International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey of Biometric, Multimodal Biometric Systems

Dhanashri J. Ghate[1], Savitri B. Patil[2]

[1]Department of Computer Engineering, GHRCEM Wagholi, Pune University, India

[2]Department of Information Technology, GHRCEM Wagholi, Pune University, India

Abstract: ***Now a days Security of computer science and information technology is an important issue. Authentication and identification are related to the security. The traditional methods for confirming person identity involve use of ATM, Pins, and Password which can be lost or stolen. So it is needed to have a system which provide security and overcome the limitations of traditional methods. A biometric is the automated method of identifying the person identity. Also biometric of the individual cannot be hacked easily like password and pin. Unimodal biometric system uses only one biometric as verification tool. It has some limitations. Multimodal biometric system uses more than one biometric as verification tool and overcome limitations of unimodal biometric system. So it is required to have survey on biometric and multimodal biometric system that provides more security in many applications and also need to know different algorithms used in biometric system.***

Keywords: Unimodal, Multimodal Biometrics, Fusion Levels, PCA, LDA

1. Introduction

Identity management systems are those which have the job of providing authorized user easy access to data and provide the security. Many methods which are knowledge based may involve use of pins, password, ID cards etc. This type of information may get stolen or lost by the user. Biometric authentication is based on physiological or behavioral characteristic of the person. The common physiological characteristics are retina, iris, fingerprint, palmprint, hand geometry, face, vein geometry etc. The common behavioral characteristics are keystroke, voice, and signature dynamics. Biometrics is the pattern recognition technique that takes the biometric data as the input, extract the features from input image and then compares feature set with the template which is stored in the database and gives the result that the person is identified or not. The paper is organized as follows. A general biometric system is discussed in Section II, whereas need of multimodal biometrics is illustrated in Section III., Multimodal biometric system and Different fusion techniques in section IV , Operational modes in section V , Advantages in section VI, Application in section VII, Challenges are presented in Section VIII, Algorithms in section IX., Conclusion in section X .

2. General Biometric System

2.1 Processing Modes of Biometric System

1)Enrollment mode
2)Verification mode
3)Identification mode

1) Enrollment Mode
In order to check the person identity, it is required to have template in the database. Template of the individual is the features which are extracted from the image of that person.

2) Verification Mode
Validating the person by comparing the persons captured data with his own template which is stored in the database.

3) Identification Mode
In identification mode, the system recognizes an individual by searching the templates of all the users in the record for a equivalent. So the structure conducts a one to many comparisons to establish an individual identity or fails, if the subject is enrolled in the system record.

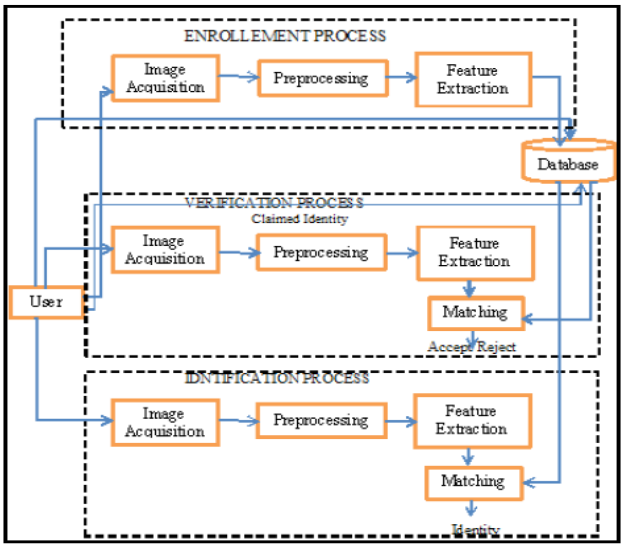

Figure 1: Modes of biometric system

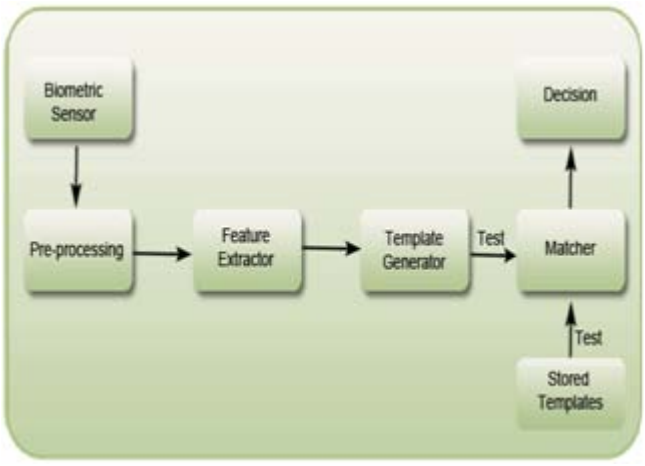

Figure 2: Block diagram of biometric system

2.2 Biometric System Working

Biometric system works as follows.

