IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13377

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

R. Sowmya[1], Niraj Kumar Patel[2], Rahul Pratap Shah[3], P. Sai Teja[4]

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[1]

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[2-4]

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.

I. INTRODUCTION

Face identification is a pivotal component in numerous real world applications, serving as a cornerstone for user authen tication in various domains. With the exponential growth of digital services and the proliferation of smart devices, the demand for robust and efficient face identification pro tocols has never been greater because they do not require 1, complex hardware [48]. From unlocking smartphones to se curing 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 confi dentiality. 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 identi f ication protocols [3], [6], [9], [17], [25], [28], [33], [41], [47]. 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 =1,000registeredusersand1.4secondand11secondsfor N =10,000 and N = 100,000 registered users, respectively, to authenticate one user.

In today's digital world, secure user authentication has become a critical requirement for web-based systems and online services. Traditional authentication methods such as usernames, passwords, PINs, and security questions are widely used but suffer from major limitations. These credentials can be easily forgotten, stolen, guessed through brute-force attacks, or shared with unauthorized individuals. As cyber threats continue to grow, relying solely on text-based authentication is no longer sufficient to ensure system security. Biometric authentication has emerged as a powerful alternative, as it verifies identity using unique biological traits such as fingerprints, iris patterns, voice, and facial features. Among these,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13377

face recognition is one of the most convenient and user-friendly techniques because it is contactless, natural, and does not require specialized hardware beyond a camera.

II. RELATED WORK

Several researchers have explored advanced authentication mechanisms to secure web-based systems and cloud platforms. Biometric authentication models have gained significant attention due to their ability to provide stronger identity verification compared to traditional password-based methods. Among these, face recognition systems have been widely studied for their convenience and non-intrusive nature. These systems enable automated user verification by analyzing facial features captured through cameras. However, traditional face recognition systems often rely on static verification methods and may face challenges related to scalability, spoofing attacks, and real-time performance.

Recent studies have proposed multi-factor authentication approaches that integrate biometric recognition with additional verification factors such as passwords, tokens, or one-time passwords. While these methods enhance system security, they may also introduce additional computational overhead and user interaction complexity in large-scale web applications.

To address these challenges, researchers have begun exploring intelligent and adaptive authentication frameworks that incorporate machine learning and behavioral analysis to improve authentication reliability. Real-time biometric recognition systems, particularly those based on deep learning techniques, have demonstrated improved accuracy in identifying users across large databases using 1-to-N matching approaches. These systems compare an input facial image against multiple stored templates to identify the correct user. However, ensuring secure storage, fast processing, and resistance to spoofing attacks remains a critical challenge.

The main objective of this research is to design a **secure and real-time 1-to-N face recognition system for web-based user authentication**. The proposed system aims to enhance authentication security by integrating deep learning–based face recognition with secure data protection mechanisms. The system focuses on extracting unique facial features and comparing them with a database of registered users to perform rapid identification. It incorporates anti-spoofing mechanisms to prevent attacks such as photo, video replay, and impersonation.

The scope of the research includes developing a scalable face recognition architecture capable of performing efficient 1-to-N matching in real time for large user databases. The system also integrates encryption techniques to securely store facial templates and user credentials. Advanced feature extraction methods and neural network models are used to improve recognition accuracy under varying lighting conditions, facial expressions, and pose variations.

Additionally, the system includes a decision-making module that analyzes authentication attempts and detects suspicious activities using machine learning techniques. This helps mitigate threats such as spoofing, brute-force login attempts, and unauthorized access. The project also focuses on implementing secure communication protocols for transmitting authentication data between the client and the server.

Performance evaluation is conducted by testing the system under different real-time scenarios and potential attack conditions. The research ultimately aims to provide a **highly secure, scalable, and user-friendly authentication solution** that improves access control, data privacy, and system reliability for modern web-based applications.

