ADAPTATION AND IMPLEMENTATION TO A GRADUATE COURSE DEVELOPMENT IN BIOMETRICS

Eric P. Kukula[1], Nathan C. Sickler[2], and Stephen J. Elliott Ph.D. [3]

Abstract — *Biometric research centers on five fundamental areas: data collection, signal processing, decision-making, transmission, and storage. Traditionally, research occurred in subsets of the discipline in separate departments within universities such as algorithm development in computer science, and speech and computer vision in electrical engineering. In the fall semester of 2002, a class in Biometric Technology and Applications was developed to encourage cross-disciplinary education, where all areas of the biometric model would come together and address issues such as research methodologies and the implementation of biometrics in society at large. The course has been modified to accommodate a wider audience, incorporate graduate student research, which is the foundation for modular mini-courses tailored to specific majors and issues. Having an interdisciplinary group of student's better mirrors the makeup of jobs involved in biometrics, such as management, marketing, or research. The challenge lies in providing a course that accounts for these diverse needs.*

Index Terms — *Biometrics, Curriculum Development, Technology, Graduate Education*

MOTIVATION AND BACKGROUND

Biometric identification technology is defined as the "automatic identification or identity verification of (living) individuals based on behavioral and physiological characteristics" [1]. The nucleus of biometric research is divided into five fundamental areas: data collection, signal processing, decision-making, transmission, and storage. Traditional research in biometrics has been undertaken separately in different subsets of the discipline, such as voice or speech processing, or algorithm development. These subsets have been developed in separate departments or disciplines within academia; for example, algorithm development has occurred traditionally within computer science, while speech and computer vision development has been developed in electrical engineering.

Furthermore, dissemination of results is traditionally divided along technology lines. As such, biometric research is a convergence of numerous disciplines like Electrical Engineering, Computer Science, Political Science, Ergonomics, Statistics, and Technology. In the fall semester of 2002, a class was developed in Biometric Technology and Applications designed to encourage cross-disciplinary education, where all five functions of the biometric model come together in a multi-disciplinary approach. Encompassing these various disciplines into one educational environment will encourage discussion on issues such as rigorous methodologies for measuring statistical effectiveness and the implementation of biometrics in society at large.

During the fall of 2002, TECH 581S was offered for the first time, with 20 students participating. The course development and syllabus was outlined in a paper by [2], and described the course overview, outline, as well as objectives. Over the past two semesters, the course has been modified to account for a wider audience, as well as to incorporate graduate student research, and to use the course as a foundation to develop modular short courses that can be tailored to specific educational programs and real world issues, such as aviation security.

Another motivating factor in adapting the course was to cater to a wider audience. In the first semester of the course, the majority of students enrolled were junior or senior undergraduate students in Computer Information Systems Technology or Industrial Technology, both housed in the School of Technology. The second semester saw an increase in the number of non-undergraduate technology majors. Out of 27 students that were enrolled, seven were outside of these majors, including students in Aviation Technology, Computer Science, and Information Security. Furthermore the course was added as a School of Management elective and an Information Security elective. Widening the base of students creates new opportunities for the class, as this wider interdisciplinary group of students better mirrors the makeup of jobs that are involved in biometrics, whether they are in management, sales, marketing, or algorithm development, testing, and integration.

The challenge was therefore to provide a course that accounted for the needs of such a group of students.

