Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.049611

ARTICLE

Enhancing Security and Privacy in Distributed Face Recognition Systems through Blockchain and GAN Technologies

Muhammad Ahmad Nawaz Ul Ghani[1], Kun She[1,*], Muhammad Arslan Rauf[1], Shumaila Khan[2], Javed Ali Khan[3], Eman Abdullah Aldakheel[4] and Doaa Sami Khafaga[4]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China

[2]Department of Computer Science, University of Science & Technology, Bannu, 28100, Pakistan

[3]Department of Computer Science, University of Hertfordshire, Hatfield, AL10 9AB, UK

[4]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11671, Saudi Arabia

*Corresponding Author: Kun She. Email: kun@uestc.edu.cn

Received: 12 January 2024 Accepted: 29 March 2024 Published: 15 May 2024

ABSTRACT

The use of privacy-enhanced facial recognition has increased in response to growing concerns about data security and privacy in the digital age. This trend is spurred by rising demand for face recognition technology in a variety of industries, including access control, law enforcement, surveillance, and internet communication. However, the growing usage of face recognition technology has created serious concerns about data monitoring and user privacy preferences, especially in context-aware systems. In response to these problems, this study provides a novel framework that integrates sophisticated approaches such as Generative Adversarial Networks (GANs), Blockchain, and distributed computing to solve privacy concerns while maintaining exact face recognition. The framework's painstaking design and execution strive to strike a compromise between precise face recognition and protecting personal data integrity in an increasingly interconnected environment. Using cutting-edge tools like Dlib for face analysis, Ray Cluster for distributed computing, and Blockchain for decentralized identity verification, the proposed system provides scalable and secure facial analysis while protecting user privacy. The study's contributions include the creation of a sustainable and scalable solution for privacy-aware face recognition, the implementation of flexible privacy computing approaches based on Blockchain networks, and the demonstration of higher performance over previous methods. Specifically, the proposed StyleGAN model has an outstanding accuracy rate of 93.84% while processing high-resolution images from the CelebA-HQ dataset, beating other evaluated models such as Progressive GAN 90.27%, CycleGAN 89.80%, and MGAN 80.80%. With improvements in accuracy, speed, and privacy protection, the framework has great promise for practical use in a variety of fields that need face recognition technology. This study paves the way for future research in privacy-enhanced face recognition systems, emphasizing the significance of using cutting-edge technology to meet rising privacy issues in digital identity.

KEYWORDS

Facial recognition; privacy protection; blockchain; GAN; distributed systems

1 Introduction

Machine learning (ML) has gained considerable interest in academic and industrial circles, demonstrating its versatility across various domains [1]. This interest has led to the development of a decentralized training framework, facilitating collaborative engagement of multiple participants in ML model training while ensuring the confidentiality of their individual training data. Privacy regulations such as the General Data Protection Regulation (GDPR) [2] and the California Consumer Privacy Act (CCPA) [3], enforce stringent privacy protocols for individuals' privacy rights through secure collection, access, and storage of their user data. In response to concerns about personal data privacy, a decentralized method called federated learning [4] has been introduced. This approach enables collaborative machine learning while maintaining data privacy by allowing individuals to share only model parameters, rather than sensitive training data.

Furthermore, the adoption of privacy-enhanced face recognition has increased due to concerns surrounding data security and privacy, as well as the growing need for facial recognition technology [5]. By employing state-of-the-art Generative Adversarial Networks (GANs) to create synthetic faces [6], utilizing distributed computing for increased scalability, and implementing the secure framework of Blockchain for user identification, we may integrate innovative methodologies to address users' privacy. The main goal is to achieve a harmonious equilibrium between guaranteeing precise facial recognition and protecting individuals' data in an increasingly networked world [7]. Despite its widespread usage in fields such as access control, law enforcement, security, surveillance, internet communication, and entertainment [8], the pervasive use of face recognition technology has raised significant concerns about data monitoring and user privacy preferences [9]. The face recognition system follows a systematic structure: Initially, an image is retrieved from the database, followed by the application of the face detection process. Subsequently, features are extracted to identify the face from the feature storage database. This sequential process ensures the verification and identification, as depicted in Fig. 1.

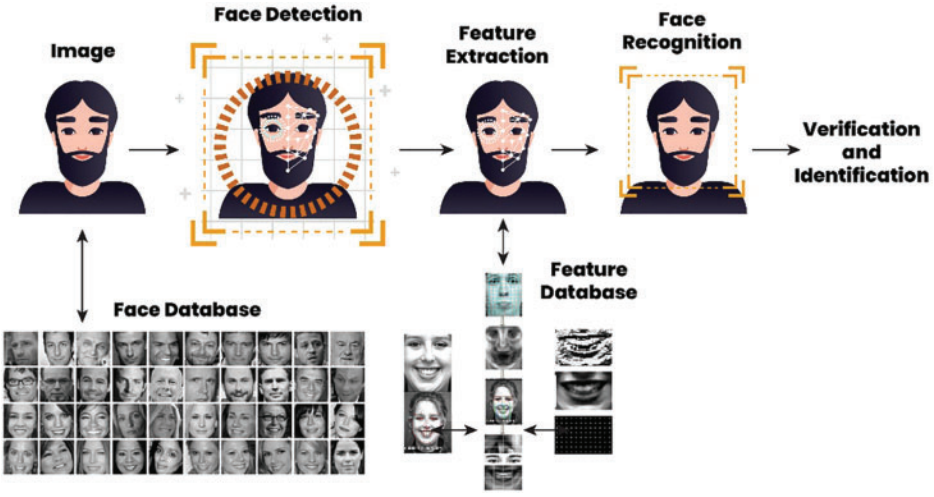

Figure 1: Generic structure of face recognition system

The primary challenge lies in developing a decentralized, distributed system capable of managing a significant volume of secure facial data while preserving personal privacy integrity [10]. This study proposes a decentralized and distributed facial recognition system as a solution to address the privacy and security concerns arising from the rapid increase in facial data collection. The proposed system

aims to achieve precise and highly secure facial analysis and recognition, along with enhanced privacy protection, by leveraging advanced technologies such as Blockchain, GANs, smart contracts, and distributed computing [11].

