RESEARCH ARTICLE OPEN ACCESS

A Survey on Applications, challenges and Research Areas of Multimodal Biometrics

Mohamed Sadiq. B[1], Dr. Chetana Prakash [2]
1(Department of MCA, Bapuji Institute of Engineering & Technology, and Davanagere
Email: sadiqbmd@gmail.com)
2 (Department of CS&E, Bapuji Institute of Engineering & Technology, and Davanagere
Email: chetana.p.m@gmail.com)

Abstract:

Today biometric recognition is one of the most important techniques for the security. Biometrics uses various physiological or behavioral characteristics. Common physiological biometric measurements include fingerprints, iris, face, hand, retina, signature, speech, rhythm, etc. Biometric technique provides the separate characteristics of a person which is always prevalent. Thus the benefit to a biometric is that it does not change or lose. 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 A Survey on Applications, challenges and Research Areas of Multimodal Biometrics.

Keywords — **Multimodal biometrics, FAR, FRR,Biometric fusion.**

I. INTRODUCTION

Information security and authentication of a person have become an important factor in security systems. Personal Identification Numbers or passwords and key devices such as smart cards are not reliable and accurate techniques in secure environments. Today biometric recognition is one of the most important techniques for the security. Biometrics uses various physiological or behavioral characteristics and it refers to the physiological or behavioral characteristics of a person to authenticate any once identity [1]. 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].

Single biometric systems have limitations like uniqueness, high spoofing rate, high error rate, non-universality and noise. And Acceptance Rate (FAR) and False Rejection Rate (FRR). Multimodal biometric identification system is utilized for solving these limitations. Multimodal biometric is the field of pattern recognition research recognizing the human identity based on physical patterns or behavioral patterns of human. Different biometric features are used by these Biometric systems, where more than one physiological or behavioral trait for identification is used. Multimodal biometric systems are expected to be more reliable due to the presence of multiple pieces of evidence. Biometric fusion is generally placed in terms of both classifications and levels. The classifications define how biometric characteristics are made for fusion and the levels define how the fusion performed.

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.

II. 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 [4]. 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 [5]. 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.

III. RELATED WORKS

Gokberk et al. [6] have combined multiple algorithms for 3D face recognition. Xu et al.[7] have also combined different algorithmic approaches for 3D face recognition. Chang et al. [8] used a multi-sample approach with 2D face images as a baseline against which to compare the performance of multi-sample 2D + 3D face. Chandran et al. [9] 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.

Chin et al. [10] integrate palm print and fingerprint at feature level. Series of preprocessing steps are applied on palm and finger print to increase efficiency and for feature extraction of 2D. Gabor filter is used and fusion is performed at feature level. Shahin et al. [11] 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. Yao et al. [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. [13] 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 re used for self learning. Tayal et al. [14] presented multimodal iris and speech authentication system using decision theory. Iris and speech biometrics are combined using energy compaction and time requency resolution.

Chu et al. [15] presented multimodal biometrics using face and palm at score level fusion. Poinsot et al. [16] 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.

TABLE-1
SHOWS FEW MORE CURRENT WORK ON DIFFERENT TYPES OF MULTI-BIOMETRIC WITH DIFFERENT LEVELS OF FUSION AND THE FUSION STRATEGIES.

Table-1: Work on different types of multi-biometric

Modality	Level of Fusion	Fusion Strategies	Authors
Fingerprint, Palm print, and Hand-Geometry	Feature Level	ANN	Farhat Anwar, et al [24]
Speech, Signature, and Face	Matching Level	Likelihoods Ratio	Yannis Stylianou, et al[25]
Face and	Matching	Voting k- NN	A. Teoh, et al

Speech	Level		[23]
Palmprint and Face	Matching Level	Sum of Score	Nageshkumar , et al [21]
Fingerprint and Hand-Geometry	Combination Approach	Sum, Max, Min Scores	Anil Jain, et al [22]

IV. BASIC BIOMETRIC SYSTEM

A simple biometric system has a sensor module, a feature extraction module and a matching module (Figure 1). Sensor module (Image acquisition): a suitable sensor to acquire the raw biometric data of an individual to be stored in the database. Feature extraction: a suitable algorithm for feature extraction. It may also require enhancement algorithm to improve the quality of acquired image. Database module: which acts as a respiratory of biometric information? People have to enroll before they can use biometric systems. Enrolment involves a copy of a person's biometric feature being taken, converted into a digital format and stored on an electronic database. Matching module: The extracted features are compared against the stored templates to generate match score.

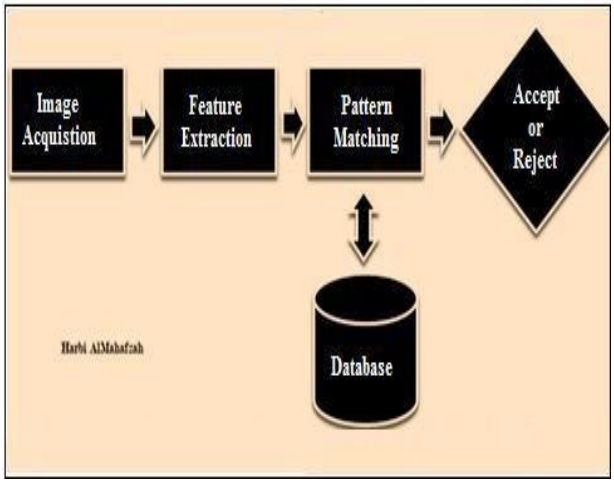

Figure-1: A Basic Biometric System

V. CHARACTERISTICS OF BIOMETRIC

Following are the characteristics of biometric: [17][18]

- Universality: Every person should have the biometric characteristic.
- Uniqueness: No two persons should be the same in terms of the biometric characteristic.
- Permanence: The biometric characteristic should be invariant over time.
- Collectability: The biometric characteristic should be measurable with some (practical) sensing device.
- Acceptability: The particular user population and the public in general should have no (strong) objections to the measuring/collection of the biometric characteristic.
- Performance: Refers to the level of accuracy and speed of recognition of the system given the operational and environmental factors involved.
- Resistance to Circumvention: Refers to the degree of difficulty required to defeat or bypass the system.

