International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 2, Issue 4, pp: (86-94), Month: October - December 2014, Available at: www.researchpublish.com

Face Recognition for Security System with the Removal of Lighting Effects

Ashly Mathew[1], Somy P Mathew[2]

[1]M.Tech Student of ECE Department [2]Assistant professor of ECE Department
[1,2,]Viswajyothi College of Engineering and Technology, Vazhakulam, India

Abstract: **Nowadays, mobile security has become increasingly important in mobile computing. Mobile devices like PDA, Mobile phones etc are vulnerable to theft because of their small size. So a simple and convenient authentication system is required to protect private information stored in the mobile devices. This paper proposes a biometric authentication method using face and teeth modalities for mobile devices. Image based authentication is performed based on the Embedded Hidden Markov Model algorithm. Scores obtained from multiple modalities are integrated into a single score. Based on the fused score the person is accepted or rejected.**

Keywords: **Biometric traits, Embedded Hidden Markov Model, Image Authentication, Lighting effects.**

I. INTRODUCTION

BIOMETRICS technologies are referring to identifying individuals based on their distinguishing biological or behavioural traits. The biometric systems that offer a reliable and user-friendly approach are in high demand for mobile devices because mobile devices are often exposed in public places where they are vulnerable to theft or loss. Aside from hardware loss, users may also be concerned about the exposure of sensitive information stored in mobile devices. Therefore we present a biometric mobile device security system that combines information obtained from face, teeth and voice modalities to improve the performance of security systems.

Biometrics using facial features is unreliable due to changing make-up, moustache, beard, hair style etc. Thus, teeth image is also suggested as a biometric trait for individual authentication, instead of using a facial image only. Although teeth authentication is also affected by lighting effects like the face, it is few sensitive or ineffective to factors such as face expression, make-up, moustache, beard, and hair style. Biometrics utilizing teeth images is reliable and robust, since teeth are unique to each individual and hardly change during adulthood.

Based on these studies, we propose an enhanced security system using face and teeth modalities for mobile devices. The proposed system has an advantage that the face and teeth traits can be simultaneously captured by a mobile device equipped with a camera. Thus, impostors attempting to use the device can be prevented in practical applications. Several fusion techniques such as the weighted-summation rule, Fisher classifier and Gaussian classifier can be employed to integrate the face and teeth modalities at a fusion stage.

The proposed system was evaluated using a database collected via a laptop, i.e., one of the mobile devices. The database consists of 10 images for each of 4 subjects, i.e., 7 images for authorized individual and a single image for each unauthorized person. From the experimental results, the proposed multimodal personal authentication approach worked well. Removal of lighting effects [3], [4] also improved the performance of the proposed system compared to the other approaches [1], [2].

The remainder of this paper is organized as follows. In section 2 we present outline of the proposed system. Sections 3 describes image based authentication. Section 4 describes the fusing method used to combine the two modalities. The experimental results are presented in section 5, and we conclude in section 6.

II. PROPOSED METHOD

This paper proposed a biometric mobile device security system that integrates information obtained from face and teeth modalities. The whole architecture of the proposed system is depicted in Fig. 1.

