JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Face Recognition System for Identity Theft Protection

Shraddha.S.Banne
Assistant Professor
Dept. of Computer Engineering
Guru Gobind Singh College Of Engineering and Research Center
SPPU University,
Nashik, India

Mrunalini S. Shimpi
Student
Dept. of Computer Engineering
Guru Gobind Singh College Of Engineering and Research Center
SPPU University,
Nashik, India

Vaibhav S. Maurya
Student
Dept. of Computer Engineering
Guru Gobind Singh College Of Engineering and Research Center
SPPU University,
Nashik, India

Rida A. Shaikh
Student
Dept. of Computer Engineering
Guru Gobind Singh College Of Engineering and Research Center
SPPU University,
Nashik, India

Saklen S. Maniyar
Student
Dept. of Computer Engineering
Guru Gobind Singh College Of Engineering and Research Center
SPPU University,
Nashik, India

***Abstract*— The project aimed to develop a facial recognition system that utilized liveliness detection to authenticate users by scanning facial gestures like shape and motion, eye blinking. The system's primary objective was to enhance user privacy and authenticity by providing a reliable and efficient tool for authentication. The system targeted both government and private business sectors, offering a robust solution to prevent identity theft.The system scanned registered users and authenticated them for accessing purchased courses. Identity theft was a significant concern in online education platforms, where unauthorized access to paid courses could occur. To address this, our system served as a secure authentication mechanism, ensuring only registered and authenticated individuals could access paid courses.By incorporating liveliness detection techniques, the system could distinguish between real faces and potential impersonations, enhancing overall security. This advanced feature alleviated the risk of the identity theft and ensured that only legitimate users could access paid courses.In conclusion, the implementation of face recognition technology in online education platforms safeguarded the integrity of these platforms and protected the interests of institutions and users alike. By enforcing strict authentication measures, the system effectively prevented from access which are not authorised and ensured that only genuine individuals benefited from paid courses.**

Keywords:- *- Face Recognition, Security, Identity Theft Protection, Authentication, Liveliness Detection.*

I. INTRODUCTION

Project Idea: - Identity theft was a pervasive issue in our digitally-driven world, where personal information was increasingly vulnerable to theft. To address this concern, robust security measures were imperative. Face recognition technology emerged as a promising solution in the fight against identity theft.

A Face Recognition System was designed to protect individual' identitie by the verifying their authenticity across digital and physical environments. Leveraging advanced facial recognition algorithms, the system accurately identified individuals, ensuring secure access to financial services, online platforms, and physical spaces.

.

Motivation of the Project: - The motivation behind this project stemmed from several factors. Firstly, face recognition systems had significantly improved in accuracy, with error rates nearing human recognition levels. This advancement enabled reliable identity verification, even under challenging conditions such as the poor lighting or partial face occlusion. Secondly, the system reduced reliance on vulnerable passwords, which were common targets for identity thieves. By eliminating the need for passwords, face recognition systems enhanced security by making it harder for thieves to access sensitive information.Lastly, face recognition systems offered convenience, as they were often more user-friendly than traditional identity verification methods like entering PINs or swiping cards. Overall, the project aimed to address the pressing issue of identity theft through the implementation of advanced face recognition technology.

II. LITERATURE SURVEY

The examination of digital technologies' transformative effects on daily activities underscores the heightened vulnerability to identity theft and unauthorized access to personal information. Addressing these challenges, the study investigates the evolution of face recognition technology as a promising solution for identity theft protection. It delineates the widespread applications of face detection and recognition across domains such as security, surveillance, and access control, emphasizing its superiority over traditional methods due to enhanced security and convenience. Furthermore, the survey explores the integration of face recognition with iris scanning and palm vein technology for multi-factor authentication, highlighting its potential to bolster overall security systems and provide resilient defense against identity theft and unauthorized access.

