

# Biometric Technology Update: Match-on-Card

Yau Wei Yun

Dept. Manager, Inst. for Infocomm Research;  
Chair, Biometrics Technical Committee

Interfest 2005

# Known Issues of Biometric Passport

1. Unauthorized snooping of biometric and passport information
2. Encryption security concern when allowing worldwide interoperability for data access (can you trust all?)
3. Use of biometric data for unintended future applications.
4. Privacy concern – no user control over private info

## Mitigation:

- Does not allow biometric info to be released
- Encrypt and decrypt biometric info on card, only release the necessary passport info for border control (sufficient info for any particular application)

# Biometric & Smartcard

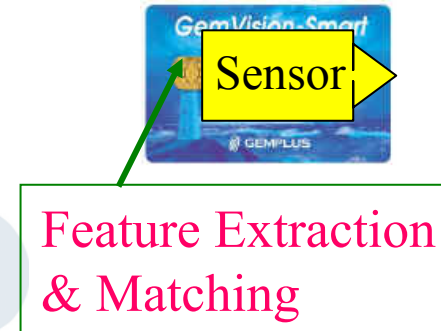
## Template-on-Card



## Match-on-Card



## System-on-Card



+ Low cost card suffices

– Dependent on integrity of token; privacy & security issues

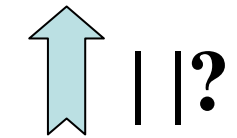
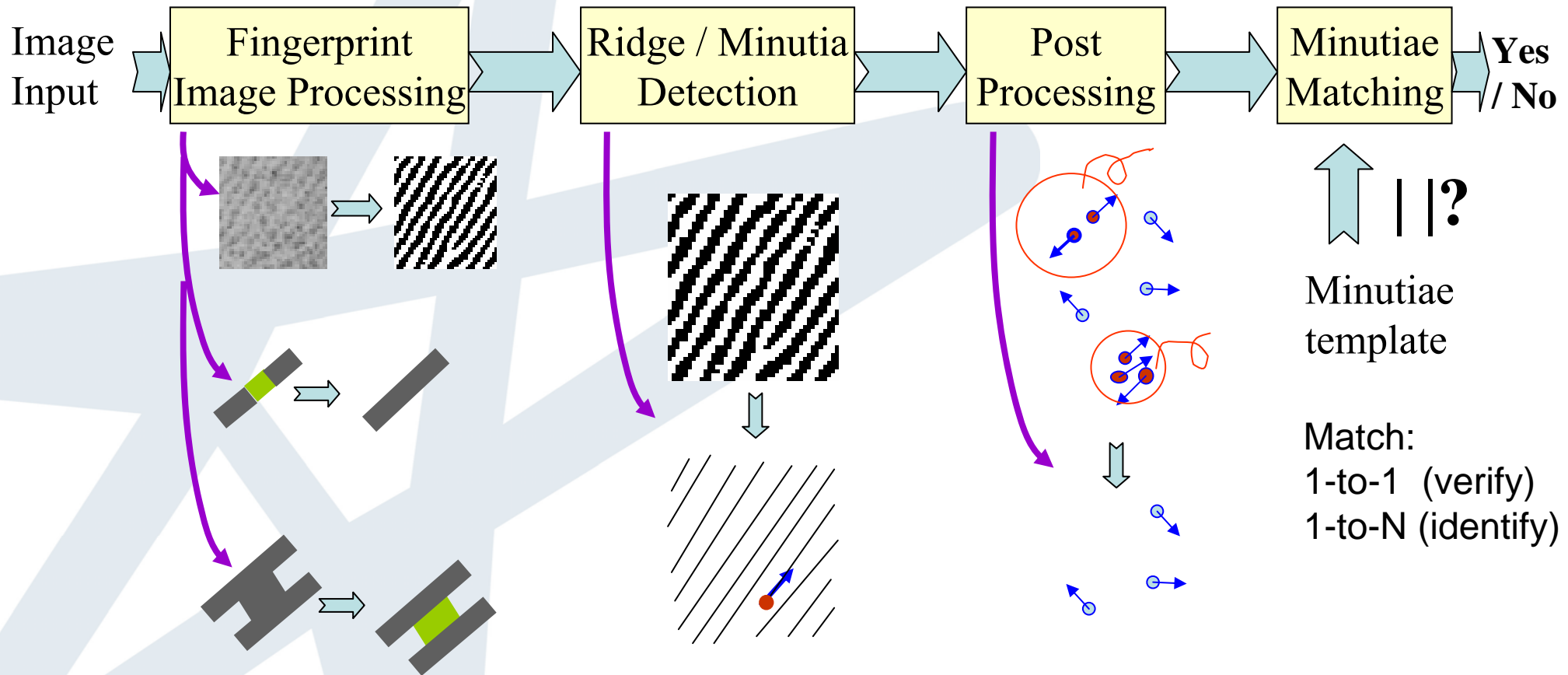
+ Biometric templates do not leave smart card. Higher security & Less privacy concern.

