Biometric Authentication

My body is my password

Lecture 1

Biometrics Authentication:
Introduction

Outline

- **Why Biometrics?**
- **What about Biometrics?**
- **Biometric Applications**
- **Useful Links**

Why Biometrics?

Why Security in e-World

❑ We enter *the age of universal electronic connectivity* $\Rightarrow$ *called e-World:*

- $\Rightarrow$ *e-commerce*
- $\Rightarrow$ *e-shop*
- $\Rightarrow$ *e-phone*
- $\Rightarrow$ *e-backing*
- $\Rightarrow$ *e-purse*
- $\Rightarrow$ *e-government ……*

Why_security

❑ In an *e*-world, the more and more activities are related to INTERNET.

❑ With Internet development, there exist some troubles and problems.

- $\Rightarrow$ *Viruses*
- $\Rightarrow$ *Computer theft*
- $\Rightarrow$ *Hackers*
- $\Rightarrow$ *Unauthorized access ……*

e-Banking

Security Solutions

Why?

❑ All these problems threaten the prosperity and productivity of corporations and individuals.

⇒ Security is increasingly important.
⇒ Two approaches:
— "Make Water Clear" - "使 水 变 清"
— "Make Water Chaotic" - "把 水 搅 混"

❑ One security solution: **Authentication**

⇒ Verify message and user.

❑ In fact, there is an ever growing need to identify individuals in *e*-world.

-- *Should this person be given access to a secure system?*
-- *Does this person have authorization to perform a given transaction? ……*

User Authentication Problem

Why?

❑ Every day, questions like "Who Are You?" that are related to establishing the identity of individuals are asked *millions times*.

PROBLEM 1: (Credit Card)
Each year, billions of dollars are lost through the fraudulent use of credit cards.

PROBLEM 2: (Benefit Care)
A lot of money losses due to the abuse of health care unemployment insurance benefits and welfare systems.

PROBLEM 3: (Immigration)
Many individuals illegally enter the country each year using falsified travel documents.

User Authentication

- User authentication (identity verification)
  - Convince system of your identity
  - Before it can act on your behalf
- Sometimes also require that the computer verify its identity with the user
- User authentication: Three methods
  - What you know
  - What you have
  - What you are/do
- All then involve some validation of information supplied against a table of possible values based on users claimed identity

Know

Are/Do Have
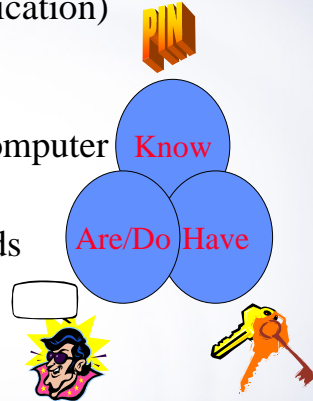
Method 1: What You Know
- Passwords or Pass-phrases

$\Rightarrow$ **Knowledge-based**
  -- **Use** "something that you know"
  -- **Examples**: password, PIN

abc0123
Passwords/PINs
What you know

- Verify identity by checking that password is correct
- More often use a one-way function, whose output cannot easily be used to find the input value
  - either takes a fixed sized input (e.g., 8 chars)
  - or accept a variable sized input to create the value
- Important that passwords are selected with care to reduce risk of exhaustive search
- Other solution: One-shot (one-time) passwords

Method 2: What You Have

⇒ **Token-based**

-- **Use** "something that you have"

-- **Examples:** credit card, smart card, keys

- Verify identity based on possession of some object, often also combined with a password
- Magnetic Card, Magnetic Key
  - possess item with required code value encoded in it
- Smart Card or Calculator
  - may interact with system
  - may require information from use
  - could be used to actively calculat
    - a time dependent password
    - a one-shot password

Keys   Cards

What you have

What Problems

❑ At the NY Times web site, about 1,000 people per week forget their passwords

❑ Common hacker tools can typically guess 30% or more of the passwords on a network
  – Some hackers claim 90% success

❑ Tedious, time-consuming, inefficient & expensive

Lost your Key ?

Forgot your Password ?
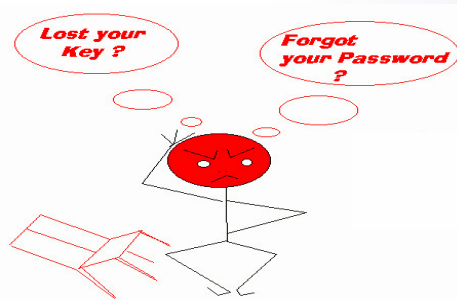
Method 3: What You Are/Do

- Verify identity based on your **physical characteristics** or **behavioural patterns**, known as biometrics **Flash**
- Characteristics used include:
  - signature (usually dynamic)
  - fingerprint
  - hand geometry
  - face or body profile
  - speech
  - retina pattern
- Comparison: Biometrics
  - More security
 - More reliable

---

What about Biometrics?

Body Language: Biometrics

❑ No two people are the same.

❑ With this in mind, we can use the methods that enable the unique characteristics of eyes, faces and voices to be converted into data keys that enhance security and convenience.

Biometrics Authentication:
Security and Privacy Concerns

❑ Biometrics can overcome some of the limitations, hence it offers *greater security and convenience* than traditional methods.

❑ In some applications, biometrics can **replace** or **supplement** the existing technology. In others, it is the only viable approach.

❑ Biometrics-based identification is emerging as the most reliable method.
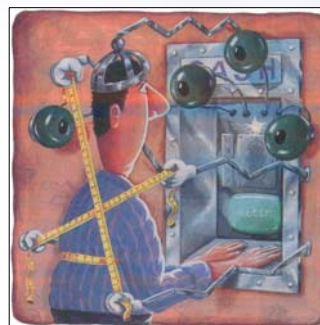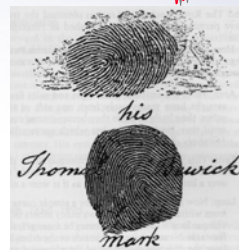
History of Biometrics

What?

