HKIE THE HONG KONG INSTITUTION OF ENGINEERS 香港工程師學會

A comprehensive review of AI-powered facial recognition systems with enhanced privacy features

Praveen Kumar J[1], Anwar Basha H[2], O Pandithurai[3], G Saikrishnan[4]

[1,3] Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India.

[2] Department of Computer Science and Engineering (AI & ML), Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India.

[4] Department of Mechanical Engineering, Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India.

ABSTRACT

Facial recognition systems that use artificial intelligence (AI) have transformed a number of applications, such as identity verification, security, and surveillance. However, issues with data security and privacy have become significant obstacles. AI-driven facial recognition systems are thoroughly examined in this paper, with a particular emphasis on improved privacy features. The study examines the most cutting-edge privacy-preserving facial recognition techniques currently in use, such as homomorphic encryption, secure multi-party computation, and differential privacy. For academics, practitioners, and developers in the field, the discussion of each approach's advantages, disadvantages, and potential future paths offers insightful information.

KEYWORDS facial recognition, artificial intelligence, homomorphic encryption, differential privacy, multi-party computation

CONTACT Anwar Basha H anwar.mtech@gmail.com

Received 9 January 2026

1. Introduction

Artificial Intelligence (AI) has produced intolerably accurate and effective facial recognition systems. Facial recognition has numerous applications like identity verification, access restriction, and medical diagnosis (Fuad, 2021). With the power of AI, facial recognition systems can efficiently and automatically extract the characteristics of faces.

Traditionally, features must be manually extracted and matched in conventional facial recognition systems. Doing this is very time consuming and also often error prone. AI-powered facial recognition systems can process high volumes of data at high speed (Becerra-Riera, 2019). Nonetheless, there are also problems of bias, fairness, and privacy associated with AI-guided facial recognition systems. Facial recognition technologies must not amplify social inequities, in order to be fair and transparent in their functioning. Facial recognition systems also involve serious privacy issues. Facial recognition technologies can monitor individuals without their consent (Pagnin, 2017). Ensuring fairness, transparency, and privacy in facial recognition system development is critical.

Research is being conducted on powerful AI algorithms to mitigate bias, ensure fairness, and put privacy first. This paper gives a detailed survey of LiDAR-based techniques for facial recognition techniques. Privacy concerns represent one of the major challenges that facial recognition technologies encounter. These systems' ability to surveil and identify people without their consent raises serious ethical and legal concerns. Researchers have begun investigating new solutions that prioritise privacy without sacrificing functionality to solve these problems. Facial recognition systems protect private information and sensitive data with favourable learning and differential privacy (Yang, 2019).

To reduce the privacy threat of facial biometrics, a range of measures have already been implemented for privacy-first and utility-aware biometric recognition. Here the state of the art of privacy-preserving schemes for biometric recognition is summarised. Each country in the United Nations must adhere to ethical and legal standards for artificial intelligence in order to form a Global Community for Development and Implementation of Artificial Intelligence (AI) (McMahan, 2017).

It is imperative that the utilisation of AI within the workplace is assessed under the European Union's General Data Protection Regulation (GDPR) and the European Union's Artificial Intelligence Act in light of the fact that both recognise that the collection of personal data from persons raises three key concerns, specifically privacy, consent, and accountability.

The above will be adopted by the Global Community for Development and Implementation of AI in its operationalisation. It will be within an architecture that enables the formulation and enforcement of regulations to facilitate ethical use of AI globally as well as compliance with the local laws on data protection and fairness of AI systems. The following requirements for AI systems designated as high risk are included in the General Data Protection Regulation: clarity, fairness, dependability, and human oversight. The Institute of Electrical and Electronics Engineers (IEEE) has developed its own set of standards

for ethical AI design. This is classified as IEEE P7000. It will set out the ethical AI design principles.

AI systems should be fair, interpretable, and non-biased. An upcoming framework for AI powered facial recognition is self-supervised learning that utilises unlabelled data to pre-train and fine-tune models. The method lessens heavy dependence on costly manual annotations needed by existing datasets making model training efficient. This progress is beneficial for facial recognition since the data collections needed for this are costly and may violate privacy. The recent work showed that competitive performance can be achieved on SOTA benchmark datasets via self-supervised pre-training on unlabelled data and fine-tuning on limited labelled data. Training facial recognition systems with unlabelled data will not only result in larger and more efficient systems but also be devoid of massive labelled datasets thereby addressing the concern of privacy.

The importance of ethical guidelines and legal regulation cannot be stressed enough as facial recognition technology progresses further. All over the world, policymakers and institutions are recognising the need for setting up regulations for facial recognition technology, to ensure their ethical use and privacy rights. The frameworks stress the significance of obtaining informed consent, collecting less data, and being accountable while using AI driven systems. Collaborative academicians and claimants who bridge the research advancement with ethical and legal standards will offer future facial recognition an effective law enforcement tool to benefit society without harming privacy and fairness.