1. Sensor Module: Biometric data of the individual is captured by different sensors.
2. Preprocessing: In this, the captured image is preprocessed i.e. the image is converted into the required size or filters are used to remove the noise from image.
3. Feature Extraction: Features are extracted from the image that is captured and processed.
4. Matching module: In this module the features extracted from the input data are compared against the template stored in the database.
5. System database module: Database is taken to store the templates of user.

3. Need of Multimodal Biometric

Most of the real world problems use unimodal biometric system which depends on the evidence of single source of information for authentication. This system has some limitations like

- Noise in the sensed data
- Intra class variation
- Inter class variation
- Non universality
- Spoofing

4. Multimodal Biometric System

In multimodal biometric, two or more physiological or behavioral characteristics are utilized for identification. Multimodal biometric system overcomes the limitations of unimodal biometric system. The multimodal biometric system significantly improves the recognition performance of a biometric system besides improving population coverage, deterring spoof attacks, and reducing the failure-to-enroll rate. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. The main aim of multi modal biometric is to reduce,

1) FAR(False Acceptance Rate): Biometric system will incorrectly allow access by an unauthorized user.
2) FRR(False Rejection Rate): It is the measure of biometric system that it fails to authenticate the person identity.
3) FTE (Failure To Enroll Rate): Biometric system fails to create template from the input image. This is caused due to use of low quality image.

4.1 Fusion in multimodal biometric system:

In the biometric fusion, classification result from the each biometric channel is combined.
Biometric data from two or more biometric system can be combined using possible four level of fusion:

1) Fusion at Sensor level: Data taken from two different sensors can be combined, so that the template created from the combination of these two will be better than using them individually. It means that, the combined template gives more accuracy than the individual.
2) Fusion at Feature extraction level:Two different sensors capture the two different images. After that the images are pre processed. Information from the both of them is taken by using different algorithms and it is stored as the feature vector. After this, the feature vectors of both the images are combined and stored as the one joint feature vector. it will be used in the classification
3) Fusion at Matching score level:
4) Instead of combining the feature vector the individual matching score is calculated. After this, the score of the individual is compared with the template stored in the database. Based on matching score of the individual matched with the template it is further used for the classification.
5) Decision Level Fusion:
6) Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes- accept or reject. A majority vote scheme can be used to make the final decision.

5. Operational Modes of Multimodal Biometric Systems

A multimodal biometric system can operate in three different modes.

1. Serial Mode: In this mode of operation, the output of one biometric trait is used to narrow down the number of possible identities before the next trait is used. Therefore multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously. Further, a decision could be made before acquiring all the traits. This can reduce the overall recognition time.
2. Parallel Mode: In this mode of operation information from multiple traits is used simultaneously to perform recognition.
3. Hierarchical Scheme: In this mode of operation, individual classifiers are combined in a treelike structure.

6. Advantages of Multimodal Biometric System:

1. **Non-universality:** Multimodal biometric system solves the problem of non universality which is occurred in unimodal biometric systems. For example, if the persons cut finger prevents him from successfully enrolling into a fingerprint system, then the availability of another biometric trait, say face, can be used in the inclusion in the biometric system.
2. **Indexing Large-scale Biometric database:** Multimodal biometric systems can make easy filtering of large scale biometric databases.
3. **Spoof Attacks:** It becomes increasingly difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual.
4. **Noise in Sensed Data:** Multimodal biometric system considers the problem of noisy data. During preprocessing of image, filteration of image is carried out and the noise from image is removed out.
5. **Fault tolerance:** A multimodal biometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become

unreliable due to sensor or software malfunction, or deliberate user manipulation.

7. Applications of Multimodal Biometric System

Most of the biometric applications are related to security also, used in commercial, forensic, government and public sectors.