III. LITERATURE SURVEY

Based on the backgrounds described above, we ask the fol lowing research questions in this article: RQ1: Can wedesign an efficient 1:N private face identi f ication protocol without homomorphic encryption? RQ2: Can we find an approach that balances privacy properties and identification time for a 1:N private face identification protocol? We address these questions through cryptographic re search. Our goal is to design a private face identification protocol based on more light-weighted cryptographic tools, especially without relying on homomorphic encryption. Al though several works [6], [9], [25], [28] already utilize other cryptographic tools, parts of the procedures for these works are still based on homomorphic encryption. Our pri mary motivation is, consequently, to design a 1:N private face identification protocol protocol without homomorphic encryption. Meanwhile, improving computational efficiency could be possible through a moderate relaxation of privacy measures. Several recent works [17], [33], [41] have succeeded in significantly improving identification time by leaking some information, as discussed below. However, the amount of leakage in these schemes may be somewhat large. To mini mize leakage while achieving fast protocols, we aim to find an efficient scheme that strikes a balance between efficiency and privacy in real-world applications.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13377

Title: Crypto Mask: Privacy-preserving face recognition,

Author: J. Bai, X. Zhang, X. Song, H. Shao, Q. Wang, S. Cui, and G. Russello.

Year: 2023.

Description:
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 {\thicksim}5 \times and {\thicksim}144 \times speed-ups in terms of computation and communication, respectively.

Title: A review on protection and cancelable techniques in biometric systems.

Author: J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega.

Year: 2023.

Description:
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.

Title: “Ulixes: Facial recognition privacy with adversarial machine learning.

Author: T. Cilloni, W. Wang, C. Walter, and C. Fleming.

Year: 2022.

Description:
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.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13377

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. Finally, we challenge the effectiveness of Ulixes against adversarially trained models and show that it is robust to countermeasures.

Title: HERS: Homomor phically encrypted representation search.

Author: J. Engelsma, A. Jain, V. Boddeti, and J. Engelsma.

Year: 2022.

Description:
We present a method to search for a probe (or query) image representation against a large gallery in the encrypted domain. We require that the probe and gallery images be represented in terms of a fixed-length representation, which is typical for representations obtained from learned networks. Our encryption scheme is agnostic to how the fixed-length representation is obtained and can therefore be applied to any fixed-length representation in any application domain. Our method, dubbed HERS (Homomorphically Encrypted Representation Search), operates by (i) compressing the representation towards its estimated intrinsic dimensionality with minimal loss of accuracy (ii) encrypting the compressed representation using the proposed fully homomorphic encryption scheme, and (iii) efficiently searching against a gallery of encrypted representations directly in the encrypted domain, without decrypting them.

IV. PROPOSED WORK

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.

V. PROPOSED SYSTEM ADVANTAGES

- Live Face Detection: Uses OpenCV to capture and process facial data directly from the user's webcam.
- Real-Time Verification: Matches faces instantly at the time of login without manual review.
- Dynamic Data Retrieval: Automatically fetches associated user data from the database on successful recognition.
- High Security: Reduces risk of spoofing and unauthorized access by requiring physical presence.
- Modular & Extendable: The architecture allows easy addition of new features like liveness detection or role-based access.

The LBPH algorithm
The Local Binary Patterns Histograms (LBPH) algorithm is a classical and widely used method for face recognition, particularly suited for real-time applications with constrained hardware. At its core, LBPH is a *texture-based* feature extraction technique that captures the local patterns in a face image by analyzing the relationships between each pixel and its neighbouring pixels. The algorithm begins by converting a face image to grayscale, since color information is not necessary for capturing the texture features that distinguish one face from another. For every pixel in the image, LBPH examines a small neighbourhood — typically a 3×3 window — and compares the central pixel's intensity value with each of its eight surrounding pixels. For each neighbour, if the intensity value is greater than or equal to the centre pixel, the comparison yields a binary value of 1; otherwise, it yields 0. These individual binary outcomes are then concatenated in a predetermined order (such as clockwise) to form an 8-bit binary pattern (for example, 11100011), which is then converted into a single decimal number between 0 and 255.

Once every pixel has been processed in this way across the entire face image, the result is a new representation where each pixel encodes a local binary pattern. The next important step is to divide this LBP-encoded image into a grid of cells — for example 8×8 or 7×7 partitions — so that spatial information about the distribution of texture patterns is preserved. In each cell, a histogram is computed over all the LBP codes (from 0 to 255) that occur in that cell, effectively summarizing how frequently each local pattern appears in that region. These histograms are then concatenated across all

