Biometrics Education with Hands-on Labs

Li Yang
University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
(423)-425-4392
Li-Yang@utc.edu

Kathy Winters
University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
(423)-425-4278
Kathy-Winters@utc.edu

Joseph M. Kizza
University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
(423)-425-4043
Joseph-Kizza@utc.edu

ABSTRACT
Biometrics is an emerging field via the automated use of unique and measurable physiological or behavioral characteristics to determine or verify identity. Biometrics has a variety of applications in governments, military and commercial areas. The Department of Computer Science and Engineering at the University of Tennessee at Chattanooga offers a biometrics course for senior undergraduate students through integration of engineering, statistics, mathematics, policy and ethics. In order to expose students to the area of biometrics with minimum costs, we employ open-source based software to design a series of hands-on labs including fingerprint, face, handwriting, and voice biometrics. Our lab design can serve as a model of biometrics education for programs that have limited budget which may prohibit the use of expensive commercial biometrics devices and software.

Categories and Subject Descriptors
K.3.2 [**Computer and Education**]: Computer Information Science Education – *computer science education, curriculum.*

General Terms
Documentation, Security

Keywords
Biometrics, Hands-on labs, Education

1. INTRODUCTION
The Department of Computer Science at University of Tennessee at Chattanooga (UTC) offers a B.S. in with Information Security and Assurance (ISA) concentration, a M.S. with ISA concentration and two certificates: Nos. 4011 and 4012. 4011 is Information Systems Security (INFOSEC) Professionals, and 4012 is Senior System Managers. The courses in above programs have been certified by the Committee on National Security Systems (CNSS), the National Security Agency (NSA), and Department of Homeland Security (DHS). Among the ISA core courses at UTC, biometrics is one of the major components because it is an emerging technology to reinforce the authentication techniques. Due to budget limitation, an ISA program may not afford expensive commercial biometrics devices and software. In order to expose students to labs in biometrics, we design a set of hands-on lab based on open source software. This paper creates a model for the program that has limited budge but is interested in Biometrics education. We discuss the knowledge domain of each biometrics technology, together with its corresponding hands-on labs. The paper is organized as follows: Section 2 introduces the basic concepts and processes of biometrics. Section 3, 4, 5, 6 describes the knowledge domain and hands-on labs including fingerprint, face, handwriting, and voice biometrics respectively. Section 7 discusses other biometrics. Section 8 elaborates challenges and future of biometrics and section 9 offers the concluding remarks.

ACM Southeast Conference'08, Month 28–29,2008, Auburn, AL, USA.

2. BIOMETICS INTRODUCTION
There are several techniques that can be applied for verifying and confirming a user's identity. They can be broadly classified as something the user knows, such as a password or PIN, something the user has, such as a smart card or ATM card, and something that is a part of the user, such as a fingerprint or iris. The strongest authentication involves a combination of all three. A biometric authentication system uses the physiological (fingerprints, face, hand geometry, iris) and/or behavioral traits (voice, signature, keystroke dynamics) of an individual to identify a person or to verify a claimed identity. Biometric technology is used for many applications such as providing time and attendance functionality for a small company and ensuring the integrity of a 10 million-person voter registration database. The benefits of using biometrics include increased security, increased convenience, and reduced fraud or delivery of enhanced services.

The process flow of biometrics includes enrollment and verification/identification. During the enrollment stage, a user is initially enrolled in biometric system by providing his or her biometric data, which is converted into an enrollment template. During the verification/identification stage, the user again provides his or her biometric data, which is converted into a live template. A template is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches. It can be understood as a compact representation of the collected feature data, where useless or redundant information is discarded. Biometric data such as fingerprints and facial images cannot be reconstructed from biometric templates because

templates are extractions of distinctive features and are not adequate to reconstruct the full biometric image or data. Unique templates are generated every time a user presents his or her biometric data. A biometric algorithm allows the matching of an enrolled template with a live template just created for verification of identity, thus determining their degree of similarity or correlation. The process of matching biometric templates results in a score, which is compared against a threshold to determine how closely they match. If the score exceeds the threshold (the match is close enough), the result is a match and non-matching otherwise. A threshold is a predefined number, which establishes the degree of correlation necessary for a comparison to be deemed a match. Thresholds can vary from user to user, from transaction to transaction, and from verification attempt to verification attempt. A system can be either highly secure for valuable transaction or less secure for low-value transaction, depending on their threshold settings. Traditional authentication can not offer such flexibility.

