ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Biometric Recognition Using Unimodal and Multimodal Features

Sarala Patil

Department of Computer Engineering, G.H. Raisoni COE & Management, Wagholi, Pune, MH, India

ABSTRACT: Biometrics is the discipline and technology of measuring and examining biological data of human body, extracting a different feature set from the acquired data, and comparing this set against to the database temples set in the database. Tentative studies highlight that Unimodal biometric scheme had many drawbacks regarding performance and correctness. Multimodal biometric systems perform best as compare to unimodal biometric systems and are popular even then more complex also. We experiment and examine the accuracy and enactment of multimodal biometric authentication systems using state of the art Commercial Off- The-Shelf (COTS)products. In the proposed research work we discuss fingerprint as well as face biometric systems, conclusion and fusion techniques used in these approach. We also discuss their benefits over unimodal biometric systems.

KEYWORDS: Assessment, Multimodal Biometrics, verification, Normalization, Feature vector, Fusion, face, Matching feature, and fingerprint.

I. INTRODUCTION

The Multimodal biometric systems are provide recognition and human protection over last few decades. Because of this cause MBS are modified to lots of fields of applications. Several of these multimodal systems are individual computer dialog interface based systems where the user interacts with the PC in the course of voice or vision or any other pointing tool in order to complete a specific job. Multimodal biometric systems are those which uses or are capable of using more than one physiological or behavioral feature for conscription, verification,or detection. A biometric system is fundamentally a pattern detection system. This method measure and analyze individual body' Physiological characteristics like human fingerprints, eye as well as retinas and irises, different voice patterns, facial patterns and hand dimensions for confirmation purposes or behavioral characteristics. The biometric identifiers cannot be omitted. In spite of inbuilt reward, unimodal biometric solutions as well have restrictions in terms of accurateness, enrolment rates, and receptiveness to spoofing. This restriction occurs in several relevance domains like face recognition. The accurateness of face recognition is exaggerated by explanation and facial lexis. The biometric system cannot eradicate spoof attacks such as finger print spoofing. A modern report by the National Institute of Standards and Technology (NIST) to US accomplished that around two percent of the inhabitants does not have a comprehensible fingerprint [1]. Inspite

of using unimodal biometric system so as to have poor feat and accurateness, we learn and suggest a new approach to the multimodal biometric system. This recent Multimodal biometric systems act upon improved than unimodal biometric systems and are trendy even more intricate as well.

II. LITERETURE SURVEY

A Multi modal biometric system uses more than one physiological or behavioral characteristic for acceptance, verification or empathy. The given NIST detail recommends a method employing several biometrics in a encrusted loom. The cause to unite different modalities is to recover positive reception rate. The intend of multi biometrics is to lessen one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

• Susceptibility to artifacts or mimics

Multi modal biometric systems receive input from single or numerous sensors measuring two or more unlike modalities of biometric individuality. For example a system with fingerprint and face recognition would be measured "multimodal" even if the "OR" regulation was applied, allowing individuals to be confirmed using any of the modalities [4].

A. *Multi algorithmic biometric systems*

Multi algorithmic biometric systems receive a sole sample from a solitary feeler and route that sample by means of two or more unlike algorithms.

B. *Multi-instance biometric systems*

Multi-instance biometric systems make use of individual feeler or maybe more feelers to detain samples of two or more dissimilar instances of the identical biometric characteristics like acquiring imagery from multiple fingers.

C. *Multi-sensorial biometric systems*

Multi-sensorial biometric system model the similar case of a biometric attribute with two or more noticeably unlike sensors. Dealing out of the multiple samples can be completed with one algorithm or grouping of algorithms such as face recognition relevance may well utilize both a evident light camera and an infrared camera fixed with precise rate.

III. RELATED WORK

A method that can unite the classification outcome from each biometric conduit is called as biometric blend -fusion. We require to plan the fusion. Fusion in multimodal biometric unites dimensions from unlike biometric behavior to improve the strength. At matching score, rank and decision level, the fusion has been widely calculated in the journalism. Different levels of fusion : Sensor level, feature level, matching score level and decision level fusion.

A. *Sensor level Fusion:*

We unite the biometric behavior taken from various sensors to make a merged biometric characteristic and process.

B. *Feature level Fusion:*

Indication getting from different biometric channels is initially processed, and Feature vectors are acquired discretely, by means of specific algorithm and then we add these vectors to form a merged characteristic vector which helps classification.

C. *Matching score level fusion:*

Instead of adding the feature vector, we treat them independently and individual identical biometric matching score which will be used for classification which depends upon accuracy of each ach biometric matching score..

