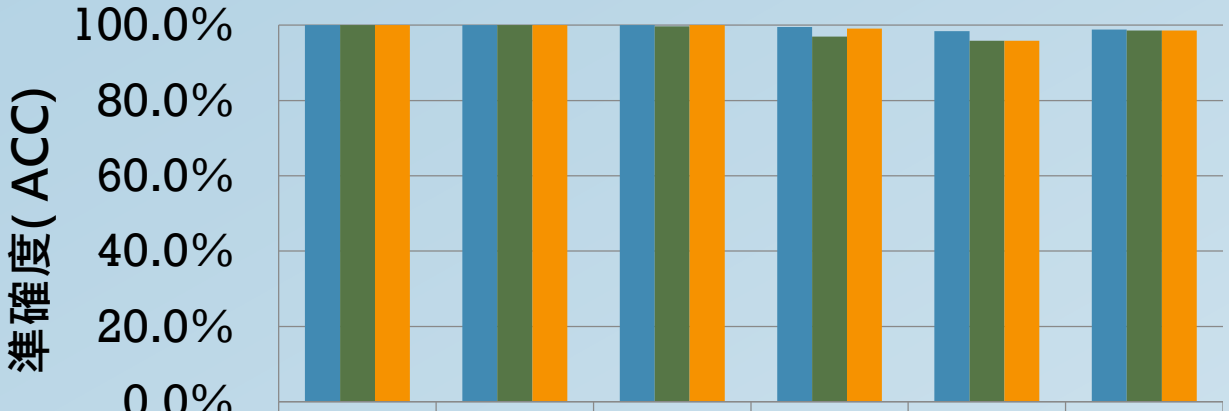
動態

攻擊者會**移動**或**扭曲**照片攻擊試圖模擬臉部動作

PAD Example#2

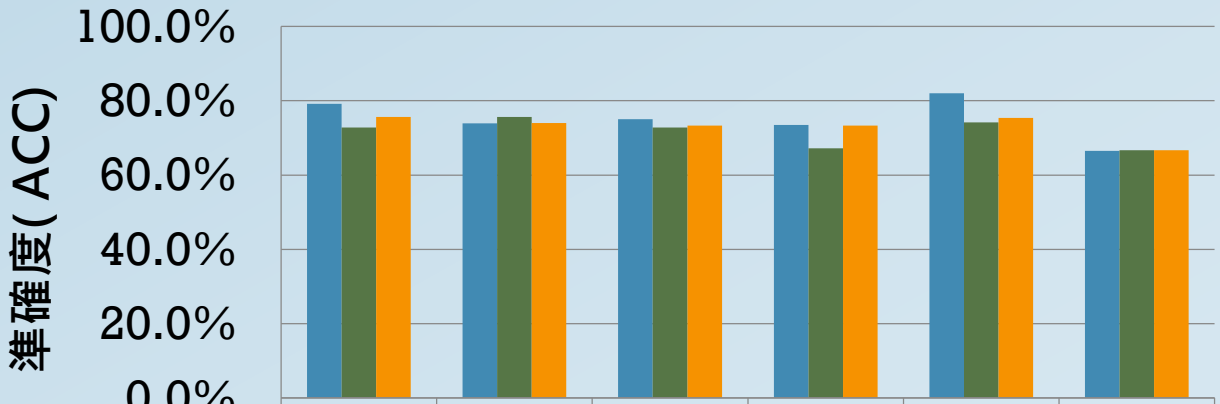
- Facial dynamics:

Static



	NB	SGD	LR	DT	KNN	SVM
EAR	100.0	100.0	100.0	99.5%	98.4%	98.8%
MAR	100.0	100.0	99.7%	97.0%	95.9%	98.6%
EAR+MAR	100.0	100.0	100.0	99.1%	95.9%	98.6%

