Advanced Signal Processing Seminar WS 2007

Topic: Biometrics

First Meeting: 15th October 2007, 5pm,
Seminarroom Inffeldgasse 16c, 2nd floor

Regular Meeting: Each Wednesday begin. with 14th November, 1pm-3pm
Seminarroom of ICG, Inffeldgasse 16 (?), 2nd floor

Assignment of Topics:

14th November: Steiner, Feuersinger

Hand geometry/Palmprint, Vein Patterns, Signature verification

21th November: Lessiak, Storer

Face recognition

28th November:Guldenshuh, Rahimzadeh Assbforoushani

Fingerprint

5th December: Gampp, Sereinig

Iris recognition

12th December: Luig, Unterkofler

Keystrokes, Ear recognition, Retina recognition, Body odour, Thermograms

9th January: Ciglar, Stark

Gait, Speaker recognition

16th January: Birchbauer (SIEMENS)

Biometric Attacks and Countermeasures, Biometric Standards

Live Demos (Palm, Vein, Face recognition)

23th January: Wohlmayr

Introduction [from Wikipedia]

Biometrics (ancient Greek: *bios* ="life", *metron* ="measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Some researchers,[1] have coined the term behaviometrics for behavioral biometrics such as typing rhythm or mouse gestures where the analysis can be done continuously without interrupting or interfering with user activities.

1. Overview

Biometrics are used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics.

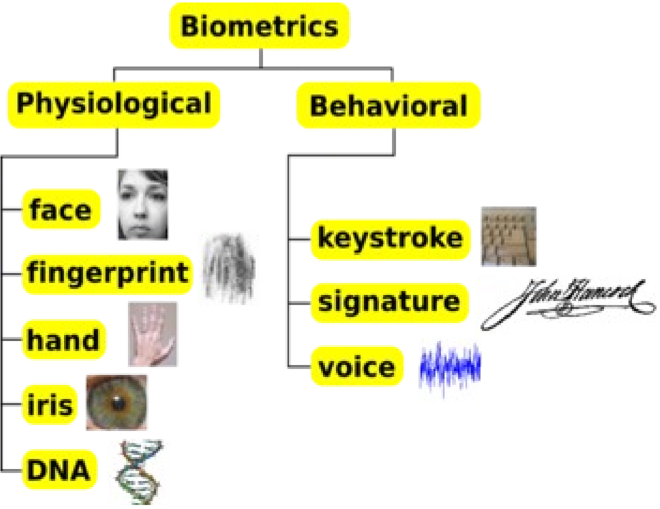
- possession-based: using oe specific "token" such as a security tag or a card
- knowledge-based :the use of a code or password.

Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample.This intends to enhance security as multiple different samples are required such as security tags and codes and sample dimensions**.**

2. Common Human biometric characteristics

Biometric characteristics can be divided in two main classes, as represented in figure on the right:

- **physiological** are related to the shape of the body. The oldest traits, that have been used for more than 100 years, are fingerprints. Other examples are face recognition, hand geometry and iris recognition.
- **behavioral** are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.



Strictly speaking, *voice* is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

Other biometric strategies are being developed such as those based on gait (way of walking), retina, hand veins, ear recognition, facial thermogram, DNA, odor and palm prints.

3. Comparison of various biometric technologies

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters[2]:

- **Universality** describes how commonly a biometric is found individually.
- **Uniqueness** is how well the biometric separates individually from another.
- **Permanence** measures how well a biometric resists aging.
- **Collectability** ease of acquisition for measurement.
- **Performance** accuracy, speed, and robustness of technology used.
- **Acceptability** degree of approval of a technology.
- **Circumvention** ease of use of a substitute.

The following table shows a comparison of existing biometric systems in terms of those parameters:

Comparison of various biometric technologies, according to A. K. Jain[2] (**H**=High, M=Medium, **L**=Low)

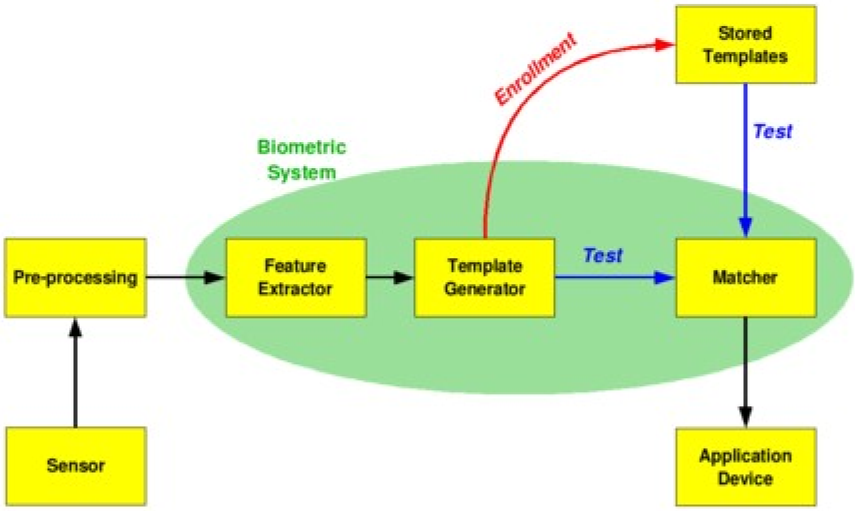
Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*

Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geomet.	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
facial thermog.	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear recog.	M	M	H	M	M	H	M

- circumventability listed with reversed colors because low is desirable here instead of high

A. K. Jain ranks each biometric based on the categories as being either low, medium, or high. A low ranking indicates poor performance in the evaluation criterion whereas a high ranking indicates a very good performance.

4. Biometric systems



The diagram on right shows a simple block diagram of a biometric system. When such a system is networked together with telecommunications technology, biometric systems become telebiometric systems. The main operations a system can perform are *enrollment* and *test.* During the enrollment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is be robust. The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalisation, etc. In the third block features needed are extracted. This step is an important step as the correct features need to be extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of all the characteristics extracted fromthe source, in the optimal size to allow for adequate identifiability.

If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching programme will analyse the template with the input. This will then be output for any specified use orpurpose (e.g. entrance in a restricted area).

5. Functions

A biometric system can provide the following two functions [3]:

- **Verification:** A pre-stored template is matchedagainst a sample directly, e.g a card or known database entry.
- **Identification:** Identifying from all the templates which one is the closest match to the input sample.

6. Performance measurement

- *false accept rate (FAR)* or *false match rate (FMR)*: the probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.
- *false reject rate (FRR)* or *false non-match rate (FNMR)*: the probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.
- *receiver (or relative) operating characteristic (ROC)*: In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the *Detection error trade-off (DET),* which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- *equal error rate (EER)*: the rate at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.
- *failure to enroll rate (FTE or FER)*: the percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the dataobtained by the sensor are considered invalid or of poor quality.
- *failure to capture rate (FTC)*: Within automatic systems, the probability that the system fails to

detect a biometric characteristic when presented correctly.

- *template capacity*: the maximum number of sets of data which can be input in to the system.

7. Performance

The following table shows the state of art of some biometric systems:

State of art of biometric recognition systems

Biometrics	EER	FAR	FRR	Subjects	Comment	Reference
Face	n.a.	1 %	10 %	37437	Varied lighting, indoor/outdoor	FRVT (2002)[4]
Fingerprint	n.a.	1 %	0.1 %	25000	US Government operational data	FpVTE (2003)[5]
Fingerprint	2 %	2 %	2 %	100	Rotation and exaggerated skin distortion	FVC (2004)[6]
Hand geometry	1 %	2 %	0.1 %	129	With rings and improper placement	(2005)[7]
Iris	< 1 %	0.94 %	0.99 %	1224	Indoor environment	ITIRT (2005)[8]
Iris	0.01 %	0.0001 %	0.2 %	132	Best conditions	NIST (2005)[9]
Keystrokes	1.8 %	7 %	0.1 %	15	During 6 months period	(2005)[10]
Voice	6 %	2 %	10 %	310	Text independent, multilingual	NIST (2004)[11]

One simple but artificial way to judge a system is by EER, but not all the authors provided it. Moreover, there are two particular values of FAR and FRR to show how one parameter can change depending on the other. For fingerprint there are two different results, the one from 2003 is older but it was performed on a huge set of people, while in 2004 much less people were involved but stricter conditions have been applied. For iris, both references belong to the same year, but one was performed on more people, the other one is the result of a competition between several universities so, even if the sample is much smaller, it could reflect better the state of art of the field.

8. Issues and concerns

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints. A theoretical example is a debit card with a personal Identification Number (PIN) or a biometric. Some argue that if a person's biometric data is stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. However, this argument ignores a key operational factor intrinsic to all biometrics-based security solutions: biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a "live" biometric sample to a pre-stored, static "match template" created when the user originally enrolled in the security system. Most of the commercially available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (for example, by using hash codes and encryption), so the problem is effectively limited to cases where the scanned "live" biometric data is hacked. Even then, most competently designed solutions contain anti-hacking routines. For example, the scanned "live" image is virtually never the same from scan to scan owing to the inherent plasticity of biometrics; so, ironically, a "replay" attack using the stored biometric is easily detected because it is too perfect a match.