The major research contributions of this research are highlighted in bullet points:

- Developed a scalable and sustainable privacy-aware facial recognition system by integrating GANs, Dlib, Ray Cluster, and Blockchain technology. This provides accurate biometrics while upholding robust user privacy.
- Created a versatile privacy computing model that distributes facial data processing across dedicated nodes in a cluster configuration. Sensitive user information is isolated and securely stored via Blockchain.
- Comprehensive experiments validate that the approach exceeds existing techniques in balancing high precision matching with low visibility of personal data, generation time and resilience against data leaks.

2 Related Work

Face identification involves recognizing an unknown face image by comparing it with a database of known faces. In this process, the most similar match is returned as the assumed identity of the subject after calculating the similarity between a specific face image and all the face images in a database as presented in Fig. 2. Numerous challenges in the field of face identification have been tackled using a variety of methods. In academics, there has been specific interest in hybrid face recognition techniques. The complexities of face identification are discussed in several papers [12]. Chaabane et al. [13] utilize statistical characteristics in their innovative approach, which accelerates identification speed and achieves an impressive accuracy rate of 99.37% on a dataset comprising 400 images from 40 individuals. Vu et al. [14] introduce "MaskTheFace," a method that enhances existing datasets and modifies facial recognition systems to accommodate individuals wearing masks, ensuring secure authentication without the need to rebuild datasets. Hariri [15] have engineered a robust system that integrates MobileNetV2, OpenCV, and FaceNet to address the need for facial identification during the pandemic, achieving exceptional accuracy rates of 99.65% for mask detection, 99.52% for identifying individuals wearing masks, and 99.96% for recognizing unmasked faces. Haider TH. ALRikabi et al. [16] proposes a Matlab-based face identification system utilizing a Quantum Neural Network (QN) for precise recognition of facial patterns against a maintained database.

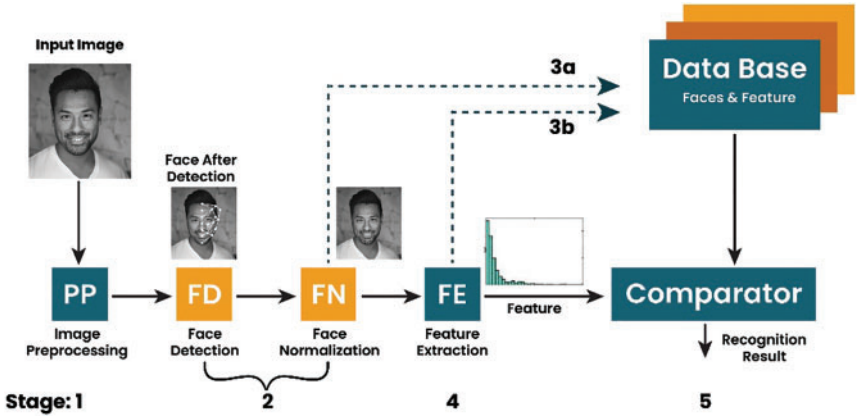

Figure 2: Traditional facial recognition systems

Prior research addresses significant privacy concerns and facets of facial recognition technology. Feng et al. [17] devised a privacy protection system for face recognition and resolution based on edge computing to mitigate the privacy risks associated with cloud computing. Tian et al. [18] propose a comprehensive approach to address privacy and fairness issues in facial image graphs. Their study employs GAN models to generate synthetic images that maintain privacy while ensuring fairness. Zhang et al. [19] investigate the resistance of customers to innovation in face recognition payments, emphasizing the influence of user behavior moderators such as gender, platform trust, and privacy concerns on user behavior.

This study introduces a novel approach to facial recognition technology, integrating adversarial image synthesis and decentralized identity management. Through the utilization of GANs for creating realistic dummy faces and the implementation of tamper-resistant Blockchain transactions for secure user verification, the system endeavors to strike a balance between performance and privacy. As previous research, concentrates on specific aspects, this study offers a comprehensive solution covering training data expansion, access control, result verification, and storage auditing, promoting responsible and ethical facial recognition practices. The summary of the main distinctions between this study and previous research are shown in Table 1.

Table 1: Comparison of proposed study with existing literature in facial recognition technology

Aspect	Existing literature	Proposed study
Technology integration	Limited integration of Blockchain and GANs	Comprehensive integration of Blockchain and GANs
Privacy enhancement	Some studies address privacy concerns using edge computing	Emphasizes privacy through Blockchain transactions and GANs synthesis
Security measures	Limited exploration of tamper-resistant Blockchain transactions	Implements tamper-resistant Blockchain transactions for secure user verification
Comprehensive approach	Focuses on specific aspects such as affect recognition or pose-invariant face recognition	Offers a holistic solution including training data expansion, access control, result verification, and storage auditing
Novelty	Some studies propose innovative techniques like federated learning	Introduces a novel approach by integrating GANs and Blockchain for facial recognition

3 Proposed Framework

The distributed face recognition system is meticulously designed with scalability, fault tolerance, interoperability, and privacy rules as top priorities. This involves implementing advanced distributed data storage techniques to ensure efficient face data processing and retrieval. Strategic placement of numerous nodes, along with GAN-based face recognition modules, enhances system efficiency and resilience. The use of a Blockchain network reinforces privacy and security by establishing decentralized data storage and access control methods. Priority is given to data encryption methods that balance computational efficiency and encryption strength, ensuring sensitive data protection

during transmission. Fig. 3 visually represents the proposed framework, encompassing the discussed design concepts and procedures for clarity and reference.