1) Commercial applications: It involves computer network login, electronic data security, ecommerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning etc.
2) Government Applications: Like, national ID card, correctional facility, driver's license, social security, welfare disbursement etc.
3) Forensic Applications: Mainly corpse identification, criminal investigation, terrorist, identification, parenthood determination, missing children, etc.
4) Public Applications: It involves canteen administration, border control, voting system, prison visitor system.
5) Transport Applications: Airport Security, Boarding Passes

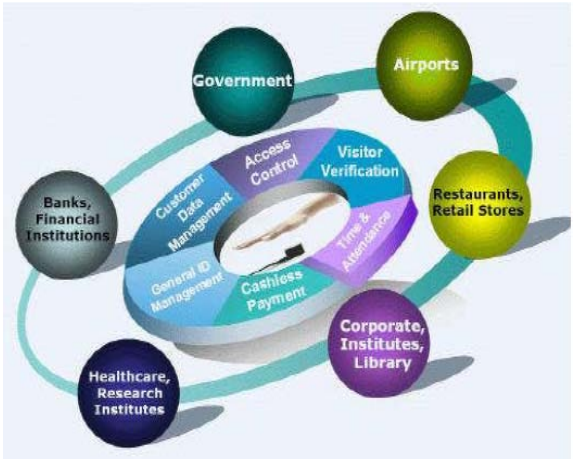

Figure 3: Applications of Multimodal Biometric System

8. Challenges to Multimodal Biometric

Based on applications and facts presented in previous section, following are the challenges in multimodal biometric system.

1) Performance of the sensors should be consistent. The sensors should be fast in collecting image from a distance also having low cost.
2) Selecting best level of fusion will have direct impact on performance and cost involved in developing a system.
3) Numbers of techniques are there for fusion in multi biometric system. So it is challenging to find the optimal solution for application provided.
4) In multimodal biometric system, information is acquired from different sources can be processed in sequence or parallel. So it is challenging to decide about the preprocessing architecture.
5) Strong understanding of biometric technologies will help in better design.
6) Scalability improvement and quality measures to assist decision making in matching process.

9. Algorithms used in Biometric Systems

9.1 PCA (Principal Component Analysis)

PCA is the statistical technique that is used to analyze data sets. The main function of PCA is to reduce the dimensionality of a data set. It is the method of identifying patterns in data and expressing the data that will highlights their similarities and differences. . Basically PCA algorithm is used only for face recognition systems also been used in palmprint and fingerprint verification.

9.1.1 Method

Step 1: Input the data set
Step 2: Subtract the mean from the
Data set.
All the x values are subtracted by the mean of all x values and all y values are subtracted by the mean of all y values. This step is required for the PCA to work properly.
Step 3: The covariance matrix are calculated for the data set. Covariance matrix can be defined as:

$$C^{m\times n} = \left(c_i, c_j = cov\left(Dim_{i,}, Dim_j\right)\right)$$

Step 4: Calculate the Eigen values and the Eigen vector of this covariance matrix.
Step 5: Chose components and obtain the feature vector. The principal component of data set is chosen such as it holds Eigen vectors with highest value. After the eigenvectors are obtained from the covariance matrix, the Eigen values are sorted according to ascending order. This yields the components in order of significance and helps to ignore the one that have lesser significance. Ignoring small Eigen values doesn't result in losing much information. After ignoring the m Eigen vectors from a original data set of n dimension, resulting matrix have a dimension of p. These eigenvectors are arranged in a column to yield the feature Vector.

$$\text{Feature Vector} = \left(eig_1\ eig_2 \ldots\ldots eig_p\right)$$

In data set, the feature vectors are obtained by leaving out the smaller, less significant values and arranging the rest in a single column.
Step 6: The new data set is derived. It is done by taking the transpose of the feature vector and multiplied by the left of original data set.
Final Data =RowFeatureVector× RowDataAdjust

2. LDA (Linear Discriminant Analysis):

LDA is a dimensionality reduction technique that is used to project a high dimensional original space into a significantly lower dimensional feature space, in which class separability is maximized. The class separability is defined as the ratio of the between-class scatter to the within-class scatter. In other words, it tries to group samples of the same class closer together while separating samples of different classes further apart. The goals of the LDA are:-

1. Selection of separator variables.
2. Selection of Discriminant functions.
3. Classification

The steps for the Discriminant analysis are as follows.

1)The best Discriminant variable is identified so that it separates the classes effectively.
2)Development of function for the computation of new index that describe dissimilarity.
3)The observations are classified based on the Discriminant function.