This survey delves into advancements in safe outsourcing of PCA-based face recognition to cloud services, highlighting the delicate balance between harnessing powerful cloud computing resources and safeguarding the confidentiality and security of sensitive facial data. It examines the efficacy of various face recognition methods, particularly focusing on eigenfaces and neural networks, elucidating the processes involved in eigenface generation and neural network training. Furthermore, the survey tackles challenges in face detection, identification, and verification, proposing a range of algorithms aimed at enhancing accuracy and robustness. The discourse extends to autonomous face detection systems in real-time video streaming, underscoring their potential in augmenting intelligence security systems, while stressing the importance of factors such as data privacy, accuracy, and cost-effectiveness in implementation. Lastly, encryption methods are discussed, drawing a comparison between the theoretical security of one-time pad encryption and the practicality of stream ciphers like RC4 in wireless communication applications.

The literature highlights a growing emphasis on customer-centric approaches in both international food chains and hotel management, driven by advancements in technology and a deeper understanding of customer preferences and needs. By adopting innovative strategies and leveraging technology effectively, businesses can enhance customer satisfaction, drive loyalty, and stay competitive in the dynamic hospitality industry.

By combining voice recognition and image processing technologies, the project aligns with current industry trends and addresses key challenges in customer management within the hospitality and food sector. This integration allows for innovative solutions such as personalized ordering systems and enhanced customer

service experiences. Moreover, the survey emphasizes the critical need for robust security measures and ethical considerations in handling customer data, underlining the importance of privacy protection in the implementation of such technologies. This holistic approach ensures that advancements in customer management not only meet industry demands but also uphold the integrity and trustworthiness of customer data.

III. PROPOSED WORK

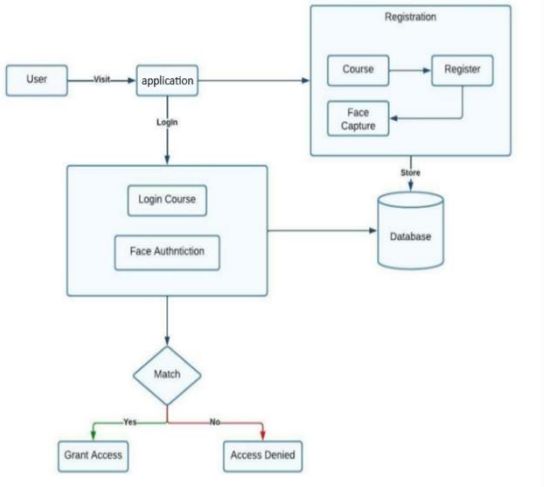


Figure 1: *System architecture*

The problem statement, objectives, and desired outcomes were clearly defined to focus on the accurate detection of the face recognition process utilizing the CNN algorithm [9]. Initially, users would open the application and review intro info after next available courses description post logging in. If interested, they proceeded to register, which involved capturing their face, student info filling and course selection after that payment process. Upon completing the registration process, they logged in again. During login, the system detected a face without requiring a username and password, it verified the face registration completed during the course registration. If the face matched, the user could proceed to the next step in the login process. At that moment, the system checked if the face registration was valid for the course. If validated, the user gained access to the course; otherwise, access was denied. This system was designed to prevent fraudulent activities by ensuring that a user or their associate could not enroll in a course without valid face registration. The dataset was divided into efficiency, validation, and test sets to assess the model's efficiency. A face recognition system for identity theft protection was developed utilizing a convolutional neural network (CNN) model trained on an anti-spoofing attack dataset, with optimization and complexity management strategies to prevent overfitting [3,6]. Techniques such as cross-validation were employed to fine-tune the model and determine the best configuration. The model's performance was evaluated using relevant metrics such as accuracy and precision, along with visualizations like Liveliness.

IV. IMPLEMENTATION

Algorithm :-

Convolutional Neural Network (CNN)

Convolutional Neural Networks (CNNs) have revolutionized the field of computer vision, particularly in tasks

like image classification, object detection, and face recognition [8]. When applied to a Face Recognition System for Identity Theft Protection in online courses, CNNs play a crucial role in verifying the identity of individuals accessing the course materials.

