ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

A Study on Multibiometric Fusion Approaches

[1]Sangeetha.S, [2]Radha.N.
[1]PSGR Krishnammal College for Women, Coimbatore, Tamilnadu, India
[2]G.R. Govindarajalu School of Applied Computer Technology, Coimbatore, Tamilnadu, India

Abstract
The biometric system is one such that can provide accurate and reliable scheme for person verification. The main aim of biometric based security system is to make sure that rendered service is accessed only by valid user. The concept of multimodel biometrics is gaining importance to realise reliable, accurate and robust authentication systems. In multimodal biometrics, information fusion can be done at various levels: sensor level, feature level, match-score level, and rank level and decision level. This paper surveys the issues of fusion at different levels and recent researches addressing these issues. Furthermore, there are several fusion rules available to combine biometric traits at different levels of fusion.

Keywords
Biometric Introduction, Fusion, Multimodal Biometric System, Biometric Recognition

I. Introduction

Biometric refers to the identification of humans by their characteristics or traits. Computer science, biometrics to be specific, is used as a form of identification and acces control. It is also used to identify individuals in groups that are under surveillance.Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. The two categories of biometric identifiers include physiological and behavioral characteristics.Biometeric would identify by ones voice, DNA, hand print or behavior.Behavioral characteristics are related to the behavior of a person, including but not limited to typing rhythm,gait and voice. A biometric system can operate in the following two modes.In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps involved in person verification.In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card,usernameor ID number (e.g.PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity".

A. Biometric Security System

There are seven Basic criteria for biometric security system

- Universality
- Uniqueness
- Permanence
- Collectability
- Performance
- Acceptability
- Circumvention

1. Universality

This parameter indicates requirements for unique characteristics of each person in the world, which cannot be replicated. For example, retinal and iris are characteristics will satisfy this requirement.

2. Uniqueness

It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users. For instance, the DNA of each person is unique and it is impossible to replicate.

3. Permanence

A permanence parameter is required for every single characteristic or trait, which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will mostly be affected by the age of the user.

4. Collectability

The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification.

5. Performance

It is the next parameter for the system, which outlines how well the security system works. The accuracy and robustness are main factors for the biometric security system. These factors will decide the performance of the biometric security system.

6. Acceptability

The acceptability parameter will choose fields in which biometric technologies are acceptable.

7. Circumvention

Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. DNA is believed to be the most difficult characteristic leading to the failure of the verification process.
A biometric system can operate in the following two modes.In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps involved in person verification.In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smartcard, username or ID number (e.g.PIN) to indicate which template should be used for comparison.'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity"
In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition'

(so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be".The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.Basic criteria for biometric system

II. Multimodal Biometric System

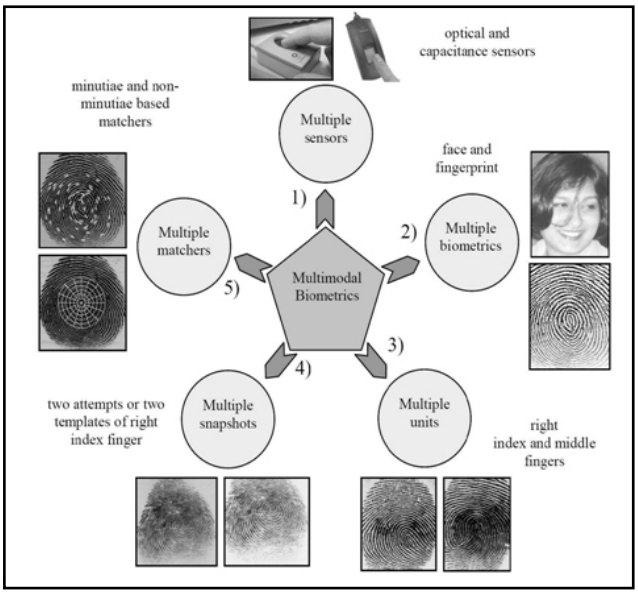


Fig. 1: Multimodal Biometric System

Multimodal biometric fuse the information obtained from different sources to overcome the limitations of unimodal biometric systems. From the point of integration mode, Multimodal Biometric System can operate in one of the different modes: Serial, parallel, hierarchical, pipelining, or sequential approach with reject option. Broadly, the information fusion is divided into three parts:

- Pre-mapping fusion
- Midst-mapping fusion
- Post mapping fusion

In pre-mapping fusion information can be combined at sensor level or feature level. Sensor-level fusion can be mainly organized in three classes:

- Single sensor-multiple instances
- Intra-class multiple- sensors
- Inter–class multiple-sensors

Feature-level fusion can be mainly organized in two categories:
1. intra-class and
2. inter-class.

