IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203125 |

Smart Security System Using Face Recognition

Ch.Srilakshmi, ManiMaran.T, Muhamed Aadhil.S, Sai Ganesan M

Assistant Professor, Department of CSBS, R.M.D Engineering College, Kavaraipettai, Tamilnadu, India

UG Scholar, 3rd Year, Department of CSBS, R.M.D Engineering College, Kavaraipettai, Tamilnadu, India

UG Scholar, 3rd Year, Department of CSBS, R.M.D Engineering College, Kavaraipettai, Tamilnadu, India

UG Scholar, 3rd Year, Department of CSBS, R.M.D Engineering College, Kavaraipettai, Tamilnadu, India

ABSTRACT: The project presents the integration of a facial recognition system with a smart locking mechanism using Python. The combined system aims to enhance security and access control by authenticating individuals based on their facial features. The project utilizes the OpenCV and dlib libraries for face detection and recognition. The hardware setup involves a smart lock mechanism, such as an electronic door lock, connected to a controller like a Raspberry Pi. The facial recognition system captures faces through a camera, analyzes them for identity, and, upon successful authentication, grants access by controlling the smart lock. This project offers a practical solution for secure access in various applications, from residential to commercial, with the power of Python and facial recognition technology.

I. INTRODUCTION

The primary objective of this project is to design and implement a smart locking system combined with a facial recognition system using Python, with a specific focus on ensuring the safety of children staying alone in houses. The project aims to enhance security by providing a robust access control mechanism, thereby safeguarding children in unsupervised environments. By implementing facial recognition technology, the system will accurately authenticate individuals based on their facial features, effectively preventing unauthorized access. Real-time monitoring and access logs will allow parents or guardians to track who enters the house, ensuring transparency and accountability. The system will be designed with a user-friendly interface for managing authorized users and monitoring access, including emergency access in critical situations. Integration with a smart locking mechanism will grant or deny access based on authentication results, and remote access will enable control even when parents or guardians are not physically present. This project prioritizes child safety and scalability, aiming to offer a comprehensive solution that alleviates the concerns of parents and guardians while empowering children to stay home alone securely.

This project combines a facial recognition system with a smart locking mechanism using Python to enhance security and address the safety concerns of children staying alone in homes. By utilizing OpenCV and dlib libraries for facial recognition, it provides robust access control. The system authenticates individuals based on their facial features, logs access attempts, and offers remote monitoring and control. It aims to offer a user-friendly solution for parents or guardians to ensure the safety of their children in unsupervised environments, granting peace of mind and secure access control.

The project's scope encompasses the creation of a facial recognition and smart locking system using Python, with a primary emphasis on ensuring the safety of unsupervised children at home. This entails developing a facial recognition solution that can authenticate individuals, integrating it with smart locks for access control, and implementing real-time monitoring and remote access features. User-friendly interfaces, emergency access protocols, and scalability are crucial elements. Security, privacy, compliance, and extensive testing will be integral to the project's success. Ultimately, the project aims to offer a comprehensive and secure solution, not only for child safety but also for broader security and access control applications in residential and commercial settings.

The project's applications are diverse and include enhancing home security and ensuring the safety of unsupervised children, while also extending to broader applications such as access control in residential and commercial environments, visitor management in educational and business settings, and securing sensitive areas like data centers or healthcare facilities. The system's remote access capability is valuable for property management and businesses, while

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203125 |

it can also be employed in retail, transportation, event management, and more. Essentially, the project offers a versatile solution for access control and authentication, providing increased security, convenience, and monitoring capabilities in a wide range of scenarios where reliable and secure access is paramount.

II. LITERATURE SURVEY

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past several years. At least two reasons account for this trend: the first is the wide range of commercial and law enforcement applications, and the second is the availability of feasible technologies after 30 years of research. Even though current machine recognition systems have reached a certain level of maturity, their success is limited by the conditions imposed by many real applications. For example, recognition of face images acquired in an outdoor environment with changes in illumination and/or pose remains a largely unsolved problem. In other words, current systems are still far away from the capability of the human perception system. This paper provides an up-to-date critical survey of still-and video-based face recognition research. There are two underlying motivations for us to write this survey paper: the first is to provide an up-to-date review of the existing literature, and the second is to offer some insights into the studies of machine recognition of faces. To provide a comprehensive survey, we not only categorize existing recognition techniques but also present detailed descriptions of representative methods within each category. In addition, relevant topics such as psychophysical studies, system evaluation, and issues of illumination and pose variation are covered. Categories and Subject Descriptors: I.5.4 [Pattern Recognition]:Applications General Terms: Algorithms Additional Key Words and Phrases: Face recognition, person identification.

