Review of Multimodal Biometrics: Applications, challenges and Research Areas

Prof. Vijay M. Mane manevijaym@rediffmail.com
Assistant Professor
Department of Electronics Engineering,
Vishwakarma Institute of Technology, Pune (India)

Prof. (Dr.) Dattatray V. Jadhav dvjadhao@yahoo.com
Professor
Department of Electronics Engineering,
Vishwakarma Institute of Technology, Pune (India)

Abstract

Biometric systems for today's high security applications must meet stringent performance requirements. The fusion of multiple biometrics helps to minimize the system error rates. Fusion methods include processing biometric modalities sequentially until an acceptable match is obtained. More sophisticated methods combine scores from separate classifiers for each modality. This paper is an overview of multimodal biometrics, challenges in the progress of multimodal biometrics, the main research areas and its applications to develop the security system for high security areas.

Keywords: Multimodal, biometrics, feature extraction, spoofing.

1. INTRODUCTION

Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity [1]. The increasing demand of enhanced security systems has led to an unprecedented interest in biometric based person authentication system. Biometric systems based on single source of information are called unimodal systems. Although some unimodal systems [2] have got considerable improvement in reliability and accuracy, they often suffer from enrollment problems due to non-universal biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data [3].

Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision. Studies have demonstrated that multimodal biometric systems can achieve better performance compared with unimodal systems.

This paper presents the review of multimodal biometrics. This includes applications, challenges and areas of research in multimodal biometrics. The different fusion techniques of multimodal biometrics have been discussed. The paper is organized as follows. Multi algorithm and multi sample approach is discussed in Section 2 whereas need of multimodal biometrics is illustrated in Section 3, the review of related work, different fusion techniques are presented in Section 4. Applications, challenges and research areas are given in Section 5 and Section 6 respectively. Conclusions are presented in the last section of the paper.

2. MULTI ALGORITHM AND MULTI SAMPLE APPROACH

Multi algorithm approach employs a single biometric sample acquired from single sensor. Two or more different algorithms process this acquired sample. The individual results are combined to obtain an overall recognition result. This approach is attractive, both from an application and research point of view because of use of single sensor reducing data acquisition cost. The 2002 Face Recognition Vendor Test has shown increased performance in 2D face recognition by combining the results of different commercial recognition systems [4]. Gokberk et al. [5] have combined multiple algorithms for 3D face recognition. Xu et al. [6] have also combined different algorithmic approaches for 3D face recognition.

Multi sample or multi instance algorithms use multiple samples of the same biometric. The same algorithm processes each of the samples and the individual results are fused to obtain an overall recognition result. In comparison to the multi algorithm approach, multi sample has advantage that using multiple samples may overcome poor performance due to one sample that has unfortunate properties. Acquiring multiple samples requires either multiple copies of the sensor or the user availability for a longer period of time. Compared to multi algorithm, multi sample seems to require either higher expense for sensors, greater cooperation from the user, or a combination of both. For example, Chang et al. [7] used a multi-sample approach with 2D face images as a baseline against which to compare the performance of multi-sample 2D + 3D face.

3. NEED OF MULTIMODAL BIOMETRICS

Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, voice etc.). These systems are vulnerable to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. It leads to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence [8]. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more reliable due to the presence of multiple, independent biometrics [9]. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a ‘live’ user is indeed present at the point of data acquisition.

4. MULTIMODAL BIOMETRICS

The term “multimodal” is used to combine two or more different biometric sources of a person (like face and fingerprint) sensed by different sensors. Two different properties (like infrared and reflected light of the same biometric source, 3D shape and reflected light of the same source sensed by the same sensor) of the same biometric can also be combined. In orthogonal multimodal biometrics, different biometrics (like face and fingerprint) are involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently. Orthogonal biometrics are processed independently by necessity but when the biometric source is the same and different properties are sensed, then the processing may be independent, but there is at least the potential for gains in performance through collaborative processing. In collaborative multimodal biometrics the processing of one biometric is influenced by the result of another biometric.

A generic biometric system has sensor module to capture the trait, feature extraction module to process the data to extract a feature set that yields compact representation of the trait, classifier module to compare the extracted feature set with reference database to generate matching scores and decision module to determine an identity or validate a claimed identity. In multimodal biometric system information reconciliation can occur at the data or feature level, at the match score level generated by multiple classifiers pertaining to different modalities and at the decision level.

Biometric systems that integrate information at an early stage of processing are believed to be more effective than those which perform integration at a later stage. Since the feature set contains more information about the input biometric data than the matching score or the output decision of a matcher, fusion at the feature level is expected to provide better recognition results. However, fusion at this level is difficult to achieve in practice because the feature sets of the various modalities may not be compatible and most of the commercial biometric systems do not provide access to the feature sets which they use. Fusion at the decision level is considered to be rigid due to the availability of limited information. Thus, fusion at the match score level is usually preferred, as it is relatively easy to access and combine the scores presented by the different modalities [1].