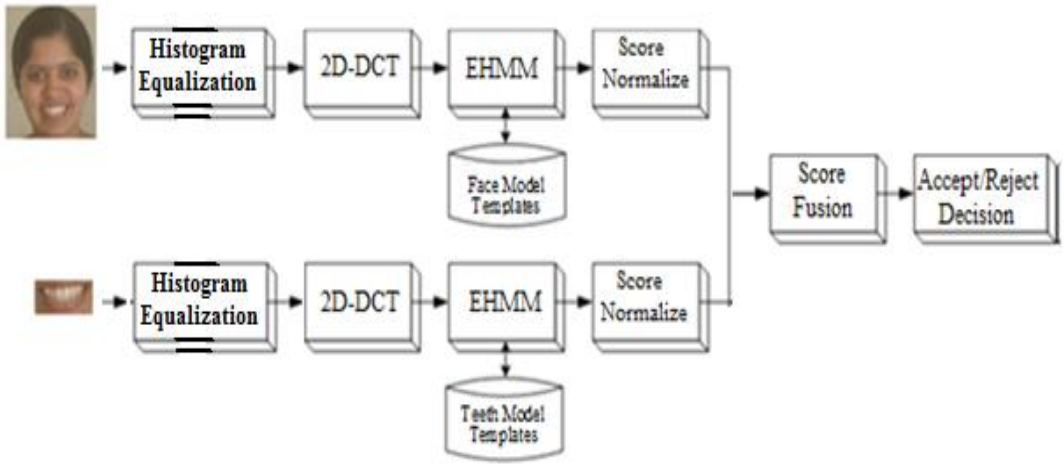

Fig.1. System architecture

The proposed system is based on image-based authentication using face and teeth modalities. Image-based authentication is comprised of the steps: image acquisition, region detection, and the authentication phase based on the EHMM (Embedded Hidden Markov Model) algorithm [5], [6]. These stages are equivalently applied for face and teeth based authentication. However, the number of EHMM states is different for each procedure. In order to model the face, we compose the state structure of EHMM using five super-states with three, five, five, five and three embedded-states, respectively.

The teeth image is modeled using three super-states and embedded-states of three, five and three in each super-state. To avoid the various illumination effects we use histogram equalization on face image and histogram equalization with a pre-processing procedure on teeth image. The pre-processing procedure is rotated-angle compensation. Rotated-angle compensation can be successfully performed since both sides of the teeth image are usually dark, and we can calculate the rotated angle with a horizontal line connecting both centers of the image.

The entire input image is rotated with the computed angle information as shown in Fig. 2 (a). The face and teeth regions are detected using the vision cascade object detector as shown in Fig. 2 (b), and the face and teeth subjects used in authentication are acquired by cropping their corresponding regions. The resultant face and teeth subjects are shown in Fig. 2 (c) and (d), respectively. After subject acquisition, the authentication phases are similarly performed with face and teeth subjects using EHMM algorithms, leading to the corresponding probabilities, respectively.

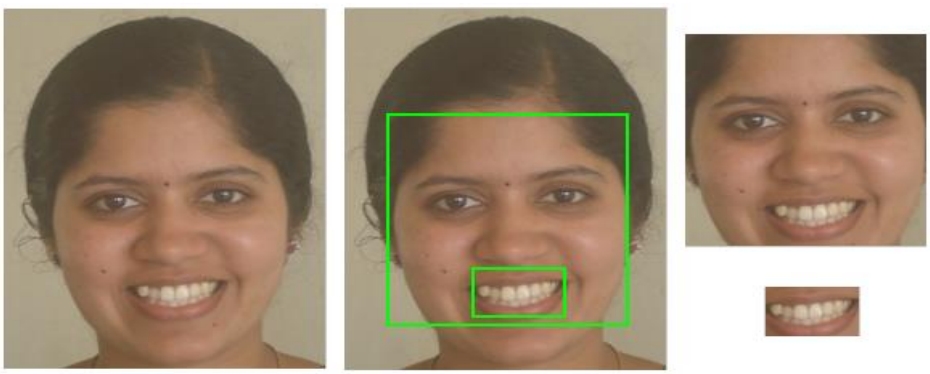

Fig. 2: Subject acquisition procedure: (a) input image rotation using computed angle information, (b) face and teeth region detection in rotated image, (c) face image as a biometric trait, (d) teeth image as a biometric trait.

The proposed system is composed by integrating the probabilities of the face and teeth authentications at the score level. Before integrating the scores of the multiple modalities into a single score, score normalization is necessary. This is because, the scores obtained from individual modalities may not be homogeneous. Score normalization involves mapping the raw scores into normalized scores of a common domain. We use the sigmoid function to map the raw scores of face, teeth and voice modalities into the [0, 1] interval. Once normalized, the normalized scores of multiple modalities can be combined using score level fusion technique. In this proposed system, weighted-summation method is used.

III. IMAGE BASED AUTHENTICATION

Image-based authentication is subdivided into face-based and teeth-based authentication. It is comprised of the following steps: image acquisition, region detection, and the authentication phase based on the EHMM algorithm. These stages are equivalently applied to face and teeth authentication.

