Designing and Teaching an Introduction to Mobile-Based Biometrics Elective Course: Initial Observations and Opportunities

Tempestt Neal, Ph.D.

Department of Computer Science and Engineering, University of South Florida, Tampa, Florida, USA

Biometric recognition plays an important role in user authentication, which in turn supports secure access control mechanisms. There is clear need, then, for not only robust authentication measures for secure system and data access, but educated individuals that can implement them. This paper describes the design and implementation of a Mobile-Based Biometrics course implemented at the University of South Florida. This paper describes the course's topics, assignments, and projects, and details the feedback received thus far from students. To our knowledge, this is the only active course focused on mobile platforms; in general, we have found that the relevancy of mobile devices to students' everyday lives helps to maintain student engagement.

Keywords: computer science education, biometrics, curriculum

Introduction

Biometric recognition is the identification or verification (or authentication) of a person's identity according to their physical (Bharadwaj et al., 2014), physiological (Riera et al., 2009), or behavioral (Stylios et al., 2021) characteristics. The National Institute of Standards and Technology (NIST) states that "biometrics, when employed as a single factor of authentication, do not constitute acceptable secrets for digital authentication — but they do have their place in the authentication of digital identities" (Grassi et al., 2017). According to NIST, biometric data can be used to prevent individuals from repudiating authentication registration and to identify enrollment fraud (Grassi et al., 2017). Thus, biometric recognition plays an important role in user authentication, which in turn supports secure access control mechanisms. However, the Cybersecurity and Infrastructure Security Agency (CISA) notes that "weak authentication is a common vulnerability for information systems — it is consistently one of CISA's top five, most frequent findings for Federal High Value Asset systems" (Cybersecurity and Infrastructure Security Agency, 2020). There is clear need, then, for not only robust authentication measures for secure system and data access, but educated individuals that can implement them, corresponding with the growing need for cybersecurity experts (Joint Task Force on Cybersecurity Education, 2018).

The Joint Task Force on Cybersecurity Education, which provides curricular guidance in cybersecurity, notes that essential cybersecurity concepts, including system access, data security, and human security, should be introduced early (Joint Task Force on Cybersecurity Education, 2018). Others have also highlighted the importance of education surrounding system and data access; Švábenský et al. (2020) examined the top cybersecurity education papers in the ACM SIGCSE and ACM ITiCSE conferences; authentication and authorization emerged as popular topics.

Biometrics have reached mass adoption primarily due to its application on commercial mobile devices (Das et al., 2018; Ellavarason et al., 2020), allowing the development of a unique course focused on mobile-based biometrics. This paper describes the design and implementation

of this course, Mobile Biometrics, implemented at the University of South Florida. We describe the course's topics and assignments, and detail student feedback. While similar biometrics courses exist at various universities, to our knowledge, none have a central focus on mobile devices. Although most students associate the course with smartphones, students are exposed to a range of mobile, computing devices (e.g., laptop computers, wearables, tablets, and smartphones). In general, we have found that the relevancy of mobile devices to students' everyday lives helps to maintain their interest, and encourages them to seek knowledge outside of the materials provided in class. Thus, the goal of this paper is to document our strategies, successes, failures, and opportunities, which could later be leveraged more broadly at other institutions, conference workshops, etc.

Related Work

Comparable biometrics courses have been/are currently offered at various institutions. Bowyer (Bowyer, 2004) detailed an undergraduate biometrics elective at the University of Notre Dame to Computer Science and Engineering majors which focuses on current events concerning biometrics and case studies. The course includes term projects covering topics like biometric market potential, personal data derived from biometrics, and algorithms for face segmentation. Another course, Biometric Technology and Applications, has a session-based design at Purdue University (Kukula et al., 2004). The first session overviews biometric technology, the second session covers biometric testing and evaluation, and the third session focuses on large-scale biometric applications such as homeland security. Sessions four through nine focus on specific biometric modalities (e.g., lip, voice, keystroke). Finally, session 10 includes the semester project and lab tests.

The U.S. Naval Academy introduced a biometric signal processing elective course for senior-level Electrical Engineering undergraduate students with an accompanying lab which integrates theories, five guest speakers, demonstrations, seminars, and field trips to the Multimedia Support Center at the Naval Academy, National Security Agency, and the National Cryptologic Museum (Ives et al., 2005). The focus of this course is on image processing and its relation to biometrics. Similarly, the Department of Computer Science at the University of Tennessee Chattanooga Information Security and Assurance concentration supports a course in biometrics (Yang et al., 2008). The course includes hands-on labs using open source software released from the Image Group at NIST for fingerprint recognition, the CSU Face Identification Evaluation system, and the Sphinx group at Carnegie Mellon University for speech recognition.

The Department of Computer Science, Mathematics and Engineering at Shepherd University developed a Biometrics and Security concentration (Liao and Guzide, 2010). Their course, CIS 361 Introduction to Biometrics, is offered to junior or senior Computer and Information Sciences or Computer Information Technology majors. It covers fundamental biometric concepts, including biometrics devices and applications; probability and statistics; fingerprint, voice, face, and iris; information security; and ethics.

