Incorporating Biometrics Technology into a Sophomore Level General Education Course

Dr. Shane Cotter, Union College

Dr. Shane Cotter came to Union College in August 2005 and is an associate professor in the Electrical and Computer Engineering Department. He teaches courses in introductory digital logic, digital design, signal processing, and computer networking. Dr. Cotter's principal research interests are in the areas of speech and image processing, wireless communications, computer networking, and biological signal processing. Prior to joining Union College, he was a visiting assistant professor in the ECE Department at the University of Miami for the 2004-2005 academic year. Dr. Cotter worked at Nokia Mobile Phones as a senior design engineer between 2002 and 2004 in the DSP/Audio group on speech codec implementation and phone acoustic properties. Dr. Cotter received his Ph.D. and M.S. degrees in Electrical Engineering with an emphasis on Digital Signal Processing from the University of California at San Diego in 2001 and 1998 respectively. He received his undergraduate degree in Electronic Engineering from University College Dublin in 1994.

Dr. Anastasia Pease, Union College

Dr. Anastasia Pease is a lecturer in English and an award-winning teacher. Her interests include literature and science, ethics and bioethics, science fiction, second language pedagogy, and cognitive science.

Incorporating Biometrics Technology into a Sophomore Level General Education Course

Introduction

Over the last decade, Union College has been attempting to integrate engineering and technology into the study of the liberal arts and has hosted a Symposium on Engineering and Liberal Education, which is now entering its sixth year. As part of this effort, and with funding from NSF and IBM, we have designed a course titled "Identity and Security in a Technological World" to fit into Union College's general education curriculum as a Sophomore Research Seminar. The course is team-taught by faculty members from the Electrical Engineering and English departments and addresses the implementation and socio-cultural impact of new identification and security systems. The course is taken by engineering and non-engineering students and blends the study of technology with literature (both fiction and non-fiction).

Biometric technology overlaps with language processing, psychology, neuroscience, biology, philosophy, ethics, and is an ideal subject area for inter-disciplinary teaching and discussion. Students in the course have many different majors and have various levels of preparation in mathematics and science. The course has no prerequisites, so it must be taught at a level to allow all students to appreciate the technical aspects of the identification systems. The students are required to come up with a research topic -- related to biometrics, identity, or security -- which they develop into a full research paper by the end of the term.

Since September 11, 2001, there has been an increased emphasis on identification and surveillance systems to enhance security. There has also been an increase in the use of biometric data in passports, border control, and secure private company access. In tandem with this, over the last decade, one's identity (and the need to verify it) has become increasingly digital. Verifying one's identity with a password can now give one access to health and financial information, as well as be used to verify financial transactions (through PayPal or other similar services). Indeed companies such as Facebook and Google, which provide most services free of charge, are largely gathering personal information that can be used for targeted advertising. Biometrics is one way in which one's digital identity can be more securely verified and is becoming more commonly used (e.g., voiceprint in banking telephone access systems).

The technical course content focused on the acquisition and storage of biometric data (handprint, face, fingerprint, and voice data), which are extensively used in personal identification and forensic investigations of crimes. Students learned how current biometric and forensic systems work, and explored their uses, merits, and limitations. Through a collaboration with IBM and its Smarter Planet initiative, a business development executive from IBM explained how current voice identification technology is being developed and used in an industrial setting.

Alongside exploring the technical implementation of these systems, students were also asked to ponder a future world where all biometric and personal data, including genetic and healthcare records, as well as shopping patterns, etc. will be easily accessible in real time. The technologies that allow the tracking of individuals anywhere in the world bring forth questions of

security, privacy, and identity. Reading Science Fiction stories, along with news and science articles, students explored the ethics, the dangers, and the advantages of a Big Brother world.

Course Topics

The course was taught in two class periods of 115 minutes each week in a 10 week trimester term. In lectures, there was a mixture of presentation, experimentation, and discussion on different topics related to biometrics technology, privacy, and security. We briefly outline the topics covered in the following paragraphs.

