AC 2010-1359: LABORATORY EXERCISES FOR AN UNDERGRADUATE BIOMETRIC SIGNAL PROCESSING COURSE

Shane Cotter, Union College

Laboratory Exercises for an Undergraduate Biometric Signal Processing Course

Introduction

The ability of investigators to analyze sound, image, and video data and to efficiently search through large databases of biometric data such as fingerprints or facial images has revolutionized the field of forensics over the last couple of decades. These technologies are routinely used in popular television shows such as *Crime Scene Investigation* and *NCIS* among others. Indeed, it is seldom that one of these shows does not feature a biometric identification such as fingerprint identification, face identification, or speaker identification.

Since September 11, 2001, there has been a much greater emphasis placed worldwide on security, and biometric technologies have been adopted to enhance existing security measures. Biometrics such as fingerprints and a digital image are stored in an RFID chip embedded in the passports of citizens in a large number of European countries. The United States has introduced the US-VISIT program and gathers face and fingerprint data from travelers entering its borders[1]. While governments have acted to increase security, access to both public and private buildings and sensitive areas are being more rigorously controlled and biometric technology is being more widely used for identity verification. As one example, the successful use of fingerprinting at Walt Disney World shows that a biometric system can be used in a large commercial setting and is readily accepted by people[2]. Biometric technology has also been incorporated into popular laptops from Lenovo[3] among others.

Although biometric technology is increasingly important in forensics and security applications and is currently a very active research area, this topic has predominantly been addressed at the graduate level due to the mathematical background required for research in the area. In a recently funded NSF proposal[4], we have proposed the development of a biometric signal processing course targeted towards undergraduate students. An important component of the project was the proposed development of a set of laboratories which would give undergraduate students in Electrical and Computer Engineering (ECE) the opportunity to explore these important technologies. In this paper, we detail these newly developed laboratories (based on a 10 week term) that allow students to gain hands-on experience with real-world biometric technologies.

Each set of laboratories is based on a different clue and the ultimate goal of each laboratory experiment is to identify the persons responsible for an imaginary crime. The first three laboratories are based on a speech signal clue and this gives students an opportunity to review material from their introductory signal processing course while also introducing the building blocks of a pattern recognition system: signal preprocessing and enhancement, feature extraction, and classification. The second set of three laboratories focuses on face recognition. The three stages of the recognition task are reinforced by breaking the task into separate experiments, and in each laboratory one part of the recognition system is implemented. In the third set of laboratories, a fingerprint image is presented as a clue and students develop some of the code for the fingerprint recognition system. In the final couple of weeks, student groups are assigned different projects that modify the basic classifiers developed during the previous weeks. Students implement these projects and determine the effect of the project on recognition performance.

In the sections below, we first outline the objectives underlying the development of the laboratories and describe the hardware and software that was purchased for the laboratories. Then, each set of laboratories for speaker, face, and fingerprint recognition is described in detail. Finally, we outline the assessment that will be used to determine whether the developed laboratories have successfully met our objectives.

Laboratory Development Objectives

Very often in the ECE undergraduate curriculum students are frustrated by the lack of opportunities to experiment with real cutting-edge applications and the associated hardware and software. We wanted to develop a set of laboratories at a reasonable cost which would give students hands-on experience with common biometric sensors and the associated signal processing and software. The hardware sensors and software outlined in the next section provide students with an environment for experimenting with sensors and software used in biometric applications. Students gather biometric data from a number of their friends (10 per student) and have the opportunity to interact with each of the sensors and explore the software tools available for processing the data.

In developing the laboratories, we wanted to engage students in the laboratory exercises, and the topic of biometric identification offers a unique opportunity to increase student enthusiasm in the laboratory. It is a rare night on television that biometric technology is not used on a prime time show and a fingerprint, facial image, voice sample, palm print, shoe print or other clue is used en route to solving a particular crime. Each set of laboratories has been framed as solving a crime based on a particular clue: a noisy voice print, a low resolution image, and a latent fingerprint. As an introduction to the experiments on each of the different modalities, video clips will be shown from popular television shows where the technology that students will be developing is used. Students will be excited to learn about how the technology works and how its performance compares to the very fast and amazingly accurate idealized technology depicted on television.

