Journal of King Saud University - Computer and Information Sciences 36 (2024) 102036

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University - Computer and Information Sciences

journal homepage: www.sciencedirect.com

Full length article

Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition

Muhammad Ahmad Nawaz Ul Ghani [a], Kun She [a,*], Muhammad Arslan Rauf [a], Masoud Alajmi [b], Yazeed Yasin Ghadi [c], Abdulmohsen Algarni [d]

[a] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China
[b] Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[c] Department of Computer Science, Al Ain University, United Arab Emirates
[d] Department of Computer Science, King Khalid University, Abha 61421, Saudi Arabia

ARTICLE INFO

Keywords:
Face recognition
GANs
Blockchain
Clustering
Privacy
Security

ABSTRACT

In recent years, facial recognition technology has become increasingly integrated into society, making privacy protection crucial. Previous techniques offered minimal secrecy safeguards through simple obscuration methods. This paper addresses the strict privacy requirements of face image data by developing a novel framework that synergistically integrates Generative Adversarial Networks (GANs), clustering algorithms, and Blockchain technology. The methodology proposes a cutting-edge Privacy-Preserving Self-Attention GAN (PPSA-GAN) to generate realistic synthetic facial imagery. An integrated mini-batch K-means clustering algorithm anonymizes these images into distinct groupings, maximizing privacy preservation. Blockchain integration complements the system by fortifying trust through decentralized ledgers for transparent yet secure data storage and auditing. Rigorous benchmarking on the CelebA dataset confirms the PPSA-GAN architecture's state-of-the-art performance, attaining an impressive Inception Score of 13.99 and a Fréchet Inception Distance of 35.50. The mini-batch clustering forms 125 distinct clusters, effectively anonymizing facial attributes within the synthetic images. Blockchain integration further bolsters privacy assurances via tamper-proof historical records, showcasing precision, recall, F1-score, and accuracy values of 0.948, 0.938, 0.943, and 0.947, respectively. This multifunctional framework represents a novel contribution, fostering an ethical technological ecosystem that balances progress and privacy. Prospective deployment horizons encompass identity verification, surveillance infrastructure, and augmentation of medical image repositories, seeding an enlightening future for facial recognition domains.

1. Introduction

The development of artificial intelligence (AI) models is a result of the notable advancements in AI technologies, particularly in machine learning and deep learning (Liu et al., 2023). These models are useful in many image processing and data analysis applications; one of its most remarkable features is that they may provide realistic and captivating samples without requiring complex structural characteristics (Wang et al., 2021; Taha et al., 2023). Because AI frameworks can use generative models, there has been a lot of interest in their use. These models generate samples with properties present in the training data that are similar to the sample distributions they are taught (Makhzani et al., 2015). Data privacy seems to be a major issue when sharing data from human wearable devices in emerging computing domains like federated learning, edge computing, and adversarial machine learning (Liu et al., 2021b). The acquisition of multimedia data, especially images and movies, has been considerably enhanced by recent developments in multimedia devices, including phones, cameras, and sensors.

A significant number of images are being used widely by individual users on social networks, governments, and corporations as a result of

* Corresponding author.
E-mail addresses: ghaniokara@hotmail.com (M.A.N. Ul Ghani), kun@uestc.edu.cn (K. She), marslanrauf@hotmail.com (M.A. Rauf), ms.alajmi@tu.edu.sa (M. Alajmi), Yazeed.ghadi@aau.ac.ae (Y.Y. Ghadi), a.algarni@kku.edu.sa (A. Algarni).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2024.102036
Received 29 November 2023; Received in revised form 11 April 2024; Accepted 11 April 2024
Available online 16 April 2024

the development of the Internet of Things (IoT) and the Internet of Multimedia Things (IoMT). The most prevalent sort of data is image data, which has the potential to reveal private information if it contains sensitive information (Yu et al., 2020). Weak security mechanisms on Internet of Things (IoT) devices are linked to multiple privacy risks, including automatic data exchange and the sharing of indirect identifiers through connected devices. The public has recently become more aware of the serious worry of privacy leaks caused by data mining assaults on photographs.

In recent years, there has been a growing emphasis on data integrity and validation, with Generative Adversarial Networks (GANs) emerging as a viable method for distinguishing between legitimate and faked data due to their adversarial training mechanisms (Goodfellow et al., 2014). Aleroud et al. (2023) have focused primarily on strengthening privacy and anonymity for Internet of Things (IoT) users through the use of GANs and micro aggregation, lowering dataset size while maintaining data accuracy. This situation highlights the critical necessity for strengthening privacy protections as emerging technologies continue spreading. Despite rapid advances in facial recognition capabilities, lingering worries over data security remain unresolved (Saabia et al., 2019; Mahmoud et al., 2011). Contemporary investigations exploring advanced obfuscation techniques for safeguarding sensitive visual data indicate that adaptive protections still lag behind needs (Yu et al., 2020; Abd El-Hafeez, 2010).

To balance expanding facial analytics utilities while still respecting user privacy, active efforts have focused on methodologies encompassing scrambling personal identification markers and pinpointing sensitive content. However, originally promoted strategies like image blurring often critically degrade accuracy and usability. Tackling such limitations necessitates sophisticated frameworks united innovations in adversarial learning and tamper-resistant historical records (Yu et al., 2016; Ullah et al., 2018).