Rukhin and Malioutov [10] proposed fusion based on a minimum distance method for combining rankings from several biometric algorithms. Fusion methods were compared by Kittler et al. [11], Verlinde et al. [12] and Fierrez-Aguilar et al. [13]. Kittler found that the sum rule outperformed many other methods, while Fierrez-Aguilar et al. [13, 14] and Gutschoven and Verlinde [15] designed learning based strategies using support vector machines. Researchers have also investigated the use of quality metrics to further improve the performance [16, 14, 17–21].

Many of these techniques require the scores for different modalities (or classifiers) to be normalized before being fused and develop weights for combining normalized scores. Normalization and quality weighting schemes involve assumptions that limit the applicability of the technique. In [22], Bayesian belief network (BBN) based architecture for biometric fusion applications is proposed. Bayesian networks provide united probabilistic framework for optimal information fusion. Although Bayesian methods have been used in biometrics [16, 23–25], the power and flexibility of the BBN has not been fully exploited.

Brunelli et al. [26] used the face and voice traits of an individual for identification. A Hyper BF network is used to combine the normalized scores of five different classifiers operating on the voice and face feature sets. Bigun et al. [16] developed a statistical framework based on Bayesian statistics to integrate the speech (text dependent) and face data of a user [27]. The estimated biases of each classifier are taken into account during the fusion process. Hong and Jain associate different confidence measures with the individual matchers when integrating the face and fingerprint traits of a user [28]. They also suggest an indexing mechanism wherein face information is used to retrieve a set of possible identities and the fingerprint information is then used to select a single identity. A commercial product called BioID [29] uses the voice, lip motion and face features of a user to verify the identity. Aloysius George used Linear Discriminant analysis (LDA) for face recognition and Directional filter bank (DFB) for fingerprint matching. Based on experimental results, the proposed system reduces FAR down to 0.0000121%, which overcomes the limitation of single biometric system and proves stable personal verification in real-time [30].

5. APPLICATIONS

The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data. A homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification.

Enterprise solutions require the oversight of people, processes and technologies. Network infrastructure has become essential to functions of business, government, and web based business models. Consequently securing access to these systems and ensuring one's identity is essential. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Key application areas include customer verification at physical point of sale, online customer verification etc.

6. CHALLENGES AND RESEARCH AREAS

Based on applications and facts presented in the previous sections, followings are the challenges in designing the multi modal systems. Successful pursuit of these biometric challenges will generate significant advances to improve safety and security in future missions. The sensors used for acquiring the data should show consistency in performance under variety of operational environment. Fundamental understanding of biometric technologies, operational requirements and privacy principles to enable beneficial public debate on where and how biometrics systems should be used, embed privacy functionality into every layer of architecture, protective solutions that meet operational needs, enhance public confidence in biometric technology and safeguard personal information.

Designing biometric sensors, which automatically recognize the operating environment (outdoor / indoor / lighting etc) and communicate with other system components to automatically adjust settings to deliver optimal data, is also the challenging area. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures to enroll [IJBB5].

The multimodal biometric systems can be improved by enhancing matching algorithms, integration of multiple sensors, analysis of the scalability of biometric systems, followed by research on scalability improvements and quality measures to assist decision making in matching process. Open standards for biometric data interchange formats, file formats, applications interfaces, implementation agreements, testing methodology, adoption of standards based solutions, guidelines for auditing biometric systems and records and framework for integration of privacy principles are the possible research areas in the field.

7. CONCLUSIONS

This paper presented the various issues related to multimodal biometric systems. By combining multiple sources of information, the improvement in the performance of biometric system is attained. Various fusion levels and scenarios of multimodal systems are discussed. Fusion at the match score level is the most popular due to the ease in accessing and consolidating matching scores. Performance gain is pronounced when uncorrelated traits are used in a multimodal system. The challenges faced by multimodal biometric system and possible research areas are also discussed in the paper.

8. REFERENCES

1. A. K. Jain, A. Ross and S. Prabhakar, "*An introduction to biometric recognition*". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

2. Chander Kant, Rajender Nath, "Reducing *Process-Time for Fingerprint Identification System*", International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1-9, 2009.

3. A.K. Jain, A. Ross, "*Multibiometric systems*". Communications of the ACM, vol. 47, pp. 34-40, 2004.

4. Phillips, P.J., P. Grother R.J. Michaels, D.M. Blackburn and E. Tabassi and J.M. Bone, "FRVT 2002: overview and summary", March 2003.

5. Gokberk, B., A.A. Salah. and L. Akarun, "Rank-Based Decision Fusion for 3D Shape-Based Face Recognition," LNCS 3546: AVBPA, pp. 1019-1028, July 2005.