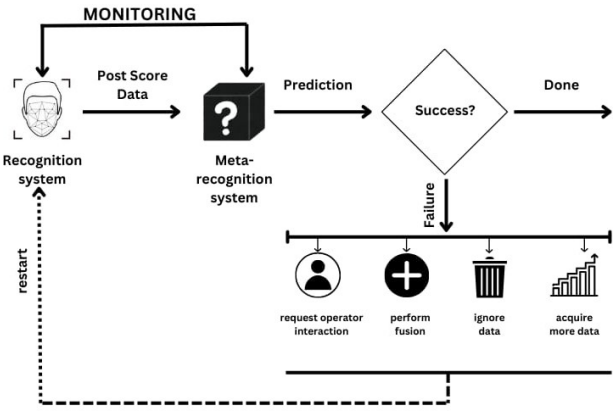

Figure 1. AI-driven facial recognition mechanism

Finding the ideal balance between accuracy, justice, and privacy is critical to the future of facial recognition technology. The development of highly accurate, transparent, and privacy-preserving systems by researchers can help to build trust and ensure the ethical application of this technology.

A thorough assessment of the most recent developments in AI-driven facial recognition is the goal of this review paper, which also focuses on improved privacy aspects. Through analysing the problems and solutions in this area, it is intended to help create facial recognition systems that are morally and practically sound.

2. Literature review

Deep learning can be considered an important part of facial recognition evolution which refers to the use of convolutional neural network (CNN)-aided deep learning algorithms for face feature extraction and face identification. According to some researchers, CNN-based facial recognition models outperform the alternatives based on various benchmark datasets (Wang, 2021). Recent methods investigated include transfer learning and fine-tuning for facial recognition. The methods utilise CNN-trained models and fine-tune the target dataset to identify individuals. The aim of this research is to enhance the facial recognition of CNN, through transfer learning. Federated learning (FL) enables models for facial recognition to be trained on edge devices while keeping the unprocessed data on the device and sending the model update to the server for aggregation. Federated Averaging is used in FL introducing noise to updates and additional clients for differential privacy (DP) and for SMPC for encrypted aggregation. FL handles data that is not identically and independently distributed and achieves high accuracy on the LFW data set and also ensures that users' sensitive data is not revealed to the server (Yang, 2019).

Pose and illumination invariant facial recognition allows accurate identification of individuals despite variations in facial lighting and positioning. To overcome this issue, a number of techniques such as 3D face models and feature extraction techniques have been developed for pose and illumination invariant facial recognition (Yang, 2022)

Multi-modal facial recognition approaches combine multiple modalities, such as face, fingerprint, and iris, to recognise individuals. Different CNN architectures have been developed for facial recognition due to deep learning. A multi-model approach combines multiple biometric features to achieve a more reliable system. The use of a multi-model strategy has been widely accepted for multi-biometric facial recognition. Multi-task learning is a technique that aims to enhance face privacy in facial recognition by simultaneously studying related tasks such as face verification and attribute prediction. Alternatively, it can involve simultaneously learning multiple related tasks so that common representations can be shared across tasks, which helps to avoid learning that is over-fitted to individual tasks' sensitive data. Models may generalise better, tasks' accuracy may improve, and privacy may be maintained through this. A frequently utilised MTL framework in supervised learning entails a deep model which shares, or partially shares, the feature extractor and each has feature heads adapting to the task to optimise their goals simultaneously (Zhang & Yang, 2021). The facial

recognition system with privacy focus will protect personal data, while also maintaining an accurate identification more or less, using methods like cryptographic protocols and by swapping data in null space which is private with public. The advent of homomorphic encryption and differential privacy has made it feasible to work on facial recognition without ever exposing individual data (Pradel & Mitchell, 2021). To improve accuracy in recognition, RNN-based facial recognition was utilised to identify temporal patterns of facial data. Models like LSTM networks and RNNs use sequential features of a face to enhance facial recognition precision of dynamic closed-set classification designs (ElGamal, 1985). FaceNet-type models learn a compact embedding while improving facial recognition precision in clustering and verification assignment (Schroff, 2015).

This CNN architecture "VGGFace" is a good network for facial recognition. VGGFace is better at extracting and recognising facial features for testing. To train a deep convolutional network, the dataset is employed. The facial recognition domain has seen many ResNet-based works. The use of deep residual learning enhances the feature representation as demonstrated by "ResNetFace". This aids recognition accuracy on difficult datasets (Jing et al, 2022). Adversarial training enhances the performance of privacy-conscious facial recognition. Examples of attacks such as FGSM or PGD introduce small changes to the input thereby causing an error in the model. Robust training against adversarial inputs solves this issue. This prevents the extraction of private data including model inversion attacks. GANs create artificial adversarial instances, leading to improved generalisation. The accuracy of the models on datasets is enhanced.