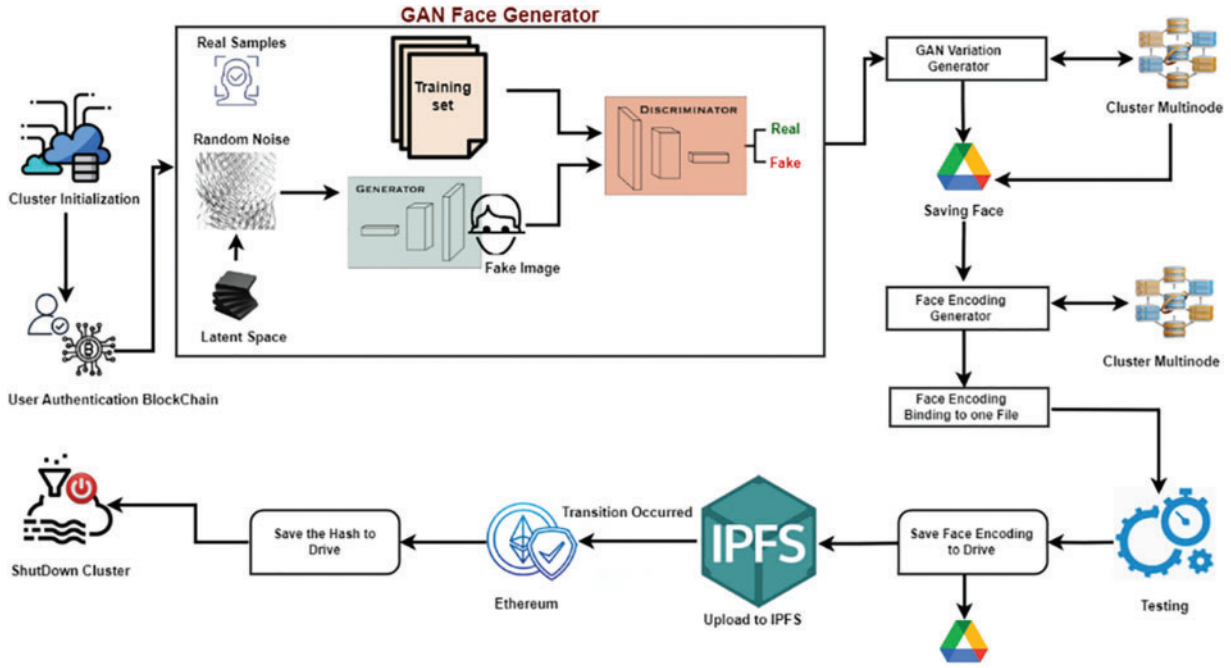

Figure 3: Workflow of the proposed framework for secure and scalable face recognition

The proposed methodology ensures secure communication and data management through a series of steps. Beginning with cluster initialization using Blockchain, nodes are configured and authorized, followed by GAN Face Generator and Variation Generator modules for synthetic face creation. The Cluster Multimode Model optimizes resource usage and scalability. Faces are securely stored, encoded, and associated with identities for streamlined management. Testing assesses encoding performance, with results stored in decentralized cloud services. Ethereum Blockchain ensures transparency and integrity, capturing transactional data. The workflow concludes with the cluster's graceful shutdown, preserving operational effectiveness. This advanced approach integrates cutting-edge technologies for robust, scalable, and private face recognition, marking a significant breakthrough in the field.

3.1 Generative Adversarial Network

GAN is a type of machine learning model that can generate synthetic data that resembles the existing data. The basic idea of GANs is that two neural networks, consists of a generator and a discriminator, engaging in an adversarial training process illustrated in Fig. 4.

The discriminator is trained to distinguish between these images, and its loss (Li_discriminator) is computed by comparing its output for actual and synthetic images. The discriminator (Wd) weights are then updated by gradient descent. The generator's task is to produce false images that can deceive the discriminator; the generator loss (Li_generator) is calculated using the discriminator's output for synthetic images. The generator's (Wg) weights are suitably adjusted. Periodic updates on the average discriminator and generator losses are provided by the program, which offers insightful information on the continuous training process. When the discriminator and generator losses are confirmed to have stabilized and converged, the training is considered complete.