This research puts forward a novel consolidation embedding privacy-focused enhancements within adversarial learning architectures, markedly amplifying output quality. By concentrating the model focus on salient inputs, these enhancements significantly boost realism and noise reduction. Extensive benchmarks against state-of-the-art methodologies exhibit the proposed mechanism's unmatched capabilities in delivering privacy-preserving synthetic facial imagery without compromising on quality or versatility Ongoing initiatives seek to extend this approach across affiliated application terrains, including biometrics, surveillance, and other fields where user privacy and data security are paramount (Feuerpfeil et al., 2020; Eman et al., 2023). This research fills a knowledge gap by incorporating GANs for data generation and clustering for image anonymization, as well as Blockchain for data integrity and authenticity preservation, addressing the challenges of securely storing generated images and data annotation in today's data-rich environment.

By fusing GANs and Blockchain, this study seeks a novel solution that enhances the AI's generative models while reinforcing generated content's storage and traceability to ensure resilience against tampering and unauthorized alterations. The proposed innovation lies in harnessing the power of GANs alongside the security features of Blockchain to create a new paradigm where generated images are realistic, traceable, and verifiable. Although both technologies have been extensively studied in isolation, their integrated application remains relatively new. The recognition of a substantial technological gap in data integrity, as evidenced in academic literature and practical applications, has motivated us to explore this issue further. Here are the principal contributions of this study:

- Develop a robust GAN-based framework augmented with a privacy-preserving self-attention (PPSA) mechanism to generate synthetic facial images that exhibit high realism, closely resembling real faces, while maintaining stringent privacy safeguards.
- Integrate Blockchain technology with the PPSA GANs framework to establish an immutable ledger for securely storing and auditing facial recognition transactions.
- Implement mini-batch clustering algorithms as part of the privacy preservation strategy, augmented by the self-attention mechanism, to further enhance data anonymization and fortify user privacy.
- Evaluate the performance and practical applicability of the integrated system in real-world scenarios, such as identity verification and access control.

The rest of the paper is structured as follows: In Section 2, a thorough assessment of the literature is presented, including earlier studies on GANs, clustering strategies, and Blockchain technology concerning the creation of face images and privacy protection. The suggested research framework is described in depth in Section 3, along with the PPSA-GAN model's architecture, the addition of mini-batch clustering, and the use of Blockchain for data security. Section 4 presents the experimental results, which serve to validate and benchmark the proposed framework using both quantitative metrics and qualitative evaluations. A comprehensive analysis is provided in Section 5, which discusses the limitations, and time computation, compares various methods, and discusses the ramifications of the results. The ablation study is discussed in Section 6. The main contributions and future directions are outlined in Section 7 Conclusion, which also emphasizes the research's importance in creating morally sound facial recognition technologies.

2. Related work

This section overviews the most recent literature on image privacy protection, deep learning for object identification in images, and multi-task learning. Generative Adversarial Networks (GAN) for data creation and perturbation are among the deep learning approaches that have been the subject of the majority of recent investigations (Chen et al., 2019). It is now known that while GAN is a privacy-enhancing technique, there is a chance that the training sample privacy information may be unintentionally disclosed. The distribution is concentrated around training samples as a result of the adversarial training techniques and the deep neural network's high model complexity (Xie et al., 2018). Bonneau et al. (2009) proposed "privacy suites" that provide users with a set of privacy options specified by "expert" users or trustworthy persons. This method allows frequent users to utilize a preset configuration or modify it modestly.

Using their exact location and time of day, Ravichandran et al. (2009) investigated how to predict a user's privacy preferences with relation to location-based data. A privacy wizard was developed by Fang and LeFevre (2010) to enable users to share login credentials with their peers. Initially, this wizard asks users to grant privacy labels to individual friends. Subsequently, it utilizes this data to construct a classifier that use friend profile classification to automatically assign privacy labels to friends without labels.

Recent research has focused on enhancing GAN training efficiency and performance, including the application GAN (Goodfellow et al., 2014), including applying batch normalization, input normalization, and various activation functions that can be deployed (Ali et al., 2019b). For example, Wasserstein distance has been introduced as a new objective, with non-zero gradients anywhere in the Wasserstein GAN (WGAN) work (Karras et al., 2017). Its implementation was simple: removing the objective's sigmoid function and adding weight clipping to the discriminator network. It is shown that WGAN is free of many of the issues with the original GAN, including unstable training procedures and mode collapse. The Loss-Sensitive GAN is a related project to the WGAN, with the aim of maximizing loss for bogus data and minimizing loss for real data. The objective functions used in this

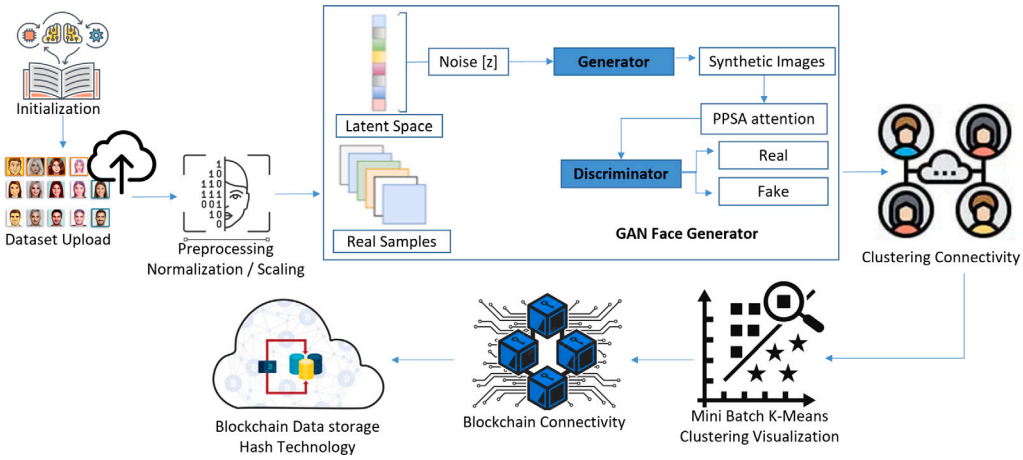

Fig. 1. Architecture diagram of methodological structure where interconnected modules depict the sequential data flow.

work have non-vanishing gradients, which is a common feature of Least Square GAN, WGAN, and Loss-Sensitive GAN.