3. Key contribution and novelty

3.1. Encryption-centric perspective on facial privacy

Pandemic monitoring showed that COVID-19 should be reined in, and rolled back. The supplies of masks were used up entirely in the pandemic. It, however, was noticed that without a mask, people are easily recognisable just in time through Fare Recognition. Therefore, the cat tracker can easily aim at accomplishing this.

3.2. Unified classification framework

The survey classifies existing approaches for the development of privacy-preserving data mining based on the type of algorithm, level of privacy and cost of computation, and application domain. The majority of surveys use the learning model or application as the main idea of classification. The suggested classification outlines the trade-offs associated with the realistic scenario, taking biometrics' real-world deployment into account.

Table 1. Comparative summary of facial recognition and privacy-preserving techniques.

Category	Representative Works	Algorithm Type	Privacy Strength	Computational Cost	Application Domain
Models for Deep Facial Recognition	(Wang, 2021), (Schroff, 2015), (Jing, 2022), (Gong, 2019), (Fuad, 2021), (Simonyan, 2014)	CNN, Metric Learning, ResNet, RNN	Low	Low–Medium	Verification of facial, surveillance, and video analytics
Facial Recognition That is Strong and Masked	(Alzu'bi, 2021), (Yin, 2019), (Becerra-Riera, 2019)	Deep CNN + Transfer Learning	Low	Medium	Forensic analysis of masked faces
Secret Key Cryptography	(ElGamal, 1985), (Paillier, 1999), (Cheon, 2017), (Brakerski, 2014), (Van Dijk, 2010)	PHE, FHE	Very High	High–Very High	Encryption-based secure computing and inference
Encrypted Face Identification	(Gilad-Bachrach, 2016), (Yang, 2022), (Pradel, 2021)	DL + HE	High	High	Biometric authentication in the cloud
Distributed Learning in Biometric Systems	(Kairouz, 2021), (Yang, 2019), (McMahan, 2017), (Li, 2020)	FL + DL	Medium–High	Medium	Collaborative biometric education
Differential Privacy Methods	(Dwork,2008), (Dwork, 2014), (Abadi, 2016)	DP + ML/DL	Medium	Medium	Model training with privacy standard
Threats to Security and Their Defences	(Pagnin, 2017), (Abdullahi, 2024), (Goodfellow, 2014), (Sarwar, 2019)	Adversarial Defence, Filtering	Medium	Medium	Monitoring, biometric safeguarding
Surveying Datasets and Multimodal	(Al-Mannai, 2024), (Becerra-Riera, 2019)	Multimodal Analytics	Low–Medium	Medium	Designing and Evaluating Datasets
Joint Security	(Yang, 2022), (Pradel, 2021)	DL + HE / FL	High	Medium–High	Safe biometric identification

3.3. Bridging theory and deployment feasibility

Unlike survey papers that speak about the theoretical privacy guarantees, the focus of this paper is the feasibility aspect. It includes the computational overhead, scalability, and performance drop under encryption. Consequently, this work offers guidelines and information useful for a researcher and practitioner in designing a deployable privacy-preserving biometric system.

3.4. Comparative analysis across privacy paradigms

The framework is comparable to other techniques for data protection such as anonymisation and cryptography. However, privacy mechanisms in federated learning still have more to achieve. For instance, the utilisation design of current techniques functioning efficiently for the uni-modal data techniques may not work well for the multi-model versions.

3.5. Regulatory and ethical alignment

Some of the global regulatory frameworks, with which the existing technical methods are compliant, are GDPR, EU AI Act, IEEE Ethical Standards, etc. It is worth mentioning that other survey papers do not make any linkage to regulations.

3.6. Identification of open challenges and research gaps

This article first introduces a proposed taxonomy which will summarise the state of the art of all known approaches for privacy-preserving machine learning on encrypted data. A comparative analysis of these methods will be presented that covers their differences and drawbacks. Ultimately, a set is talked about.

4. Methodology

Over the years, the technology has evolved along with some deep learning solutions that enhance reliability and accuracy. In recent times, techniques have been proposed to secure the facial recognition system, privately and accurately. As you read through the section above, you must have got an understanding of the working of an AI facial recognition system and its components. In the next lesson of facial recognition using AI, you will understand its components and evaluation. AI facial recognition systems enhance accuracy and security.

