International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE AND REAL-TIME 1-TO-N FACE RECOGNITION SYSTEM FOR WEB-BASED USER AUTHENTICATION

E. MOUNIKA REDDY [1], RAKHASHI NIKHITA [2], PINGILI LAKSHMI DEEKSHITHA REDDY [3], JATAVATH MADHU [4], ADUPALA RAM CHARAN REDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In traditional user authentication systems, identity verification is commonly based on textual inputs like usernames, passwords, or personal IDs, which are often vulnerable to misuse, forgetfulness, or theft. Existing systems that attempt face-based recognition either store static images or depend on manual matching, lacking automation and real-time detection capabilities. These approaches do not support live face capturing and fail to fetch dynamic user-related information from a database, resulting in inefficient or insecure identification mechanisms. The proposed system addresses these limitations by introducing a live face capturing and identification framework integrated with OpenCV. When a user registers, their face is captured in real-time using the system's web interface connected to the webcam through OpenCV. The captured image is then stored securely in the server's file system or database. During login or verification, the system again uses OpenCV to capture a fresh face image and compares it with stored images using face similarity techniques. Upon successful matching, all relevant user information is dynamically fetched from the database and displayed securely on the interface. This system ensures that only the rightful user gains access to sensitive data, enhancing both security and user experience. The modular architecture seamlessly integrates live camera input via OpenCV, secure data storage, and efficient face comparison logic, offering an intelligent and

real-time authentication mechanism suitable for modern web applications.

Index Terms – Face recognition, user authentication, OpenCV, biometric authentication, live face capture, facial verification, real-time identification, secure login system, image matching, database integration, computer vision, web-based security.

I. INTRODUCTION

Face identification is a pivotal component in numerous real world applications, serving as a cornerstone for user authentication in various domains. With the exponential growth of digital services and the proliferation of smart devices, the demand for robust and efficient face identification protocols has never been greater because they do not require 1, complex hardware [48]. From unlocking smartphones to securing access to sensitive facilities, the reliance on facial recognition technology underscores its indispensable role in modern society. As face data can be considered sensitive information, it is imperative to maintain its privacy [37]. Research on privacy-preserving face identification aims to authenticate users using facial images while safeguarding their privacy. This research can be categorized into two main areas [5]: one-to-one (1:1) and one-to-many (1:N) face identification protocols. In a 1:1 system, users register their face data and later authenticate themselves using facial recognition, with the system maintaining privacy by not storing or accessing the plain face data. This privacy-preserving approach extends to systems with multiple users, where user IDs are incorporated into registration and authentication queries to ensure confidentiality. In a 1:N system, multiple users register their face data, and individuals authenticate without the system knowing their identity among the registered users, further enhancing privacy while maintaining the security of the authentication process. Initiated by the work of Erkin et al. [19], numerous works have proposed explicit schemes for 1:N private face identification protocols. To the best of our knowledge, the state-of-the-art scheme is the CryptoMask scheme [3], recently proposed by Bai et al. in 2023.

All these previous works utilized homomorphic encryption as the main tool to achieve privacy. Due to the inherent inefficiency of homomorphic encryption, these result in somewhat inefficient protocols, with the only exception of CryptoMask, which still uses homomorphic encryption but combines this with other

techniques to obtain an efficient scheme. CryptoMask requires only around 0.2 second for N =1,000 registered users and 1.4 second and 11 seconds for N =10,000 and N = 100,000 registered users, respectively, to authenticate one user.

II. RELATED WORK

A. *CryptoMask: Privacy-preserving face recognition*

Face recognition is a widely-used technique for identification or verification, where a verifier checks whether a face image matches anyone stored in a database. However, in scenarios where the database is held by a third party, such as a cloud server, both parties are concerned about data privacy. To address this concern, we propose CryptoMask, a privacy-preserving face recognition system that employs homomorphic encryption (HE) and secure multi-party computation (MPC). We design a new encoding strategy that leverages HE properties to reduce communication costs and enable efficient similarity checks between face images, without expensive homomorphic rotation. Additionally, CryptoMask leaks less information than existing state-of-the-art approaches. CryptoMask only reveals whether there is an image matching the query or not, whereas existing approaches additionally leak sensitive intermediate distance information. We conduct extensive experiments that demonstrate CryptoMask's superior performance in terms of computation and communication. For a database with 100 million 512-dimensional face vectors, CryptoMask offers ≈5 times and ≈144 times speed-ups in terms of computation and communication, respectively.