[1] Eric P. Kukula, Biometric Standards, Performance, and Assurance Laboratory, Room 242, 401 N. Grant St, West Lafayette, IN 47906, USA, sjelliott@tech.purdue.edu
[2] Nathan C. Sickler, Biometric Standards, Performance, and Assurance Laboratory, Room 242, 401 N. Grant St, West Lafayette, IN 47906, USA, sjelliott@tech.purdue.edu
[3] Stephen J. Elliott, Ph.D., Biometric Standards, Performance, and Assurance Laboratory, Room 242, 401 N. Grant St, West Lafayette, IN 47906, USA, sjelliott@tech.purdue.edu

COURSE ADAPTATION AND IMPLEMENTATION

The first step focused on the weaknesses of the current course. During the first session of the graduate course in Biometrics, students were placed in groups and did a literature review on possible major attacks to biometric devices. At that time, Matsumoto had just released work on sensor vulnerabilities, specifically relating to fingerprinting. His premise was fingerprints could be recreated using gelatin and the sensor would acquire the image [3]. One student group replicated his work and found several weaknesses in his methodology. This group then presented the results to the other research groups in the class, who then adapted the methodology to see whether they could spoof the sensors. From this work, the students managed to find weaknesses in sensors when fingerprints were taken cooperatively. This research is continued today by examining whether non-cooperatively lifted fingerprints can be created to spoof fingerprint devices. Not only does this have specific cultural and security repercussions, but also the creation of low cost fake fingers provides another insight to the security of fingerprints.

In the second offering of the course, groups were smaller and the projects were more diverse, resulting in a course-load that was harder to manage. Smaller groups of two, or even individual projects may have enhanced individual learning, but it was not as effective as the first semester group work. Therefore, it was decided that for the next offering, one semester long project would be assigned to the group, split up into different projects, centering on specific individuals strengths, directly relating to their respective fields.

The authors also examined the weaknesses of the course and specifically technology students' knowledge in the key biometric areas. This revealed weaknesses in the areas of biometric equations and the underlying mathematics, specifically a lack of knowledge on image processing; and the how to develop algorithms. These issues will be particularly addressed in the adapted course through the inclusion of graduate research in these specific fields.

The objectives of the initial course are shown below:

a) Classify biometric applications.
b) Identify techniques for testing biometric devices.
c) Apply "best practice" techniques for biometric project management and implementation.
d) Understand which biometrics technology is best for a given application.
e) Understand the ethics of biometric technologies.
f) Understand the fundamentals of fingerprinting, iris scanning, speaker verification, hand geometry, dynamic signature recognition, facial recognition, and multi biometrics – voice, lip and facial recognition.
g) Understand the limitations of biometric technologies.

New objectives were developed, as a result of the change in curriculum, as well as experience with the course. The first objective was to examine the fundamentals of testing and evaluation of biometric technologies. This is a broader objective from which to provide a stronger foundation for the students. This also ties into the new group project that is described later.

The second objective was to understand the process of biometric standards, performance, and assurance, all of which play a key role in biometric development and will contribute to the growth of the sector. Students with a detailed understanding of the standards process will be invaluable to potential employers, as the role of standards within the biometric industry continue to grow in importance. Industry is now working on standards that include interchange formats, technical interfaces, application profiles for interoperability and data interchange for transportation workers and border control applications. Understanding performance is also important in the biometrics field. Reference [4] outlined weaknesses in facial recognition when measuring algorithm performance vis-à-vis illumination levels. Reference [5] observed that there were challenges with the quality of fingerprints across different populations, specifically between the elderly and eighteen to twenty-five year olds. As students start to work in the field of biometrics or the security industry, they will need to understand how tests are developed, formulated and results presented. Biometric performance can vary drastically depending on the conditions with which the test was done, and as such can impact an implementation [6]. The third aspect of this objective is assurance of the biometric, specifically with regard to its vulnerability of the biometric sensor relationship.

The third objective was to examine the advantages and disadvantages of each biometric technology. Given the foundation established in the first two objectives, students will gain a broader understanding of the technology. For example, if objectives one and two were not covered before the specific technology, students may just examine the technology as opposed to the applications and environments that the technology is used in.

The fourth objective was to adapt and implement the concepts already developed in the first three objectives and relate them to specific biometric applications.

The fifth objective was to generate, evaluate, and critically report on real world biometric implementations. The School of Technology strategic plan is to provide students with an applied focus. By having students critically evaluate biometric systems, they are be better placed to evaluate their own implementation schemes, developed as part of semester project.

