Fuzzy Logic Weight Estimation in Biometric-Enabled Co-authentication Systems

Van Nhan Nguyen, Vuong Nguyen, Minh Nguyen, Tran Dang

Fuzzy Logic Weight Estimation in Biometric-enabled Co-Authentication Systems

Van Nhan Nguyen, Vuong Quoc Nguyen, Minh Ngoc Binh Nguyen, and Tran Khanh Dang

Faculty of Computer Science and Engineering, HCMC University of Technology, VNUHCM, Ho Chi Minh City, Vietnam
khanh@cse.hcmut.edu.vn

Abstract. In this paper, we introduce a co-authentication system that combines password, biometric features (face, voice) in order to improve the false reject rate (FRR) and false accept rate (FAR) in Android smartphone authentication system. Since the system performance is often affected by external conditions and variabilities, we also propose a fuzzy logic weight estimation method which takes three inputs: password complexity, face image illuminance and audio signal-to-noise-ratio to automatically adjust the weights of each factor for the security improvement. The proposed method is evaluated using Yale [5] and Voxforge [1] Databases. The experimental results are very promising, the FAR is 0.4 % and FRR almost equal 0% when the user remembers his password.

Keywords: Co-authentication, fuzzy logic weight estimation, biometric features, privacy.

1 Introduction

Nowadays, private information (bank accounts, email passwords, credit card numbers, etc.) is usually stored in personal mobile devices storage. This leads to the urgent need of secured authentication mechanism. However, current authentication systems still witness weaknesses, which allow attackers to access sensitive information illegally. For example, most classical user authentication relies on tokens and passwords which may be easily lost. Password-based authentication is not highly secured, but it is still used widely because of simplicity. In order to support users with other authentication methods and take advantage of mobile device sensors, some research of biometric-based authentication have been conducted which bring potential results.

Regarding biometric-based co-authentication [3], [8], the use of "Fuzzy logic control system" as a method to estimate weight of biometric factors has been presented in many papers, such as [7] and [2]. In detail, the two systems proposed in [7] and [2] include membership functions and fuzzy logic rule sets for only three biometric traits (face, voice and fingerprint). In this paper, we present one construction that offers multi-feature verification system involving biometrics

(face, voice) and non-biometric feature (password) to make the authentication system adaptive to mobile devices.

The rest of the paper is structured as follow: in section 2 , we introduce the general concepts and co-authentication system structure; in section 3, we describe all components of Fuzzy Logic Weight Estimation System ; in section 4, the experimental results for system performance evaluation is shown; finally, in section 5, we conclude the paper with findings and directions for future research.

2 Co-Authentication System

The system proposed in this paper consists of *Fuzzy Logic Weight Estimation System* and other five main supporting components: *Face Authenticator*, *Voice Authenticator*, *Password Authenticator*, *Score & Decision Fusion* and *Co-Authentication*. System structure is described in Fig. 1.

Firstly, user's biometric features are extracted and transformed into suitable forms through *Face Authenticator* and *Voice Authenticator*. These two components are in charge of extracting necessary information of biometric for authentication process in the system. Besides, *Password Authenticator* takes user's password and then, sends out password information.

Secondly, along with the information extracted by three authenticators, the weights of three features (face, voice and password) measured by *Fuzzy Logic Weight Estimation System* are put into the *Score & Decision Fusion* component. *Score & Decision Fusion* produces a number after calculating a specified formula using the previous weights as inputs.

Finally, based on that number, *Co-Authentication* can make the decision whether user access is accepted or rejected.

2.1 Biometric Authenticator

Enrollment. First of all, two pre-processed vectors: P_{e1} and P_{e2} are generated from real-valued representation of the biometric samples: R_{e1} and R_{e2} by the *Pre-Processing* module. In this stage, we perform histogram equalization for face feature and pre-processing steps (normalization, silence removal, pre-emphasising, framing, windowing) for voice feature. Then, feature vectors F_{e1}, F_{e2} ($\mathrm{F_{ei}} \in \mathrm{R^{N_F}}$, i=1,2) are extracted by *Biometric Feature Extractor*. In this step, we use Eigenface method proposed by Turk and Pentland in [11], and Mel-Frequency Cepstral Coefficients (MFCCs) algorithm in [10] for face and voice feature extraction respectively. Finally, in order to protect biometric templates, we transform feature vectors to different forms, called distance vectors: d_{e1} and d_{e2} by *Biometric Vector Transformator*. The detail of this technique is shown in [12].