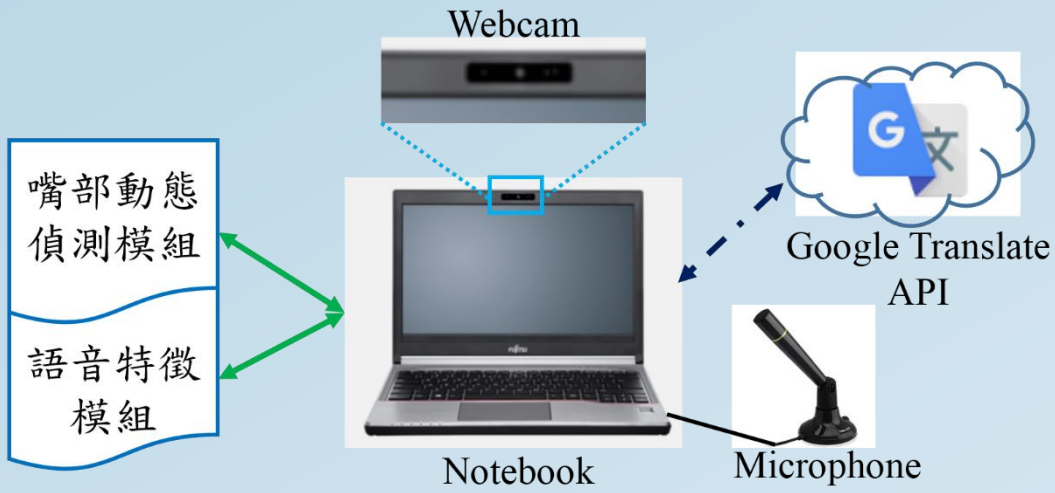
Dynamic

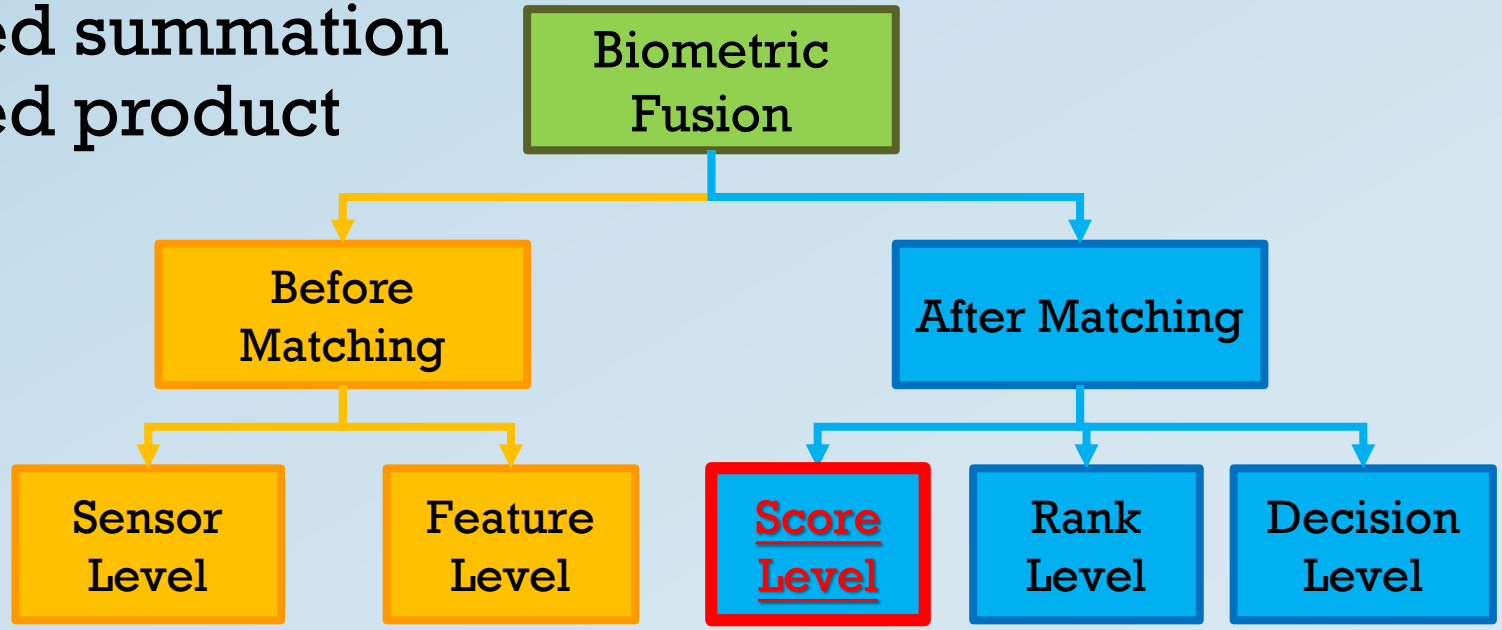


	NB	SGD	LR	DT	KNN	SVM
EAR	79.2%	73.9%	75.0%	73.5%	82.0%	66.5%
MAR	72.8%	75.6%	72.8%	67.2%	74.2%	66.7%
EAR+MAR	75.6%	74.0%	73.3%	73.3%	75.4%	66.7%

