Applications of Principal Component Analysis in Multimodal biometrics system

Chhaya S..Khandelwal, Assitant Professor, Department of Electronics and Telecommunication, MGM,s Jawaharlal Nehru Engineering College, Aurangabad, (M.S.) , India.
chhaya.khandelwal@rediffmail.com
Ranjan Maheshwari, Professor, Department of Electronics, RTU, Kota(Rajasthan), India.
ranjan@rtu.ac.in
Ulhas Shinde,Principal, Department of Electronics and Telecommunication, CSMSSCOE, Aurangabad, India. drshindeulhas@gmail.com

Abstract: Unimodal biometric systems have many problems like intra-class changes, spoof attacks, limited degrees of independence, noise data, non-universalism and unacceptable error rates. Use this problem to use the multimodal biometric system. It uses many sources of information.. The use of multimodal biomatrics automatically discriminate between subjects and protect data. It also protects resources access from unauthorized users. We develop a biometric identification system that represents a valid alternative to conventional approache. In proposed multimodal biometrics system for identity verification using fingerprint and iris trait. The training data base contains the iris and fingerprint for individual matches and matching between query images and enrolment templates .The principal component analysis and Minutiae extraction methods for individual matches. The proposed system use rank level fusion method for increasing the efficiency and accuracy.

Keywords ——PCA, Multimodal biometrics, fingerprint recognition, iris recognition, minutiae extraction.

I. INTRODUCTION

The term biometrics is derived from the Greek words Bio& Metric .Bio means life and Metric is to measure. The applications of biometrics is security. It is recognizing a person based on a physiological or behavioral characteristic. (e.g. face fingerprints, hand geometry, handwriting, iris, retinal, vein, voice etc.) Biometric technologies are secure identification and personal verification solutions [1]. As security breaches and frauds increase in transactions, the need for safe identification and personal verification techniques is becoming accurate. In recent years, biometrics authentication has seen considerable improvement in reliability and with some characteristics that provide good performance and accuracy. Even the best biometric traits are facing many problems; Some of them are embedded in technology. In particular, biometric credentials.

There are many biometrics-based technologies. Professional research today And many have been deployed worldwide in educational and commercial research laboratories. At present, there are mainly eight different biometrics, including face, fingerprint, iris, retina pattern, hand geometry. Signatures, voice prints and themograms are actually deployed for verification.

A simple biometric system consists of four basic components: A simple biometric system consists of four basic components:

1)Sensor module that receives biometric data;

2) Feature extraction module is processed to remove feature vectors;

3) Matching module where query images are compared with nomination templates;

4) Decision-making module in which the user's identity is accepted or rejected.

Any human physical or behavioral symptoms can work as a biometric feature unless it meets the following requirements[1][2][8]

1)Universality Except for some exceptions such as physical deformity, everyone should have it;

2) Collectibles The facility should be sensitized to the given system.

3) Specification. No two people should have the same characteristics;

 DOI : 10.35291/2454-9150.2019.0257

4) Stability. It should be immutable in a period of time.

II. LITERATURE SURVEY

Multimodal techniques are not new to the medical world. In routine medical checkups also, it is often preferred have a primary and a confirmatory examination. The inclusion of evidence from more than one sources would enhance the overall Accuracy of the system.[15]

Abhishek K. Nagar,et.al.[3] A detailed analysis of trade-off between matching accuracy and security in proposed multi-antibiomic cryptosystems based on two-well-known databases (a real), feature-level fusion framework using two-well-known biometric cryptosystems, namari, fuzzy walt and fuzzy commitment . And a virtual multimodal database)

Vincenzo Conti et.al.[4] An innovative approach to fusion features. In more detail, the frequency based approach results in a homogeneous biometric vector that integrates iris and fingerprint data. Successfully, a humming-distance-based matching algorithm is related to integrated homogeneous biometric vectors.

. Robert Snelick et.al.[5]state-of-the-art commercial off-the-shelf (COTS) fingerprint and face biometric systems on a population approaching 1,000 people.

A. Muthukumar et.al[6]A multimodal an evolutionary algorithm, system based on particle swarm Optimization that is suitable for different safety environments.

