TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 15, No. 3, September 2015, pp. 591 ~ 596
DOI: 10.11591/telkomnika.v15i3.8447

Providing Authentication by Using Biometric Multimodal Framework for Cloud Computing

R. Parimala*[1], C. Jayakumar[2]
[1,2]Bharathiar University, Coimbatore, India
[1]S.S.K.V College of Arts and Science for Women, Kanchipuram, India
[2]CSE Department, RMK Engineering College, Kavaraipettai, India
*Corresponding author, e-mail: parimalasuresh80@gmail.com[1], cjayakumar2007@gmail.com[2]

Abstract

Secret knowledge, like remembering password or token based authentication systems are deemed inconvenience and difficult to use for users such as password may be forgotten or token may be lost. So burdens like remembering password and stolen or forged token based authentication have raised a current trend of biometric authentication system. Now in this current tech world, everyone needs security everywhere to protect our personal gadgets. So to keep it secured, biometric based approach can be applied for better convenience and ease of use for the user. In this paper, a novel hybrid multimodal approach for ear recognition and finger print recognition has been presented for better robustness and efficiency which can be applied in various fields of applications like authentication in banking transactions. Biometric based human recognition is rapidly gaining popularity due to breached of traditional security systems and the lowering cost of sensors. This paper comprehensively reviews multimodal recognition using ear pattern and finger print data, it is concluded that further research should investigate fast and fully automatic ear-finger print multimodal systems robust to occlusions and deformations.

Keywords: *multimodal biometrics, ear pattern, finger print, security, authentication*

1. Introdution

Currently the authentication methods can be broadly divided into three main areas which are:

a) Knowledge based
b) Token based
c) Biometric based authentication

A large number of users believe that an alternative method like biometrics to security would be a good idea. Because password may be forgotten and token may be lost. In this paper, study on multimodal biometrics using ear and finger print biometrics approach has presented to authenticate cloud users. First of all, ear does not change during human life as ascertained by Prague Doctor Inhofe [1], whereas face changes more significantly than any other part of human body. Other than those cosmetics, beard, mustache, hairstyle, emotions shows different state of mind such as happiness, sadness, fear or surprise. In addition to this color distribution is more uniform in ear rather than human face, iris or retina there is while working with grayscale, one does not lose much information. Besides ear is smaller than face, which means that it is possible to work faster and more efficiently with the image with the lower resolution which can be easily acquired by a camera. In addition, it is important to note that ear images cannot be disturbed by glasses, beard or makeup. Those are the reasons why ear biometric has been chosen by comparing with other biometrics such as face, iris & retina. However, sometimes occlusion by either hair or earrings is possible. Nevertheless, one can get rid of these negative points for typical applications. In addition with ear biometric, another biometric finger print recognition technique has added to increase the robustness and efficiency of the system.

Received June 4, 2014; Revised August 3, 2015; Accepted August 17, 2015

2. Biometric Systems

Biometric recognition systems represent pattern recognition systems, capable of recognizing individuals based on their physiological or behavioural traits [2]. These traits are considered to be unique to each individual and unlike knowledge or token-based security mechanisms cannot be forgotten, lost or stolen. The most common traits used for biometric recognition are: faces, fingerprints, irises, palm-prints, speech etc.

Biometric systems typically conduct one of two tasks: *identification* or *verification/authentication*. The verification/authentication task tries to validate the identity claim of the user currently presented to the system, while the identification task tries to determine, which of the registered user the acquired “live” biometric sample corresponds to. Hence, the identification problem is commonly considered to be a one-to-N matching problem, while the verification/authentication problem is considered to be a one-to-one matching problem. Biometric systems always comprise the same basic components regardless of whether they are designed for the cloud or any other platform.

a) A data acquisition component (or sensor) that captures a still image or video sequence of a user trying either to enroll into the system or to use the system for authentication/identification purposes.

b) A template generation component that uses machine learning, computer vision and pattern recognition techniques to derive a biometric template from the input data.

c) A database of biometric templates belonging to enrolled/registered users, and

d) A matching component that compares the biometric template derived from the “live” image with the appropriate template(s) stored in the database of the system and based on the outcome makes a decision regarding the identity of the user currently presented to the system. While the basic layout of a biometric recognition system is more or less the same on any platform (and biometric modality), there are, however, a number of aspects that are specific to the cloud.

