Multimodal biometric authentication

Lokeswara Rao Bhogadi [1], **N. Bhagyalaxmi** [2]

[1] Profeesor &amp; HOD, Dept. of ECE, CMR College of Engineering &amp; Technology

[2] Assistant professor, Dept. of ECE,CMR College of Engineering &amp; Technology

Abstract: In the present era of information technology, there is a need to implement authentication and authorization techniques for security of resources. There are number of ways to prove authentication and authorization. But the biometric authentication beats all other techniques. Biometric techniques prove the authenticity or authorization of a human being based on his/her physiological or behavioural traits. Biometrics is a technique by which an individual's identity can be authenticated by applying the physical or behavioural trait. Physical traits like fingerprints, palm, iris etc. are based on the physical characteristics which are generally inherent and unique. Behavioural traits like voice, signature or keystroke dynamics etc. on the other hand, are quantifiable characteristics.They also protect access of resources from unauthorized users. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a verification / identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. A multimodal biometric identification system aims to fuse two or more physical or be havioural traits. Multimodal biometric system is used in order to improve the accuracy. Multimodal biometric identification system based on iris, palm and fingerprint trait based on fusion logic is proposed. Typically in a multimodal biometric system, each biometric trait processes its information independently. The processed information is combined using curve let transform.

Keywords: Iris; finger print and palm images; MATLAB software

1. Introduction

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioural characteristic. Biometric systems can be classified into two types namely unimodal and multimodal biometric systems.

A unimodal biometric system is one in which only a single type of the constituent components is present. In multi-modal biometric system, more than one type of the component is present. Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic. Among the features measured are: face, fingerprint, hand geometry, iris, retinal, signature and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Unimodal biometric systems are often affected by the following problems:

(1) Noisy sensor data: Noise can be present in the acquired biometric data mainly due to defective or improperly maintained sensors.

(2) Lack of individuality: Features extracted from biometric characteristics of different individuals can be quite

doi: 10.18063/wct.v2i1.417

similar. A small proportion of the population can have nearly identical facial appearance due to genetic factors (e.g., father and son, identical twins, etc.)

Multimodal biometric systems

Use of multiple biometric indicators for identifying individuals is known as multimodal biometrics. Combining the evidence obtained from different modalities using an effective fusion scheme can significantly improve the overall accuracy of the biometric system.

A multimodal biometric system can reduce the FTE/FTC rates and provide more resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources.Multimodal biometric systems integrate information presented by multiple biometric indicators. The information can be consolidated at various levels by fusion using curve let transform.

The biometric system has the following two modes of operation.

Enrollment mode: In this mode the system acquires the biometric of the user and stores required data obtained from the people in the database. These templates are tagged with the user's identity to facilitate authentication.

Authentication mode: This mode also acquires the biometric of the person and uses it to verify the claimed identity. This provides enhanced security system against illegal access through multimodal biometric authentication.

Advantages of multimodal biometrics are more secure, more accurate, reduce false accept rate (FAR), reduce false reject rate (FRR) and reduce failure to enrol rate (FTE).

Disadvantages of multimodal biometrics are high cost, missing body part problem and increase in system development and complexity.

Application of multimodal biometrics is security, used in passport verification, in aadhaar authentication and crime investigation.

2. Description of biometric system

2.1 Fusion in multimodal biometric systems

A mechanism that can combine the classification results from each biometric channel is called as biometric fusion.

Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths. Fusion at matching score, rank and decision level has been extensively studied in the literature. Various levels of fusion are: sensor level, feature level, matching score level and decision level.

2.1.1 Sensor level fusion

The biometric traits taken from different sensors are combined to form a composite biometric trait and process.

2.1.2 Feature level fusion:

Signal coming from different biometric channels are first pre-processed and feature vectors are extracted separately using specific algorithm and these vectors are combined to form a composite feature vector. This is useful in classification.

2.1.3 matching score level fusion:

The feature vectors are processed separately and individual matching score is found. The accuracy of each biometric matching score will be used for classification.