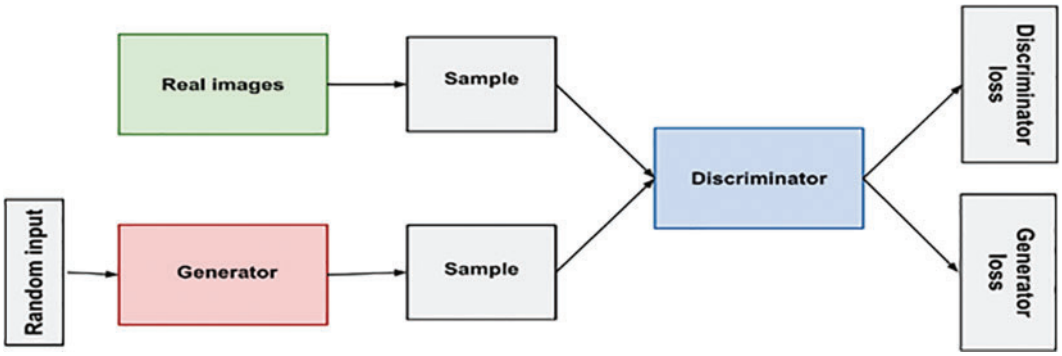

Figure 4: Synthetic image generation and model training process

Algorithm 1 offers step-by-step instructions for training the facial recognition system and emphasizes crucial mathematical ideas to enhance model performance. The pre-trained GAN model was modified to fit the system under demonstration after being trained on the same publicly accessible data. The goal of this model is to produce realistic, high-quality facial imagegraphs. Firstly, the generator (G) and discriminator (D) networks' primary hyper-parameters and random weights. The training loop consists of sampling and processing actual (Xi_real) and synthetic (Xi_synthetic) face images over epochs (t) while iterating over the current batch (i).

Algorithm 1: StyleGAN-based synthetic face generation

1. **Initialize** the StyleGAN model parameters, denoted by Θ, for face generation.
2. **For** testing and validation:
   a. Request synthetic faces from the StyleGAN model by sampling from the latent space Z.
   b. Obtain the synthetic faces $\{\hat{X}_i\}$ for testing and validation purposes.
3. **END For**
4. **For** training dataset augmentation:
   a. Let X_R represent the training dataset of real faces and X_S denote the set of synthetic faces generated by StyleGAN.
   b. Augment the training dataset by merging the real and synthetic faces:
   $X_{augmented} = X_R \cup X_S$
   where $\cup$ denotes the set union operation.
5. **End procedure.**

3.2 Model Training

This research emphasizes the crucial role of face recognition model training in establishing a reliable framework. The core strategy relies on state-of-the-art facial recognition skills from pre-trained deep neural networks, supported notably by the open-source Dlib toolbox. The effectiveness of facial recognition systems is linked to the quality and breadth of training data, influencing the model's ability to accurately identify individuals. The utilization of pre-trained deep neural networks enables accurate extraction of complex facial traits, ensuring precise recognition even in challenging scenarios. This initiative leverages recent advancements in machine learning and computer vision through the Dlib toolbox, creating a highly reliable and accurate face identification system.

Precise facial mapping, feature extraction, and matching are made possible by Dlib's powerful image analysis pipelines and model structures. Fig. 5 presents the results of the face generation process, which are based on GANs. This illustrates how well the GAN-based method produces realistic facial images. The model's output is a testament to these techniques and shows how helpful this study was in attaining accurate and efficient face recognition.

Figure 5: GAN-based synthetic face generation

This strategy describes a methodical way to use StyleGAN, a GAN, to create synthetic faces that then add to the training dataset of face recognition systems. To make face creation easier, the StyleGAN model's parameters are first initialized. Synthetic faces are requested from the StyleGAN model by sampling from the latent space during testing and validation, and the resulting synthetic faces are retrieved for assessment. The real face dataset is then supplemented in the training dataset augmentation phase by integrating it with the set of synthetic faces produced by StyleGAN through the use of the set union procedure. By adding synthetic faces alongside actual faces, this augmentation procedure seeks to increase the training dataset's variety and resilience, which might improve the performance and generalization capacity of the face recognition model. This method helps to reduce biases and boost accuracy in practical face recognition applications by exposing the model to a wider variety of facial variants.

Algorithm 2 delineates the face recognition and verification methodology utilized in this research. Leveraging the robust Dlib library, discriminative face embeddings are extracted, encoding facial characteristics resilient to challenging conditions. Upon acquiring a face image, the algorithm computes its embedding vector and compares it against a database of known embeddings using distance metrics. A positive identity match is declared if the minimum distance falls below a predefined threshold, indicating sufficient similarity to a stored embedding. Conversely, a negative verification is returned for unknown individuals.

Algorithm 2: Face recognition using facial embedding

Input: A face image (displayed), a database of recognized faces, and their corresponding facial embeddings.

Output: Positive or negative identity verification result, identifying a specific person's name with high accuracy (if positive).

Procedure:

1. **Take Face Image**
2. **Use**

   Dlib to extract the facial embedding E_{input} from the input face image.
3. **Repeat** for each recognized face in the dataset.
   - **a. Calculate**

     Cosine similarity score (S) between the input facial embedding and each know facial embedding.

     $$S = \frac{E_{input}.E_{known}}{||E_{input}||.||E_{known}||}$$

   - **b. Set**

     Similarity criterion (T) to determine if the input face matches a known face (e.g., $S>T$)
   - **c. If**

     match is discovered ($S>T$):
   - **d. Provide**

     Successful identity verification outcome.
   - **1. Retrieve**

     The name of the identified person linked to the corresponding recognized face.
   - **e. End Loop**
4. **If**

   No match is found for any know face ($S \leq T$ for all faces):
5. **Return**

   Negative identity verification.

3.3 Integrating Blockchain to Improve System Performance

Blockchain technology, which was first developed for cryptocurrencies, is used in this study. Important Ethereum components enable DApp interaction via MetaMask and seamless asset management. We eliminate the need for node hosting with Infura Ethereum API endpoints, ensuring smooth Blockchain access. Kaleido, a Blockchain platform-as-a-service, uses solidity-based smart contracts to expedite the establishment and management of corporate consortium networks. These contracts govern user addresses, IPFS image encoding, registration, authentication, and dynamic updates. The foundation for data protection, accountability, and trust-based, decentralized regulation automation in facial recognition is Blockchain technology.