Authentication. Like enrollment phase, a new biometric sample is taken and transformed into distance vectors: d_{a1} and d_{a2}. Euclidean distance between new distance vectors and stored distance vectors is then computed using following

equation:

$$D_i = \sqrt{\sum_{k=0}^{M} (d_{ei_k} - d_{ai_k})^2} \tag{1}$$

where M is the length of the distance vector and $i = 1, 2$. Distance D is calculated by the average of all distances D_i. Next, score s and validating variable d are obtained using Equation 2:

$$\begin{cases} s = 0, d = false, & \text{if } D > D_{thres} \\ s = S_{thres} + (S_{Range} - S_{thres}) \frac{D_{thres} - D}{D_{thres}}, d = true, & \text{if } D \leq D_{thres} \end{cases}, \tag{2}$$

where D_{thres} is pre-set distance threshold, S_{thres} is pre-set score threshold and S_{Range} is the range of score value.

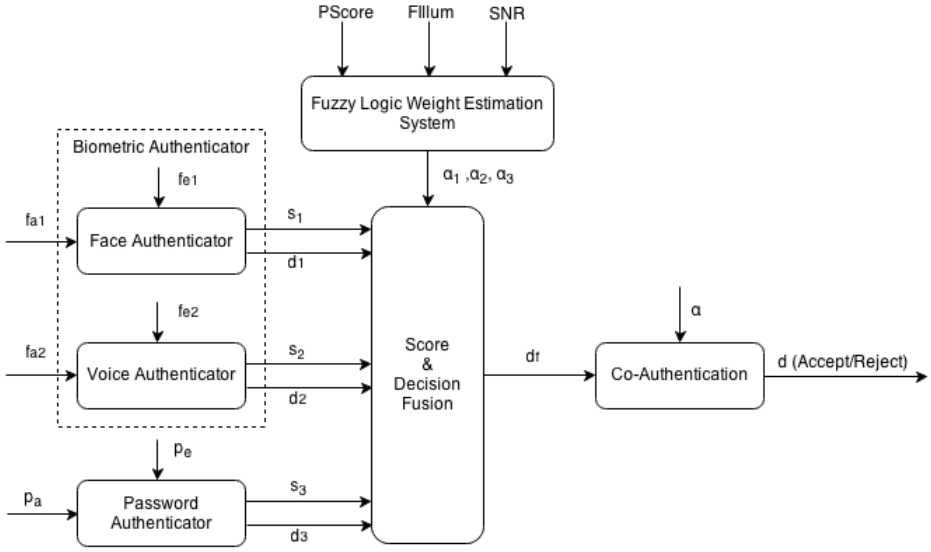


Fig. 1: Co-Authentication system architecture

2.2 Password Authenticator

In *Password Authenticator*, we use salted hashing algorithm to protect user's password. During the enrollment phase, P_e is hashed into hash value H_e using *SHA-256* algorithm. This value is then stored in database for later phase. In the authentication phase, the hash value of P_a is compared with H_e to generate d and s (see Equation 3):

$$\begin{cases} d = false, s = 0, & \text{if } H_e \neq H_a \\ d = true, s = S_{default}, & \text{if } H_e = H_a \end{cases}, \tag{3}$$

where $S_{default}$ is pre-set score value.

2.3 Score & Decision Fusion

The final value d_f is computed from the triad of score (s_1, s_2, s_3), validating value (d_1, d_2, d_3) and weight value $(\alpha_1, \alpha_2, \alpha_3)$ which are the output values of face, voice and password authenticator. We use two methods for obtaining weight value $(\alpha_1, \alpha_2, \alpha_3)$: (i) average score fusion (each α_i equals to $\frac{1}{3}$) , (ii) fuzzy logic fusion. The experimental results of each method are shown in Section 4.

$$d_f = \begin{cases} s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3, & \text{if } d_1 = d_2 = d_3 = true \\ 0, & \text{if } d_1 = false \text{ or } d_2 = false \text{ or } d_3 = false \end{cases} \quad (4)$$

where $\alpha_1 + \alpha_2 + \alpha_3 = 1$. Noted that, (s_1, s_2, s_3) is normalized to range of $[0, 100]$.

2.4 Co-Authentication

The final decision d (Accept/Reject) is determined based on the final score d_f and a pre-set threshold α. If d_f is greater than α, user is granted access to the system, otherwise, user is denied.

