WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Review on Eyes and Prints: A Next-Gen Approach to Cloud-Backed Security and Law Enforcement

Pranav Jejurkar[1], Aayush More[1], Durgesh Joshi[1], Prof. R.M. Shaikh[2]

[1] *Computer Engineering Student ,LoGMIEER ,Nashik*
[2] *H.O.D. , Asst. Professor, Computer Engineering Department, LoGMIEER, Nashik*

A B S T R A C T

In an age of heightened security concerns and IoT expansion, "Eyes and Prints" introduces an innovative smart door lock system integrating biometric authentication, cloud storage, and mobile access. This review paper explores its development, architecture, and potential impact. The system features a doorbell with a secure fingerprint sensor and an outdoor camera for visitor authentication, coordinated by a Raspberry Pi hub. It securely transmits data to a cloud-based database, accessible via a user-friendly mobile app.The paper discusses the project's objectives, including security enhancement, access control, and visitor authentication, along with the methodologies used for implementation. Real-world applications encompass residential security and visitor authentication for law enforcement. The project contributes to the IoT-based security field by providing an innovative solution to contemporary security challenges. This paper aims to advance IoT-based security systems, offering efficient access control in our increasingly connected world.

Keywords: IoT-based Smart Door Locks, Biometric Authentication, Cloud-Based Security, Law Enforcement, Fingerprint Sensor, Raspberry Pi

1. Introduction

The "Eyes and Prints" project signifies a groundbreaking venture in the realm of modern security and access control. This review paper delves into the development and integration of a smart door lock system that harnesses IoT technology, biometric authentication, cloud-based storage, and mobile application access. This comprehensive exploration delves into the system's architecture, including a doorbell with a secure fingerprint sensor and an outdoor camera for visitor authentication, all managed by a central Raspberry Pi hub. Data is securely transmitted to a cloud-based database, and users can access real-time logs, visitor images, and camera feeds through an intuitive mobile application. Our paper delves into the project's objectives, its technical intricacies, and its potential applications in residential security and visitor authentication for law enforcement. It underscores the project's innovative approach to contemporary security challenges. Through this review paper, we aim to contribute to the burgeoning field of IoT-based security systems, fostering efficient and secure access control solutions in our increasingly connected world.

1.1 Motivation

The motivation behind this review paper lies in the imperative need for innovative security solutions in the IoT era. As security concerns continue to escalate, the integration of biometric authentication, cloud technology, and mobile access in smart door lock systems has become increasingly relevant. The "Eyes and Prints" project presents a forward-looking approach that addresses contemporary security challenges and offers efficient access control in an interconnected world. By examining this project, we aim to contribute to the advancement of IoT-based security systems, fostering safer and smarter living environments.

2. Literature Survey

2.1 Smart security system for door access based on unique authentication - K.Umamaheswari , P.Mahitha

Smart voice password and biometric based security system for door locking in smart homes:

A smart door locking system based on biometric and voice password unique identification, has been developed to enhance the security level of door access. This will provide access to only authorized persons. If an unauthorized person tries to intrude, the verification fails, and the buzzer will be activated with a beep sound and the owner will receive an alert message. The data of the persons tried to access the door will be stored.

2.2 A systematic review on Fingerprint based Biometric Authentication System - Hemalatha S

Real-time Fingerprint Recognition System:

In the process of analyzing fingerprint-based authentication systems, multiple works have been considered. The ultimate goal is to understand the needs of fingerprint-based recognition systems and study the merits, demerits and shortfalls of existing systems. It is understood that biometric templates like fingerprints are highly robust and reliable for the purpose of authentication when compared with passwords, PINs or highly stuffed keys. It is also noted that there exists a significant difference between the fingerprint-samples of a single person captured at different occasions. Thus, the comparison task is considered to be a probabilistic one which is really a vice versa of strict matching of passwords or keys.