2.1.4 decision level fusion:

Each modality is first pre-classified independently. Multimodal biometric system can implement any of these fusion strategies or combination of them to improve the performance of the system. Palm, iris and fingerprint are used in multimodal biometric system by using fusion process.

2.2 Palm:

Palm print recognition inherently implements many of the same matching characteristics that have allowed fingerprint recognition and is one of the most well-known and best publicized biometrics. Both palm and finger biometrics are represented by the information presented in a friction ridge impression. This information combines ridge flow, ridge characteristics and ridge structure of the raised portion of the epidermis. The data represented by these friction ridge impressions allows a determination that corresponding areas of the friction ridge impressions either originated from the same source or could not have been made by the same source. Because fingerprints and palms have both uniqueness and permanence, they have been used for over a century as a trusted form of identification. However, palm recognition has been slower in becoming automated due to some restraints in computing capabilities and live-scan technologies.

2.3. Fingerprint

A fingerprint is the feature pattern of one finger. It is an impression of the friction ridges and furrows on all parts of a finger. These ridges and furrows present good similarities in each small local window like parallelism and average width.

An image of the fingerprint is captured by a scanner, enhanced and converted into a template. Scanner technologies can be optical, silicon, or ultrasound. Ultrasound while potentially the most accurate has not been demonstrated in widespread use.

2.4. Iris recognition

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The iris is a muscle within the eye that regulates the size of the pupil, controls the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle. Although the coloration and structure of the iris is genetically linked, the details of the patterns are not. The iris develops during prenatal growth through a process of tight forming and folding of the tissue membrane. Prior to birth, degeneration occurs, resulting in the pupil opening and the random unique patterns of the iris. Although genetically identical, an individual‘s iris is unique and structurally distinct, which allows for it to be used for recognition purposes.

Block diagram and flow chart

Block diagram:

The block diagram of fusion based multimodal biometric authentication is shown in **Figure 1.**

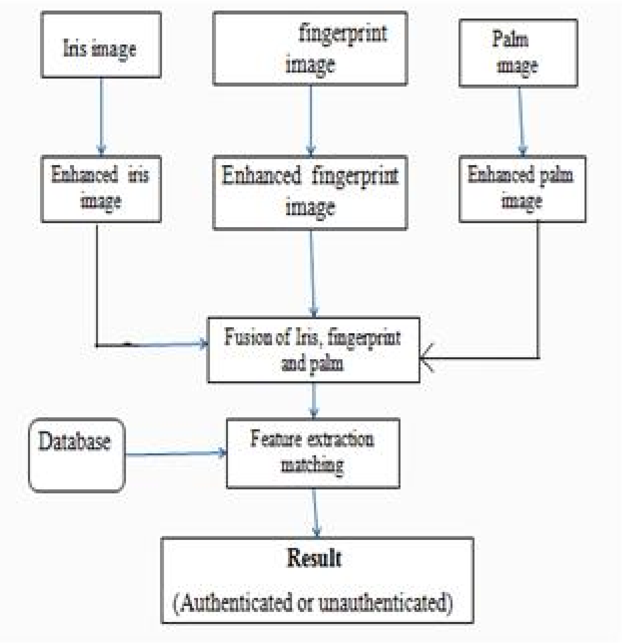
Iris image
fingerprint image
Palm image
Enhanced iris image
Enhanced fingerprint image
Enhanced palm image
Fusion of Iris, fingerprint and palm
Database
Feature extraction matching
Result
(Authenticated or unauthenticated)

Figure 1; Block diagram of fusion based multimodal biometric authentication.

Fusion based multimodal biometric authentication is implemented using curvelet transform. This fusion process is done with the help of MATLAB. This process is implemented by selecting images of fingerprint, iris and palm from database and are fusioned with the help of curvelet transform.