Intra-class is again classified into four subcategories:
(a). Same sensor-same features,
(b). Same sensor-different features,
(c). Different sensors-same features, and
(d). Different sensors-different features.

A. Performance

The following are used as performance metrics for biometric systems:

1. False Accept Rate or False Match Rate (FAR or FMR)

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs, which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.

2. False Reject Rate or False Non-Match Rate (FRR or FNMR)

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs, which are incorrectly rejected.

3. Receiver or Relative Operating Characteristic (ROC)

The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold, which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

4. Equal Error Rate or Crossover Error Rate (EER or CER)

The rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

5. Failure to Enroll Rate (FTE or FER)

The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

6. Failure to Capture Rate (FTC)

Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

7. Template Capacity

The maximum number of sets of data, which can be stored in the system.

III. Levels of fusion

A Mechanism that can combine the classification results from each biometric channel is called as biometric fusion. We need to design this fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths. Various levels of fusion are: Sensor level, feature level, matching score level and decision level.

A. Sensor Level Fusion

The sensor level fusion can be performed only if the sources are either samples of same biometric trait obtained from multiple compatible sensors or multiple instances of same biometric trait obtained using a single sensor. Since sensor level fusion combines the information from different sensors, it requires some preprocessing such as sensor calibration and data registration before performing the fusing.

B. Feature Level Fusion

In feature-level fusion, the feature sets originating from multiple feature extraction algorithms are consolidated into a single feature set by the application of appropriate feature normalization, transformation and reduction schemes.

The primary benefit of feature-level fusion is the detection of correlated feature values generated by different feature extraction algorithms and, in the process, identifying a salient set of features that can improve recognition accuracy. Eliciting this feature set typically requires the use of dimensionality reduction/selection methods and, therefore, feature-level fusion assumes the availability of a large number of training data. Also, the feature sets being fused are typically expected to reside in commensurate vector space in order to permit the application of a suitable matching technique upon consolidating the feature sets.

C. Matching score level fusion

At this level, the match scores output by multiple experts are combined to generate a new output (a scalar or vector) that can be subsequently used for decision-making. Fusion at this level is the most commonly discussed approach primarily due to the ease of accessing and processing match scores (compared to the raw data or the feature set extracted from the data). Fusion methods at this level can be broadly classified into three categories: density-based schemes (generative approach), classifier-based schemes (discriminative approach) and transformation based Schemes.

D. Rank-Level Fusion

In HCI applications, the output of the system can be viewed as a ranking of plausible hypotheses. In other words, the output indicates the set of possible hypotheses sorted in decreasing order of confidence. The goal of rank level fusion schemes is to consolidate the ranks output by the individual expert systems in order to derive a consensus rank for each hypothesis.

Ranks provide more insight into the decision-making process of the matching compared to just the best hypothesis, but they reveal less information than match scores. However, unlike match scores, the rankings output by multimodal experts are comparable.

E. 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; different levels of fusion are shown in below fig. 2

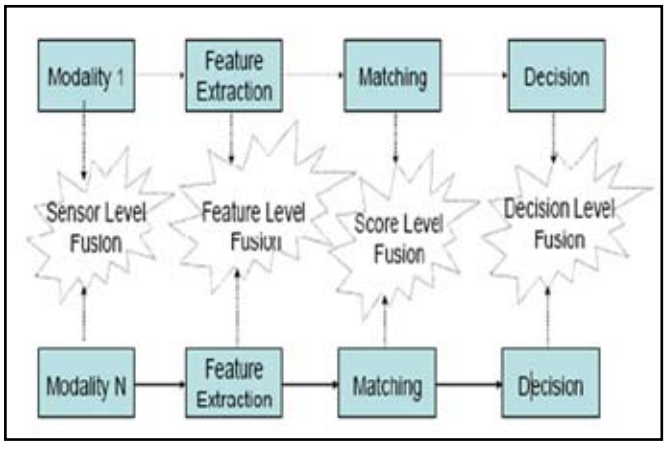


Fig. 2: Fusion at Different Levels

IV. Literature Survey

Beginning from late 90's, the research on multimodal started, and different multimodal biometrics has been developed with combination of various trait, that is, face and finger print, face and iris, iris and finger print etc. The most commonly used biometrics is face, that is, either as a single trait or combined with other trait as multimodal biometrics. Face is most common biometric which is used alone or in combination with other biometrics. In 1998, Hong proposed a bimodal approach and Jain [2] for a Principal Component Analysis (PCA) based face and a minutiae-based fingerprint identification system with a fusion method at the decision level.