4.1. Data acquisition and preprocessing

Edge devices with HD cameras and sensors collect facial data. In order to ensure the privacy of the raw data, a newly developed pre-processing-based adaptor method which comprises Gaussian blurring and High Dynamic Range image acquisition was used. This measure ensures that only high-quality data is kept and the users' privacy is maintained. Initially, image capturing is performed, and then, it is pre-processed and the acquired data is enhanced.

4.2. Face detection and feature extraction

Multi-task Cascaded Convolutional Networks (MTCNNs) enable face detection and alignment in the suggested pipeline. The networks assist in obtaining the five facial landmarks, which are then changed to a standard source axis. All the data is rendered homogenous for the later stages that assist to improve accuracy in the end. MTCNN architecture has three stages which are Proposal Network (P-Net) Refine.

4.3. Mechanisms for privacy and security

User data is secured using differential privacy, homomorphic encryption, and federated learning in this system. Moreover, it makes use of secured model deployment and transfer along with secure data storage to protect sensitive data from threats. The dependability of the system is observed and secured against new attacks.

4.4. Model training and explainability

The facial recognition model trains on a very large collection of faces. The rate of falsely accepting a genuine user will be low. An XAI framework has been added for explainable prediction of the model. The EAI techniques which we proposed generate saliency maps and visual explanations for accountability and trust in AI systems.

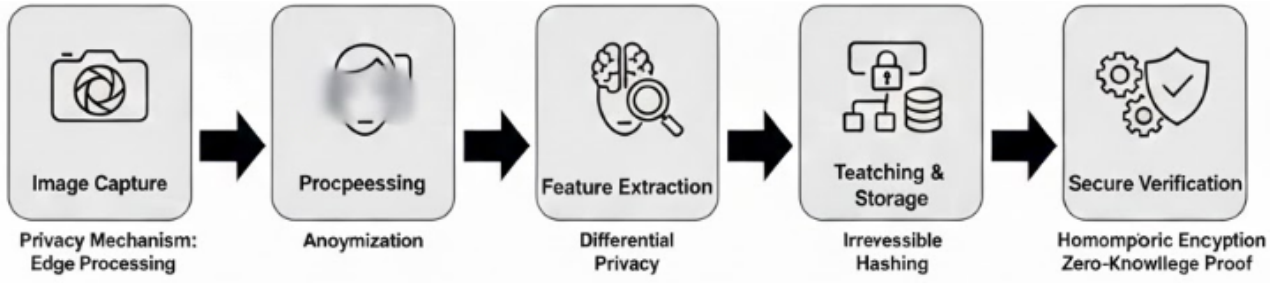

Figure 2. Workflow of AI-based facial recognition with privacy mechanisms.

4.5. Performance evaluation and system comparison

This system's accuracy is benchmarked against several leading facial recognition systems used worldwide. Detection, identification accuracy, and confidence reliability are assessed via performance metrics like identification accuracy, detection recall, and F1-score. The security has been enhanced with hardened model deployment pipelines, cryptographic securing of storage, and encrypted transport. It has an interactive interface that provides instant feedback on the response from the system.

5. AI-powered face identification systems

With facial recognition technologies utilising artificial intelligence, it represents safety and privacy risks. Homomorphic encryption, federated learning, differential privacy, and biometric template protection enhance privacy without sacrificing any functions of the system. Such strategies help in keeping the information safe and preserve the accuracy of the model. Decentralised approaches and secure multi-party computing are used so that data cannot be misused to further enhance the privacy of the users. These privacy-preserving methodologies need to be improved further in order to mitigate the public concern and make AI more applicable to facial recognition.

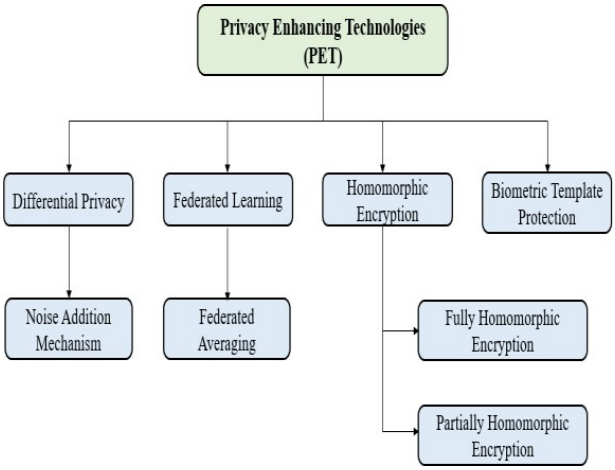

Figure 3. Privacy-enhancing technologies.