Klemperer et al. (2012) explored the value of user-provided keywords and descriptions when tagging images to help users create and manage access-control rules more intuitively. Moreover, virtual batch normalization (VBN) has improved neural network performance, particularly in enhancing the performance of Deep Convolutional GANs (DCGAN). VBN normalizes individual samples based on statistics derived from a predetermined reference batch, though it is computationally intensive, requiring concurrent forward propagation of two mini-batches (Karras et al., 2017).

With the help of Generative Adversarial Networks (Yan and Mikolajczyk, 2015) there were able to produce 64 × 64 resolution images from textual descriptions. Qi et al. (2021) Presented StackGAN, a two-phase method to improve the generative process: the first stage produces images with minimal visual content in low resolution, and the second stage refines them to produce images with more detailed visual information in high resolution. By simultaneously approximating multiple distributions, the authors of the StackGAN method were able to stabilize GAN training and handle both conditional and unconditional generative tasks. Utilizing a text-conditioned auxiliary classifier to diversify artificial images and enhance their structural coherence, TAC-GAN (Yan and Mikolajczyk, 2015) was created to integrate class information from text descriptions. In their work paper, Feuerpfeil et al. (2020) used a deep convolutional generative adversarial network (DCGAN), mainly applied to the well-known CelebFaces qualities Dataset (CelebA), to integrate specified qualities or circumstances to generate facial images. CDCGAN was used to describe this unique architectural design. The dependent network was developed to investigate the current state of the generative adversarial learning field. The three features (classes for glasses, pink cheeks, and goatees) were used to successfully produce fresh face images based on a portion of the original dataset.

The pursuit of enhancing Blockchain technology by leveraging innovative approaches to address its inherent challenges has led to the exploration of various solutions. Zheng et al. (2020) proposed a secret-sharing technology built upon GANs. This approach seeks to tackle three critical issues in the Blockchain ecosystem: low security, difficult recovery of lost keys, and inefficient communication. Corresponding to this, Heidari et al. (2023) introduced an instruction detection system (IDS) platform to enable secure data transfer over the Internet of Drones. Ensuring decentralization and privacy preservation, this system leverages Blockchain and zero-knowledge proof techniques to improve the registration and verification processes. Blockchain was used by the authors (Hu et al., 2019) to store detection results. But they created a Blockchain-driven reward system for their multi-microgrid (MMG) Collaborative Intrusion Detection (CID) system. A reduction in the false negative rate (FNR) is achieved with this cooperative approach. Single points of failure (SPoF) in data storage are eliminated.

To enhance the security and stability of the Intrusion Detection System (IDS) model training during the Federated Learning (FL) process, several studies (Liu et al., 2021a; Ali et al., 2019a) have integrated Blockchain technology. To improve the security and integrity of the IDS models, He et al. (2022) created a FL-based CID framework for UAV networks that uses Blockchain to store and distribute training models. The integration of federated learning and blockchain technologies can enable the development of secure and privacy-preserving generative adversarial networks (GANs) for advanced face recognition applications in high-performance computing (HPC) systems, where federated learning can significantly improve the performance of anomaly detection models while reducing the required training data by up to 15x (Farooq and Borghesi, 2023). As noted by He et al. (2022), Ullah et al. (2022), the aggregation process is still centralized even with the use of Blockchain in training. By using consensus methods based on Blockchain technology, the research by El Koshiry et al. (2023), in contrast of decentralizes the aggregation process. The process of aggregating local gradient updates into a global model is handled by multiple consensus nodes, such as miners, as opposed to a single central server. This ensures that the global model is properly aggregated even when individual hosts are attacking or malicious.

The existing literature has identified specific gaps that the proposed research aims to solve, particularly in achieving more efficient and secure data generation and preservation, especially in contexts where privacy and data integrity are critical. Existing frameworks often lack holistic integration of enhanced privacy defenses alongside high-fidelity synthetic data generation and resilient storage protocols. This research pioneeringly addresses these unmet needs through a consolidated framework synergizing generative adversarial networks (GANs) for quality image synthesis, clustering algorithms for anonymization, and blockchain's tamper-proof ledgers to enable trusted traceability. This unified amalgamation of state-of-the-art techniques creates an enhanced architecture harnessing complementary strengths to tackle pressing data privacy, integrity, and efficiency challenges pervasive in modern digital ecosystems.