A. Face Based Authentication

The face authentication is composed of image acquisition, pre-processing procedure, face region detection and authentication phase as sequential steps. The main problem related to face based authentication is lighting problem. The illumination problem occurs in an uncontrolled environment where "the same face appears different due to a change in lighting". One solution to this problem involves pre-processing the images and introducing contrast normalization and compensation. The cascade object detector uses the Viola-Jones algorithm to detect people's face.

Pre-processing procedure segments an image into different regions according to its different local illumination conditions. Then, every region is processed according to its local illumination condition so as to alleviate the side lighting effect caused by uneven illumination. When an image has even lighting, the illumination property of the whole image is homogeneous. So the segmentation step only generates one region, i.e., the whole image. Thus, this method is adaptive to the actual image illumination conditions, and it is region-based. Region-based histogram equalization is applied on the low-frequency coefficients to minimize illumination variations under different lighting conditions.

After histogram equalization, Cascade object detector is used to detect the face region. The cascade object detector uses the Viola-Jones algorithm to detect the face. The basic principle of the Viola-Jones algorithm is to scan a sub-window capable of detecting faces across a given input image. 2D-DCT is performed on the face region which is detected using Viola-Jones face detector. The computed coefficients are then ordered in a zig-zag fashion to reflect the amount of information stored in each coefficient. Lower order coefficients usually contain more information. After ordering the 2D-DCT coefficients, they are used to form an observation vector of EHMM. In order to model the face, we compose the state structure of EHMM using five super-states with three, five, five, five and three embedded-states, respectively. Each super-state represents the vertical face features such as forehead, eyes, nose, teeth and chin in the face image, and each embedded state in the super-state represents the horizontal local features.

The EHMM $\lambda = (A, B, \Pi)$ is initialized. The training data is uniformly segmented from top to bottom in N = 5 states and the observation vectors associated with each state are used to obtain initial estimates of the observation probability matrix B. The initial values for A (the state transition probability matrix) and Π (the state probability distribution matrix) are set given the left to right structure of the face model. In the next steps the model parameters are re-estimated using the EM procedure to maximize $P(O \mid \lambda)$ where O is the observation vector. The iterations stop, after model convergence is achieved, i.e., the difference between model probability at consecutive iterations (k and k + 1) is smaller than a threshold C,

$$\left| P\left(O \mid \lambda^{(k+1)}\right) - P\left(O \mid \lambda^{(k)}\right) \right| < C$$

In the recognition/ testing phase, a set of test images, not used in the training, are considered to determine the recognition performances of the system. After extracting the observation vectors as in the training phase, the probability of the observation vector given each EHMM face model is computed. A face image t is recognized if

$$p(O^{(t)} \mid \lambda_t) = p(O^{(t)} \mid \lambda_n)$$

B. Teeth Based Authentication

The teeth authentication is composed of image acquisition and teeth region detection with pre-processing procedure, feature extraction of teeth image and authentication phase as sequential steps. In this system, the AdaBoost algorithm based on Haar-like features for teeth region detection, and the EHMM algorithm with 2D-DCT as feature vector are used in the process of teeth authentication.

The first phase of teeth authentication is the detection of the teeth region in the acquired images. The proposed system utilizes the AdaBoost algorithm based on Haar-like features introduced by Viola and Jones [7]-[10]. Haarlike features are used in the process of searching for the teeth region, and prototypes have been trained to accurately represent the teeth region through the AdaBoost learning algorithm. After detecting the teeth region, the detected teeth region undergoes the pre-processing procedure, i.e., rotated-angle compensation, to improve performance.

Feature extraction of a teeth image using 2D-DCT consists of two steps [8]. In the first step, the pre-processed teeth image is divided in small block images. In the next step, the 2D-DCT coefficients of the image block are calculated. The computed coefficients are then ordered in a zig-zag fashion. These coefficients are used to form an observation vector of EHMM.

IV. SCORE NORMALIZATION AND FUSION

A. Score Normalization

Normalization involves transforming the raw-scores obtained using different modalities to a common domain using a mapping function. We use the sigmoid function to normalize the raw-scores of face and teeth. The normalization method using the sigmoid function maps the raw-scores to the [0, 1] interval, and is defined by

$$\sigma_i = \frac{1}{1+\exp\left(-\tau_i\left(O_{i,orig}\right)\right)}$$

Where, $\tau_i(o_{i,orig})$ is defined $\left[o_{i,orig} - (\mu_i - 2\sigma_i)\right]/2\sigma_i$, $o_{i,orig}$ is the raw-score of i^{th} modality, o_i is normalized-score, and μ_i and σ_i are the mean and the standard deviation of the raw scores, respectively.