3 Fuzzy Logic Weight Estimation System

The performance of one co-authentication system is often affected by many external factors (lighting conditions, noise or strength of passwords), so the weight assigned to each individual authentication component should reflect the reliability of its use in the system. In this work, we propose a *Fuzzy Logic Weight Estimation System* in order to adjust the weight for authentication components depending on the external factors mentioned above.

3.1 Output Variables

Output of the system are three fuzzy variables $\mathrm{W_{face}}$, $\mathrm{W_{voice}}$ and $\mathrm{W_{Pass}}$ which correspond to three weights for face-based authentication, voice-based authentication and password-based authentication respectively. These values range from 0 to 1 (higher values implying higher confidence). The fuzzy sets of these output variables are triangular membership functions that define three levels of output weight (high/medium/low) for each variable. Before these weights are used in score fusion, they need to be normalized (see Equation 5):

$$W^j_{normalized} = \frac{W_j}{\sum_{i=1}^{n} W_i}, \quad (5)$$

where $\mathrm{W_j}$ is j^{th} weight and n is the total number of weights.

3.2 Input Variables

There are three input variables, FIllumi, PScore and SNR corresponding to illuminance of face images, strength of passwords the signal-to-noise-ratio of audios. The fuzzy sets of these variables are trapezoidal membership functions (see Equation 6) that define three levels of input variables (high/medium/low).

$$f(x) = \begin{cases} 0, & , (x < a) \text{ or } (x > d) \\ \frac{x-a}{b-a}, & , a \leq x \leq b \\ 1, & , b \leq x \leq c \\ \frac{d-x}{d-c}, & , c \leq x \leq d \end{cases} \tag{6}$$

FIllum. FIllum is illuminance of face images, this value ranges from 0 to 255 and it is estimated using two following steps:

1. Convert the input face image to grayscale (see Equation 7):

$$P_{Bi} = 0.299R_i + 0.587G_i + 0.114B_i, \tag{7}$$

   where R_i, G_i and B_i are Red, Green and Blue values of i^{th} pixel.
2. Calculate the average brightness of the grayscale image (see Equation 8):

$$FIllum = \frac{\sum_{i=1}^{n} P_{Bi}}{n}, \tag{8}$$

   where P_{Bi} is the grayscale value of i^{th} pixel and n is the total number of pixels.

Illuminance is divided into five groups: very low [0-40], low [40-109], medium [110-146], high [147-214] and very high [215-255], their Equal error rate (ERR)

Table 1: ERR of five different illuminance groups

Illuminance	Very low	Low	Medium	High	Very high
ERR	$> 50\%$	46%	24%	48%	$> 50\%$

are shown in Table 1. Based on the ERRs of the illuminance groups, parameters used by FIllum membership functions are selected and detailed in Table 2:

Table 2: The parameters used by FIllum membership functions

Parameters	$\text{FIllum}_{\text{high}}$	$\text{FIllum}_{\text{med}}$	$\text{FIllum}_{\text{low}}$
a	128	64	$-\infty$
b	215	110	$-\infty$
c	$+\infty$	146	40
d	$+\infty$	192	128

SNR. SNR is defined as the power ratio between a signal (meaningful information) and the background noise (unwanted signal):

$$SNR = 10 \log_{10} \frac{P_{signal}}{P_{noise}}, \tag{9}$$

where SNR is measured in decibel (dB), P_{signal} is the peak speech power and P_{noise} is the mean noise power. The SNR values are obtained by using the WADA algorithm [9]. SNR is divided into five groups of intervals: very low [10-16], low [17-22], medium [23-43], high [44-50] and very high [51-60] (their ERR are shown in Table 3). We observe that utterance with higher SNR tends to have

Table 3: ERR of 5 different SNR groups

SNR (dB)	Very low	Low	Medium	High	Very high
FAR	16%	8.3%	7.8%	7%	6.5%

lower ERR. Based on this observation, we select parameters for SNR membership functions. The parameters are shown in Table 4:

Table 4: The parameters used by SNR membership functions

Parameters	SNR_{high}	SNR_{med}	SNR_{low}
a	40	18	$-\infty$
b	50	22	$-\infty$
c	$+\infty$	40	16
d	$+\infty$	45	22

PScore. PScore represents the password strength. In this paper, we measure this value using the method proposed by Jamuna KS, Karpagavalli S, and Vijaya MS in [4]. The strength of passwords ranges from 0 to 100 and it is categorized into 5 classes (see Table 5). Based on this categorization, parameters