The television program *Mythbusters* attempted to break into a commercial security door equipped with biometric authentication as well as a personal laptop so equipped[12]. While the laptop's system proved more difficult to bypass, the advanced commercial security door with "live" sensing was fooled with a printed scan of a fingerprint after it had been licked. Assuming the tested security door is representative of the current typical state of biometric authentication, that it was so easily bypassed suggests biometrics may not yet be reliable as a strong form of authentication.

Marketing of biometric products: Despite confirmed cases of defeating commercially available biometric scanners, many companies marketing biometric products (especially consumer-level products such as readers built into keyboards) still claim the products as replacements, rather than supplements, for passwords. Furthermore, regulations regarding advertising and manufacturing of biometric products are (as of 2006) largely non-existent. Given the low security, consumer-level products are most likely to be bought and used by most people, leading to the risk of large-scale economic and social problems associated with biometric identity theft.

Sociological concerns: As technology advances, and time goes on, more and more private companies and public utilities will use biometrics for safe, accurate identification. However, these advances will raise many concerns throughout society, where many may not be educated on the methods. Here are some examples of concerns society has with biometrics:

- Physical - Some believe this technology can cause physical harm to an individual using the methods, or that instruments used are unsanitary. For example, there are concerns that retina scanners might not always be clean.
- Personal Information - There are concerns whether our personal information taken through biometric methods can be misused, tampered with, or sold, e.g. by criminals stealing, rearranging or copying the biometric data. Also, the data obtained using biometrics can be used in unauthorized ways without the individual's consent.

Danger to owners of secured items: When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. In 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car[13].

9. References

1. http://www.cilab.upf.edu/biosecure1/public_docs_deli/BioSecure_Deliverable_D10-2-3_b3.pdf
2. *Jain, A. K. (28-30 April 2004), "*Biometric recognition: how do I know who you are?*", Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE* ***12th****: 3 - 5*
3. *Jain, A. K.; A. Ross & S. Pankanti (June 2006), "*Biometrics: A Tool for Information Security*", IEEE Transactions On Information Forensics And Security* ***1st*** *(2)*
4. P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, *Face Recognition Vendor Test 2002: Overview and Summary* (Online) [1]
5. C. Wilson, A. R. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. J. Micheals, S. Otto, and C. Watson, *Fingerprint vendor technology evaluation 2003: summary of results and analysis report*, NIST Internal Rep. 7123, Jun. 2004 [Online] [2]
6. R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, *Performance evaluation of fingerprint verification systems*, IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, Jan. 2006
7. E. Kukula, S. Elliott, *Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance*, IEEE 2005
8. International Biometric Group, *Independent Testing of Iris Recognition Technology*, May 2005 (Online) [3]
9. *NIST Iris Challenge Evaluation*, (Online) [4]
10. S. Hocquet, J. Ramel, H. Cardot, *Fusion of Methods for Keystroke Dynamic Authentication*, Automatic

Identification Advanced Technologies, 2005. Fourth IEEE Workshop on 17-18 Oct. 2005 Page(s):224 - 229

11. D. A. Reynolds, W. Campbell, T. Gleason, C. Quillen, D. Sturim, P. Torres-Carrasquillo, and A. Adami, *The 2004 MIT Lincoln laboratory speaker recognition system*, in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Philadelphia, PA, Mar. 2005
12. Video of the Mythbusters episode on how to hack fingerprint scanners [5]
13. BBC News: Malaysia car thieves steal finger [6]
14. Article describing Disney's 2006 biometric initiative replacing hand geometric scanners with fingerprint readers
15. Biometric Identification System for Access.

Outline of the Seminar [Talks on the following list of topics]

The list of literature is not restricted to the given papers.You are encouraged to use additional papers.

Common Biometrics:

1. **Fingerprint**

- S. Pankanti, S. Prabhakar, and A.K. Jain, "On the individuality of fingerprints", IEEE Trans. on PAMI, 24(8), 1010-1025, 2002.
- M.D. Garris, E. Tabassi, and C.L. Wilson, "NIST Fingerprint Evaluations and Developments", Proceedings of the IEEE, 94(11),1915-1926, 2006.
- A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints", Proceedings of the IEEE, 85(9),1365-1388, 1997.
- A.R. Roddy and J. D. Stosz, "Fingerprint features– statistical analysis and sstem performance estimates", Proceedings of the IEEE, 85(9),1390-1421, 1997.