– Requires smart card with higher processing power and memory.

+ Biometric templates & sensors always in smart cards: Highest security, little privacy concern, interoperable, scalable, mobile.

– Requires very high end proprietary cards

# Fingerprint Recognition Process



Minutiae  
template

Match:  
1-to-1 (verify)  
1-to-N (identify)

# What you may get .....



Same finger



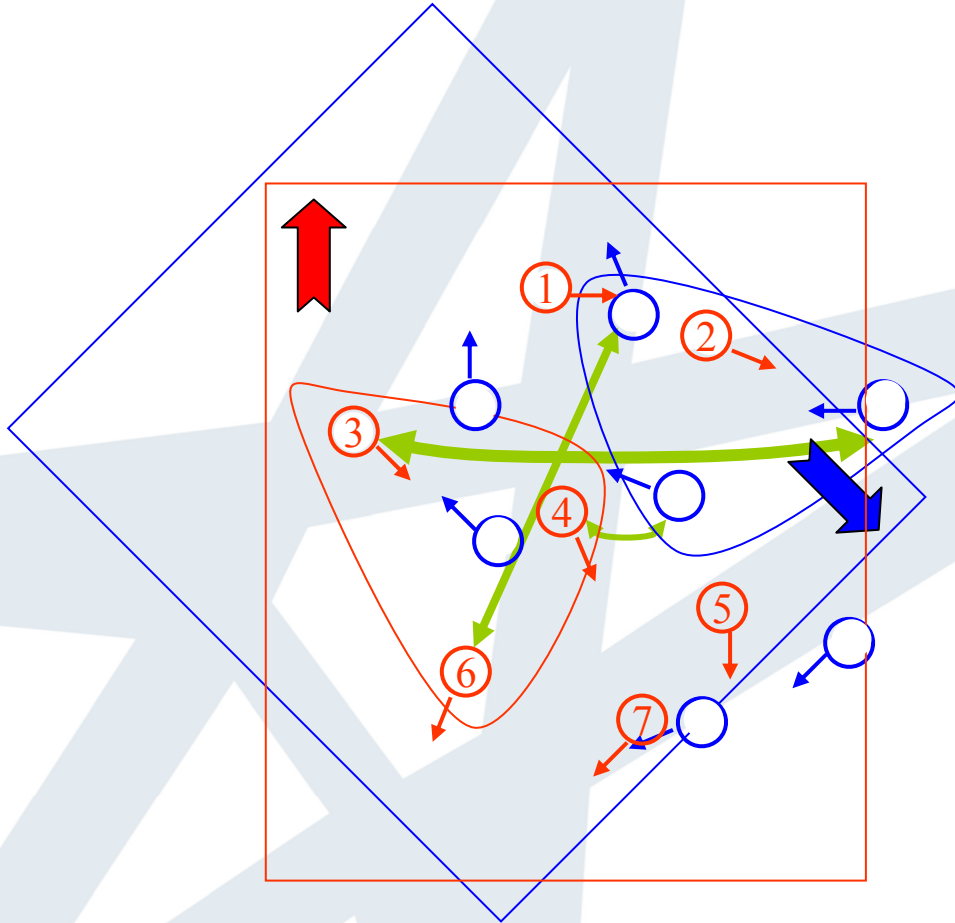
Different finger

(D. Maltoni et al. "Handbook of Fingerprint Recognition")