2.3 A Real-Time Face Detection Method Based on Blink Detection - Hui Qi, Chenxu Wu, Ying Shi, Xiaobo Qi, Kaige Duan, And Xiaobin Wang

Real-Time Video Face Recognition:

This paper proposes a real-time face detection method based on blink detection called LBAS_Resnet50 to solve the problems of illumination and expression changes in the process of real-time face recognition. The model takes ResNet50 as the basic network structure and sends the texture features extracted by the LBP algorithm into the basic network to improve the tolerance to illumination in the recognition process. Then by adding BiLSTM to obtain context information, it is convenient to extract time series features, so as to improve the accuracy of real-time recognition. At the same time, the channel attention mechanism is added to extract key feature information and assign important weights, and SPP pooling is used to improve the robustness of the model. Finally, the real face is judged by eye blink detection. The experimental results indicate that the method proposed in this paper has a good effect on the accuracy of anti-spoofing real-time face recognition. Due to the different structures of paper, electronic device screens and real faces, the facial images acquired by cameras differ in brightness and illumination information. In the next research, we will consider efficiently separating brightness and reflected light features from RGB images to further improve model performance. In addition, we will consider applying sparse representation to deep learning based on face recognition.

2.4 Surveillance System for Real-Time High-Precision Recognition of Criminal Faces from Wild Videos - Hyun-Bin Kim, Nakhoon Choi, Hye-Jeong Kwon, And Heeyoul Kim

Crime Prevention Using Computer Vision:

The proposed system analyzes video footage captured by surveillance cameras in real-time. By using a method that iteratively detects and identifies faces in each frame, the footage can be analyzed immediately without storing it. By proposing a face recognition method that uses down-sampling to identify face positions and utilizes them in the original quality image, the performance of face detection and identification can be improved on the same hardware to enable real-time detection. It contributes to improving the precision of object tracking by storing the location of the detected face in the video and the identification information predicted by the system. The face tracking ID unit also compensates for the problems of the prediction unit when performing face recognition in video data. The face tracking ID unit minimizes the prediction flipping problem caused by the congested embedding problem due to the large size of the embedding DB through the identification score accumulation method. The threshold value used in the identification score accumulation method was detected through experiments to find the optimal threshold. In addition, a data set was created for evaluation and measurement in the overall experiment. Since the proposed system uses the input and output formats of common face detection and identification systems, it ensures freedom of tuning, which allows practical users to easily apply different models suitable for specific domains. This is evidenced by the improvement in accuracy and F-1 score during migration in the experiments according to the identification method. In addition, two parameters can be utilized to derive the final score for the tracked object, allowing a high precision or recall being selected. In our experiments, we obtained an accuracy of 0.900 and an F-1 score of 0.943 for ($\alpha = 4.5$, $\beta = 15$).

2.5 A Novel Front Door Security (FDS) Algorithm Using GoogleNet-BiLSTM Hybridization - Luiz Paulo Oliveira Paula, Md. Whaiduzzaman, Nuruzzaman Faruqui, Imran Mahmud, (Senior Member, IEEE), Eric Charles Hawkinson , And Sandeep Trivedi ,(Senior Member, IEEE)

Front Door Security Algorithm using Human Activity Recognition:

The research paper presents an innovative automatic Front Door Security (FDS) algorithm using Human Activity Recognition (HAR) to detect security threats at the front door from a real-time video feed with 73.18% accuracy. The FDS algorithm uses an innovative combination of GoogleNet- BiLSTM hybrid network to classify activities, such as attempts to break the door by kicking, punching, or hitting, as well as gun violence. The paper discusses the design of the hybrid network, the selection and processing of the video data set, and the training of the LSTM network. It also presents the experimental results and performance evaluation of the proposed algorithm, demonstrating its potential for ensuring better safety with 71.49% precision, 68.2% recall, and an F1- score of 0.65. The paper also discusses the application of AI technology in strengthening front-door security and highlights the significance of applying AI in physical security. Additionally, the limitations and future scope of the proposed system are discussed, with the authors emphasizing the need for further research to improve the system's service quality and robustness. Overall, the paper showcases the potential of the FDS algorithm in providing an automatic and intelligent security system for front doors at an affordable cost.