Here's how it typically works:

1. Data Collection and Pre-processing: The system gathers a large dataset of facial images, representing both legitimate users and potential imposters. These images are pre-processed to ensure uniformity in terms of size, lighting conditions, and orientation.

2. Training Phase: During the training phase, the CNN learns to extract meaningful features from facial images that are discriminative for identity verification. This is achieved through multiple layers of convolutional, pooling, and fully connected layers, which enable the network to automatically learn hierarchical representations of facial features.

3. Feature Extraction : CNNs are adept at learning hierarchical representations of features [10,11]. In the context of face recognition, lower layers might learn basic features like edges and textures, while higher layers might learn more complex features like facial contours, eyes, nose, and mouth.

4. Identity Verification : Once the CNN is trained, it can be deployed to verify the identity of individuals accessing the online course materials. When a user attempts to access the course, their facial image is captured through a camera or uploaded from a device. This image is then fed into the CNN, which extracts relevant features and compares them to the features of enrolled users.

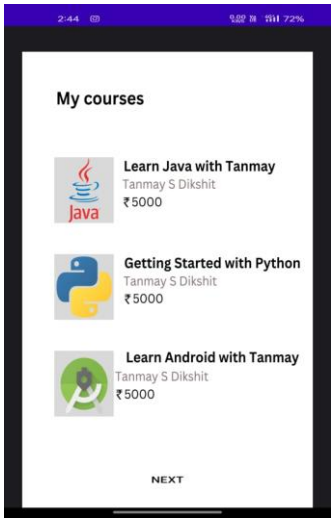
5. Matching and Decision Making : The extracted features are compared using similarity metrics such as cosine similarity or Euclidean distance. If the features closely match those of an enrolled user, the system grants access to the course materials. Otherwise, access is denied, alerting the system administrators about a potential identity theft attempt.

6. Adaptation and Improvement : The system may continually adapt and improve over time through techniques like fine-tuning the CNN with new data, incorporating feedback mechanisms, and updating the network architecture to enhance accuracy and robustness against identity theft attempts.

Overall, by leveraging CNNs in a Face Recognition System for Identity Theft Protection in online courses, institutions can enhance security measures, safeguarding the integrity of their educational platforms and protecting the identities of legitimate users. whole.

Screeshots –

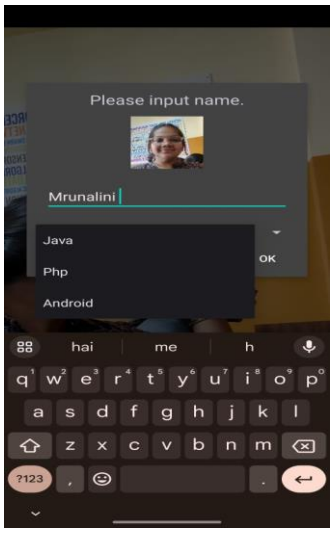
I. Courses



II. Login & Registration

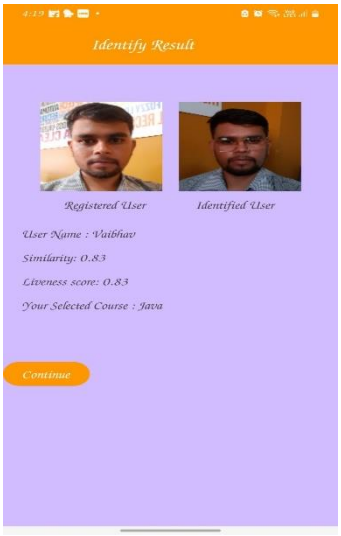
III. Face Recognition

IV. Enter Details & Course



IV. Login successful

VI. Course access



RESULT

The Face Recognition System for Identity Theft Protection in Online Education project successfully developed the potential of Face Recognition System technology to safeguard online education platforms from unauthorized access and revenue loss. By leveraging the capabilities of facial recognition algorithms, the project sought to develop a system that could accurately and efficiently verify user identities, thereby preventing fraudulent access to paid course materials. The project's findings held significant implications for the online education industry, demonstrating the feasibility of utilizing face recognition technology to enhance Safety and protect intellectual property. Moreover, the system provided a valuable framework for developing and implementing scalable and efficient user authentication and access control solutions. Furthermore, it highlighted the capacity of the face recognition technology to improve the overall user experience and foster trust within the online education community. Overall, the Face Recognition System for Identity Theft Protection project made significant contributions to the field of computer science and the online education industry, with the aim of positively

impacting society as a whole.