Sumit Shekhar,,et.al.[7] Multipurpose quality measurement is also offered to weigh each module because it fuses. In addition, we also kernel the algorithm to handle non-purity in the data. The optimization problem is solved using an alternative direction method. Various experiments show that the proposed method is comparable to competitive fusion-based methods.

III. BIOMETRIC SYSTEM

A biometric system is essentially a pattern recognition system that receives biometric data from one person, which removes the attribute set with acquired data and compares this query image with the Enrollment template in the database. Depending on the context of the application, a biometric system may also work in verification mode or identity mode. The effectiveness of a biometric system can be seen by the following characteristics: performance, scalability.

A.Materials and Methods

Block diagram of unimodal and multimodal biometrics system

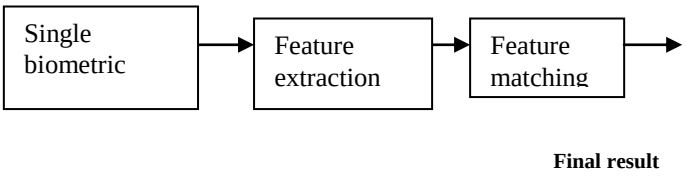

Fig1.Unimodal biometrics

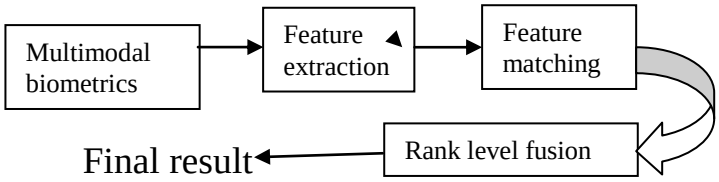

Fig2: Multimodal biometrics

A biometric system has four important modules. The sensor module receives biometric data from a user; Feature Extraction Module Processes Acquired Processes Biometric data and a feature set to show it; Comparison of extracted feature with matching module archived templates using a classified or matching Algorithm to generate matching score; In the decision-making module score is used to either identify the identified user or to verify the identity of the user .Sanderson and Paliwal [9] .Classified information is Fusion in two broad categories in biometric systems:

The former classification fusion is a combination of information Before applying any classifier or matching Algorithm. In the fusion after classification, there is information Combined after classifier decisions Received. Figure 1 shows the block diagram Unimodal and Figure 2 shows the block diagram Multimodal biometric system In an uneven biometric The system, the first step is the enrollment phase The next feature is the extraction phase in which the features of each person identified, are extracted and the next feature is the matching phase in which there are attributes Compared with data base and get output.[11].In a multimodal biometric system, the images are average and normalized after the enrollment phase and then given to its matching phase in which the features are matched and then it is ranked according to the availability of the data and achieved the result. goes.

3.1 Fingerprints as a Biometric:-

An fingerprint friction streak is an impression from the surface of the anger-tip. Fingerprint has been used for personal identification for several decades, recently automated due to progress in computing capabilities.Fingerprint recognition is now one of the most important and popular biometric techniques one day, primarily due to the inherent inherent inherent acquisition, many sources available for archiving (ten fingers), and for use and collections established by law enforcement agencies is.

***Preprocessing*:** We collected live data from the Computer Science Department to improve the quality of the image, and

 DOI : 10.35291/2454-9150.2019.0257

then performed preprocessing on the fingerprint image. First of all, we captured the fingerprint image using Futronic FS88. Then the histogram of the image was equal. it usually increases the global contrast of an image and was enhanced using FFT. After FFT, in the increased image, add some broken points to some wrongly on the lines, and to remove some intuitive connections in between ridges.

We also processed with histogram equalization after the FFT transform. Then thresholded the image. We extracted the singularity region with the help of Adaptive threshold. Adaptive binarization method is performed to binarize the fingerprint image. Fingerprint image binarization is transforming the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. Region of Interest(ROI) is useful to be recognized for each fingerprint image.To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check. While the second is intrigued from some Morphological methods. Features are extracted using minutia and matching is done using edge. We have use confusion matrix.The field of machine learning and specifically the problem of statistical classification ,Each column of the matrix represents the instances in a Predicated class while each row represents the instances in an actual class .We have Find out Recall, Precision using following formula

Recall(cl)=tp(cl)/(tp(cl)+fn(cl))

Precision:

spe(cl)=tn(cl)/(fp(cl)+tn(cl));

pre(cl)=tp(cl)/(tp(cl)+fp(cl));

F-score: The harmonic mean of precision and recall(sensitivity)

f_sco(cl)=2*tp(cl)/(2*tp(cl)+fp(cl)+fn(cl)) we have see in Table no.1.