2. **Face recognition**

- S. Romdhani, J. Ho, T. Vetter, and D. J. Kriegman, " Face recognition using 3-D models: Pose and Illumination", Proceedings of the IEEE, 94(11),1977-1999, 2006.
- K.W. Bowyer, K.I. Chang, P.J. Flynn, and X. Chen, "Face recognition using 2-D, 3-D, and Infrared: Is multimodal b etterthan multisample?", Proceedings of the IEEE, 94(11),2000-2012, 2006.
- B.V.K. Vijaya Kumar, M. Savvides, and C. Xie, "Correlation pattern recognition for face recognition", Proceedings of the IEEE, 94(11),1963-1976, 2006.
- P.Sinha, B. Balas, Y. Ostrovsky, and R. Russel, " Face recognition by humans: Nineteen results all computer vision researchers should know about", Proceedings of the IEEE, 94(11),1948-1962, 2006.
- J. Zhang, Y. Yan, and M. Lades, "Face recognition: Eigenface, elastic matching, and neural nets", Proceedings of the IEEE, 85(9),1423-1435, 1997.
- J.J. Weng and D.L. Swets, "Face recognition", In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages ?-86, Kluwer Academic Press, Boston, 1999.

3. **Speaker recognition**

- D.A. Reynolds, "Automatic speaker recognition: Current approaches and future trends" Proc.

IEEE AutoID 2002, pp. 103-108, 2002.

- P.S. Aleksic and A.K. Katsaggelos, “Audio-Visual biometrics”, Proceedings of the IEEE, 94(11), 2025-2044, 2006.
- J.P. Campbell, “Speaker recognition: A tutorial”, Proceedings of the IEEE, 85(9),1437-1462, 1997.
- D.A. Reynolds, T.F. Quatieri, and R.B. Dunn, “Speaker Verificaiton Using Adapted Gausssina Mixture Models”, Digital Signal Processing, 10, pp. 19-41, 2000.
- J.P. Campbell and F. Meade, “Speaker Recognition”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 165-190, Kluwer Academic Press, Boston, 1999.

4. **Iris Recognition**

- J. Daugman, “Probing the uniqueness and randomness of IrisCodes: Results from 200 Billion Iris Pair Comparisons”, Proceedings of the IEEE, 94(11),1927-1935, 2006.
- J.R. Matey, O. Naroditsky, K.Hanna, R. Kolczynski, D.J. LoIancono, S. Mangru, M. Tinker, T.M. Zappia, and W.Y. Zhao, “Iris on the move: Acquisition of images for iris recognition in less constrained evnvironments”, Proceedings of the IEEE, 94(11),1936-1947, 2006.
- J. Daugman, “How Iris Recognition Works”, IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21-30, 2004.
- R.P. Wildes, “Iris recognition: An emerging biometric technology”, Proceedings of the IEEE, 85(9),1348-1363, 1997.
- J. Daugman, “Recognizing persons by their iris patterns”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 103-122, Kluwer Academic Press, Boston, 1999.

5. **Hand geometry/Palmprint**

- R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, “Biometric identification through hand geometry measurements,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1168–1178, 2000.
- D. Zhang, W.-K. Kong, J. You, and M. Wong, “Online palmprint identification,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 2, pp. 1041–1050, 2003.
- R.L. Zunkel, “Hand geometry based verification”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 87-102, Kluwer Academic Press, Boston, 1999.

6. **Signature verification**

- V.S. Nalwa, “Automatic on-line signature verification”, Proceedings of the IEEE, 85(2):215-239, 1997.

Additional Biometrics:

1. **DNA**
2. **Retina Recognition**

- R. Hill, “Retina identification”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 123-142, Kluwer Academic Press, Boston,

1999.

3. **Thermograms**

- F.J. Prokoski and R. Riedl, “Infrared identification of faces and body parts”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 191-212, Kluwer Academic Press, Boston, 1999.

4. **Gait**

- M.S. Nixon, and J.N. Carter, “Autmatic recognition by gait”, Proceedings of the IEEE, 94(11),2013-2024, 2006.
- M.S. Nixon, J.N. Carter, D. Cunado, P.S. Huang, and S.V. Stevenage, “Automatic gait recognition”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 231-248, Kluwer Academic Press, Boston, 1999.

5. **Keystrokes**

- F. Bergadano, D. Gunetti, and C. Picardi, “User authentication through keystroke dynamics” ACM Transactions on Information and System Security (TISSEC), 5(4): 367-397, 2002.
- M.S. Obaidat and B. Sadoun, “Keystroke dynmaicsbased authentication”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 213-229, Kluwer Academic Press, Boston, 1999.

6. **Ear recognition**

- M. Burge and W. Burger, “ Ear biometrics in computer vision”, Proceedings of the Intern. Conf. on Pattern Recognition, pp. 826-830, 2000.
- M. Burge and W. Burger, “Ear biometrics”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 273-285, Kluwer Academic Press, Boston, 1999.

7. **Skin reflectance**

- **http://www.lumidigm.com/**

8. **Lip motion**

9. **Body odour**

- K.C. Persaud, D.-H.Lee, and H.-G- Byun, “Objective odour measurements”, In A.K. Jain, R.M. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society,* pages 251-270, Kluwer Academic Press, Boston, 1999.