- Biometrics from the worlds "Bio" and "metrics". Bio means living things. Metrics means measure.

- Currently, Biometrics stands for measuring human's features for personal identification.

- We have used biometrics more than five thousand years – face recognition

- In the late 19th century, we have used fingerprint for criminal identification.

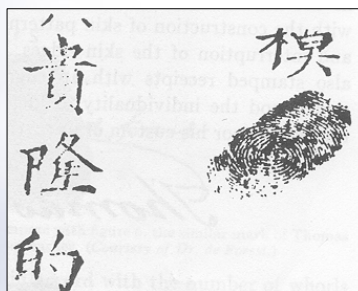- We also use signatures for government, legal and commercial transactions long time.

History of Biometrics
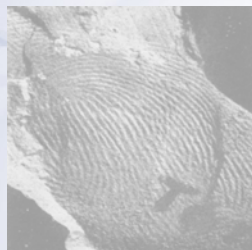
What?

Fingerprint on Palestinian lamp (400 A.D.)
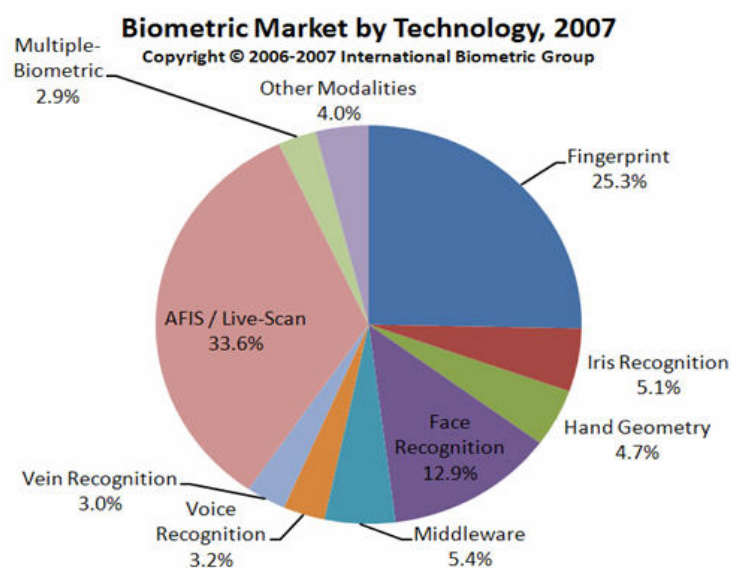
Bewick's trademark

A Chinese deed of sale (1839) signed with a fingerprint

History of Automatic Biometrics

What?

- Since 1960, we started to design automatic methods for biometrics recognition.
  - Automated Fingerprint Identification System 1960
  - Speaker Identification, *Science, News Series*, vol. 166, no. 3903, 1969.
  - Computer Recognition of Human Faces, T. Kanade, Birkhauser, Basel and Stuttgart, 1977.
  - Retinal Identification," *US Patent* No. 4109237, 1978.
  - Authentication by Keystroke Timing, Rand Report, R-256, *NSF, Rand Corp.*, 1980.
  - Automatic Signature Verification, *IEEE Trans, SMC-C* 1983
  - Iris Recognition, J. Daugman, *IEEE PAMI* 1993
  - Automated personal identification by palmprint, D. Zhang, et al., *Optical Engineering*, 1998.

Market Share

Biometric Market by Technology, 2007
Copyright © 2006-2007 International Biometric Group

Multiple-Biometric 2.9%
Other Modalities 4.0%
Fingerprint 25.3%
AFIS / Live-Scan 33.6%
Iris Recognition 5.1%
Hand Geometry 4.7%
Face Recognition 12.9%
Vein Recognition 3.0%
Voice Recognition 3.2%
Middleware 5.4%

Fingerprint Recognition

❑ *Current State*

↖ *Stability and uniqueness:* Based on a century of examination, it is estimated that the chance of two people, including twin, having the same print is less than one on a billion.

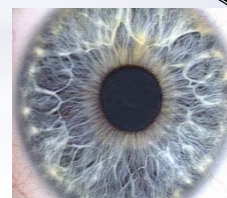↖ Fingerprint identification is the most widespread application in biometrics. First commercial system in 1971.

❑ *Feature Set*

Minutiae - Endpoint & junction of print ridges, and position, direction & relation between them

Singular Point

Iris Verification

❑ *Current State*

↖ Analyze features found in the colored ring of tissue that surrounds the pupil, use a fairly conventional camera element and require no close contact between the user and the reader.

↖ As a high accuracy biometrics, iris has more details than a fingerprint. Highly detailed and unique texture will remain stable over decades of life.

❑ *Feature Set*

Textures with striations, contraction furrows, pits, collagenous fibers, filament, crypts (darkened areas resembling excavations), serpentine vasculature, rings, and freckles

Face Recognition

❑ *Current State*

↖ Face is the most common biometrics. Using the whole face for automatic identification is a complex task because its appearance is constantly changing.

↖ One effective approach may employ rule-based logic and a neural network for the image classification process. The first face system is introduced in 1992.

❑ *Feature Set*

Facial geometry -

Size of eye, distance from eye to mouth, middle of mouth to chin, side of eye to cheek, size of mouth, radius vectors and feature points

---

3D Hand Geometry   Hand

❑ *Current State*

-- It is a simple biometric, which features are obtained by 3D shape. Analysis is based on measurement and comparison of geometries. Usually a verification system with a smart card.

-- As a biometric application, one hand geometry identification device is commercially available in 1994.