Table 5: Different classes of password strength

Class	Very weak	Weak	Good	Strong	Very strong
Score	< 20	21 - 39	40 - 59	60 - 79	80 - 100

used by PScore membership functions are selected and detailed in Table 6:

Table 6: The parameters used by PScore membership functions

Parameters	$\text{PScore}_{\text{high}}$	$\text{PScore}_{\text{med}}$	$\text{PScore}_{\text{low}}$
a	60	20	$-\infty$
b	80	40	$-\infty$
c	$+\infty$	60	20
d	$+\infty$	80	40

3.3 Fuzzy Control Rules

The general form of fuzzy control rules which are used in the system is:

R_i IF(x is (Y/N)) and (y is (Y/N)) and (z is (Y/N)) then t is V_i,

where x, y, z and t are linguistic variables representing the input variables and the output variable, respectively, and V_i is the linguistic value of t. If the condition in a rule specifies a Y concept, the input will be set equaling to the membership degree, β. For an N concept, the input will be set at $1-\beta$. Fuzzy control rules for FIllum, SNR and PScore are shown in Table 7, Table 8, and Table 9 respectively.

Table 7: Fuzzy rules for FIllum

ID	Fuzzy Rules
R_1	($\text{FIllum}_{\text{high}}$ is N) and (IF $\text{FIllum}_{\text{med}}$ is Y) and ($\text{FIllum}_{\text{low}}$ is N) then W_{Face} is High
R_2	($\text{FIllum}_{\text{high}}$ is Y)and (IF $\text{FIllum}_{\text{med}}$ is Y) and ($\text{FIllum}_{\text{low}}$ is N) then W_{Face} is Med
R_3	($\text{FIllum}_{\text{high}}$ is N) and (IF $\text{FIllum}_{\text{med}}$ is Y) and ($\text{FIllum}_{\text{low}}$ is Y) then W_{Face} is Med
R_4	($\text{FIllum}_{\text{high}}$ is N) and (IF $\text{FIllum}_{\text{med}}$ is N) and ($\text{FIllum}_{\text{low}}$ is Y then W_{Face} is Low
R_5	($\text{FIllum}_{\text{high}}$ is Y)and (IF $\text{FIllum}_{\text{med}}$ is N) and ($\text{FIllum}_{\text{low}}$ is N) then W_{Face} is Low

Table 8: Fuzzy rules for SNR

ID	Fuzzy Rules
R_1	IF(SNR_{high} is Y) and (SNR_{med} is N) and (SNR_{low} is N) then W_{Voice} is High
R_2	IF(SNR_{high} is Y) and (SNR_{med} is Y) and (SNR_{low} is N) then W_{Voice} is High
R_3	IF(SNR_{high} is N) and (SNR_{med} is Y) and (SNR_{low} is N) then W_{Voice} is Med
R_4	IF(SNR_{high} is N) and (SNR_{med} is Y) and (SNR_{low} is Y) then W_{Voice} is Med
R_5	IF(SNR_{high} is N) and (SNR_{med} is N) and (SNR_{low} is Y) then W_{Voice} is Low

Table 9: Fuzzy rules for PScore

ID	Fuzzy Rules
R_1	IF($\text{PScore}_{\text{high}}$ is Y) and ($\text{PScore}_{\text{med}}$ is N) and ($\text{PScore}_{\text{low}}$ is N) then W_{Pass} is High
R_2	IF($\text{PScore}_{\text{high}}$ is Y) and ($\text{PScore}_{\text{med}}$ is Y) and ($\text{PScore}_{\text{low}}$ is N) then W_{Pass} is High
R_3	IF($\text{PScore}_{\text{high}}$ is N) and ($\text{PScore}_{\text{med}}$ is Y) and ($\text{PScore}_{\text{low}}$ is N) then W_{Pass} is Med
R_4	IF($\text{PScore}_{\text{high}}$ is N) and ($\text{PScore}_{\text{med}}$ is Y) and ($\text{PScore}_{\text{low}}$ is Y) then W_{Pass} is Med
R_5	IF($\text{PScore}_{\text{high}}$ is N) and ($\text{PScore}_{\text{med}}$ is N) and ($\text{PScore}_{\text{low}}$ is Y) then W_{Pass} is Low