Table.No.1

Item	Recall	Specificity	precision	F-score
Fingerprint	0.9553	0.9605	0.9942	0.9576
Iris	0.8681	0.8762	0.9823	0.8712

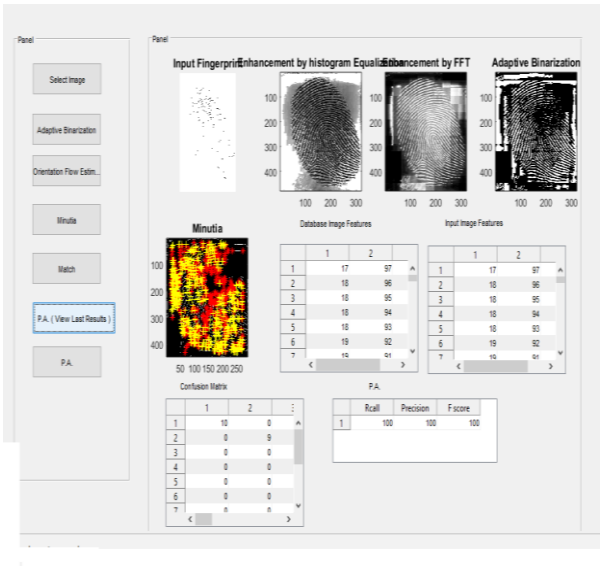

Fig.3 Fingerprint Recognition

IRIS RECOGNITION

Iris is unique to every person and remains stable on the life of a person. In the eyeball, there is a round black disk called the pupil. When exposed to light, the pupil becomes weak and shrinks in the dark. Thus the size of the pupil is different in relation to light and it comes in contact with it. Iris is the annular ring between the sclera and the pupil border, and there is a unique flower pattern for each person. The textual information remaining unique to each person.

Iris is unique to each individual and remains constant over the life of a person. The eyeball has a circular black disk in the center known as the pupil. The pupil dilates when exposed to light and contracts in dark. Thus the size of pupil varies with respect to light it is exposed to. The iris is the annular ring between the sclera and pupil boundary and contains the flowery pattern unique to each individual. This texture information unique to each person is derived from the image of the rest of the eye and is transformed into a bar to apply pattern matching algorithms between the iris database and query images. Automatic Iris recognition system has been proposed by Flom and Safir [16].

Preprocessing of iris: We had collected live data from computer science department. Then captured the image using I Scan 2 Cross Match Technologies Inc**,** and pre-processed to localize and normalize the iris. In Iris pre-processing, we reduced the papillary area to pure black, in order to properly recognize the inner papillary boundary and remove bright flashes present in the image. Location of the pupil and outer iris boundaries is the first stage in iris preprocessing. By image segmentation, the iris is detected and extracted from an eye image. Segmentation of iris depends on the quality of the eye images. The normalization process is needed to transform the located iris into a fixed dimension. We used a feature extractor to extract the features and a pattern matching module for matching. The iris was extracted from the acquired image of the whole eye.

 DOI : 10.35291/2454-9150.2019.0257

Therefore, before performing iris pattern matching, the iris was localized and extracted from the acquired image.