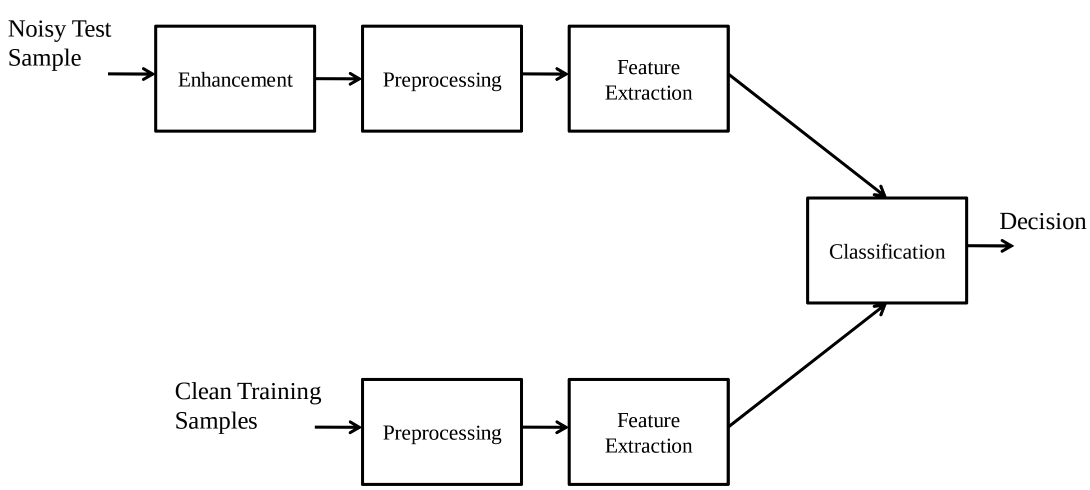

Figure 1. Pattern Recognition Block Diagram

This course is students' first introduction to pattern recognition. As shown in Figure 1, the pattern recognition process consists of three stages: enhancement and preprocessing, feature extraction, and classification. The laboratories are structured to illustrate how each biometric identification method relies on the same pattern recognition process. This structure reemphasizes for students the basic building blocks of a pattern recognition system and the tasks which must be completed in developing a complete recognition system. Our goal in developing the laboratories in this manner is to provide students with a strong understanding of the need for these different stages and the similarities in the recognition methodology across different biometric modalities. Students can then readily see how each stage can be changed to produce a different system.

Finally, we aimed to provide students with the software and hardware skills to allow them to work on projects at the end of the course. The processing that we introduce for one biometric signal can, in many cases, be readily applied to another biometric signal and there is plenty of scope for students to explore different enhancement, feature extraction, and classification methods in end of term projects. They are then able to compare the performance obtained with their new system against the baseline systems developed in laboratories. This gives students a feeling of accomplishment in developing their own code and creating their own recognizer. In many cases they will be able to improve on the baseline performance obtained in the laboratory exercises.

Laboratory Workstation Description

In developing these laboratory experiments, we wanted to provide students with hands-on experience with biometric sensors. Therefore, rather than relying on existing databases, students obtain all data used in their experiments. Fortunately, the hardware and software costs have decreased dramatically over the last decade which allowed us to put together a workstation for students to experiment with at a very reasonable cost. Table 1 details the different hardware and software used for each biometric modality (Matlab[5] is used throughout the experiments and is not included in this table.)

