

Syllabus

CYB 305 – BIOMETRIC SYSTEMS (Credit
Units: 3)

Department of Cyber Security
Faculty of Computing
University of Delta, Agbor, Nigeria

Lecturer: Dr. Okpako Abugor Ejaita

Office Location: FOC Room 2

Email: ejaita.okpako@unidel.edu.ng

Phone: +234 08163239516

Office Hours: Monday, Tuesday, Wednesday, Thursday & Friday 8:00 am - 4:00
pm

There are many ways to reach me. There is no substitute for face-to-face communication which often leads to more refined and focused questions resulting in your improved understanding. I strongly encourage you to take advantage of my office hours. Questions during class or immediately after class are always welcomed. Email is an easy way to ask questions outside of class but is not productive as face-to-face communication.

Meeting Time and Place: Thursday, 2:00pm to 4:00pm, FOC LH 4

Attendance

You are expected to attend every class. If you must miss a class, it is your responsibility to make up for the work that you missed. If you are going to be absent from any class, you must please notify the instructor in advance.

Methods of Instruction

This syllabus contains an overview of what will be covered in class; for specific information, students are referred to the class web page maintained on the University website. Assignments will be posted on University of Delta LMS or given in the class and should be submitted through University of Delta LMS. Class attendance, doing all your practical and homework will help the borderline cases.

Overview

Biometrics is an emerging field in cyber security as it identifies and verifies users using unique biological (anatomical/physiological) or behavioral traits. It has been shown to be more convenient for users, reduces fraud and more robust to security challenges and has become an indispensable ally of security, intelligence, law enforcement, and e-commerce. Identification/Authentication of individuals based on the anatomical and behavioral characteristics such as the face, the iris, gait, voice or fingerprints is a promising research domain. Biometric algorithms allow the recognition of individuals in physical or logical access control systems and thus provide an efficient and convenient alternative to knowledge based, and password based systems. This course presents an overview of the principles and use of biometric systems and algorithms. The objective of this class is to emphasize the fundamental knowledge and skill set necessary to work with biometric characteristics, implementation, and construction of biometric systems. Students will learn basic biometric characteristics, types of biometric systems/algorithms, gathering methods, processing, storing, and comparing biometric characteristics and their use in security systems, different approaches used in biometric systems, the complex and hidden relationships existing between biometric systems and environmental conditions and how they affect the performance of the biometric systems.

Objectives

The objectives of this course are to enable the student: (i) have knowledge of biometric foundations (ii) have understanding of behavioral and anatomical biometrical modalities (ii) have knowledge of data acquisition techniques (iv) aware of challenges facing commercial systems (v) aware of challenging issues in terms of security, recognition rates, privacy as well as alternatives of password and smart cards.

Learning outcomes

Upon completion of this course, students should be able to: (i) explain the working principle and different types of biometric system; (ii) discuss the trade-offs and differences between various biometric algorithms; (iii) define the modules and properties of biometric systems (iv) describe the inner workings of biometric systems; (v) collect and preprocess biometric data for biometric identifications and verifications; (vi) define the current research problems in biometric systems and develop effective solutions (vii). Identify various vulnerabilities in biometric systems

Course Contents

Introduction to biometrics, brief introduction to digital image processing, introduction to biometric algorithms and systems with emphasis on any two of the following: face, iris, fingerprint, speech & speaker. Multimodal biometrics, privacy issues, and other aspects of biometrics, applications of biometrics and future trends. The course also addresses such challenging issues as security, recognition rates and privacy , as well as alternatives of password and smart cards.

Lecture Schedules

Week	Content	Lecture notes/slides
1.	Course Overview, Last Decade of Biometrics, Applications	
2.	Overview of Biometric System Operation Brief introduction to digital image processing	
3.	Biometric System Evaluation	
4.	Face Detection	
5.	Fingerprint Recognition	
6.	Iris Recognition	
7.	Test	
8.	Behavioral Biometrics	
9.	Multi-modal Biometrics & Biometric Fusion	
10.	Biometric System Security and Spoofing	
11.	Biometric Template Protection	
12.	Revisions	
13.	Final Exam	

Examination schedule

- Attendance
- Homework
- Class Test
- Practical exercises
- End of Semester Exam

Practical Exercises

Grading

- Homework: 10% of grade
- Midterm Exam/Test: 20% of grade
- Final Exam: 70% of grade

Text & References

A.K. Jain, Arun. A. Ross, Karthik Nandakumar : Introduction to Biometrics, (2011). DOI 10.1007/978-0-387-77326-1_1512

B. Cukic and N. Bartlow. Biometric System Threats and Countermeasures: A Risk Based Approach. In Proceedings of Biometric Consortium Conference (BCC), Crystal City, USA, September 2005.

Jain, A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)

J. Daugman. Recognizing Persons by their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, Biometrics: Personal Identification in Networked Society, pages 103–122. Kluwer Academic Publishers, London, UK, 1999

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behaviour conducive to a positive learning environment. The code of student conduct is described in detail in the student handbook or University website.

Academic Honesty

"All students enrolled at the University shall follow the tenets of common decency and acceptable behaviour conducive to a positive learning environment." It is the policy of the University, that no form of plagiarism or cheating will be tolerated. Plagiarism is defined as the deliberate use of another's work and claiming it as one's own. This means ideas as well as text or code, whether paraphrased or presented verbatim (word-for-word). Cheating is defined as obtaining unauthorised assistance on any assignment. Proper citation of sources must always be utilised thoroughly and accurately. If you are caught sharing or using other people's work in this class, you will receive a 0 grade and a warning on the first instance. A subsequent instance will result in receiving an F grade for the course, and possible disciplinary proceedings. If you are unclear about what constitutes academic dishonesty, ask.

The image shows a screenshot of the UNIDEL CMS 'MANAGER COURSES' interface. The page title is 'UNIDEL CMS Courses'. The main content area is a form for adding or editing course information. It includes a 'Courseware Document' field with a 'Browse...' button and a note 'No file selected.', and an 'UPLOAD PDF DOC' button. Below this are input fields for 'Course Code' and 'Course Title'. There are also dropdown menus for '1st' and '200 Level', and a 'FOC' button. Two large text areas are provided for 'Course Objective' and 'Course Synopsis'. At the bottom, there are several input fields for 'Course Lecturer', 'Exam Mark', 'Test Mark', 'Assignment Mark', 'Lecturer Hour', 'Tutorial Hours', 'Practical Hours', and 'Course Unit'. At the very bottom of the form are 'SAVE' and 'CANCEL' buttons.