3. Proposed research framework

To validate the comprehensive solution, rigorous experimentation was undertaken on the CelebA benchmark dataset encompassing over 202,599 facial images with 40 attribute annotations per celebrity image. A multi-faceted approach was pursued, fusing a privacy-preserving self-attention GAN architecture (PPSA-GAN) with mini-batch clustering flows for anonymity alongside blockchain integration to supply reliable

and immutable audit trails. The framework's methodological interconnectivity and sequential data processing workflows are visualized in Fig. 1 to emphasize the synergistic convergence of GANs, clustering procedures, and blockchain security protocols. The methodological structure is that, first of all dataset is uploaded and becomes the main source for the data processing pipeline. Preprocessing methods, such as normalization scaling, are used after dataset gathering to guarantee data quality and feature compatibility. Normalization promotes optimal performance in following algorithms by standardizing feature scales without altering underlying data distributions. Next, using the learned patterns from the preprocessed data, a Generative Adversarial Network (GAN) Face Generator is utilized to produce realistic face images. By adding synthetic cases, this stage enriches the dataset, increasing its diversity and enabling more thorough evaluations. After processing, the data is connected by clustering to find underlying patterns or groups in the dataset. Effective cluster analysis is carried out using the Mini Batch K-Means technique, yielding information about the distribution and separation of data points among clusters. Blockchain connectivity is incorporated into the pipeline after clustering to provide secureand open data management and storage. By utilizing Blockchain technology, tamper resistance, immutability, and decentralization are used to maintain data integrity and trustworthiness. Last but not least, data storage is made secureby Blockchain applications that use hash technology to create distinct cryptographic hashes that reflect the integrity of data blocks. These hashes are safely kept on the Blockchain, guaranteeing the legitimacy of the data and enabling quick retrieval and validation. All things considered, this sophisticated data processing approach integrates cutting-edge methods, from pretreatment to Blockchain integration, to promote reliable analyses and securedata management procedures.

3.1. Privacy-preserving self-attention GAN architecture (PPSA-GAN)

Specifically, the PPSA-GAN architecture seeks to amplify GAN models with embedded privacy enhancement modules that preserve sensitive information during synthetic facial image generation. Beyond facilitating high-fidelity outputs, privacy-preservation is imperative for ethical deployment. The integration of a self-attention mechanism markably augments the generator's capabilities by enabling focused concentration on salient inputs. This allows for the accurate capture of long-range dependencies within facial datasets to produce synthetic images exhibiting greater coherence and contextual relevance. By emphasizing meaningful facets in the input while disregarding noisy or irrelevant features, self-attention significantly enhances result quality. Such adaptive feature extraction contributes to the generator's capability to generate high-quality, diverse, and contextually relevant outputs across diverse domains. Algorithm 1 presents the PPSA-GAN privacy-focused GAN that generates secure data using self-attention. Integrating privacy mechanisms with generative models produces high-fidelity, privacy-preserving synthetic data. The PPSA-GAN algorithm is a Generative Adversarial Network architecture designed for image generation and facial expression recognition tasks. It consists of a Generator, Discriminator, and Classifier. The Generator generates synthetic images, while the Discriminator distinguishes between real and fake images. The Classifier performs facial expression recognition on the generated images. The algorithm alternates between updating the Discriminator and Generator weights based on their respective loss functions. It incorporates a self-attention mechanism to capture long-range dependencies in the input data. The Discriminator maximizes its output for real images and minimizes it for generated images. The Classifier is trained on features extracted from the Generator to perform expression recognition. The algorithm monitors training progress and stops when the GAN reaches equilibrium. Overall, PPSA-GAN integrates GANs, self-attention, and a Classifier for image generation and facial expression recognition.

Algorithm 1 PPSA-GAN Architecture

Initialize Generator G and Discriminator D with weights θ_G and θ_D
Initialize Adam Optimizer for G and D with learning rate η
for epoch = 1 to 30 **do**
  for real_images in $D_{\text{preprocessed}}$ **do**
    real_labels = $1 - 0.1 \times$ random()
    fake_labels = $0.1 \times$ random()
    noise_vector = sample_noise_batch()
    generated_images = G(noise_vector)
    loss_D = $-$mean(log(D(real_images))) $-$ mean(log(1 $-$ D(generated_images)))
    $\theta_D = \theta_D - \eta \times \nabla_{\theta_D}$loss_D
    // Generator Training
    noise_vector = sample_noise_batch()
    generated_images = G(noise_vector)
    loss_G = $-$mean(log(1 $-$ D(generated_images)))
    $\theta_G = \theta_G - \eta \times \nabla_{\theta_G}$loss_G ▷ Update Generator Parameters
  end for
end for
if GAN_reached_equilibrium() **then**
  print("GAN training reached equilibrium.")
end if
// Self-Attention Mechanism
$Q = X \times W_q$
$K = X \times W_k$
$V = X \times W_v$
$S = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)$
$O = SV$
// Discriminator Architecture
loss_D = $\max(D(q)) - \log(D(q)) + \log(1 - D(G(r)))$
$\theta_D = \theta_D - \eta \times \nabla_{\theta_D}$loss_D ▷ Update Discriminator Parameters
// Classification Loss for Facial Expression Recognition
features = $G_f(\xi, \theta_f)$
predictions = G_c(features, θ_c)
Loss_c = $\sum L_c$(predictions, y_i)
$\theta_f = \theta_f - \eta \times \nabla_{\theta_f}$Loss_c ▷ Update Classifier Parameters
$\theta_c = \theta_c - \eta \times \nabla_{\theta_c}$Loss_c ▷ Update Classifier Parameters
// Equilibrium Check (Optional)
if GAN_reached_equilibrium() **then**
  print("GAN training reached equilibrium.")
end if

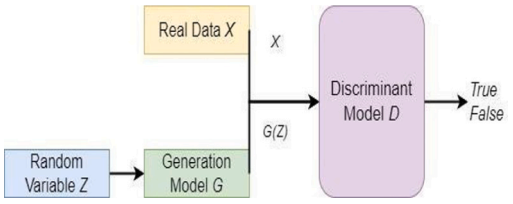

Fig. 2. Overview of the GAN working structure to present generator and discriminator.