Students were first introduced to the topic of biometrics through some introductory reading from *Biometrics: Personal Identification in Networked Society*[1] and to the impact of September 11th on civil liberties in the last ten years through a study by the American Civil Liberties Union[2]. In class, students discussed the role of biometrics and how they feel the world has changed since 9/11. Interestingly, we found that students have relatively little knowledge of the world prior to 9/11 upon which to base a comparison, as they would only have been around 8 years old at the time of the attack.

We introduced students to the technology behind a number of biometrics, and in each case the basic structure of the technology was emphasized so that students learned the fundamentals of these pattern recognition systems. As shown in figure 1, the systems all rely on the gathering of clean training samples to form the database that is used in the identification as well as in obtaining a noisy test sample from the person to be identified. For both the training and the test samples, the information is summarized by extracting relevant features from the samples and the features are used by the classification method to make the identification decision. Since there is noise in the input data, only some features of the input data are used in the classification, and there is no perfect classification method, we emphasized to students that a perfect biometric identification system with 100% correct identification will never be possible.

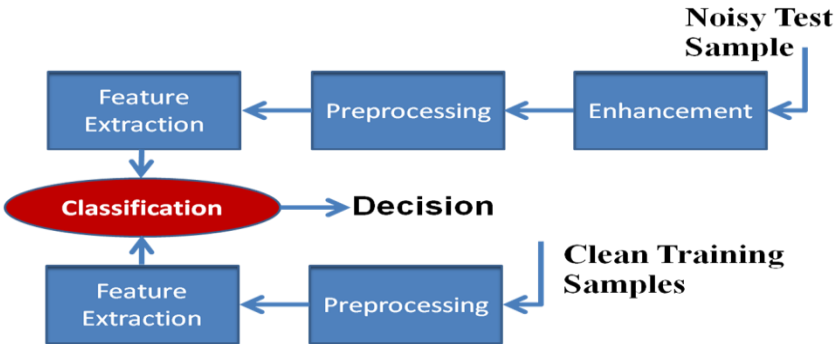

Figure 1. Biometric Identification System Block Diagram

Hand geometry based identity verification was the first biometric discussed in class. As part of the class period, students conducted a simple experiment where they sketched the outline of their hand on two separate pieces of paper. One of the pieces of paper formed an entry in the database of handprints (15 entries in total), while a single handprint was selected from the other set of handprints and used as the unknown handprint. Students were divided into groups and tasked

with identifying the correct handprint from the database, and the students found that 3 of the 4 groups misidentified the handprint assigned to them. This was surprising given the small size of the database but quickly gave students an idea of the limitations of biometric verification methods.

We were able to find a number of recent books on the broad topic of biometrics and privacy and assigned *Our Biometric Future*[3] as a required text for the class. This book primarily covers face recognition and facial emotion recognition and details a number of different case studies where the technology has been implemented with varying degrees of success. We complemented the reading with more technical material[1]; time in class was spent explaining some of the technical details behind face recognition as well as the successes and failures of the technology in real-world applications. Students completed exercises on face recognition[4] and also were asked to identify facial expressions acted out by their classmates. Furthermore, we had discussions on the implications for individual privacy where surveillance technology is widely deployed.

Fingerprint technology has been successfully deployed in a number of applications and is widely accepted because of the ease of obtaining a fingerprint and its perceived low identification error rate. Students read excerpts from *Biometrics: Personal Identification in Networked Society* [1] which explained how fingerprints are identified automatically. Students were introduced to the different classes of fingerprint (loop, whorl, arch) and the features that are used in fingerprint identification, termed minutiae, e.g., ridge ending, bifurcation, etc. In class, students were tasked with identifying their own fingerprint class and highlighting the minutiae in their own and their classmates' fingerprints. This exercise and a video about the real-world possibility of errors in fingerprint identification resulted in a lively classroom discussion as well as in several student papers about fingerprinting technology later in the term.

