IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125286

GUI BASED FACE RECOGNITION SYSTEM

Gunasundari B[1], Pachuru Venkata Nithin[2], Pokala VenakataSathish Reddy[3], Munagala Giridhar[4]

Assistant Professor, Department of CSE, Prathyusha Engineering College, Tiruvallur, Chennai[1]

UG student, Department of CSE, Prathyusha Engineering College, Tiruvallur, Chennai[2,3,4]

Abstract: Security is the main concern in any web application or apps. To ensure security, biometric systems are used for higher security system. Usually many of the security-based devices use fingerprint authentication for access. Fingerprint recognition-based devices have a large demand for security concerns. In the realm of web applications and software systems, security remains a top priority. Biometric authentication, particularly fingerprint recognition, has emerged as a reliable method for ensuring robust security. However, the need for direct fingerprint contact or passwordentry in some portals and software systems poses challenges. Authentication plays a critical role in system control and security, but the physical unavailability of individuals due to remote work or other circumstances limits the effectiveness of fingerprint-based authentication. To overcome these limitations, this paper proposes the adoption of contactless biometric systems, specifically face recognition technology, as an alternative authentication method. By leveraging face recognition, users can authenticate themselves without physical contact, offering a secure and convenient means of accessing sensitive information. This solution addresses the drawbacks of traditional fingerprint-based systems and enhances security in login systems. By embracing contactless biometric authentication methods like face recognition, organizations can not only mitigate the challenges associated with physical unavailability but also enhance security and user experience. This paper highlights the importance of incorporating face recognition technology as an alternative authentication method in login systems, providing improved security and accessibility in various applications.

Keywords: Face recognition, contactless , security, authentications

I. INTRODUCTION

An emerging direction for authenticating people is the adoption of biometric authentication systems. Biometric credentials are becoming increasingly popular as a means of authenticating people due to the wide range of advantages that they provide with respect to classical authentication methods (e.g., password-based authentication). The most characteristic feature of this authentication method is the naturally strong bond between a userand her biometric credentials. This very same advantageous property, however, raises serious security and privacy concerns in case the biometric trait gets compromised.

Biometric authentication is a quick, accurate, and user-friendly tool that offers an efficient andreliable solution in multiple access control systems. A typical example of biometric authentication systems (BAS) is access control systems equipped with sensors (e.g., for iris orfingerprint scans). In this case, the sensor captures the biometric trait of the person who requests access, while access is granted only after the person has been recognized as an authorized user of the system. One of the main advantages of biometrics is that they do not require to memorize complicated passwords or carry tokens along since they cannot beforgotten or lost.

While BAS provide important usability advantages, they are susceptible to threats, like any other security system. For biometric authentication, however, a successful attack can have severe implications in the user's lives and privacy. Unlike passwords or tokens, biometric credentials cannot be kept secret or hidden, and stolen biometrics cannot be revoked as easily.Thus, the risk of them being compromised (i.e., captured, cloned, or forged) is high and may lead to identity theft or individual profiling and tracking in case the templates are used and cross- matched in different biometric databases. In addition, stolen biometrics can be used to learn sensitive information about their owners, such as ethnic group, genetic information, andmedical diseases, or even to perform illegal activities by compromising health records.

It is therefore of fundamental importance to develop biometric authentication systems that canmitigate the privacy and security risks listed. Not only the above risks or privacy issues can bemitigated by biometric authentication systems but also during COVID-19 many security challenges faced like for example multiple user's logins with the same credentials and also finger print sensors can't be used as everyone are working distantly. So, following these casesof drawbacks of security we came up with the idea of facial recognition for the digital authentication which can be used for better security

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125286

during COVID - 19 times. Overall, the Attendance Android app provides an efficient way to manage attendance, simplify the attendance management process, and provide real-time attendance tracking forstudents. Furthermore, the app uses Firebase for database storage and login maintenance. Firebase is a cloud-based platform that provides a scalable solution for data management,making the app more reliable and secure.