# Comparison of Computing Power

	<b>Smart Card</b>	<b>PC</b>
<b>Word-length</b>	16 bits	32 bits
<b>Speed</b>	24 MHz	3.4GHz
<b>Storage</b>	1 Mbytes (flash)	200 Gbytes
<b>Memory (RAM)</b>	8 Kbytes	1 Gbytes
<b>Communication speed</b>	9.6-76.8 kbps	200+ Mbps

# Minutiae Matching Idea



Unlike PIN & password which provide exact matches, fingerprint recognition provides a degree of probability or confidence that the two fingerprints are similar.

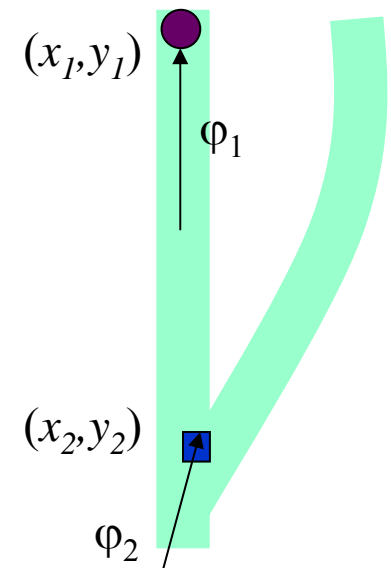
# Fingerprint Matching Process



A minutiae is described by its coordinates,  $x_k$ ,  $y_k$ , ridge direction  $\varphi_k$  ( $-\pi < \varphi_k \leq \pi$ ), and type,  $m_k$

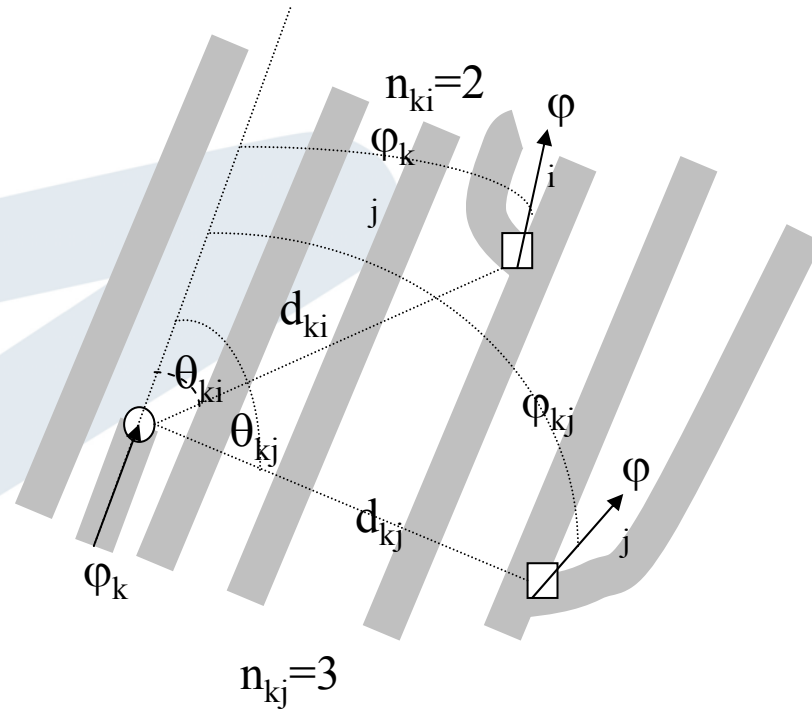
$$Fg_k = \begin{pmatrix} x_k \\ y_k \\ \varphi_k \\ m_k \end{pmatrix}$$

