CS 773C Machine Intelligence Advanced Applications
Spring 2000: Cryptography and Biometrics

Prerequisites

This course requires that the students have previously taken courses on data structures (CS308), calculus (MATH 181, MATH 182), math of computer science (CS 306), linear algebra (MATH 330), analysis of algorithms (CS465/665), and image processing (CS474/674). **If you do not meet the prerequisite requirements for this course, you should see me immediately.**

Credit hours: 3.0

Instructors: Dr. George Bebis and Dr. Peter Li
Office: 235 SCM
Phone: (775) 784 - 6463
E-mail: bebis@cs.unr.edu
URL: http://www.cs.unr.edu/~bebis/CS773C
Office Hours: TR: 2:30 - 4:00 pm or by appointment.

Required Text:

CryptographyTheory and Practice, by Douglas Stinson, CRC Press, 1995.
Notes on Biometrics will be provided in class.

Other Texts (not required):

Applied Cryptography, by B. Schneier, John Wiley & Sons, Inc., 1996.
BIOMETRICS: Personal Identification in Networked society, by A.K. Jain, R. Bolle, and S. Pankanti (eds.), Kluwer Academic Publishers, 1998.

Course description and objectives

Cryptography is the art and science of communicating in secure, private, and reliable ways. One of the basic problems in cryptography is that of encrypting and decrypting data. Encryption is the transformation of data into a form (*ciphertext*) which is ideally impossible to read without the need of appropriate knowledge. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption, that is, the transformation of data back to its original form (*plaintext*). Encryption and decryption generally require the use of some hidden information, referred to as a *key*. Keys are used to translate a message into its encrypted form, and then to decrypt it back to its original form. Modern algorithms are designed so that a user who knows the algorithm but does not know the key cannot easily derive plaintext from the corresponding ciphertext.

Biometrics refers to the identification of an individual based on his/her physiological characteristics, like a fingerprint, face, voice or behavior like handwriting or keystroke patterns. Because biometric characteristics are unique to each individual, they can be used to prevent theft of fraud. In addition, unlike a password or a PIN, a biometric cannot be lost, stolen, or recreated. Most biometric technology systems use the same basic principles of operation. First, a person must be registered, or enrolled, on the biometric system. To be authenticated, a person must provide a real-time biometric measurement. This measurement is then processed using the same algorithm that was used at enrollment. The output of the live measurement is then compared to the stored template.

The goal of the course is to introduce you to the areas of Cryptography and Biometrics. These are two different areas, however, there is a lot of interest lately in combining the two areas together under various applications. One possible application is the use of Biometrics for Encryption (referred to as Biometric Encryption). Another idea is to use Biometrics for Authentication. First, we will review the fundamentals of Cryptography and Biometrics. Then, we will concentrate on discussing a number of interesting papers (mainly on Biometrics). The course requires the completion of a semester project which should involve combining Cryptography with Biometrics. The instructors will discuss with you possible project ideas but you are encouraged to discuss your own project ideas with the instructors.

This is an **advanced level course** suited for graduate students in Computer Science and Engineering. It is primarily intended for **highly motivated** graduate students who are interested in working on the areas of Biometrics and Cryptography. There are many problems in these areas suitable for investigation by Master's/PhD's students leading to a master thesis or dissertation. The course contains three main parts:

• Lectures (instructors)
• Paper presentations/discussion (students)
• Semester project (students)

Course Outline (tentative)

• Introduction to Cryptography and Biometrics
• Review (Number Theory, Combinatorics, Linear Algebra)
• Classical Cryptography (Chapter 1)
• Biometrics (Notes)
• Shannon's Theory (Chapter 2)
• Biometrics (Notes)
• The Data Encryption Standard (Chapter 3)
• Biometrics (Notes)
• The RSA System (Chapter 4)
• Biometrics (Notes)
• Selected topics on cryptography
• Biometrics (student paper presentations)

Course Policies

We will spend almost the first half of the semester with lectures covering the fundamentals of Cryptography and Biometrics. During the second half of the semester, each student is expected to study 1-2 papers and give a presentation to the rest of the class. The presentation of the material should be **professional** as if it was presented in a formal conference. The student who is responsible for presenting a paper(s) on a specific day is expected to be well prepared and have a good understanding of the ideas discussed in the paper. Every other student is also expected to read the papers to be discuused in class and participate in class discussion.

Each student is expected to complete a research project. Projects will be done in groups of two students. Ideally, the project will target a problem relevant to the student's research interests. There will be a number of project reports during the semester as well as a demo at the end of the semester.

Grading

Your grade will determined based on homework assignments, a midterm exam, paper presentations, project reports and a demo to be given at the end of the semester. Note that good programming skills and a lot of motivation are essential in order to complete the project successfully. Programming can be done using either C or C++.

Grading Scheme

Homework: 10%
Midterm: 20%
Presentation: 20%
Interim report: 20%
Final report and demo: 30%

Important dates

3/10/2000 - last day for dropping classes
3/18/2000 3/26/200 - no classes (Spring Break)
3/28/2000 - Midterm exam
5/3/2000 - no classes (preparation for finals)
5/9/2000 and 5/10/2000 - Demos