6. Xu, C., Y. Wang, T. Tan and L. Quan, Automatic 3D face recognition combining global geometric features with local shape variation information," Aut. Face and Gesture Recog., pp. 308 -313, 2004.

7. Chang, K. I., K. W. Bowyer, and P. J. Flynn, "An evaluation of multi-modal 2D+3D face biometrics," IEEE Trans. on PAMI 27 (4), pp. 619-624, April 2005.

8. A. Ross, A.K. Jain, "*Multimodal Biometrics: An Overview*", 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, pp. 1221- 1224, 9/2004.

9. L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "*Is independence good for combining classifiers?*". in Proceedings of International Conference on Pattern Recognition (ICPR), vol. 2, (Barcelona, Spain), pp. 168–171, 2000.

10. L. Rukhin, I. Malioutov, "*Fusion of biometric algorithms in the recognition problem*". Pattern Recognition Letter, pp. 26, 679–684, 2005.

11. Kittler, "*On combining classifiers*". IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20 (3), pp. 226–239, 1998.

12. P. Verlinde, G. Chollet, M. Acheroy, "*Multimodal identity verification using expert fusion*". Information Fusion, vol. 1 (1), pp. 17-33, 2000.

13. J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, "*Fusion strategies in multimodal biometric verification*". In Proceedings of International Conference on Multimedia and Expo (ICME '03), vol.3(6–9), pp. 5–8, 2003.

14. J. Fierrez-Aguilar, "*Kernel-based multimodal biometric verification using quality signals*". Biometric Technology for Human Identification, Proceedings of the SPIE, vol. 5404, pp. 544–554, 2004.

15. B. Gutschoven, P. Verlinde, "*Multimodal identity verification using support vector machines (SVM)*".Proceedings of the Third International Conference on Information Fusion, vol. 2, pp. 3–8, 2000.

16. J. Bigun, et al., "*Multimodal biometric authentication using quality signals in mobile communications*". Proceedings of IAPR International Conference on Image Analysis and Processing (ICIAP), IEEE CS Press, pp. 2–13, 2003.

17. E. Tabassi, C. Wilson, C. Watson, "*Fingerprint image quality*". Technical Report 7151, 2004.

18. Y. Chen, S. Dass, A.J. Jain, "*Fingerprint quality indices for predicting authentication performance,.* "Fifth International Conference AVBPA Proceedings, Springer Lecture Notes in Computer Science, vol. 3546, pp. 160–170, 2005.

19. L. M. Wein, M. Baveja, "*Using Fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology Program*". Proc. National Academy Science, vol. 102 (21), pp. 7772–7775, 2005.

20. K. Nandakumar, Y. Chen, A.K. Jain, S.C. Dass, "*Quality-based score level fusion in multibiometric systems*". Proceedings of the 18th International Conference on Pattern Recognition (ICPR06), pp. 473–476, 2006.

21. J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzales-Rodriguez, "*Discriminative multimodal biometric authentication based on quality measures*". Pattern Recognition, vol. 38, pp. 777–779, 2005.

22. J.P. Baker, D.E. Maurer, "*Fusion of biometric data with quality estimates via a Bayesian belief network*". Proceedings of the Biometric Symposium, Arlington, VA, pp. 21–22, 2005.

23. J. Richiardi, P. Prodanov, A. Drygajlo, "*A probabilistic measure of modality reliability in speaker verification*". Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP '05, vol. 1, pp. 709–712, 2005.

24. A. B. J. Teoh, S.A. Samad, A. Hussain, "*A face and speech biometric verification system using a simple Bayesian structure*". Journal of Information Science Engineering, vol. 21, pp. 1121–1137, 2005.

25. E.S. Bigun, J. Bigun, B. Duc, S. Fischer, “*Expert conciliation for multimodal person authentication systems by Bayesian statistics*”. J. Bigun, G. Chollet, G. Borgefors (Eds.), First International Conference AVBPA Proceedings, Springer Lecture Notes in Computer Science, vol. 1206, pp. 291–300, 1997.

26. R. Brunelli and D. Falavigna, “*Person identification using multiple cues*”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, pp. 955–966, Oct 1995.

27. E. Bigun, J. Bigun, B. Duc, and S. Fischer, “*Expert conciliation for multimodal person authentication systems using Bayesian Statistics*”. First International Conference on AVBPA, (Crans-Montana, Switzerland), pp. 291–300, March 1997.

28. L. Hong and A. K. Jain, “*Integrating faces and fingerprints for personal identification*”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, pp. 1295–1307, Dec 1998.

29. R. W. Frischholz and U. Dieckmann, “*Bioid: A multimodal biometric identification system*”.IEEE Computer, vol. 33, no. 2, pp. 64–68, 2000.

30. Aloysius George, “*Multi-Modal Biometrics Human Verification using LDA and DFB*”, International Journal of Biometric and Bioinformatics, Vol. 2, Issue 4, pp.1 -10, 2008.