The face recognition algorithm employs facial embedding to authenticate individuals in images, calculating similarity scores between input and known faces. The method utilizes Dlib and a predetermined threshold to determine positive or negative identity verification. This process ensures accurate identification in extensive face datasets. Integration of blockchain, Google Drive, and GPU clusters facilitates secure face creation and encoding. Tasks include GAN-based synthesis, IPFS network creation, Kaleido Blockchain deployment, user identity confirmation, and resource evaluation. Secure storage involves saving IPFS hashes in Google Drive, with encoding verification through cloud

services. Cloud clusters, IPFS activation, Google Drive connection, and facial recognition activities are implemented using Dlib, storing results in JSON format.

4 Results and Discussion

Modern technologies like Blockchain, Dlib, Ray Cluster, and GANs are easily integrated into the distributed face recognition framework to maximize efficiency, strengthen security, and protect privacy. GANs are essential to this approach because they produce synthetic faces that are highly similar to their real-world counterparts, improving the quality of training and testing data. In the meanwhile, Ray Cluster enables parallelized computations, improving system scalability to effectively handle massive datasets. Dlib contributes to the dependability of the system by guaranteeing the correctness of face matching procedures.

Blockchain technology facilitates secure data sharing between dispersed nodes and decentralized identity verification by utilizing smart contracts. By integrating various state-of-the-art technologies in a harmonic way, the framework realizes a comprehensive, privacy-aware face recognition system that has great potential for practical application. To support this technical discussion, Fig. 6 provides a striking example of the benefits of GANs by demonstrating how they may produce high-quality images, highlighting their critical function in the system. Fig. 7 illustrates the operation of the face recognition system and offers insights into its performance by displaying names and clarity metrics next to recognized faces. Fig. 8 illustrates how facial landmarks evolve, offering a clear visual representation for image production and identification algorithms.

Figure 6: GAN-based performance-illustrating the superiority of GANs in generating high-quality images for enhanced face recognition systems

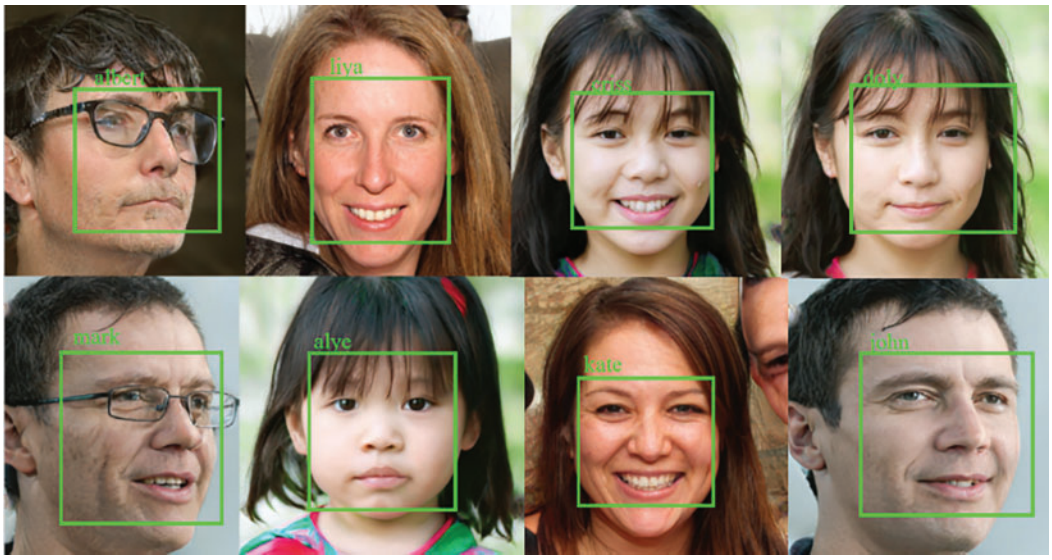

Figure 7: Face recognition system performance-names, and clarity for recognized faces, providing insights into system functionality

Figure 8: Face landmark development-depicting the clarity for image generation and recognition

4.1 Dataset

The study makes use of the CelebA-HQ[1] dataset, which consists of 70,000 high-quality PNG images with 1024 by 1024-pixel resolution. These images feature a range of demographic characteristics, such as age, race, and background, in addition to different facial accessories, such as sunglasses, hats, and eyeglasses. Dlib is used to automatically align and crop the images, reducing the impact of the initial biases. During training, a varied set of faces is collected in order to guarantee algorithmic

[1] https://paperswithcode.com/sota/image-generation-on-celeba-hq-1024x1024

inclusivity and fairness across different populations. Preprocessing methods are used to improve the caliber and variety of the training data, such as scaling, normalization, and augmentation.

4.2 Results

The performance evaluation description of the face-generating techniques used in the research is shown in Table 2 For performance evaluation, StyleGAN utilizes Dlib, custom similarity loss, Adam optimization, and trained models. Similarly, Progressive GAN uses OpenCV, Adam, custom discriminator and generator loss functions, and pre-trained models. In contrast, MGAN does not depend on pre-trained models; instead, it leverages TensorFlow, custom multitask loss, and Adam optimization. The selection of framework, custom loss functions, optimizer, and pre-trained models has a significant impact on the efficiency and accuracy of face generation methods.