VI. ADVANTAGES OF MULTIMODAL BIOMETRIC SYSTEM

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.

The advantages of multimodal biometric systems over unimodal systems are mainly due to utilization of more than one information source. Figure 2 shows a sample multimodal biometric system. The most prominent implications of this are increased and reliable recognition performance, fewer enrolment problems, and enhanced security (Ailon et al, [19]).

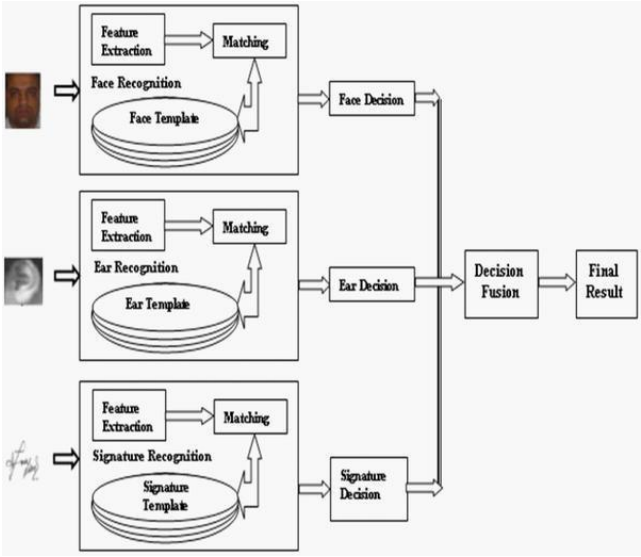

Figure 2. A sample multi-biometric system architecture (Ailon et al, [19]).

VII. APPLICATION

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. The defence 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.

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.

VIII. CHALLENGES AND RESEARCH AREAS

Following 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 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.

IX. CONCLUSIONS

The presented survey paper has addressed 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.

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. *A. Ross, A.K. Jain, "Multimodal Biometrics: An Overview", 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, pp. 1221- 1224, 9/2004.*
5. *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.*
6. *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.*
7. *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.*
8. *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.*
9. *Chandran GC, Rajesh RS (2009). Performance Analysis of Multimodal Biometric System Authentication, Int. J. Comput. Sci. Network Security, 9: 3.*
10. *. Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security.*
11. *Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein, Hand Geometry and Fingerprint Prototype Design for High Security Biometrics, CIBEC'08.*
12. *Yao YF, Jingb XY, Wong HS (2007). Face and palmprint feature level fusion for single sample biometrics recognition, Neurocomputing, 70: 1582-1586.*
13. *Zhou J, Su G, Jiang C, Deng Y, Li C (2007). A face and fingerprint identity authentication system based on multi-route detection, Neurocomputing, 70: 922-931.*
14. *Tayal A, Balasubramaniam R, Kumar A, Bhattacharjee A, Saggi M (2009). A Multimodal Biometric Authentication System Using Decision Theory, Iris and Speach Recognition, 2nd International Workshop on Nonlinear Dynamics and Synchronization.*
15. *Chu R, Liao S, Han Y, Sun Z, Li SZ, Tan T (2007). Fusion of Face and Palm print for Personal Identification Based on Ordinal Features".*
16. *Poinsot A, Yang F, Paindavoine M (2009). Small Sample Biometric Recognition Based on Palmprint and Face Fusion, Fourth International Multi-Conference on Computing in the Global Information Technology.*
17. *A.Ross, K.Nandakumar, and A.K. Jain, "Handbook of Multibiometrics", Springer-Verlag edition, 2006.*
18. *George Chellin Chandra . J, Dr. Rajesh. R.S, "Performance Analysis of Multimodal Biometric System Authentication" International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.*
19. *Ailon, N.,Charikar, M., & Newman, A. (2015). Aggregating inconsistent information: Ranking and clustering. In Proceedings of 37th Annual ACM Symposium on Theory of Computing (STOC), (pp. 684-693). Baltimore, MD: ACM.*
20. *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.*
21. *Nageshkumar.M, Mahesh.PK, and M.N. Shanmukha Swamy, "An Efficient Secure Multimodal Biometric Fusion UsingPalmprintand Face Image", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.*
22. *Anil Jain, Karthik Nandakumara, and Arun Ross, "Score normalization in multimodal biometric systems", Pattern Recognition 38 (2005) 2270–2285, 18 January 2005, www.elsevier.com/locate/patcog.*
23. *Andrew Teoh, S. A. Samad and A. Hussain, "Nearest Neighbourhood Classifiers in a Bimodal Biometric Verification System Fusion Decision", Journal of Research and Practice in Information Technology, Vol. 36, No. 1, February 2004.*
24. *Farhat Anwar, Arafatur Rahman, and Saiful Azad, "Multibiometric Systems Based Verification Technique", European Journal of Scientific Research ISSN 1450-216X Vol.34 No.2 (2009), pp.260-270© EuroJournals Publishing.*

25. *YannisStylianou, YannisPantazis, Felipe Calderero, Pedro Larroy, Francois Severin, SaschaSchimke, Rolando Bonal, Federico Matta, and AthanasiosValsamakis. "GMM-Based Multimodal Biometric Verification", Enterface'05, July18th -August 12th, MONS, Belgium - Final Project Report.*