5.1. Enhancing privacy with differential privacy

Differential privacy (DP) is now at the core of AI-enabled facial recognition systems. It improves the ability to provide high model accuracy and safeguard biometric data. Even if outsiders have access to the output from the systems, they will not be able to identify any individual record. One way that this can be achieved is through a controlled noise pattern in a dataset or type of output. The strength of data protection and the usefulness of the model depends on the privacy budget (ε). In essence, using smaller epsilon leads to stronger privacy, but often more degradation of performance. In facial recognition, security and accuracy are two essential requirements for a balanced system.

5.1. Noise addition mechanism

The addition of noise is a crucial procedure in differential privacy. The aim of this technique is to add noise to the original data such that no one can learn anything about an individual in that database. In simple terms, this technique would prevent the extraction of data. The Gaussian mechanism is often used in the training or inference of facial recognition. The Laplace mechanism is another famous mechanism which is used along with the Gaussian mechanism. Both of these mechanisms add noise to the data. Thus, it will not learn anything relating to facial recognition. However, the overall accuracy of the model will not suffer a significant drop.

5.2. Federated learning

Federated learning (FL) is a privacy-preserving framework that trains a machine learning model, by transferring learning to a number of edge devices, instead of centralising the raw data (Yang, 2019). It is important to study the significance of FL for facial recognition. It is possible to extract the biometric information of an individual from their face. Consequently, data on the local machine can be used by the user to train the model. Consequently, FL enables the implementation of a facial recognition model on decentralised data while ensuring privacy. Sending the raw data from all sources to a central server so that the model can be trained on it is called 'centralising'. Sending out biometric information of faces can give rise to fraud and identity theft issues with third parties. Hence, it is important to address this privacy issue in FR with FL. The federated learning algorithm is used to solve this problem.

5.2.1. Federated Averaging (FedAvg)

In recent times, facial authentication frameworks have integrated distributed machine learning schemes called Federated Averaging (FedAvg) (McMahan, 2017). Consequently, this enables edge devices to train localised facial datasets by sending the model updates to the server for aggregation to further improve the actual model which will be sent back to the edge devices for improvement (Kairouz, 2021). Thus, critical biometrics remain within the device while the learning process occurs in a distributed manner. New investigations on federated learning have been helpful in the creation of heterogeneity in facial recognition models (Li et al, 2020). They address uneven data distributions as well.

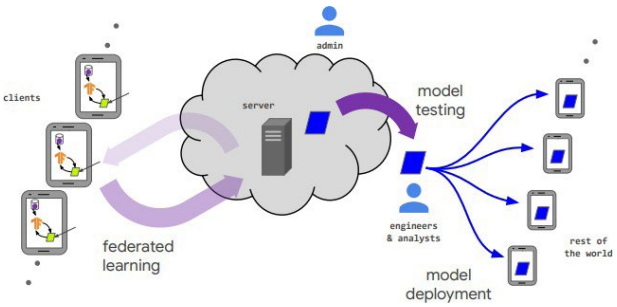

Figure 4. The lifecycle of an FL-trained model (Kairouz, 2021)

5.3. Homomorphic Encryption

Homomorphic encryption represents a cryptographic breakthrough that enables direct computation on encrypted data while preserving confidentiality. This paradigm-shifting technology allows AI systems to process encrypted facial biometrics—including feature vectors and embeddings—while maintaining end-to-end data protection (Van Dijk, 2010). It permits calculations using encrypted information. It decrypts only the last outcomes, which ensures the security of the model training as well as inference. The scheme can assess operations on encrypted cipher texts, ensuring the veracity of the resulting outputs at each encoding stage. It is incorporated to implement a facial recognition authentication system that preserves user privacy that uses biometric information.

In general, there are two types: Fully Homomorphic Encryption (FHE) and Partially Homomorphic Encryption (PHE). This enables unlimited computations on cipher texts. Fully homomorphic encryption uses a technique called bootstrapping, which is a complex way of changing the cipher text but keeping the underlying message. Lattice-based cryptography has enhanced the effectiveness of fully-homomorphic encryption. Using this method, encrypted facial data inference can be performed via neural networks.

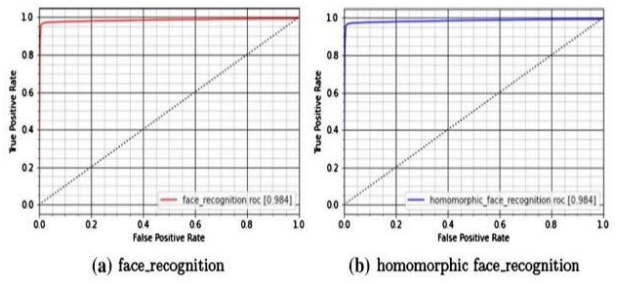

Figure 5. ROC curve analysis: facial recognition vs. homomorphic facial recognition (Yang, 2022).

