IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

File access control for multiple user system using Computer Vision

Mrs. P. Navya, Nikhil Tatikonda, Nithin Reddy Muddam and Sathwik Reddy
Associate Professor, Student/Research Scholar, Student/Research Scholar, Student/Research Scholar
Department of Artificial Intelligence and Machine Learning
Aushapur(V), Ghatkesar(M), Medchal Dist 501301, Telangana, India

Abstract : The research paper aims to develop a security system, for devices that are shared among users. It consists of three elements; locking mechanisms for files and apps to safeguard privacy and prevent access, advanced face recognition technology for precise user identification and basic image process ing techniques to enhance the reliability and accuracy of facial recognition.This comprehensive solution is designed to ensure the protection of users privacy and personal data providing an user friendly experience, for individuals who share devices across scenarios and applications.

IndexTerms **- Facial Recognition, File and App Hiding, Basic Image Processing, Security, Privacy, Data Integrity, Authorized Users, Unauthorized Access, Personalized Security, Shared Systems, Biometrics, Digital Image Processing**

INTRODUCTION

In recent years, facial detection software like Windows FaceID, Apple Face ID, and smartphone face unlock have aimed to secure data and limit unauthorized access. However, chal- lenges arise when multiple users share a system, particularly concerning private files and personalized data security. Our innovative model addresses these concerns by incorporating facial recognition, file and app locking, and basic image processing. This approach ensures individual user security in shared systems. Facial recognition accurately distinguishes users based on unique facial features, forming the foundation for personalized security measures. File and app locking lets users protect specific files and applications from unautho- rized use, maintaining privacy in communal settings. Basic image processing enhances accuracy and security, identifying potential vulnerabilities .In essence, our model provides a comprehensive solution to safeguard personalized data within shared systems, offering confidence in maintaining privacy and data integration.

1. **Facial Recognition:** This cutting-edge technology an- alyzes unique facial features to accurately identify users. Whether it's Windows Face ID, Apple Face ID, or smartphone face unlock, facial recognition forms the bedrock of person- alized security measures. By ensuring that only authorized individuals can access the system, it safeguards data and privacy.
2. **File and App Locking:** In shared systems, privacy is paramount. File and app locking empowers users to pro- tect specific files and applications from unauthorized access. Whether it's confidential documents, personal photos, or sen-

sitive apps, this feature ensures that each user's private data remains secure.

3. **Basic Image Processing:** Enhancing accuracy and secu- rity, basic image processing plays a crucial role. It identifies potential vulnerabilities and fine-tunes facial recognition al- gorithms. By optimizing image quality and minimizing noise, this step contributes to robust user authentication

The primary goal of integrating face recognition into file access control systems is to enhance security and streamline access management. By leveraging facial data, this technology aims to provide a robust and efficient method for granting or denying access to secured areas.

The objectives of this project are:

Enhanced Security: Face recognition ensures that only authorized individuals can access files and sensitive data. It eliminates the need for traditional access methods like keys orcards, reducing the risk of unauthorized entry.

Convenience and Efficiency: Users no longer need physical tokens (such as keys or access cards) to gain entry. Facial recognition simplifies the authentication process, making it more convenient for users.

Reduced Administrative Overhead: Automated face recognition reduces administrative tasks related to managing access permissions. It streamlines user authentication, mini- mizing the need for manual intervention.

Reduced Administrative Overhead: Automated face recognition reduces administrative tasks related to managing access permissions. It streamlines user authentication, mini- mizing the need for manual intervention.

LITERATURE SURVEY

[1]The system proposed by hamid explains security, as a state of being saved and protected, is explored in this paper. The focus lies on leveraging two emerging artificial intelligence technologies: Facial Recognition and Artificial Neural Networks. These technologies are employed to develop secure keyless door networks, where only authorized faces can open the door. The system includes a camera-equipped door interface with a PC for capturing and processing images. The introduction highlights the evolution of security concepts, considering viewpoints from various angles, including those of terrorist organizations. Enhanced security measures evoke feelings of happiness and peace of mind. And the authors felt that their model could be improved with independency of MATLAB. The smart lock systems is a model proposed by diamond celestine in 2020. It is a modern successor to traditional locks. It provides an overview of various smart lock technologies. The smart lock system, now widely adopted in homes and commercial buildings, offers user-friendly benefits with manageable downsides. Technology has significantly im pacted our lives, including the Home Automation System—a computerized network controlling electronic devices and mon itoring home appliances efficiently. Among emerging real-time applications, the Home Security System stands out. The smart lock system gradually replaces traditional locks due to its convenience and affordability. Smart locks operate wirelessly using cryptographic keys, granting access only to authorized personnel. Biometric systems (such as fingerprint recognition) enhance security. Some smart locks even incorporate cameras. Smart locks play a crucial role in smart connected homes, serving both commercial and residential security needs. They allow third-party access via virtual keys sent to recipients' smartphones through Wi-Fi, mobile apps, proximity sensors, and Bluetooth Low Energy (BLE). Arun Balasubramanyam proposed an approach for access control[2]. Embodiments of the present invention involve a method, system, and program product for using access-control lists (ACLs) to control ac cess to computer files. These embodiments receive and store classifications of two or more computer files where those classifications fall within a single category. The category may identify products, product lines, geographic locations, customer account identifiers, network types, server platform types, or server operating statuses associated with an access controlled file. The method checks the access-control list in response to a user's request for access to determine if the user is authorized.