B. Score Fusion

Once normalized, the normalized-scores obtained from face and teeth authentication are combined using a simple weighted-summation operation. This fusion method does not require any training phase [11], [12]. The simple weighted summation method is given by

$$S_m = p\ S_f + (1-p)S_t,\ 0 \le p \le 1$$

Where, S_f and S_t are the normalized-scores of the face and teeth, respectively, and S_m is the fused-score. p is the weight of the normalized-scores obtained from teeth authentication, while (1− p) is the weight of the normalized-scores obtained from voice authentication. If the fused score S_m is greater than or equal to a pre-defined value the person is accepted as a valid person. Otherwise, the person is rejected.

V. EXPERIMENTAL RESULT

The paper work includes the simulation of the proposed security system by using MATLAB, XILINX ISE software. The hardware implementation of the system is done in Cyclone II FPGA kit and software used for implementation is Quartus II 8.0.

A. Experimental Setup and Database Collection

The biometric mobile device security system is implemented using MATLAB on a THOSHIBA laptop equipped with a camera. We construct a database consisted by face and teeth images, under constraints such as illumination and noiseless environments, to evaluate the proposed system. Especially, we constraint the teeth images to be captured frontal views, where the teeth expressions recommended a teeth occlusion state. If the illumination intensity is low in an indoor environment histogram equalization is performed. The captured images are acquired at a resolution of 256 × 256 pixels,

where captured images are normalized to 56 × 46 pixels after the pre-processing procedure for face image and 40 × 56 for teeth image. The experimental database totally has 7 images and voices per individual. We use 5 images of individual for training, and the remaining images are used to evaluate performance. The sample biometric traits for a single person are shown in the Fig. 3. For a single person 7 different poses are considered. This is the database used for training and testing (Fig. 4).

Fig. 3: Sample biometric traits.

Fig. 4: Different poses.

B. Simulation Results in MATLAB

During the training phase, features are extracted for each image. The image is pre-processed to avoid the illumination problem. The result of histogram equalization is shown in Fig. 5. After histogram equalization the face region is detected using Viola-Jones detector as shown in Fig. 6. 2D-DCT is performed on face region. The computed coefficients are then ordered in a zig-zag fashion. After ordering, the 2D-DCT coefficients, which are computed from all block images, are used to form an observation vector of EHMM.

Fig. 5: Histogram Equalization.

Fig. 6: Viola-Jones Detector output.

For a valid person, the Image based authentication gave a positive result. The scores obtained from face and teeth authentication are combined using a simple weighted-summation operation. If the fused score S_m is greater than or equal to a pre-defined value the person is accepted as a valid person. Otherwise, the person is rejected. The MATLAB result of a valid person shown is in Fig. 7. The person is accepted since her face and teeth image are matched with the database stored in the system. The MATLAB result of an invalid person shown is in Fig. 8. The person is rejected since her face and teeth images are doesn't matched with the database stored in the system.