GROUP PROJECT

Following the experiences with two previous course strategies, it was decided that the class should do one project which would be split into specific areas, focusing on an individual's core strengths. The group project will also encompass all of the course objectives, and provide students with a real-world application from which to draw experiences on.

Successful biometric implementations are highly dependent on a number of factors, such as environment, population, user attitudes, etc. Each deployment of a biometric technology will be different, and as such have different results and performance. In order to provide the client with a successful biometric implementation, a detailed site survey has to be completed. Students at Purdue University are fortunate to have a number of facilities at their disposal to do site surveys. This semester, students did a site survey of the university recreation facility. The survey included interviews of the recreational facility administrators, a detailed building and grounds assessment, an assessment of the population, the development of a detailed test plan, and recommendation of the biometric technology and implementation strategy to use. Once all the students had completed the site survey, they presented their findings in class, and a comprehensive document was produced. Students were then positioned into four subgroups that concentrated on a number of areas.

The first subgroup was Project Management. This group created a timeline for the course project, determined system expectations from the management and staff, analyzed throughput data from the selected entry points, and summarized the site survey. They acted as managers for the other subgroups. The project management team will also report their progress to the class each week.

The second subgroup is the Administrative team. They investigated current procedures and best practices being operated at other similar facilities. They established procedures and generated instructions for the enrollment and verification of users, a procedures manual, and technical documentation. They prepared the human subjects paperwork required as part of the project.

The third group is the Network group. These individuals design and built as well as simulated the test conditions. This required the network group to provide network architecture diagrams, write a manual for the test, and to ensure that the biometric devices communicate with the database. Furthermore, the network group had to work with the administrative team to answer any questions on the use of the devices, enrollment issues, and threshold settings. The network group also provided a report summarizing the results of the scenario test, and any particular issues that they found in the lab test that affected the deployment of the biometric system.

The Implementation team designed, built and operated the final installation, trained staff; oversaw user training, and other everyday operations of the biometric system that arose during implementation.

The concept behind the group project was to simulate a real world implementation project, but within an academic setting. The groups all interacted with each together, with weekly reports submitted to each group, and collated by the project management team.

SESSION OVERVIEW

The course was divided up into ten sessions focusing on a particular concept, ranging from biometric standards, specific technologies, and implementation / project management. Each session was been restructured to give students the ability to make presentations on particular research topics relating to biometric implementations. Each session is three hours long, and was divided up into specific sections – the first, relating to contemporary issues of the specific session, for example, testing and evaluation, or homeland security. The second part of the session was for student to present on their specific findings from their own research. The third part of the session looked at specific case studies and developed a correlation with the first two parts of the session.

SESSION ONE

The first session overviewed and refreshed students of biometric technology. As the majority of students are undergraduates from the School of Technology, specifically within the Computer Information Systems Technology and Industrial Technology majors, they would have taken IT 345 Introduction to Automatic Identification and Data Capture. This course would have exposed them to the fundamentals of biometric technologies, and given them 'hands-on' experience in the laboratory. The lecture component of Session One was an introduction of Biometrics, as well as the administrative information on the course and laboratory. Students had to prepare a memorandum, outlining as many biometric implementations as they can find, and create a five minute oral presentation outlining their findings. The group will use one of these presentations to complete the next session's activities.

SESSION TWO

The second session elaborated on biometric testing and evaluation, as well as an overview of the mathematical foundation of biometrics. Students read the U.K. Biometric Best Practice document. This prepared them for group project work. The Best Practice document is a comprehensive guide to testing and evaluation. Students will have to use this document extensively in their preparation for the group project, and note any deviations from the best practice in any research that they may undertake. For an evaluation to be accepted by the biometric community, the details of the evaluation procedure must be published along with the evaluation methodology and results. Each person made a brief presentation from their homework assignment (the memorandum). Following the presentation, several of these case studies were then used to demonstrate deviations from the UK Best Practice document, and to examine the reasons behind the deviations. The next memorandum, or assignment, due in Session 3 was designed for students to conduct some preliminary research on hand geometry.