2.6 When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark - Zhizhong Huang, Graduate Student Member, IEEE, Junping Zhang, Senior Member, IEEE, and Hongming Shan, Senior Member, IEEE

Introduction to MTLFace :

The research paper proposes a unified, multi-task learning framework called MTLFace for age-invariant face recognition (AIFR) and face age synthesis (FAS). The framework includes attention-based feature decomposition to separate identity- and age-related features, and a novel identity conditional module for achieving identity-level FAS with improved age smoothness. The proposed MTLFace is evaluated on benchmark cross-age datasets and demonstrates superior performance compared to state-of-the-art methods for both AIFR and FAS. Additionally, the paper introduces a new large cross-age face dataset for tracing long-missing children and a new benchmark dataset called ECAF. The experimental results on these datasets show that MTLFace outperforms existing state-of-the-art methods for AIFR and FAS, and also achieves competitive performance for general face recognition. The framework also includes a selective fine-tuning strategy to further boost AIFR by automatically selecting high-quality synthesized faces from FAS for fine-tuning. Overall, the proposed MTLFace shows strong generalization ability and effectiveness in addressing the challenges of age-invariant face recognition and face age synthesis.

MTLFace Framework and Features:

The research paper introduces MTLFace, a multi-task framework for age-invariant face recognition (AIFR) and face age synthesis (FAS). It addresses the lack of visual results for AIFR and compromised recognition due to artifacts in FAS. MTLFace utilizes attention-based feature decomposition and an identity conditional module for identity-level FAS. Additionally, it presents a large cross-age face dataset and a benchmark for tracing long-missing children. Experimental results demonstrate MTLFace outperforms state-of-the-art methods for AIFR and FAS. MTLFace achieves continuous face age synthesis using a StyleGAN-based architecture and maintains stable training by employing perceptual image patch similarity (LPIPS) loss. While MTLFace improves discrimination of the face recognition model for face rejuvenation, it faces challenges in face aging due to ghost artifacts. The paper acknowledges limitations and discusses solutions for improving background preservation in face age synthesis. Overall, MTLFace shows significant advancements in AIFR and FAS tasks.

2.7 Finger Vein Recognition Based on Anatomical Features of Vein Patterns - Arya Krishnan and Tony Thomas

Finger Vein Recognition Based on Anatomical Features and FEBA Representation:

The research paper presents a new approach to finger vein recognition based on distinct anatomical vein patterns. It introduces a feature representation method using a 6×6 feature matrix derived from identifying six vein patterns (F1F2EB1B2A) through anatomical analysis. The proposed method offers template security and invariance to scaling, translation, and rotation changes. Experimental results showcase superior recognition performance, with an EER around 0.02% and an average recognition accuracy of 98%, compared to existing approaches. The proposed method outperforms existing methods, as shown in a comprehensive evaluation using HKPU, SDUMLA, and in-house datasets. The new approach demonstrates robustness to rotation, scaling, and translation, presenting promising results for finger vein recognition. The paper suggests future research directions to improve the feature representation by incorporating more pattern-based features and adding more sub-patterns to the fundamental F2EB2A pattern.

2.8 Multimodal Finger Recognition Based on Asymmetric Networks with Fused Similarity - Yiwei Huang, Hui Ma, And Mingyang Wang

A Multimodal Approach Using Attention Mechanisms and Fusion Networks:

The research paper proposes an end-to-end multimodal finger recognition model that integrates attention mechanisms into a similarity-aware encoder to address the limitations of existing biometric fusion methods in dealing with correlations and redundancy of multimodal features. The paper introduces a finger asymmetric backbone network (FAB-Net) for extracting intra-modal features and a novel attention-based encoder fusion network (AEF-Net) with channel attention to improve performance in multimodal biometric systems. The effectiveness of the proposed method is validated through recognition experiments on three multimodal finger databases, demonstrating its ability to generate more discriminative common representations and achieve advanced recognition accuracy. The paper provides insights into the importance of considering the correlation and redundancy of multimodal information and demonstrates the potential of the proposed approach for improving multimodal biometric recognition.