5.3.1. Fully homomorphic encryption

With Fully Homomorphic Encryption (FHE), additive and multiplication operations can be carried out on an encrypted version of the data without having to decrypt it (Cheon, 2017). For example, facial recognition AI implements personal biometric data that should be protected in order to maintain privacy (Gilad-Bachrach, 2016). FHE preserves the privacy and security of encrypted data since it decryption will only occur at the final output. Moreover, there is no limit to the number of operations possible on the cipher text.

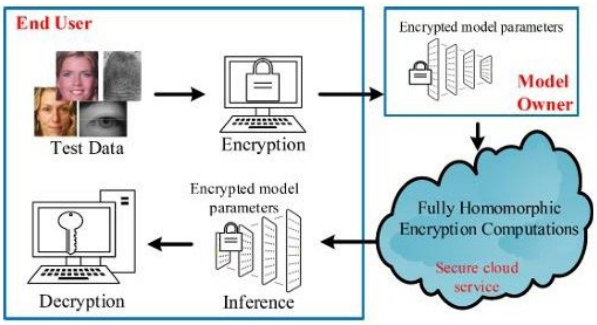

Figure 6. Fully Homomorphic Encryption (FHE) workflow (Abdullahi, 2024).

5.3.2 Partially Homomorphic Encryption

Partially Homomorphic Encryption (PHE) enables limited computations on ciphertext, restricted to either exclusively additive or multiplicative operations (Paillier, 1999). Though offering less versatility than FHE, PHE demonstrates superior computational efficiency, proving effective for constrained facial recognition applications like encrypted feature analysis (ElGamal, 1985). This approach maintains data confidentiality during processing while optimising performance for resource-sensitive implementations.

Table 2. Comparison of Fully and Partially Homomorphic Encryption.

Features	FHE (Fully Homomorphic Encryption)	PHE (Partially Homomorphic Encryption)
Operations	Supports both addition and multiplication	Supports either addition or multiplication
Privacy	Stronger, all computations on encrypted data	Moderate, may require partial decryption
Efficiency	Computationally expensive, slower	More efficient, faster processing
Use Case	Secure cloud-based facial recognition	Real-time, on-device facial recognition
Examples	BGV, CKKS, TFHE	Paillier, RSA, ElGamal

5.4. Privacy-preserving biometric templates

A room must meet these two criteria. First, the room must be rectangular. Second, there must be a door. Both of these criteria are crucial in order to ensure success in this endeavour. After meeting both of these criteria, the

next step is possible. In other words, the penance can be performed. As per the penance, 'Kreelam Kreelam' must be chanted 952 times. This can be with intervals of 10 days, in a room or even outdoors. It just be remembered that the room must meet the two aforementioned criteria.

In order to protect biometric data like facial recognition data, techniques are used that protect access to an individual's biometric data from attacks and/or usage by unauthorised users. These methods prevent the attacker from obtaining the genuine biometric feature so that recognition accuracy remains unaffected and the attacker is unable to misuse it. This system utilises facial specifications to create a template used to identify individuals. During the process of facial recognition, the AI facial recognition system produces biometric templates from facial data, which are saved in a system for future comparison, preventing the replaying of valuable biometric data and avoiding unauthorised access or reproductions.

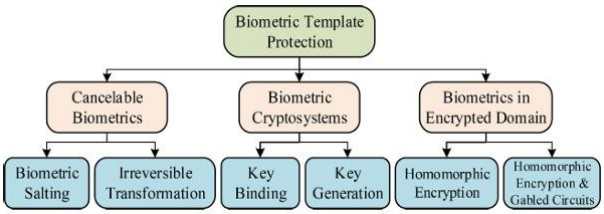

Figure 7. Biometric Template Protection Techniques (Abdullahi, 2024).

Encryption ensures data confidentiality by securing the storage and transmission of facial templates (Bringer, 2009) , making them inaccessible to unauthorised parties. Cancellable biometrics transform biometric data into this system that combines cryptographic keys and facial features to generate the biometric template. Hence, without both constitutive parts, the template cannot be used. All these techniques ensure that the template cannot be inverted and used to construct sensitive biometric data. They also assure compliance with privacy regulations, while maintaining accuracy and efficiency in signing.