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13377

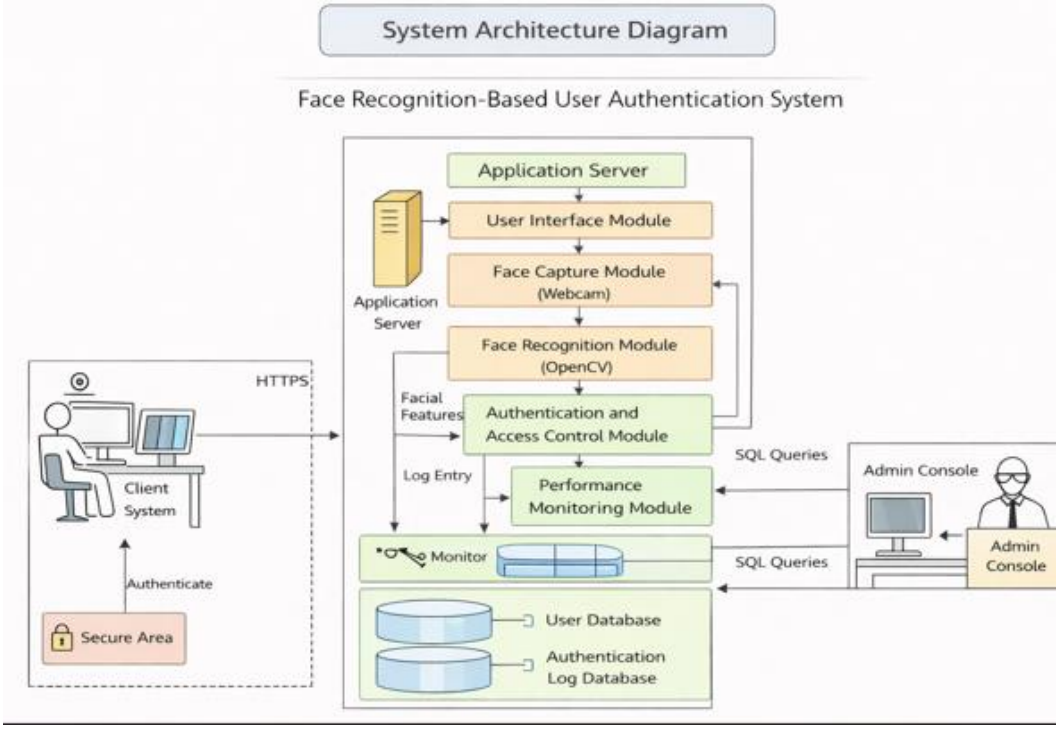
cells to form a single high-dimensional feature vector for the face image. This feature vector captures both the *local texture distribution* and rough spatial layout of important facial features, and it becomes the representative descriptor used for recognition.

During the training phase, LBPH calculates and stores the histograms for all labeled face images in a database, linking each histogram vector to an identity label.

In the recognition phase, when a new face image (e.g., from a webcam feed) is input into the system, it undergoes the same process of grayscale conversion, LBP pattern computation, cell partitioning, and histogram extraction to generate its feature vector. The system then compares this vector against the stored vectors in the training set, using a suitable distance metric — such as chi-square distance, Euclidean distance, or absolute difference — to quantify similarity. The stored histogram with the smallest distance to the query histogram indicates the closest match, and its associated label is returned as the recognized person's identity. By focusing on *local texture features* rather than global pixel intensity values, LBPH inherently exhibits robustness to variations in lighting and monotonic grayscale changes because the binary comparisons remain relatively stable under such transformations. The ability to extract discriminative features at a local level also helps the algorithm handle small facial variations and partial occlusions.

The LBPH algorithm is not based on deep learning or neural networks; instead, it is a hand-crafted feature descriptor, which makes it computationally efficient and easy to implement with libraries such as OpenCV. OpenCV natively provides an implementation as cv2.face.LBPHFaceRecognizer_create() (or related API versions), which encapsulates the feature extraction and matching pipeline and allows for incremental training updates. LBPH's simplicity and speed make it particularly effective in controlled environments and real-time systems where high throughput and low latency are critical, such as surveillance cameras, human-computer interface systems, and automated attendance applications. Its performance, however, may be less accurate on large, unconstrained datasets compared to modern deep learning-based approaches, but its explainability and lightweight nature remain strong advantages for many practical real-time recognition scenarios.

System Architecture



The **system architecture of the "Secure and Real-Time 1-to-N Face Recognition System for Web-Based User Authentication"** consists of several interconnected components that work together to verify a user's identity securely and efficiently. The process begins at the **client system**, where a user attempts to access a protected web application through a secure **HTTPS connection**. When the user initiates authentication, the system activates the **User Interface**

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13377

Module on the application server, which provides the web interface for interaction. Through this interface, the **Face Capture Module** accesses the device webcam to capture the user's facial image in real time. The captured image is then passed to the **Face Recognition Module**, typically implemented using computer vision libraries such as OpenCV or deep learning–based models, which extracts unique facial features from the image.