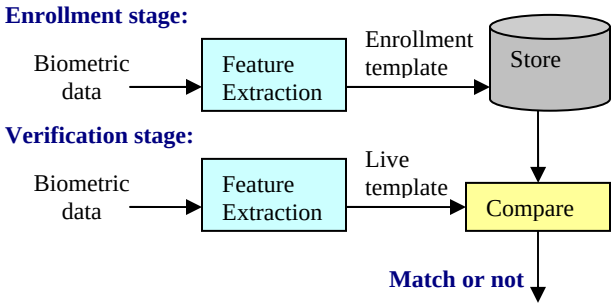

Figure 1. Two stages of biometric process flow.

Three metrics are used to indicate how well a biometric system or device performs. They are false acceptance rate (FAR), false rejection rate (FRR), and failure-to-enroll rate (FTE). If John Smith presents his biometric traits that successfully match as Jane Doe, this is classified as false acceptance. The probability of this happening is referred to as false acceptance rate (FAR). On the other hand, if John Smith presents his biometric traits to a biometric system, and fails to match as John Smith, This is classified as false rejection. The probability of this happening is the false rejection rate (FRR). If a user is new and fails to be enrolled to a biometric system, this is called – failure to enroll (FTE). Analysis of all three metrics is necessary to assess the performance of a specific technology.

3. FINGERPRINT BIOMETRICS

Fingerprints are the most widely used biometric characteristic because of their well-known distinctiveness and persistence. While law enforcement agencies were the earliest adopters of the fingerprint recognition technology, more recently, increasing identity fraud has created a growing need for biometric technology for person recognition in a number of non-forensic applications. Large volumes of fingerprints are collected and stored everyday in applications such as access control, and driver license registration.

3.1 Knowledge Domain of Fingerprint Biometrics

A fingerprint is made of a series of ridges and valleys on the surface of the finger. In a fingerprint image, ridges (also called ridge lines) are dark, whereas valleys are bright. The uniqueness of a fingerprint can be determined by the pattern of ridges and valleys as well as the minutiae points, which are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Minutia refers to various ways that the ridges can be discontinuous. For example, a ridge can suddenly come to an end (termination), or can divide into two ridges (bifurcation). Although several types of minutiae can be considered, usually only a coarse classification is adopted to deal with the practical difficulty in automatically discerning the different types with high accuracy.

Fingerprint classification means assigning each fingerprint to a class in a consistent and reliable way such that an unknown fingerprint to be searched need only be compared only with the subset of fingerprints in the database belonging to the same class. An automatic recognition of a user based on fingerprints requires that the input fingerprint be compared with a large number of fingerprints in a database. Classifying these fingerprints can reduce the search time and computational complexity, so that the input fingerprint is matched only with a subset of the fingerprints in the database. While fingerprint matching is usually performed according to fingerprint micro-features, such as ridge terminations and bifurcations (minutiae), fingerprint classification is usually based on macro-features, such as global ridge structure. All the classification schemes currently used by law enforcement agencies are variants of the so-called Henry's classification scheme. Five classes (Arch, Tented arch, Left loop, Right loop and Whorl) are commonly used by today's fingerprint classification techniques. In reality, fingerprints are not uniformly distributed among these five classes.

Minutiae detection identifies unique features of fingerprints, which are used to certify the person's identity. Straightforward matching between the unknown and known fingerprint patterns is highly sensitive to errors. Modern techniques focus on extracting minutiae points from the fingerprint image, and checking matching between the sets of fingerprint features. Two fingerprints are compared using discrete features called minutiae. The minutiae include points in a fingerprint where ridges end (called a ridge ending) or split (called a ridge bifurcation). There are on the order of 100 minutiae on a fingerprint. The location of each minutia is represented by a coordinate location within the fingerprint's image from an origin in the bottom left corner of the image. Minutiae orientation is represented in degrees with zero degrees pointing horizontal and to the right, and increasing degrees proceeding counter-clockwise. A selected fingerprint is mapped into a digital frame by a function $f(t, s, \theta)$ where t is he minutiae type, s is the site and θ is the neighborhood information.