PAD Example#3

- Bi-modal:
  - Resist to video attack
  - Speech + mouth motion
  - Challenge-response
  - Score level fusion
    - Weighted summation
    - Weighted product





PAD Example#3

- Score Level Fusion:
  - Weighted Summation Fusion

$$F = w_1 s_1 + (1 - w_1) s_2$$

s_i and w_i=[0,1] are score and weight coefficient of feature *i*.

  - Weighted Product Fusion

$$F = (s_1)^{w_1} \times (s_2)^{(1-w_1)}$$

s_i and w_i=[0,1] are score and weight coefficient of feature *i*.

PAD Example#3

- 662 videos from 28 subjects
  - 494 live clips
  - 168 spoof clips with 3 types of attacks
    - (1) Staring at the camera and say nothing.
    - (2) Moving the head and say nothing.
    - (3) Saying words excludes in the predefined words bank.

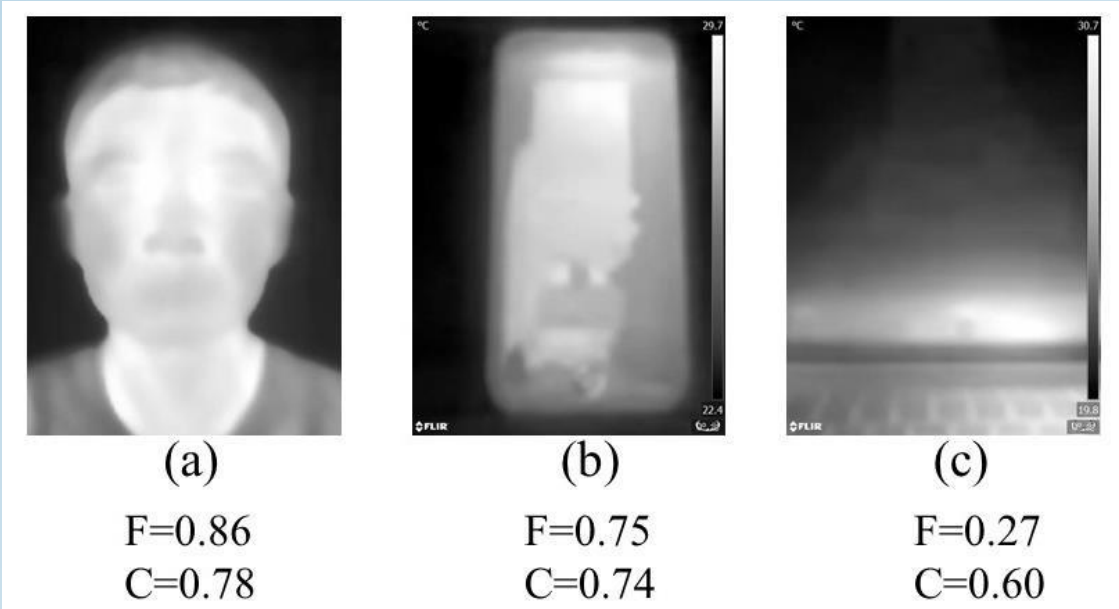
(1) (2) (3)