Our Main Idea. Filtering via Binarization: To address the above issue, our main idea (for the second protocol) is to produce a smaller set of "candidates" among the registered ones to be compared with the extracted feature vector to be authenticated. Assume that we could produce such a set of candidates, the expensive computation for securely computing cosine similarities is now required only for this smaller set, and hence the whole computation will be much faster. To obtain the candidate set, given the extracted feature vector to be authenticated, we propose to "binarize" the extracted feature vectors (both the feature vector to be authenticated and those in the registered database) and compare them using the Hamming distance. Computing the Hamming distance is much faster than the cosine similarities/distances in MPC. We then take only the top k registered features vectors that are closest, as per Hamming distance, to the one to be authenti cated, as the candidate set. More precisely, the "binarization" process renders the input feature vector, which have integer values, into binary values (Boolean) by comparing the values with zero. In terms of machine learning, this approach use the "sign" function as the learning process. With this "filtering", we must be careful that this separated process of learning.

will have a strong correlation to cosine similarities (otherwise we would not be able to use this filtering in the first place), so that we will have high accuracy in identification. We ensure this via experiments, showing that we achieve high accuracy of approximately 94% in identification when filtering about just over 0.5% . We show this in Section V. With the candidate set being only 0.5% size of the whole registered set, the MPC protocol for computing cosine distances and identifying the closest one among the candidate set is much faster than doing for the whole set. We also take a step further to enable an even faster proto col by observing that binarization to Boolean values already serves as a lossy function, where the information regarding face features is obfuscated in the process. We hence open the Hamming distances to plaintext values and compare them in the clear. This is much faster than comparing them in MPC. Importantly, note that the computation of the Hamming dis tances themselves is done in MPC, and hence the extracted feature vectors are not exposed. Only their respective Ham ming distances to others become public. We discuss some consequences of this partial leakage in Section IV-B.We also note while the Hamming distances in the filtering step are opened, the cosine distances in the final step are fully private.

Overall, the architecture is designed to ensure **real-time performance, scalability, and strong security** for web-based authentication systems. By integrating secure communication protocols, facial biometric recognition, database management, and administrative monitoring, the system provides an efficient solution for verifying user identities. The use of **1-to-N face recognition** enables quick identification among multiple registered users, while secure data storage and logging mechanisms ensure data integrity, privacy, and protection against unauthorized access. This architecture therefore supports reliable and secure authentication for modern web applications.

VI. CONCLUSION

The **Secure and Real-Time 1-to-N Face Recognition System for Web-Based User Authentication** provides an efficient and reliable solution for verifying user identities in modern web applications. Traditional authentication methods such as passwords and PINs are often vulnerable to attacks like brute force, phishing, and credential theft. By integrating biometric authentication through facial recognition, the proposed system significantly enhances security while maintaining a convenient and user-friendly authentication process. The system captures facial images through a webcam, extracts unique facial features using computer vision techniques, and performs 1-to-N matching against stored templates in the database to accurately identify users.

Overall, the proposed system improves the reliability, scalability, and security of user authentication mechanisms. By leveraging biometric technology and real-time processing, it reduces dependency on traditional credentials and enhances protection against unauthorized access. The system therefore represents a practical solution for organizations and applications that require strong and convenient user authentication.

VII. FUTURE ENHANCEMENT

Although the proposed system provides strong security and efficient performance, several enhancements can further improve its functionality and robustness. One potential improvement is the integration of **advanced deep learning models** for face recognition, which can increase accuracy in challenging conditions such as low lighting, facial occlusion, or varying camera angles. Implementing **liveness detection techniques** can also help prevent spoofing attacks that use photos, videos, or masks to bypass the authentication system.

DOI: 10.17148/IARJSET.2026.13377

Further improvements may include optimizing the system for **mobile devices and cross-platform web applications**, enabling users to authenticate securely using smartphones or tablets. Privacy-preserving techniques such as encrypted facial templates and secure biometric data storage can also be implemented to strengthen data protection. These future developments will enhance the system's reliability, scalability, and adaptability, making it suitable for a wide range of secure digital applications.

REFERENCES

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

[2]. 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.