SESSION THREE

The third session discussed issues relating to large-scale biometrics, such as national ID systems, issues relating to homeland security, drivers' licenses, and border security. There was a discussion on hand geometry implementations in universities, such as the University of Georgia, San Diego State University, and Purdue University. There were other case studies relating to hand geometry, notably the San Francisco International Airport. Hand geometry was discussed at length as it is most likely to be the biometric chosen in the semester project. The class was briefed on the group project, and developed a list of questions to ask the administrators, examined past surveys and developed a plan of action for the site survey. Each student independently visited the recreational facility and drew up their site survey assignment. They then presented this information at the beginning of Session 4. Students prepared a memorandum on dynamic signature verification. Students were responsible for completing a human subject test, in order to make them fully aware of the Institutional Review Board policy, which monitors research that involves the use of human subjects.

SESSIONS FOUR - NINE

Sessions four through nine related to specific technologies. These technologies include dynamic signature verification; gait, lip, voice, keystroke, and odor; fingerprint; face; iris; and emerging technologies. This section briefly outlines each of these specific sessions.

SESSION FOUR

Session four is a transitional session, as the class makes the move from group project presentations to specific technologies. The session started with a discussion on the findings of the site survey, and also featured a presentation from a representative of the recreational facility. The second part of the session included a discussion on dynamic signature verification. Students made a brief presentation on applications within dynamic signature verification. The lecture component outlined the fundamentals of dynamic signature verification, the differences between digitized, dynamic, and digital signatures, and how to forensically assess a signature. There was a discussion on the levels of information required to forge a signature. There was also a discussion on the signature standard currently going through the standardization process at the US level (M1).

SESSION FIVE

Session five outlined a number of different technologies, including gait, lip, voice, keystroke, and odor. One of the weaknesses of technology students is the fact that they do not have any experiences with biometric algorithms. This lecture outlined how a keystroke dynamic algorithm works, and how to create one. This session included laboratory activities, where they scheduled a two hour block of time in the Biometric Standards, Performance, and Assurance Laboratory giving them experiences in dynamic signature verification, participate in keystroke dynamic data collection, and use a web-based voice recognition demonstration. The memorandum topic for the next week was to research fingerprint technologies.

SESSION SIX

Session six examined the topic of fingerprint authentication. The session began with oral presentations of the memorandums assigned in session 5, with students describing implementations using fingerprint technologies. A graduate student presented his research on fingerprint quality [5] and a guest speaker described the implementation of fingerprinting in automatic teller machines. Finally, there was a technical presentation on pattern based fingerprint recognition, and minutiae based recognition. Students had to schedule a one hour block of time in the lab so that they can demonstrate the use of different types of fingerprint scanners available in the laboratory. The lab has quality software, and students were able to use this software to assess quality. Students had to use Minitab to perform an Analysis of Variance on dynamic signature verification. This will expose students to statistical software, specifically Minitab, and provide them with experience in analyzing data.

SESSION SEVEN

Session seven described face recognition. Again, in a similar fashion to session six, graduate students presented their work. The session began with oral presentations of the memorandums assigned in session six, based on facial recognition applications. A graduate student presented his research [4] and an undergraduate student presented his work on an implementation at Purdue University airport [9]. There was a demonstration of face recognition and the effects of light on performance. Again, this is another example of graduate research being transformed into the classroom.

SESSION EIGHT

Session eight outlined iris recognition, where students presented their research memorandums on iris recognition deployments during the first part of the session. Following the presentations, a lecture on iris recognition was given, outlining the fundamentals of the technology, the structure of the eye, followed by the iris recognition standard. Students scheduled a session in the laboratory to learn about client server software and how to enroll and deploy iris templates across a system. Other experiments will include habituation experiments on the Panasonic Authenticam iris camera. These laboratory activities were scheduled out of class, and lasted approximately 50 minutes.