Hardware/Software Component	Biometric Modality	Price
Goldwave Audio Software	Speech	$50
Logitech USB Desktop Microphone	Speech	$30
Sennheiser HD-280 Headphones	Speech	$85
Logitech Webcam Pro 9000 & Software	Face	$100
Digital Persona U.are.u 4500 Reader	Fingerprint	$96
Griaule Fingerprint SDK	Fingerprint	$45

Table 1. Biometric hardware and software costs

The total cost comes to just over $400 which is very reasonable and cheaper alternatives are available for the hardware sensors which would bring the cost closer to $300. One of our NSF project goals is to disseminate these laboratories to other interested schools and the relatively low cost should allow most schools to readily adopt these laboratories. Figure 2 gives a screenshot which illustrates the different software outlined in Table 1.

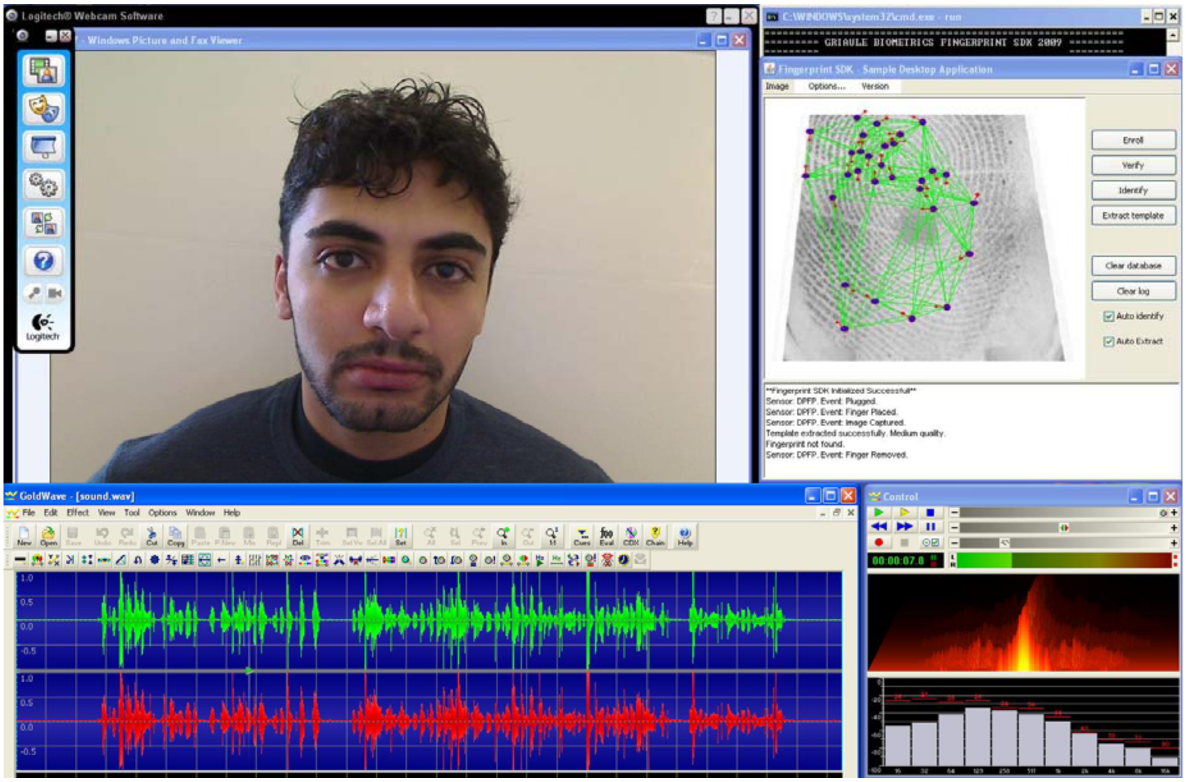

Figure 2. Software (Logitech,Goldwave,Griaule) used in laboratory modules.