❑ *Feature Set*

Geometric feature - shape and characteristics of finger/hand like size of palm, finger length, width, area, thick and their relationship between fingers etc
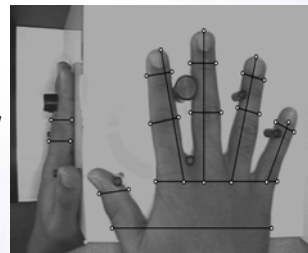
Voice Identification

Voice

❑ *Current State*

Voice

↖ Utilizes the distinctive aspects of the voice to verify the identity of an individual. The least invasive of the biometric recognition technologies and the most natural to use is speech system.

↖ Have the most potential for growth, because it requires no new hardware — most PCs already contain a microphone.

↖ Just say a phrase, about a second long - any language or dialect - chosen by the user. A typical case is AT&T Smart Card.

❑ *Feature Set*

Cadence, frequency, pitch & tone of an individual's voice.

Lecture 1 - 23

Signature Recognition

Signature

❑ *Current State*

Signature

↖ Analyzes the way a user signs his/her name to measures the physical activity of signing.

↖ It should distinguish between person's habitual parts and those that vary with almost every signing.

↖ Two methods: **on-line** & **off-line**, where wired pens & sensitive tables are needed for on-line signature.

❑ *Feature Set*

Behavioral components of the signature, such as shape, velocity, stroke order, off-tablet motion, pen pressure and timing information captured during the act of signing, etc.
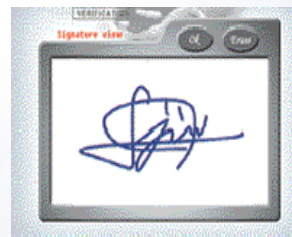
Lecture 1 - 24

Why New Biometrics in the Biometric Family?

Why?

❑ Two kinds of biometrics

<u>Physical Biometrics</u>
Fingerprint, face, iris, etc.

<u>Behavioral Biometrics</u>
Voice, signature, etc.

⇒ *Why do we need new one?*

❑ Two main reasons:

-- Current biometric limitations

-- Selection of biometrics: Application dependent

Retina

Retina

- Compared with iris, Retina analyzes the layer of blood vessels situated at the back of the eye.
- The pattern of the blood vessels is unique in each individual
- Extremely accurate for identification
- By using a low-intensity light source through an optical coupler to scan the unique patterns of the retina.
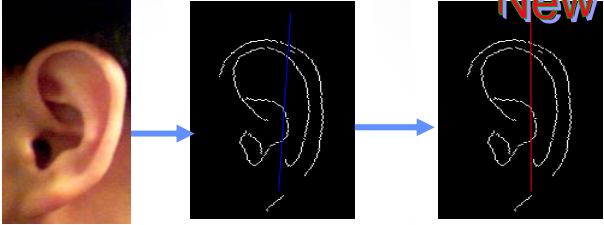

Iris   Optic Nerve   Lens   Fovea   Cornea   Retina
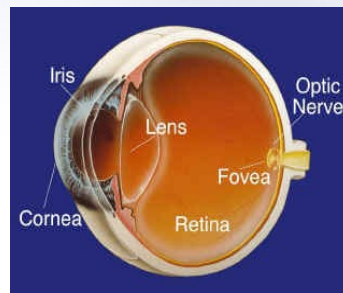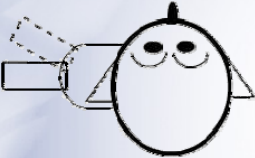
Twin Retina Comparison
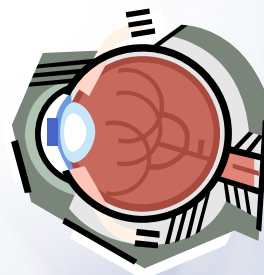
Ear

Gallery image Day variation Lighting variation Pose variation

New

Edge Detection   **Image Rotation**

❑ *Feature Set*

Ear geometry and Textures

Ellipse Model   **Mask Design**   **Complete Mask**

Thermogram

- Medium accuracy
  - Non-intrusive
- View-dependent
- Depends heavily on factors like emotion of the subject, body temperature.
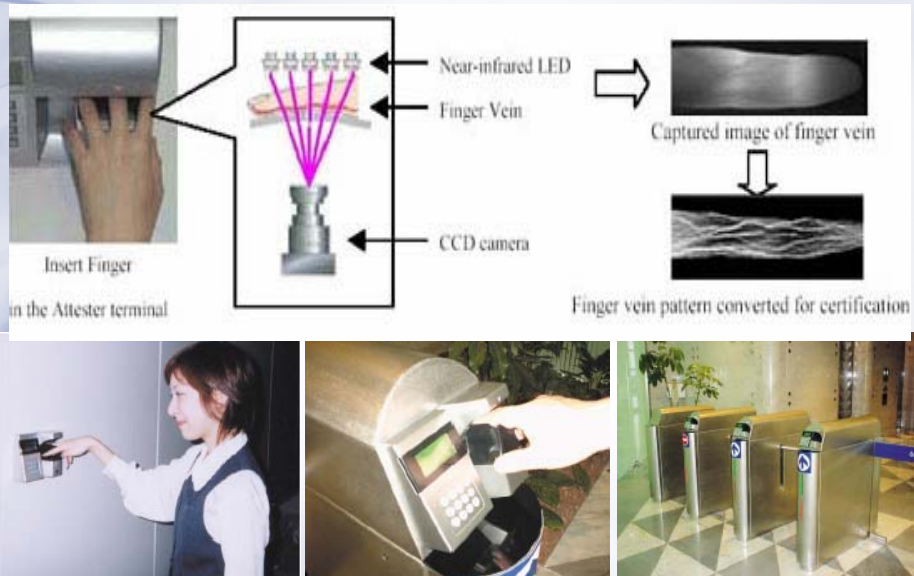
Finger Vein Patterns

❑ The system is developed by Japan and the access control is used in Hitachi Tower (2003) *