Finally, Union College designed a course in Biometric Signal Processing for junior and senior level undergraduate students in Electrical and Computer Engineering (Cotter, 2011) consisting of lectures and a hands-on lab. Through the course, students also hone in on Digital Signal Processing by focusing on speaker recognition systems. Students also develop image processing skills through face and fingerprint recognition systems. Union College later developed the course "Identity and Security in a Technological World" to fit into Union College's general education curriculum (Cotter and Pease, 2013). The course is taught by faculty in the Electrical Engineering

and English departments, leading to an interdisciplinary, socio-cultural look into identity and security, such as the role of biometrics in casinos and banks, biometrics for online transactions, airport security, and online privacy.

Course Organization and Delivery

Mobile Biometrics has been offered by the Department of Computer Science and Engineering during the Fall semester since 2018 at the University of South Florida, a large public university in the southeast United States. Although all enrolled students (undergraduate and graduate) participate together, there is a separate section for undergraduate and graduate course registration. Thus, a total of eight courses have been offered since 2018. The course is held for 75 minutes twice a week over 16 weeks. It is offered in-person, with the exception of the Fall 2020 offering, which was facilitated virtually via Microsoft Teams due to the COVID-19 pandemic. The course aims to develop students' (1) knowledge of biometric foundations; (2) understanding of behavioral and physical biometric modalities; (3) knowledge of data acquisition techniques on mobile platforms; (4) abilities to build and evaluate a biometric system; (5) abilities to relate classwork to published literature; (6) awareness of spoofing and anti-spoofing techniques; and (7) awareness of challenges in commercial systems.

Textbooks and Reading Materials

Mobile Biometrics heavily relies on ongoing research in the field; as such, we found it difficult to decide on a single textbook for the course over the years. Two textbooks that have been used consistently thus far include:

- Jain, Anil K., Arun A. Ross, and Karthik Nandakumar. Introduction to biometrics. Springer Science & Business Media, 2011.
- Guo, Guodong, and Harry Wechsler, eds. Mobile Biometrics. Vol. 3. IET, 2017.

Other materials are provided via scientific research articles and news articles available via the web.

Enrollment

Figure 1 shows the student enrollment over the past four years, including first day, after six weeks, and final headcounts (the university course withdrawal policy includes a mandatory first day of attendance, a week-long drop/add period during the first week of the semester, and a course withdrawal deadline around the midpoint of the semester). The seat caps for undergraduate and graduate sections are 40 and 20 students, respectively. Figure 1 shows a steady increase in enrollment for the undergraduate section, with an expected increase to nearly 45 students (given an increase in the seat cap) in the Fall 2022 section according to a linear forecast. There is also strong retention of undergraduate students throughout the semester, with at most two students withdrawing from the course during the Fall 2020 offering. On average, the undergraduate course enrollment decreases by one student each year.

The graduate-level course shows less consistency in retention, with an average decrease in enrollment post first day of 3.5 students. Some students have expressed the need to drop the course due to scheduling conflicts, alternative learning opportunities (e.g., internships), employment conflicts (e.g., teaching assistantships), unfamiliarity with the Python programming language, initial

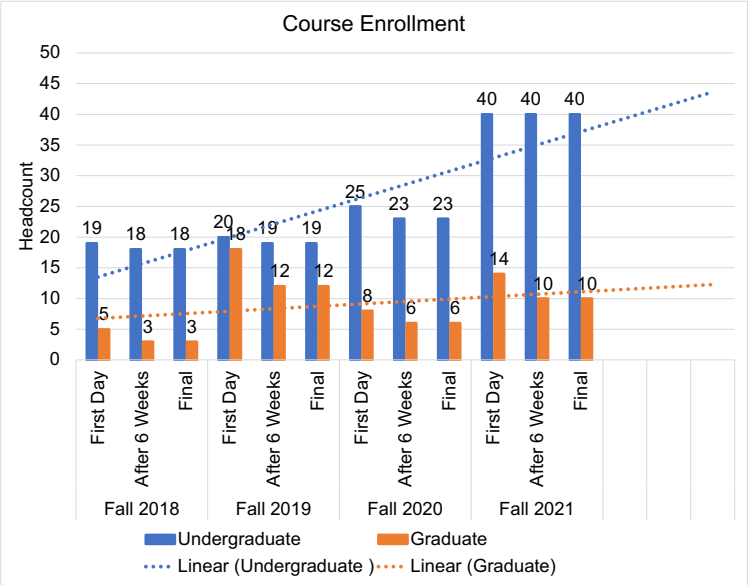

Figure 1: Undergraduate and graduate student headcounts over the past four years in Mobile Biometrics.

		Y1	Y2	Y3	Y4
UG	Avg. Grade	89.95	91.27	87.08	91.66
	No. of Assignments	12	22	20	15
G	Avg. Grade	83.94	94.35	95.95	96.45
	No. of Assignments	14	22	20	15

Table 1: Average grades and number of assignments.

intimidation of the course project, and the need to register for another course to meet graduation requirements.