- Affected by position and orientation of fingerprint



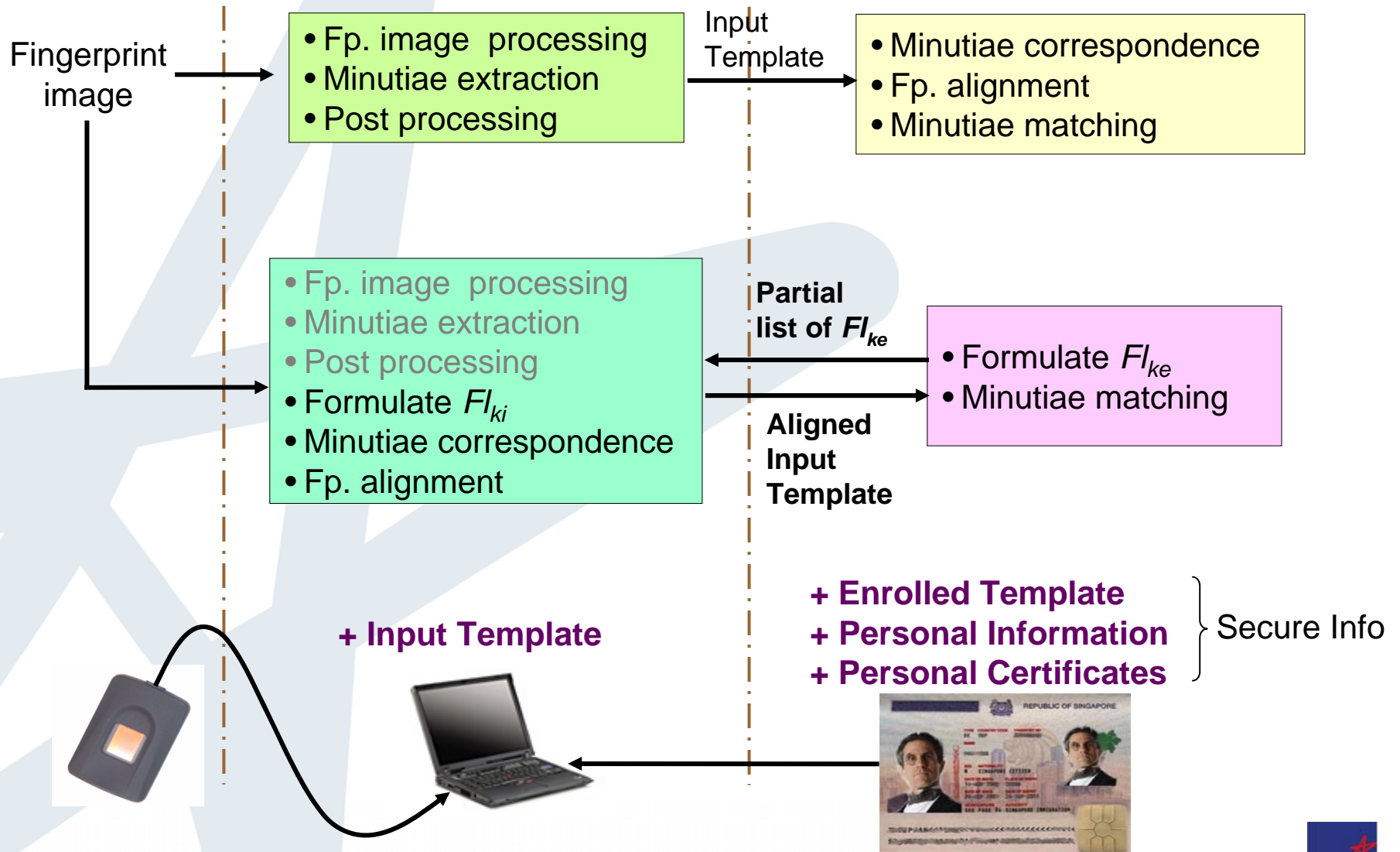
- Perform minutiae grouping (ex: into triplets) and describe each minutia in a group-based feature vector ( $Fl_k$ ).
- Position and Orientation independent

$$Fl_k = \begin{pmatrix} d_{ki} \\ d_{kj} \\ \theta_{ki} \\ \theta_{kj} \\ \varphi_{ki} \\ \varphi_{kj} \\ n_{ki} \\ n_{kj} \\ m_k \\ m_i \\ m_j \end{pmatrix}$$