Fingerprint matching compares data from the input against all appropriate records in the database to determine if a probable match exists. Minutia relationships, one to another are compared based on not only locations within an X-Y co-ordinate, but also the linked relationships within a global context. Each template comprises a multiplicity of information chunks, every information chunk representing a minutia and comprising a site, a minutia slant and a neighborhood. Each site is represented by a pair of values $s = (x, y)$ where x and y are two coordinates. A live template is compared to a stored measured template chunk-by-

chunk. The live information on site, minutia slant and neighborhood of the reference are compared with those from the stored template. If the matching rate of all information is equivalent to or superior to the predetermined threshold, the live template matches the stored (latent) template.

Fingerprint recognition is a complex pattern recognition problem; designing algorithms capable of extracting salient features and matching them in a robust way is quite hard, especially in poor quality fingerprint images. There is a popular misconception that automatic fingerprint recognition is a fully solved problem since it was one of the first applications of machine pattern recognition almost fifty years ago. On the contrary, fingerprint recognition is still a challenging and important pattern recognition problem.

3.2 Hands-on Labs on Fingerprint Biometrics

We use the software released from the Image Group of the National Institute of Standards and Technology (NIST). NIST Fingerprint Image Software Version 2 (NFIS2) contains software technology developed for the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS), and it is designed to facilitate and support the automated manipulation and processing of fingerprint images.

We investigate PCASYS, MINDTCT, NFIQ and BOZORTH3. PCASYS is a neural-network based fingerprint classification system that automatically categorizes a fingerprint image into the class of arch, left or right loop, scar, tented arch, or whorl. This is an updated system that includes the use of a robust Multi-Layered Perceptron (MLP) neural network. It is a no cost system. MINDTCT is a minutiae detector that automatically locates and records ridge ending and bifurcations in a fingerprint image. This system includes minutiae quality assessment based on local image conditions. The FBI's Universal Latent Workstation (ULW) uses MINDTCT, and it is also a no cost system. NFIQ is a fingerprint image quality algorithm that analyses a fingerprint image and assigns a quality value of 1 (highest quality) – 5(lowest quality) to the image. Higher quality images produce significantly better performance with matching algorithms. BOZORTH3 is a minutiae-based fingerprint matching algorithm that does both one-to-one and one-to-many matching operations. It accepts minutiae generated by the MINDTCT algorithm.

This hands-on lab is set up under the Linux environment. Students use Perforce to access NIST server to download non-export control part including PCASYS, MINDTCT and others. NFIQ and BOZORTH3 are under export control laws which can be obtained via sending email to NIST (nbis_ec@nist.gov).

4. FACE BIOMETRICS

Face recognition is fast, cheap and unobtrusive. Moreover, they are very robust against changes in the environment when combined with voice-recognition and can be used as person identification.

4.1 Knowledge Domain of Face Biometrics

Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure its characteristics and make positive identifications. Facial recognition utilizes distinctive features of the face including distinct micro elements such as mouth, nose, eyes, cheekbones, chin, lips, forehead, and ears. In addition to these, upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes, the distance between the eyes, the length of the nose, and the angle of the jaw are used. Facial recognition programs use facial micro features to create a unique file called a *template*.

Using the templates, the software then compares that image against a stored image and produces a score that measures how similar the images are to each other. Face physical traits can be captured by either live scans or through use of photograph or videos. Typical sources of images for use in facial recognition include video camera signals and pre-existing photos such as those in driver's license databases, including the distance between the micro elements, a reference feature, the size of the micro element, amount of head radiated from the face (unseen by human eye), and the heat that can be measured using an infrared camera.

The enrollment and matching face biometrics algorithms fall into categories: eigenface, local feature analysis, neural network, and automatic face processing. As with all biometrics, four steps are used by these algorithms: sample capture, feature extraction, template comparison, and matching. Enrollment generally consists of a 20-30 second enrollment process whereby several pictures are taken of one's face. Ideally, the series of pictures will incorporate slightly different angles and facial expressions, to allow for more accurate matching. After enrollment, distinctive features are extracted (or global reference images are generated), resulting in the creation of a template. Verification and identification involves a similarity comparison between the newly created match template and the reference template or templates on file. The point at which two templates are similar enough to match, known as the threshold, can be adjusted for different personnel, PC's, time of day, and other factors. There are several approaches to face biometrics.

