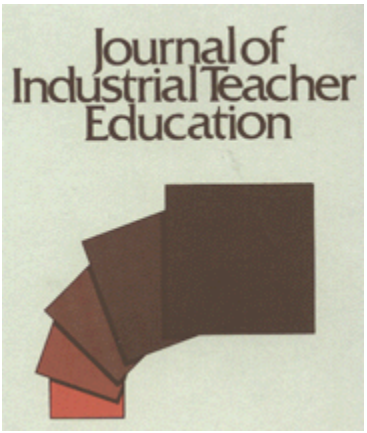

Current Editor:
Janet Z Burns jburns@gsu.edu

Winter 2004 **Volume 41, Number 4**

DLA Ejournal Home | JITE Home | Table of Contents for this issue | Search JITE and other ejournals

At Issue

An Introduction to Biometrics Technology: Its Place in Technology Education

Stephen J. Elliott
Jerry L. Peters
Teresa J. Rishel
Purdue University

Biometric identification technology, the automatic identification or identity verification of individuals based on physiological and/or behavioral characteristics, date back over 50 years to the earliest digital computers. By 2004, personal computers (PCs) or network access, e-commerce and related fields, physical access, and telephony are expected to surpass the traditional biometric sector revenue streams such as criminal identification and citizen identification (International Biometric Group, 2002). Biometrics revenues are expected to grow from $250 million in 1999 to $1.9 billion in 2005 (International Biometric Group). With the increased focus on biometrics technology from the media, many students may be inquiring about such technology and the role that it will play in their life. Additionally, from an industry point of view, many businesses will be

looking for qualified individuals who have had experience with biometrics technology, who understand the core components of the model, and who can identify both the advantages and disadvantages.

From an academic viewpoint, technology educators can use biometrics to inspire students into undergraduate degrees in technology. This article provides the technology educator with a primer on biometrics technology and ties the specific definitions and concepts to the International Technology Education Association (ITEA) Standards for Technological Literacy (2000)

Where appropriate, the relevant standard is shown in conjunction with the biometric concept in accordance with the appropriate grade level, although the majority of the information in this paper is aimed at those teaching students in 9th through 12th grades.

Biometrics in Secondary Education

Biometrics technology has recently seen an increase in deployment as it is implemented into airports, manufacturing facilities, and schools. As students become more familiar with the technology through media exposure, many will have questions about and interest in this use of technology. Additionally, because the technology lends itself well to demonstrations, many vendors provide schools with demonstration software and peripherals such as web cameras and fingerprint sensors, which allows students to interact directly with biometrics technology. Integrating biometrics technology into the curriculum provides students with a strong understanding of the subject matter. Churma (1999) stated that students benefit from such integration " . . . when it allows them to visualize problems and solutions . . . [and] helps students move from concrete to abstract learning" (p. 10). It will enable them to make informed decisions about how this technology is being introduced into society, as well as to determine the best methods of analyzing the results of its introduction.

By increasing the amount and kinds of information to which students have access and the ways they can transform and use this information, biometrics technology increases the possibilities for students to take responsibility for their own learning. They can seek relevant and useful information, assess it, and solve complex problems. As Dewey (1919) purported, good education and true knowledge is that which can be used to solve problems, not simply to answer drill and skill problems. Further, teaching for the future requires teaching for today, which is best achieved through the use of problem solving, which allows students to learn to think. This form of progressive education emphasizes an active form of learning in which limits are not imposed upon the curriculum, allowing students to access a wealth of information and ways to use it.

Biometrics technology pursues and provides answers to the questions and dilemmas of tomorrow's world, which is becoming an increasingly necessary part of the knowledge base of technological understanding. Students pursuing careers in technology must be knowledgeable and informed in a broad range of related topics. With the increase in the need for and use of biometrics technology in today's society, a proportionate need increases for preparing technology students. As biometrics technology continues to impact and inform a global society, particularly in cultural and social interactions and contexts, it is imperative that future technologists are prepared to assume their place in the next generation for improvements, advancements, and innovative discoveries.