Finger Vein Scanner

Near-infrared LED

Finger Vein

CCD camera

Insert Finger

in the Attester terminal

Captured image of finger vein

Finger vein pattern converted for certification
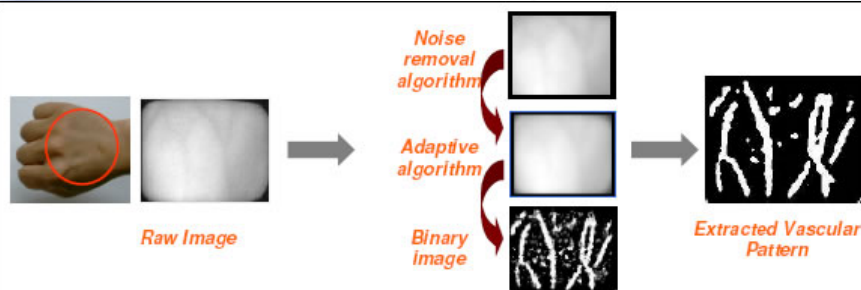
Hand Back Vein

❑ Korea designed the vein print identification system, which uses infrared photography.

Noise removal algorithm

Adaptive algorithm

Binary image

Raw Image

Extracted Vascular Pattern

Lip print *
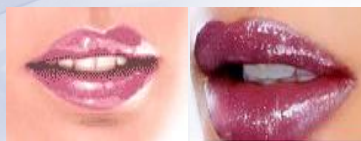
❑ Using histogram equalization to enhance the images

❑ Apply multi-resolution analysis to the enhanced images.

❑ Distance-based matching.
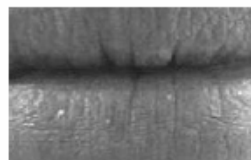
(a)　(b)
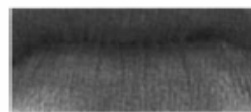
(c)　(d)

Nailbed

❑ *The system is developed by AIM Technology Inc.

OCT is an amplitude-based detection system that uses interference heterodyne, which detects the part of the back-scattered light energy that is coherent with the reference beam.

Briefringent cell is a special layer of skin cell which lines on the top of the finger nailbed

reflected probe

briefringent cell layer

nailbed

nail plate   nail bed

Light Source

Fingernail or Naliplate

Nailbed

Dental Biometrics

Incisors
Canine
Molars

(a)   (b)   (c)

(d)   (e)

Body Odor

Odor identification and e-nose

THE SWEET SMELL OF SUCCESS

NO-BO
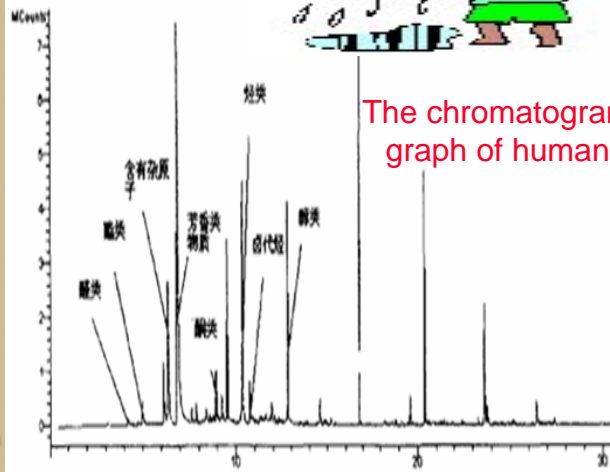
The chromatogram graph of human

Gait Biometrics

❑ **UK and CAS's projects**

Unwrapping by contour following

(x_i, y_i)

(x_c, y_c)

Im

Re
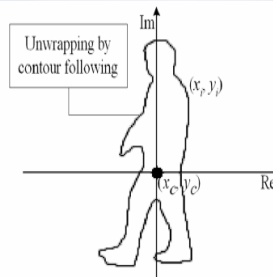
Flash
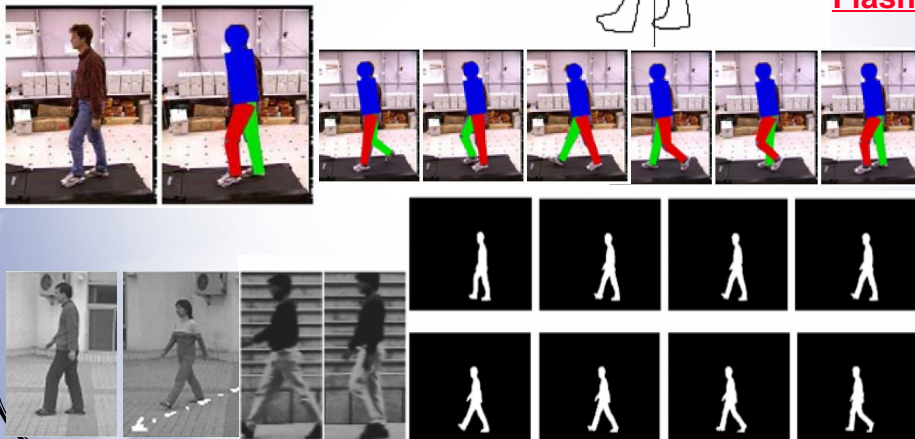
Blood Pulse / Cardiac Pulse

(http://perso.wanadoo.fr/fingerchip/ biometrics/types/cardiac.htm)

Palm Vein Biometrics

❑ **Fujitsu in Japan shows this product**
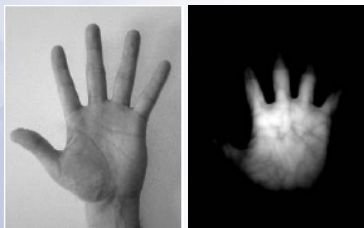
Contactless palm vein recognition unit
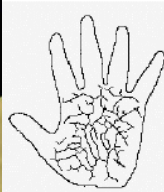
Infrared image

Vein and hand contour

Palm Vein Biometrics

❑ A new technology that uses infrared scanners to snap a digital picture of the inside of a person's hand. LiveGrip technology analyzes highly unique internal features of the human hand such as veins, arteries and fatty tissues.