Eigenface is one of the most famous face recognition approaches; it is a fast, simple, and effective method, but does not scale and it is light condition invariant. Eigenfaces are a set of "standardized face ingredients", derived from statistical analysis of many pictures of faces. Each eigenface represents only certain features of the face. Any human face can be considered to be a combination of these standard faces. One person's face might be made up of 10% from face 1, 24% from face 2 and so on. This means that if you want to record someone's face for use by face recognition software you can use far less space than would be taken up by a digitized photograph. The face is then mapped to a series of eigenvectors, mathematical properties, describing the unique geometry of a particular face forming a biometric template.

If one uses all the eigenfaces extracted from original images, one can reconstruct the original images from the eigenfaces. But one can also use only a part of the eigenfaces. Then the reconstructed image is an approximation of the original image. To ensure that losses due to omitting some of the eigenfaces can be minimized, choose the most important features (eigenfaces), and assign them weights. Similar faces (images) possess similar features (eigenfaces) to similar degrees (weights). The original images of the training set are transformed into a set of eigenfaces *E*. Afterwards; the weights are calculated for each image of the training set and stored in the set *W*. Upon observance of an

unknown image *X*, the weights are calculated for that particular image and stored in the vector *WX*. *WX* is compared with the weights of images, of which one knows for certain that they are faces (the weights of the training set *W*). One way to do it would be to regard each weight vector as a point in space and calculate an average distance *D* between the weight vectors from *WX* and the weight vector of the unknown image *WX* (the Euclidean distance would be a measure for that). If this average distance exceeds some threshold value, then the weight vector of the unknown image *WX* lies too "far apart" from the weights of the faces. In this case, the unknown *X* is considered not a face. Otherwise (if *X* is actually a face), its weight vector *WX* is stored for later matching.

In **local feature analysis**, a face is represented as a graph, whose nodes, positioned in correspondence to the facial fiducial points, are labeled with a multi-resolution description of the surrounding gray level image. A fiducial point is a point or line on a scale used for reference or comparison purposes. This approach is much better than the others in terms of rotation, light and scale invariance. Given a new image, the system localizes the face and the facial features, extracts the facial fiducial points, determines the head pose and creates a gallery to be used for comparison.

Linear Discriminant Analysis (LDA) is based on the algorithm written by Zhao and Chellapa [5]. When used in the Face Identification and Evaluation System each human subject forms a class. The algorithm uses Fisher's Linear Discriminants. LDA training attempts to produce a linear transformation that emphasize differences between classes while reducing differences within classes. The goal is to form a subspace that is linearly separable between classes. LDA training requires training data that has multiple images per subject. LDA training is performed by first using Principle Components Analysis (PCA) to reduce the dimensionality of the feature vectors. After this LDA is performed on the training data to further reduce the dimensionality in such a way that class distinguishing features are preserved. A final transformation matrix is produced by multiplying the PCA and LDA basis vectors to produce a full input image to LDA space transformation matrix. The final output of the LDA training is the same as PCA. The algorithm produces a set of LDA basis vectors. These basis vectors produce a transformation of the feature vectors. Like the PCA algorithm, distance metrics can be used on the LDA feature vectors.

Bayesian Intrpersonal/Extrapersonal Classifer is used by the Colorado State University (CSU) distribution methodology. Is based on an algorithm by Maghaddam and Pentland [6]. It examines the difference between two photos as a way of determining whether the two photos are of the same subject. Difference images which originate from two photos of different subjects are said to be extrapersonal whereas images which originate from two photos of the same subject are considered interpersonal.

The **Elastic Bunch Graph Matching (EBGM)** is based on an algorithm from the University of Southern California (USC) [11]. The algorithm locates landmarks on an image, such as the eyes, nose, and mouth. Gabor jets are extracted from each landmark and are used to form a face graph for each image. A face graph serves the same function as the projected vectors in the PCA or LDA algorithm; they represent the image in a low dimensional space. After a face graph has been created for each test image, the algorithm measures the similarity of the face graphs.

