Secured Access of Locker using Multimodal Biometrics

T.S. Sasikala, Dr. J.Jeya A Celin

Abstract - Biometrics refers to the science of automatic recognition of individuals based on some specific physiological and/or behavioural features. Multimodality is the usage of more than one physiological or behavioral characteristic to identify an individual. It involves the fusion of two or more technologies such as fingerprint, facial recognition, iris scanning, hand geometry, signature or speech recognition. The fusion is done by running the two (or more) biometric against two (or more) different algorithms. This paper presents the use of multimodal biometrics in order to identify or to verify a person who want to access control of the locker.

1.Introduction

Recently, many research efforts have tackled the problem of devising practical systems for personal identification and verification relying on biometrical data. The biometrics features of an individual are unique and provide a very convenient method for personal identification. According to [5] biometrics provided it has the following desirable properties:

- universality - every person. should have the
- Characteristic uniqueness - no two persons should possess the same characteristic
- permanence - the characteristic should not change with time
- measurability ~ it should be possible to measure the characteristic in a quantitative manner.**,**

- Sasikala T.S is a Assistant Professor at Dept. of Software Engineering in Sun College of Engineering and Technology Nagercoil. Email: sasikalaselva2012@gmail.com
- Dr. J.Jeya A Celin is a Professor at Dept. of Information Technology in Noorul Islam University, Thuckalay. Email : jeyacelin@gmail.com

There are several currently available systems for on-line fingerprint verification [5], [6] and on-line signature verification [7]. Biometric systems based on single source of information are called unimodal systems. Although some unimodal systems [1]. have got considerable improvement in reliability and accuracy, they often suffer from enrollment problems due to non-universal biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data [4]. Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. To overcome the achieve the desired performance we go for multimodal biometrics . The use of multi-modal biometrics aims to increase accuracy of the verification or identification of people. The problem in using multi-modal biometrics is the choice the biometric technologies to be used in the system. the person to be identified must pass all the tests, and every test can have a different weight in the system.

2. Proposed Method

First of all, a fingerprint sensor is posted on the door, a camera for iris recognition , and a microphone for voice recognition are placed inside the locker room . There are two possibilities: if the person is identified as the right person , then he/she can take control of the locker. if it's an intruder, the locker can announce a message which says he/she is a thief.

2.1 Finger print recognition

According to the glossary of the Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) [2], “a fingerprint is an impression of the friction ridges of any part of the finger”. Finger-scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications. The uniqueness of friction ridges tells us that no two fingers or palm prints are ever exactly alike; even two recorded successive impressions from the same finger are not identical [3]. Fingerprint patterns do not change significantly throughout life . One main shortcoming for fingerprint identification systems is that small injuries and burns highly affect the fingerprint. In fact, injury, whether temporary or permanent, can interfere with the scanning process. Also Fingerprint recognition may not work for the people with faint fingers or dry fingers.

2.1.1 Fingerprint capturing

Fingerprint recognition system uses platen or scanner to capture an fingerprint image. Image quality is measured in dots per inch. Today’s scanner acquire images of 500 DPI.

2.1.2 Preprocessing

High quality image must be converted to a usable format. The gray areas from the image must be eliminated by converting the fingerprint image’s gray pixel to Black and White depending on their pitch. Which results in a series of thick black ridges contrasted to white valleys.

2.1.3 Feature Extraction

The fingerprint comprises ridges and valleys that form distinctive patterns such as swirls, loops and arches. The ridges and valleys are characterized by minutiae. All these are extracted from the fingerprint. Fingerprint ridges show a loop patterns as shown in fig 1

Figure 1. Fingerprint ridges showing a loop pattern

2.1.4 Verification

Using Vendors proprietary algorithms fingerprint minutiae are mapped. Based on which verification is done.

2.2 Iris recognition

iris recognition is the most promising for the environments mentioned [11]. The potential of the human iris for biometric identification comes from the anatomy of the eye [12]. The iris is a dynamical tissue that is highly protected against the outer by the cornea and whose modification implies surgery with a high risk of damaging the vision, it is the externally – visible, colored ring around the pupil. The iris patterns are both highly complex and unique. An iris ‘scan’ is a high-quality photograph of the iris taken under near-infrared illumination.