3.1.1. Generator architecture

Within this GANs architecture, meticulous attention was directed towards the construction of the generator. The generator network, denoted as G, aims to generate synthetic data instances that can effectively deceive the discriminator, as shown in Fig. 2. Where the Generator creates synthetic images to deceive the Discriminator in adversarial training. This competition strengthens both networks, enhancing the generator's ability to produce realistic data.

Employing transposed convolutions (deconvolutions), here adeptly composed the transformation of the noise vector, effectually yielding a synthetic image. The objective was to formulate a generator endowed

with the capacity to generate synthetic images; discerning them from authentic data became a formidable task. The loss function for the generator is defined as in Eq. (1):

$$\mathrm{GNLF} = \min(\mathrm{GN}) \sum \left[E[p_{\mathrm{inf}}(q)] \cdot \log(1 - \mathrm{DN}(q))\right] \quad (1)$$

In this equation, 'E' represents the expectation value, 'p_inf(q)' signifies the probability distribution of 'q' belonging to the original information, 'DN' denotes the discriminator network, and 'q' represents the initial image. 'GN' means the generator network responsible for producing the secret key.

3.1.2. Self-attention mechanism

In this research integrated a self-attention mechanism to improve the generator's ability to produce realistic data. This pivotal addition allows the generator to capture long-range dependencies and produce more coherent images. The self-attention mechanism, represented by a self-attention layer, operates on intermediate feature maps, enabling the Generator better to understand global dependencies during the image generation process. This added capability dramatically contributes to the quality of the synthetic data produced. The input sequence X has a T length and a d dimension. The number of attention heads is H. We begin by projecting the input sequence X into queries (Q), keys (K), and values (V) using learned projection matrices.

(1) Query, Key, and Value Projection:

$$Q = XW_q$$
$$K = XW_k$$
$$V = XW_v$$

(2) Self-Attention Scores:

$$S = \mathrm{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)$$

(3) Output of Self-Attention:

$$O = SV$$

In these equations, Q, K, and V are obtained by projecting the input feature maps X using learnable weight matrices W_q, W_k, and W_v. The self-attention scores S are computed by applying the softmax function to the scaled dot product of Q and K, where $\sqrt{d_k}$ is a scaling factor. Finally, the output O is calculated as the weighted sum of the values V based on the self-attention scores S.

3.1.3. Discriminator architecture

In parallel, the discriminator was intricately devised, replete with convolutional layers geared towards the processing and assessing of images, differentiating between genuine and counterfeit instances. The discriminator network, denoted as D, is designed to distinguish between real and synthetic data instances. Its pivotal role lay in its adversarial confrontation with the generator. By categorizing images as real or spurious, the discriminator assumed the mantle of the generator's adversary. This adversarial interplay compelled the generator to continually refine its creative process, aiming to deceive the discriminator adeptly. This dynamic interplay facilitated the evolution of increasingly realistic images over time. The loss function for the discriminator is defined as in Eq. (2):

$$\mathrm{DNLF} = \max(\mathrm{DN}) \sum [E[p_{\mathrm{inf}}(q)] \cdot \log(\mathrm{DN}(q))] + E[p_{\mathrm{inf}}(q)] \cdot \log(1 - \mathrm{DN}(\mathrm{GN}(r))) \quad (2)$$

In this equation, 'DN' represents the discriminator network responsible for distinguishing real and fake data, 'q' denotes the original image, 'GN' signifies the generator network, and 'r' represents the data retrieved from the transformation domain. The DNLF loss function serves to enhance the discriminator's classification accuracy. Given that the generated key should closely resemble the data in the transformed domain, the Discriminator Network faces a challenging task in differentiating between them. Intricate Generator and Discriminator architectures enable high-quality image generation and discerning real from synthetic in Fig. 3. Complex neural networks empower GAN models to create realistic, nuanced data.

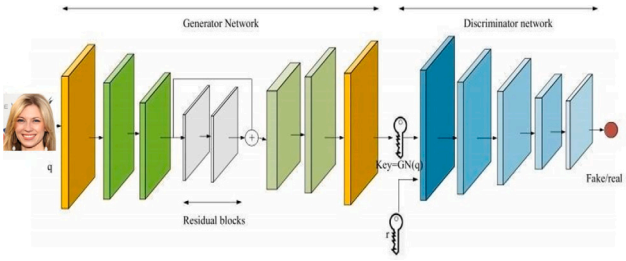

Fig. 3. GAN Intricate architectures empower generator and discriminator.

Table 1
GAN architecture, Multiple convolutional and deconvolutional layers systematically transform latent vectors into realistic synthetic images.

Layer	Kernel	Neurons	Activation
Fully connected	4 × 4	8192(4 × 4 × 512)	–
Convolutional	4 × 4	256	ReLU
Convolutional	4 × 4	128	ReLU
Convolutional	4 × 4	3	Tanh

We consistently utilized the Binary Cross-Entropy Loss function to evaluate this model's performance throughout the training phase. This pivotal loss function served as a critical metric, effectively quantifying the discriminator's ability to distinguish between authentic and synthetic images while assessing the generator's capability to produce images that effectively deceived the discriminator.