Course Assignments

The breakdown of the semester by topic and assignments is outlined in Table 2. The majority of instructional time (approximately 6 of 16 weeks) is dedicated to introducing the fundamentals of biometric systems and programming in Python. Two weeks are dedicated to teaching face recognition. One week is generally dedicated to other topics, including motion and gait recognition, keystroke dynamics and touch gesture recognition, user-device interaction recognition, fingerprint recognition, spoofing and attack countermeasures, and practical and commercial considerations. Remaining instructional time are dedicated to exams, project presentations, and in-class project work groups. Table 1 shows the average grades and number of assignments for each course so far; this table shows consistently good grades, with 17 assignments per course on average.

Topic	*Assignment(s)*	*Time*
Introduction to biometric systems; Multimodal biometric systems; Evaluating the performance of biometric systems	Reading relevant research articles (e.g., (Jain et al., 2011, 2004; Ross et al., 2008; Neal and Woodard, 2016; Patel et al., 2016; Meng et al., 2015)) and Q&A (e.g., defining concepts, comparing biometric modalities for different use cases, discussion on continuous authentication, etc.)	2-3 weeks
Introduction to programming in Python and scikit-learn for machine learning	Plotting score distributions, ROC curves, and DET curves in Python using randomly generated data	2-3 weeks
Motion and gait Recognition (vision, floor pressure, and sensor-Based Systems, with emphasis on accelerometer and gyroscope-based approaches)	Reading relevant research articles (e.g., (Gafurov et al., 2006)); Preprocessing, normalizing, and computing the magnitude vector of gait data	1 week
Keystroke dynamics and touch gestures	Introduction to variance-based feature selection (self-learning) on touch data	1 week
User-device interaction (e.g., mobile app use) for mobile biometrics	In-class discussion.	1 week
Face recognition	Implement k-Nearest Neighbors on landmark-based facial features, report performance on changing k. Compare with a Naive Bayes classifier. Implement PCA for face recognition.	2 weeks
Fingerprint recognition	Implement the Zhang Suen thinning algorithm in Python.	1 week
Spoofing and adversarial attacks and countermeasures	Create a lecture on adversary attacks.	1 week
Practice considerations	In-class discussion and Ted talk development.	1 week

Table 2: Topics and corresponding course assignments covered throughout the semester.

Course Modules and Assignments

Weeks 1-6: Biometric Systems and Python

The first several weeks of the course introduces students to biometric systems; frequently referenced literature are cited here: (Jain et al., 2011, 2004; Ross et al., 2008; Neal and Woodard, 2016; Patel et al., 2016; Meng et al., 2015). Students discuss advantages and disadvantages of knowledge-based, token-based, and biometric authentication systems, and learn the components of biometric systems (i.e., data collection, feature extraction, enrollment, matching, and decision). Classifications of biometric systems are introduced (e.g., cooperative/non-cooperative, overt/covert, habituated/non-habituated, attended/non-attended, controlled/uncontrolled, open/closed), and students discuss how these classifications apply to mobile platforms. Students are also introduced to the seven properties of biometric systems (e.g., universality, uniqueness, permanence, measurability, performance, acceptability, and circumvention). We discuss both physical and behavioral modalities most suitable/researched for mobile platforms, including those facilitated by physical, environmental, movement, location, and interactive sensing.

The first few weeks are also dedicated to classification and machine learning algorithms. Students are taught fundamentals such as features/attributes/predictors, supervised learning, feature spaces, viewing images as a collection of pixels, and simple classification algorithms such as k-Nearest Neighbors (selecting k and a distance metric) and thinking about classification in terms of probabilities using Bayesian classification.

Finally, students are taught how to measure the performance of biometric systems, and how to plot performance plots using Python. Students are introduced to many standard performance measures (selecting a decision threshold, computing false positives and negatives and true

positives and negatives, computing performance rates, Receiver Operating Characteristic and Detection Error Tradeoff curves, and score distribution plots). Students are provided starter code to facilitate plotting in Python.

Weeks 7-9: Behavioral Biometrics

About three weeks are dedicated to behavioral biometrics, including motion and gait recognition, touch/keystroke dynamics, and user-device interaction. Students are exposed to vision, floor sensors, and wearable sensor-based gait approaches, with emphasis on the latter. Sensors such as accelerometers and gyroscopes are discussed in detail. Keystroke dynamics on varying input mechanisms (QWERTY keyboards of different sizes, 3D keyboards, capacitive touch keyboards), along with keystroke dynamic and touch gesture features are discussed. The Android API for detecting multi-touch events are brought to students' attentions. Some semesters have also included materials on user-device interaction, i.e., patterns associated with the user's interaction with the services on their devices (e.g., application use, call and text messaging patterns) with supporting related literature (e.g., (Neal et al., 2015)).

Weeks 10-12: Physical Biometrics

Lectures on physical biometrics focus on face and fingerprint recognition. Face recognition lectures define levels 1, 2, and 3 facial features (easily observed features, local information, and micro-level features, respectively), and introduce appearance, model, and texture-based face modeling approaches (Jain et al., 2011). We cover Principal Component Analysis (PCA), Elastic Bunch Graph Matching, and Local Binary Patterns (LBP); students are provided with starter Python code to implement PCA and LBP. Importantly, these lectures focus significantly on intra-class and inter-class variations (illumination, occlusions, facial expressions, etc.); students discuss problems related to such variations specific to mobile devices by examining images like those in Figure 3, which helps generate ideas for their projects.