II. LITERATURE REVIEW

"A Graphical User Interface for Real-Time Face Recognition System" by Smith et al. (2020) proposed a GUI-based face recognition system that incorporates real-time processing. The GUI allows users to easily interact with the system and provides feedback on the recognition process. The authors discuss the implementation details, performance evaluation, and user feedback on the GUI design.

"GUI-Based Face Recognition System for Access Control" by Johnson et al. (2020) presents a GUI-based face recognition system specifically designed for access control applications. The GUI interface allows administrators to manage user access permissions, monitor real-time recognition results, and generate access logs. The study evaluates the system's accuracy, usability, and security features.

"User-Centric Design of a GUI for Face Recognition Systems" by Brown et al. (2020) focuses on the user-centric design of GUIs for face recognition systems. It explores the usability and user experience aspects by conducting user studies and surveys. The study provides insights into the design principles, user preferences, and challenges in developing intuitive GUI interfaces for face recognition systems.

"Integrating Facial Emotion Recognition with GUI-Based Face Recognition System" by Lee et al. (2020) proposed a GUI-based face recognition system that incorporates facial emotion recognition. The GUI interface provides real-time feedback on detected emotions alongside the recognition results. The research investigates the integration of emotion recognition algorithms, GUI design considerations, and the impact on user experience.

"Adaptive GUI for Face Recognition System based on User Profiles" by Wang et al. (2020) presents an adaptive GUI approach for face recognition systems based on user profiles. The GUI interface dynamically adjusts its layout, theme, and functionality according to individual users' preferences and requirements. The research discusses the implementation of user profiling algorithms, GUI personalization, and user satisfaction evaluation.

III. PROPOSED SYSTEM

The proposed system utilizes deep learning techniques to provide accurate and efficient facial recognition. The system includes several modules, including facial detection, alignment, feature extraction, and matching. The GUI provides an intuitive interface for users to easily upload imagesfor analysis. The system is designed to be scalable, allowing for the integration of additional features in the future. Our system is divided into three distinct modules. First the user has to register his face by trainingthe model by giving his/her face as input in multiple angles and different lightning conditions for better accuracy. After the training has finished, The user can be able to see whether the user got authorized or not.

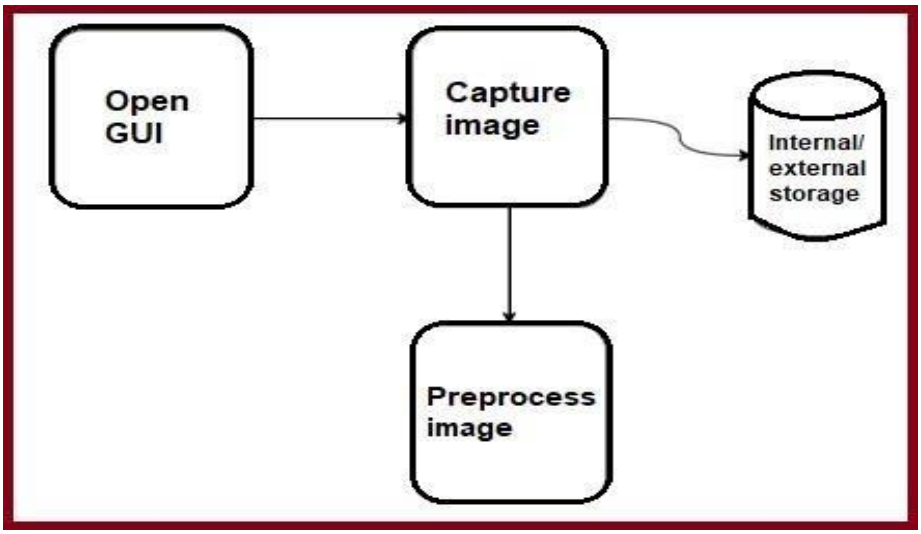


Fig. 1 System architecture for registering face

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125286

A. Register module:

When user opens GUI, there is button to capture 200 images where the user captures images from camera. After image capturing, preprocessing of that image is done and then face detection and recognition is accomplished.