The PPSA-GAN model comprises a generator and a discriminator, both integral to the generation and evaluation of synthetic images. The generator, composed of multiple layers, transforms latent vectors of random noise into realistic images. Starting with a fully connected (linear) layer, it progressively upsamples the latent vector into larger images through a sequence of transposed convolutional layers enhanced with batch normalization. The initial deconvolutional layer transforms the latent vector into a (4 × 4 × N) tensor, where 'N' represents the depth of the first deconvolution layer (conv-dim). Subsequent layers employ transposed convolutions with varying kernel sizes, strides, and padding to produce images of increasing resolution. The final deconvolutional layer upscales the tensor to 32 × 32 × 3, representing RGB images, ensuring compatibility with the input dataset. The first deconvolutional layer performs transposed convolution with a kernel size of 4, a stride of 1, and zero padding. The second deconvolutional layer continues to upsample the previous output, utilizing a transposed convolution with a kernel size of 4, a stride of 2, and padding of 1. Finally, the third deconvolutional layer further upsamples the tensor to 32 × 32 × 3, representing the RGB image, as shown in Table 1. The discriminator, pivotal in discerning real images from synthetic ones, comprises three convolutional layers with leaky ReLU activation functions. These layers process RGB images, progressively learning to distinguish between genuine and generated images. Table 2 presents the properties of the first convolutional layer, which processes RGB images with three input channels and applies a kernel size of 4, a stride of 2, and a padding of 1. Subsequently, this model employs a second convolutional layer with identical parameters. The third convolutional layer, which further increases the depth to 'conv-dim', uses the same kernel size, stride, and padding as the previous layers.

3.1.4. Training process

During the training process, carefully considered the extensive scale of dataset, leading us to conduct training throughout 30 epochs. This

Table 2
Discriminator architecture successive convolutional layers filter inputs to classify images.

Layer	Kernel	Neurons	Activation
Convolutional	4 × 4	32	LReLU
Convolutional	4 × 4	64	LReLU
Convolutional	4 × 4	128	LReLU
Fully connected	–	1	–

choice was driven by the substantial temporal and computational resources required for an extended training duration, potentially extending to hours or even days. This approach allowed us to strike a delicate balance between achieving satisfactory results regarding the generated images and conserving computational resources. The GAN operates through a dynamic interplay between the generator and discriminator during training. This training process functions competitively, where the generator strives to generate data that can effectively deceive the discriminator. Conversely, the discriminator aims to improve its proficiency in distinguishing real data from synthetic data.

3.1.5. Equilibrium

Ideally, during GAN training, the process reaches an equilibrium where the generator generates data almost indistinguishable from real data. The discriminator becomes uncertain about whether the encountered data is real or fake, with a size of 1. After that, there is ReLU and batch normalization. Subsequently, four modules undergo convolution operation, in turn. Next comes convolution, followed by the average pooling operation with a 2 × 2 window size. Following the average pooling process, dropout is employed. Two fully connected layers and one Softmax layer receive the extracted features as input at the end. There are seven different categories for the 512-dimensional feature vector, and the classification yields the facial expression recognition outcomes. The classification loss Ec of the classifier is defined as in Eq. (3):

$$E_c(\theta_f, \theta_c) = \sum_{i=1}^{N} L_c\left(G_c\left(G_f(x_i;\theta_f);\theta_c\right), y_i\right) \tag{3}$$

where x_i represents the original input image, θ_f denotes the feature extractor's parameter (G_f), θ_c represents the classifier's parameter (G_c), y_i stands for the actual label, and L_c signifies the classification loss. Achieving equilibrium involved meticulous minimization of the loss function. To optimize the model, we employed the Adam Optimizer — a widely adopted choice within the GAN framework for its proven efficacy and adaptability. Skillful use of the Adam optimizer dynamically adjusted weights for both the discriminator and the generator, expediting the convergence process and fostering a more stable training trajectory. This calibrated approach led the proposed GAN model to converge towards an optimal equilibrium. In this state, the Generator flawlessly produced synthetic data of a highly authentic nature, while the Discriminator adeptly distinguished between real and counterfeit images. The success of this convergence owes much to the judicious selection of the Adam Optimizer. This choice accelerated convergence dynamics and substantially contributed to the model's enhanced performance. The optimization of the generator's parameters θ_G aimed to produce synthetic images that deceive the discriminator is defined as in Eq. (4):

$$\theta_G \leftarrow \theta_G - \eta \cdot \nabla_{\theta_G} L_G \tag{4}$$

Similarly, aiming to enhance the discriminator's ability to distinguish between real and generated images, the discriminator's parameters θ_D are updated using gradient descent is defined as in Eq. (5):

$$\theta_D \leftarrow \theta_D - \eta \cdot \nabla_{\theta_D} L_D \tag{5}$$

The iterative training process spans multiple epochs, with each epoch encompassing the sequential training of the discriminator and generator networks on real and synthetic image batches. In each epoch, the discriminator's parameters are updated by minimizing its adversarial loss, guided by the divergence between its predictions for real images and synthetic images generated by the generator. Concurrently, the generator's parameters