[3]The study by Takahisa on file access destination has brought to light disparities in national laws concerning the GDPR's application to the processing of personal data for scientific purposes. These differences could impair data subject protection standards, impede information interchange, and produce legal ambiguities. While it is stressed how important it is to notify data subjects, there have been criticisms of several GDPR rules, including those found in Articles 13 and 14. Particular weaknesses include a lack of instructions regarding the rights of data subjects and how to get in touch with supervisory authorities. Furthermore, the GDPR is unclear regarding how to notify data subjects of modifications to the terms of processing. Despite these obstacles, it has been proposed that some of these restrictions may be addressed by the EDPB's interpretation of the transparency principle.

[4]The research of Ashi, Rahul and srishti on data hiding techniques using steganography highlighted future scope in the area. It explores the basic principles of steganography, emphasizing the delicate trade-off that the method's intrinsic security and capacity must make. It presents ideas intended to reduce the chance of steganalysis detection while simul taneously improving security and capacity. The conversation continues by examining image steganography, which is a widely used and complex technique for data concealing. It emphasizes how simple this technique is—only the sender and recipient are aware of it. The idea of maintaining image integrity by locating areas with the least amount of distortion lies at the heart of this technique. The review also exam ines steganography techniques, classifying them as spatial or transform domain operations that modify an image's statistical properties. It talks about ways to make these algorithms better, like maximizing embedding efficiency and reducing distortion.

METHODOLOGY

The first step is to capture an image of the user's face. Then, the system compares the captured image to a database of known faces. If a match is found, the system proceeds to 2nd step verification. If no match is found, the system may prompt the user to answer a security question for recognition of the user. This mechanism helps the model to continue security even in case of face recognition failure. The reasons of face recognition failure can be low light, changes in facial structure, camera issues etc. The code imports necessary Python libraries and modules for different functionalities, such as cv2 for face recognition and os for automation in background. It initializes face recognition to detect admins and unknown users, forms a square around the face and labels the admin. Upon face recog nition, grants access to pc and hides specific unassigned files. In case of unknown users, asks a security question to bypass. It Forces PC to sleep mode after verification failure. We used Pycharm environment to execute this project. The code makes use of PyCharm environment and command prompt to run. It opens up a 'video' window for face recognition.

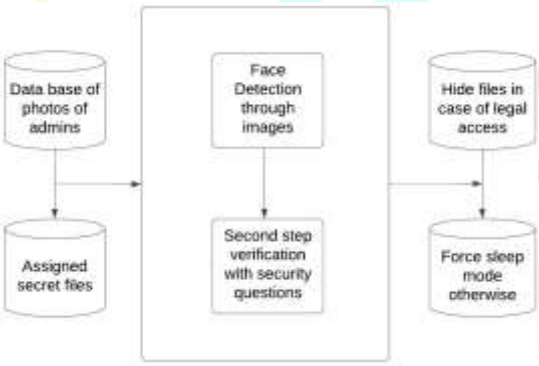

Figure 1. System Architecture

The above chart displays the architecture of the model. We can get an understanding of the design of the proposed model.

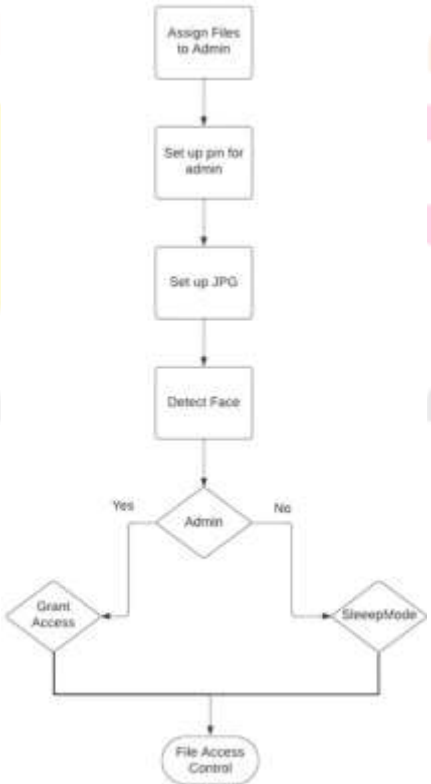

Figure 2. Flow chart of process

EXPERIMENTAL RESULTS

The below are the images of the result after running our code.

