IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

A Literature Review on Multimodal Biometrics

Sourabh Jain
Students, Department of MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *A Biometric system which relies on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements. Unimodal biometric systems have evolved from many years. But Unimodal biometric system performance has various problems such as noisy data, intra-class variations, confined degrees of freedom, non-uniformity, spoof attacks, uniqueness, diverseness, environmental, physical health, if biometric data is stolen it cannot be changed and hence causing serious security threat etc. so multimodal biometric system has been used to overcome limitations of single (Uni modal) biometrics system. Unimodal biometric systems do not have High security. Iris and fingerprint biometrics are more simple, accurate, and reliable as compared to other available traits [11]. Moreover, fusion of iris and fingerprint is more reliable than fusion of each one with another biometric like face [12].*

Keywords: Multimodal Biometrics, fusion, face, iris, fingerprint, review

I. INTRODUCTION

The unimodal biometric system employs a single biometric trait to identify the user. It is reliable and accurate but it can face with some these problems:

1. Noise in sensed data: Noise and variations in biometric information might make false matches in the database.
2. Non-universality: There are some exceptions, in which an individual is not able to provide a particular biometric.
3. Intra-class variation: The biometric data acquired during verification will not be identical to the data used for generating templates during enrolment for an individual.
4. Inter-class similarities: It refers to the overlap of feature spaces corresponding to multiple individuals.
5. Spoof attacks: biometric systems are vulnerable to spoof attacks.

Best solution to solve such problems is creating multimodal systems which are based on multiple sources of information [22]. The fusion methodologies used in the system are the actual things that reduce spoof attacks by making it difficult to crack the fused data.

System security consists of a few parts like authentication authorization and accountability.[4] Biometrics is the most used approach for the identification of an individual using some behavioral a character such as fingerprint, signature, voice recognition, palm, iris, face recognition, keystroke etc.

Biometrics	Review
Face	It is easy to use but, Face recognition accuracy decline with age.
Fingerprint	Fingerprint remains constant throughout the life and does not change over the time or age.
Iris	According to performance analysis iris gives high performance [2][25]
Ear	Ear is recognized on its outlook. Though it is easy to use, it cannot achieve the best results in security and an individual identity.
Palm	It can be used to achieve higher security, performance, privacy and accuracy than fingerprint since fingerprint can be collected without persons knowledge.
Voice	It improves ease of use and can be used for number of applications. Drawbacks are privacy concern, low accuracy.
Finger vein	It achieves high accuracy and pattern does not change throughout life.

Table 1: comparison of different modalities

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

The Biometric system improved the recognition technique by determining the physiological, and behavioural traits. Physiological characteristics which remain constant lifetime include fingerprint, face, retina, DNA, iris etc. and each of those properties area unit exceptional to each person. Behavioural traits are signature, voice, speech patterns, gait, keystroke etc which amend with time due to age, disease, fractured, accident and several other things affect behaviour. The main purpose of biometrics is to not carry identity cards and other information, and also to improve security as biometrics are personal traits and hence cannot be guessed like passwords. In biometric mode there are two types one is identification another is verification, in identification data is captured through various sensors and in verification, the collected data is evaluated from a database for registered matches. Because of increasing the security gaps and transaction fraud, need for secure identification and personal verification is undoubtable and biometric systems are being the base of secure identification and verification solutions [29] [30]. There are various measuring techniques used for calculating accuracy of the algorithm, these are False Acceptance Rate (FAR), False Rejection Rate (FRR) and Genuine Acceptance Rate (GAR). Less the percentage of FAR, FRR more is the system working accurately.

1.1 Multimodal Biometrics

The performance is measured using following factors: uniqueness, Permanence, Measurability, universality, Performance, Acceptability and Circumvention [1].

Performance

Any biometric system generates 2 styles of scores in matching part viz. A genuine score and an impostor score.

A genuine matching score is generated once 2 feature vectors appreciate a similar individual are compared, and an impostor matching score is generated when featuring vectors from two different individuals are compared. To evaluate the performance of a biometric system following methods are used:

- **False Accept Rate:** FAR gives the percentage of invalid inputs which incorrectly matches with a non-matching template in the database.
- **Genuine Acceptance Rate:** GAR is another metric for FRR used to measure performance of a system.
- False Reject Rate: FRR provides the percentage of valid inputs that area unit incorrectly rejected.
- **Matching Time:** The time used for matching data taken from sensors with database is called matching time. Lesser the match time better is performance [5]. Below is the table 1 which shows FAR and FRR of finger print, face and iris recognition under different thresholding values [5].