3. Finger Print Recognition

The functionality of the existing local version of the FingerIdent system can be divided into two main categories:

a) **User registration (enrollment**), during which a biometric template of a given user is constructed and stored in the system’s database.

b) **User verification**, during which the identity claim of a given user is validated.

The registration process uses a fingerprint reader to capture the (biometric) fingerprint data. In the next phase the quality of the captured sample is evaluated and if it is found to be adequate, the system extracts features from it and stores them in the form of a biometric template in the database. During the verification process features from the captured “live” fingerprint are again extracted and compared to those stored in the database. The comparison is made based on pattern matching procedures, which form the foundation for the validation of the identity claim. An illustration of both function is shown in Figure1.

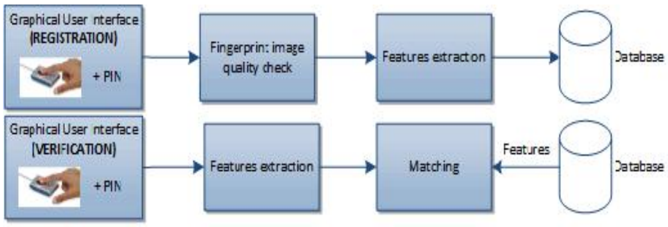


Figure 1. Simplified block diagram of biometric registration and verification

To reach the goal of devising a cloud-based biometric service, one needs to migrate the presented functionality of the local FingerIdent system to the cloud and provide the necessary infrastructure for accessing the biometric service. Details on this procedure are given in the next section.

3.1. Designing Cloud Biometric Services

We move the biometric engine as well as the biometric database to the cloud. Note that the verification process with the described design is conducted using the following scenario [Figure 2]:

a) The fingerprint of a given user is first captured via a fingerprint scanner (here scanner libraries that allow capturing fingerprint images need to be integrated into the local (desktop or/and web) application);

b) The application then communicates through a (REST) API with the biometric web service hosted in the cloud and sends an encoded image to the fingerprint processing library (i.e. FingerIdent library) that provides the functionality for the cloud service;

c) The transmitted fingerprint image is processed in the cloud and finally the result is sent back to the local application.

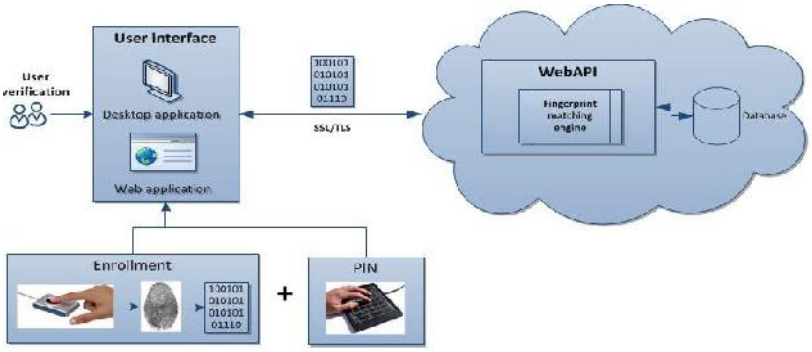


Figure 2. Scheme of the biometric verification system in the cloud

d) The use of the HTTPS protocol for data transfer.

e) The use of certificates (the SSL protocol).

f) The encryption of passwords and other data (such as biometric templates) in the database.

g) The protection of the access to the cloud-service with a complex 40-digit password. The cloud-based service is designed modularly, which makes upgrading the service a relatively simple task. Equally important is the fact that the same design is also suitable for other biometric modalities and allows for devising multi-modal person authentication as well.

3.2. Moodle with Fingerprint Verification

To demonstrate the effectiveness of the presented solution and to provide a proof-of-concept, the e-learning environment Moodle [3] is augmented with biometric authentication capabilities by integrating it with the cloud-based fingerprint verification service. Since Moodle is also designed modularly, the biometric authentication procedure is implemented as an additional (optional) authentication scheme, which can complement the existing procedures and provide an additional level of access security. A block diagram of the integration is shown in Figure 3.

The main problem faced during integration is the compatibility of various fingerprint readers with different browsers. Each manufacturer of fingerprint readers offers their own protocols and libraries to access the corresponding hardware. A standard is not yet available.
The solution developed in the scope of this case study uses an ActiveX component to access the hardware. ActiveX components are officially supported only on Internet Explorer, which represents a weakness in the implementation. As future work, an extension of the presented solution is planned, so it can work with other popular browsers, such as Firefox, Opera or Chrome too. After the integration of the fingerprint authentication service into the Moodle framework, the screen was modified to account for t functionality. The result of this procedure is shown in Figure 4. Note how the added biometric authentication functionality seamlessly integrates into the existing framework.