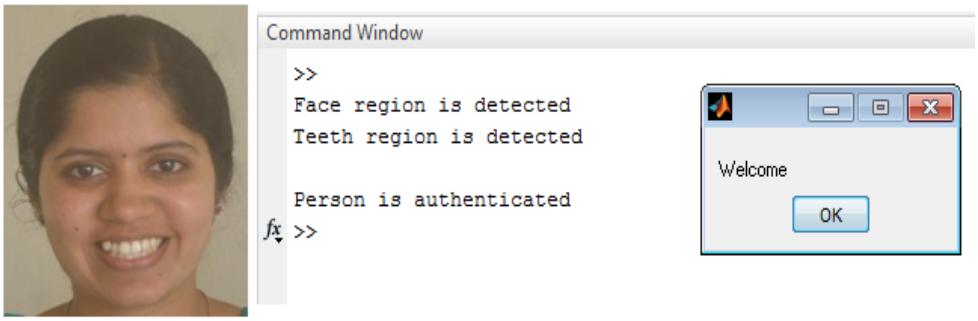

Fig. 7: MATLAB result for an accepted person

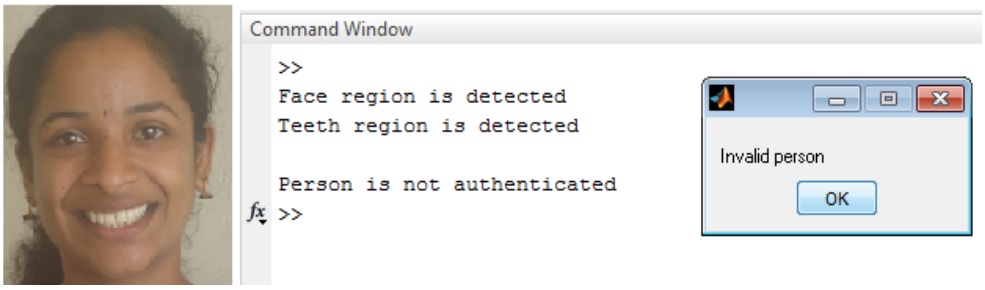

Fig. 8: MATLAB result for a rejected person

C. Simulation Results in XILINX

The proposed security system is designed using VHDL language and simulated with the use of XILINX's ISE. Under poor illumination condition the pre-processing of train and test image is performed using kernel multiplication. Xilinx simulation result of histogram equalization is shown in Fig. 9(a). The corresponding image thus obtained in MATLAB is shown in 9(b). After histogram equalization, the face and teeth regions are detected. In VHDL the face and teeth regions are detected using blob method. The pre-processing of teeth region is done in VHDL. i.e., the centroid of the teeth region is calculated. 2D-DCT of face and teeth region is performed based on row-column algorithm. Xilinx simulation result of face and teeth regions detection is shown in Fig. 10(a). Corresponding images obtained in MATLAB are shown in Fig. 10(b) and (c).