Moreover, in collaboration with IBM and its Smarter Planet initiative, we were able to arrange for Dr. David Nahamoo, who is an IBM Fellow and the Speech Chief Technical Officer and Strategist at IBM Research, to give a guest lecture to students. Dr. Nahamoo explained in detail to students how speaker recognition systems work and went on to discuss problems that are encountered when these systems are deployed in real application environments. In particular, he outlined how this technology makes accessing one's bank account information and authorizing transactions over the phone more efficient. Once again, students were asked to contemplate the strengths and the weaknesses of this technology.

Furthermore, while the course introduced the technology of biometric identification to students and explained – in general terms -- how this technology works, it also had students read non-fiction articles and fiction stories about biometric technology and privacy issues. The assigned text for the course, *Our Biometric Future* [3], largely focused on face recognition technology and its deployment. The author is skeptical of the merits of the technology and highlights some of the limitations and failures of this technology. For example, a chapter is devoted to the case study of Ybor City, where surveillance cameras with face recognition capability were used in a system in 2001 before being dismantled due to poor performance. This text served as a counterweight to the technical content of the course where recognition figures in the high 90% range (under ideal conditions) are quoted for a variety of biometric identification systems, and served to inform

students of some of the other issues relevant to these systems, such as the influence of culture on surveillance, racial bias, and real-time implementation.

Along with this textbook and other readings that we discuss below, we were able to find a variety of different videos to use in class. These videos were drawn from sources such as the BBC, PBS, Ted Talks, Open University and were short in duration (about 5-10 minutes). These worked well to break up the lecture period and engage the students, and gave us access to a range of expert views and analyses that broadened the discussion in class. In addition, we had the students watch the 1997 movie *Gattaca*[5] which depicts a dystopian future where genetic data are used from birth to determine a person's future, and biometrics are used to track every individual.

Students read the classic Philip K. Dick story *Minority Report*[6] and a more recent novel *Little Brother*[7] by Cory Dortorow. These fiction stories describe a world where there is almost unlimited surveillance and almost all information about an individual is accessible by the authorities. While they are set in the future, the stories are not that far removed from the present, as many of the technologies discussed are being developed or are already available. For instance -- as in Minority Report -- predicting criminal intentions through behavioral cues and biological indicators has been researched since 9/11, and the technology already exists for the fingerprint, gait, and face recognition systems mentioned in *Little Brother*. These stories serve to make the students aware of the trade-offs between surveillance and identification systems and individuals' right to privacy. Another important issue these texts raise is one of security theater: At what point should the line be drawn between having a feeling of security and actually being secure; also, should we sacrifice our individual privacy rights for the former, or only the latter?

To further illustrate the value of personal information and the need to protect one's privacy online, we had students study an article related to privacy on Facebook[8] and followed this up with classroom discussion. The researchers followed a large number of Facebook users to find how they set their privacy settings and how knowledgeable they were about the different privacy controls (which seem to change frequently). Participants in the study found that they had difficulty in keeping track of all their friends, and the dynamic nature of these online social networks means that sometimes it is difficult to control who has access to posted material.

To showcase these issues, we had Quinn Norton, a freelance journalist who writes about technology and social networks, give a guest lecture to students. She covered how privacy becomes a very real concern in different parts of the world, where individuals have to learn to see themselves as the many digital networks see them. In particular, Quinn talked to students about the use of technology in the Arab Spring movements, which started in December 2010 and led to regime changes in a number of countries like Egypt and Tunisia. The ability to organize using social media was a hallmark of these uprisings, but access to one person's Facebook account could lead hostile authorities to have access to the thoughts and whereabouts of a whole group of people. Therefore, Quinn also discussed some ways in which organizers are cloaking their identity using a variety of encryption technologies and using proxy servers outside the reach of local authorities.

While we covered a range of topics in the lectures and gave students different viewpoints on biometric systems and privacy issues, we felt that there were a lot of topics that we could only

touch on briefly, and these were left as research topics that could be explored by students if they were interested.