2.2.1 Image acquisition

Iris recognition systems use small, high-quality cameras to capture a black and white high-resolution photograph of iris. Once the image is captured, the iris' elastic connective tissue-called the trabecular meshwork-is analyzed, processed into an optical "fingerprint," and translated into a digital form. The image of the iris is acquired from an iris

camera and is filtered and recognized in order to obtain a code called IrisCode, which has only 512 bytes. The comparison between two irises is made by calculating the Hamming distance between two codes. This procedure is extremely rapid.[10]

2.2.2 Pre-processing

The photographs taken, as it can be seen in Fig. 2.a, cover the whole eye of the user. the eyelids almost always cover some part of the iris Therefore, during the whole process, the algorithms will be based on its lateral cones [9]. After the camera locates the eye, an algorithm narrows in from the right and left of the eye to find the riis's outer edge. The iris scan algorithm then locates the inner edge of the iris at the pupil. A black and white image of the iris is used for feature extraction

2.2.3 Feature extraction

Visible characteristics like trabecular meshwork, rings, furrows, freckles, and corona are extracted from the preprocessed iris. Iris-scan algorithm map segments of the iris into hundreds of independent vectors. The characteristics derived from iris features are the orientation and spatial frequency .

2.2.4 Verification

Iris scan technology is capable of searching hundreds of thousands of records per second. In verification system a user must claim an identity before interacting with the system. If falsely accepted, he or she has already made the decision to claim another's identity and the user can easily be held culpable for ensuring system misuse. A falsely matched user may be granted access to resources to which he or she is not entitled, but the lack of an identity claim reduces the person's culpability. While highly resistant to false matching, iris-scan technology is not immune to this happening [8].

2.3 Voice recognition

Voice recognition utilizes the distinctive aspects of the voice to verify the identity of individuals. It verifies the identity of the individual who is speaking [15]. Biometric technology reduces each spoken word to segments composed of several dominant frequencies called formants. Each segment has several tones that can be captured in a digital format. The tones collectively identify the speaker's unique voice print. Voice prints are stored in databases in a manner person similar to the storing of fingerprints or other biometric data[16]. The system includes four important stages: endpoint detection, noise cancellation, feature extraction and pattern comparison. The voice recognition **is** divided into two sessions: (i) the enrollment session, (ii) the verification session. The front end of voice recognition module is given in fig 2. The enrollment session is used to add a new user to the database or update a current user's profile or utterance templates. During enrollment, a user **is** required to register by submitting a form after which he will he assigned a unique ID and asked to begin the voice recording session During a subsequent verification session, the user will be prompt for his-ID and the same recording process is executed

2.3.1 Preprocessing

After acquiring sufficient data for enrollment or verification voice-scan system process the vocal recordings, which eliminates gaps at the beginning and end of the recording.

2.3.2 Feature Extraction

Distinctive features like pitch, fundamental frequency, intensity, short-time spectrum of speech, formant frequencies, linear prediction coefficients, cepstral coefficients, spectrograms and nasal coarticulation are extracted from the

preprocessed voice and are stored in the form of template in a database.

2.3.2 Verification

Voice scan technology is capable of searching millions of records per second. In verification system a user must claim an identity before interacting with the system. If falsely accepted, he or she has already made the decision to claim another's identity and the user can easily be held culpable for ensuring system misuse. Here the system request the user to say some word. Based on the voice the user is capable of recognizing the person as a right one or the intruder.

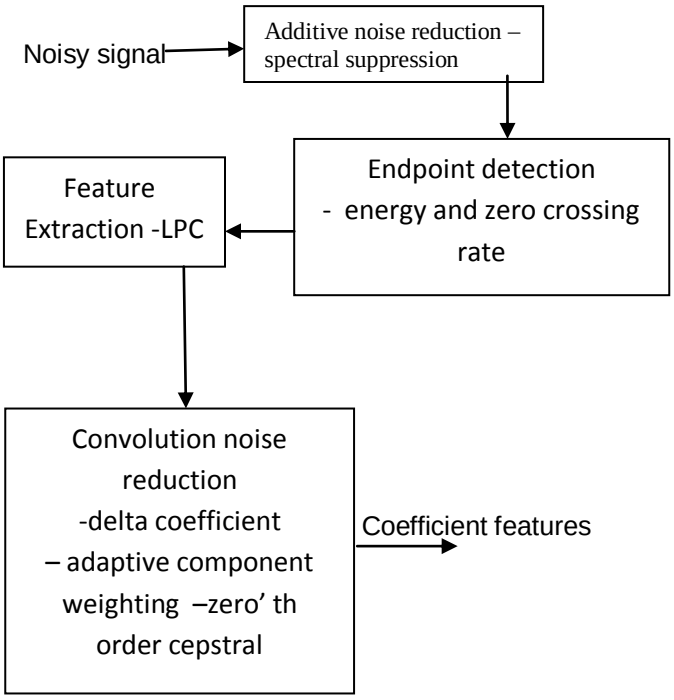

Figure 2 The front-end of the speaker verification module.