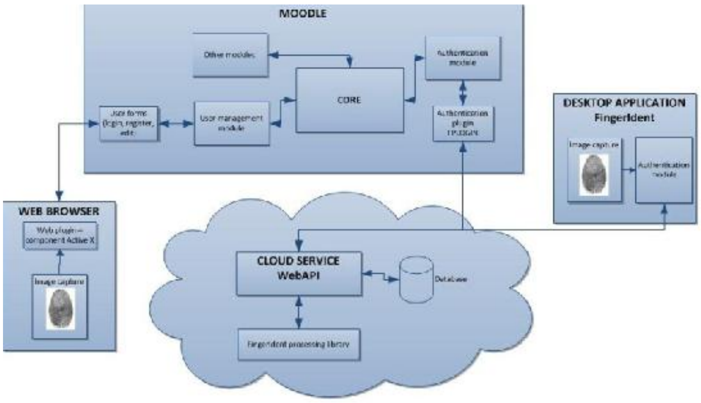
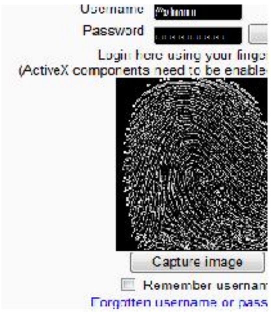

MOODLE
Other modules
Authentication module
CORE
User forms (login, register, edit)
User management module
Authentication plugin FPLOGIN
DESKTOP APPLICATION FingerIdent
Image capture
Authentication module
WEB BROWSER
Web plugin – component Active X
Image capture
CLOUD SERVICE WebAPI
Database
FingerIdent processing library

Figure 3. Cloud fingerprint verification in Moodle



Username

Password

Login here using your finge
(ActiveX components need to be enable

Figure 4. Customized Moodle login

4. Ear Segmentation

First of all ear images and finger print data were collected. Next color normalization was applied because of the lighting conditions of individual images of the ear. The image acquisition system captures ear as a larger portion of image that also contains data from immediately surrounding ear region. Thus, prior to performing segmentation and feature extraction it is necessary to localize only that portion of the image that contains antihelixes, crus of helix, concha and tragus of the ear as shown in Figure 5, i.e.external ear. Here, the idea which is ear images can be seen as a composition of micro-patterns was taken which can be well described by fusion of two techniques such as DWT (using haar wavelet) and GLCM, into account. Afterwards, in order to get the features user can adjust the location of ear center. Then, those features were combined with DWT (using haar wavelet) and GLCM. The results of previous steps give representation of ear. Next to increase the accuracy of authentication system, the solid judgment on authenticating users can be achieved by a fusion of multiple sub authentication systems.

In this experiment color image cannot be taken. That is why this image has to be converted into gray scale image by using the function 'rgb2gray'. Then the centroid of the image was found. Then the image was cropped as depicted in the following Figure 6.

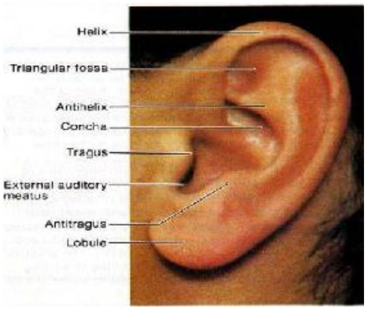


Figure 5. The surface anatomy of the auricle of the ear

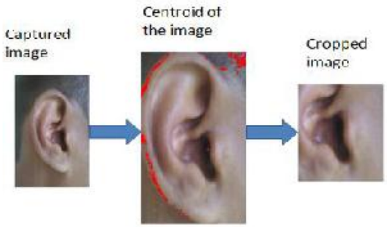


Figure 6. The process of cropping the image with respect to the centroid

4.1. Discrete Wavelet Transform (DWT)

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. It captures both frequency and location information. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale: finally resulting in (2^n-1) differences and one final sum. The Haar wavelet's mother wavelet function Φ(t) can be described as Φ(t) = { 0 ≤ t≤ 1, otherwise.

