SJSU SAN JOSÉ STATE UNIVERSITY

College of Science · Computer Science

Topics in Information Security Section 01

CS 266

Fall 2024 3 Unit(s) 08/21/2024 to 12/09/2024 Modified 08/20/2024

Contact Information

Instructor: Dr. Amith Kamath Belman

Email: amith.kamathbelman@sjsu.edu
Office: DH 251

Office Hours

Monday, 9:00 AM to 11:00 AM, online via Zoom

(Requires zoom SJSU Login)

https://sjsu.zoom.us/j/85711967061?pwd=gvVgXsPej2YG8739kJe3oBCIDW2490.1
Password: 266658

Course Information

Lecture

Tuesday, Thursday, 10:30 AM to 11:45 AM, Interdisciplinary Science 870

Course Description and Requisites

Advanced topics in the area of information security. Content differs with each offering. Possible topics include, but are not restricted to: Network Security, Software Reverse Engineering and Cryptanalysis.

Prerequisite(s): CS 166 and Graduate standing. Allowed Declared Major: Computer Science, Bioinformatics, Data Science. Or instructor consent.

Letter Graded

Classroom Protocols

Regular attendance is an integral part of the learning process. Please arrive to class on time and make sure your cell phones are silent during the lecture.

Class time will be spent in interactive lecture. You are required to bring your wireless laptop to class. Your laptop must remain closed except for designated activities.

This class is designed with a heavy emphasis on peer learning. Many sessions are spent with peers presenting their work as a method of knowledge sharing. Students are expected to be respectful and courteous in all such interactions.

Recording and Privacy

Recording any class activities, including lectures, is only allowed with the instructor's permission. You are not permitted to share or distribute class recordings. Instructor-generated materials (like syllabi, lectures, and presentations) are protected by copyright. Violation may result in referral to Student Conduct and Ethical Development office.

Program Information

Diversity Statement - At SJSU, it is important to create a safe learning environment where we can explore, learn, and grow together. We strive to build a diverse, equitable, inclusive culture that values, encourages, and supports students from all backgrounds and experiences.

Course Goals

Through this course on applied biometric security, the students will:

- Understand the basics of biometric security.
- Learn feature extraction from popular biometric data such as fingerprint, face, gait, keystrokes, iris etc.
- Evaluate suitable similarity measures for biometric data.
- Learn vulnerabilities of biometric security systems.
- Gain hands-on experience on implementing a biometric system.
- Critically evaluate recent published literature and develop a research paper.

Course Learning Outcomes (CLOs)

At the completion of this course, students will be able to:

- Explain foundational principles underlying biometric security systems.
- Develop algorithms for feature selection and authentication using biometric data.
- Evaluate literature in the vulnerabilities of biometric security systems and vulnerabilities in algorithms.

- Explain and develop spoofing attacks on basic biometric authentication systems.
- Develop a deep and comprehensive final paper.

Course Materials

Research papers

- There is no text book for this course. All material is from research publications in conferences or journals.
- PDF copies of research publications and notes will be provided on canvas.

Software

- Any programming language with strong support for ML and AI libraries (Python or Weka or R or MATLAB).
- Students are expected to provide a working demonstration of their project by the end of the semester.

Datasets

- Sample datasets will be provided for initial discussions. (Student projects can be based on datasets outside of those provided)
- Sources for open source datasets will also be shared.

Course Requirements and Assignments

Quizzes

There are 2 quizzes throughout the course covering recently discussed topics. Quizzes will be conducted on canvas during class time.

Midterm Exam

There is one midterm exam that will take place in the classroom during class time. This is a handwritten exam to be submitted on paper.

Final Exam

The final exam is scheduled according to the SJSU Final Exam Schedule, on Friday, December 13th, 9:45 AM-12:00 PM.

This is a handwritten exam to be submitted on paper.

Assignments

There are two written assignments. The assignments are a mix of mathematical problems that require solving by hand and coding-based questions that require various ML operations to be performed on biometric datasets. For implementation-based questions students can use any coding language to clearly demonstrate the requirements. Screenshots, code, and clear explanations are required for each task. All work must be done individually. Violating this will result in an assignment grade of zero and possible academic dishonesty penalties.

Late submissions are not accepted.