Data Collection

Students are initially tasked with gathering biometric information from a number of their friends to be used as training samples for their databases and as test samples. This gives students experience with using the hardware and software outlined in the previous section. Institutional Review Board (IRB) approval was obtained to gather this data and each subject is required to sign a consent form. To safeguard the biometric data, the data is associated with randomly generated fake names[6] (with the correct gender) and the real identity is never associated with a saved version of the file.

Students collect speech information by having subjects read a line in a noise free environment. Then a fan is turned on and some white noise is played in the background while the subject rereads the same line of text. A photograph of the subject with a neutral facial expression is taken under controlled lighting and with a neutral background. The subject is then photographed with the light turned low, a facial expression other than neutral, and at a distance of 5m from the camera. Next, three different fingerprint images of the index finger are taken (where the subject is asked to press forcefully, with medium force, and lightly on the scanner). Partial fingerprints are also obtained by having each subject just press a part of their finger on the sensor. This exercise impresses on students the necessity of having clean training data which is used to populate the database and a consistent method for obtaining and saving the data.

Students now have the clean data that can be used to create the reference databases for identification and noisy data samples which are used to test the success of their identification methods. Next, we describe the laboratories which have been developed for each of the biometric identification tasks. Each task is framed as a clue (stated at the beginning of each section below) which has been obtained from an investigation and students seek to match the information recovered from the crime scene to one of the subjects in their database. In describing the laboratories below, we have omitted the mathematical details of the methods, which can be found elsewhere, and given an overview of the laboratories and the methods explored.

Laboratories 1-3: Speaker Recognition

Clue 1: This message has been recorded from a telephone call made by one of the criminals. The criminal distorted his/her voice by changing the sampling rate to conceal his/her identity and there is a lot of background noise. Using your knowledge of sampling rates and filtering, employ Goldwave and Matlab to process the speech. Then, implement a speaker identification system to determine a list of suspects.

Students are already familiar with one-dimensional signal processing from prerequisite courses in systems and digital signal processing. This makes speaker recognition the ideal starting point as concepts such as sampling, filtering, and time/frequency domain can be covered quickly to refresh students' memories while the basic building blocks of a pattern classifier (as shown in Figure 1) can be introduced for this application.

Preprocessing and Enhancement: The first task the students must perform is to find the true sampling rate of the waveform which has been modified in the test file. A number of different possible sampling rates are given to students and, using Goldwave[7], they change the sampling rate and listen to the speech with each of the new sampling rate to determine the true sampling rate. The speech is then converted to the same sampling rate as the training samples so that a comparison can be made between different speakers. The noisy utterance must be enhanced and Goldwave is used for this purpose; its speech enhancement algorithm uses spectral subtraction to remove the background noise and students compare the spectrograms of the noisy and enhanced signals. The students then cut out the phrase "package received" from each of the training utterances and the test utterance to use in the identification experiment.

Feature Extraction: As one of the oldest sets of features used for speech[8,9], and a necessary first step for many other related feature vectors, we decided to use the Linear Prediction Coefficients (LPC) as the features in the speaker identification system. This method can be explained relatively easily and implementation of the method introduces students to a number of important speech processing operations:

1. The speech is passed through a pre-emphasis filter to mitigate the drop-off in power at higher frequency (this filtering is done in the time domain).
2. Speech is separated into frames of duration 20ms with an overlap of 10ms between adjacent frames.
3. Each frame is windowed using a Hamming window to smooth out the discontinuity between one frame and the next frame.

4. The Levinson-Durbin recursion is explained to students and they are guided through an implementation of the algorithm so that they determine the LPC coefficients.

Classification: The final step in the speaker identification system is to match the test utterance against the database of utterances from known speakers. A complication with speech is that utterances are often at different rates and this means that an algorithm which accounts for this variability must be employed. Statistical methods based on Gaussian Mixture Models (GMM) and Hidden Markov Models (HMM) have been very successfully used in speaker identification[8], but we felt that this material was too complex for most undergraduate students. A relatively simple method for comparing the utterances is Dynamic Time Warping[8,9] which allows for a choice between a number of different vectors at each time point and finds a path that minimizes the difference between the test sample and training sample. Each of the training samples must be compared to the test sample and the training sample which yields the lowest cost is identified as the speaker. The algorithm is explained in detail to students and they are guided to complete the laboratory in a step-by-step fashion.

