e-ISSN: 2349-9745
p-ISSN: 2393-8161

6FLHQWLILF-RXUQDO,PSDFW)DFWRU6-,)

,QWHUQDWLRQDO-RXUQDORI0RGHUQ7UHQGVLQ(QJLQHHULQJ
DQG5HVHDUFK
ZZZLMPWHUFRP

MULTI-MODULE BIOMETRICS SYSTEM USING FACE AND EAR DETECTION

[1]Priti Shende, [2]Adesh Tayade, [3]Shrikant Taware, [4]Amol Thorat
[1,2,3,4]Electronics and Telecommunication, DYPIET Pimpri Pune

Abstract - The term Biometrics is becoming highly important in computer security world. The human physical characteristics like fingerprints, face, Ear, hand geometry, voice and iris are known as biometrics. These features are used to provide an authentication for computer based security systems. The existing computer security systems used at various places like banking, passport, credit cards, smart cards, PIN , access control and network security are using username and passwords for person identification. The username and passwords can be replaced and/or provide double authentication by using any one of the biometric features. In this paper, the main focus is on the various biometrics, their applications and the existing biometrics recognition systems.

Use of Biometrics are the most secure method for security at several system. In recent years Biometric based Authentication systems have gained more attention due to frequent fraudulent attacks. This study investigates the need for multiple sensors, multiple recognition algorithms and multiple fusion levels and their efficiency for a Person Authentication System (PAS) with face and ear biometrics. The final DJJUHJDWLRQRIVFRUHVZKHWKHU7KH3HUVRQLV$XWKHQWLFDWHGRUQRW¶

Keywords² Biometric; *Image quality; Fusion; Multi-modal Ear, Face.*

I. INTRODUCTION

7KHWHUPELRPHWULFVLVGHULYHGIURPWKH*UHHNZRUGVELRPHDQLQJOLIHDQGPHWULFPHDQLQJWRPHDVXUH

Biometric is the science of establishing identity of an individual based on the physical, Chemical or Behavioral attributes of the person. Biometric-based authentication is the automatic identity verification, based on individual physiological or behavioral characteristics, such as fingerprints, voice, face and iris. Since biometrics is extremely difficult to forge and cannot be forgotten or stolen, Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional authentication schemes. Biometric system identifies or verifies a person based on his or her physiological characteristics such as fingerprint, face, palm print, iris etc or behavioral characteristics such as voice, writing style, and gait.

A biometric is a unique, measurable characteristic or trait for automatically recognizing or verifying the identity of a human being. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information and property.

With the increased use of computers or vehicles of information technology, it is necessary to restrict access to sensitive or personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification

icenses may be forged, stolen, or lost .Thus biometric systems of identification are enjoying a renewed interest.

Recognition requires the system to look through many stored sets of characteristics and pick the one that matches the unknown individual being presented. Various types of biometric systems are being used for real±time identification; the most popular are based on face recognition and fingerprint matching. However there are other biometric systems that utilize iris and retinal scan, speech, gesture recognition, and hand geometry.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. The basic idea behind biometrics is that our bodies contain unique properties that can be used to distinguish us from others. A biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user.

II. BASIC PRINCIPLES

A. Block Diagram

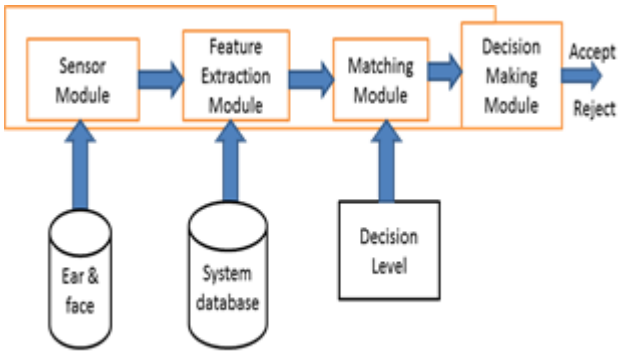

Fig: Block Diagram Of Multimodal Biometric System

There are mainly five modules ±Sensor module, Feature extraction module, Matching module, Decision making module and Cryptographic key generation module.

1. Sensor module:

The first Block of our system is Sensor Module. It is the interface between the real world and the system. It has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired.A sample of the biometric feature is captured, processed by a computer, and stored for later comparison.

2. Feature extraction module:

The second Block is the feature extraction module. The input to the feature extraction module is the output of the sensor module.In this block features needed are extracted after preprocessing. In preprocessing, it remove artifacts from the sensor, to enhance the input This step is an important step as the correct features

need to be extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identifiability.All Biometric authentications require comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample.

3. Matching module:

The third Block of our system is matching module. This block is most important block of our project. In this block, extracted features which is the output of the feature extraction module is compared with the template which are stored in the system database. The output of matching module is given as a input to the decision making module.

4. Decision making module:

The fourth Block of our system is decision making module. We have done the fusion of face and fingerprint at the decision making module. Decision making module worked as a fusion level. Depending upon the output of the decision making module, user is ask to enter the cryptographic key.

B. Algorithm

Algorithm for Feature extraction of Biometric Characterstic Using ICA:

Step 1: Get the image data in matrix form.
Step 2: Calculate the mean.
Step 3: Subtracting the mean of the data from each data element.
Step 4: Calculate the covariance matrix.
Step 5: Calculate the eigenvectors and the eigenvalues of thecovariance matrix.
Step 6: Choosing components and forming vectors.
Step 7: Deriving the new data set.

III. CONCLUSION

Reliable user authentication is highly significant in this web enabled world. Consequences of an insecure authentication system can be catastrophic and may include loss of information, denial of service and loss of data integrity.The current generation of biometric authentication devices offers cost and performance advantages over manual security procedures.

Accuracy of our system will be more than that of the other system. These methods have shown that, using biometrics for identification or verification-based security systems is a promising technology.

REFERENCE

[1] Neerja & Ekta Walia ,³ Face Recognition Using Improved Fast PCA $OJRULWKP´&RPSUHVVLRQ,PDJHDQG6LJQDO Processing.
>@/8&$6&(DU%LRPHWULFVDVXUYHRIGHWHFWLRQ IHDWXUHH[WUDFWLRQDQGUHFRJQLWLRQPHWKRGV3XEOLV in IET Biometrics Revised on 10th Nov 2011 and 5th April 2012.
[3]. YONG-0(,$*0%,³)DFHDQG(DU5HFRJQLWLRQ Based on Multi-$JHQW3URFHHGLQJVRIWKH6HYHQWK International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008.
[4]. Anil K. Jain, Patrick Flynn, Arun RoVV³+DQGERRN2I%LRPHWULFV´Springer Publication, ISBN 978-0-387-71040-2.
>@/DQVD\6PLWK$WXWRULDORQSULQFLSDO&RPSRQHQWVDQDOVLV)HEUXDU\
[6]. A.A. Darwish, R. Abd Elghafar and A. Fawzi Ali, A.A. Darwish, ³0XOWLPRGDO)DFHDQG(DU,PDJHV´ Journal of Computer Sciences 5 (5):374-379,2009 ISSN 1549-3636.
[7] Gayatri Umakant Bokade and Ashok. M. Sapkal, "Feature Level Fusion of Palm and Face for Secure Recognition", International Journal of Computer and Electrical Engineering, Vol.4, No.2, 2012(11).