Flow Chart

The flow chart of fusion based multimodal biometric authentication is shown in **Figure 2.**

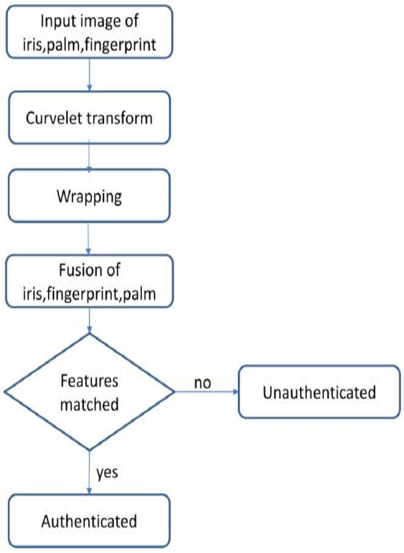

Figure 2; Flow chart.

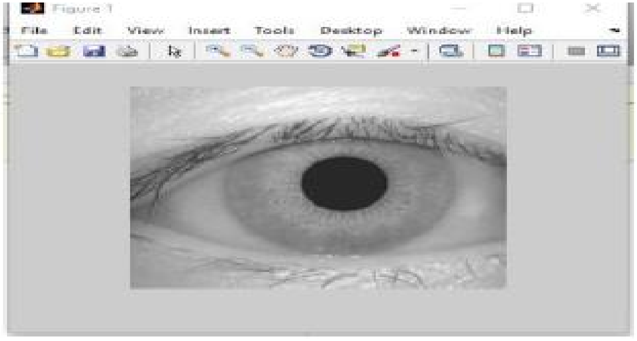

Figure 3; Selecting image of iris from database.

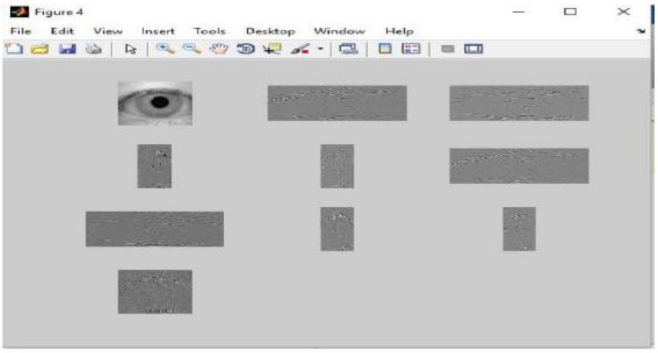

Figure 4; Selected image of iris.

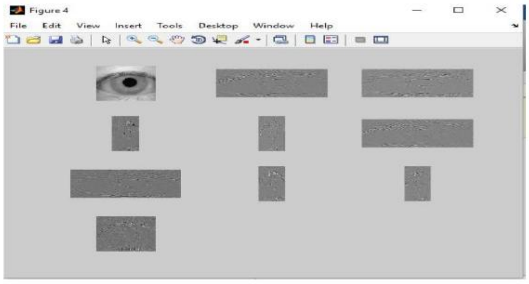

Figure 5; Segmentation of selected image of iris and enhancing.

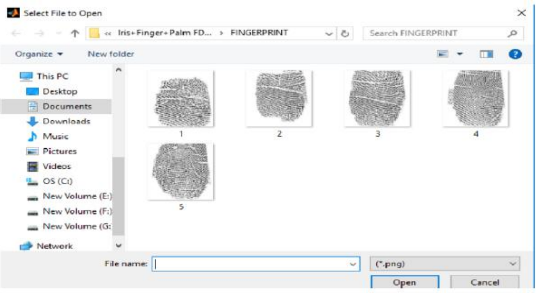

Figure 6; Selecting image of finger print from database.

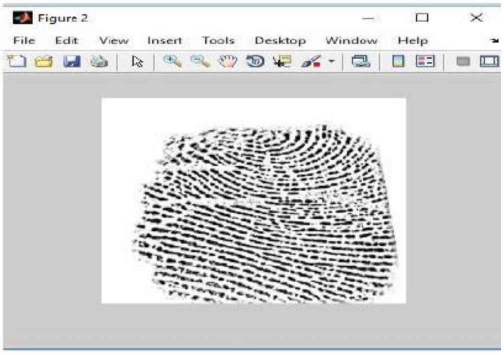

Figure 7; Selected image of finger print.