Laboratories 4-6: Face Recognition

Clue 2: A photograph of one of the criminals, taken from afar, has been obtained. Use Matlab to crop the face image from the photograph and to increase the size of the face to match the face sizes in your database. By implementing a face recognition system, determine a list of possible suspects from this photograph.

Preprocessing and Enhancement: This course represents students' first exposure to image processing and a laboratory section is dedicated to familiarizing the students with image processing and some Matlab functions. Methods for reading, writing, and displaying images are first introduced. Then, the concepts of quantization, resolution, and image resizing are explored. Finally, pixel-wise intensity transformation and image filtering are used to enhance some images. There are excellent resources for introducing these image processing tools[10,11] and these form the basis for this laboratory. These tools are used to standardize the size of the facial images in the training set. The test image given to students is from a distance of 5m and students must crop and resize the face image to match the size of the training images in their database. They can also choose to enhance their image using one of the transforms or filters that they have used previously in the laboratory session to more closely match the training images.

Feature Extraction: Principal Component Analysis (PCA) has been successfully applied to face recognition, and while its performance has been improved upon since it was first introduced in 1991, a recognition rate in excess of 90% is obtainable[12]. This feature extraction method was chosen as it can be readily understood by undergraduate students and its implementation is relatively straightforward. Students are guided through the implementation of the PCA method and the principal components are extracted from the database of training images. The projection of each of the training images along the principal component directions is used to give the feature vector associated with each image. The PCA feature vector is obtained from the test vector in exactly the same manner that each of the training feature vectors was obtained.

Classification: The test feature vector must be classified as one of the training images and this is achieved using the k-Nearest Neighbor (kNN) Classifier[13]. The concept behind this classifier is very intuitive and is easily understood by students. The implementation of the classifier which just requires a computation of the Euclidean distance between the test vector and each of the training vectors and sorting the distances is easily accomplished.

Laboratories 7-8: Fingerprint Recognition

Clue 3: A fingerprint has been lifted from the crime scene and must be compared against the fingerprints in your database. Using the supplied code to locate the centerpoint, develop the Matlab code to extract a set of features from the training and test fingerprint images. Determine a list of possible subjects by comparing the fingerprint against your database of fingerprints.

Fingerprints have a long history of use as a biometric identifier and the automatic identification of fingerprints has been the subject of intense research for several decades[14]. Most systems rely on the extraction of minutiae (ridge endings, bifurcations) from the fingerprints as a feature extraction stage. A comparison between minutiae is used to determine a fingerprint match. An alternative approach is to filter a fingerprint image using 2-D Gabor filters to generate a *fingercode* which can then be used to compare fingerprints[15]. These filters are optimal in capturing the orientation information along with the position information from a 2D image, and they have been applied to a wide variety of problems. In the context of biometric identification, they have been used in iris, face, and (as we will explain) fingerprint recognition. These laboratories (due to limited time) focus on the feature extraction stage in fingerprint identification. Students generate the fingercode and this exercise gives students experience with using the Gabor filters and further practice with image filtering.

Preprocessing and Enhancement: The fingerprint image can be processed to improve the recognition performance by applying morphological operators and enhancing the image contrast. However, these are left as project exercises for some student groups and the unenhanced fingerprint images are used in these experiments.