Tentative topics for assignments:

Assignments	Points/Percent
Assignment 1 – Biometric modalities, performance measures and analysis, limitations, spoofing attacks, fingerprints and face recognition. Implementation of feature extraction and similarity metrics.	100 pts (10%)
Assignment 2 – Classification systems, Attacks and Evaluation ROC and DET curves, Speaker verification, ECG, PPG and spoof prevention mechanisms.	100 pts (10%)

Project and Research paper

As the course progresses students, either individually or as groups of two, must chose a topic for further exploration and pose a clear problem statement to be solved within the semester's time frame. Deliverables include detailed research paper (ACM or IEEE conference format), periodic presentations, results, code, dataset (if any) and reference papers.

Attendance

You are expected to attend all class meetings as you are responsible for all the material discussed. Active participation is essential to ensure maximum benefit. If students are absent from class, it is students' responsibility to check on announcements made while students were absent.

There are certain presentation days when student groups are assigned to present their project proposals and final projects. The students must attend and present their work on the assigned dates. No rescheduling is allowed without compelling reasons and permission from the instructor.

✔ Grading Information

The final grade in the course will be calculated based on the assignments, quizzes, midterm and final exam and project . No extra credit options will be given

Note: no make-up exams or quizzes, except emergency cases verified with official documents.

Late Work

Late work will not be accepted unless an emergency occurs, and an extension has been approved.

Academic Dishonesty

Students who are suspected of cheating will be referred to the Student Conduct and Ethical Development office and depending on the severity of the conduct, will receive a zero on the assignment or a grade of F in the course. Grade Forgiveness does not apply to courses for which the original grade was the result of a finding of academic dishonesty.

Criteria

Type	Weight	Topic	Notes
Homework Assignments	20%		
Quizzes	5%		
Midterm Exam	20%		
Final Exam	20%		
Project	35%		Includes project presentation, demonstration and report/paper submission.

Breakdown

Grade	Range	Notes
A +	98 to 100%	
A	93 to 97.99%	
A -	90 to 92.99%	
B +	87 to 89.99%	
B	83 to 86.99%	
B -	80 to 82.99%	
C +	77 to 79.99%	
C	73 to 76.99%	
C -	70 to 72.99%	

Grade	Range	Notes
D	60 to 69.99%	
F	below 60%	

University Policies

Per University Policy S16-9 (PDF) (http://www.sjsu.edu/senate/docs/S16-9.pdf), relevant university policy concerning all courses, such as student responsibilities, academic integrity, accommodations, dropping and adding, consent for recording of class, etc. and available student services (e.g. learning assistance, counseling, and other resources) are listed on the Syllabus Information (https://www.sjsu.edu/curriculum/courses/syllabus-info.php) web page. Make sure to visit this page to review and be aware of these university policies and resources.

Course Schedule

Tentative Course Schedule

When	Topic	Notes
Week 1, Aug 22	Course Logistics, Introduction, Syllabus Review	Pre-course survey and Take-home syllabus quiz. Research papers will be added in this column of the syllabus over the semester.
Week 2, Aug 27, 29	Basics, Working of a Biometrics system,	
Week 3, Sept 3, 5	A physiological biometric system- Speed run, Fingerprint as a biometric	
Week 4, Sept 10, 12	Fingerprint as a biometric, Facial recognition systems	Sept 12th Assignment 1- Due Oct. 4th.
Week 5, Sept 17, 19	Facial Recognition Systems and Exercises	
Week 6, Sept 24, 26	Proposal Presentations	4 groups 24th, 4 groups 26th
Week 7, Oct 1, 3	Proposal Presentations, Performance Evaluation	4 groups on Oct 1

When	Topic	Notes
Week 8, Oct 8, 10	Feature definition, extraction and reduction for multimodal biometric, Quiz 1, Review for Midterm	Quiz 1 on Oct 10th.
Week 9, Oct 15, 17	Midterm Exam, IRIS, Hand Geometry, Retinal scanning as authentication	Midterm Exam on Oct 15th.
Week 10, Oct 22, 24	Behavioral biometrics – Keystrokes and Gait .	
Week 11, Oct 29, 31	Foundational Classifiers, Continuous Authentication.	
Week 12, Nov 5, 7	Attacks on Biometric System	Nov. 5 Assignment 2- Due Nov. 20th.
Week 13, Nov 12, 14	Attacks on Biometrics systems, Data poisoning methods	
Week 14, Nov 19, 21	Security for biometrics, Quiz 2, Review	Quiz 2 on Nov 21
Week 15, Nov 26	Final Project Presentations	4 groups
Week 16, Dec 3, 5	Final Project Presentations	4 groups Dec. 3, 4 groups Dec. 5
Final Exam	December 13th, 9:45 AM-12:00 PM.	Research paper submission due Dec. 10th