Biometric s Method	False Rejection Rate (FRR)	False Acceptance rate (FAR)
Fingerprin t	< 1%	0.1%
Face	<1%	0.1%
Iris	0.00066 %	0.00078%

Table 2: FAR and FRR of finger, face and iris

Thresholding value: It is predefined value decided by the manufacturer. We use score between sensor collected data and the trained data. Higher the score of collected data more are the chances of getting authenticated. If the score is higher than predefined thresholding value then it is accepted otherwise it is rejected.

With this technique implementation if the imposter score is more than threshold value than it may be falsely accepted. So, to overcome this if thresholding value is increased then there are chances of more FRR i.e., genuine users might ger rejected.

1.2 Fusion of Multiple Biometrics

Sensors, feature extraction, matching, decision making are four important modules of biometric system.[23] Multimodal biometric systems can be accomplished at different levels of fusion and achieve higher recognition performance than the unimodal system. Fusion of different types give different results and one can achieve their desired result. Fusion at feature level is more fruitful as it has more information about input trait than other levels of fusion after matching.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Fusion in multimodal biometrics is categorized in two main parts one is fusion before matching and other is fusion after matching [8]. In the first category first data is collected from different sensors and then their result is acquired and after that the fusion is done and, in the end, it is matched with existing data set to check authenticity; examples are Sensor level fusion and feature level fusion. In second category initially after collection of data through different sensors each result is matched with data set and then fusion of multibiometric is done for ex. match score level fusion and decision level fusion are classified as fusion after matching.[2]

- **Sensor level fusion:** Raw data obtained directly from sensors are fused without any feature extraction and represented as a single unit.
- **Feature-level fusion:** In feature-level fusion, Feature vectors are extracted from multiple sensors and they are combined and made as single feature vector and then checked for authentication.
- **Match score level fusion:** In this level of fusion match scores from each trait is calculated and combined to give the resultant score.

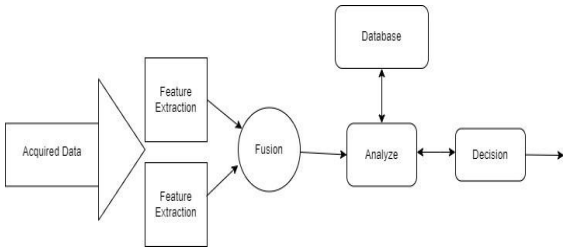

Diagram 1: Algorithms for Match Score Level Fusion

Decision level fusion: fusion is done only after the decision output from each and every biometric is available. Then, the decision from each biometric trait is combined to give the final result. This is the highest level of fusion with respect to human biometrics traits.

Rank Level Fusion: Rank level fusion is basically used for identification more than verification. First, we compare obtained image with database and then do the fusion after that get the ranking, the trained set having lowest ranking is a correct match. Md. Maruf Monwar and Marina L.

Gavrilova carried out rank level fusion with face, signature, and ear biometric traits. They performed experiments with PCA and fisher's LDA.[9] The rank was combined with the highest rank, Borda count, and logistic regression.

Fusion level	Limitations
Sensor level	The noise goes as it is into matching hence low efficiency
Feature level	Uncertainty between incompatible biometrics increase complexity
Match Score level	There are no homogenous scores obtained from various matchers. It is not necessary that the scores obtained should be within the same scope. It is important to apply normalization schemes
Decision level	Decision from each biometrics sensor is collected before fusing them. More or less acts like unimodal system

Table 2: Comparison and limitations of different fusion levels

Techniques Issues: One basic issue is an information fusion system to detect the type of information that should be fused by fusion modal. In raw data not containing the true biometric signal of an individual but also corrupted by various types of noise developing efficient matching algorithms is often the most important and thus fusion at sensor or feature levels introduce additional processing complexities.[35][36] Another challenge could be the sensors used for fusion should perform accurately in different environmental conditions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Biometric Identifiers	Year and Authors	Fusion Level and Approach
Face, Ear, Signature	Md. Maruf Monwar et al.	Rank, Logical regression
Signature, Voice	Gracia – salicetti et al.	Match Score
Fingerprint	Nandakumar et al.	Match score
Face + fingerprint	Sheetal Chaudhary &RajenderNath [33]	Match score (Multiple support vectors)
Face, fingerprint, iris	2014	Gabor and FOCC
3D ear, face	2013	PCA to the nearest
Hand- geometry, finger, palm, print	2003	Match score level fusion
Fingerprint, face, speech	1999	Cryptographic algorithm
Ecg, sound	bugdol, and mitas (2014)	feature level
Iris, palmprint	hariprasath. et.al (2012)	feature level
finger vein+hand vein	trabelsi et al (2013)	match score
Face + iris	Mansoura [32]	Score level (FFT, SVD)

Table 3: Different existing multimodal biometrics systems

II. REVIEW CRITERIA

1. Ajay kumar and Sumit Shekhar suggested combination of multiple palmprint representations to achieve improvement in the performance with compare to individual performance [10].
2. Dua et al. [37] suggested a feed- forward architecture and uses a k- means clustering algorithm to distinguish iris patterns.
3. Minaee et al. [38] came up with a Face Recognition System based on Scattering Transform technique for feature extraction, and SVM for classification. Scale invariant scattered features can be used to improve inaccuracy which is missing in this system.