(http://www.biometricwatch.com/Technologies/LiveGrip_recognition/livegrip.htm)

Keystroke Biometrics
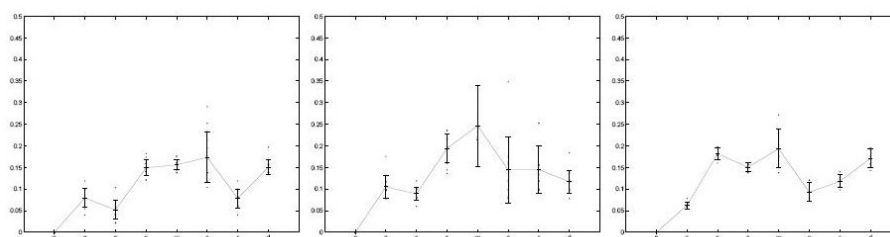
Latencies between keystrokes when writing word "**password**" by three different persons. The word was written several times. The lines represent average latencies and error-bars represent standard deviations.
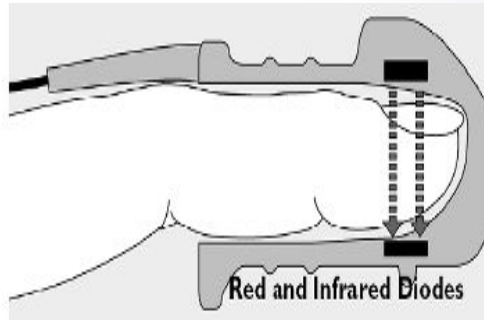
Possible measurements
Latency between consecutive keystrokes
Duration of the keystroke, hold-time
Overall typing speed
Frequency of errors
The habit of using additional keys
The force used when hitting keys

Palmprint Biometrics

❑ *History*

- Palmprint explanation from Chinese Hand Book for fortune telling had been exited over a few thousand years.
- Some useful knowledge about palmprints such as principal lines have been well-defined.
- Some policemen have used palmprints in their inspection for a long time since they are stable physical characteristics.
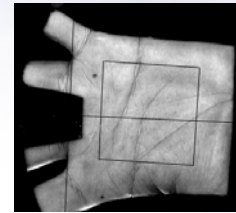
❑ *New Biometrics*

Automated palmprint authentication technology has been developed since 1996 – First research paper (1998); First palmprint identification prototype (2000) and First research book (2004).

Other Biometrics

- **Gesture**
  - Behaviors features from a sequence of images. Not contact, but low accuracy.
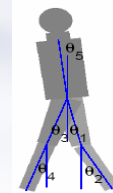
- **DNA**
  - Cannot separate identical twins and easy steal from other's DNA.

Features used by Nakajima

- **Footprint**
  - Inconvenience to capture the data and no high accuracy.

Normalized foot for template matching

- **Footstep**

Location of sensor

human foot

floor

MAT sensor

Shoe sensor
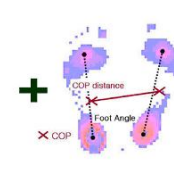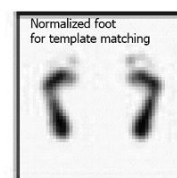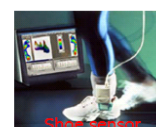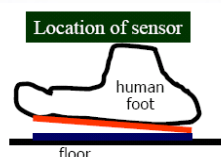
Multi-Biometrics

- Limitations of using a single biometric
  - FTE (~4% of fingerprints are of poor quality)
  - Noise in sensed data (e.g., voice altered by cold)
  - Lack of permanence (time variant)
  - Easier to spoof (circumvention)
  - May not meet FAR/FRR requirements

- Multi-biometrics: Use of multiple biometric traits to identify an individual

- Integrates multiple biometric authentication technologies
  - Uses multiple biometric features ⟹ Improves accuracy
  - Provides multiple biometric methods ⟹ Improves usability, availability, acceptability

---
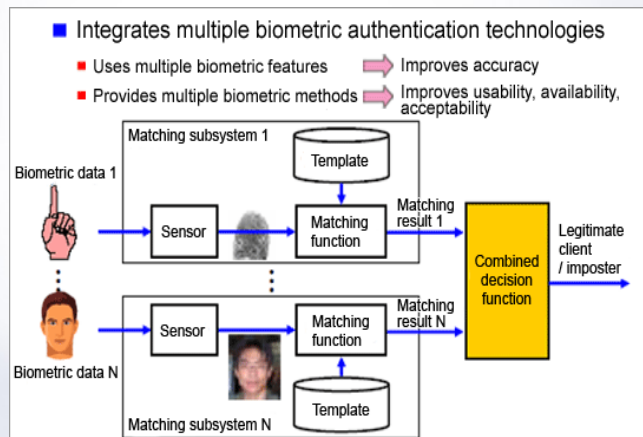
Sample: Multimodal Biometrics

BioID combines face, voice and lip movement recognition - static and dynamic features. It can be implemented whenever persons must be clearly identified.

True multimodality with BioID.

Facial features   Voice/Speaker   Lip movement
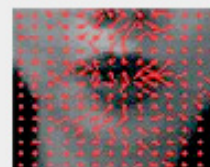
Simultaneous non-intrusive analysis. You just need to be.