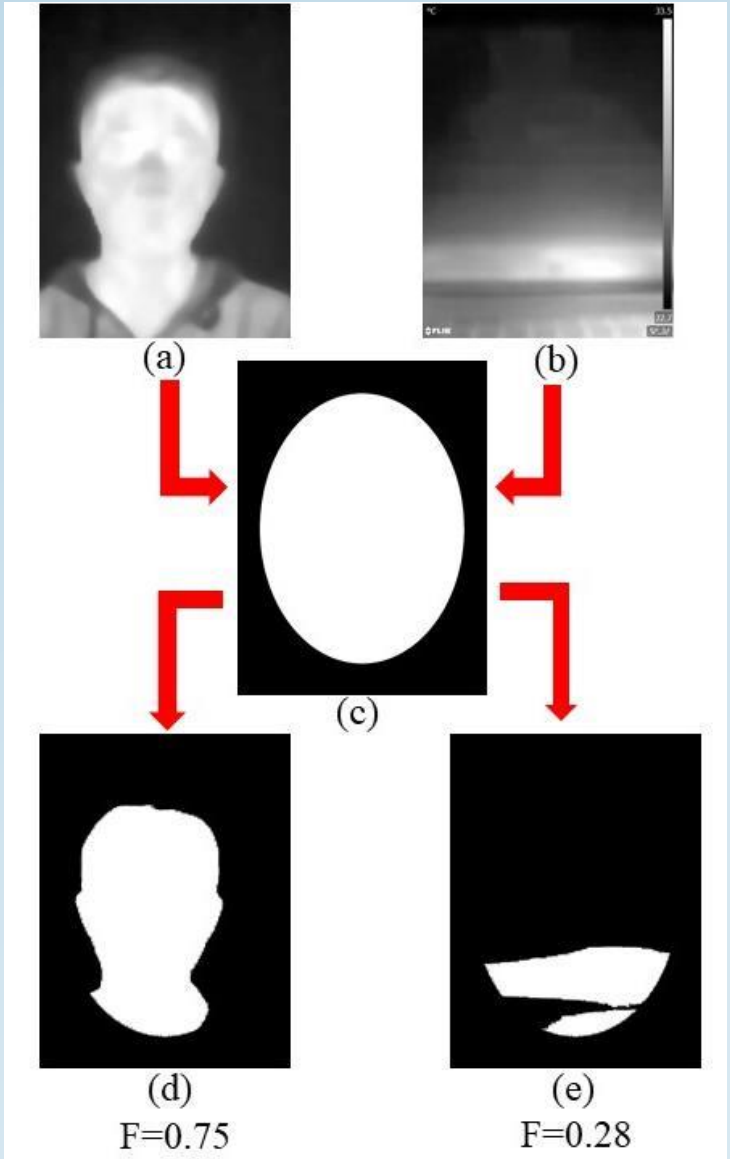
PAD Example#3

	Summation		Weighted Summation Fusion		Weighted Product Fusion	
Classifier	ACC(%)	HTER (%)	ACC(%)	HTER (%)	ACC(%)	HTER (%)
Decision Tree	93.05	5.84	94.56	4.04	91.84	5.47
Random Forests	92.75	7.34	94.86	4.62	91.84	5.47
k-nearest Neighbor	92.15	9.19	94.56	5.21	91.84	5.47
Average	92.65	7.45	**94.66**	**4.62**	91.84	5.47

PAD Example#4

- Hardware-based:
  - Resist to photo attack
  - Thermal images
  - Bit-mask + Circularity