Definitions

The first technology education content standard states that "Students will develop an understanding of the characteristics and the scope of technology" (ITEA, 2000, p. 210). Biometrics, an abbreviation of biometric authentication, is a subset of the larger human identification science (Wayman, 2000). Biometric authentication is the "automatic identification or identity verification of (living) individuals based on behavioral and physiological characteristics" (Wayman, p. 269). Biometric authentication focuses on several key terms, including authentication, enrollment, template, threshold, and verification. Authentication is any process through which one proves and verifies certain information (RSA Security, 2000). An individual enrolls in the system by providing a biometric sample, for example, his/her hand, to a specific device. A template stores biometric information created from a series of samples taken at the enrollment stage. Typically, the template is created when the user interacts with the system for the first time and is an average of samples taken at the time of enrollment. A threshold is acceptance or denial of a biometric sample based upon the score falling above or below a threshold. The threshold is variable so that the levels of security can change (Association for Biometrics, 1998). Verification is the process of comparing a submitted biometric sample with a previously stored biometric template in order to determine the identity of the subject (Wayman). Verification is synonymous with one-to-one, identification with one-to-many.

General Biometric Model

Standard 2 (ITEA, 2000) indicates that students develop an understanding of the core concepts of the technology, in this case biometrics. The generic biometric system consists of five different sections: data collection, signal processing, decision, transmission, and storage. Each section of the system can be broken down into smaller parts.

Within the technology education environment, the best subsystem to describe is the data collection subsystem. This subsystem is comprised of the biometric, presentation, and sensor. When an individual interacts with the device, he/she presents a biometric, for example, a hand, to the sensor. Even when all of these subsystems are present, there may still be problems associated with data collection. For example, when a finger is presented to the sensor, the finger may not be properly aligned; or it may be too moist or too dry. This scenario relates well to the requirement for grades six to eight, where the standard requires that students understand that "technological systems include input, processes, output and at times, feedback" (ITEA, 2000, p. 38).

Biometrics technology is used in a number of different applications, such as ATM machines, hand recognition machines at Walt Disney World for season pass holders, and iris recognition devices at selected airports for immigration control. Whatever the specific application, the technology interacts with individuals; therefore, for a successful implementation, students need to understand the technology as part of the social, cultural, and environmental context (Standard 4). An example of applying this standard to the biometric scenario is found in Standard 4(d), "The use of technology affects humans in various ways, including their safety, comfort, choices, attitudes about technology's development and use" (ITEA, 2000, p. 60).

According to Ashborne (2000), biometrics literature rarely discusses user psychology. If a user does not want to use the system, he/she may not be consistent in the use of that system (e.g., the presentation of a finger to a sensor), and will produce a wide variance in distance measurements and a resulting higher-than-average error rate. This will affect the performance of the system.

The additional effect of rejecting the user, even if claiming the correct identity, provides more reason for the individual to be noncooperative with the system. Conversely, someone who is enthusiastic about the device will produce lower-than-average error rates. For welfare/social payment transactions and prison visitor systems, there are tangible benefits for users to accept the system. Electronic transactions (due to their tangible benefits) may induce the individual to perform at a lower-than-average error rate (Ashborne). This is also an example of Standard 4(i), "Making decisions about the use of technology involves weighing the trade-offs between the positive and negative effects" (ITEA, 2000, p. 62).

General Application Classifiers

A discussion on biometrics use and its cultural, moral, and social ramifications depends largely on applications, which are classified into seven categories: cooperative or non-cooperative, covert or overt, habituated or unhabituated, attended or nonattended, environment, classification of user, and system characteristics. Cooperative versus noncooperative refers to the action of the deceptive user, commonly termed "wolf" in the biometrics literature. In an application verifying the positive claim of identity, such as access control, the deceptive user is cooperating with the system in order to be recognized as someone he/she is not (Wayman, 2000). A noncooperative application is one in which a deceptive user is not cooperating with the system in order not to be identified. When a claimant is unaware that a biometrics identifier is being used, the use of the system is considered covert. Should the user be aware that the biometric identifier is taken, the system is overt.

Using the biometrics device daily, such as entry to a particular room or to log on to a network computer, creates habituation. However, if the use of the biometric device is infrequent, then the system is considered unhabituated. All systems will be unhabituated at the installation of the system and may have a mixture of habituated and unhabituated users throughout the operation of the device as new claimants and frequent and infrequent claimants use the device.

A biometrics device is considered nonattended if it does not have an operator or someone guiding users with the device. A standard environment is the environment in which the biometrics device operates. The final category classifies the users of the system; will they be employees of the company (private) or customers (public)? If there is a requirement to share biometrics information with other biometrics systems, then the system is open; if not, it is closed.