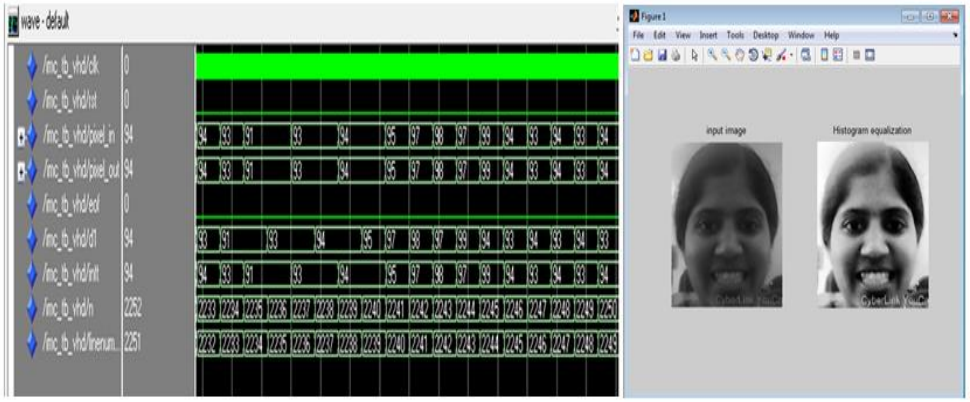

Fig. 9: Xilinx result of Histogram Equalization

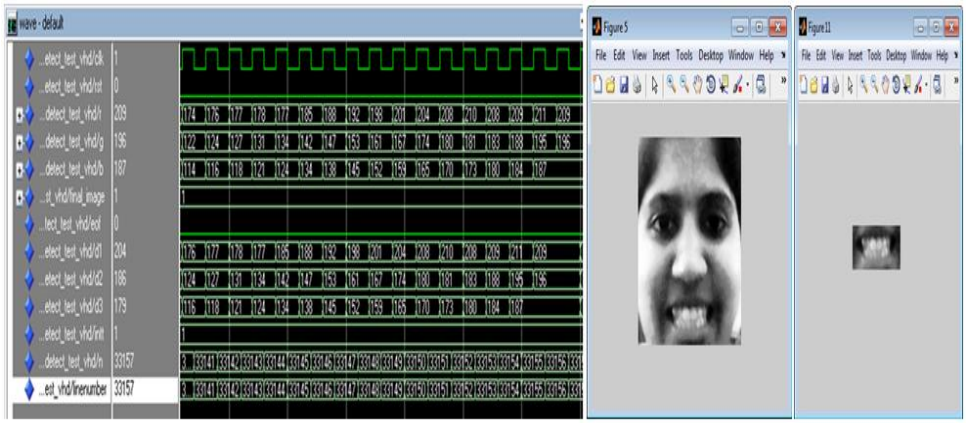

Fig. 10: Xilinx result of face and teeth region detection

The proposed system is implemented using Cyclone II FPGA kit. The test and train images are given to the FPGA board from MATLAB using UART with the help of USB blaster. A camera is interfaced with the FPGA board in order to make the system real-time. The processed data is send back to MATLAB via UART from FPGA board. A clock frequency of 50MHz is applied to the system, which is the maximum frequency available on the board. Implementation diagram of the proposed system is shown in Fig. 11. Implementation result of mobile device security system in Quartus is shown in the Fig. 12.

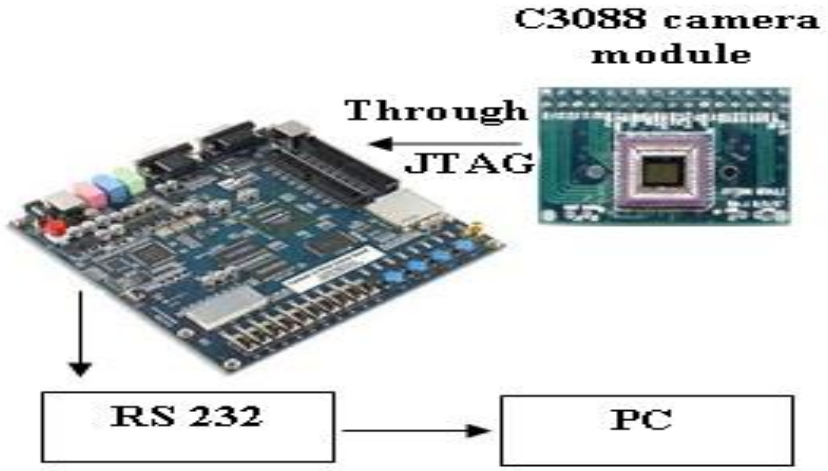

Fig. 11: Implementation Diagram

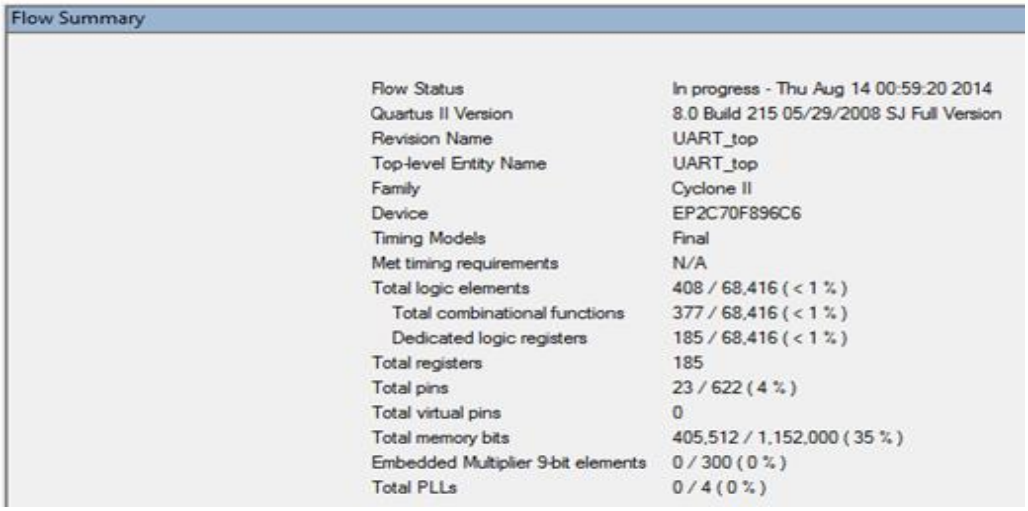

Fig. 12: Flow summary of Biometric Mobile Device Security System

D. Comparison with Other Algorithms

The effectiveness of the proposed system is shown by comparing its results with those of the popular methods, such as PCA, ICA and LDA. The recognition rates are illustrated in Table I. it is shown that our proposed method outperforms all other methods.