In 2000, Frischholz and Dieckmann [3] developed a commercial multimodal approach, BioID. Lip motion and face images were extracted from a video sequence and the voice from an audio signal for verifying the person. Fierrez-Aguilar and Ortega-Garcia (2003) [4] proposed a multimodal approach using face and minutiae-based fingerprint verification system, and an online signature verification system. Face combined with other biometrics at different level of fusion, that is, feature, score and decision (Ross and Jain, 2003). Kumar et al. (2003) [1] presented multimodal personal verification system using hand images by combining hand geometry and palm image at the feature level and match score level. Fusion at the match score level had good performance as compared to unimodal biometric.

In 2004,Toh et al. developed [5] a multimodal biometric system using hand geometry, fingerprint, and voice at match-score-level fusion. Chandran et al. (2009) [7] presented iris and finger print multimodal biometrics to improve the performance. They presented multimodal biometrics using two-lip texture, lip motion and audio and they performed the fusion by reliability weighting summation. Brunelli and Falavigna (2005) [13] presented multimodal face and voice for identification. Kumar et al. (2007) presented multimodal personal verification system using hand images by combining hand geometry and palm image. Directional convolution masks are used to extract the palm futures from normalized palm image,whereas, finger length and width is extracted for hand geometry palm and finally, different level of fusion is performed Chin et al. (2009) [8] integrate palm print and fingerprint at feature level. Series of preprocessing steps are applied on palm and fingerprint to increase efficiency and for feature extraction of 2D.Gabor filter is used and fusion is performed at feature level. Shahin et al. (2008)[6] used three trait, that is, hand veins, hand geometry and fingerprint to provide high security by calculating the ridges, and the direction is calculated in frequency domain.

The approach of applying multiple algorithms to single sample is described in [14]. In [14] three different minutiae based fingerprint matching approaches i.e. Hough transform based matching, String distance based matching and 2D dynamic programming based matching are integrated using a logistic regression transform to reduce False Rejection Rate (FRR) for a given False Acceptance Rate (FAR).

Yao et al. (2007) [12] performed feature level fusion on palm print and face for single sample, and features are extracted using PCA over Gabor filter. Zhou et al. (2007) presented multimodal authentication system using face and fingerprint, and multi route detection is used by using SVM fusion, whereas, the face image with zero turning is used as face template and other face images are used for self learning. Tayal et al. (2009) [11] presented multimodal iris and speech authentication system using decision theory. Iris and speech biometrics are combined using energy compaction and time frequency resolution. Chu et al. (2007) presented multimodal

biometrics using face and palm at score level fusion. Poinsot et al. (2009)[10] presented palm and face multimodal biometrics for small sample size problems and Gabor filter is used for feature extraction of both palm and face images. Veins recognition utilized the vascular patterns, visible with infrared light illumination inside the human body, that is, hand, finger etc. Thus finger veins identification is difficult to falsify.

Yang et al. (2009) presented finger veins recognition by using the feature combination extracted through circular Gabor filter and the feature are exploited on structural, topological and local moments. The segmentation of finger veins was based on multichannel and even the symmetric Gabor filter in spatial domain used eight orientation filters to exploit veins. Information in finger and finger veins image is segmented using threshold. Kang and Park (2009) [9] presented multimodal finger, veins recognition using score level fusing for finger geometry and finger veins. Based on SVM and minutiae point of finger veins, geometric features with sequential deviation are utilized for finger veins and geometry identification, respectively.

V. Design Issues

A variety of factors should be considered when designing a multimodal biometric system. These include, (a). The choice and number of biometric traits, (b). The level in the biometric system at which information provided by multiple traits should be integrated, (c). The methodology adopted to integrate the information, and (d). The cost versus matching performance trade off. The choice and number of biometric traits is largely driven by the nature of the application, theoverhead introduced by multiple traits (computational demandsand cost, for example), and the correlation between the traits considered (uncorrelated information is preferred since the performance improvement is more pronounced in this case). In a cell phone that is equipped with a camera, it might be easier to combine the face and voice traits of a user, while in an ATM application it might be easier to combine the fingerprint and face traits of the user. In identification systems comprising of a large number of users (in the order of millions), an indexing mechanism may be facilitated using a multimodal approach.