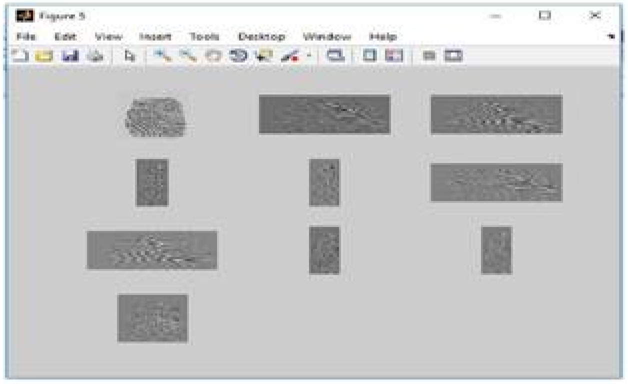

Figure 8; Segmentation of selected image of finger print and enhancing.

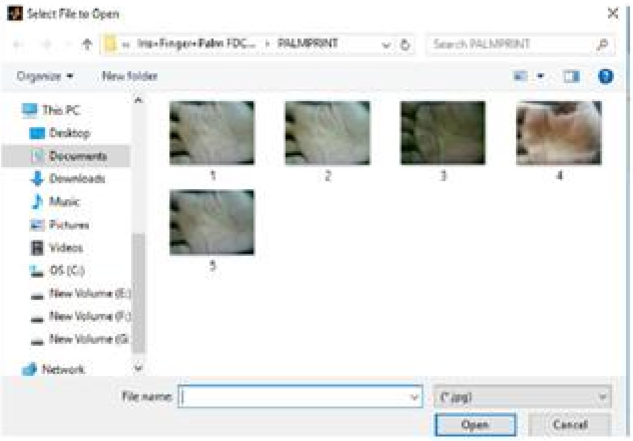

Figure 9; Selecting image of palm from database.

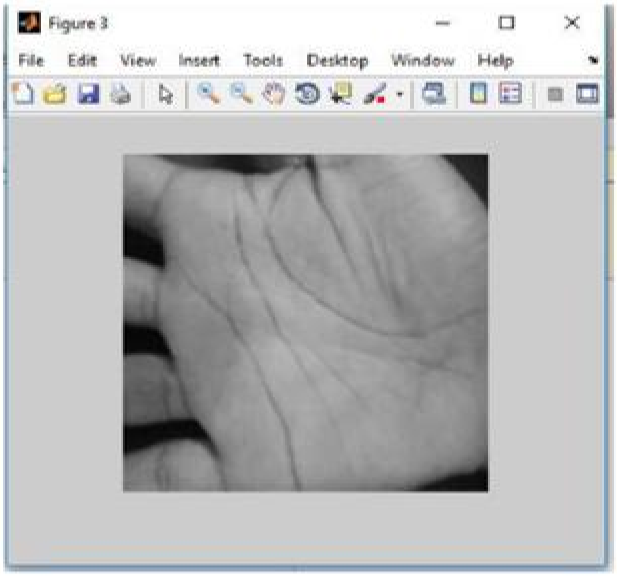

Figure 10; Selected image of palm.

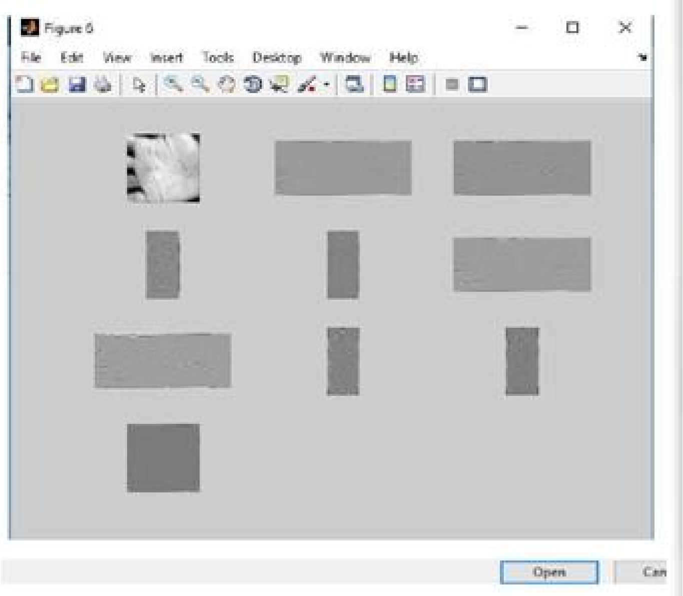

Figure 11; Segmentation of selected image of palm and enhancing.