2.1 Applications

The biometric uses in various sectors such as commercial application, government application, forensic application, border management, civil application, customer verification point of sale enterprisesolution require oversight of people, processes and technologies. securing access to these systems and ensuring one's identity is essential [28] [26], [27]. Multiple biometrics are used to prevent stealing of possessions that mark the authorised person's identity for example licences or properties and to prevent fraud act like fake id badges, or licence to ensure safety and security**.** Multimodal biometrics reduce the security threat to a large extent as it is very hard to crack fused data. This marks to be its most significant application.

III. CONCLUSION

[1]. A research-based review is performed on a multimodal biometric authentication system. The main Objectives of this research paper is to write comparative study of different biometrics and results achieved by them. And also write reviews given by previous authors. The methods used in biometrics performances measurement like FAR, FRR, GAR are discussed in the paper. Finally fusion of different modalities is discussed.

[2]. In most of the cases best results are achieved by palmprint, fingerprint and iris. Though it still needs some improvement like multiple combinations of single modality [10]. From above survey we also conclude that most of the existing systems have conventional methods for feature extraction which leads to loss of data or inaccuracy. To improve accuracy use of advanced methodologies is required ex. Neural network for classification, convolutional neural network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

REFERENCES

[1]. Islam, S.M.S., R. Davies, M. Bennamoun, R.A. Owens and A.S. Mian, 2013. Multibiometric human recognition using 3D Technology features. Pattern Recogn., 46(3): 613-627

[2]. S. Aruna Irani, R. Gobinath "Literature review on multimodal Biometrics" International Journal of Engineering & Technology, 7 (2.26) (2018) 31-34

[3]. e, M., S.J. Horng, P. Fan, R.S. Run, R.J. Chen, J.L. Lai, M.K. Khan and K.O. Sentosa, 2010. Performance evaluation of score level fusion in multimodal biometric systems.

[4]. Ashish Mishra, "Multimodal Biometrics it is: Need for Future Systems" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.4, June 2010

[5]. Deepakkumar Verma, "Performance analysis of biometrics systems: A security perspective" International Journal of Advanced Research in Computer and Communication Engineering Vol. 8, Issue 4, April 2019

[6]. S. Aruna Irani, R. Gobinath "Literature review on multimodal Biometrics" International Journal of Engineering & Technology, 7 (2.26) (2018) 31-34

[7]. Divyakant T. Meva, C. K. Kumbharana "Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication" International Journal of Computer Applications (0975 – 8887) Volume 66– No.19, March 2013

[8]. Anil Jain, Karthik Nandakumar, Arun Ross, Score Normalization in Multimodal Biometric Systems, Pattern Recognition, 2005

[9]. Md. Maruf Monwar, Marina L. Gavrilova, Multimodal Biometric System Using Rank-Level Fusion Approach, IEEE Transactions on Systems, Man and Cybernatics – half B: Cybernatics, Vol. 39, No. 4, August 2009, pp. 867-878

[10]. Ajay Kumar, Sumit Shekhar, Personal Identification Using Multibiometrics Rank-Level Fusion, IEEE Transactions on Systems, Man and Cybernatics- Part C: Applications and reviews

[11]. Houda Benaliouche and Mohamed Touahria "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint" Hindawi Publishing Corporation The Scientific World Journal Volume 2014, Article ID 829369, 13 pages http://dx.doi.org/10.1155/2014/8293 69

[12]. M. Abdolahi, M. Mohamadi, and M. Jafari, "Multimodal biometric framework combination utilizing unique mark and iris with fluffy rationale," International Journal of Soft Computing and Engineering, vol. 2, no. 6, pp. 504– 510, 2013.

[13]. M. Abdolahi, M. Mohamadi, and M. Jafari, "Multimodal biometric framework combination exploitation finger impression and iris with formal rationale," International Journal of Computing and Engineering, vol. 2, no. 6, pp. 504– 510, 2013.

[14]. Aarohi Vora, Chirag Paunwala, Mita Paunwala, "Improved Weight Assignment Approach for Multimodal Fusion", IEEE International Conference on Circuits, Systems, Communication and Information Technology Applications, CSCITA, pp.70- 74, April2014.