On the topic of fingerprint recognition, lectures begin with a discussion fingerprint ridge development, data collection via capacitive touchscreens, and levels 1, 2, and 3 fingerprint features – that is, ridge orientation and singular points, the ridge skeleton and minutiae points, and information embedded within the fingerprint ridges (Jain et al., 2011).

Week 13: Attacks Against Biometric Systems

Students are provided instructions on developing a presentation consisting of the following content:

(1) A summary of Chapter 7 in *Mobile Biometrics* (Guo, 2017)
(2) Labeling of the attack points of a biometric system using the articles below:
    - *Biometric Attack Vectors and Defences* (Roberts, 2007)
    - *Biometric Authentication: System Security and User Privacy* (Jain and Nandakumar, 2012)
(3) Summary of key findings in *Snoop-Forge-Replay Attacks on Continuous Verification With Keystrokes* (Rahman et al., 2013)
(4) Summary of key findings in *Walk the Walk: Attacking Gait Biometrics by Imitation* (Mjaaland et al., 2011)

Figure 2 shows an example slide of one student.

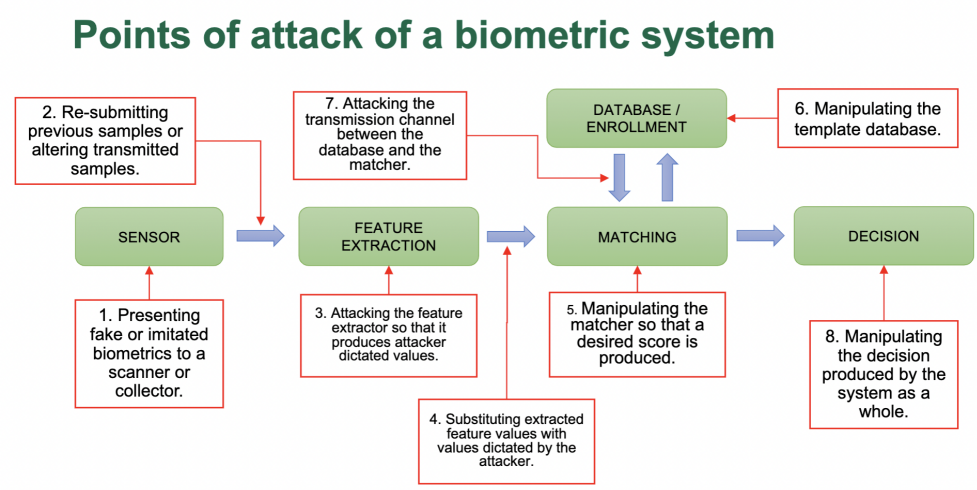

Figure 2: An example slide of the attack points in biometric systems produced by a student enrolled in the Fall 2021 course.

Week 14: Practical/Commercial Considerations

Students are assigned a self-learning assignment at the close of the course concerning real-world considerations. They are instructed to watch one of three Ted Talks. Thus far, students have been assigned the following talks to watch with a group of their peers: (1) J. Buolamwini's *How I'm Fighting Bias in Algorithms*[1]; (2) T. Wang's *Human Insights Missing from Big Data*[2]; (3) S. Suwajanakorn's *Fake Videos of Real People — and How to Spot Them*[3].

After watching the video, groups are tasked with commenting on what they learned from the talk, the presenter's presentation skills, and how they feel the talk's content relates to the course. The group then decides on a current topic in biometrics on which to develop a similar "Ted" talk, mimicking the presentation quality and presenter's delivery of the actual Ted talk they watched in advance using materials from a variety of credible resources (e.g., academic research articles, credible news sources, professional blogs, published statistics, textbooks, etc.).

Course Projects

Year 1

The goal of the project for Year 1 was to allow students to implement a behavioral biometric system. Students were tasked with working in a group (group members were assigned) to explore the research literature, develop their project idea, and then implement the idea. After exploring published research literature, students had to propose a project inspired by their readings addressing some identified challenge. The project had to include two or more of the following: data preprocessing, enhancement, or noise reduction; feature selection; machine learning; multimodal

[1] https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms?language=en

[2] https://www.ted.com/talks/tricia_wang_the_human_insights_missing_from_big_data?language=en

[3] https://www.ted.com/talks/supasorn_suwajanakorn_fake_videos_of_real_people_and_how_to_spot_them?language=en

(a) Example of multiple people in the frame, facial occlusions, and bright lighting.

(b) Example of extreme facial expression outdoors.

(c) Example of windy conditions.

(d) Example of extreme facial expressions indoors.

Figure 3: Example images provided during lecture that stimulate discussion on intra-class and inter-class variations, particularly deriving from use of personally owned computing devices in different environments.

biometrics; or feature, score, or decision fusion. Importantly, the projects required an independent variable (e.g., subject's gender) with a dependent variable of authentication performance. Students were provided with publicly available data to complete their projects (i.e., keystroke dynamics (Killourhy and Maxion, 2009) and gait (Casale et al., 2012)).

Year 2

Feedback from Year 1 led to changes in the project for Year 2; namely, allowing students to collect data on their own. In Year 2, students were tasked with developing a face recognition system using face images from their group members. Students were instructed to capture 25 30-second videos exhibiting variations in lighting, pose, facial expressions, distance from the camera, and occlusions. Frames were extracted to create a face image dataset.