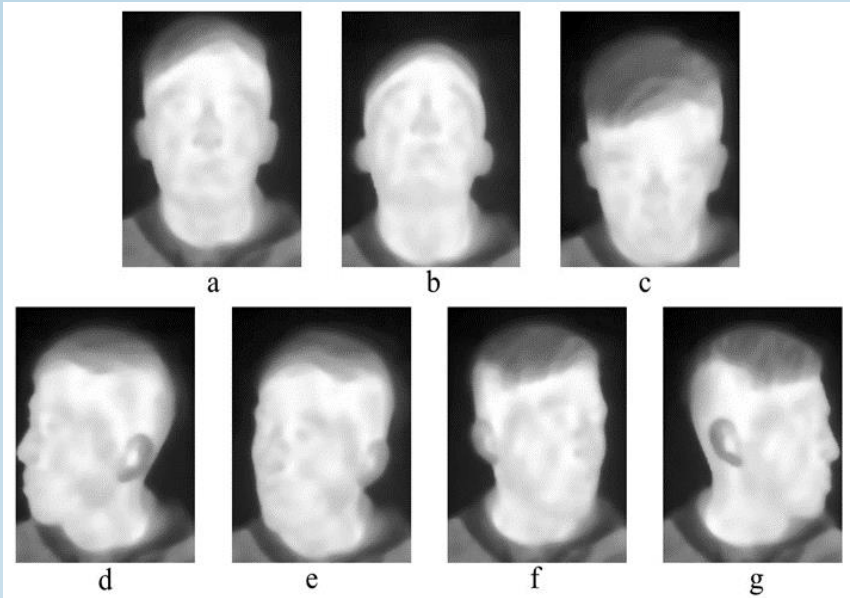


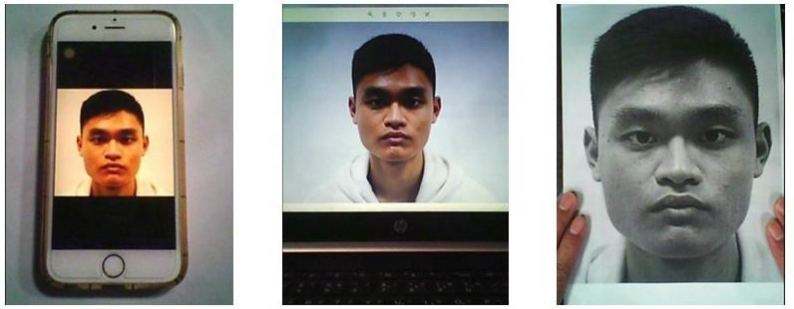


PAD Example#4

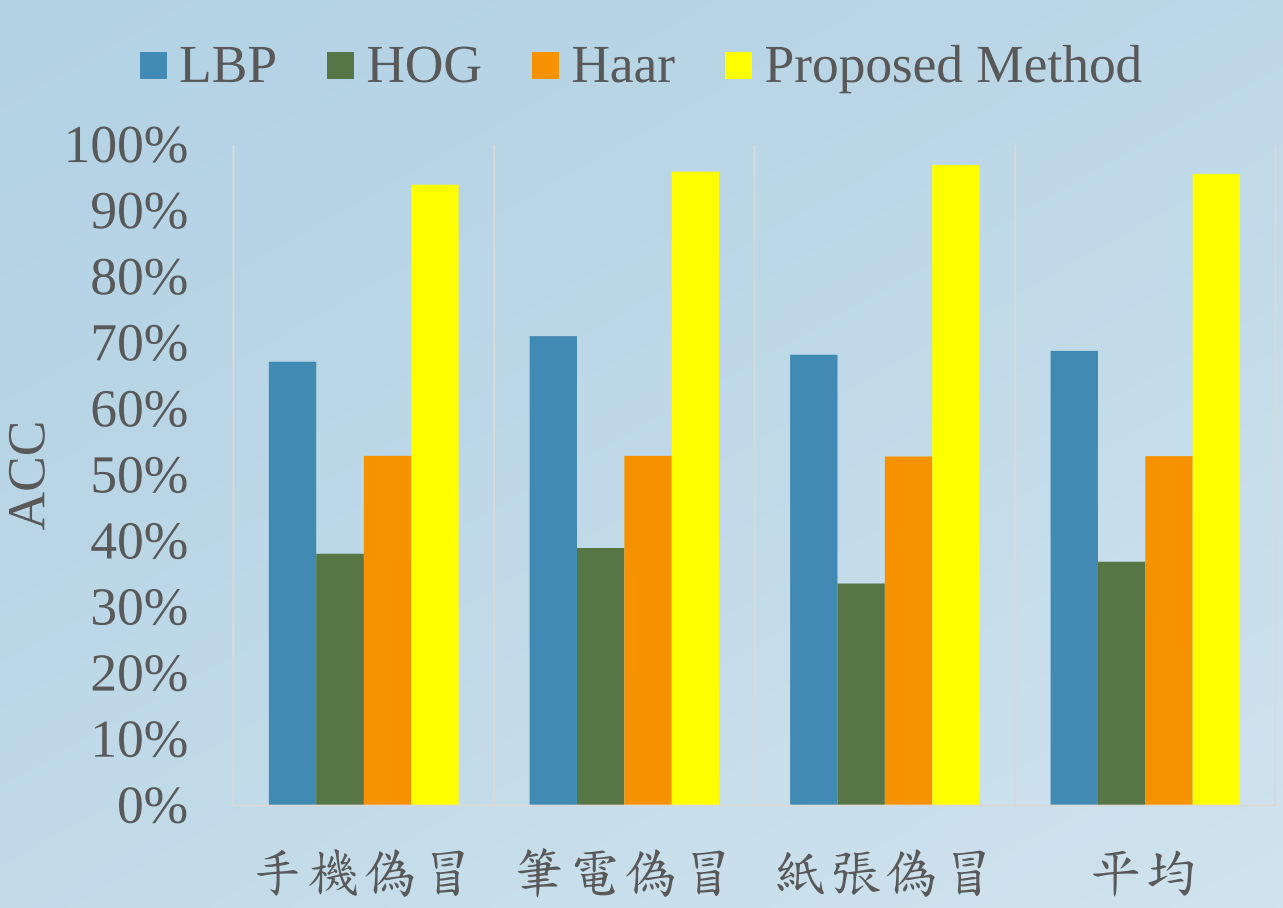
- Hardware-based:

