WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey On Multimodal Authentication System With Gender Classification

U. Chaitanya[1], B Nikitha[2], Ashwapuram Arshith Madhav[3], Buragadda Hariprasad Goud[4]

[1,2,3,4]Department of Information Technology, Mahatma Gandhi Institute of Technology, Hyderabad-7, India

uchaitanya_it@mgit.ac.in[1], bnikitha_it201207@mgit.ac.in[2], aarshithmadhav_it201205@mgit.ac.in[3], bhariprasadgoud_it215a1202@mgit.ac.in[4]

ABSTRACT

Biometric authentication is a method which takes the users biological traits as input and identifies whether the user is a authenticated person or not. In this process we take various biological characteristics, including fingerprints, voice patterns, retinas, and facial features. The unimodal biometric system takes only one biometric trait of the user in order to see whether the person is authenticated person or not. Whereas in multimodal biometric we take two or more than two biometric traits of the person to check whether the person is authenticated person or not. The main aim of using the multimodal biometric system over the unimodal biometric system is to enhance the accuracy of identification and enhance the security. Gender classification using multimodal biometrics involves in classifying the gender of the person by combining the multiple biometric traits of the person. By combining the multiple biometric traits of the person the gender identification becomes easier and the output obtained can be more accurate. The approach for combining the multiple biometric traits integrates various traits like facial features, iris, and fingerprints. By making the fusion of these biometric traits using any robust algorithm we can over the limitations of the unimodal biometric system. By using these fusion algorithms it results in improved gender classification performance. The combination of this various biometric traits like facial features, iris and fingerprint has a very effective and accurate approach for the gender classification which can applied for the various applications and security systems.

Keywords-Unimodal, Multimodal, Authentication, Gender Classification, Fusion.

INTRODUCTION

Biometric authentication is very effective in identity verification using the biological or the behavioural traits of the person. This also used to enhance the security in the various applications. The multimodal biometric authentication is more secure, convenient and personalized approach than the unimodal biometric. In the olden days one used the various traditional methods like passwords or PINs which can hacked easily. For the biometric authentication we can use the various biometric traits like facial features, iris, finger prints, voice patterns, etc. These biometric characteristics can be captured from the sensors, web cameras and then converted into digital templates and can be stored for the comparison at the time of authentication. One of the main advantage of the biometric authentication is that it doesn't allow unauthorized access since forging one's biometric trait is very challenging. This can be one of the solution for securing sensitive data, physical access points, and digital devices. Biometric systems are widely used in smartphones, laptops, and access control systems, transforming the way individuals interact with technology. While offering high security, biometric authentication also makes the user experience easy by eliminating the need to remember complex passwords. As the technology gets growing many challenges like privacy concerns, potential data breaches can be seen. The adoption of the biometric system is growing across the various places like finance, healthcare, and government. Biometric system can be used for the user friendly identification and for security purposes.

The biometric authentication can be divided into two main types namely unimodal biometrics and multimodal biometrics. Both having their own advantages and disadvantages. In unimodal biometric authentication. we use only single biometric trait. In the unimodal biometric we commonly use the biometric traits like fingerprint, facial recognition, iris or voice. These traits are used for authenticating the person uniquely. They are simple to understand and apply but they have their own advantages and disadvantages. The disadvantages may include the challenges related to accuracy or the high false positives and negatives. Whereas, in multimodal biometric we use more than one biometric traits or combination of two or more biometric traits for the authentication. Moreover, the multimodal biometric approach me those drawbacks in order to enhance system reliability. We can consider the example like a combination of fingerprint and facial recognition or iris gives you more accurate and reliable biometric system compared to that of the single biometric like finger , face and iris separately. The main advantage of multimodal systems is that it has more accuracy and recognition rate compared to that of the unimodal system. These multimodal biometric system are highly advantageous since it has high security