3D Biometrics

❑ TBS Announces First Touchless, 3D Live-Scan Fingerprint System

http://www.send2press.com/newswire/2005-04-0405-008.shtml
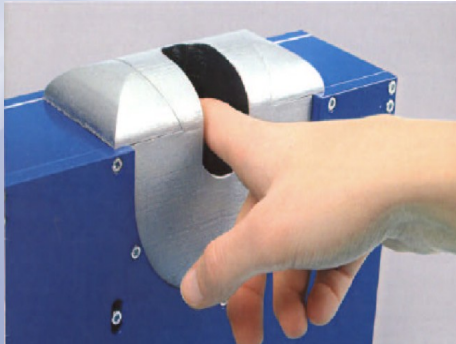
Biometric Applications

Taxonomy of Biometrics Applications

Applications

Biometrics Systems

Personal Authentication	Medical Diagnosis	Future Expectation	Ethnology Exploration
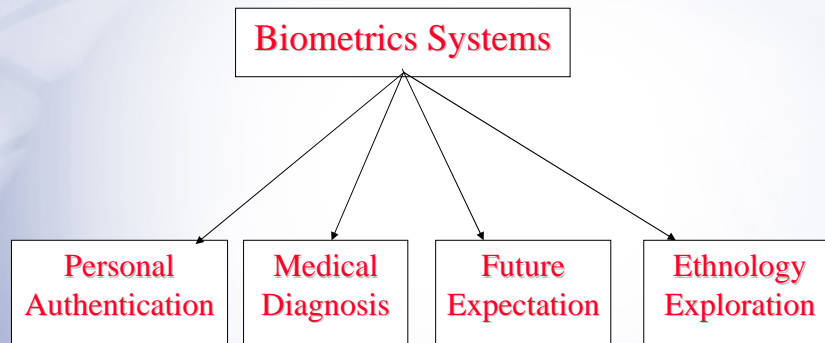
Taxonomy by Application Type

Biometric Applications

Biometrics

Four general classes:

- **Access (Cooperative, known subject)**
  - Logical Access (Access to computer networks, systems, or files)
  - Physical Access (access to physical places or resources)
- **Transaction Logging**
- **Surveillance (Non-cooperative, known subject)**
- **Forensics (Non-cooperative or unknown subject)**

* There are two types of identification system. The first one can reject unknown user. The second one only return a userID, whose feature is the most similar to the input features.

- The first approach normally uses for commercial applications
- The second approach normally uses for forensic applications

Selecting Biometrics Technology

Applications

- Selection of biometrics technology: **Application dependent**
- Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters

Two kinds of Criteria

User Criteria	Technology Criteria
1. **Effort** • How much time and effort is required on the part of the user. 2. **Intrusiveness** • How intrusive the users perceives the system to be.	1. **Cost** • Cost of hardware capture device 2. **Accuracy** • How well the system identifies individuals

---

Issues to Consider

Applications

1. Size of user group.
2. Place of use and mobility of user.
3. Ease of use & user training.
4. Error incidence (age, environment, health).
5. Security & Accuracy requirement.
6. User acceptance, privacy & anonymity.
7. Long term stability (mature tech, standard, support).
8. Cost –
   - Research & evaluation
   - Hardware & Software
   - Installation & testing
   - User education & productivity
   - Exception handling for those who can't use
   - Maintenance

Applications

Factors for Choosing Biometrics

- **Distinguished trait**
  — Is the trait being measured unique?
  — i.e. Fingerprints - 100 years of history, well accepted
  — Height and weight - not very unique, subject to change

- **Easy to sample**
  — Time needed to collect a sample
  — User acceptance: face scan is good, but blood sample is bad
  — Cost for sampling equipment

- **Low system cost**
  — Total cost of purchasing equipment, enrolling users, etc

- **Bottom Line**
  — Fast and accurate, low-cost, and easy to use.

Biometrics: A New Era in Security

- ❑ Google: over 5 millions items
- ❑ Yahoo: around 45 millions items

Annual Biometric Industry Revenues, 2007-2012 ($m USD)
Copyright © 2006-2007 International Biometric Group

Year	Revenue
2007	3012.6
2008	3836.2
2009	4634.3
2010	5633.9
2011	6553.8
2012	7407.7
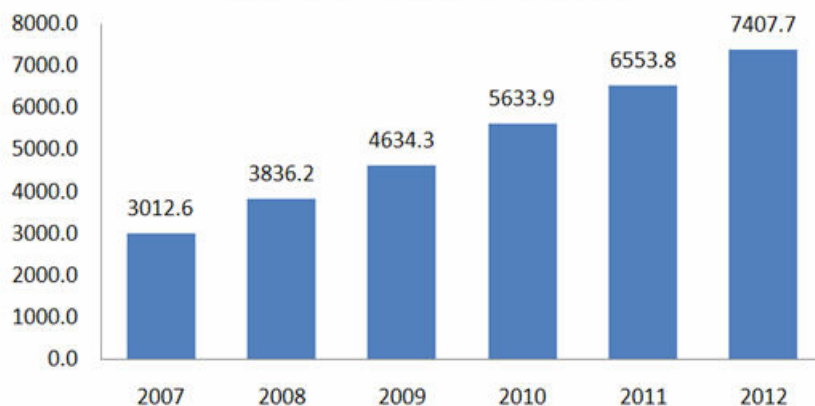
Example: Cogent System

❑ Cogent Systems is a leading provider of Automated Fingerprint Identification Systems (AFIS) and biometric access control solutions to governments, law enforcement agencies and commercial customers worldwide (http://www.cogentsystems.com/)

"Cogent has the most technically advanced products available today..."
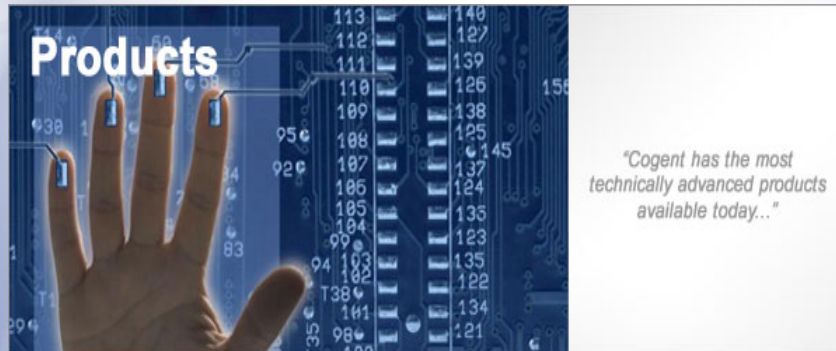
Biometrics Applications