6. Conclusion

The growing artificial intelligence and deep learning model development have led to facial recognition development. In addition, some states are already utilising them to enhance accuracy and efficiency. Yet, this popularity brings along serious implications for privacy, security, and ethics. This paper examines the approaches for the development of an AI-based facial recognition system, as well as integrating mechanisms that would enhance the privacy of user data. The safety of sensitive facial information without impacting performance can be guaranteed through secure biometric representation, decentralised model training, encrypted computing, and privacy-preserving noise addition. Integrating mechanisms ensures safe computations and prevents leakage. It also helps in facilitating the transparency of the system. This special feature was designed to help policymakers, researchers, advocacy groups, and the public to understand Ameca's behaviour. Moreover, an explainable AI box has been integrated which helps in interpretability and accountability of facial recognition decisions. This study consolidates various evaluation metrics, privacy-enhancing strategies, and high-security mechanisms into a single unit to improve and design a secure facial recognition system. Enhancing these mechanisms, reducing AI biases, and adopting new regulations must be the key objective for future development in this area. We need to gain public confidence in the use of AI-based facial recognition technology in the real world by balancing innovation and ethical issues.

Table 3. Performance comparison on Facial Recognition Datasets.

Method	Encryption Type	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Secure Feature Matching	PHE	LFW	95.6	95.2	94.8	95.0
Homomorphic Feature Comparison	FHE	LFW	94.8	94.5	94.1	94.3
Proposed Encrypted Framework	**FHE**	**LFW**	**96.9**	**96.5**	**96.2**	**96.3**
Plain CNN-based Facial Recognition	None	CASIA-WebFace	97.6	97.2	97.0	97.1
Secure Feature Matching	PHE	CASIA-WebFace	94.2	93.8	93.5	93.6
Proposed Encrypted Framework	**FHE**	**CASIA-WebFace**	**96.1**	**95.7**	**95.4**	**95.5**

Notes on contributors

Mr Praveen Kumar J serves as an Assistant Professor in the Department of Computer Science and Engineering at Rajalakshmi Institute of Technology, Chennai. He holds a Master of Technology (M.Tech) in Information Technology from Vellore Institute of Technology, Vellore, Tamil Nadu, India. He is currently pursuing his Ph.D. at Anna University, Chennai, Tamil Nadu, India. With strong expertise in his domain, he is actively involved in teaching, research, and academic development, contributing to the advancement of knowledge and the professional growth of students. His academic and research interests span Machine Learning, Computer Vision, Data Science, and Deep Learning, where he focuses on exploring innovative methodologies and practical applications that address real-world challenges. Through his dedication to education and research, he continues to play a significant role in mentoring students and shaping the next generation of technology professionals.

Dr Anwar Basha H is working as an Associate Professor in the Department of Computer Science & Engineering (AI & ML), Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India. He obtained his B.E. degree from Anna University, Chennai. He obtained his M.Tech degree from Dr. MGR Educational and Research Institute University, Chennai. He obtained his Ph.D. in CSE from Saveetha Institute of Medical and Technical Sciences, Chennai. He has many certifications like Microsoft Certified Azure Fundamentals, AWS Certified Cloud Practitioner, and IBM Certified Data Science Foundation. He has more than 17 + years of teaching experience. He has around 2 years of industrial work experience. He has published papers in various international conferences and peer-reviewed international journals. He has served in many international conferences as a Session Chair, Programme Committee Member, Reviewer, and Organising Chair. He is a reviewer in IOS Press, Springer, Elsevier, Taylor and Francis, IOP, and Wiley Journal. He is an Editorial member in the Journal of Advanced Research in Applied Science. He has authored a text book “Cloud based Security Management”. Currently, he is working on Multi-Cloud Storage, Big Data Analytics, and Cyber Security. He has visited countries like the UAE, Thailand, and Afghanistan.

Dr O Pandithurai is a Professor in the Department of Computer Science and Engineering at Rajalakshmi Institute of Technology. His research interests include Artificial Intelligence, Data Science, Internet of Things (IoT), and Machine Learning. He has made significant contributions to the academic community through numerous publications in international peer-reviewed journals and by presenting research papers at various international conferences across India. His work reflects a strong commitment to advancing research and fostering innovation in emerging areas of computer science and engineering. In addition to his research and teaching responsibilities, Dr. O. Pandithurai actively contributes to the scholarly community as a reviewer and editor for several reputed journals. He has also served in various academic roles at international conferences, including Session Chair, Reviewer, Organising Chair, and Technical Programme Committee (TPC) Member, in conferences held across India and abroad.

Dr G Saikrishnan obtained his Ph.D. in the field of Brake Friction Composites from the Department of Rubber and Plastics Technology, Anna University – Madras Institute of Technology, Chennai, Tamil Nadu, India. He is currently serving as an Associate Professor in the Department of Mechanical Engineering at Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India. He has significant academic and research experience in the development and characterisation of advanced materials, particularly in the field of friction and composite materials. His work focuses on improving the performance, durability, and environmental sustainability of braking systems through innovative material design and engineering. Dr. Saikrishnan has actively contributed to the academic and research community through publications in reputed national and international journals, conference presentations, and collaborative research activities. He is also actively involved in guiding undergraduate, postgraduate, and Ph.D. research scholars, mentoring them in research methodology, material development, and experimental analysis.