Student Research Topics

Students were required to come up with their own research topics related to the very broad course topic of "Identity and Security in a Technological World". As an initial step, students were asked to come up with a topic description for their paper in the third week of the term. Students received help on sources for their research paper from the college librarians and learned how to use different databases and how to search effectively for materials in academic databases. In this day and age, moving beyond a simple Google search on to a topic to find trustworthy and useful sources is a valuable skill, and students had their sources assessed by the librarians using the following criteria: Currency, Relevance, Authority, Accuracy, and Purpose[9]. Once they had a research topic and sources, students put an initial draft together in the seventh week, and the draft was graded and returned to them. They had the remainder of the term, up to the tenth week, to rewrite their papers and turn them in as their final drafts.

Students chose a variety of topics for their final papers. While no student delved into the technical details of how a biometric system works (beyond what was covered in class), students were comfortable reading technical material and exploring their chosen research topics. As examples, students chose to look at the role of biometrics in casinos and banks and the systems' potential as identification methods for online transactions. Other students looked at airport security before and after 9/11, government use of biometrics, and privacy issues related to the use of Facebook and government powers (e.g., wiretapping, laws introduced post 9/11).

Student Assessment

Students were given weekly quizzes to ensure that they kept up with the reading in the class. Points were also awarded for general participation in class discussion, attendance, enthusiasm, and attending the library sessions. However, the students' final grade largely depended on the work they did for their final research paper. They were allowed to submit an initial draft, which they received constructive comments on, and then had to turn in a final research paper at the end of term. They also had to put together a presentation of their research and were given 10 minutes of class time to present PowerPoints of their findings to their classmates. We used peer evaluation forms to get feedback from students on the presentations and combined the peer evaluations with our own assessment of the presentations. Also, students were required to present their research at a poster session to the campus community in the final week of classes.

Student Privacy Questionnaire

We were interested in determining what students' views were on privacy and security and whether these changed between the beginning and end of the course. We drafted a questionnaire that used similar questions to those posed in a recent book on biometrics[10] and gave the questionnaires out to students on the first and last days of the course. The questionnaires were divided into two sections (See figures 2 and 3 below.) The average scores from the questionnaires are given in figure 4.

By circling your choice, on a scale of 1 (not at all concerned) to 5 (very concerned), indicate how much you care about the following issues:
1. Unwanted e-mails or spam
2. Identity theft
3. Someone revealing your personal information to government without your permission
4. Someone revealing your personal information to private companies without your permission
5. Loss of civil liberties as part of the war on terror

Figure 2. Questionnaire Part I: Privacy Issues

As shown in figure 4, there was little change in student attitudes to each of the privacy issues addressed in questions 1-5 (Figure 2) between the start and end of the class. Students remained most concerned with identity theft among these five issues, while the gathering of personal information by private companies and government were of less concern.

By circling your choice, on a scale of 1 (strongly disagree) to 5 (strongly agree), indicate your level of agreement with the following statements:
6. I trust my college to keep my personal information private.
7. I trust my doctor to keep my personal information private.
8. I decide when and where my personal information is shared.
9. The government should develop strong laws to protect the privacy of my personal information.
10. My personal information will never be completely private, no matter what I do or what the government does.

Figure 3. Questionnaire Part II: Personal Information Privacy

Figure 4 shows that there were some changes in student attitudes for the set of questions related to personal information privacy addressed in questions 6-10 (Figure 3). Students seemed to realize at the end of the course that the ways their personal information is shared are less under their control than they realized at the start of the course, as seen by the drop in the average response to question 8. This realization is confirmed by responses to question 10, where students more strongly agree after the course that their personal information will never be completely private/secure. After the class, students were less trustful of the college's keeping their information private but maintained the same level of trust in their doctor with their personal information. Students agreed that the government should play a role in keeping information private, but there was no change in their level of agreement between the start and end of the class.