3.2. Integrating mini-batch K-means clustering

Clustering is a machine learning and data analysis technique that involves grouping data points based on their similarity or inherent patterns to uncover hidden structures or relationships, enabling comprehensive analysis and insights extraction. This work employs effective divided k-means clustering methods that can reveal latent patterns in large-scale facial image datasets to strengthen anonymity barriers. In contrast to standard clustering techniques, divided k-means does not require entire dataset ingestion; instead, it processes random data partitions at random times in each cycle. This guided stochastic sampling significantly lowers memory requirements and processing overhead, allowing for quick analysis of large quantities. The sensitivity to initial centering circumstances caused by gradient descent traps is reduced by random batching. The resulting cluster centroids clearly show up as distinct clusters, confirming the technique's usefulness for extracting significant facial attributes to improve privacy. While accelerating convergence and bolstering result robustness, it critically retains clustering precision compared to established non-mini-batch methodologies. This optimal balance between expedited clustering and accurate partition fidelity powered by selective batch sampling aptly supplements existing GAN-driven facial image syntheses and privacy enhancement modules. These centroids are plotted alongside data points and color-coded differently for clarity and ease of interpretation. Algorithm 2 presents Privacy-Preserving Self-Attention GAN (PPSA-GAN) architecture, clustering using Mini-Batch K-Means. Integration Merging GANs and clustering strengthens privacy protections for images. Integrating state-of-the-art techniques creates an enhanced system harnessing complementary strengths. First, it initializes the Generator and Discriminator weights and optimizers, then trains them alternately using the previous algorithm's procedure. After training, it randomly initializes K centroids and assigns data points to clusters based on proximity. It then iteratively refines the clustering by processing mini-batches: sampling a mini-batch, assigning its points to clusters, updating centroids based on assignments, and updating global assignments. This iterative process continues until reaching the maximum iterations, outputting the trained PPSA-GAN model, final cluster assignments, and centroids. Incorporating clustering aims to group similar data points, potentially improving the Generator's performance by leveraging these clusters during training.

3.3. Blockchain for secure data storage

To ensure the security and integrity of data throughout the entire process, leveraged Blockchain technology. Blockchain provides an immutable and tamper-proof ledger for storing critical information, such as metadata, data provenance, and access control rules. As each stage of data processing pipeline progresses, relevant information is recorded on the Blockchain, creating a transparent and traceable record of data transformations and operations. To achieve this, we have devised a BlockData class. This container holds the essential information required to create individual blocks within the Blockchain. Integrating mini-batch k-means with a Blockchain offers a robust solution for clustering and securely storing representative synthetic images. This fusion integrates the efficiency of mini-batch k-means, well-suited for large datasets, with Blockchain's security and immutability attributes. A mining block is used to create a new block. First, it calculates a nonce value such that the hash of the block data starts with a certain number of leading zeros. This is a primary proof-of-work mechanism, similar to

Algorithm 2 PPSA-GAN Architecture with Mini-Batch K-Means

Require: $D_{\text{preprocessed}}$, K, B, max_iter
Ensure: Trained PPSA-GAN model (G, D), Final cluster assignments C, Final centroids μ
Initialize G and D with weights θ_G and θ_D
Initialize Adam Optimizer for G and D
for epoch in range$(1, 31)$ **do**
  for real_images in $D_{\text{preprocessed}}$ **do**
    # Discriminator Training (as in previous algorithm)
    # Generator Training (as in previous algorithm)
  end for
end for
μ = randomly_initialize_centroids($D_{\text{preprocessed}}, K$)
C = assign_to_clusters($D_{\text{preprocessed}}, \mu$)
iter_count = 0
while iter_count < max_iter **do**
  mini_batch = random_sample($D_{\text{preprocessed}}, B$)
  $C_{\text{mini\_batch}}$ = assign_to_clusters(mini_batch, μ)
  μ = update_centroids(mini_batch, $C_{\text{mini\_batch}}, K$)
  C = update_global_assignments($C, C_{\text{mini\_batch}}$)
  iter_count+ = 1
end while
Output: Trained PPSA-GAN model (G, D), Final cluster assignments C, Final centroids μ

what is used in many Blockchain systems. Each block within Blockchain comprises several crucial components:

Index: This serves as a unique identifier for every block.

A timestamp:: This record the time at which the block is added to the Blockchain.

Image data:: This represents the actual content of the image that intend to store within the block.

A nonce:: This is a random number that comes into play during the mining process, as explained below.

Now, the mining process involves a simulation where actively search for the appropriate nonce. When integrated with the block's data, this nonce generates a hash with a specified number of leading zeros. The number of leading zeros required determines the complexity of the mining process. More leading zeros indicate a higher level of complexity, which, in turn, requires more computational effort to identify the correct nonce. This deliberate increase in computational power enhances the security of Blockchain, making it resistant to fraudulent interference.

As new blocks are mined, they seamlessly integrate into the existing Blockchain structure, effectively extending it. This continuous network of interconnected blocks ensures the continuity and integrity of the data, serving as a robust safeguard against tampering and data alterations. To facilitate the visualization of Blockchain and its associated data and compare it to its corresponding block index and hash value. This comparison aids in evaluating how well the image data fits into the overarching Blockchain structure.