[15]. A. Kumar, D. C. M. Wong, H. C.Shen1, and A. K. Jain, — Personal verification using palmprint and hand geometry biometric,‖in Proc. 4th Int. Conf. Audio- Video-Based Biometric Person Authentication , J. Kittler and M Nixon, Eds., 2003 vol. LNCS 2688, pp 668–678

[16]. Aarohi Vora, Chirag Paunwala, Mita Paunwala, "Nonlinear SVM Fusion of Multimodal Biometric System", International Multi Con-ference on Innovations in Engineering and Technology, IMCIET 2014 under International Conference on Communication and Com-puting track, ICCC 2014, Elsevier, pp. 30- 35, August 2014.

[17]. A. Jain, K. Nandakumar, A. Ross, "Score Normalization in Multimodal Biometric Systems", Pattern Recognition, vol. 38, no.12, pp. 2270-2285, December 2005.

[18]. Arun Ross, Anil Jain, "Information fusion in biometrics", Pattern Recognition Letters, Elsevier, vol. 24, no.13, pp. 2115- 2125, Sep-tember 2003.

[19]. Poinsot A, Yang F, Paindavoine M (2009). Small Sample Biometric Recognition Based on Palmprint and Face Fusion, Fourth International MultiConference on Computing in Global Information Technology.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

[20]. Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein, Hand Geometry and Fingerprint Prototype Design for High Security Biometrics, CIVIC 08.

[21]. Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Coordinating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security.

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

[23]. F. Perron, J. L. Dugelay, "Introduction it la Biometric Authentification", des Individus par Traitement Audio-Video, Traitement du SignalVolume 19, pp 253-265, 2002.

[24]. Mehdi Ghayoumi "A review of multimodal biometrics system: fusion methods and their applications".

[25]. Mohammad Al Rousan and Benedetto Intrigila "A Comparative Analysis of Biometrics Types: Literature Review" Journal of Computer Science.

[26]. C.Sanderson, K Kuldip,"Multi-modular individual confirmation framework in view of face profiles and discourse", Signal Processing and Its Applications, ISSPA ,1999.

[27]. R.Frischholz, U. Dieckman. "A Multimodal Biometric Identification System", IEEE Computer, 33(2): pp. 64-68, 2000.

[28]. K.Nandakumar, Y.Chen, S.C.Dass, and A.K.Jain,"Likelihood ratio based biometric score fusion", IEEE Trans. Pattern Anal. Machine Intelligence 30, 2, pp.342-347, 2008.

[29]. A. K. Jain, A. Ross, and S. P, "An introduction to biometric recognition," IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4-20.

[30]. L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?," in Proc. of Int'l Conf. on Pattern Recognition (ICPR), vol. 2, pp. 168-171, 2000.

[31]. Agarwal R., Singh Jalal A., and Arya K. V., "A multimodal liveness detection using statistical texture features and spatial analysis," Multimedia Tools and Applications, vol. 79, no. 11, pp. 1-25, Jan. 2020, doi: 10.1007/s11042-019-08313-6

[32]. Mansoura L., Noureddine A., Assas O., and Yassine A., "Biometric recognition by multimodal face and iris using FFT and SVD methods With Adaptive Score Normalization," 2019 4th World Conference on Complex Systems (WCCS), 2019, pp. 1-5, doi: 10.1109/ICoCS.2019.8930748.

[33]. Chaudhary S. and furthermore, Nath R., "A strong multimodal biometric framework coordinating iris, face and unique mark utilizing different SVMs," International Journal of Advanced Research in Computer Science, vol. .7, no. 2, 2016, doi:10.26483/ijarcs.v7i2.2647.

[34]. Kabir W., Ahmad M. O., and Swamy M. N., "A multi-biometric system based on feature and score level fusions," IEEE Access, vol. 7, pp. 59437-59450, 2019, doi: 10.1109/ACCESS.2019.2914992.

[35]. K.Nandakumar, Y.Chen, S.C.Dass, and A.K.Jain,"Likelihood ratio based biometric score fusion", IEEE Trans. Pattern Anal. Machine Intelligence 30, 2, pp.342-347, 2008.

[36]. A.A.Ross, K.Nandakumar, and A.K.Jain," Handbook of Multibiometrics", (Springer Publisher), International Series on Biometrics, Vol. 6, 2006.

[37]. Dua M., Gupta R., Khari M., and Crespo R. G., "Biometric iris recognition using radial basis function neural network," Soft Computing, vol. 23, no. 22, pp. 11801-11815, 2019, doi: 10.1007/s00500-018-03731-4.

[38]. Minaee S., Abdolrashidi A., and Wang Y., "Face recognition using scattering convolutional network," 2017 IEEE signal processing in medicine and biology symposium (SPMB), 2017 Dec 2, pp. 1-6, doi: 10.1109/SPMB.2017.8257025.