Table 2: An analysis of several methods, such as optimizer, loss functions, and pre-trained models, is included in the summary of face generation strategies

Models	Loss function	Optimizer	Pre-trained
StyleGAN	Custom Similarity Loss	Adam	Dlib
Progressive GAN	Custom Discriminator + Generator Loss	Adam	OpenCV
CycleGAN	Custom Adversarial Loss	Adam	TensorFlow
MGAN	Custom Multitask Loss	Adam	TensorFlow

Similarly, Fig. 9 shows a detailed overview of each job in the system, including its ID, job description, current state, and related function or class name. This detailed data is crucial for monitoring and optimizing task execution, allowing for the discovery of possible bottlenecks, resource-intensive procedures, and chances for efficiency improvements. This data allows for a more in-depth knowledge of resource allocation and overall system efficiency by outlining the time and memory needs of each activity.

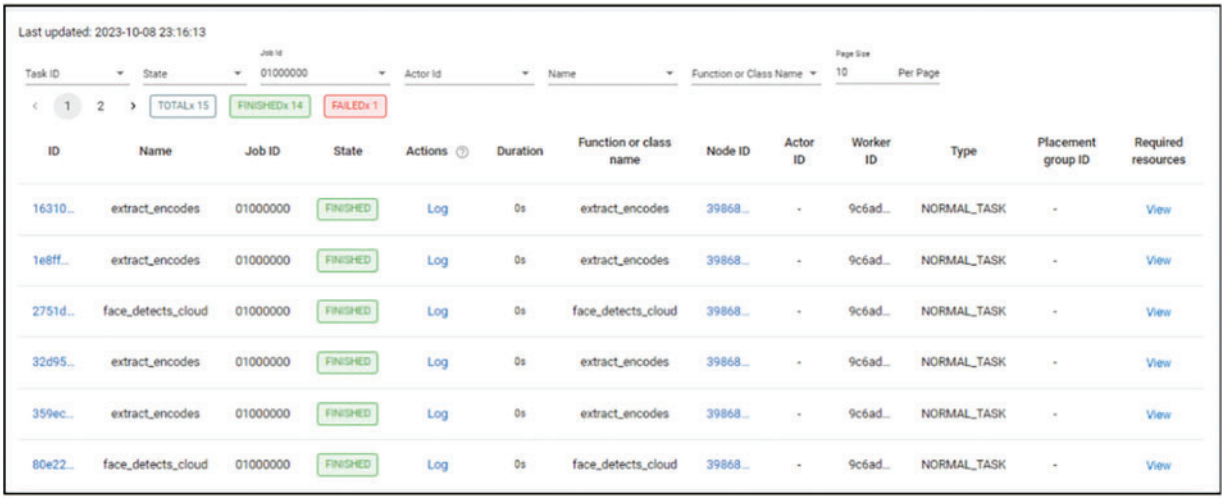

Figure 9: Ethereum blockchain transactions execution details–individual ID, name, Job ID, status and function or class name for system task management and performance analysis

Table 3 provides a comprehensive comparison between our proposed StyleGAN model and various other models, including Progressive GAN, CycleGAN, MGAN, and baseline models like VGG [20], CNN [21], and ResNet20 [22]. The evaluation encompasses crucial criteria such as image size, dataset size, epoch count, and accuracy. Notably, StyleGAN exhibits superior performance, particularly excelling in processing extensive 1024 × 1024 CelebA-HQ images. Leveraging TensorFlow and custom loss functions, StyleGAN achieves efficient processing over a dataset comprising 70,000 images across 10 epochs. This computational efficiency is attributed to the integration of Dlib and bespoke loss functions within the StyleGAN framework, as visually represented in Fig. 10.

Table 3: A comparison was made between the presented model StyleGAN with baseline techniques such as Progressive GAN, CycleGAN, MGAN, VGG, CNN, and ResNet20

Method	Dataset	Image_size	No. of samples	No. of epochs	Accuracy (%)
StyleGAN (Our)	CelebA-HQ	1024 × 1024	70,000	10	93.84
Progressive GAN	FFHQ	1024 × 1024	70,000	10	90.27
CycleGAN	CelebA	178 × 218	200,000	10	89.80
MGAN	CASIA WebFace	60 × 60	10,000	10	80.80
VGG	CIFAR-10	32 × 32	60,000	10	83.0
CNN	FCV Fingerprints	384 × 384	120,000	10	89.32
ResNet20	CIFAR-10	32 × 32	60,000	10	92.43