- $Fl_k$  does not contain the original info and recovery of original info is not possible if not all  $Fl_k$  are available.

# Scalable Match-on-Card



# Performance Achieved

## Fingerprint Matching on Smart Card

### Scalable version:

- Sharp 16-bit Java Card running at 25MHz CPU : **0.9** to **2.2** sec.
- Oberthur 8-bit Java Card running at 30MHz CPU : **0.75** to **2.5** sec

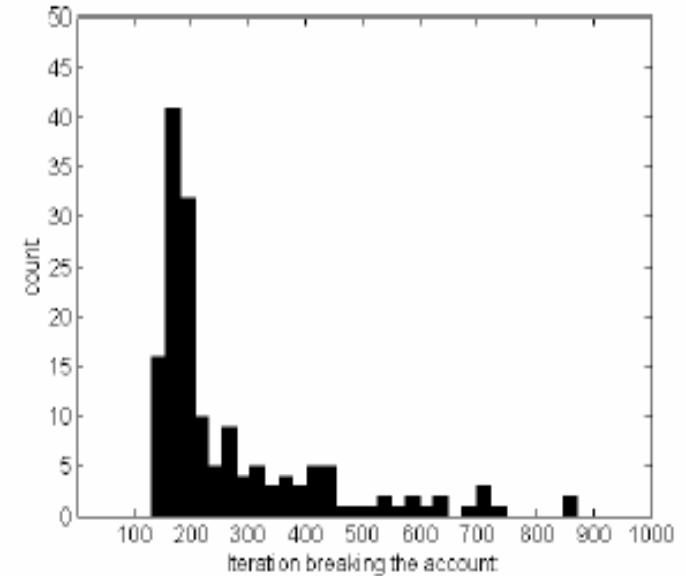
### Accuracy:

- FVC2000 ST Database: **FAR 0.001%**, **FRR < 2%**

# Reducing Vulnerabilities

## Methods of attack:

1. Hill climbing attack based on iteration with minutia template
  2. Quantized hill-climbing based on iterative manipulation of fingerprint pattern template (ex: in Fourier domain) of a biometric encryption system.
- Both attacks require:
    - a) a matching score output
    - b) large iteration (>100 iterations.Ex: U Uludag & A.K. Jain: Mean: 271 iterations, assuming FAR=0.1%)



Histogram of number of attempts at which the accounts are broken.

## Prevention by MOC:

- a) not to produce matching score, but to release secure information upon successful authentication.
- b) to limit number of trials (ex: 100), and to completely destroy the card's secure content subsequently if trials exceeded.

# Bio-Crypto-Smartcard

## Biometric feature + secret key

- Determine fingerprint feature  $\mathbf{f}$  ( $f_1, f_2, \dots, f_n$ ).
- Determine parameter  $r_i$  and random integer  $k_i$  for  $i^{\text{th}}$  feature.
- $\mathbf{K} = \{k_1, k_2, \dots, k_n\}$  is the random integer key
- Combine biometric feature and secret key using:

$$\mathbf{C} = \{c_i = f_i - r_i k_i\}_{i=1}^n$$

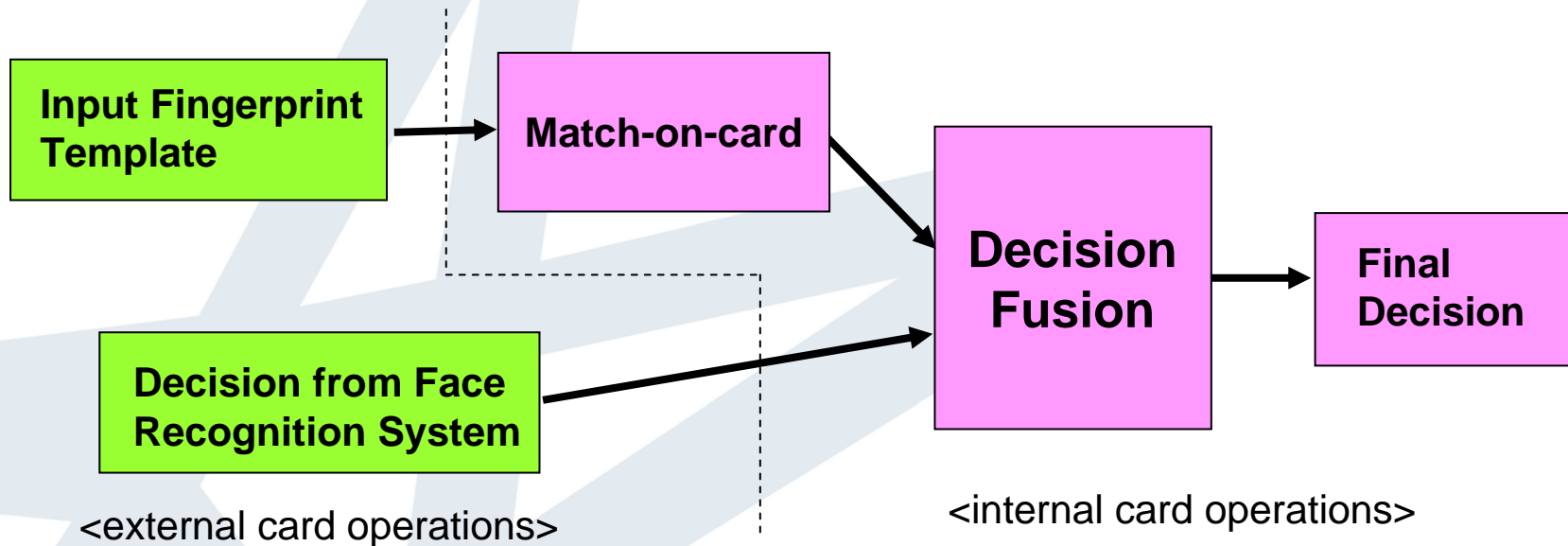
- Save  $\mathbf{C}$ ,  $\mathbf{K}$  and  $r_i$  into smartcard and discard the others
- To recover key, extract  $\mathbf{C}$  and  $r_i$  from smartcard and  $\mathbf{f}$  from user's fingerprint

$$\mathbf{K}' = \{k'_i = (f'_i - c_i) / r_i\}_{i=1}^n$$

- Authentication is successful if  $\mathbf{K}' = \mathbf{K}$
- No storage of biometric template
- Keys can be changed for various applications

# Multi-modal Fusion

Combines the decision from multiple biometric technology.