Feature Extraction: The algorithm consists of first finding the centerpoint of the fingerprint. By itself, this is a complicated procedure[15] and a Matlab p-file (which is encrypted) is supplied to students to generate this point. The students are responsible for generating the fingercode and are guided through the procedure in the laboratory. The steps involved are summarized here and explained in greater detail elsewhere[15]:

1. Tessellate the region around the center point into a series of 7 concentric bands with the radius increasing by 10 pixels at a time. A sample fingerprint and the bands extracted from the fingerprint are shown in Figure 3 below. The band closest to the center is ignored. Then divide each band into sectors determined by lines at 0, 45°, 90°, 135° (these correspond to the angles of the Gabor filters used in step 3).
2. In each sector (48 in total), normalize the gray values to a constant mean M and variance V (both chosen as 100 in the original paper[15]). This has the effect of removing the effects of sensor noise and gray level differences due to differences in finger pressure between sectors.

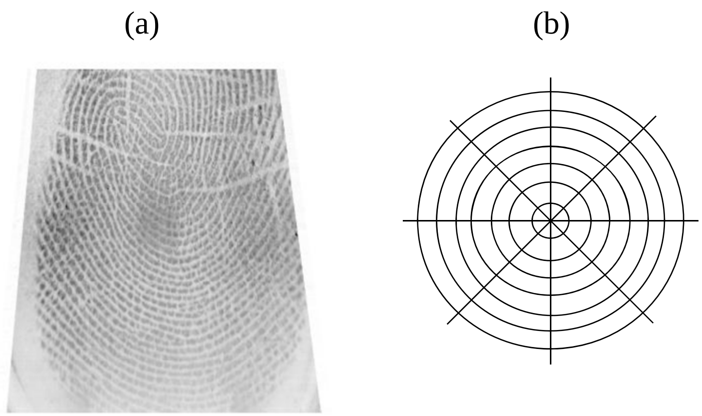

Figure 3. (a) Fingerprint image obtained from sensor and (b) tessellation of the fingerprint image in obtaining fingercode.

3. Filter the entire fingerprint region using a bank of 4 Gabor filters aligned at angles 0, 45°, 90°, 135° to give a set of 4 different images. The Gabor filters are of size 33×33 and are convolved with the fingerprint image. The Gabor filters enhance the ridges and valleys that are oriented at the same angle as the filter and suppress the ridges and valleys oriented at other angles.
4. For each of the 4 filtered images generated, the same sectors (as shown in Figure 3) are extracted and the standard deviation of the sector is computed. In total, there are 192 standard deviation computations (4 filtered images × 48 sectors) and these values are used to give the fingercode vector.

Classification: Once the fingercode routine has been completed, the students generate fingercodes for all the training samples as well as the test sample. The nearest neighbor classifier developed for the face recognition experiment is used to determine the top matches from the available database of fingerprints. The use of this classifier emphasizes the similarity between different biometric recognition systems.

Laboratories 9-10: Student Projects

In the final two laboratories students undertake a project on a particular biometric. With the base recognition systems constructed in the previous laboratories, we have designed a larger number of projects which can be undertaken by students to modify these systems. The projects can be completed in a 2 week period and incorporate some of the material from the previous 8 weeks, but they also challenge the students to use this material in a slightly different application. As examples, we give two project titles associated with each of the three different biometric modalities:

- Implement spectral subtraction for speech enhancement
- Implement a speaker recognition system using mel frequency cepstral coefficients
- Implement a face recognition system based on Linear Discriminant Analysis
- Implement a face recognition system using Gabor filters to extract features

- Employ morphological operators and enhancement methods to the fingerprint images
- Implement a center point detection algorithm for fingerprint recognition

For each project, the team of students is provided with a clear description of what the project entails and they are guided to an implementation which can be completed in the two week time frame. The students are expected to compare the performance of their new recognition system (which very often involves just changing one block in the pattern recognition system from Figure 1) with the baseline recognition system which was developed during the previous laboratories.