4.2. Gray-Level Co-Occurrence Matrix (GLCM)

GLCM is a tabulation method of how often different combinations of grey levels occur in image neighborhoods. Key components in creating the GLCM are the direction (E, W, N, S, NE, NW, SE, SW) and distance between the reference pixel and neighbor pixel.

After manipulating, we have got four matrices as follows:

A – Auxiliary matrix } approximation co-efficient matrix
H – Horizontal matrix
V – Vertical matrix
D – Diagonal matrix

Afterwards we have to calculate the mean and variance of all four matrices as depicted above.

4.3. Deriving Statistics from a GLCM

After creating the GLCMs, several statistics can be derived from them using the 'graycoprops' function. These statistics provide information about the texture of an image. The following table lists the statistics which can be derived.

Table 1. The statistics which provide information about the texture of an image

Property	Description
Contrast	It measures the intensity contrast between a pixel & its neighbor over the whole image.
Correlation	It measures how correlated a pixel is to its neighbor over the whole image.
Energy	It returns the sum of squared elements in the GLCM.
Homogeneity	It measures the closeness of the distribution of elements.

5. Conclusion

In this paper, an up-to-date review of existing approaches for two promising biometric traits, the ear and the fingerprint are described. Techniques involving data acquisition, detection, representation and multimodal recognition with these two modalities are categorized and analyzed, thus providing the reader with a comprehensive overview of the research field. It is found that many solutions have been proposed with unimodal approaches and most of them report quite high recognition and low error rates in a controlled scenario, however, they suffer a significant decrease in accuracy in the presence of pose and expression variations and occlusions. Although it is perceived that the accuracy and robustness can be increased with fusion of ear and fingerprint, very few such approaches have been proposed. The identification and discussion of the underlying problems and challenges in this paper imply that significant further research should be performed in the area of developing fast and fully automatic ear-fingerprint multimodal systems using low-cost acquisition devices and with a data or feature level of fusion.

References

[1] H Sieger, N Krischnik, S Moller. *POSTER: User Preferences for Phones.* Proceeding of 6th Symposium on Usable Privacy and Security.

[2] AK Jain, A Ross, S Prabhakar. An Introduction to Biometric Recognition. *Transactions on Circuits and Video Technology.* 2004; 14(1): 4-20.

[3] E Kohlwey, A Sussman, J Trost, A Maurer. *Leveraging the Cloud Meeting the performance requirements of the Next Generation Biometric Systems*. In the IEEE World Congress on Services. 2011.

[4] V Štruc, J Žganec. Recognition Technology for Biometrics service. 2012: 68-75.

[5] J Bule, P Peer. Fingerprint Verification as a Service in KC CLASS. 2012: 76-82.

[6] The KC Class project. http://www.kc-class.eu/.

[7] D Gonzales Martinez, FJ Gonzels Castano, E Argones Rua, JL Ala Castro, DA Rodriguez Silva. *Secure Crypto-Biometric System for Cloud Computing*. In Internationa Securing Services on the Cloud.

[8] H Vallabhu, RV Satyanarayana. Biometric Authentication as a Service on Cloud: Novel Solution. *International Journal of Soft Computing and Engineering*. 2(4): 163.

[9] S Suryadevara, S Kapoor, S Dhatterwal, R Naaz, A Sharma. Tongue New Prospects of Cloud Computing Security. In International Conference on Information and Network Technology. 2011; 4.

[10] SNS Raghava. *Iris Recognition on Handoop: a Biometrics System Implementation on Cloud Computing.* In Proceedings of IEEE CCIS.

[11] C Senk, F Dotzler. *Biometric Authentication as a Service for Enterprise Identity Management Deployment: A Data Protection Pers.* International Conference on Availability, Reliability and Security.

[12] E Kohlwey, A Sussman, J Trost. Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next Generation Biometric Systems. *Congres on Services*. 597.

[13] DM Dakhane, AA Arokar. Data Secuity in Cloud Computing for Biometric Application. *International Journal of Scientific & Engineering Research.* 3(6): 1.

[14] Cloud computing use case discussion group. Cloud Computing Use Cases: White Paper. available from: http://cloudusecases.org. 2012.

[15] Homepage of the Animetrics cloud recognition solution. 2013; (37): 115-122. *Privacy*. 2012; 10: 22-27. IEEE Technology, for Big Data Biometrics: Proceeding of Services. 597-601.