2.9 Invisible Adversarial Attacks on Deep Learning-Based Face Recognition Models - Chih-Yang Lin, (Senior Member, IEEE), Feng-Jie Chen, Hui-Fuang Ng, (Member, IEEE), and Wei-Yang Lin (Member, IEEE)

Mask generation method based on facial landmark detection and super-pixel segmentation:

The paper proposes a method for generating imperceptible adversarial face images based on facial landmark detection and super-pixel segmentation. The paper highlights the vulnerabilities of existing face recognition systems to adversarial attacks. The proposed method involves extracting facial landmarks, segmenting super-pixels, and inserting adversarial noise within the masked areas. Experimental results demonstrate the success of the proposed method in fooling face recognition systems in real-world scenarios. The study utilizes performance metrics such as Attack Success Rate (ASR) and Structural Similarity Index Measure (SSIM) to evaluate the effectiveness of the proposed method. The results show that the proposed method can generate imperceptible adversarial samples with high SSIM values and maintain attack success in real-world scenarios, such as when captured by a camera or

subjected to different lighting conditions and camera viewing angles. The proposed method is shown to be effective against various face recognition models and robust against different adversarial defense mechanisms.

3. Methodology

3.1 Minutiae-based Matching for Fingerprint Detection:

Our methodology for fingerprint detection revolves around a minutiae-based matching algorithm, prioritizing accuracy and uniqueness in fingerprint recognition. In the preprocessing stage, we enhance fingerprint images using histogram equalization and adaptive filtering to ensure clarity in ridge and valley structures. Additionally, morphological operations are applied for noise and artifact removal. Minutiae extraction involves the identification of minutiae points shown in Fig.1, including ridge endings and bifurcations, achieved through local ridge orientation and curvature analysis. The resulting minutiae features are organized into a template structure using the Delaunay triangulation method. The matching process utilizes a modified Euclidean distance metric for minutiae template comparison, and a similarity score is computed based on the number and spatial distribution of matched minutiae points. Thresholding is implemented through adaptive thresholding informed by statistical analysis of the dataset, with iterative adjustments using Receiver Operating Characteristic (ROC) analysis for an optimal balance between false positives and false negatives.

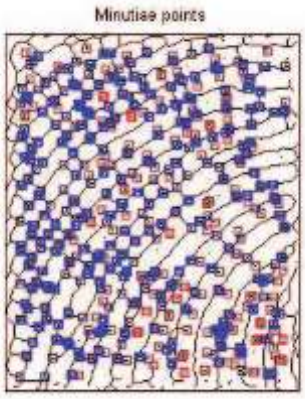

Fig. 1 - Minutiae Points in fingerprint image

3.2 Viola-Jones Face Detection Algorithm:

In conjunction, our face detection methodology integrates The Viola-Jones algorithm, renowned for its speed and accuracy. Haar-like features are computed using integral images, representing diverse facial characteristics such as edge features, line features, and four-rectangle features. Training a cascade of classifiers involves Adaboost training with a diverse dataset to construct a robust classifier from weak classifiers based on Haar-like features shown in Fig. 2. The cascade structure, implemented in multiple stages, facilitates rapid rejection of non-face regions. The sliding window approach systematically scans the image using a sliding window mechanism with varying window sizes to detect potential face regions. Non- maximum suppression is applied to eliminate redundant detections. To reduce false positives, post-processing techniques such as connected component analysis and aspect ratio filtering are employed. Parameter optimization, including the minimum detection confidence threshold, enhances overall detection performance. The integration of these algorithms ensures a robust and efficient biometric recognition system, suitable for comprehensive security and law enforcement applications.

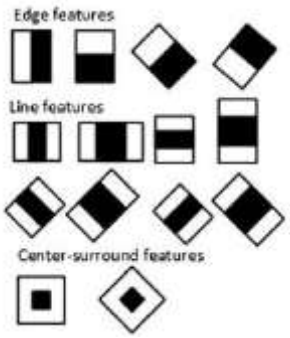

Fig. 2 - Haar-Like Feature

4. Conclusion

The "Eyes and Prints" project represents a significant step towards modernizing security systems, providing a secure and user-friendly solution for access control. By leveraging IoT technologies, biometric authentication, and cloud storage, the system not only enhances security but also aids law enforcement efforts. The detailed system requirements, operating environment specifications, and testing guidelines provide a comprehensive framework for successful implementation.