Assessment

All students have already taken an introductory signal processing course prior to this course and the Discrete Time Signals and Systems Concept Inventory (DT-SSCI) test instrument[16] will be used to objectively establish their level of understanding of fundamental signal processing concepts (e.g., sampling, filtering, etc.) on the first day of the course. While completing the laboratory exercise, students will apply signal processing methods to both speech and image data to create biometric systems. At the conclusion of the course, the same DT-SSCI exam will be administered to determine objectively whether the course has improved the students' understanding of these core concepts. It is postulated that the application of signal processing to real systems, and the interest that students will have in successfully solving clues to determine the identity of the persons involved, will encourage them to better understand signal processing concepts. Moreover, students will see these fundamental signal processing concepts applied in 2D which may improve some students' understanding.

A number of the objectives (discussed earlier) behind the development of these laboratories will be assessed through focus group interviews. In particular, we wish to assess to what extent working with biometric technology and doing hands-on experiments motivated student learning, and whether students felt more engaged by this laboratory experience than other laboratories in their undergraduate courses. We want to determine if students are more confident in their signal processing knowledge and applying this knowledge to real applications at the conclusion of the course. We also want to assess how confident students would be in designing a pattern recognition system. Finally, we wish to determine if they were adequately prepared for the project portion of the course and how well they could work together as part of a team during the term.

Conclusion

We have described a set of laboratory experiments which have been developed for an undergraduate course in Biometric Signal Processing. The laboratories have been designed to be hands-on for students, and hardware and software costs have been kept low. The laboratories allow students to experiment with speaker, face, and fingerprint recognition. The fundamental pattern recognition steps of preprocessing and enhancement, feature extraction, and classification are clearly emphasized in the development of each system. Students are given end of term projects where they construct their own classifier by changing one element of the pattern classifier. They compare the performance of their new system to the baseline system developed in laboratories. Student learning is assessed by using the Discrete Time Signals and Systems Concept Inventory validated test instrument and focus groups.

Acknowledgement

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

Bibliography

1. US-VISIT, http://www.dhs.gov/files/programs/usv.shtm.
2. J.R. Vacca, *Biometric Technologies and Verification Systems*, Butterworth-Heinemann, 2007.
3. IBM Fingerprint Readers, http://www.pc.ibm.com/us/security/fingerprintreader.html.
4. S. Cotter, "CSI Union: understanding forensic and biometric technologies", NSF CCLI Award DUE-0837458, June 2009.
5. Matlab, ver. R2009a, Jan. 2009, www.mathworks.com.
6. Fake Name Generator, Corban Works LLC, http://www.fakenamegenerator.com/.
7. GoldWave Audio Editor, ver. 5.55, Goldwave Inc., http://www.goldwave.com/.
8. J.P. Campbell Jr., "Speaker recognition: a tutorial", Proc. IEEE, Vol. 85 (9), pp. 1437-1462, Sept. 1997.
9. L. Rabiner and B.-H. Juang, *Fundamentals of Speech Recognition*, Prentice Hall, 1993.
10. Matlab Image Processing Toolbox - Getting Started, http://www.mathworks.com/access/helpdesk/help/toolbox/images/f0-3373.html.
11. R. Gonzalez and R. Woods, *Digital Image Processing*, Prentice Hall, Third Edition, 2008.
12. M. Turk and A. Pentland, "Eigenfaces for recognition", *Journal of Cognitive Neuroscience*, Vol. 3(1), pp. 71-86, Jan. 1991.
13. T.M. Cover and P. Hart, "Nearest neighbor pattern classification", *IEEE Transactions on Information Theory*, Vol. 13 (1), pp. 21-27, Jan. 1967.
14. D. Maltoni et al., *Handbook of. Fingerprint Recognition*, 2nd Edition, Springer, 2008.
15. A. K. Jain et al., "Filterbank-based fingerprint matching," *IEEE Trans. Image Processing*, vol. 9(5), pp. 846-859, May 2000.
16. K. Wage, J. Buck, C. Wright, T. Welch, "The signals and systems concept inventory", *IEEE Transactions on Education*, Volume 48, Issue 3, pp. 448-461, Aug. 2005.