4.2 Hand-on Lab on Face Biometrics

For this hands-on lab, UTC uses the CSU Face Identification Evaluation system available through the website http:www.cs.colostate.edu/evalfacerect/). This system includes standardized image pre-processing software, four distinct face recognition algorithms, analysis software to study algorithm performance, and Unix shell scripts to run standard experiments. All code is written in ANSII C. This system includes algorithms for performing all four approaches to facial recognition; Eigenfaces, combined Principle Components Analysis and Linear Discriminant Analysis algorithm (PCA+LDA), Bayesian Intrapersonal/Extrapersonal Classifier (BIC), and Elastic Bunch Graph Matching (EBGM). The PCA+LDA, BIC, and EBGM algorithms are based upon algorithms used in the Facial Recognition Technology (FERET) study contributed by the University of Maryland, Massachusetts Institute Technology (MIT), and USC respectively.

Two different analysis programs are included in the evaluation system. The first takes as input a set of probe images, a set of gallery images, and similarity matrix produced by one of the four algorithms. It generates a Cumulative Match Curve that plots recognition rate as a function of recognition rank. The second analysis tool generates a sample probability distribution for recognition rate at recognition rank 1, 2, etc. It takes as input multiple images per subject, and uses Monte Carlo sampling in the space of possible probe and gallery choices. This procedure will, among other things, add standard error bars to a Cumulative Match Curve. It will also generate a sample probability distribution for the paired difference between recognition rates for two algorithms, providing an excellent basis for testing if one algorithm consistently out-performs another.

5. HANDWRITING BIOMETICS

In the past decades, researchers have been working on handwriting recognition, which aimed at designing systems able to understand personal encoding of natural languages.

5.1 Knowledge Domain of Handwriting Biometrics

Methods and recognition rates of handwriting depend on the level of constraints on handwriting. The constraints are mainly characterized by the: types of handwriting, number of scriptors, size of the vocabulary and spatial layout. Recognition strategies heavily depend on the nature of the data to be recognized. In the cursive case, the problem is made complex by the fact that the writing is fundamentally ambiguous as the letters in the word are generally linked together, poorly written and may even be missing. On the contrary, hand printed word recognition is more related to printed word recognition, the individual letters composing the word being usually much easier to isolate and to identify.

Character Recognition techniques can be classified according to the way preprocessing is performed on the data, and the type of the decision algorithm. Preprocessing techniques include 1) the use of global transforms (correlation, Fourier descriptors, etc.), 2) local comparison (local densities, intersections with straight lines,

variable masks, characteristic loci, etc.), and 3) geometrical or topological characteristics (strokes, loops, openings, diacritical marks, skeleton, etc.). Various kinds of decision methods can be used in the preprocessing techniques, which include statistical methods, neural networks, structural matching (on trees, chains, etc.) and stochastic processing (Markov chains, etc.).

Handwritten Word Recognition employs either a holistic approach or an analytical approach. The holistic approach is to globally perform recognition on the whole representation of words and there is no attempt to identify characters individually. The main advantage of holistic methods is that they avoid word segmentation. The analytical approach is to deal with several levels of representation corresponding to increasing levels of abstraction (usually the feature level, the grapheme or pseudo-letter level and the word level). Words are not considered as a whole, but as sequences of smaller size units which must be easily related to characters in order to make recognition independent from a specific vocabulary.

5.2 Hands-on Lab on Handwriting Recognition

UTC uses a form-based handprint recognition system provided by the National Institute of Standards and Technology (NIST). It is used for optical character recognition and is available on CD-ROM. The source code is written in C and contains algorithms from the current and a previous version. Included in the new version are new utilities to several new features including: generalized form registration, intelligent form removal with character stroke preservation, text-line isolation in handprinted paragraphs, adaptive character segmentation based on writing style, and sophisticated Multi-Layer Perceptron (MLP) neural network classification. A software implementation of the machine learning algorithm used to train the new MLP is included, enabling recipients to train the neural network for pattern recognition applications other than character classification. A host of data structures and low-level utilities are also provided. These include the application of spatial histograms, affine image transformations, simple image morphology, skew correction, connected components, Karhunen Loève feature extraction, dictionary matching, and many more. The software has been successfully compiled and tested on LINUX workstations. The software test-bed can be obtained free of charge on CD-ROM by sending a letter of request via postal mail or FAX to NIST.