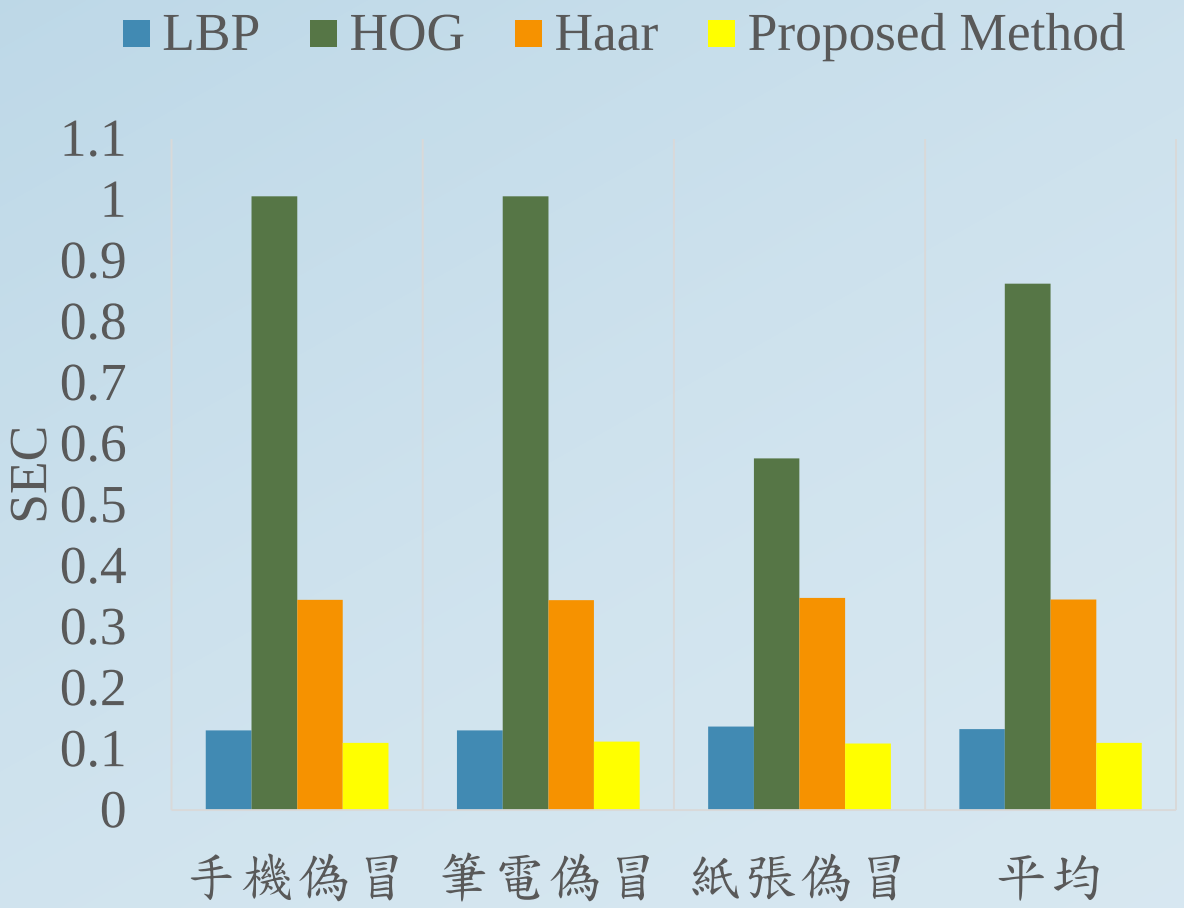
TFPA資料庫資訊表	
總數	
人臉熱影像(張)	1,379
偽冒影像(張)	591
合計	1,970





PAD Example#4





Conclusions

- Although biometric authentication devices can be susceptible to **spoof attacks**, different **anti-spoofing** techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks.

Q & A

Thank you for listening!