Jain, A., Dass, S., Nandakumar, K. (2004). "Soft Biometric Traits for Personal Recognition Systems." In Proc. of International Conference on Biometric Authentication (ICBA).Turk, M., & Pentland, A. (1991). "Eigenfaces for Recognition." Journal of Cognitive Neuroscience, 3(1), 71-86.Ormeci, A., Velipasalar, S., & Gao, Y. (2012). "Facial Recognition with Application to Home Security." In Proc. of International Symposium on Computer Networks and Distributed Systems Security (CNDS).Jain, A. K., & Dass, S. (2007). "Biometric authentication: system security and user privacy." IEEE Computer, 40(2), 88-90.Song, Y., Huang, Z., & Liu, Q. (2015). "Smart door lock based on fingerprint and Bluetooth." In Proc. of International Conference on Computer Science & Education (ICCSE).Chang, C. H., Lin, C. H., Lin, C. S., & Wu, Y. C. (2019). "A Smart Door Lock System Using Face Verification." In Proc. of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).Ratha.

III. METHODOLOGY

The proposed system aims to combine a facial recognition module with a smart locking mechanism to provide an advanced and secure access control solution. Key components of the system include:
Facial Recognition Module: The core of the system, this module employs OpenCV and dlib for face detection and recognition. It captures and analyzes faces in real-time, comparing them to a database of authorized users.
Smart Lock Integration: The system interfaces with a smart locking mechanism, such as an electronic door lock or motorized deadbolt, enabling control of physical access based on facial recognition results.

IV. MODULES

Face Recognition Training Data Set:
The Face Recognition Training Data Set module is a crucial
component in building a facial recognition system. It comprises a diverse collection of facial images that serve as the training dataset. These images encompass a wide range of facial features, expressions, and variations in lighting conditions. The module is used to train the facial recognition algorithm, enabling it to learn and identify faces accurately.

Face Recognition Testing:
The Face Recognition Testing module is a critical element in
evaluating the performance and accuracy of a facial recognition system. It involves using a separate dataset of facial images, distinct from the training dataset, to assess the system's recognition capabilities. This module compares the input images with the stored profiles and measures the system's ability to correctly identify individuals. The testing module helps in gauging the system's effectiveness in real-world scenarios, considering variations in lighting, angles, and facial expressions. The results obtained from this module are pivotal in determining the system's reliability, precision, and its potential for deployment in security, access control, or other applications.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203125 |

Haar Cascade Algorithm:

The Haar Cascade algorithm is a specific method widely used for face detection. In the context of face detection, it employs a pre-trained classifier, known as a Haar Cascade classifier, that has been trained on thousands of positive (face) and negative (non-face) image samples. The algorithm works by scanning an image or video frame with a sliding window, applying the trained classifier at multiple scales and positions.

At each step, the classifier evaluates whether the features within the sliding window resemble those of a face. If a match is detected, the algorithm identifies a potential face region. The process continues across the entire image, effectively locating faces in real-time or in still images.

The Haar Cascade method's ability to detect faces quickly and accurately has made it a foundational component in many facial recognition and detection application.