6. VOICE BIOMETRICS

Voice biometrics is the only commercial biometrics that process acoustic information. Voice biometrics has the ability to work with standard telephone equipment, which makes it possible to support broad-based deployments of voice biometrics in a variety of settings.

6.1 Knowledge Domain of Voice Biometrics

Each individual has individual voice components called phonemes. Each phoneme has a pitch, cadence, and inflection. These three give each one of us a unique voice sound. Voice biometrics works by digitizing a profile of a person's speech to produce a stored model called voice print or template. Biometric technology reduces each spoken word to segments composed of several dominant frequencies called formants. Each segment has several tones that can be captured in a digital format. The tones collectively identify the speaker's unique voice print. Voice prints are stored in databases in a manner similar to the storing of fingerprints or other biometric data. *Voice verification* verifies the vocal characteristics against those associated with the enrolled user. The US PORTPASS Program, deployed at remote locations along the U.S.–Canadian border, recognizes voices of enrolled local residents speaking into a handset. This system enables enrollees to cross the border when the port is un-staffed. Voice verification can be applied in a variety of areas, such as on-line banking, on-line security trading, and access control to corporate databases, on-line information services.

Voice recognition systems are different from voice verification systems although the two are often confused. Voice recognition is used to translate the spoken word into a specific response. The goal of voice recognition systems is simply to understand the spoken word, not to establish the identity of the speaker. A good familiar example of voice recognition systems is that of an automated call center asking a user to "press the number one on his phone keypad or say the word 'one'." Template matching is the simplest technique of voice recognition and has the highest accuracy when used properly. After a user speaks a word or phrase into a microphone, the electrical signal is digitized and stored in memory. To determine the meaning of this voice input, the computer attempts to match the input with a digitized voice sample, or template that has a known meaning. Voice recognition can be applied to hands free devices, software applications, spoken multiple choice in interactive voice response systems, and applications for people with disabilities.

6.2 Hands-on Lab on Voice Recognition

The Sphinx group at Carnegie Mellon University (CMU) provides a set of speck recognition software. Sphinx engines and tools are derived from BSD, and based, in particular, upon the license for the Apache web server. Sphinx provides a basic level of technology to anyone interested in creating speech-using applications without the once-prohibitive initial investment cost in research and development.

7. OTHER BIOMETRICS

Other physiological biometrics includes iris, hand, and retina. Iris-scan is to utilize the distinctive features of the human iris in order to identify or verify the identity of individuals. *Iris-scan technology* requires the acquisition of a high-resolution image of the eye, illuminated by an infrared imager, in order to effectively map the details of the iris. The iris-scan algorithm then locates the inner edge of the iris at the pupil. The patterns that constitute the visual components of the iris are surprisingly distinctive. A primary visible characteristic is known as the trabecular meshwork, a tissue that gives the appearance of dividing the iris in a radial fashion. *Hand-scan* utilizes the distinctive aspects of the hand – in particular, the height and width of the back of the hand and fingers – to verify the identity of individuals. Features acquired by hand-scan systems are not highly distinctive. Therefore, the technology cannot be used for identification and is not ideally suited for extremely high security implementations. *Retina scan* technology utilize the distinctive characteristic of the retina—the surface on the back of the eye that processes light entering through the pupil—for identification and verification. The retina's intricate network of blood vessels is a physiological

characteristic that remains stable throughout the life of a person. As with fingerprints and iris patterns, genetic factors do not determine the exact pattern of blood vessels in the retina.

Other behavioral biometrics include signature and keystroke biometrics. *Signature-scan* utilizes the distinctive aspects of the signature to verify the identity of individuals. The technology examines the behavioral components of the signature, such as stroke order, speed, and pressures, as opposed to comparing visual images of signatures. *Keystroke-scan* utilizes a person's distinctive typing patterns for verification. Using normal computer keyboards, keystroke-scan measures variables such as the length of time a user holds down each key and the time elapsed between keystrokes. Keystroke-scan is normally deployed in conjunction with passwords and is not currently implemented to monitor users typing on the fly.