D. *Decision level fusion:*

Every modality is first pre-classified separately. Multimodal biometric system can put into practice whichever of these fusion strategy or grouping of them to advance the performance of the system; various levels of fusion are shown in below figure-I

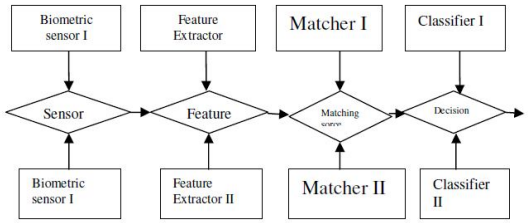


Figure –I. Fusion levels in multi modal biometric system

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

IV. SYSTEM ARCHITECTURE

At this time we talk about current architecture. In the literature Jain and Ross has discussed a multimodal biometric system with face and finger print and anticipated different levels of combination of the fusion as shown in Figure-II

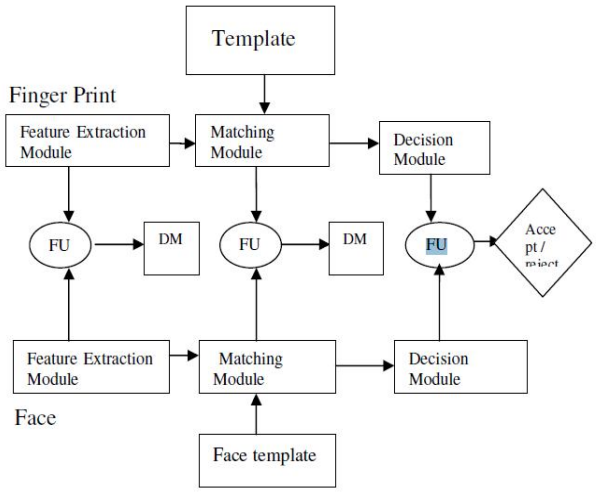


Figure – II Multimodal biometric system using face and fingerprint (FU – fusion DM – Decision Module)

Yan and Zang have projected a relationship sieve bank dependent fusion for multimodal biometric system and they utilized this work for Face and Palm print biometrics. In connection with sieve Bank, the free relationship filters skilled for a specific modality is intended by improving the in general inventive relationship outputs. Hence, the unlikeness between Face & Palm print modalities have been considered and helpful information in different modalities is entirely subjugated. PCA was utilized to lessen the measurements of characteristic set and then the considered correlated sieve/filter bank (CFB) was utilized for fusion. In fig. III it's shown that the fusion system architecture wished-for by them, the recognition rates they got are in the array of 0.9765 to 0.9964 by the projected system

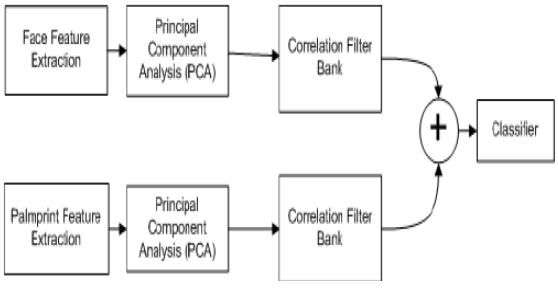


Figure III: Correlation Filter bank based fusion

V. UNIMODAL BIOMETRIC SYSTEM

Here squashy biometric characters need the individuality and stability to recognize an individual distinctively and dependably, they present some proof about the user uniqueness that could be helpful. This paper represents a outline for integrating the additional information with the harvest of a main biometric system. A probable key to the difficulty of conniving a reliable and comprehensible biometric system is to use additional information about the user such as age, weight, height, gender, traditions and eye color to perk up the performance of the main biometric system. Mainly

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

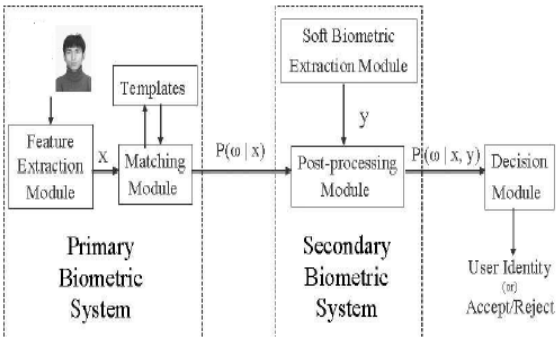
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

practical biometric systems gather such information about the users in enrollment. Though, this information is not at present used during the regular identification/confirmation phase. Merely when a real user is incorrectly discarded by the system, an individual operator stepladder to authenticate the squashy biometric character of the individual. If these traits can be routinely acquired and used in the conclusion making procedure, the overall performance of the system will enhance and requirement of manual intrusion will be lessened. The additional information by itself is not enough to institute the uniqueness of a individual as these characteristics are anonymous, changeable, and can be effortlessly spoofed.