References

[1] Wang, Mei, and Weihong Deng. "Deep face recognition: A survey." Neurocomputing 429 (2021): 215-244.

[2] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." IEEE transactions on information theory 31.4 (1985): 469-472.

[3] Schroff, Florian, Dmitry Kalenichenko, and James Philbin. "Facenet: A unified embedding for face recognition and clustering." Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.

[4] Alzu'bi, Ahmad, et al. "Masked face recognition using deep learning: A review." Electronics 10.21 (2021): 2666.
[5] Yin, Xi, et al. "Feature transfer learning for face recognition with under-represented data." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2019.
[6] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999.
[7] Jing, Hongrong, et al. "A face recognition algorithm based on improved resnet." Frontiers in Computing and Intelligent Systems 1.1 (2022): 22-25.
[8] Goodfellow, Ian, et al. "Generative adversarial networks." Communications of the ACM 63.11 (2020): 139-144.
[9] Gilad-Bachrach, Ran, et al. "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy." International conference on machine learning. PMLR, 2016.
[10] Cheon, Jung Hee, et al. "Homomorphic encryption for arithmetic of approximate numbers." Advances in cryptology–ASIACRYPT 2017: 23rd international conference on the theory and applications of cryptology and information security, Hong kong, China, December 3-7, 2017, proceedings, part i 23. Springer International Publishing, 2017.
[11] Al-Mannai, Kamela, et al. "Multimodal Face Data Sets—A Survey of Technologies, Applications, and Contents." IEEE Access (2024).
[12] Brakerski, Zvika, and Vinod Vaikuntanathan. "Efficient fully homomorphic encryption from (standard) LWE." SIAM Journal on computing 43.2 (2014): 831-871.
[13] Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. Springer Berlin Heidelberg, 2010.
[14] Yang, Tao, et al. "Privacy enhanced cloud-based facial recognition." Neural Processing Letters (2022): 1-9.
[15] Bringer, Julien, Hervé Chabanne, and Bruno Kindarji. "Error-tolerant searchable encryption." 2009 IEEE International Conference on Communications. IEEE, 2009.
[16] Kairouz, Peter, et al. "Advances and open problems in federated learning." Foundations and trends® in machine learning 14.1–2 (2021): 1-210.
[17] Pradel, Gaëtan, and Chris Mitchell. "Privacy-preserving biometric matching using homomorphic encryption." 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2021.
[18] Gong, Sixue, Yichun Shi, and Anil K. Jain. "Recurrent embedding aggregation network for video face recognition." arXiv preprint arXiv:1904.12019 (2019).
[19] Yang, Qiang, et al. "Federated machine learning: Concept and applications." ACM Transactions on Intelligent Systems and Technology (TIST) 10.2 (2019): 1-19.
[20] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, 2017.
[21] Fuad, Md Tahmid Hasan, et al. "Recent advances in deep learning techniques for face recognition." IEEE Access 9 (2021): 99112-99142.
[22] Becerra-Riera, Fabiola, Annette Morales-González, and Heydi Méndez-Vázquez. "A survey on facial soft biometrics for video surveillance and forensic applications." Artificial Intelligence Review 52.2 (2019): 1155-1187.
[23] Kairouz, Peter, et al. "Advances and open problems in federated learning." Foundations and trends® in machine learning 14.1–2 (2021): 1-210.
[24] Pagnin, Elena, and Aikaterini Mitrokotsa. "Privacy-preserving Biometric authentication: challenges and directions." Security and Communication Networks 2017.1 (2017): 7129505.
[25] Abdullahi, Sani M., et al. "Biometric template attacks and recent protection mechanisms: A survey." Information Fusion 103 (2024): 102144.
[26] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." arXiv preprint arXiv:1412.6572 (2014).
[27] Li, Tian, et al. "Federated learning: Challenges, methods, and future directions." IEEE signal processing magazine 37.3 (2020): 50-60.
[28] Zhang, Yu, and Qiang Yang. "A survey on multi-task learning." IEEE transactions on knowledge and data engineering 34.12 (2021): 5586-5609.
[29] Dwork, Cynthia. "Differential privacy: A survey of results." International conference on theory and applications of models of computation. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.
[30] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." arXiv preprint arXiv:1409.1556 (2014).
[31] Sarwar, Omair, Bernhard Rinner, and Andrea Cavallaro. "A privacy-preserving filter for oblique face images based on adaptive hopping Gaussian mixtures." IEEE Access 7 (2019): 142623-142639.
[32] Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends® in Theoretical Computer Science 9.3–4 (2014): 211-407.
[33] Abadi, Martin, et al. "Deep learning with differential privacy." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.