Figure 3. Before restricting the file access

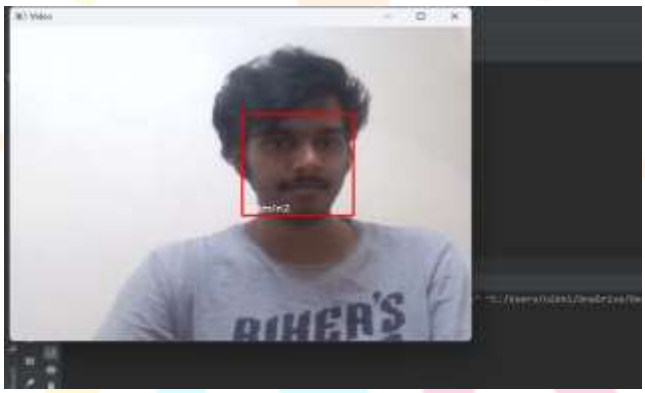

Figure 4. Face recognition of one of the admins

Figure 5. security question for second step verification

Figure 6. Hiding the files

CONCLUSION

In Conclusion, this project successfully demonstrates the capabilities of long facial recognition systems as compared tonormal file access control methods. It implements a framework for accessing the files based on the features extracted from a set of existing image files. The project achieves the following:

1) **Data Preprocessing:** Successfully extracts images from provided files and compares them to the image.
2) **Feature Extraction:** Extracts relevant features from the image, providing essential information for the model.
3) **Facial detection:** Detects the faces in the database, if the features match, the file will be opened and if not asks for a relevant question.
4) **Access control:** Access control only enables the files to be opened for the right user.
5) **Intruder Detection:** Uses the trained model to detect intruders, sending the concerned parties an image of them via mail.

One of the main limitations to consider is

1. **Operating systems:** Facial detection may not be com- patible with all operating systems or platforms, or may requirespecific hardware or software to function properly. This may limit the availability and scalability of facial detection access control systems. The below are some possible advancements in AI in future.
2. **Using AI to improve accuracy and anti-spoofing:** AI- driven identity verification for access control can become more capable and accessible in the future. AI can enable facial recognition systems to incorporate multifactor authentication, video authorization, and other features to create a more secure and convenient access control solution.
3. **Integrating with other biometric modalities:** Facial recognition can be combined with other biometric modalities, such as iris, fingerprint, or voice, to provide a more robust andreliable access control system. This can also increase the user acceptance and trust in the technology.
4. **Adapting to different environments and scenarios:** Facial recognition can be enhanced to work in different lighting, angles, expressions, or occlusions, and to supportand enforce mask-wearing mandates. This can improve the performance and usability of the technology in various settings and situations.
5. **Implementing real-time facial recognition with Node.js and OpenAI:** Facial recognition can be implemented using Node.js and OpenAI, which are high-performance back- end technologies and advanced artificial intelligence platforms. This can enable real-time facial recognition for access control with low latency and high scalability.
6. **Ensuring privacy and compliance:** Facial recognition can be improved to ensure the privacy and compliance of the users and the data. This can involve using encryption, anonymization, consent, and audit mechanisms to protect the biometric data from breaches or misuse. This can also in- volve following the data protection laws and regulations, such as GDPR or CCPA. The file access control using computer vision solves the security issue of secret files in a single user system where there can be multiple admins. And also makes the pc not accessible to unknown users by forcing the sleep mode. It utilizes computer vision, face recognition and os to make all these possible

ACKNOWLEDGMENT

We would like to thank Mrs. P. Navya for her valuable comments and suggestions to improve the quality of the paper. We are also grateful to Dr. K. Shirisha Reddy for helping us review our work regularly. We would also liketo thank the Department of Computer Science Engineering(AI and ML), VBIT Hyderabad for providing us with all the help we needed.

REFERENCES

[1]Rana Hamid, "Develop of security system using facial recognition," https://www.researchgate.net/publication/341261991_Home_ Automation_Security_System_Based_on_Face_Detection_and_ Recognition_Using_IoT.
[2] Arun Balasubramanyam, Mary E. Rudden and Donald E. Schaefer et al, "Access controller that controls access to files by using access control list," https://shorturl.at/vzDJ0.
[3] Takahisa Shirakawa et al, "File access destination control device and method," https://shorturl.at/rxBW4.
[4] Ashi Tyagi and Rahul veer Singh et al, "Data hiding techniques using steganography algorithms," https://www.researchgate.net/publication/ 342261832_Data_Hiding_Techniques_Using_Steganography_ Algorithms.
[5] Micheal, Amer, Gerges and Nidal, "Face recognition security sys tem," https://www.academia.edu/11766244/Development_of_Security_ System_using_Facial_Recognition. [
6] Hoo-Ki Lee, Sung-Hwa Han and Daesung Lee et al, "Kernel-based container file access control architecture to protect important application information," https://shorturl.at/lmBHQ.
[7] Akihiro Urano, Takaki Nakamura, Hitoshi Kamei, Masakuni Agetsuma and Yasuo Yamasaki et al, "Face recognition security system," https: //shorturl.at/bcx25.
[8] Rossana Ducato et al, "Data protection, scientific research, and the role of information," https://www.sciencedirect.com/science/article/pii/ S0267364920300170.
[9] Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer, Josef Küng et al, "A systematic literature review for authorization and access control: definitions, strategies and models," https://rb.gy/q1y94t.
[10] Sana Ghafoor, Dr Khattak, "Home automation security system based on face detection and recognition using iot," https://www.researchgate.net/ publication/259027363_Face_Recognition_Security_System