Students built upon their prior homework assignments on PCA and LBP for feature extraction, and assignments requiring k-NN and Naive Bayes classifiers for matching. They also used prior assignments where they wrote code to assess the performance of a biometric system to analyze their systems. In essence, this project was a collection of prior assignments, but with a more hands-on experience for students in the data collection process. They had to implement some unique component not already explored in the course, like using certain images to analyze certain forms of intra-person variation.

Year 3

Students positively responded to the project in Year 2, so very few changes were made in the subsequent year. In Year 3, instead of using only the group's images, students were provided access to the dataset representative of the entire class. Further, students were allowed to pick their group members. They were also provided greater agency over the capabilities of their developed face recognition systems; students were encouraged to develop their projects around sound research questions, using their choice of train/test splitting of the data (e.g., k-fold cross validation, leave-one-out cross validation, etc.), pre-processing techniques, and/or incorporating fusion.

Model	Hyperparamters	Data Transformers	Accuracy
ViT	1e-5 learning rate	n/a	6%
ResNet	1e-5 learning rate	n/a	0%
FCC	2e-2 learning rate, 32*32 image size	Grayscale	100%
KNN	5 neighbors, 250*250 image size	Blur	74.6%
Random Forest	Gini impurity, 250*250 image size	Blur	73.2%
SVM	rbf kernel, 250*250 image size	Grayscale	77.3%
Voting Classifier	hard voting, 250*250 image size	Grayscale	78.03%
Voting Classifier	hard voting, 92*112 image size	Grayscale,Blur,Face Capture	90.00%

Table 1: Overall results of all models, hyperparameters listed were found to be optimal.

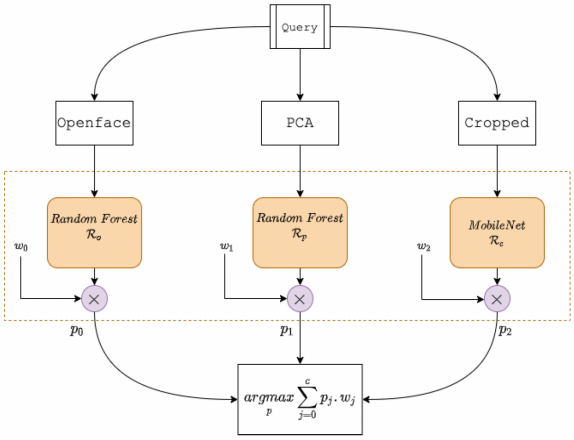

Figure 2: Ensemble architecture: The openface, PCA and aligned features are first extracted from the query image. These features are then fed to their corresponding models they were trained on. Each model has a weight attached to it

Figure 4: Examples of content provided in students' project reports reflecting use of more sophisticated technologies.

Year 4

We continued to observe the project's positive impact on engagement and learning. Students appreciated the flexibility of the project, along with developing a security-focused system that they would have otherwise not been able to explore outside of this course. Thus, we continued the project into Year 4, with subtle changes. These included instructing students to capture photos instead of videos, and manipulating some of their photos with artistic effects and filters — that is, attention for the Year 4 project was placed on images that might be acquired through apps such as Snapchat, an instant messaging service that offers dozens of filters and lenses for its users to overlay on their images. Notably, we observed that more students used more sophisticated techniques, including deep learning, data augmentation, use of OpenFace[4], ensemble methods, etc. Figure 4 depicts two of such cases.

The Literature Review

In Year 2, we tested out the requirement of a literature review as a way of immersing students more deeply into ongoing research. Students could choose among the following topics for their review:

[4] `http://multicomp.cs.cmu.edu/resources/openface/`

2D and 3D Face; Fingerprint; Voice; Gait/Movement/Motion; Touch/Swipe Gestures; Keystroke Dynamics; Physiological Measurements (e.g., wearables).

After Year 2, we realized most undergraduates were struggling to keep up with the pace of developing a literature review in a single semester. While we paired undergraduates with a graduate student to allow the gradaute student to serve in a leadership role throughout the review's development, the fact that undergraduates outnumbered the graduate students nearly 2:1 and many graduate students did not have significant prior writing experience, this assignment was taxing and distracting for students.

In Year 3, we adjusted the assignment to be an optional, extra credit component for undergraduates and a requirement for graduate students. Topics included: heartbeat-based biometrics; channel state information-based biometrics; Internet-of-Things (IoT)-based biometrics; wearable sensor-based biometrics; electroencephalogram-based biometrics; electromyogram-based biometrics; and electrooculogram-based biometrics. We noticed only one undergraduate student participated in Year 3. However, the literature reviews produced by the graduate students were better quality compared to Year 2, with the caveat of being shorter in length (5 to 12 pages) since for all but one, they were written by a single author. Nonetheless, we have observed that the literature review assignment was overwhelming for students, and took away from students focusing on some of the more hands-on components of the course (e.g., the project). We did not implement the literature review in Year 4, but are considering alternatives for future course offerings (e.g., requiring more detailed Related Works sections in the project reports).