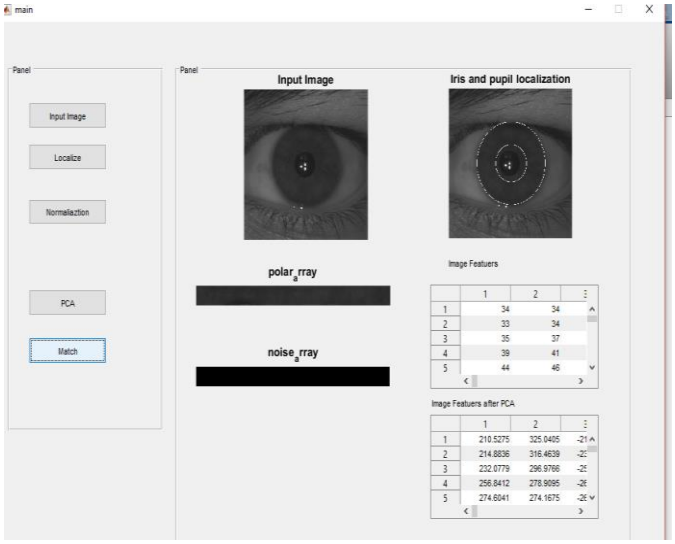

Fig.4 Iris Recognition

Principal Component Analysis (PCA) is a statistical process, which uses an orthogonal change to convert a set of correlated variables into linearly unrelated variables, which is called the principal component. It is used to reduce the signal in signal processing. Properties used for PCA eigenvectors PCA is mostly used to create data analysis and predictive models. It is often used to visualize genetic distances and relativity among the population.

PCA can be done by eigenvalue decomposition of a data covalent matrix.

Calculate PCA using the Covaraince method.

1) Organize the data set

2) Calculate the empirical mean

3) Calculate deviation from mean

4) Find covalent matrix

5) Find the eigenector and eigenvalues of the Covariance matrix

6) Calculate the cumulative energy content for each eigenvector

7) Choose a subset of aiens vector in the form of base vectors

Base vectors are eigenvectors. Eigenvectors are defined in image location. They can be seen as images. Therefore, they are usually referred to as Eigen images. Eigenimage recognition is derived from the German prefix Eigen, which means self or individual. The first Eigenimage is the average image, while the rest Eigen diagrams represent variations from this average image. When a particular image is projected at the image space, then its vector (each is made up of its weighted values in relation to Eigen images) describes the importance of each attribute in the image in the image space. In our system, the Eigenimage approach is used. It has many advantages.In the context of personal identification, background changes can be controlled and a compact representation of an image in the Eigenimage approach, which can be clearly expressed by the feature vector with some elements. In addition, it can be operated efficiently using different indexing techniques such as retrieval, it is possible to index an eigen image-based template database. In addition, the Eigenimage approach is a generalized template-matching approach, which has been..[2][12]

Fusion in multimodal biometrics

In a multimodal biometric system, after the enrollment phase, the images are average and normalized and then given to its matching phase in which the features are matched and then it is ranked according to the availability of data and the results are obtained. Later, we add both methods using the rank mode fusion.

Fusion: Rank-level fusion is a relatively new fusion approach. When the production of each biometric match is a subset of possible matches sorted in decreasing order, then fusion can be done at the rank level. The aim of the rank level fusion is to consolidate the rank output by the individual biometric subsystem (matchers) so that consensus rank can be obtained by using three methods to combine the ranks determined by different matchers for each match. [13] .

1. The Highest Rank Method,

2. The Borda Count Method and

3. The Logistic Regression Method.

In the highest rank method, each possible match is assigned the highest (minimum) rank, as computed by different

matchers. The Borda count method uses the sum of the ranks assigned by individual matchers to calculate the final

rank. In the logistic regression method, a weighted sum of the individual ranks is calculated. The weight to be

assigned to different matchers is determined by logistic regression.[6][14]

IV. Experimental Results

The results are tested on iris and fingerprint images collected by SAP Labs. The database includes a total of 55 people per person (55 × 10) = 550.for fingerprint and (55 × 10) = 550 iris and ten of the 1100 images with ten iris images per person and ten fingerprint images. Iris images are acquired using the IIS 2 Cross Match Technologies Inc. Iris scanner. However, fingerprint images are obtained using the Futuronic FS22. Fingerprint scanner this level.he results are tested on iris and fingerprint images collected by the SAP lab. The database consists of Ten iris images and Ten fingerprint images per person with a total of 55 persons having (55×10)=550.for fingerprint and (55×10) =550 for iris and total 1100 images. The iris images are acquired

 DOI : 10.35291/2454-9150.2019.0257

using I Scan 2 Cross Match Technologies Inc. iris scanner. However, fingerprint images are acquired using Futronic FS88. fingerprint scanner At this level, Are personal results Calculate Individual accuracy for Iris is 92.92% and fingerprint is 97.73%

V. CONCLUSION

Multi-biometrics is a new and exciting field of information science research that is guided by the understanding of the characteristics and methods of accurate and reliable personal information representation for subsequent decisions and reconciliation. In recent years, there has been a significant increase in research activity for use by public and security services to understand all aspects of biometric information system representation and to support decision-making, and Use to support decision-making, for use by public and security services, and to understand the complex processes behind biometric matching and recognition. There are two model fingerprints and iris in this paper. These two modes give a novel result which can be used for further purposes.