VI. PROCESS FRAMEWORK OF UNIMODAL

In our outline, the biometric identification system is separated into two subsystems. One subsystem is the main biometric system and it is based on conventional biometric identifiers such as fingerprint, face and hand based geometry. Other subsystem, is resultant secondary biometric system, is based on squashy biometric characteristics such as age, gender, and height. In figure 3 it's shown as the architecture of a individual identification system which uses both of primary and squashy biometric measurements.



Module Integration of Biometric Traits with Fingerprint Biometric Scheme
(x is the facial feature vector and y is the squashy biometric feature vector)

The initial difficulty is that all the *m* soft biometric variables have been calculated evenly. In use, various soft biometric variables may contain additional information than the rest. In example, the height of a individual can provide more information about a individual rather than gender. Hence, we have to bring in a weighting system for the squashy biometric characteristics depends on an catalog of uniqueness and stability, i.e., the characteristics which have less unevenness and greater unique ability will be given extra weight in the calculation of the concluding matching possibilities. a further impending drawback is that any charlatan can effortlessly spoof the system as the soft traits have an identical say in the conclusion as the main biometric characteristics and it is moderately simple to enhance individual's soft biometric attribute through the application of cosmetics and wearing other garnishes (e.g. mask, shoes with heels, etc.). Hence to stay away from this crisis, we allot lesser weights to the soft biometric characteristics as compared to that assigned to the main biometric characteristic. This degree of difference weighting in addition has a different implied benefit. Yet if a soft biometric characteristic of an individual is calculated wrongly (male individual is confirmed as a female individual), there is a less decrease in this individual's prospect and the individual is not instantly abandoned. In the case, when the main biometric created a acceptable match, the individual may be confirmed. When several soft biometric characteristics not matching, then there is considerable lessening in the posteriori prospect and the individuals may be probably abandoned. When the devices which calculated the soft biometric characteristics are considerably correct then the condition has much less possibility of happening. The beginning of the weighting system outcome in the following discriminant purpose for end individual.

VII.ALGORITHM

Face Feature Recognition algorithm
Input: Input image feature vector

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Output: Relevance distance between both images

Step 1: Extract Low-level Features:
For each face image I,
weexcerpt the output of k low-level features fi=1:::k
and concatenate these vectors to form a big feature
Vector
F(I) = hf1(I);
fk(I)i.

Step 2. Compute Visual Traits: For every extracted featurevector F(I), we compute the result of n trait classifiers
Ci=1:::n
in order to produce a "trait vector" C(I)
for the face,

C(I) = hC1(F(I));
Cn(F(I))i.

Step 3. Perform Verification: To choose if two face objects I1 and I2 are of the similar person, we associate theirtrait trajectories using a concluding classifier D which describesour verification purpose v:*v(I1; I2) = D(C(I1);C(I2))*
v(I1; I2) should be optimistic when the face objects I1

VIII. APPLICATION

Some forms of corporeal biometric identification comprise the following:

- Fingerprint Recognition system
- Iris Recognition system
- Retina Recognition system
- Finger Geometry Recognition system
- Signature/Handwriting Recognition system
- Voice Recognition system
- Facial Proportions Recognition system
- Hand Geometry Recognition system
- Gesture Recognition system

VIII. CONCLUSION

A outline was established with assessing the recital of multimodal biometric systems.We have examined moderately large face and fingerprint data sets over a band of normalization of score and fusion methodologies. The outcome of this learning displays multimodal biometric systems can perform better than uni-modal biometric systems. Also additional gain of fusion at this stage is that existing and proprietary biometric systems does not require to be enhanced which allows a widespread middleware layer to lever the multimodal applications with a less extent of widespread information. Furthermore, the future scope is to explore substitute normalization and fusion techniques. The single-mode biometrics testing, has accomplished correctly and calculated the performance of biometric systems, testing must be happened with data sets on the arrange of tens of thousands subjects and that no inferences be haggard from the testing performed on short subject populations to evaluate the system' scalability. Thus, future tactics comprise mounting the testing database to achieve these greater sizes. Also in addition, to evaluate the achievability of such systems for large-scale deployments, we will perform the testing by using COTS products.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

REFERENCES

[1] "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, andinteroperability," NIST Report to the United States Congress, Nov.2002.
[2] Biometrics: Personal Identification in networked Society, A.K. Jain, R. Bolle, and S. Pankanti,eds., Kluwer Academic, 1999.
[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition.Springer,2003.
[4] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach,"
[5] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 10, pp. 955- 966, Oct. 1995.
[6] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226- 239, Mar. 1998.
[7] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification," IEEETrans. Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, Dec. 1998.
[8] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for PersonIdentity Verification," IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.
[9] A. Ross and A.K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol. 24,no. 13, pp. 2115-2125, 2003.
[10] P.J. Huber, Robust Statistics. Wiley, 2013.