Student Feedback

Undergraduate Student Comments

Our institution's administered assessment of instruction has accumulated a breadth of student ratings and comments that have been used to alter the course delivery over time. Overall, the course has been well received, and has been described as "*...one of the coolest electives I've taken...*". Another student wrote that they "*really loved this class and I'm so glad I took it, one really interesting elective that should definitely be offered more. I think it gives insight to a technology that has become so ubiquitous around us and really makes use of a lot of concepts learned in earlier classes like statistics and linear systems.*" Another student noted that the course connects "*boring concepts like normal distributions*" to "*cool things later on*", and as a result, "*should be shown to more pre-CS majors*".

However, some students have voiced concerns with some course requirements. One student enrolled commented "*I hate that we had a literature review. I don't plan on doing research so this all felt pointless and tedious.*" The following year, the literature review assignment was made optional for undergraduate students as additional complaints were expressed during class time; in short, many undergraduate students were unfamiliar with a literature review and its writing process, and felt it was too time consuming considering undergraduate students typically have more courses than graduate students. However, one student commented "*this course was unfair to undergraduate students because we had the exact same assignments as Masters/PhD students. The one difference was a "Literature Review" which was optional but encouraged for undergraduate students.*" Another student commented on the course's use of machine learning: "*I thought this was a cyber security course. This is a machine learning course and I wish I had that background*

knowledge before because my computer could not handle the huge datasets that we sometimes needed for processing in this class. I wish it was more clear during the first week that this course would be heavy on machine learning/Artificial Intelligence and research papers."

Some students offered recommendations to improve the course. Multiple students disliked being assigned their group members; "*...let us pick our groups and not assigned us groups.*" Other students wanted more hands-on assignments; "*...try to incorporate a bit more hands on stuff instead of the pure mathematical statistics, like trying to see if someone can fool a fingerprint reader and make it like extra credit.*" "*An extra hands-on project or a larger-scale project instead of a Literature Review might have been more useful for the future of students and would have made the class even more interesting.*" "*This field of computer science should be more hands-on with in-lab experience with biometric systems.*"

Graduate Student Comments

Similar to the undergraduate section, graduate student comments reflected a positive view of the course overall. One student wrote "*Quite literally, the only class I have had so far at USF that is fun to go to. The only class whose assignments I do immediately because they don't feel torturous to go through.*" Another commented "*The class was very interesting. I learned a lot in it, and could definitely see myself using the concepts learned in this course in the future.*" Another student wrote "*Mobile Biometrics is a course that helped me gain a lot of insights into the biometric authentication domain. All the theory and practical assignments of the class made it easier to understand the topic sustaining interest in the subject throughout the semester.*"

Perhaps due to fewer enrolled graduate students, comments recommending significant course changes or strong dislikes for course content were not provided. However, one of the more difficult aspects of this course is deciding how much guidance to provide to appropriately match the expectations of undergraduate and graduate students simultaneously. Thus far, students are provided Python code that require their edits. This mostly targets students with no Python programming experience. However, one graduate student preferred to "*[write] code from scratch rather than editing on the given code.*"

Discussion

Mobile Biometrics focuses on a unique security topic that has generated increasing interest and participation since its launch. This section details observed challenges thus far, and opportunities to enhance the course in coming years.

Challenges

One open challenge is understanding why graduate students drop the course at a greater rate than undergraduates. We hypothesize that by increasing graduate student retention, this could potentially increase the number of graduate students seeking Ph.D. degrees (thus far, most graduate students enrolled in the course are Masters students).

Another challenge encountered thus far is how to appropriately design assignments that challenge both undergraduate and graduate students. To separate the learning objectives at each level, additional questions in assignments have been assigned for graduate students, graduate stu-

dents have been assigned a literature review, and graduate students have been assigned additional assignments. However, there has yet to be a solid approach to achieve the desired balance — that is, engaging, understandable, and rigorous material for both undergraduate and graduate students. The most promising solution thus far was implemented in Fall 2021, where the grading scheme for the project was weighted to account for the make-up of the student groups (e.g., all graduate students versus all undergraduates).

Third, this course is not designed to leverage existing Python programming skills. A significant amount of instructional time is dedicated to encouraging comfortability with Python. In addition, assignments requiring programming are accompanied with starter code to assist with the assignment's successful completion. Overall, student feedback reflects an appreciation for providing code in advance and demonstrating code during class time. However, some students fail to truly translate their knowledge of programming more generally to the specific language of Python. This could be attributed to working with data types/sources that students have not worked with in the past (e.g., images, accelerometer readings, etc.), using a new language to develop an entire project, etc.

Further, like Mobile Biometrics, similar courses have found no single textbook covering the scope of material being taught (Ives et al., 2005). For example, Sánchez et al. (2014) offered a Biometrics course to Computer Science, Telecommunications, and Mathematics students; they advised for enrolled students to have a background in digital image processing, pattern recognition, statistics, and mathematical fundamentals — a wide scope unlikely to be found in a single textbook. As such, we have heavily relied on published academic literature as reading material. However, this presents a challenge with interpretability; while some articles used in the course are outdated, they are skillfully written and are easy to read. A challenge is identifying relevant, recently published literature that is appropriate for novice learners.