9.2.1 Method

1. The data set and the test sets are formulated.
2. The mean of each data set and entire data set is calculated.
3. Within class and between classes scatters are calculated using the equations

$$S_w = \sum_j p_j \times (cov_j)$$

$$S_w = 0.5 \times cov_1 + 0.5 \times cov_2$$

Where, the second equation is used for two class problems. Expected covariance of each of the classes is the within class scatter and the covariance matrices are symmetric and computed by,

$$cov_j = (x_j - \mu_j)(x_j - \mu_j)^T$$

Where S_w is the within class scanner.
The between class scatter is given
By following equation.

$$S_b = \sum_j (\mu_j - \mu_3) \times (\mu_j - \mu_3)^T$$

4. Set of Eigen vectors whose Eigen values are nonzero is linearly independent and invariant under the transformation. Zero Eigen values represent the linear dependency between the features. The Eigen vectors with nonzero Eigen values are considered and that of zero Eigen values are discarded to obtain a non redundant set of features.
5. Obtain the transformation matrices. Using single LDA transform, the data sets are transformed.
The test vectors are also transformed and classified.
6. Euclidean Distance or RMS distance is used to classify point s after the completion of transformation.

3. ICA (Independent Component Analysis):

ICA is the unsupervised computational and statistical method for discovering intrinsic hidden factors in the data. ICA exploits higher-order statistical dependencies among data and discovers a generative model for the observed multidimensional data. ICA can be applied to feature extraction from data patterns representing time series, images or other media.

Let X→R^N is a vector of images
Where, N is the dimensionality of image space. Its covariance matrix is given by the equation

$$E\{X - E|(X)[X - E(X)]^T\}$$

Where E () is expectation operator. T is transpose operator.

Comom developed an algorithm consisting of three operations for deriving the ICA transformation F. whitening, rotation and normalization is the three operations where whitening performs the transformation of random vector X into another vector U which has a unit covariance matrix. Source separation is performed by the rotation operator by minimizing mutual information approximated by higher order cumulants. Derivation of unique independent components in terms of orientation, order of projection and unit term is done by normalization. For enhanced performance, ICA is required to carry out in a compressed and whitened space where information regarding original data is preserved and discarding small trailing Eigen values.

10. Conclusion

Now a days Security of computer science and information technology is an important issue. Authentication and identification are related to the security. The traditional methods for confirming person identity involve use of ATM, Pins, and Password which can be lost or stolen. So it is needed to have a system which provide security and overcome the limitations of traditional methods. So in this paper unimodal and multimodal biometric techniques are discussed. Also fusion methods, operational modes, applications challenges faced by multimodal biometric system are given. PCA, ICA, LDA are studied.

References

[1] Anil K. Jain, Arun Ross and Salil Prabhakar,"An Introduction to Biometric Recognition", Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004
[2] Anu, Madhwendra Nath,Dr.harvir,"A review on biometric fusion",computer science and management studies ,Volume 2, Issue 5, May 2014 ISSN: 2321-7782
[3] Savitri B. Patil, "A Study of Biometric, Multimodal Biometric Systems: Fusion Techniques, Applications and Challenges", IJCST Vol. 3, Issue 1, Jan- March 2012
[4] Lindsay I Smith, “A tutorial on Principal Components Analysis”, February 26, 2002
[5] A.K. Jain, A. Ross,“Multibiometric systems”, Communications of the ACM, Vol. 47, pp. 34-40, 2004
[6] Taruna Panchal Dr. Ajit Singh,"Multimodal Biometric System",Computer Science and Software Engineering,Volume 3, Issue 5, May 2013 ISSN: 2277 128X
[7] D.Gayathri, Dr.R.Uma Rani,"Multimodal Biometric System: An Overview",Computer and Communication Engineering,Vol. 2, Issue 1, January 2013
[8] Aamir Khan, Hasan Farooq,"Principal Component Analysis-Linear Discriminant Analysis Feature Extractor for Pattern Recognition",Computer Science Issues, Vol. 8, Issue 6, November 2011 ISSN: 1694-0814
[9] Prof. Vijay M. Mane,Prof. (Dr.) Dattatray V. Jadhav,"Review of Multimodal Biometrics: Applications, challenges and Research Areas",Biometrics and Bioinformatics, Volume 3, Issue 5
[10] Mr. Sarath P.S, Ms. Kumary R Soumya,"Study on Face Recognition Algorithm",Computer Engineering,8727Volume 16, Issue 2,Mar-Apr. 2014 ISSN: 2278-0661