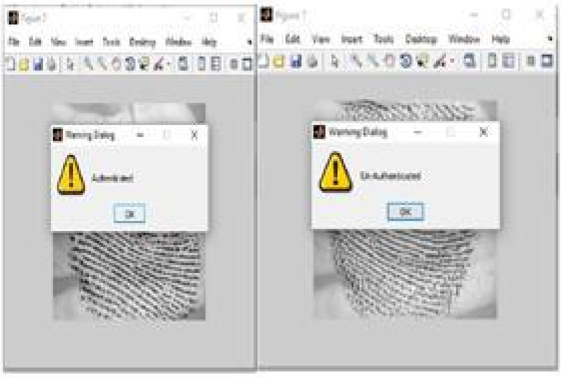
Figure 7
File Edit View Insert Tools Desktop Window Help
Figure 7
File Edit View Insert Tools Desktop Window Help

Warning Dialog

Authenticated

OK

Warning Dialog

Un-Authenticated

OK

Figure 12; Authenticated or Unauthenticated based on selected image.

4. Conclusion

Though the time taken in multimodal biometric systems is larger than the unimodal systems still it is used in place where security is the chief concern. By using appropriate normalization and fusion techniques, a high security multimodal biometric system can be achieved. If a user cannot provide a good fingerprint image (due to dry fingers, cuts, etc.), then iris and palm may be better biometric indicators. There is no security system that is completely out of spoofing. Every system is breakable. The techniques used to prevent the attacks help to increase the time and cost. Fingerprints can be easily forged from touched surfaces and can be copied in a small amount of time using readily available materials. All the liveness detection mechanisms in fingerprint systems can be easily overwhelmed using wafer thin gelatin and silicon artificial fingerprints. But it is very difficult to fake the iris systems because they use physiological reactions to changing illumination conditions for liveness detection. A physical modeling of iris device will be needed to defeat them which are very hard and expensive. Also a fake iris printed on a contact lens can be easily detected using a check to see special properties introduced by the printing. So iris systems can be used for high security applications and network security. But iris and retina systems are very expensive and their user acceptability is low compared to face and fingerprint recognition systems. This makes them a bad choice for common applications. Biometric systems using fingerprints and face are sufficiently robust to be used as an authentication system for time and attendance and access control for low security systems No biometric system is optimal. The decision to which biometric is to be used should be made on the basis of the type of application and the level of security. Multimodal biometric systems address several problems present in unimodal system. In applications such as border entry/exit, access control, civil identification and network security, multi-modal biometric systems are looked to as a means of (a) reducing false acceptance and false rejection, (b) providing a secondary means of enrolment, verification and identification if sufficient data cannot be acquired from a given biometric sample and (c) combating attempts to spoof biometric systems through non-live data sources such as fake fingers. The performance of multimodal biometric system shows great promise to personal identity in the biometric authentication society.

References

1. Jain AK, Ross A. Multibiometric systems. Communications of the ACM 2004; 47(1): 34-40.
2. Ross A, Jain AK. Information fusion in biometrics. Pattern Recognition Letters 2003; 24 (13): 2115–2125.
3. Huber PJ, Statistics R (John Wiley &amp; Sons, 1981).
4. Snelick R, Indovina M, Yen J, *et al*. Mink multimodal biometrics: issues in design and testing, in proceedings of fifth international conference on multimodal interfaces. 2003: 68–72.
5. Indovina M, Uludag U, Snelick R, *et al*. Combining COTS finger and face biometrics for identity verification, in Proceedings of Workshop on MultiModal User Authentication 2003: 99-106.