Applications

Forensic	Government	Commercial
Corpse Identification	National ID Card Biometric Passport	ATM Internet Banking
Criminal Investigation	Driver's License Voter Registration	Access Control Computer Login
Parenthood Determination	Welfare Disbursement	Cell Phone
Missing Children	Border Crossing	E-Commerce Smart Card

Biometrics Applications

Applications

Biometrics	Applications	Summary of Application
Dental	Recognition	Forensics
DNA	Recognition	Forensics, medicine, genetics
Fingerprint	Recognition/ Verification	Immigration & naturalization, welfare distribution, military identification, forensics, access control
Face	Recognition/ Verification	Suspect description & identification, missing persons, licenses, credit card, welfare distribution
Hand	Verification	Access control, immigration and naturalization, services distribution
Signature	Recognition/ Verification	Signature verification, identification from handwriting
Iris	Verification	Access control
Voice	Recognition/ Verification	Speaker verification, phone service, speaker verification, access control

---

Biometrics in Banking

Application

Banking Services

Biometrics

Bankbook

Credit Card

Telephone Banking

Intelnet Banking

Cheque

Safe Deposit Box

Face

Hand/Finger

IRIS

Fingerprint

Palm print

Voice

Signature
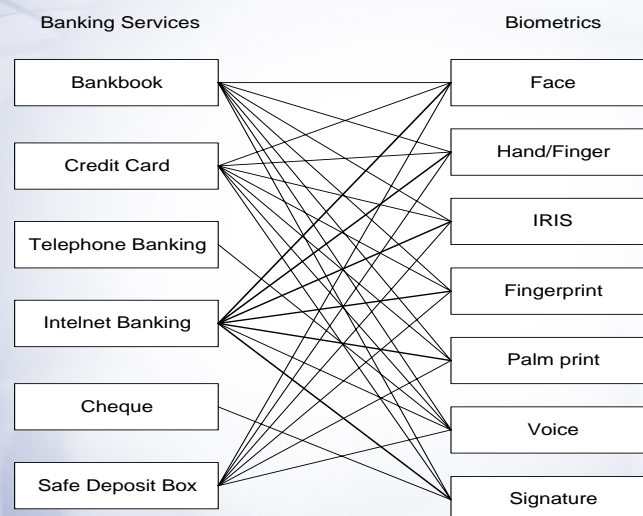
Current Real Applications

BenGurion Airport - Hand Geometry

FacePass - Face Verification

Heathrow Airport - Iris

INSPASS - Hand Geometry

Grocery store payment - Fingerprint

US-VISIT Program

Mouse Biometrics

Login by Biometric

❑ * The fingerprint recognition is used as login in the notebook (Acer 730).

* http://www.zaobao.com/it/itweek.html

Internet Security

❑ * NEC: a fingerprint system (800 dpi /US$330) for internet security.

Face Verification

❑ * A face verification system in NEC.

* http://www.zaobao.com/it/itweek.html * http://www.zaobao.com/it/itweek.html

---

Other Biometrics Applications*

* http://www.zaobao.com/it/itweek.html

e-Channel

Fujutsu Palm ATM

Fingerprint Cell Phone

Xmicro Fingerprint Mouse

Citizen-facing Applications

- *EU visa system*, the biggest biometric project in the world, 70 million datasets, fingerprints & faces (under proposed)
- UN tests iris recognition systems on refugee
- *Biometric ID cards*, Hong Kong/Malaysia, fingerprint & face
- Security in Casino, Foxwoods, facial recognition
- Border security, Germany, face
- Passport, UK government, fingerprint, face, iris (under discussion)

Face scan at airports
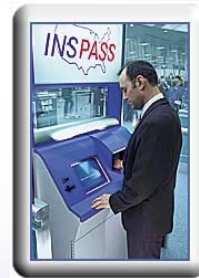
Hand Geometry for Immigration

* All above projects have been reported in Biometric Technology Today.

Forensic-facing Applications

- Smart gun, Smith & Wesson, the world's largest handgun manufacturer, fingerprints
- Florida Supreme Court – Fingerprints
- Car Security, BMW, fingerprint
- School Security, National School Fitness Foundation, fingerprint.

* All above projects have been reported in Biometric Technology Today.

Employee-facing Applications

- Mobile phone, Sagem, fingerprints
- New York State Office of Mental Health – Fingerprints
- St Vincent's Healthcare Trust – Fingerprints
- Microsoft .Net Authentication - Faces

Time & Attendance

01 | 10 | 02

07:57:34 A.M.

Start | End | Xfer | Inq?

Type ID
Swipe ID
Select payment
—OR—
Pay cashier
Cred |Debit| EBT |

Fingerprint at check-out counter

Fingerprint employee attendance system:
http://www.lucky-tech.com/iguard-videodemo.htm
http://65.211.242.195/Admins/index.html

Customer-facing Applications

Applications

BioPay services
http://www.tmcnet.com/usubmit/2003/Sep/1020276.htm

Iris-based ATM

Smart card with fingerprints

Application

EXAMPLE 1:
  Access Control

qooɹobǝu‾voɩɔǝ.ʍ

EXAMPLE 2:
  Law Enforcement

EXAMPLE 3:
  Smart Card

face_card.swf

EXAMPLE 4:
  Bio-Pay

Fingerprint.wmv

Popular Biometric Organizations

- Biometric consortium (USA) (http://www.biometrics.org/)
- Association for biometrics (UK) (http://www.afb.org.uk/)
- National Institute of Standards and Technology, Speech Group (USA) (http://www.itl.nist.gov/iad/894.01/)
- National Institute of Standards and Technology, Image Group, fingerprint (USA) (http://www.itl.nist.gov/iad/894.03/databases /defs/nist_nfis.html)
- National Institute Technical Authority for Information Assurance (UK) (http://www.cesg.gov.uk/)
- International Biometric Group (http://www.biometricgroup.com/)
- Biometric Digest (http://www.biodigest.com/)
- Japan Biometric Authentication Association (http://www.biometrics.gr.jp/)