5. Results and Discussions

The "Eyes and Prints" project presents a compelling approach to smart door lock systems, aiming to enhance security and offer valuable functionalities. Let's delve into the key findings and explore their implications.

Unlocking Security: The project successfully implemented two-factor authentication with fingerprint and password, demonstrating accurate user identification. Non-deletable cloud-based logs, including timestamps and camera footage, offer a robust record of activity, potentially aiding law enforcement investigations. However, concerns regarding data privacy and potential misuse require further exploration and adherence to stringent regulations.

Visualizing Security: The live camera feed, accessible through the mobile app, empowers users with real-time monitoring capabilities. This transparency fosters a sense of security and allows for remote verification of activity. However, the review should delve into the video quality and field of view, ensuring they adequately capture relevant details.

Mobile Convenience: The mobile app facilitates user interaction with the system, offering log access and camera viewing. This convenience streamlines security management and promotes user engagement. Further exploration of the app's usability and accessibility is crucial to ensure its effectiveness for diverse user groups.

Performance and Limitations: While the project details lack specific performance metrics, future evaluations should assess accuracy, reliability, and latency to gauge overall effectiveness. Additionally, the review should discuss potential limitations, such as power consumption or potential network disruptions, and suggest mitigation strategies.

Future Horizons: The "Eyes and Prints" project sets a promising foundation for further advancements. Integration with smart home ecosystems could expand its functionalities and seamlessly blend into existing security protocols. Additionally, exploring alternative authentication methods, such as voice recognition or facial recognition, could enhance user experience and cater to various needs.

Overall, the "Eyes and Prints" project exhibits significant potential in revolutionizing smart door lock solutions. While acknowledging its strengths in security features and user convenience, the review should delve deeper into data privacy concerns, performance evaluations, and potential future directions to provide a comprehensive assessment of its impact and pave the way for further innovation.

References

1. K. Umamaheswari and P. Mahitha, "Smart security system for door access based on unique authentication," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 1474- 1477, doi: 10.1109/I-SMAC52330.2021.9640855.

2. S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-4, doi: 10.1109/ic- ETITE47903.2020.342.

3. H. Qi, C. Wu, Y. Shi, X. Qi, K. Duan and X. Wang, "A Real-Time Face Detection Method Based on Blink Detection," in IEEE Access, vol. 11, pp. 28180-28189, 2023, doi: 10.1109/ACCESS.2023.3257986.

4. H. -B. Kim, N. Choi, H. -J. Kwon and H. Kim, "Surveillance System for Real-Time High-Precision Recognition of Criminal Faces From Wild Videos," in IEEE Access, vol. 11, pp. 56066-56082, 2023, doi: 10.1109/ACCESS.2023.3282451.

5. L. P. O. Paula, N. Faruqui, I. Mahmud, M. Whaiduzzaman, E. C. Hawkinson and S. Trivedi, "A Novel Front Door Security (FDS) Algorithm Using GoogleNet-BiLSTM Hybridization," in IEEE Access, vol. 11, pp. 19122-19134, 2023, doi: 10.1109/ACCESS.2023.3248509.

6. Z. Huang, J. Zhang and H. Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 6, pp. 7917-7932, 1 June 2023, doi: 10.1109/TPAMI.2022.3217882.

7. A. Krishnan and T. Thomas, "Finger Vein Recognition Based on Anatomical Features of Vein Patterns," in IEEE Access, vol. 11, pp. 39373-39384, 2023, doi: 10.1109/ACCESS.2023.3253203.

8. Y. Huang, H. Ma and M. Wang, "Multimodal Finger Recognition Based on Asymmetric Networks With Fused Similarity," in IEEE Access, vol. 11, pp. 17497-17509, 2023, doi: 10.1109/ACCESS.2023.3242984.

9. C. -Y. Lin, F. -J. Chen, H. -F. Ng and W. -Y. Lin, "Invisible Adversarial Attacks on Deep Learning- Based Face Recognition Models," in IEEE Access, vol. 11, pp. 51567-51577, 2023, doi: 10.1109/ACCESS.2023.3279488.