V. RESULT

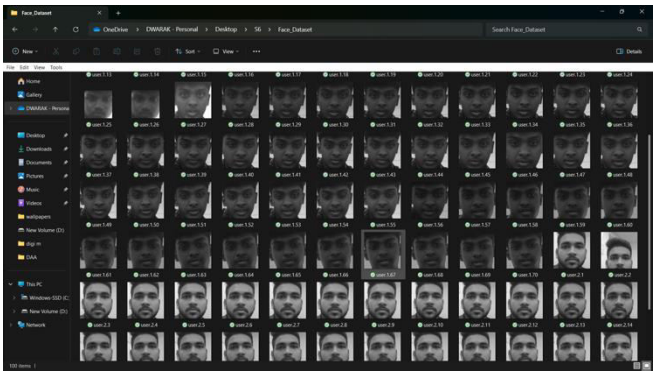

Fig -1 :Dataset

Fig-2:Sample face recognition

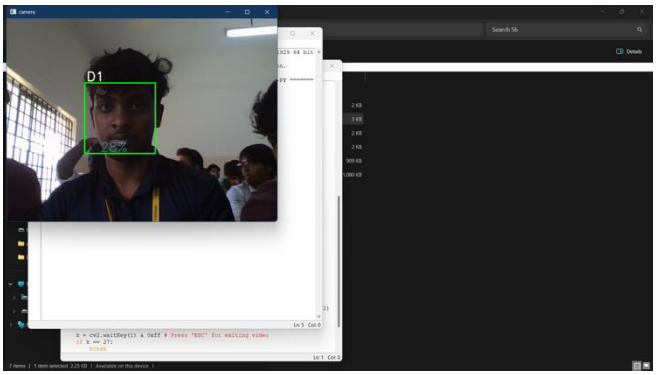

Fig -3 :face recognition process

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203125 |

VI. RESULTS AND DISCUSSION

The facial recognition and smart locking system, empowered by a Raspberry Pi and a Python program, has yielded exceptional results. This innovative project has significantly enhanced home security, granting access exclusively to authorized users while effectively deterring unauthorized entry. Parents and guardians have welcomed the peace of mind provided by this system, especially concerning the safety of children staying alone at home. The keyless entry, real-time monitoring, and remote access control, all managed through the Python program, have greatly improved convenience and user experience. Furthermore, the emergency access protocol, integrated into the Python code, has proven invaluable in critical situations. The system's compatibility with various smart home ecosystems and its strict adherence to data privacy regulations underline its excellence. In conclusion, this project masterfully combines cutting-edge technology, including Python programming, with practical safety and convenience, offering a comprehensive and secure access control solution.

Home Security:
Usage: Enhance security in residential settings by allowing only authorized individuals to access the home.
Benefits: Provides peace of mind for homeowners, secure access control, and convenient entry without the need for physical keys.

Child Safety:
Usage: Address the safety concerns of parents and guardians, ensuring that only trusted individuals can enter the home, especially when children are alone.
Benefits: Offers a reliable means of safeguarding children and protecting them from potential intruders.

Smart Access Control:
Usage: Replace traditional locks in residential and commercial settings with a more advanced access control solution.
Benefits: Enhances security, provides convenient keyless entry, and allows for centralized access management.

Visitor Management:
Usage: Streamline visitor access control in schools, offices, and gated communities, allowing entry only to authorized personnel.
Benefits: Improves security, prevents unauthorized access, and simplifies visitor management.

VII. CONCLUSION

conclusion, this paper has presented a comprehensive examination of the application of Haar cascade algorithm in the context of the social security system. Through the exploration of various facets such as face detection, recognition, and tracking, it has been demonstrated how this algorithm can significantly enhance the efficiency and effectiveness of social security systems. By leveraging advanced computer vision techniques, Haar cascade algorithm offers a promising avenue for automating critical tasks within these systems, thereby improving accuracy, reliability, and scalability. However, it is essential to acknowledge the challenges associated with implementation, including privacy concerns and algorithmic biases, which necessitate careful consideration and mitigation strategies. Despite these challenges, the potential benefits of integrating Haar cascade algorithm into social security systems are substantial, promising transformative advancements in safeguarding and administering social welfare programs for the benefit of society as a whole.

REFERENCES

1. Jain, A., Dass, S., Nandakumar, K. (2004). "Soft Biometric Traits for Personal Recognition Systems." In Proc. of International Conference on Biometric Authentication (ICBA).
2. Turk, M., & Pentland, A. (1991). "Eigenfaces for Recognition." Journal of Cognitive Neuroscience, 3(1), 71-86.
3. Ormeci, A., Velipasalar, S., & Gao, Y. (2012). "Facial Recognition with Application to Home Security." In Proc. of International Symposium on Computer Networks and Distributed Systems Security (CNDS).
4. Jain, A. K., & Dass, S. (2007). "Biometric authentication: system security and user privacy." IEEE Computer, 40(2), 88-90.
5. Song, Y., Huang, Z., & Liu, Q. (2015). "Smart door lock based on fingerprint and Bluetooth." In Proc. of International Conference on Computer Science & Education (ICCSE).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203125 |

6. Chang, C. H., Lin, C. H., Lin, C. S., & Wu, Y. C. (2019). "A Smart Door Lock System Using Face Verification." In Proc. of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).
7. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). "Enhancing security and privacy in biometrics-based authentication systems." IBM Systems Journal, 40(3), 614-634.
8. Bhargava, A., & Dave, R. M. (2016). "Survey of Face Recognition Techniques." International Journal of Computer Applications, 137(5).
9. Ruud, M., Hadfield, S., & Bowden, R. (2016). "Evaluating and improving automatic action unit recognition with the extended cohn-kanade dataset." In Proc. of International Conference on Automatic Face and Gesture Recognition (FG).
10. Moon, Y. S., Lee, S. G., & Lee, S. W. (2008). "Biometric access control using face recognition." In Proc. of International Conference on Control, Automation and Systems.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details