Opportunities

Hands-On Learning

Similar courses include a lab (e.g., (Ives et al., 2005; Yang et al., 2008; Liao and Guzide, 2010)). The Cyber Identity and Behavior Research Lab at the University of South Florida, housed in the Department of Computer Science and Engineering, has incrementally acquired mobile devices (smartphones, laptops, tablets, and wearables) over the past four years which could potentially support hands-on learning experiences in Mobile Biometrics should we continue to acquire devices. In addition, the Cyber Identity and Behavior Research Lab is purposefully designed to allow data capture in a home-like environment (see Figure 5), which could encourage students to ideate around the concept of smart homes and personal computing devices typically used at home. Some students have already noted the desire for such a lab as discussed in Section 4.

Dataset Development

Thus far, 131 students have enrolled in Mobile Biometrics. We have explored the idea that by engaging in conversations on the significance of data collection, students might be inclined to allow their data collected for course projects to be used by the broader research community. While we obtained Human Subjects Approval (#Pro00041935) from our Institutional Review Board starting the Fall 2019 semester to request and store course data, we have not been successful at doing so.

Figure 5: Cyber Identity and Behavior Research Lab set up at the University of South Florida that is now equipped with mobile devices that can be used as a lab for Mobile Biometrics.

We can only request data after the course has ended to not cause any undue pressure for students to consent to data sharing. However, we find that very few students respond to these requests after the semester has ended. Nonetheless, given the popularity of the course, this could be a source of research data under improved, though currently identified, means to contact students after the conclusion of the course.

Recruiting Students into Research

Thirty-one graduate students have enrolled in the course since 2018. We have found that this course stimulates important conversations around research, research labs and their ongoing projects at our institution, AI, cybersecurity, image processing/computer vision, usability, and the human aspect of authentication. These are all healthy conversations surrounding graduate-level research-focused degrees. Similar to Kukula et al. (2004), we have recruited three students into the Cyber Identity and Behavior Research Lab, two Ph.D. students and one Supervised Research undergraduate student, and hope to continue doing so.

Applied Research Courses

While this course resembles others, its applicability to mobile platforms distinguishes it from others. Notably, applied research courses provide invaluable *tangible* learning outcomes. "Educators know that students who can see the impact of their work are often more invested in their learning . . . [S]tudents who have a chance at finding those solutions on their own may also feel more empowered, developing a stronger belief in their own abilities and seeing their self-confidence skyrocket" (Barack, 2019). We have observed that students embrace the novelty of the course project, and have a sense of pride when they demonstrate their finished projects. Further, we find that students appreciate the uniqueness of the course's topic area; while it certainly builds on prior core courses and skills, it stands on its own as a computing course with real-world application. Our

hope is that its design can influence other applied research courses.

Collaborating with Complementary Courses

We see an opportunity to collaborate with complementary courses like Deep/Maching Learning, Artificial Intelligence, Affective Computing, Computer Vision, etc. for the course project. Since these areas are closely married, it could allow students enrolled in Mobile Biometrics to, for example, learn a skill in one of the other courses (e.g., Support Vector Machines in Machine Learning or an image processing skill in Computer Vision) that can be applied to their course project. Ideally, this would increase interest in graduate research and increase the complexity of course projects.

Guest Lectures

Comparable courses include guest lectures (e.g., (Kukula et al., 2004; Ives et al., 2005)). While Mobile Biometrics has yet to do this, we plan to do so in the future, intentionally seeking three guest lecturers per course, each representing a prominent person from academia, industry, and government. We have found that students often ask questions during class about each of these sectors.

Mobile-Based Biometric Applications

Many research articles are emerging that are not primarily focused on authentication or identification, but rather on the application of mobile-based biometrics as a proxy of, for example, behavior before and after some intervention (e.g., (King et al., 2022)). There is an opportunity to incorporate such applications into the course material through revised lectures, guest speakers, or course projects supervised by both the course instructor and a researcher working in the domain at hand.

Conclusion

This paper details Mobile Biometrics, an elective that introduces students to mobile-based biometrics. This course has generated increasing interest, reflected by growing enrollment trends and consistently positive course reviews. However, there remains work to be done to achieve balance in appropriately supporting both undergraduate and graduate learners, in addition to improving the course through lab activities, guest lectures, a curation of research literature, among others.

References

Barack, L. (2019, Feb). Seeing tangible outcomes builds deeper student stem engagement. https://www.k12dive.com/news/seeing-tangible-outcomes-builds-deeper-student-stem-engagement/547510/. K-12 DIVE.

Bharadwaj, S., M. Vatsa, and R. Singh (2014). Biometric quality: a review of fingerprint, iris, and face. *EURASIP journal on Image and Video Processing 2014*(1), 1–28.

Bowyer, K. (2004). An elective course in biometrics and privacy. In *34th Annual Frontiers in Education, 2004. FIE 2004.*, pp. S3E–12.

Casale, P., O. Pujol, and P. Radeva (2012). Personalization and user verification in wearable systems using biometric walking patterns. *Personal and Ubiquitous Computing 16*(5), 563–580.

Cotter, S. and A. Pease (2013). Incorporating biometrics technology into a sophomore level general education course. In *2013 ASEE Annual Conference & Exposition*, pp. 23–729.