8. CHALLENGES AND TRENDS

Significant progress is required for the U.S. to realize fundamental improvements across all biometrics modalities and their systems and thereby enable more advanced operational systems. An analysis of common needs within the driving forces of biometrics identifies four main challenges: biometrics sensors, biometrics systems, biometrics systems interoperability and communication and privacy. Biometrics sensors should provide rapid collection of biometric data in mobile and harsh environments that meet technical, safety and quality standards, quality collection of biometric data of non-cooperative users at distances. Biometrics systems should ensure consistently high recognition accuracy under a variety of operational environments, have the ability to determine which components are most appropriate for a given application, and support remote unattended enrollment and recognition of end-users with varying sensors. Biometrics systems should have the ability to easily, rapidly and seamlessly integrate system components into functioning systems and then swap components as needed without losing functionality, to validate and verify the authenticity and use restrictions of data collected from multiple sources, to build an understanding of enterprise-wide implementations across multitude of constituencies. As to communications and privacy, privacy functionality should be embedded into every layer of the architecture, from the sensor through the system to the interoperable biometric network. Biometrics systems should incorporate privacy-protective solutions that meet operational needs enhance public confidence in biometrics technology and safeguard personal information. Concerns about identity theft through biometrics use have not been resolved. If iris scan is stolen, this can lead to someone else accessing personal information or financial accounts, and the damage could be irreversible. Often, biometric technologies have been rolled out without adequate safeguards for personal information gathered about individuals. Also, the biometric solution to identity theft is only as good as the information in the database that is used for verifying identity.

9. CONCLUSION

We discussed what is covered in the course of biometrics, together with its corresponding hands-on labs. The processes of biometrics, fingerprint, face, handwriting, and voice biometrics are elaborated in detail. We also discussed the challenges and future of biometrics. This paper aims to create a model for programs interested in developing curriculum on Biometrics with hands-on experiences.

10. REFERENCES

[1] Craig I. Watson, Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet and Kenneth Ko, User's Guide to NIST Biometric Image Software (NBIS), National Institute of Standards and Technology, 2006. http://fingerprint.nist.gov/NFIS/

[2] Craig I. Watson, Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe and Stanley Janet, User's Guide to NIST Fingerprint Image Software 2 (NFIS2), National Institute of Standards and Technology, 2006. http://www.itl.nist.gov/iad/894.03/nigos/NBIS/request_ecc_cd.html

[3] Ross Beveridge, David Bolme, Marcio Teixeira and Bruce Draper, The Colorado State University (CSU) Face Identification Evaluation System User's Guide: Version 5.0, Computer Science Department Colorado State University, 2003, http://www.cs.colostate.edu/evalfacerec/algorithms5.html

[4] M. A. Turk and A. P. Pentland. Face Recognition Using Eigenfaces. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, pages 586 – 591, June 1991.

[5] W. Zhao, R. Chellappa, and A. Krishnaswamy. Discriminant analysis of principal components for face recognition. In *Wechsler, Philips, Bruce, Fogelman-Soulie, and Huang, editors, Face Recognition: From Theory to Applications*, pages 73–85, 1998.

[6] B. Moghaddam, C. Nastar, and A. Pentland. A bayesian similarity measure for direct image matching. *International Conference on Pattern Recognition (ICPR)*, B:350–358, 1996.

[7] The National Biometrics Challenge, *National Science and Technology Council, Subcommittee on Biometrics*, 2006.

[8] Lodge Juliet, *Trends in Biometrics*, December 2006, http://www.libertysecurity.org/article1191.html

[9] P. Jonathon Phillips, Alvin Martin, C.l. Wilson, Mark Przybocki, "An Introduction to Evaluating Biometric Systems," Computer, vol.33, no.2, pp. 56-63, February 2000.

[10] Michael D. Garris, James L. Blue, Gerald T. Candela, Patrick J. Grother, Stanley A. Janet and Charles L. Wilson, NIST Form-Based Handprint Recognition System (Release 2.0), NISTIR 5959, *National Institute of Standards and Technology*, April 2003. http://www.itl.nist.gov/iaui/vip/databases/defs/nist_ocr.html

[11] Markowitz, J. A. Voice biometrics. *Communications ACM* 43(9), pp. 66-73, 2000.

[12] Carnegie Mellon University (CMU) http://cmusphinx.sourceforge.net/html/cmusphinx.php

[13] Amir Nanavati, Michael Thieme Raj Nanavati, *Biometrics: Identity Verification in a Networked World*, Wiley, 2002.

[14] Paul Reid, *Biometrics for Network Security*, Prentice Hall, 2004