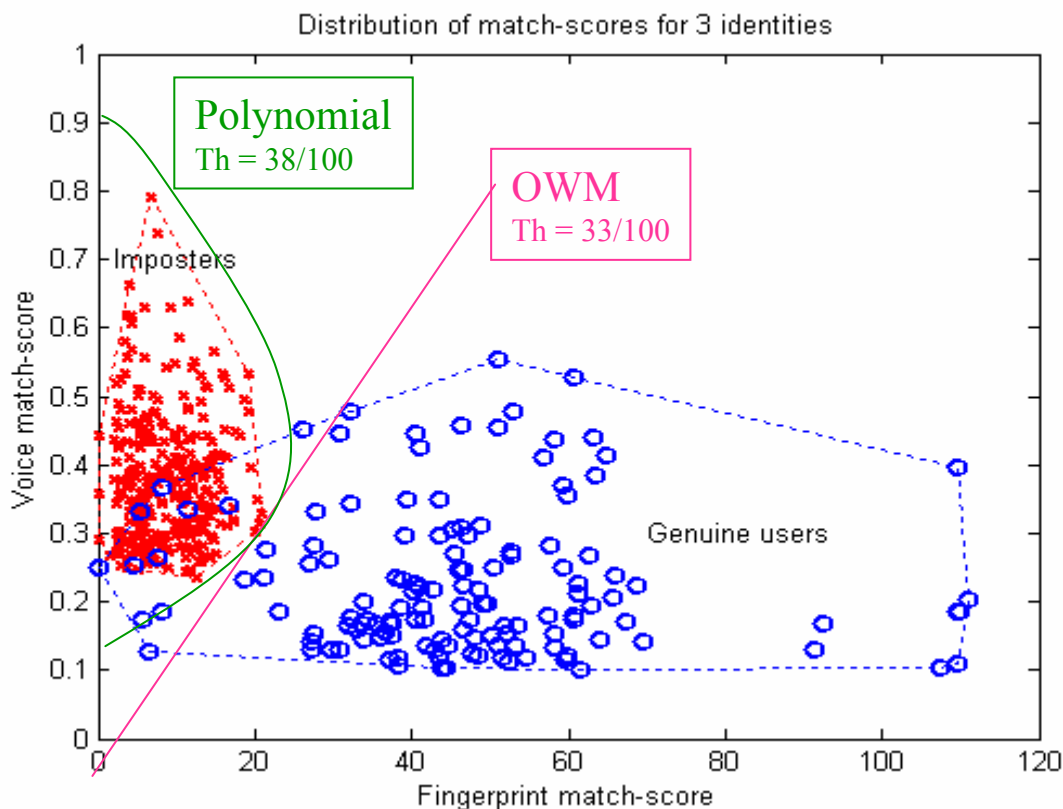
Attractive when cost of individual biometric tech is low

Projected price for large quantity:

Fingerprint module:  $\leq$  US\$5

Solid state camera module:  $\leq$  US\$10

# Critical to have good decision fusion algorithm.



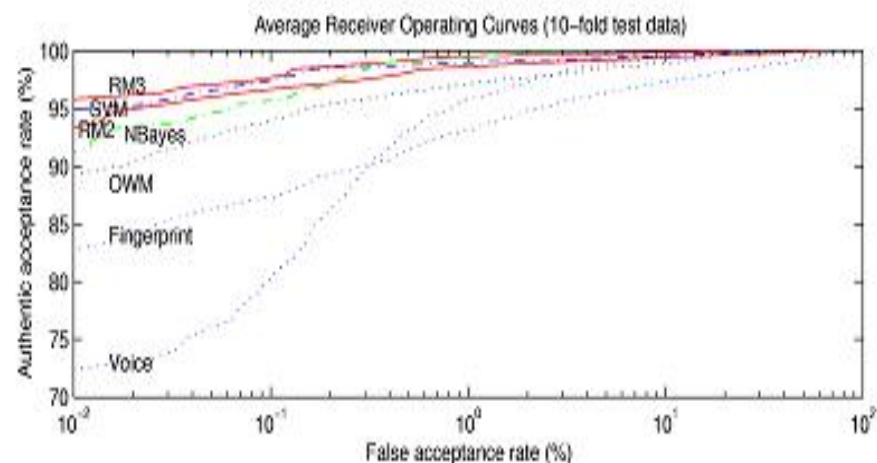
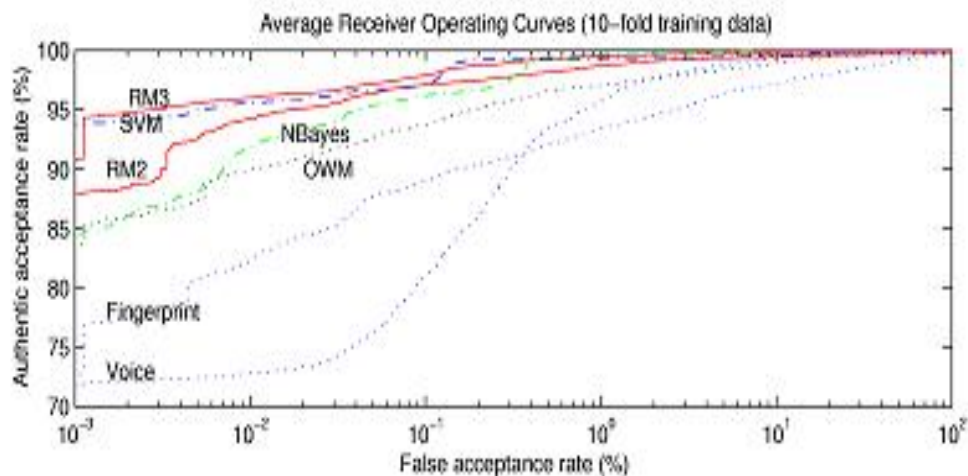
- Global fusion function
- User-specific fusion function