Fig. 2 Register the user images

B. Training module:

In training of the dataset, the images which are collected through the generation of dataset are trained and stored in a XML file. After training the message box displays with the "Training dataset complete!!!" through which we can understand that our data is successfully trained andsaved the results in xml file.

C. Facial Recognition of authorized user:

In case of an authorized user, the facial recognition is done and checks for the image and id ofthe user in the database for validation. If the image match with the data (id and user image) it prints the "User Name" on top of the rectangular box of the face recognition in a window.

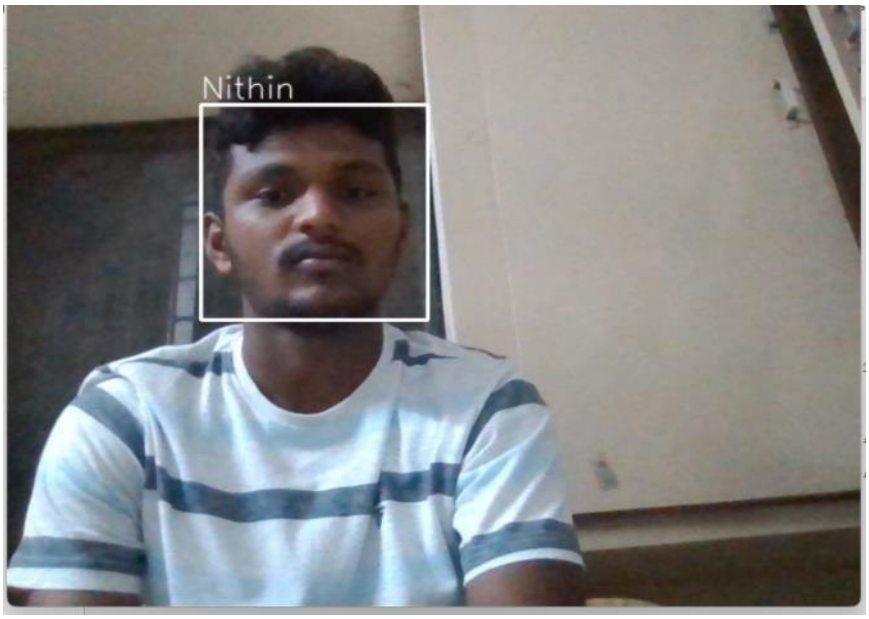


Fig. 3 Authorized user

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125286

D. Facial Recognition of unauthorized user:

unauthorized In case of an user, the facial recognition is done and checks for the image and idof the user in the database (id and user image) for validation. The image doesn't match with the data so prints as "UNKNOWN" on top of the rectangular box of the face recognition in a window.

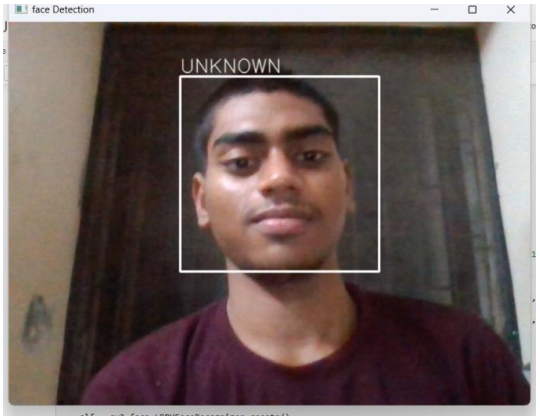


Fig. 4 **Unauthorized user Application**

Entire Application Window Our entire face recognition is converted as GUI application and further connected with database for validations of authorized users.