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

[4]. 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 Ac cess, vol. 11, pp. 8531–8568, 2023.

[5]. 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.

[6]. O. Catrina and S. de Hoogh, "Secure multiparty linear programming using fixed-point arithmetic," in Proc. Eur. Symp. Res. Comput. Secur., Berlin, Germany, 2010, pp. 134–150.

[7]. M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Pri vacy preserving face recognition utilizing differential privacy," Comput. Secur., vol. 97, 2020, Art. no. 101951.

[8]. H. Chun, Y. Elmehdwi, F. Li, P. Bhattacharya, and W. Jiang, "Out sourceable two-party privacy-preserving biometric authentication," in Proc. 9th ACM Symp. Inf., Comput. Commun. Secur., 2014, pp. 401–412.

[9]. T. Cilloni, W. Wang, C. Walter, and C. Fleming, "Ulixes: Facial recognition privacy with adversarial machine learning," Proc. Privacy Enhancing Technol., vol. 2022, no. 1, pp. 148–165, 2022.

[10]. R. Cramer, I. Damgård, and J. B. Nielsen. Secure Multiparty Computa tion and Secret Sharing, New York, NY, USA: Cambridge Univ. Press, 2015.

[11]. I. Damgård, M. Geisler, and M. Krøigaard, "Efficient and secure comparison for on-line auctions," in Proc. Inf. Secur. Privacy: 12th Australas. Conf., Heidelberg, Germany, 2007, pp. 416–430.

[12]. A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satya narayanan, "Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops, 2017, pp. 1387–1396.

[13]. J. Deng, J. Guo, X. Niannan, and S. Zafeiriou, "Arcface: Additive an gular margin loss for deep face recognition," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., 2019, pp. 4690–4699.

[14]. N. Dowlin et al., "CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy," in Proc. Int. Conf. Mach. Learn., 2016, pp. 201–210.

[15]. P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, and C. Busch, "On the application of homomorphic encryption to face identification," in Proc. Int. Conf. Biometrics Special Int. Group, 2019, pp. 1–5.

[16]. J. Engelsma, A. Jain, V. Boddeti, and J. Engelsma, "HERS: Homomor phically encrypted representation search," IEEE Trans. Biom., Behav., Ident. Sci., vol. 4, no. 3, pp. 349–360, Jul., 2022.

[17]. Á. Erdélyi, T. Barat, P. Valet, T. Winkler, and B. Rinner, "Adaptive cartooning for privacy protection in camera networks," in Proc. IEEE 11th Int. Conf. Adv. Video Signal Based Surveill., 2014, pp. 44–49.

[18]. Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Proc. 9th Int. Symp. Privacy Enhancing Technol, Heidelberg, Germany, 2009, pp. 235–253.

[19]. D. Evans, V. Kolesnikov, and M. Rosulek, "A pragmatic introduction to secure multi-party computation," Found. Trends Privacy Secur.,vol.2, no. 2/3, pp. 70–246, 2018.

[20]. [21] L. Fan, "Image pixelization with differential privacy, in Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy, 2018, pp. 148–162.

[21]. L. Fan, "Practical image obfuscation with provable privacy," in Proc. Int. Conf. Mach. Learn., 2019, pp. 784–789.

[22]. H. Fradi, V. Eiselein, I. Keller, J.-L. Dugelay, and T. Sikora, "Crowd context-dependent privacy protection filters," in Proc. 18th Int. Conf. Digit. Signal Process., 2013, pp. 1–6.

[23]. O. Goldreich, Foundations of Cryptography: Basic Applications,vol.2. Cambridge, UK: Cambridge Univ. Press, 2004.

[24]. M.Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryp tion," Pattern Recognit., vol. 67, pp. 149–163, 2017.

DOI: 10.17148/IARJSET.2026.13377

[25]. H. Gunasinghe and E. Bertino, "PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 4, pp. 1042–1057, Apr. 2018. 984

[26]. Y. Guo, L. Zhang, Y. Hu, X. He, and J. Gao, "MS-CELEB-1M: A dataset and benchmark for large-scale face recognition, in Proc. 14th Eur. Conf. Comput. Vis., 2016, pp. 87–102.

[27]. A. Ibarrondo, H. Chabanne, V. Despiegel, and M. Önen, "Grote: Group testing for privacy-preserving face identification," in Proc. 13th ACM Conf. Data Appl. Secur. Privacy, 2023, pp. 117–128.