These application classifiers are important when assessing the system. Standard 13 states that "When presented with a particular product, or system, the technology literate person should be able to gather information about it, synthesize this information, analyze trends, and draw conclusions regarding its positive or negative effects" (ITEA, 2000, p. 133).

General User Perception Classifiers

Jain, Bolle, and Pankanti (1999) also classified biometrics based on seven different factors: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention. Comparisons among biometrics technologies can be determined after the classification of the application. For example, if there were a comparison between fingerprint and hand geometry devices, both systems should be within the same application category.

Evaluation Classifiers

When evaluating devices, three separate classifications exist: technology, scenario, and operational (Phillips, Martin, Wilson, & Przybocki, 2000). Technological evaluation is the comparison of competing algorithms from a single technology, using a precollected database. Evaluation is off-line and is repeatable. A universal sensor collects the data, although the performance of the algorithms will depend on the environment and the sample. Scenario evaluation refers to the testing of the system in a simulated environment or application. Both the population and the environment remain the same. Operational testing is determining the performance of a complete system within an operational environment.

Performance Parameters

When evaluating and testing biometric devices, the measurement of five parameters is typically proposed: the false match rate, false nonmatch rate, binning error rate, penetration coefficient rate, and transaction time. Moreover, it is useful to have some measurements on the failure to enroll and failure to acquire rates. In testing devices, it is important to test them with the target application in mind.

According to Dunn (1998), a false match rate is the percentage of impostors wrongly matched on a single comparison. False nonmatch rate is the percentage of valid users wrongly not matched. Equal error rate is when the false match rate equals the false nonmatch rate. Transaction time is the amount of time required to complete the transaction. Failure to acquire is the rate to which the device has failed to acquire a sample, and failure to enroll is the rate to which the device has failed to enroll an individual. The variables and their relationships among each other have consequences for determining the appropriate technology for biometrics transactions.

Negative and Positive Identification

There are two applications of biometrics technology: positive identification, which proves you are who you say you are, and negative identification, which proves you are not who you say you are not. For positive identification, the claim of the individual is verified through the comparison of the sample to an enrolled template. In a negative identification system, the user makes no claim to identity, which requires a search of the entire database (Mansfield & Wayman, 2002). Therefore, when enrolling in a negative identification system, there is a comparison of the enrollment template with all of the other enrollment templates in the system to make sure that there is not a match (Mansfield & Wayman).

Positive identification does not require the use of biometrics. Other forms of physical identification, such as drivers' licenses, passports, and passwords, can positively identify the individual. Conversely, negative identification can only be achieved using biometrics. Some applications require the use of negative identification, such as biometrics on commercial drivers' licenses. The one-driver, one-license, and one-record goal requires a form of negative identification. When enrollment occurs in a negative identification system, the system compares the samples with all of the templates in the database to ensure that there are no duplicate records (Wayman, 2000).

Hypothesis Testing

Statisticians use hypothesis testing to test two formulations to be made on objective terms, with a knowledge of the risks associated with reaching the wrong conclusion (Montgomery, 1996). Two kinds of errors are made when using hypothesis testing; the first is when the null hypothesis is rejected when it is true, defined as a Type I error. The second error is not rejecting the null hypothesis when it is false, defined as a Type II error. The relationship between negative and positive identification and Type I and Type II errors relates to the determination of the hypotheses. Under positive identification (I am who I say I am), a Type I error occurs when rejecting the null hypothesis when it is true. For negative identification, the reverse is true, shown in Table 1.

Table 1
Identification and Types of Errors

Error	Positive identification	Negative identification
Type I	False nonmatch	False match
Type II	False match	False nonmatch

Biometrics Testing

The National Physical Lab in the United Kingdom has just completed testing various devices over the same population to determine the performance of the devices. However, at the time of writing, the results were still confidential, as vendors had not yet agreed to the release of the results. The Sandia National Laboratories in New Mexico released a report, A Performance Evaluation of Biometric Identification Devices (Holmes, Wright, & Maxwell, 1991), which examined six different devices: fingerprint, hand geometry, signature dynamics, retinal vascular pattern, and two voice vendors. The sample size was 100 people, with 80 people remaining fairly active in the participation. The population consisted of employees or contractors of Sandia National Labs. Each volunteer user enrolled and trained on all of the verifiers, with both male and female trainers. Furthermore, the first few weeks of the test data were not included in the final study, creating a habituated system. All devices were set up using the manufacturers' recommendations and were commercially available (Holmes, et al.).