3.4 System Architecture

Fig. 2 shows the flow of *Fuzzy Logic Weight Estimation System*. Input of the system is numerical measurement of an external factor. First of all, this input factor is fuzzified. In detail, for each linguistic variable, the crisp value is converted to fuzzy value by evaluating the values of the corresponding membership functions. For example, if the input factor FIllum = 80, the degree of "medium illuminance" is 0.35. After fuzzification, the system will infer results from the

logical rules (fuzzy rules) using the linguistic variables. The degree of the rule antecedents is then computed by taking the minimum of all present degrees. This degree is also chosen as the degree with which the rule is fulfilled. E.g. the FIllum = 80 fulfills the first rule with degree(R1) = min{1 - $\text{FIllum}_{\text{high}}$(80), $\text{FIllum}_{\text{med}}$(80), 1 - $\text{FIllum}_{\text{low}}$(80)} = min{1 - 0, 0.35, 1 - 0.55} = 0.35. The fuzzy outputs for all rules are then aggregated to one fuzzy set. The degree of a linguistic variable is computed by taking maximum of all rules describing this variable i.e. degree(medium) = max{degree(R2), degree(R3)}. Finally, to get the weight (degree of support) of the feature, defuzzification using standard centroid-of-area technique is performed. Details about fuzzy logic system can be found in [6].

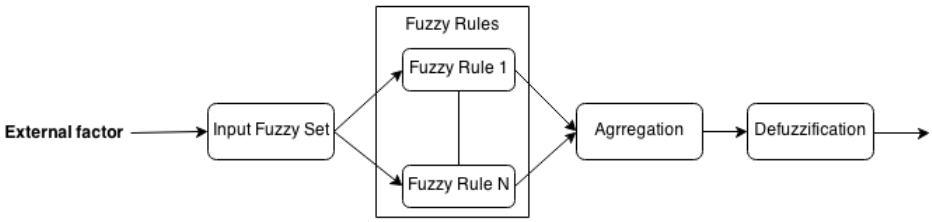


Fig. 2: Fuzzy logic weight estimation system

4 Experimental Results

We conduct four experiments to evaluate authentication performance of the proposed system as well as individual systems such as face-based authentication system and voice-based authentication. To perform these experiments, we use 110 face images and 110 utterances of 20 different people which are selected randomly from The Extended Yale Face Database B [5] and Voxforge [1] respectively.

4.1 Face-based Authentication

Firstly, we use 60 images of 10 different people (6 images per person) to evaluate the False reject rate (FRR) of face-based authentication. The first image of one person is used for enrollment and the remaining 5 images are used for authentication. Then, in order to evaluate the False accept rate (FAR), we use 50 images of 10 other people to authenticate with the enrolled images. The FAR and FRR of face-based authentication are depicted in Fig. 3a. With the best distance threshold is 870, the FAR is 24% and the FRR is 20%.

4.2 Voice-based Authentication

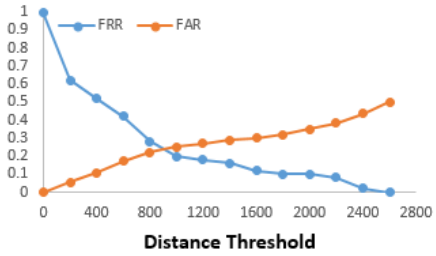
The settings to measure the FRR and FAR of this experiment are similar to the settings used in face-based authentication. The FAR and FRR of voice-based authentication are shown in Fig. 3b. The best distance threshold is 17.5, and with this threshold, the FAR and FRR are 13% and 10% respectively.

4.3 Co-Authentication System Using Average Score Fusion

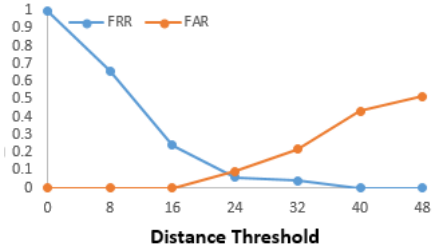
To begin, 60 test sets of 10 different people are used to estimate the FRR of the system. A test set of each person, which includes a face image, an utterance and a password, is used to enroll. The five other test sets are used for authentication. Next, to evaluate the FAR, 50 remaining test sets of 10 other people are used to authenticate with enrolled test sets. The FAR and FRR of the system are depicted in Fig. 3c. As can be seen, the FAR is 1.4% and the FRR is 2% at the score threshold of 50.