and can authenticate the person more accurately in any applications. To implement the multimodal biometric system we need more recourses compared to of we required for the unimodal biometric system. The
unimodal biometric authentication is more simple and more straightforward, multimodal systems has a higher level of security and accuracy which strengths the modalities of multiple biometric. The choice between the two depends on the specific requirements and the desired level of security for a given application. Gender classification using multimodal biometrics involves the using of multiple biometric of the person in order to identify the gender of a person. In the previous gender classification mainly depend on unimodal features like facial features, voice characteristics. Multimodal biometric authentication and gender classification aim to address the limitations of unimodal approaches, by offering a more reliable and accurate solution. By integrating various biometric modalities, the system can account for variations in individual characteristics and mitigate the impact of environmental factors that might affect a single modality.
Applications for gender classification using multimodal biometrics can be used around various domains, including security, access control, and demographic analysis. Security systems can utilize this technology for the person identification processes, while marketing research may use it for demographic profiling.

LITERATURE SURVEY

In [9], authors used the unimodal biometric trait for the age and gender classification. They used the iris for the gender and age detection. A dataset comprising 1,716 images from the left and right irises of 190 subjects was collected. 570 left irises were uniformly resized to dimensions of 250 by 250 pixels. Among these, 342 images were employed for the training phase, while the remaining 228 were designated for testing purposes. The images underwent pre-processing, including segmentation, filtering, and normalization through Daugman's rubber sheet model[9]. Feature extraction from iris images was accomplished through the utilization of pre-trained deep learning networks. For iris recognition, the process involves passing through image acquisition, segmentation techniques, and normalization techniques to generate a template used for measuring the biometric system.
The system's performance was evaluated using metrics like Accuracy, Precision, and Recall. Among these metrics, the age group of 20-24 demonstrated the most favourable outcomes across all parameters, owing to the ample data available for training the system within that age range. The findings indicate that increased data used for training correlates with enhanced system performance. Moreover, regarding gender prediction, noteworthy discrepancies were observed in performance metrics with higher threshold values. Optimal results were achieved when the threshold value reached 0.75, as it consistently yielded the best outcomes across all metrics.
In [10,11,13], the authors defined about the multimodal biometric traits for the authentication, age and gender classification. In et al. [10], the authors have used the multimodal biometric traits like face, iris and fingerprints for the gender classification. The classifiers employed include Linear Discriminant Analysis, K-Nearest Neighbour classifier, and Support Vector Machine. Notably, the Support Vector Machine (SVM) classifier achieved the maximum accuracy of 99.8%, while the minimum accuracy of 91.4% was recorded with Linear Discriminant Analysis. In [15], the authors have used the ear and face profile images for the age and gender classification. In this they have used the various fusion methods like data fusion, feature fusion, score fusion. The various datasets that has been used are UND-F, UNDJ2, and FERET datasets for gender and age classification [13].
In [12], the authors have behavioural biometrics like the handwritten signatures for the gender classification. The system consists of the various steps like dataset collection, data pre-processing, feature extraction, and classification. Despite prior research achieving promising results in gender classification, there remains significant potential for the development of a more robust algorithm with effective discriminatory features. This study explores feature-level fusion of Local Binary Pattern (LBP), Histogram of Oriented Gradients (HOG), Statistical, and Textural features using a dataset of 4,790 high-quality signature images (250 males and 229 females). The proposed algorithm demonstrates high accuracies, achieving 96.17% for k-NN, 98.72% for Decision Tree, and 100% for Support Vector Machine. These findings highlight the algorithm's effectiveness in gender classification, indicating its potential for real-world applications.
In [11] the paper introduces a resilient multimodal gender identification approach leveraging deep features computed through an off-the-shelf pretrained deep convolutional neural network architecture. This architecture is specifically based on the AlexNet. In this the model consists of the 20 consecutive layers, each layer encompassing varying window sizes of convolutional layers, which is followed by connected layers for the high feature extraction and classification. Various experiments were being carried out on the SDUMLA-HMT multimodal database which has 15,052 images, efficacy of the proposed methodology. The confusion matrix of different features on SDUMLA HMT database is carried out using various algorithms. The various algorithms used are Naïve Bayes, KNN City block, KNN Euclidean, SVM, Decision Tree. The average accuracy is calculated for all the classifiers and compared with each to identify the classifier with the highest accuracy. The deep convolution method is used and only 99.9% of accuracy on the SDUMLAHMT multimodal biometric database is achieved.