Manufacturers rarely release the performance of their products in terms of false accepts and false reject rates. The accepted practice in measuring performance is through Receiver Operating Characteristic (ROC) curves. Although common in the medical field, ROC analysis is also prevalent in the discipline of signal detection theory. ROC curves consist of two key descriptors, sensitivity and specificity, with sensitivity being true positives and specificity being true negatives. Furthermore, additional measures of great interest in both positive and negative identification are the failure to enroll and failure to acquire rates (Mansfield & Wayman, 2002).

Enrollment Selection

The first choice the tester must make is the enrollment data and its selection. Presentation of the biometrics sample to the sensor for the first time requires an enrollment template to be collected, typically between one and three trials. When testing a biometrics device, there is an assumption that measurements are time

invariant. Research studies by PenOp have revealed that even in a constant environment, signatures from individuals change, depending on the time of day, cyclically over periods of weeks, and can simultaneously change progressively over a period of months. This is called template aging. Another error is the time delay between enrollment of the template and the later measurements. Wayman (2000) suggested that the ideal time between enrollment and sampling should be similar to that experienced in the application, yet acknowledges that this may increase test time and expense. Signature verification poses an additional problem. Nonbehavioral biometrics recommends that a time interval between consecutive testing be equal to or greater than the time taken for that specific body part to heal. In the case of fingerprint, healing is defined as the finger obtaining its normal characteristics.

Conclusion

The increased utilization of biometrics technology in the past few years has contributed to a strong growth pattern as the technology is used in a variety of facilities, including schools. Due to media exposure, students' familiarity with technology will continue to increase proportionately, which will result in an increased curiosity about biometrics technology. Thus, implementing this technology as part of the technology education curriculum will provide students with many and varied opportunities to work with the new technology, learn about it, and become informed consumers on the introduction of this technology into society. As well, it will result in providing those interested in a career in technology with a broad range of knowledge and enable them to pursue specializing in biometrics. As part of the curricular focus on technology, the technology education standards will place a comprehensive emphasis on the introduction of biometrics technology, problem solving, exploration, and useful implementation of the technology into society.

References

Ashborne, J. (2000). *Biometrics: Advanced identity verification*. New York: Springer-Verlag.

Association for Biometrics. (1998). *Glossary of biometric terms*. Retrieved from http://afb.org.uk/public/gloosuk1.html

Churma, M. (1999). *A guide to integrating technology standards into the curriculum*. Upper Saddle River, NJ: Prentice-Hall.

Dewey, J. (1919). *Experience and education*. New York: Touchstone.

Dunn, J. (1998). *Biometrics and the future of money*. Hearings before the Subcommittee on Domestic and International Monetary Policy of the House Committee on Banking and Financial Services. 105th Congress.

Holmes, J. P., Wright, L. J., & Maxwell, R. L. (1991). *A performance evaluation of biometric identification devices*. Albuquerque, NM: Sandia National Laboratories.

International Biometric Group. (2002). *Biometric market report 2000 - 2005*. Retrieved from http://www.biometricgroup.com/e/biometric_market_report.htm

International Technology Education Association. (2000). *Standards for technological literacy: Content for the study of technology*. Reston, VA: Author.

Jain, A., Bolle, R., & Pankanti, S. (1999). *Biometrics: Personal identification in networked society* (2nd ed.). New York: Kluwer Academic Publishers.

Mansfield, N., & Wayman, J. L. (2002). *U.K. biometric working group best practice document*. Teddington, UK: National Physical Laboratory.

Montgomery, D. (1996). *Design and analysis of experiments* (5th ed.). New York: John Wiley & Sons.

Phillips, P., Martin, A., Wilson, C., & Przybocki, M. (2000, February). An introduction to evaluating biometric systems. *IEEE Computer*, 56-63.

RSA Security. (2000). *What is a digital signature and what is authentication?* RSA Security. Retrieved from http://www.rsasecurity.com/rsalabs/faq/2-2-2.html

Wayman, J. L. (2000). *National biometric test center collected works*. San Jose, CA: National Biometric Test Center.

Elliott is Assistant Professor in the Department of Industrial Technology at Purdue University in West Lafayette, Indiana. Elliott can be reached at elliott@purdue.edu.