Separation between genuine-users and imposters for fingerprint and voice biometric

# Multi-modal Biometric Fusion

Developed a reduced multivariate polynomial algo for multi-modal biometric (data) fusion.

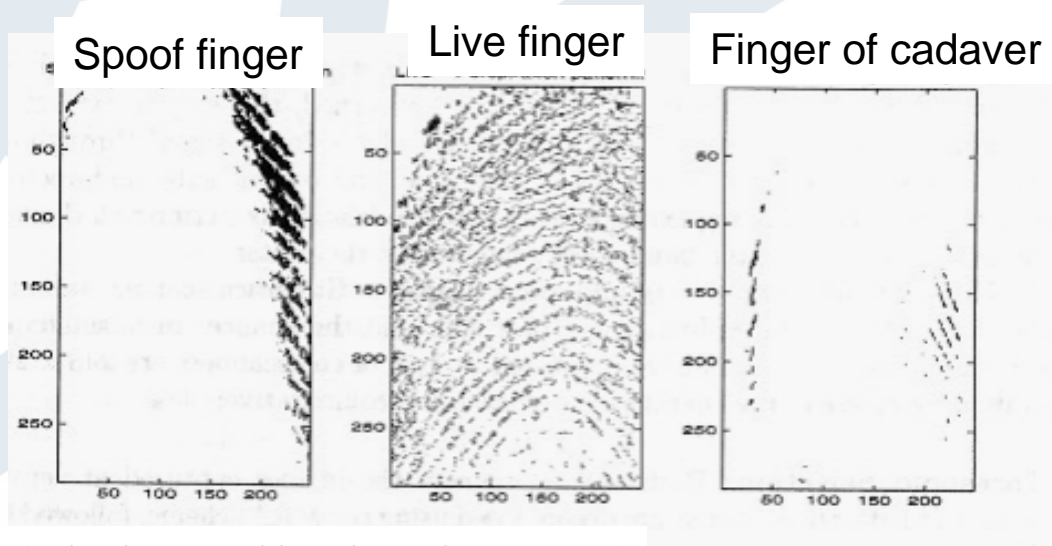
- **Simple:** low memory usage as no dimension explosion
- **Fast single step training:** linear in parameter space
- **Good classification accuracy:** better or comparable to existing popular algorithms (Neural Network, SVM, kNN ...)



# What about fake finger?

## Finger Vitality Detection

- Detect heat, optical and electrical conductivity of finger.
- Measure pulse and blood pressure
- Multiple touches (ex: tip, then touch) or multiple finger
- Detect finger perspiration and periodicity of sweat pores
- Multiple biometric fusion
- Man in-the-loop!



(Schuckers & Abhyankar, BioAW 2004)

# Conclusion

---

- Fingerprint match-on-card system is feasible for large-scale biometric application such as national ID and e-passport
- It overcomes some of the security & privacy issues facing the usual biometric system.

THANK YOU