ACKNOWLEDGMENTS

We are thanks to Computer science Department at Dr .B.A.M .U. Aurangabad. They have given me the opportunity for collecting data in SAP Lab.

The Authors are indebted to their respective institutions and also to the National Institute of Electronics and Information Technology, Aurangabad, where the first author is registered for her research work and the other authors are registered as supervisors. Thanks to Ranjan Maheshwari sir who provided valuable guidance.

REFERENCES

[1] Kresimir Delac 1, Mislav Grgic 2, A survey of biometric recognition methods , 46th International Symposium

[2] Electronics in Marine,Elmar-2004, 16-18 June 2004; Zadar, Croatia

[3] Anil Jaina, Karthik Nandakumara, Arun Rossb, Score normalization in multimodal biometric systems, Pattern Recognition 38 (2005) 2270– 2285, accepted18 January 2005

[4] Abhishek K. Nagar, Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and Anil K. Jain, Fellow, IEEE ,Multibiometric Cryptosystems Based on Feature-Level Fusion, IEEE Tractions on Information Forensics and Security, vol.7, no.1, February 2012.

[5] Vincenzo Conti, Carmelo Militello, Filippo Sorbello, Member, IEEE, and Salvatore Vita bile, Member, IEEE, A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems, IEEE Tractions on system, Man, and. cybernetics— part C: Application and Reviews, vol. 40, no. 4, July 2010

[6] Robert Snelick1, Umut Uludag2*, Alan Mink1, Michael Indovina1 and Anil Jain2 Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 27, No. 3, Mar2005, pp 450-455.

[7] A. Muthukumar1, C. Kasthuri2 and S. Kannan3,Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris ,ICTACT Journal on Image and video processing, February 2012, volume: 02, Issue: 03

[8] Sumit Shekhar, Student Member, IEEE, Vishal M. Patel, Member, IEEE Nasser M. Nasrabadi, Fellow,IEEE, and Rama Chellappa, Fellow, IEEE,Joint Sparse Representation for Robust Multimodal Biometrics, IEEE Tractions on pattern analysis and machine Intelligence, vol. 36, no. 1,January 2014.

[9] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE, An Introduction to Biometric Recognition, IEEE Tranctions on circuits and systems for video Technology,Vol.14,No.1,January 2004.

[10] C. Sanderson, K.K. Paliwal, Information fusion and person verification using speech and face information, Research Paper ID IAP-RR 02-33, IDIAP, September 2002.

[11] U. M. Bubeck and D. Sanchez, Biometric authentication: Technology and evaluation, San Diego State Univ., San Diego, CA, 2003. Tech. 9.Rep.

[12] Md.Maruf Monwar , and Marina L. Gavrilova, ultimodal biometric system using Rank Level Fusion Approach, IEEE Transactions on System, Man and Cybernetics – Part B: Cybernetics, Vol.39, No.4, August 2009.

[13] M. P. Down and R. J. Sands, “Biometrics: An overview of the technology, challenges and control considerations,” Inf. Syst. Control J., vol.4, 2004; pp. 53– 56

[14] S. Prabhakar, S. Pankanti, A. K. Jain,Biometric Recognition: Security and Privacy Concerns, IEEE Security & Privacy, March/April 2003; pp. 33-42.

[15] .A.Muthukumar1,C. Kasthuri2 and S. Kannan3,Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris ,ICTACT Journal on Image and video processing, February 2012, volume: 02, Issue: 03

[16] C.S Khandelwal, R Maheshewari, U.B. Shinde,” Review paper on applications of principal component analysis in multimodal biometrics system”Procedia Computer Science 92, 481-486.

[17] L. Flom, & A. Safir, Iris Recognition System, U.S. Patent No. 4641394, 1987.

 DOI : 10.35291/2454-9150.2019.0257