SJSU SAN JOSÉ STATE UNIVERSITY

College of Science · Computer Science

Biometric Security with AI

CS 228

Fall 2025 Section 01 In Person 3 Unit(s) 08/20/2025 to 12/08/2025 Modified 08/19/2025

Contact Information

Instructor: Dr. Amith Kamath Belman

Email: amith.kamathbelman@sjsu.edu
Office: MH 411

Office Hours

Tuesday and Thursday, 1:30 PM to 2:30 PM, In person at MH 411

Course Information

Lecture

Tu Th 3:00PM - 4:15PM
DH 450

Course Description and Requisites

Applied biometric security with AI and ML, including biometrics systems, such as fingerprint, face, Iris, palm, gait, keystroke. Machine Learning and Deep Learning driven authentication and analysis. Security of ML approaches, data poisoning attacks and spoof resistant systems. A substantial course project is required.

Prerequisite(s): CS 171 or instructor consent. Graduate student standing in Computer Science, Bioinformatics, Data Science. Or instructor consent.
Grading: 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

This course aims to:

- Provide a comprehensive understanding of biometric security concepts.
- Enable students to analyze vulnerabilities and security risks in biometric systems.
- Equip students with practical skills in designing, implementing, and testing biometric security systems.
- Foster the ability to critically evaluate recent research in biometric security and develop the skills to write and present research papers on advanced topics in the field.

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.

Other Readings

- (Optional) Introduction to Biometrics, Anil K. Jain , Arun A. Ross , Karthik Nandakumar , Thomas Swearingen. Springer Cham, ISBN: 978-3-031-61675-4.
- (Optional) Introduction to Machine Learning with Applications in Information Security, Mark Stamp, CRC Press, ISBN: 9781032207179

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 Culminating Activity

The final research paper must be submitted by 2:30 PM on Dec 11th as part of final culminating activity for the course.

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.

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 found 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	25%		
Quizzes	10%		
Midterm Exam	25%		
Project	40%		Includes project proposal presentation (5%), final presentation and demonstration (15%) and research paper submission (20%).

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%	
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

Date	Day	Topics	Research papers and Other Information
21-Aug	Thur	Course Logistics, Introduction, Syllabus Review	
26-Aug	Tue	Basics math refresher: Distributions, Gradients, Hough Transforms, ML concepts, Feature definition, Extraction and Reduction, Foundational Classifiers	
28-Aug	Thur		
2-Sep	Tue	Foundational Classifiers, and Neural Networks	
4-Sep	Thur		
9-Sep	Tue	Neural Networks, Performance Evaluation, Working of a Biometric System	Assignment 1 Due Oct 9th
11-Sep	Thur		
16-Sep	Tue	Fingerprint as a biometric, Facial Recognition Systems	
18-Sep	Thur		
23-Sep	Tue	Proposal Presentations	
25-Sep	Thur		
30-Sep	Tue	Proposal Presentations,	
2-Oct	Thur		
7-Oct	Tue	IRIS and Hand Geometry, Retinal Scanning, Continuous Authentication	
9-Oct	Thur		

14-Oct	Tue	Continuous Authentication	
16-Oct	Thur	Quiz and Midterm Review	Quiz 1, Oct 16th
21-Oct	Tue	Midterm Exam	
23-Oct	Thur	Midterm discussion, Behavioral Biometrics	
28-Oct	Tue	Behavioral Biometrics, Intro to attacks on Biometric Systems	
30-Oct	Thur		
4-Nov	Tue	Attacks on biometric systems: Presentation attacks, Frog boiling attacks, Federated learning vulnerabilities	Assignment 2 Due Dec 2nd
6-Nov	Thur		
11-Nov	Tue	Veteran's Day - Campus Closed	
13-Nov	Thur	Attacks on biometric Systems: Data poisoning attacks, security for biometrics	
18-Nov	Tue	Attacks on biometric Systems: Data poisoning attacks, security for biometrics, Review	
20-Nov	Thur	Quiz 2	Quiz2, Nov 20th
25-Nov	Tue	Final Project Presentations	
27-Nov	Thur	Thanksgiving Holiday - Campus Closed	
2-Dec	Tue	Final Project Presentations	
4-Dec	Thur		
11-Dec	Thur 1:00PM 3:00PM	Final culminating activity- Research Paper Due by 2:30 PM	