3. Locker Access Control Process Description

This Application uses Multimodal Biometrics. Its uses Biometric Characteristics like Fingerprint, iris, and Voice recognition to open a Locker. A user who wants to open the Locker needs to pass all the three tests. First when the user enter into the room a camera captures the iris of the person, the fingerprint scanner on the door senses the finger print and a microphone records the voice. After capturing all the biometric data's the system must perform a test. Fig 3 shows the modal of Locker identification system.

If the user passes all the test the person can access the locker. Else he/she needs to go for all the three test once more. A person is allowed to give 3 chances. If he/she is fails in all the three chances he/she is identified as the criminal and same person is handed over to the police or some other crime identification department.

Advantages

- It reduces the False Match Rate.
- Highly Secure

Disadvantage

- It increases False Non-Match rate
- Highly complex

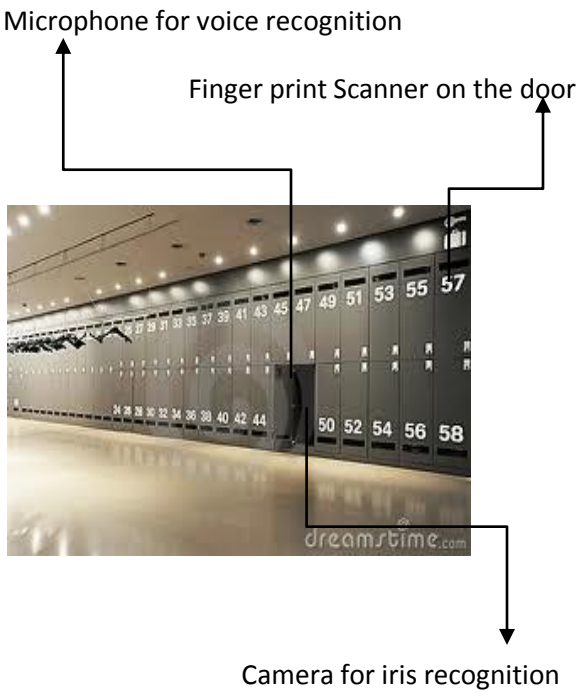

Fig3. Modal of Locker Identification System

4. Conclusion

Characteristic of the human body. It depends on the sensor or the algorithm used, if the person is accurately identified. By using many biometric systems, the security will increase considerably. The combination of these biometric technologies is crucial because if a weaker characteristic is chosen together with an accurate one, then the result won't be very satisfying. The main contributions in this paper is that I proposed a multimodal biometric system that uses three sensors in order to positively or negatively identify a person that wants to use a car. Most of the actual biometric systems use only a single characteristic of the human body. It depends on the sensor or the algorithm used, if the person is accurately identified. Using Multi modal biometric systems, the security will increase considerably. Fusion of two or more biometric technology will certainly increase the level of accuracy. This system may give a beep sound of a user try to use a locker that does not belongs to him.

5. References

1. Chander Kant, Rajender Nath, "Reducing Process-Time for Fingerprint Identification System", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1-9, 2009.

2. SWGFAST, "Glossary", http://www. swgfast.org/Glossary_Consolidated_ver_1.pdf, visited on 15/10/2007.

3. D.R. Ashbaugh, "Ridgeology", Journal of Forensic Identification, 41(1), pp 16-64 (1991).

4 . A.K. Jain, A. Ross, "Multibiometric systems". Communications of the ACM, vol. 47, pp. 34-40, 2004.

5. T. Elgamal and K.E.B. Hickman, "Secure socket layer application program apparaNs and method," US *Potent* 5657390, 1997

6. R. Iain, L. Hong, and R. Bok, "On-line fingerprint verification," *IEEE* Trans. Palfern Analysis *and Machine Intelligence,* vol. 19, no**.** 4, pp. 302-313, 19977.R. Jain, R. B o k and S. Pankanti (eds.), Biomelrics:, Perspnal Idenrflcofion *in Networked Society,* Kluwer Publishen, Boston, MA, 1999

8. Samir Nanabati, Michael Thieme, Raj Navati, " Biometrics Identity verification in a Networked World", Wiley Computer Publishing

9. R. Sanchez-Reillo, C. Sanchez-Avila, J.A. Martin- Pereda, "Minimal Template Size for Iris Recognition". Proc. of the First Joint BMES/EMBS Intemational Conference (Atlanta, USA), 13-16th October, 1999. p. 972

10. C. Lupu, V. Lupu, " Multimodal Biometrics for Access Control in an intelligent Car" , 3rd International Symposium on Computational Intelligence and Intelligent Informatics - ISCIII 2007 - Agadir, Morocco * March 28-30, 2007

11. J**.** G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence". IEEE Trans. PAMI, vol. 15, no **11,** Nov. 1993.

12. M.L. Berliner, "Biomicroscopy of the Eye". Paul B. Hoeber, Inc. 1949.