B. *A review on protection and cancelable techniques in biometric systems*

An essential part of cloud computing, IoT, and in general the broad field of digital systems, is constituted by the mechanisms which provide access to a number of services or applications. Biometric techniques aim to manage the access to such systems based on personal data; however, some biometric traits are openly exposed in the daily life, and in consequence, they are not secret, e.g., voice or face in social networks. In many cases, biometric data are non-cancelable and non-renewable when compromised. This document examines the vulnerabilities and proposes hardware and software countermeasures for the protection and confidentiality of biometric information using randomly created supplementary information. Consequently, a taxonomy is proposed according to the operating principle

and the type of supplementary information supported by protection techniques, analyzing the security, privacy, revocability, renewability, computational complexity, and distribution of biometric information. The proposed taxonomy has five categories: 1) biometric cryptosystems; 2) cancelable biometrics; 3) protection schemes based on machine learning or deep learning; 4) hybrid protection schemes; and 5) multibiometric protection schemes. Furthermore, this document proposes quantitative evaluation measures to compare the performance of protection techniques. Likewise, this research highlights the advantages of injective and linear mapping for the protection of authentication and identification systems, allowing the non-retraining of these systems when the protected biometric information is canceled and renewed. Finally, this work mentions commercial products for cancelable biometric systems and proposes future directions for adaptive and cancelable biometric systems in low-cost IoT devices.

C. Grote: Group testing for privacy-preserving face identification

This paper proposes a novel method to perform privacy-preserving face identification based on the notion of group testing, and applies it to a solution using the Cheon-Kim-Kim-Song (CKKS) homomorphic encryption scheme. Securely computing the closest reference template to a given live template requires K comparisons, as many as there are identities in a biometric database. Our solution, named Grote, replaces element-wise testing by group testing to drastically reduce the number of such costly, non-linear operations in the encrypted domain from K to up to $2\sqrt{K}$. More specifically, we approximate the max of the coordinates of a large vector by raising to the α-th power and cumulative sum in a 2D layout, incurring a small impact in the accuracy of the system while greatly speeding up its execution. We implement Grote and evaluate its performance.

D. Ulixes: Facial recognition privacy with adversarial machine learning

Facial recognition tools are becoming exceptionally accurate in identifying people from images. However, this comes at the cost of privacy for users of online services with photo management (e.g. social media platforms). Particularly troubling is the ability to leverage unsupervised learning to recognize faces even when the user has not labeled their images. In this paper we propose Ulixes, a strategy to generate visually non-invasive facial noise masks that yield adversarial examples, preventing the

formation of identifiable user clusters in the embedding space of facial encoders. This is applicable even when a user is unmasked and labeled images are available online. We demonstrate the effectiveness of Ulixes by showing that various classification and clustering methods cannot reliably label the adversarial examples we generate. We also study the effects of Ulixes in various black-box settings and compare it to the current state of the art in adversarial machine learning. Finally, we challenge the effectiveness of Ulixes against adversarially trained models and show that it is robust to counter measures.

III. PROPOSED METHODOLOGY

The proposed system introduces a smart, real-time facial authentication platform powered by OpenCV for live video capture. Unlike static verification models, this approach uses dynamic face input directly from a connected camera, ensuring the user is physically present during authentication. When a user registers, their facial features are captured through OpenCV's real-time stream, processed, and securely stored.

During verification, the system captures a new live image, compares it against stored entries using facial similarity algorithms, and, upon a successful match, auto-fetches personalized data from the database tied to that user. The design ensures seamless integration of facial recognition with dynamic content delivery, improving not only the accuracy of the identification process but also the overall user experience and security posture of the system.