TABLE I: RECOGNITION RATE COMPARISONS BETWEEN DIFFERENT METHODS ON DIFFERENT DATABASES

Method	Yale B	Extended Yale B	Real-Time
PCA	85	88	80
ICA	86	88.5	83
LDA	86.5	89.5	85
EHMM with lighting effects	95	95	97
Proposed Method (EHMM without lighting effects)	98	98.5	100

VI. CONCLUSION

Recently, there have been many studies on multimodal biometric approaches that integrate the information generated by multiple biometric sources in a wide variety of fields, since they usually perform better than the methods based on a single biometric trait. On this basis, we proposed a personal authentication method using face and teeth modalities for security. The main problem related to authentication is lighting problem. The illumination problem occurs in an uncontrolled environment where "the same face appears different due to a change in lighting". One solution to this problem involves pre-processing the images and introducing contrast normalization and compensation.

The proposed method was widely composed of image-based authentication using face and teeth. Image-based authentication consists of image acquisition, region detection with a pre-processing procedure, and an authentication phase. These stages were similarly applied to the face and teeth. We compose the security system by fusing the scores using a weighted-summation method. The fused-score is used to classify the unknown user into the acceptance or rejection. The proposed security system is simulated in MATLAB, Modelsim and experimentally validated using Cyclone II FPGA.

We plan, in future works, to enhance the performance of the system by integrating another biometric trait. Furthermore, we would like to extend this study to consider other fusion methods.

REFERENCES

[1] Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong, "Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security" IEEE Transactions on Consumer Electronics, vol. 56, no. 4, November 2010.

[2] Dong-Ju Kim and Kwang-Seok Hong, "Multimodal Biometric Authentication using Teeth Image and Voice in Mobile Environment", IEEE Transactions on Consumer Electronics, vol. 54, no. 4, pp. 1790- 1797, 2008.

[3] Shan Du and Rabab K. Ward, "Adaptive Region-Based Image Enhancement Method for Robust Face Recognition under Variable Illumination Conditions", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 20, No. 9, September 2010.

[4] K. Venkataramani, S. Qidwai, and B. VijayaKumar, "Face authentication from cell phone camera with illumination and temporal variations," IEEE Trans. on Systems, Man and Cybernetics, vol. 35, no. 3, pp. 411- 418, 2005.

[5] Nefian, M. Hayes, "An Embedded HMM-based Approach for Face Detection and Recognition", IEEE International Conference on Acoustic Speech and Signal Processing, vol. 6, 1999.

[6] L. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition", Proc. IEEE. Vol. 77(2), 257-286, 1989.

[7] Tae-Woo KIM, Tae-Kyung CHO, "Teeth Image Recognition for Biometrics", IEICE Transactions on Information and Systems, vol. E89- D, no. 3, pp.1309-1313, 2006.

[8] K. Prajuabklang, P. Kumhom, T. Maneewarn, K. Chamnongthai, "Real-time Personal Identification from Teeth-image using Modified PCA", Proceeding of the 4th information and computer Engineering Postgraduate Workshop, vol. 4, no. 1, pp. 172-175, 2004.

[9] Dong-Ju Kim, Jeong-Hoon Shin, Kwang-Seok Hong, "Teeth recognition based on multiple attempts in mobile device", Journal of Network and Computer Applications, vol. 33, no. 3, pp. 283-292, 2010.

[10] Dong-Ju Kim, Jong-Bae Jeon and Kwang-Seok Hong, "Performance Evaluation of Feature Vectors for Teeth Image Recognition", The 4th Conference On New Exploratory Technologies (NEXT 2007 KOREA), October 25-27, 2007.

[11] Ross, A.K. Jain, "Information fusion in biometrics", Pattern Recognition Letter, vol. 24, pp. 2115-2125, 2003.

[12] Anil K. Jain, Arun Ross, Salil Prabhakar, "An introduction to biometric", IEEE Transaction On Circuits and System for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.