REFERENCES

[1] Face Recognition System for Financial Identity Theft Protection, author:Thidarat Pinthong', Worawut Yimyam², Narumol Chumuang², Mahasak Ketcham

[2] Lerner, J., Schoar, A. (2005). Does legal enforcement affect financial transactions? The contractual channel in private equity. The Quarterly Journal of Economics, 120(1), 223-246.

[3] Patil, N., Bhise, A., & Tiwari, R. K. (2022). GRAPE QUALITY PREDICTION WITH PRE-POST HARVESTING USING FUSION DEEP LEARNING. International Journal of Food and Nutritional Sciences. 11(5). 2320 7876.

[4] Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., ... Sudjianto, A. (2007, October). Wirevis: Visualization of categorical, time-varying data from financial transactions. In 2007 IEEE Symposium on Visual Analytics Science and Technology (pp. 155-162). IEEE.Lov Kumar1, Quality Assessment of Web Services using multivariate adaptive regression splines Dept. CSE National Institute of Technology, Rourkela lovkumar505@gmail.com, 2015
IEEE

[5] Laurie, S., Mortimer, K. (2019). How to achieve true integration: the impact of integrated marketing communication on the client/agency relationship. Journal of Marketing Management, 35(3-4), 231-252.

[6] Wang, X., Wang, Y., Zhu, X., Luo, C. (2020). A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. Optics and Lasers in Engineering, 125, 105851.

[7] S. Jadhav. Gesture Voice: Revolutionizing Human-Computer Interaction with an AI-Driven Virtual Mouse System. (2024), Turkish Online Journal of Qualitative Inquiry, 15(3), https://doi.org/10.53555/tojqi.v15i3.10282

[8] K Chude, A Karwa, M Sah. (2022). Multi-factor Authentication for Physical Access. International Journal of Scientific Research in Engineering and Management (IJSREM), 6(5).

[9] Patil, N., Bhise, A., & Tiwari, R. K. (2023). GRAPE QUALITY PREDICTION IN PRE - POST HARVESTING WITH IMPLEMENTATION OF FUSION DEEP LEARNING. Journal of Analysis and Computation (JAC). 0973-2861

[10] Li, G., Zhang, Z., Zhang, J., Hu, A. (2020). Encrypting wireless communications on the fly using one-time pad and key generation. IEEE Internet of Things Journal.

[11] Argyris, A., Pikasis, E., Syvridis, D. (2016). Gb/s one-time pad data encryption with synchronized chaos-based true random bit generators. Journal of Lightwave Technology, 34(22), 5325-533 1.

[12] Chen,F. L., Liu, W. F., Chen, S. G., Wang, Z. H. (2018). Public-key quantum digital signature scheme with onetime pad private-key. Quantum Information Processing , 17(1), 10

[13] Gulve, S. (2020). Image Scene Understanding-Object Detection in Aerial Images using Convolutional Neural Networks. *International Journal for Sci. Res. & Dev*, *8*(10), 194-197.

[14] Patil, N., Bhise, A., & Tiwari, R. K. (2024). Fusion deep learning with pre-post harvest quality management of grapes within the realm of supply chain management. *The Scientific Temper*, *15*(01), 1764–1772. https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.1.26

[15] N. Patil, R. K. Tiwari and A. Kumar, "Pre and Post Harvesting using Deep Learning Techniques: A comprehensive study," *2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, Jamshedpur, India, 2022, pp. 207-211, doi: 10.1109/ICRTCST54752.2022.9781959.