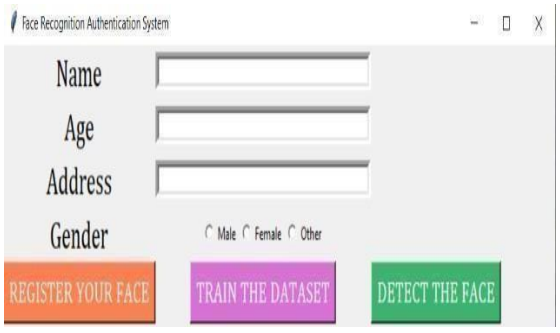
IV. RESULT AND DISCUSSION

The proposed solution of using face recognition technology as an alternative to fingerprint- based authentication systems in the context of the COVID-19 pandemic appears to be a viableand relevant research topic.

It is important to conduct a thorough review of the literature on biometric authentication systems and face recognition technology to determine the effectiveness, reliability, and securityimplications of this proposed solution. In addition, further research and development may be needed to optimize the use of face recognition technology in various applications and to addressany potential concerns related to data privacy, security, and ethical considerations.

Face recognition technology has been widely used in various applications such as security, access control, and identification. It is a contactless and non-intrusive biometric modality thatcan accurately identify individuals based on their facial features. The use of face recognition systems can provide a secure and convenient means of authentication in situations where physical contact is not possible or desirable. However, it is important to note that face recognition systems also come with their own set ofchallenges and limitations, such as accuracy and privacy concerns. Therefore, proper measuresmust be taken to ensure the protection of personal data and prevent unauthorized access.

The proposed solution of using face recognition for login systems where fingerprint authentication is traditionally used can be a practical and secure alternative during the COVID-19 pandemic. However, further research is needed to explore the effectiveness andsecurity of this approach The proposed system offers numerous advantages over existing facial recognition systems, including improved accuracy, reliability, and user-friendliness. The system can be used for various applications, including access control, attendance tracking, law enforcement, and personalized marketing. However, there are still challenges to be addressed



International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125286

V. CONCLUSION

Our proposed system of facial recognition system using LBPH algorithm can be used as authentication system which provides additional security to the system based on login. LBPH is one of the easiest face recognition algorithms and is provided by the OpenCV library which makes the implementation easy. Algorithm shows great results, mainly in a controlled environment. Through this paper we showed the performance results between 76% to 85. The proposed system is more suitable and shows better results of performance for larger data

REFERENCES

[1] M. I. P. Nasution, N. Nurbaiti, N. Nurlaila, T. I.F. Rahma and K. Kamilah, COVID-19 andemic," 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), 2020, pp. 48-51,doi:.1109/IC2IE50715.2020.9274654.

[2] Aayat Shdaifat,Randa Obeidallah, Ghadeer Ghazal, Alaa Abu Srhan, Nesreen Rabah Abu Spetan, “A proposed Iris Recognition Model for Authentication in Mobile Exams” International Journal of Emerging Technologies in learing, June 2020, DOI: 10.3991/ijet.v15i12.13741

[3] M. Pradhan, "Next Generation Secure Computing: Biometric in Secure E- transaction," International Journal of Advance Research in Computer Science and Management Studies, vol. 3, no. 4, pp. 473-489, 2015.

[4] Y. Kao, H. Gu and S. Yuan, "Personal Based Authentication by Face Recognition," 2008 Fourth International Conference on Networked Computing and Advanced Information Management, 2008, pp. 581-585, doi: 10.1109/NCM.2008.167

[5] Belhumeur, P, hespanha, J, and Kriegman, D, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection", IEEE Trans. Pattern Analysis Machine Intelligence, vol. 19, no. 7, pp. 711-720.

[6] Choi I., Kim D.Facial fraud discrimination using detection and classification Bebis G., Boyle R., Parvin B., Koracin D., Chung R., Hammound R., Hussain M., Kar- Han T., Crawfis R., Thalmann D., Kao D., Avila L. (Eds.), Advances in Visual Computing, Springer Berlin Heidelberg, Berlin, Heidelberg (2010), pp. 199- 208, 10.1007/978-3-642-17277-9_21

[7] Yang L., Fan Z., Ling S., Junwei H. Face recognition with a small occluded training set using spatial and statistical pooling Inform. Sci., 430–431 (2018), pp. 634-644, 10.1016/j.ins.2017.10.042