SESSION NINE

Session nine concluded the discussion on specific biometric technologies and how they relate to industrial case studies. Students presented a memorandum on emerging technologies, and the formal lecture discussed these and the current state of the art technologies. The second part of the session discussed the semester project.

SESSION TEN

Session ten was the final session of the semester, and included feedback from the semester project, analysis of the laboratory tests, as well as the implementation of the hand geometry project at the recreational facility. The session also included a guest speaker who will pose a problem to the class, and they will then break up into groups and present back to the guest approximately 45 minutes later. This will be a capstone to all the knowledge gained in the course.

GRADUATE RESEARCH INITIATED BY THE COURSE

Over the past year, the TECH 581 class has encouraged students to participate in applied research. Three students that have taken the course are now pursuing Masters Degree's in the School of Technology, specifically relating to biometrics. Some of these examples are highlighted below.

Reference [4] research focused on the influence of variations in illumination levels on the performance of a face recognition algorithm, specifically testing the significance between verification attempts and enrollment conditions with respect to factors of age, gender, ethnicity, facial characteristics and facial obstructions. Reference [4] evaluated the performance of a commercially available facial recognition algorithm for the verification of an individual's identity (1:1) across varying three illumination levels.

This preliminary study showed that for low light enrollment the verification rate for low light attempts was

FIGURE 1: SAMPLE VERIFICATION IMAGES

89.62%, 57.40% for medium light attempts, and 58.70% for high light attempts. For medium light enrollment the verification rate for low light attempts was 73.88%, 91.48% for medium light and 95.37% for high light attempts. For both low and medium light enrollments there was a statistically significant difference between verification attempts at $\alpha = 0.01$. Lastly, for high light enrollment, the verification rate for low light attempts was 80.55%, 89.44% for medium light attempts, and 94.25% for high light attempts. For the high light enrollment, there was no statistically significant difference between verification attempts made at low, medium, or high light at $\alpha = 0.01$. The broader impact of this work is that facial recognition technology from still or video sources is becoming a practical tool for law enforcement, security, and counter-terrorist applications despite the limitations of current technology. At this time, facial recognition holds promise and has been implemented in limited applications, but has not been exhaustively researched in adverse conditions, which initiated this research aimed at improving algorithms to compare images or representations of images to recognize a suspect in varying conditions [7].

Another image quality issue is the lack of substantial research with the elderly population. According to the Fingerprint Verification Competition website [8]; "interest in fingerprint-based biometric systems has grown significantly," and as such, a fingerprint verification competition using fingerprint images was undertaken. Even this competition, one of the widest publicized competitions in fingerprinting, still has relatively small and homogenous databases. Database 1 in the competition had fingerprints that were obtained from a low cost sensor, using up to four fingerprints from each volunteer, aged mainly between 20 to 30 year olds and about 50% male. Database 2 was acquired by using a low cost capacitive sensor, again with a population of half males, aged between 20 to 30 year olds. Database 3 had fingerprints from 19 volunteers aged 5 to 73, with 55% male distribution. One third of the volunteers in this database were over 55, and one third of the volunteers were under 18 years of age. Database 4 was made up of computer-generated fingerprints [8]. It is clear that the elderly are not well represented in this database as they are not an easy population to gain access to. Therefore, in many cases, biometric testing does not include them. By partnering with the Gerontology department, the PI gained access to a large testing pool, and therefore contributed significantly to the biometric community. Furthermore, this is of significant societal interest, as many countries are examining biometric deployments on identity cards.