Some Biometric Conferences

- International Conf. on Biometrics, 5-7 Jan 2006, Hong Kong (http://www4.comp.polyu.edu.hk/~icba/)
- Workshop on Multimodal User Authentication, Santa Barbara, CA, USA, Dec 11-12, 2003 (http://mmua.cs.ucsb.edu/)
- Biometric Technology for Human Identification (OR30), SPIE International Symposium on Defense and Security, 12-16 April, 2004, Orlando, USA (http://biometrics.cse.msu.edu/DSS_CFP.pdf)
- The Speaker and Language Recognition Workshop, 31 May- 4 June, 2004, Toledo Spain (http://www.odyssey04.org/home.asp)
- The Government Security Expo and Conference, July 28-29, 2004 Washington, DC, USA (http://www.govsecinfo.com/)
- IEEE Symposium on Security and Privacy, May 9-12, 2004, California, USA (http://www.cs.berkeley.edu/~daw/oakland04-cfp.html)
- IEEE Conference on Technologies for Homeland Security, 21-22 April, 2004, Cambridge, MA, USA (http://www.ieeeboston.org/homeland_2004.pdf)
- International Symposium on the Forensic Sciences, Wellington, New Zealand, 28 March-2 April 2004. (http://www.anzfss2004.org.nz/main_page.htm)

Useful Links

Researchers
http://www.cse.msu.edu/~jain/
http://bias.csr.unibo.it/research/biolab/bio_tree.html
http://www.cl.cam.ac.uk/users/jgd1000/
http://www.engr.sjsu.edu/biometrics/index.htm
http://bias.csr.unibo.it/maio/
http://www.citer.wvu.edu/research/index.php
http://www.sinobiometrics.com/index.html

Researching Company
http://www.biometricgroup.com/ or
http://www.ibgweb.com/

Biometric Glossary
http://www.resonancepub.com/biometricgl.htm
http://www.afb.org.uk/docs/glossary.htm

Public Domain
http://directory.google.com/Top/Computers/Security/Biometrics/
http://dmoz.org/Computers/Security/Biometrics/
http://groups.yahoo.com/group/biometrics/messages

Useful Links

BioAPI Consortium
http://www.bioapi.org/

Biometric Identification (Online Resources)
http://www.tml.hut.fi/Opinnot/Tik-110.501/1998/papers/12biometric/biometric.htm

Fake Fingerprint
http://cryptome.org/fake-prints.htm

Face Recognition Vendor Tests
http://www.frvt.org/

Fingerprint Verification Competitions
http://bias.csr.unibo.it/fvc2000/
http://bias.csr.unibo.it/fvc2002/
http://bias.csr.unibo.it/fvc2004/

Signature Verification Competition
http://www.cs.ust.hk/~dyyeung/

Useful Links

http://www.crimescope.com/home.htm (fingerprint and palmprint)
http://www.afix.net/ (fingerprint)
http://www.authentec.com/ (fingerprint)
http://www.biomet.ch/index.htm (fingerprint)
http://www.timetrak.com/text/products/hardware/T016.htm (fingerprint)
http://www.biometricaccess.com/ (fingerprint)
http://www.secugen.com/ (fingerprint)
http://www.sw.nec.co.jp/english/pid_e/mechanism.html (fingerprint matching mechanism)
http://www.identix.com/products/pro_livescan_TPpro.html (fingerprint/ palmprint)
http://www.necsolutions-am.com/idsolutions/products/Identification.cfm (fingerprint/ palmprint)
http://www.crossmatch.net/products_livescan_id10.html (fingerprint/ palmprint)
http://www.printquest-apis.com/ (fingerprint/ palm)
http://www.iridiantech.com/ (iris)
http://www.sensar.com/ (iris)
http://www.eyenetwatch.com/iris/scanners.htm (iris)
http://www.viisage.com/ (face)
http://www-white.media.mit.edu/vismod/demos/facerec/ (face)
http://www.cs.colostate.edu/evalfacerec/index.html (face)
http://www.recogsys.com/products/personal_id.htm (hand)
http://pr.fujitsu.com/en/news/2003/03/31.html (palm vein)
http://pr.fujitsu.com/en/news/2002/08/28.html (palm vein)
http://www.mmigroup.net/en/index_en.php (signature)
http://www.cybersign.com/ (signature)
http://www.topazsystems.com/ (signature)
http://www.nuance.com/ (speech)
http://www.buytel.com/ (voice)
http://www.verivoice.com/ (voice)
http://www.voice-security.com/Biomet.html (voice)
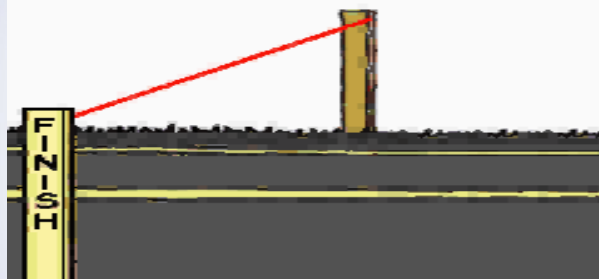
Questions?

1. Suppose that you could understand what about biometrics. Do you have any idea to find at least one new biometrics from human body except the current biometrics list in this lecture note?

2. Biometrics technology could be a good solution in security problem. Do you think other applications using biometrics? Could you also list at least one application which may use biometrics technology as well?