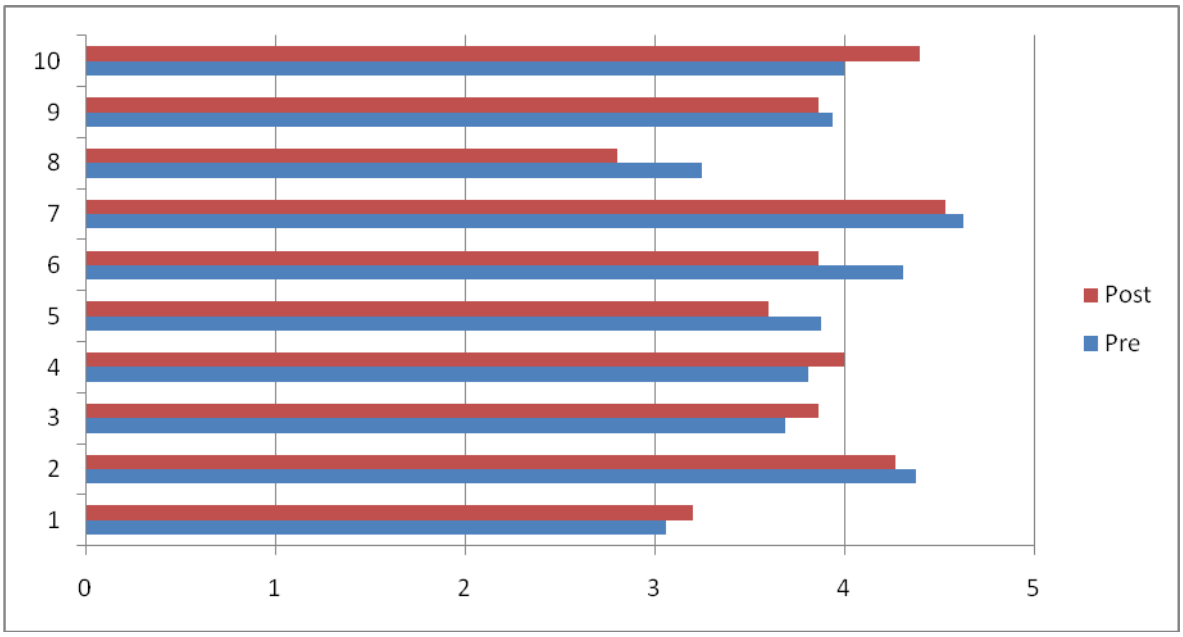

Figure 4. Results of Pre and Post Class Survey

Conclusion

Based on student evaluations, students enjoyed the course and the blend of technical and non-technical material; only one student commented on finding it "difficult to bring the two aspects of the class together". There were multiple positive comments on the in-class exercises, which students found both fun and educational, and this is an aspect of the course that could be expanded upon in future offerings. We did not do any experiments on speaker identification in this first offering of the course, but this could easily be incorporated into the future courses. Also, we only had students look at finding some minutiae in their own fingerprints, but this exercise could be extended to include lifting fingerprints from different surfaces and running experiments with different fingerprint scanners. With the increasing use of biometric technology and the evolving debates centered on personal information and privacy, we will be able to continually update the course content to impress on students the relevance of the course and the ways identity, security, and privacy are intertwined in today's digital world.

Acknowledgement

This work was partially supported by NSF CCLI Award DUE-0837458 and IBM.

Bibliography

1. A.K. Jain et al., Biometrics: Personal Identification in Networked Society, Kluwer Academic, Boston, Mass, 2005
2. D. Himberger et al.,"Civil Liberties and Security: 10 Years after 9/11", The Associated Press-NORC Center for Public Affairs Research, September 2011

3. K. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance,* NYU Press, New York, 2011
4. BBC Face Memory Test, British Broadcasting Company, 12 Apr. 2005, http://www.bbc.co.uk/science/humanbody/sleep/tmt/instructions_1.shtml.
5. *Gattaca*, dir. Andrew Niccol, Columbia Pictures, October, 1997.
6. P.K. Dick, *Minority Report*, from *The Philip K. Dick Reader*, Kensington Publishing Corporation, New York, 2001.
7. C. Doctorow, *Little Brother*, Tom Doherty Associates, New York, 2008.
8. M. Johnson, S. Egelman, and S. Bellovin, "Facebook and privacy: it's complicated", *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12). ACM, New York, NY.
9. "Evaluating Information – Applying the CRAAP Test", Meriam Library, California State University, Chico.
10. Lisa Nelson, *America Identified: Biometric Technology and Society*, The MIT Press, Cambridge, MA, 2011.