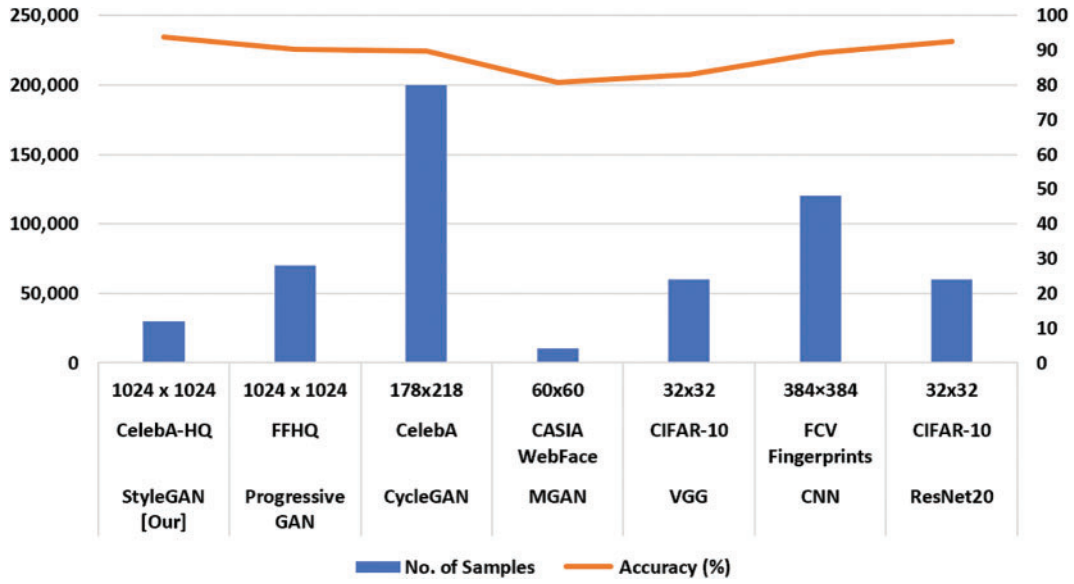

Figure 10: Comparison of the proposed model with rest of discussed models including progressive GAN, Cycle GAN, MGAN, VGG, CNN, and ResNet20

In contrast, Progressive GAN, despite requiring more epochs due to a smaller dataset, showcases remarkable generation time efficiency for large images through OpenCV and generic losses. This makes it well-suited for real-time applications leveraging OpenCV's edge features in embedded systems. Resource-constrained implementations may opt for lightweight models like MGAN and VGG, albeit

with a trade-off in accuracy. Dlib's face analysis pipelines can mitigate these accuracy costs, enhancing the reliability of these models. Crucially, StyleGAN outperforms all counterparts with an exceptional accuracy rating of 93.84%. The study underscores the synergistic effects of custom losses, Dlib, and Adam optimization in producing high-fidelity face embeddings crucial for accurate identification tasks. Additionally, tests on StyleGAN derivatives consistently validate correctness and speed, affirming the inherent advantages of the framework. Fig. 11 visually compares the outputs of StyleGAN, Progressive GAN, CycleGAN, and WGAN, highlighting StyleGAN's superior performance in terms of high resolution and image integrity.

Figure 11: GAN model outputs-A visual comparison of outputs generated by StyleGAN, progressive GAN, CycleGAN, and WGAN when processing random images, underscoring the superior performance of StyleGAN in high-resolution and image fidelity

The observed speed-accuracy tradeoffs show that StyleGAN is suitable for high-performance areas where privacy-preserving identification is required overall. Compared with baseline attempts based on CNN/VGG architectures, StyleGAN outputs show increased perceptual quality and feature retention as seen by the lower Fréchet Inception Distance (FID) and similarity losses. TensorFlow outperforms competitors like OpenCV, Dlib, and MGAN when datasets grow exponentially, underscoring StyleGAN's comparative advantage in the face recognition space. StyleGAN distinguishes itself as a robust and versatile method that surpasses alternative models in terms of precision, effectiveness, and confidentiality preservation. It is at the forefront of facial recognition technology because to its adaptability to a wide range of application situations and its ability to handle increasingly large datasets effectively.

Ablation Study: The ablation study systematically evaluates key components, including Blockchain authentication, GAN-based image synthesis, Ray parallelization, and Dlib biometrics, within the privacy-enhancing face recognition framework. Disabling blockchain compromises cryptography-backed integrity, limiting synthetic facial variety impacts model robustness, eliminating distributed computing hampers efficiency, and excluding Dlib facial mappings impairs out-of-the-box recognition capabilities. This underscores the vital importance of each element, showcasing their collective role in an effective, safe, and precise face recognition system with enhanced privacy. The symbiotic integration of trustless identity, artificial biometrics, scalable infrastructure, and performant algorithms achieves a balance between accuracy, security, and privacy in ethical facial analysis.

5 Conclusion

In the dynamic landscape of digital technology, facial recognition systems have become pervasive across various industries, giving rise to concerns about data security, privacy, and ethical implications. Addressing these challenges, our research presents an inclusive framework for privacy-centric face recognition. Leveraging advanced technologies such as distributed computing, Blockchain, and GANs, our system marks a paradigm shift. Notably, GANs generate highly realistic synthetic faces, diversifying training data while safeguarding user privacy. The incorporation of Blockchain ensures secure and immutable identity verification, mitigating data tampering risks and unauthorized access. Enhanced by distributed computing, our study demonstrates resilience and scalability, efficiently processing extensive face data while adhering to stringent privacy protocols. The research validates the framework's efficacy, surpassing alternative approaches in privacy preservation and performance. Our system contributes significantly to advancing face recognition technology, striking a delicate balance between privacy, scalability, and accuracy. Ultimately, the study aims to offer secure facial recognition system.

Acknowledgement: The authors would like to acknowledge Princess Nourah bint Abdulrahman University Riyadh, Saudi Arabia, for paying the Article Processing Charges (APC) of this publication.

Funding Statement: This project is funded by "Researchers Supporting Project Number (PNURSP2024R409)", Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author Contributions: Conceptualization, Methodology, and Writing original draft, Muhammad Ahmad Nawaz Ul Ghani; Supervision, Kun She; Review and editing, Arslan Rauf, Shumaila Khan, Javed Ali Khan, Eman Abdullah Aldakheel and Doaa Sami Khafaga.

Availability of Data and Materials: Data will be made available on request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Raju, B. C. Rao, K. Saikumar, and N. L. Pratap, "An optimal hybrid solution to local and global facial recognition through machine learning," in *A Fusion Artif. Intell. Internet Things Emerg. Cyber Syst.*, vol. 6, no. 1, pp. 203–226, 2022. doi: 10.1007/978-3-030-76653-5.