4.4 Co-Authentication System Using Fuzzy Logic Fusion

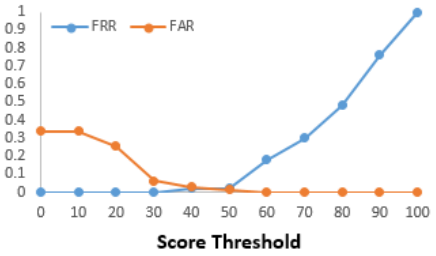
The settings to measure the FRR and FAR of this experiment are similar to the settings used in co-authentication system using average score fusion. The FAR and FRR of the system are illustrated in Fig. 3d. With the best score threshold of 45, the FAR and FRR are 0.4% and 0% respectively.



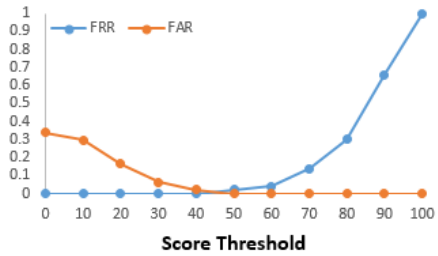
(a) FAR and FRR for face-base authentication



(b) FAR and FRR for voice-base authentication



(c) FAR and FRR for co-authentication system using average score fusion



(d) FAR and FRR for co-authentication system using fuzy logic fusion

Fig. 3: Experimental results

5 Conclusions and Future Works

In this paper, we presented a co-authentication system that combines password-based, face-based and voice-based authentication. Co-authentication system using average score fusion produced relative FAR and FRR improvement of 22.6%

and 18% compared with face-based authentication, 11.6% and 8% compared with voice-based authentication. We also proposed a *Fuzzy Logic Weight Estimation System* in order to accounted for external factors which affect authentication performance such as lightning conditions, noise and strength of passwords. As a result, the combination of co-authentication system and fuzzy logic weight estimation system generated further relative improvement of 1% and 2% on FAR and FRR compared with co-authentication system using average score fusion.

However, the proposed system accounted for only three external factors (lightning, noise and strength of passwords). Some additional factors such as user's head pose in face verification, quality of utterances in voice verification and other ones are need to be considered in the future.

References

1. Voxforge database. http://voxforge.org. Accessed: 2013-11-26.
2. Vincenzo Conti, Giovanni Milici, Patrizia Ribino, Filippo Sorbello, and Salvatore Vitabile. Fuzzy fusion in multimodal biometric systems. In Bruno Apolloni, RobertJ. Howlett, and Lakhmi Jain, editors, *Knowledge-Based Intelligent Information and Engineering Systems*, volume 4692 of *Lecture Notes in Computer Science*, pages 108–115. Springer Berlin Heidelberg, 2007.
3. Tran Tri Dang, Quynh Chi Truong, and Tran Khanh Dang. Practical construction of face-based authentication systems with template protection using secure sketch. In *ICT-EurAsia*, pages 121–130, 2013.
4. Jamunna.K.S. Dr.Vijaya.M.S., Karpagavalli.S. In *In proceeding of International Journal of Recent Trends in Engineering*. Academy Publishers, 2009.
5. A.S. Georghiades, P.N. Belhumeur, and D.J. Kriegman. From few to many: Illumination cone models for face recognition under variable lighting and pose. *IEEE Trans. Pattern Anal. Mach. Intelligence*, 23(6):643–660, 2001.
6. M. Hellmann. Fuzzy logic introduction. *Epsilon Nought Radar Remote Sensing Tutorials*, 2001.
7. H.P. Hui, H.M. Meng, and Man-Wai Mak. Adaptive weight estimation in multibiometric verification using fuzzy logic decision fusion. In *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on*, volume 1, pages I–501–I–504, 2007.
8. E. Jonsson. Co-authentication - a probabilistic approach to authentication, 2007. Supervised by Assoc. Prof. Christian D. Jensen, IMM, DTU.
9. Chanwoo Kim and Richard M. Stern. Robust signal-to-noise ratio estimation based on waveform amplitude distribution analysis. In *INTERSPEECH*, pages 2598–2601. ISCA, 2008.
10. Tiwari and Vibha. Mfcc and its applications in speaker recognition. *International Journal on Emerging Technologies*, I(1):19 – 22, 2010.
11. Matthew Turk and Alex Pentland. Eigenfaces for recognition. *J. Cognitive Neuroscience*, 3(1):71–86, January 1991.
12. K.N. Plataniotis Yongjin Wang. In *Biometrics Symposium*. Springer-Verlag, 2007.