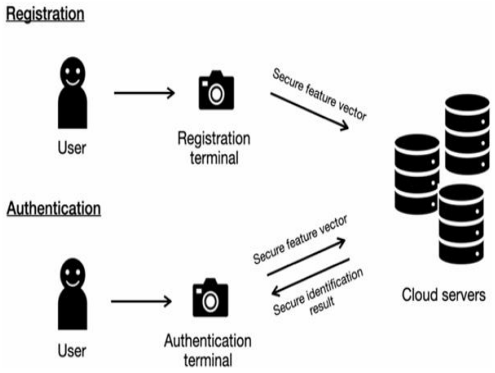
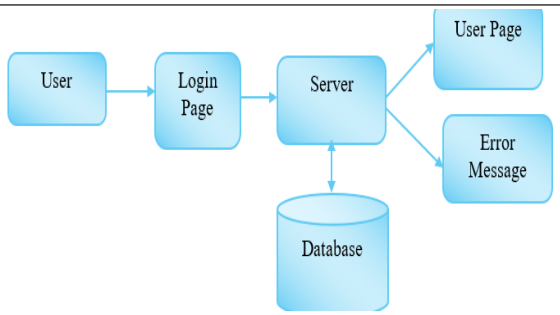


Fig. 1: System Overview

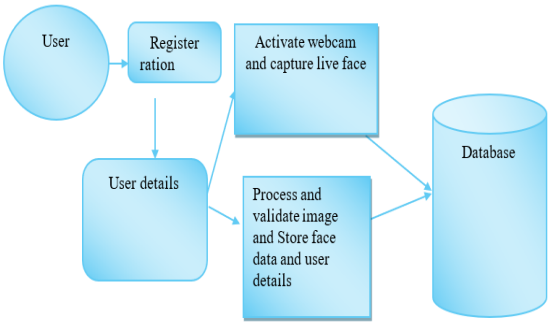
3.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



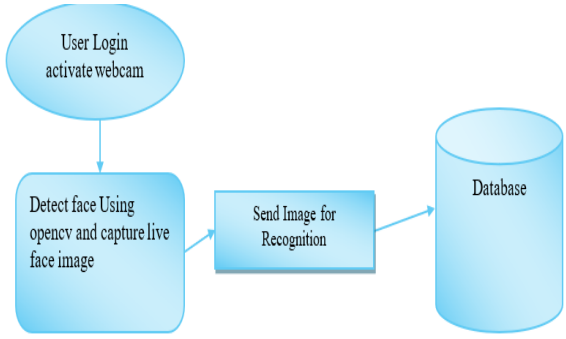
3.2 User Registration Module

This module is responsible for enrolling new users into the system. During registration, the user provides basic details and allows access to the webcam. Using OpenCV, the system captures the user's face in real time, processes it, and securely stores the facial image along with user information in the server file system or database. This stored facial data serves as the reference for future authentication.



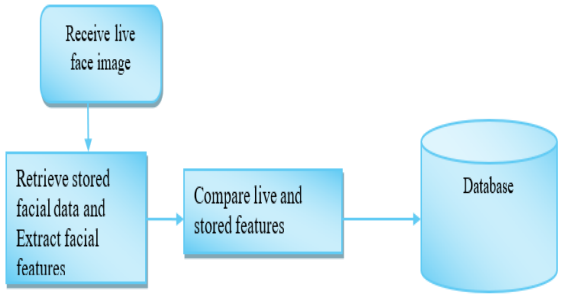
3.3 Live Face Capture Module

This module enables real-time face detection and image acquisition during authentication. It uses OpenCV to continuously access the webcam and detect the user's face, ensuring that the image is captured from a live person rather than a static photograph. This improves security and prevents spoofing attacks.



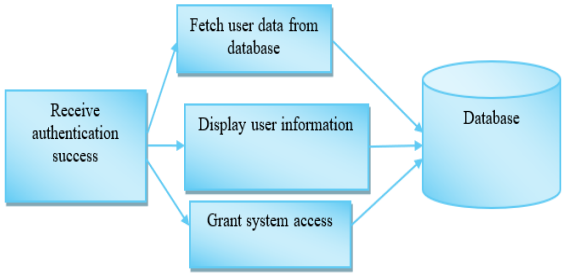
3.4 Face Recognition and Matching Module

This module performs the core authentication task by comparing the live captured face with the stored facial data of registered users. Face similarity algorithms are applied to calculate a matching score. If the similarity score exceeds a predefined threshold, the user is considered valid; otherwise, access is denied.