[28]. H. Kaur and P. Khanna, "Privacy preserving remote multi-server bio metric authentication using cancelable biometrics and secret sharing," Future Gener. Comput. Syst., vol. 102, pp. 30–41, 2020.

[29]. H. Kikuchi, K. Nagai, W. Ogata, and M. Nishigaki, "Privacy-preserving similarity evaluation and application to remote biometrics authentica tion," in Proc. 5th Int. Conf. Model. Decis. Artif. Intell., 2008, pp. 3–14.

[30]. B. Knott, S. Venkataraman, A. Hannun, S. Sengupta, M. Ibrahim, and L. van der Maaten, "Crypten: Secure multi-party computation meets machine learning," in Proc. Adv. Neural Inf. Process. Syst. 34: Ann. Conf. Neural Inf. Process. Syst., pp. 4961–4973, 2021.

[31]. K. Kobayashi, K. Iwamura, K. Kaneda, and I. Echizen, "Surveillance camera system to achieve privacy protection and crime prevention," in Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., 2014, pp. 463–466.

[32]. J. Kolberg, P. Drozdowski, M. Gomez-Barrero, C. Rathgeb, and C. Busch, "Efficiency analysis of post-quantum-secure face template pro tection schemes based on homomorphic encryption," in Proc. Int. Conf. Biometrics Special Int. Group, 2020, pp. 1–4.

[33]. P. Korshunov and T. Ebrahimi, "Using face morphing to protect pri vacy," in Proc. IEEE 10th Int. Conf. Adv. Video Signal Based Surveill., 2013, pp. 208–213.

[34]. Y. Lindell, "Secure multiparty computation (MPC)," Commun. ACM (CACM), vol. 64, no. 1, pp. 86–96, 2021.

[35]. Y. Ma, L. Wu, X. Gu, J. He, and Z. Yang, "A secure face-verification scheme based on homomorphic encryption and deep neural networks," IEEE Access, vol. 5, pp. 16532–16538, 2017.

[36]. B. Meden et al., "Privacy–enhancing face biometrics: A comprehensive survey," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 4147–4183, 2021.

[37]. K. Messer, J. Matas, J. Kittler, K. Jonsson, J. Luettin, and G. Maître, "XM2VTSDB: The extended M2VTS database," in Proc. 2nd Int. Conf. Audio Video-Based Biometric Pers. Authentication, 1999, pp. 965–966.

[38]. R. B. Miller, "Response time in man-computer conversational trans actions," in Proc. 1968, Fall Joint Comput. Conf., Part I, 1968, pp. 267–277.

[39]. T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio, and K. Taka hashi, "Cancelable permutation-based indexing for secure and effi cient biometric identification," IEEE Access, vol. 7, pp. 45563–45582, 2019.

[40]. V. N. Boddeti, "Secure face matching using fully homomorphic encryp tion," in Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst., 2018, pp. 1–10.

[41]. M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI- A sys tem for secure face identification," in Proc. IEEE Symp. Secur. Privacy, 2010, pp. 239–254.

[42]. P. Paillier, "Public-key cryptosystems based on composite degree resid uosity classes," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., 1999, pp. 223–238.

[43]. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.

[44]. C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EurasipJ.Inf.Secur., vol. 2011, no. 1, pp. 1–25, 2011.

[45]. N. Ruchaud and J.-L. Dugelay, "ASePPI: Robust privacy protection against de-anonymization attacks," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops, 2017, pp. 1352–1359.

[46]. A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy preserving face recognition," in Proc. Int. Conf. Inf. Secur. Cryptol., Heidelberg, 2010, pp. 229–244.

[47]. Q. N. Tran, B. P. Turnbull, and J. Hu, "Biometrics and privacy preservation: How do they evolve?," IEEE Open J. Comput. Soc.,vol.2, pp. 179–191, 2021.

[48]. Q. N. Tran, B. P. Turnbull, M. Wang, and J. Hu, "A privacy-preserving biometric authentication system with binary classification in a zero knowledge proof protocol," IEEE Open J. Comput. Soc., vol. 3, pp. 1–10, 2022.

[49]. T. Winkler and B. Rinner, "TrustCAM: Security and privacy-protection for an embedded smart camera based on trusted computing," in Proc. IEEE 7th Int. Conf. Adv. Video Signal Based Surveill., 2010, pp. 593–600.

