Biometrics (CSE 40537/60537)

University of Notre Dame, Fall 2014

Adam Czajka, August 21, 2014

Course webpage: `http://zbum.ia.pw.edu.pl/EN/node/38`

1 Aim

The aim of this course is to introduce the principles of biometric authentication. The course will study those biometric characteristics which have commercial implementations, as well as emerging techniques, discussing hopes and fears related to the presented modalities. Important part of this course will be devoted to the security of biometrics (in particular liveness detection) and secure biometric implementations. The course will show how to apply statistics for biometric reliability evaluation. Each lecture will refer to selected examples of real systems and applications.

2 Course structure

- 36 lectures (50 minutes each),
- 5 practical classes with biometric data capture (50 minutes each),
- 5 assignments to be realized at home or university lab (using Matlab codes delivered by an instructor, and own biometric data captured during practical classes).

3 Suggested prerequisites and reading

Prerequisites in statistics (estimation and hypotheses testing), image processing (1D and 2D filtering), basic principles of symmetric and asymmetric cryptography will help in faster adoption of the discussed topics. There are no required textbooks, however the following suggested reading may be considered:

- Jain, A.K., Ross, A., Nandakumar, K. *Introduction to Biometrics*. Edition 2011
- Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., *Handbook of Fingerprint Recognition*. Second edition 2009
- Burge, M.J., Bowyer, K., *Handbook of Iris Recognition*. Edition 2013
- Marcel, S., Nixon, M.S., Li, S.Z., Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (Advances in Computer Vision and Pattern Recognition). Edition 2014

4 Attendance

The attendance on lectures is not mandatory. However, attending the lectures allows for discussion and will help in gathering knowledge necessary for assignments, quizzes and a final test. Attendance is expected during practical classes, when the biometric data capture is realized. Organizing additional data capture sessions (apart from those scheduled) is difficult, and will be done only in exceptional cases.

5 Grading

- 50% for assignments (5 assignments $\times$ 10%)
- 30% for quizzes (approx. 10 quizzes $\times$ 3%)
- 20% for final test

6 Lectures (synopsis)

Notion of biometrics (3 lectures). Development of biometric authentication. Basic terms, biometric data, biometric characteristics, biometric features, biometric templates and references. Expected properties of biometric identifiers. Basics in biometric errors estimation. Enrollment, verification and identification.

Fingerprint recognition (5 lectures). Fingerprint capture, sensor types, latent fingerprints. Fingerprint image preprocessing, segmentation, binary and skeletal images. Fingerprint singularities, detection of loops, deltas, whirls and cores, using singularities in fingerprints classification. Galton's details, base and complex minutiae, detection of minutiae. Fingerprint recognition, minutiae- and correlation-based methods. Fingerprints in forensics and biometrics, similarities and differences.

Iris recognition (5 lectures). Eye and iris morphogenesis, genetic penetrance. Principles of iris image capture, iris sensors. Iris image preprocessing, segmentation, formatting and filtering. Daugman's method, iris code, statistical properties of the iris code. Other iris coding methods, wavelet analysis.

Face recognition (2 lectures). Face detection in still images and sequences. Face features. Face space, principal component analysis and its application, *eigenfaces*, linear discriminant analysis and its application, *Fisherfaces*. Face recognition methods.

Other, selected physical biometric methods (2 lectures). Use of vein patterns of a hand, finger and retina. Thermal imaging and geometry of a hand.

Recognition of handwritten signatures (2 lectures). Signature capture, off-line (scanned) and on-line (captured by tablets) signatures. Signature as a multidimensional curve, two- and multi-dimensional analyses. Signature features, hidden and visible features. Use of dynamic time warping in signature recognition.

Other, selected behavioral biometric methods (3 lectures). Speaker recognition, formants, speaker features in time, frequency and cepstrum domains, homomorphic deconvolution of voice signals. Use of electroencephalogram (EEG) in biometrics.

Security of biometrics: presentation attack detection (3 lectures). Static and dynamic liveness features. What we want to detect (subversive actions) vs. what we can detect (suspicious actions). Liveness detection in finger- and eye-based biometrics. Selected liveness detection techniques, frequency analysis for paper printouts detection, pupil dynamics and blood pulse analyses for detection of sophisticated eye and finger spoofing trials.

From biometric methods to biometric systems (3 lectures). Multiple biometrics, merging biometric information and decisions. System level issues, template aging, user perspective, interoperability of devices and methods. Development of a biometric system, programming interfaces, biometric data exchange, biometric standards.