CONCLUSION

The implementation of a multimodal biometric authentication system, integrating face, iris, and fingerprint fusion, coupled with gender classification, signifies a robust and comprehensive approach to enhance security protocols. This amalgamation of diverse biometric modalities not

only ensures the authentication but also it makes sure of high degree of accuracy and reliability. The fusion of facial, iris, and fingerprint recognition, alongside gender classification, creates a multifaceted authentication model that excels in both precision and inclusivity.

This innovative solution not only mitigates the vulnerabilities associated with single modal systems but also sets the stage for advanced and adaptive security measures in the ever evolving landscape of biometric technology.

REFERENCES

[1] Abhijit Patil, Kruthi R, Shivanand Gornale, Analysis of Multi-modal Biometrics System for Gender Classification Using Face, Iris and Fingerprint Images, I.J.Image, Graphics and Signal Processing, 2019.

[2] Faluyi Bamidele Ibitayo, Ojo Olufemi Ariyo, Atobatele Oluwatobi O, Development Of Iris Based Age And Gender Detection System, International Journal of Progressive Sciences and Technologies (IJPSAT), 2022.

[3] S. S. Gornale, Abhijit Patil and Veersheety C, Fingerprint Based Gender Identification Using DWT and Gabor Filters, International Journal of Computer Oct-2020.

[4] Na Rae Baek, Se Woon Cho, Ja Hyung Koo, Noi Quang Truong, And Kang Ryoung Park, Multimodal Camera-based Gender Recognition Using Human-body Image with Two- step Reconstruction Network, IEEE Access 2019.

[5] Chunyu Zhang ,Hui Ding , Yuanyuan Shang , Zhuhong Shao, and Xiaoyan Fu1, Gender Classification Based on Multiscale Facial Fusion Feature, Hindawi, 2018.

[6] Vidhya Keren T, Serin J, Mary Ivy Deepa I S, V.Ebenezer, A.Jenefa, Gender Classification from Fingerprint Using Hybrid CNN-SVM, Journal of Artificial Intelligence and Technology (2023).

[7] K. S. Arun and K. S. Sarath, A machine learning approach for fingerprint based gender identification, Biometric Recognition CCBR 2011.

[8] Wenyao Xu, Xi Long, Yan Zhuang, Feng Lin, Human gender classification: a review, International Journal of Biometrics January 2016.

[9] Dogucan Yaman, Fevziye Irem Eyiokur, Hazım Kemal Ekenel, Multimodal Age and Gender Classification Using Ear and Profile Face Images, IEEE Xplore, 2019.

[10] Vidhya Keren T, Serin J, Mary Ivy Deepa I S, V Ebenezer, A Jenefa, Gender Classification from Fingerprint Using Hybrid CNN-SVM, Journal of Artificial Intelligence and Technology (2023).

[11] Faluyi Bamidele Ibitayo, Ojo Olufemi Ariyo, Atobatele Oluwatobi O, Development Of Iris Based Age And Gender Detection System, International Journal of Progressive Sciences and Technologies (IJPSAT) August 2022.

[12] Shivanand S. Gornale, Sathish Kumar, Abhi Patil and Prakash S. Hiremath, Behavioral Biometric Data Analysis for Gender Classification Using Feature Fusion and Machine Learning, Frontiers in Robotics and AI, published: 07 May 2021.

[13] SaiHomitha Nookala, Vasavi Balabhadra, Bhavana Mareedu, Suneetha Bulla ,Gender Classification Using a Convolutional Neural Network (CNN), Research square 2024.