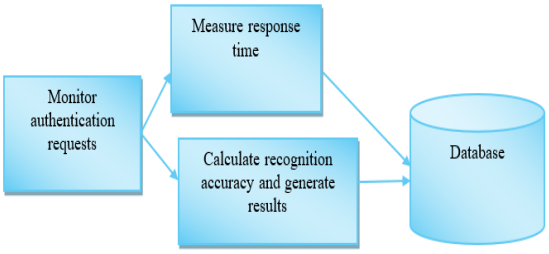
3.5 Secure Authentication and Data Retrieval Module

This module manages access control after successful face recognition. Once authenticated, it creates a secure session for the user and retrieves the corresponding user information from the database. The retrieved data is displayed securely on the interface, ensuring confidentiality and integrity.



3.6 System Monitoring and Performance Evaluation Module

This module evaluates the overall performance of the system by monitoring parameters such as face recognition accuracy, authentication time, and system reliability. It helps assess the effectiveness of the real-time face authentication mechanism and supports comparison with traditional authentication methods.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed **OpenCV-based face recognition system** can accurately identify users in real time by comparing live facial images with stored database records. It improves security by reducing dependence on passwords and allowing only authorized users to access sensitive information. The system also supports dynamic retrieval of user details after successful verification. Overall, it provides a reliable and efficient solution for web-based user authentication.



Fig. 2: Registration

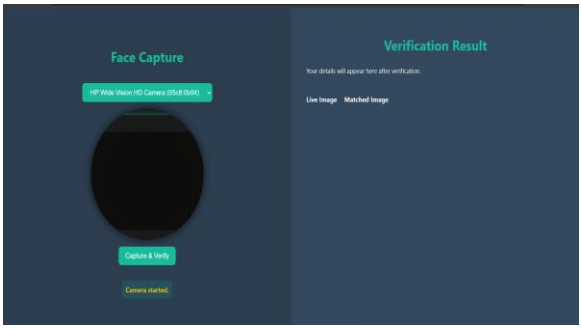


Fig. 3: Capture Face



Fig. 5: Verification Result

V. CONCLUSION

This work presented novel private 1:N face identification protocols based entirely on secure multi-party computation (MPC), demonstrating that strong privacy guarantees and practical performance can coexist. The first protocol achieves full privacy protection of facial data and performs efficiently for small-scale databases, while the second protocol strategically allows limited leakage to enable scalable identification, achieving real-time performance even with 30,000 users. By integrating live face capture and recognition using OpenCV, the proposed system overcomes limitations of traditional authentication methods that rely on static credentials or stored images. Unlike existing approaches that lack automation, real-time detection, or theoretical privacy guarantees, this framework supports dynamic face acquisition, secure comparison, and instant retrieval of user information. The experimental results and comparisons with prior MPC- and HE-based solutions confirm that the proposed protocols offer a superior balance between privacy, efficiency, and usability, making them well suited for real-world, large-scale authentication scenarios.

REFERENCES

[1] 2025. [Online]. Available: https://www.transfermarkt.co.uk/premier-league/besucherzahlen/wettbewerb/GB1/plus/?saison_id=2023

[2] 2025. [Online]. Available: http://www.espn.com/mlb/attendance VOLUME 6, 2025

[3] J. Bai, X. Zhang, X. Song, H. Shao, Q. Wang, S. Cui, and G. Russello, "CryptoMask: Privacy-preserving face recognition," in Proc. Int. Conf. Inf. Commun. Secur., Singapore, 2023, pp. 333–350.

[4] D. Beaver, "Efficient multiparty protocols using circuit randomization, in Proc. Adv. Cryptol., Heidelberg, Germany, 1992, pp. 420–432.

[5] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega, "A review on protection and cancelable techniques in biometric

systems," IEEE Access, vol. 11, pp. 8531–8568, 2023.

[6] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," IEEE Signal Process. Mag., vol. 30, no. 2, pp. 42–52, Mar. 2013.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. RAKHASHI NIKHITA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. PINGILI LAKSHMI DEEKSHITHA REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. JATAVATH MADHU pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. ADUPALA RAM CHARAN REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.