VI. Conclusion

Multibiometrics is a new and exciting area of information science research for accurate and reliable personal information representation for matching. This is specifically focused to find a good combination of multiple biometric traits and various fusion methods to get the optimal identification. Biometric fusion is defined broadly as the use of multiple types of biometric data or methods of processing to improve the performance of biometric systems. Fusion works by combining information from multiple sources.

References

[1] A. Ross, A. K. Jain,"Information Fusion in Biometrics", Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.

[2] L. Hong, A. K. Jain,"Integrating faces and fingerprints for personal identification", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 20, No. 12, pp. 1295– 1307, Dec. 1998.

[3] R.Frischholz, U.Dieckmann,"BiolD A multimodal biometric identification system, computer", Vol. 33, No. 2, and pp. 64-68, Feb 2000.

[4] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, J. Gonzalez Rodriguez,"A comparative evaluation of fusion strategies for multimodal biometric verification", in Proc. 4th Int, Conf, Audio-video-based Biometric PersonAuthentication, J. Kittler and M. Nixon, Eds., 2003, Vol. LNCS 2688, pp. 830–837.

[5] K. A. Toh, X. D. Jiang, W. Y. Yau,"Exploiting global and local decisions for multi-modal biometrics verification", IEEE Trans. Signal Process. Vol. 52, No. 10, pp. 3059–3072, Oct. 2004.

[6] Shahin MK, Badawi AM, Rasmy ME,"A Multimodal Hand Vein, Hand Geometry and Fingerprint Prototype Design for High Security Biometrics", CIBEC'08, 2008.

[7] Chandran GC, Rajesh RS,"Performance Analysis of Multimodal Biometric System Authentication", Int. J. Comput. Sci. Network Security, 9: 3, 2009.

[8] Teddy Ko,"Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition", Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05), 2005.

[9] Poinsot A, Yang F, Paindavoine M,"Small Sample Biometric Recognition Based on Palmprint and Face Fusion", Fourth International Multi-Conference on Computing in the Global Information Technology , 2009.

[10] Shahin MK, Badawi AM, Rasmy ME,"A Multimodal Hand Vein, Hand Geometry and Fingerprint Prototype Design for High Security Biometrics", CIBEC'08, 2008.

[11] Chin YJ, Ong TS, Goh MKO, Hiew BY,"Integrating Palmprint and Fingerprint for Identity Verification", Third International Conference on Network and System Security, 2009.

[12] Kang BJ, Park K,"Multimodal Biometric Authentication Based on the Fusion of Finger Veins and Finger Geometry", Optical Eng., 48, 2009.

[13] Poinsot A, Yang F, Paindavoine M.,"Small Sample Biometric Recognition Based on Palmprint and Face Fusion", Fourth International Multi-Conference on Computing in the Global Information Technology, 2009.

[14] Tayal A, Balasubramaniam R, Kumar A, Bhattacharjee A, Saggi M.,"A Multimodal Biometric Authentication System Using Decision Theory", Iris and Speech Recognition, 2nd International Workshop on Nonlinear Dynamics and Synchronization, 2009.

[15] Y.Yao, X. Jing, H. Wong,"Face and palmprint feature level fusion for single sample biometric recognition, Nerocomputing, Vol. 70, No. 7-9, pp. 1582–1586, 2007.

[16] R. Brunelli and D. Falavigna, "Person identification using multiple cues," IEEE Transactions on PAMI, vol. 12, pp. 955–966, Oct 1995.

[17] A. K. Jain, S. Prabhakar, S. Chen,"Combining Multiple Matchers for a High Security Fingerprint Verification System", Pattern Recognition Letters, Vol 20, No. 11-13, pp. 1371-1379, 1999.

ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)



S.Sangeetha received BCA degree in Computer Application from Bharathiyar Univ., Coimbatore, Tamilnadu India in 2008. In 2011 completed MCA degree in Computer Application from Anna Univ., .At present doing M.Phil degree in Bharathiyar Univ., Her areas of interest include Data Mining and Biometric.



Ms.N.Radha has 14 years of teaching experience. Her areas of interest include Network Security and Object Oriented Programming. She is pursuing her doctoral program in the area of Biometric Security. She has presented 4 papers in National Conferences and 3 papers in International Conferences. She has to her credit 6 publications in International Journals. She has attended National and International Seminars, Symposiums, Conferences and Faculty Development Programme. She has guided 9 M.Phil scholars and is currently guiding two M.Phil Scholar.