Cotter, S. F. (2011). Assessing the impact of a biometrics course on students' digital signal processing knowledge. In *2011 ASEE Annual Conference & Exposition*, pp. 22–245.

Cybersecurity and Infrastructure Security Agency (2020). Capacity enhancement guide: Implementing strong authentication. `https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Implementing_Strong_Authentication_508_1.pdf`.

Das, A., C. Galdi, H. Han, R. Ramachandra, J.-L. Dugelay, and A. Dantcheva (2018). Recent advances in biometric technology for mobile devices. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–11.

Ellavarason, E., R. Guest, F. Deravi, R. Sanchez-Riello, and B. Corsetti (2020, dec). Touch-dynamics based behavioural biometrics on mobile devices – a review from a usability and performance perspective. *ACM Comput. Surv. 53*(6).

Gafurov, D., K. Helkala, and T. Soendrol (2006). Gait recognition using acceleration from mems. In *First International Conference on Availability, Reliability and Security (ARES'06)*, pp. 6 pp.–439.

Grassi, P., J. Fenton, and M. Garcia (2017, 2017-12-01). Digital identity guidelines [including updates as of 12-01-2017].

Guo, G. (Ed.) (2017). *Mobile Biometrics*. Security. Institution of Engineering and Technology.

Ives, R., Y. Du, D. Etter, and T. Welch (2005). A multidisciplinary approach to biometrics. *IEEE Transactions on Education 48*(3), 462–471.

Jain, A., A. Ross, and S. Prabhakar (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology 14*(1), 4–20.

Jain, A. K. and K. Nandakumar (2012). Biometric authentication: System security and user privacy. *Computer 45*(11), 87–92.

Jain, A. K., A. A. Ross, and K. Nandakumar (2011). *Introduction to biometrics*. Springer Science & Business Media.

Joint Task Force on Cybersecurity Education (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY, USA: Association for Computing Machinery.

Killourhy, K. S. and R. A. Maxion (2009). Comparing anomaly-detection algorithms for keystroke dynamics. In *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, pp. 125–134.

King, S. L., J. Lebert, L. A. Karpisek, A. Phillips, T. Neal, and K. Kosyluk (2022, May). Characterizing user experiences with an sms text messaging–based mhealth intervention: Mixed methods study. *JMIR Form Res 6*(5), e35699.

Kukula, E. P., N. C. Sickler, and S. J. Elliott (2004). Adaptation and implementation to a graduate course development in biometrics. In *World Conference on Engineering and Technology Education*. Citeseer.

Liao, W. and O. Guzide (2010). Work in progress: On the development of a biometrics course and its relationship with stem curricula. In *ASEE North Sectional Conference*.

Meng, W., D. S. Wong, S. Furnell, and J. Zhou (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys Tutorials 17*(3), 1268–1293.

Mjaaland, B. B., P. Bours, and D. Gligoroski (2011). Walk the walk: Attacking gait biometrics by imitation. In M. Burmester, G. Tsudik, S. Magliveras, and I. Ilić (Eds.), *Information Security*, Berlin, Heidelberg, pp. 361–380. Springer Berlin Heidelberg.

Neal, T. J. and D. L. Woodard (2016). Surveying biometric authentication for mobile device security. *Journal of Pattern Recognition Research 1*(74-110), 4.

Neal, T. J., D. L. Woodard, and A. D. Striegel (2015). Mobile device application, bluetooth, and wi-fi usage data as behavioral biometric traits. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6.

Patel, V. M., R. Chellappa, D. Chandra, and B. Barbello (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine 33*(4), 49–61.

Rahman, K. A., K. S. Balagani, and V. V. Phoha (2013). Snoop-forge-replay attacks on continuous verification with keystrokes. *IEEE Transactions on Information Forensics and Security 8*(3), 528–541.

Riera, A., A. Soria-Frisch, M. Caparrini, I. Cester, G. Ruffini, N. Boulgouris, K. Plataniotis, and E. Micheli-Tzanakou (2009). Multimodal physiological biometrics authentication. *Biometrics: Theory, Methods, and Applications*, 461–482.

Roberts, C. (2007). Biometric attack vectors and defences. *computers & security 26*(1), 14–25.

Ross, A., K. Nandakumar, and A. K. Jain (2008). *Introduction to Multibiometrics*, pp. 271–292. Boston, MA: Springer US.

Stylios, I., S. Kokolakis, O. Thanou, and S. Chatzis (2021). Behavioral biometrics continuous user authentication on mobile devices: A survey. *Information Fusion 66*, 76–99.

Sánchez, A., J. Vélez, A. Moreno, and E. Nunes (2014). Effectively integrating a course on biometrics in a computer vision master's degree. In *IWSSIP 2014 Proceedings*, pp. 43–46.

Švábenský, V., J. Vykopal, and P. Čeleda (2020). *What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences*, pp. 2–8. New York, NY, USA: Association for Computing Machinery.

Yang, L., K. Winters, and J. M. Kizza (2008). Biometrics education with hands-on labs. In *Proceedings of the 46th Annual Southeast Regional Conference on XX*, ACM-SE 46, New York, NY, USA, pp. 18–23. Association for Computing Machinery.