[2] S. Z. E. Mestari, G. Lenzini, and H. Demirci, "Preserving data privacy in machine learning systems," *Comput. Secur.*, vol. 137, no. 6, pp. 103605, 2024. doi: 10.1016/j.cose.2023.103605.

[3] D. Almeida, K. Shmarko, and E. Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks," *AI Ethics*, vol. 2, no. 3, pp. 377–387, 2022. doi: 10.1007/s43681-021-00077-w.
[4] E. Farooq and A. Borghesi, "A federated learning approach for anomaly detection in high performance computing," in *Proc. IEEE ICTAI*, Atlanta, USA, 2023, pp. 496–500.
[5] M. O. Oloyede, G. P. Hancke, and H. C. Myburgh, "A review on face recognition systems: Recent approaches and challenges," *Multimed. Tools Appl.*, vol. 79, no. 37, pp. 27891–27922, 2020. doi: 10.1007/s11042-020-09261-2.
[6] Z. Qin, Q. Chen, Y. Ding, T. Zhuang, Z. Qin and K. K. R. Choo, "Segmentation mask and feature similarity loss guided GAN for object-oriented image-to-image translation," *Inform. Process Manag.*, vol. 59, no. 3, pp. 102926, 2022. doi: 10.1016/j.ipm.2022.102926.
[7] R. A. Waelen, "The struggle for recognition in the age of facial recognition technology," *AI Ethics*, vol. 3, no. 1, pp. 215–222, 2023. doi: 10.1007/s43681-022-00146-8.
[8] C. Bouras and E. Michos, "An online real-time face recognition system for police purposes," in *Proc. ICOIN*, Jeju Island, Korea, 2022, pp. 62–67.
[9] R. Datta Rakshit, A. Rattani, and D. R. Kisku, "An LDOP approach for face identification under unconstrained scenarios," *J. Exp. Theor. Artif. Intell.*, vol. 11, no. 14, pp. 1–49, 2023. doi: 10.1080/0952813X.2023.2183274.
[10] Y. Lu, "Implementing blockchain in information systems: A review," *Enterp. Inf. Syst.*, vol. 16, no. 12, pp. 2008513, 2022.
[11] G. Revathy, K. Bhavana Raj, A. Kumar, S. Adibatti, P. Dahiya and T. M. Latha, "Investigation of E-voting system using face recognition using convolutional neural network (CNN)," *Theor. Comput. Sci.*, vol. 925, no. 2, pp. 61–67, 2022. doi: 10.1016/j.tcs.2022.05.005.
[12] S. Iqbal, A. N. Qureshi, M. Alhussein, K. Aurangzeb, and M. S. Anwar, "AD-CAM: Enhancing interpretability of convolutional neural networks with a lightweight framework-from black box to glass box," *IEEE J. Biomed Health*, vol. 28, no. 1, pp. 514–525, 2023. doi: 10.1109/JBHI.2023.3329231.
[13] S. B. Chaabane, M. Hijji, R. Harrabi, and H. Seddik, "Face recognition based on statistical features and SVM classifier," *Multimed. Tools Appl.*, vol. 81, no. 6, pp. 8767–8784, 2022. doi: 10.1007/s11042-021-11816-w.
[14] H. N. Vu, M. H. Nguyen, and C. Pham, "Masked face recognition with convolutional neural networks and local binary patterns," *Appl. Intell.*, vol. 52, no. 5, pp. 5497–5512, 2022. doi: 10.1007/s10489-021-02728-1.
[15] W. Hariri, "Efficient masked face recognition method during the COVID-19 pandemic," *Signal Image Video P*, vol. 16, no. 3, pp. 605–612, 2022. doi: 10.1007/s11760-021-02050-w.
[16] H. T. S. ALRikabi, I. A. Aljazaery, J. S. Qateef, A. H. M. Alaidi, and M. Roa'a, "Face patterns analysis and recognition system based on quantum neural network QNN," *Int. J. Interac. Mob. Tech.*, vol. 16, no. 8, pp. 35–48, 2022. doi: 10.3991/ijim.v16i08.30107.
[17] W. Feng *et al.*, "A privacy protection scheme for facial recognition and resolution based on edge computing," *Secur. Commun. Netw.*, vol. 2022, pp. 12, 2022. doi: 10.1155/2022/4095427.
[18] H. Tian, T. Zhu, and W. Zhou, "Fairness and privacy preservation for facial images: GAN-based methods," *Comput. Secur.*, vol. 122, pp. 102902, 2022. doi: 10.1016/j.cose.2022.102902.
[19] M. Zhang, L. Wang, Y. Zou, and W. Yan, "Analysis of consumers' innovation resistance behavior to facial recognition payment: An empirical investigation," in *Proc. WHICEB*, Wuhan, China, 2022, vol. 01, pp. 129–138.
[20] Z. Shen, T. Zhong, H. Sun, and B. Qi, "RRN: A differential private approach to preserve privacy in image classification," *IET Image Process*, vol. 17, no. 7, pp. 2192–2203, 2023. doi: 10.1049/ipr2.12784.
[21] M. Mohammadi, F. Sabry, W. Labda, and Q. Malluhi, "Privacy-preserving deep-learning models for fingerprint data using differential privacy," in *Proc. ACM IWSPA*, Charlotte, NC, USA, 2023, pp. 45–53.
[22] J. W. Lee *et al.*, "Privacy-preserving machine learning with fully homomorphic encryption for deep neural network," *IEEE Access*, vol. 10, pp. 30039–30054, 2022. doi: 10.1109/ACCESS.2022.3159694.