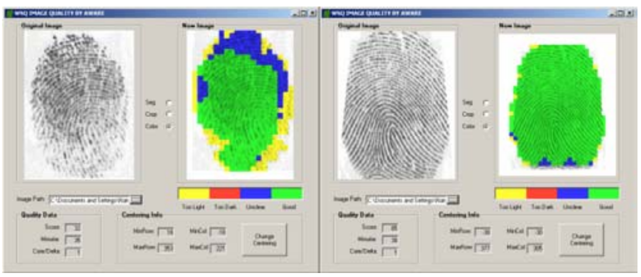

Figure 4. Visual display of the effectiveness quality of the low quality dry image (left) and the high quality normal image (right). A green area has good image quality, and all other colors indicate poor image quality.

The collection of this data, whether it be for template aging, system performance, or image quality is extremely important for the biometric research community, and society at large, because we do not know the answer to this fundamental question – how distinctive are individuals?

If a biometric is not as distinctive as first thought, then one person may be mistaken for another, and the premise that biometrics are unique is then flawed. This is a fundamental research question posed by the biometric research community, and can only be answered by significant data collection efforts across a number of years, as well as across varying demographics. Comprehensive data collection in this area will contribute significantly to the field. Understanding how distinctive individuals behave, under a number of different environmental conditions relates to system performance. If an individual enrolls under one condition, such as a well-lit environment, can the system acquire a good image in another environment, such as a low light condition [4]? If the individual cannot be verified, and is falsely rejected, then this may affect their opinion of the specific biometric, and the way they interact with it (if at all), at subsequent visits. Proper presentation will produce a better quality image, which therefore increases the performance of the device, and provides better results. Also, with increased performance, user psychology about the device may also improve.

CONCLUSION

This paper was written to provide practitioners with an update to the graduate course in Biometrics as first outlined in [2]. As courses develop and evolve, they change to accommodate new technologies and information. This course, in its third semester has continued to advance the biometrics education offered by the Department of Industrial Technology, provide students with the knowledge required to design, build, and implement biometric solutions with commercially available off-the-shelf products. The support of several biometrics vendors has also helped in the development of this course, as well as a grant from the e-Enterprise Center at Discovery Park, Purdue University.

REFERENCES

[1] Wayman, J., & Alyea, L. (2000). Picking the Best Biometric for Your Applications. In SJSU Biometrics. San Jose, California: San Jose State University. Retrieved April 14, 2000 from the World Wide Web: http://www.engr.sjsu.edu/biometrics/publications_tech.html

[2] Elliott, S. J., & Sutton, M. J. (2002a). Graduate Course Development in Biometrics. Proceedings of the 2002 ASEE/SEFI/TUB International Colloquium, Berlin, Germany.

[3] Matsumoto, H. M. T., Yamada, K., Hoshino, S. (2002). Impact of Artificial Gummy Fingers on Fingerprint Systems. Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[4] Kukula, E. P., & Elliott, S. J. (2003). Securing a Restricted Site - Biometric Authentication at Entry Point. 2003 IEEE International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, ROC.

[5] Sickler, N. C., & Elliott, S. J. (2003, May). An Evaluation of Fingerprint Quality Across an Elderly Population vis-à-vis 18-25 year olds. Poster session presented at Energizing the Enterprise: Technology Connecting Science, Business, Manufacturing, and Service: An Overview of Purdue University Wide Research on the Use of Computing and Communications to Impact the Enterprise, West Lafayette, IN.

[6] Wheeler, G., Courtney, P., Cootes, T., & Taylor, C., "Performance Assessment of a Face-Verification Based Access Control System," presented at Fourth IEEE International Conference on Automatic Face and Gesture Recognition, 2000.

[6] Morton, J. M., Portell, C. M., Elliott, S. J., & Kukula, E. P. (2003) Facial Recognition at Purdue University's Airport 2003-2008. 2003 IEEE International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, ROC.

[7] Paul, R. "3-D Face Modeling and Display," Director of Central Intelligence Agency February 27, 2002.

[8] Fingerprint Verification Competition (2003). Retrieved June 16, 2003 from http://bias.csr.unibo.it/fvc2002/