Security of biometrics: system perspective (3 lectures). Secure transfer of biometric data. Merging biometrics and cryptography, template protection. Merging biometrics and steganography, embedding steganographic signatures in biometric data. Secure storage, use of smart cards, principles of *match-off-card* and *match-on-card* techniques. Use of biometric data intrinsic properties in security enhancements, dynamic coding, information quantization.

Statistical evaluation of biometrics (3 hours). Technology, scenario and operational evaluations. Errors of biometric systems, false non-match vs. false rejection, false match vs. false acceptance. Error curves, ROC, DET, CMC. Statistical error estimation, hypothesis testing. Principles of biometric database collection and usage.

Biometric passports (2 hours). Structure of biometric passports. Capturing and formatting of passport-compliant biometric data. Security of biometric passports, basic access control, passive and active authentication, extended access control. Public key infrastructure in a biometric passport system.

7 Practical classes and assignments

The aim of the practical classes is to interface with authentic, commercial biometric sensors. The aim of each assignment is to practice the entire biometric recognition process, or liveness detection process for selected methods.

Practical classes use analysis and capture software designed in MATLAB and C/C++ (with the use of hardware SDKs) by a tutor and specially for this course. The hardware is used by students for collection of their biometric samples.

Problems to be solved at home are defined to let students work alone or in groups (depending on the topic). Students use MATLAB software prepared by a tutor to easily perform all the exercises. The estimated burden for each assignment is 3-4 hours.

Fingerprint recognition (individual work).

- **at the classroom:** capture of all fingerprint; instructions what to be done at home; NOTE: keep own fingerprint images until the end of the course, since they will be used again in liveness detection training;
- **at home:** analysis of the images of all fingerprints in Matlab (segmentation, quality assessment, skeletal image generation, singular points detection and fingerprint classification); minutiae detection and comparison; calculation of basic error estimates (FNMR, FMR, EER) given the obtained distributions of within- and between-class matching scores.

Iris recognition (individual work).

- **at the classroom:** capture own iris images; instructions what to be done at home; NOTE: keep own iris images until the end of the course, since they will be used again in liveness detection training;
- **at home:** manual segmentation of iris images; selection of filters and adjustment of image filtering parameters to obtain maximum separation between within- and between-class matching score distributions; calculation of basic error estimates (FNMR, FMR, EER) given the obtained distributions.

Handwritten signatures (work in groups of 2-3 students).

- **at the classroom:** capture of on-line signatures and signature skilled forgeries (done by others in the group);
- **at home:** calculation of signature features ('hidden' and 'visible'); matching of signatures in a feature domain; matching of signatures in a time domain (use of dynamic time warping – DTW); selection of DTW components to obtain maximum separation of within- and between-class matching score distributions; calculation of basic error estimates (FNRM, FMR, EER) given the obtained distributions.

Liveness detection in fingerprint biometrics (work in groups of 2-3 students).

- **at the classroom:** preparation and capture of artificial (wood glue) fingers based on own fingerprint images captured at the beginning of the course; instructions what to be done at home);
- **at home:** use of an example liveness detection method (sweat pores detection) to distinguish between authentic fingers and artifacts; selection of filtering parameters to obtain maximum separation between scores for living and artificial fingerprints;

Liveness detection in iris biometrics (work in groups of 2-3 students).

- **at home before the classes:** preparation of artificial eyes: paper printouts (instructions how to do this, and the Matlab supporting software will be given);
- **at the classroom:** capture of artificial eyes; instructions what to do at home;
- **at home:** use of an example liveness detection method (Fourier analysis) to distinguish between living and forged eyes; selection of filtering parameters to obtain maximum separation between scores for living and artificial irises.

8 Objectives

At the end of the course students should be able to:

- describe principles of the selected physical and behavioral biometric methods, and know how to deploy them in authentication scenarios,
- organize and conduct biometric data collection processes, and understand how to use biometric databases in system evaluation,
- calculate distributions of within- and between-class matching scores, and calculate various error estimates based on these distributions,
- understand the biometrics security issues, and know how to deploy selected liveness detection techniques to make a system spoof-resistant,
- understand differences between a biometric method and a biometric system,
- deploy statistical methods in biometric system evaluation,
- itemize the most up-to-date examples of real biometric applications in human authentication.

9 Code of Honor

This class follows the binding Code of Honor at Notre Dame (`http://honorcode.nd.edu`). The graded work you do in this class must be your own. In the case where you collaborate with other students make sure to fairly attribute their contribution to your project.

10 Contact

Dr. Adam Czajka
Office: 355C Fitzpatrick Hall
Office phone: (574) 631-0697
Office hours: 10:00–11:00am
Email: `aczajka@nd.edu` (preferred way of contact)