This proposed system capitalizes on Blockchain principles, including the mining process, cryptographic hashing, and the preservation of immutable data. In computing the process, it provides a secure storage solution and authorized verification for a specific image data set. This approach enhances accountability and integrity within the Blockchain ecosystem have established. Algorithm 3 presents Blockchain Integration with Mini-Batch K-Means Clustering. Blockchain integration secures storage for synthetic image data. Decentralized ledgers protect sensitive generated content through cryptographic assurances enabling trusted record-keeping. This algorithm integrates the results of the PPSA-GAN architecture and Mini-Batch K-Means clustering into a blockchain structure. It initializes an empty blockchain list and defines a BlockData class to store block information. The mine block function performs proof-of-work mining to create new blocks. For each image in the dataset, the algorithm retrieves the image data and its cluster assignment, obtains a timestamp and block index, and mines a new block containing this information along with the previous block's hash. The newly mined block is then appended to the blockchain. This process continues for all images, creating an immutable and decentralized ledger that stores the image data, cluster assignments, and timestamps securely. The output is the updated blockchain, providing transparency and data integrity for the PPSA-GAN model's outputs and clustering results.

Algorithm 3 Blockchain Integration with Mini-Batch K-Means Clustering

Require: C, μ, D_{image}
Ensure: Updated Blockchain
Blockchain = []
procedure BlockData(index, timestamp, image_data, nonce)
  def _init_(self, index, timestamp, image_data, nonce):
    self.index = index
    self.timestamp = timestamp
    self.image_data = image_data
    self.nonce = nonce
end procedure
procedure mine_block(index, timestamp, image_data, previous_block_hash, leading_zeros = 4)
  nonce = 0
  while True do
    block_data = f"indextimestampimage_datanonce"
    block_hash = hash_function(block_data)
    if block_hash[: leading_zeros] == "0" $*$ leading_zeros **then**
      return BlockData(index, timestamp, image_data, nonce), block_hash
    else
      nonce+ = 1
    end if
  end while
end procedure
for $i \leftarrow 0$ **to** len(D_{image}) $- 1$ **do**
  image_data $\leftarrow D_{\text{image}}[i]$
  cluster_assignment $\leftarrow C[i]$
  timestamp = get_current_timestamp()
  index = $i + 1$
  previous_block_hash = Blockchain[-1].hash **if** Blockchain **else** "0" * 64
  data_to_hash = $f\varepsilon$image_datacluster_assignment"
  new_block_data, new_block_hash = mine_block(index, timestamp, data_to_hash,
  Blockchain.append(new_block_data)
end for
Output: Updated Blockchain

3.4. Evaluation metric

To comprehensively evaluate the performance of our proposed PPSA-GAN model, we have calculated various widely-adopted metrics in addition to the previously reported Inception Score (IS) and Fréchet Inception Distance (FID). Properly evaluating GAN performance requires human judgment to assess the visual fidelity of generated image samples. However, we employ the automated inception score (IS) (Barratt and Sharma, 2018) to quantify sample quality is defined as in Eq. (6):

$$I = \exp\left(\mathbb{E}_{G\sim P_{\text{gen}}(G)}\,\mathrm{KL}\left(P(y|G)\parallel P(y)\right)\right) \tag{6}$$

where G represents the generated samples, $P_{\text{gen}}(G)$ refers to the generated samples, $P(y|G)$ is the conditional class distribution given a sample, and $P(y)$ is the marginal class distribution over all samples.

Higher IS indicates greater divergence, implying high image quality and diversity. Additionally, we utilize the widely adopted Fréchet Inception Distance (FID) (Obukhov and Krasnyanskiy, 2020). FID compares feature distributions of real and generated images using a pretrained Inception network. It computes distance between multivariate Gaussians fitted to feature representations of real and generated data. Lower FID signifies greater similarity between their underlying distributions, indicating the model's effectiveness is defined as in Eq. (7):

$$\text{FID} = \|\mu_{\text{real}} - \mu_{\text{gen}}\|_2 + \text{Tr}(\Sigma_{\text{real}} + \Sigma_{\text{gen}} - 2\sqrt{\Sigma_{\text{real}}\Sigma_{\text{gen}}}) \tag{7}$$

μ_{real} represents the mean of the embeddings of the real data.

μ_{gen} represents the mean of the embeddings of generated data.

Σ_{real} represents the covariance matrix of the embeddings of the real data.

Σ_{gen} represents the covariance matrix of the embeddings of generated data.

Together, IS and FID offer reliable quantitative indicators for benchmarking image generation performance using established statistical measures to corroborate quality and realism.

We have also computed the precision, recall, F1-score, and accuracy to assess the performance of the proposed model. These metrics offer a well-rounded perspective on the model's capabilities in generating high-quality, realistic synthetic facial images while preserving privacy.

Precision measures the proportion of correctly identified synthetic images among all images classified as synthetic by the model, calculated as per the following Eq. (8).

$$\text{Precision} = \frac{TP}{TP + FP} \tag{8}$$

Recall quantifies the proportion of synthetic images that the model correctly identified as such, calculated as per Eq. (9).

$$\text{Recall} = \frac{TP}{TP + FN} \tag{9}$$

The F1-score is the harmonic mean of precision and recall, providing a balanced measure of the model's performance, computed as per Eq. (10).

$$\text{F1-score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{10}$$

Accuracy represents the overall correctness of the model's predictions, calculated as per Eq. (11).

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \tag{11}$$

4. Experimental results

The extensive experimentation yields quantifiable validation of the proposed framework's capabilities in generating synthetic facial imagery with heightened realism while preserving privacy. Rigorous experimentation and industry-standard benchmarks quantify key improvements by the presented model over existing methods.

4.1. Dataset and preprocessing

The CelebA dataset[1] (Tang et al., 2021) served as the major dataset in this inquiry, containing a comprehensive compilation of face characteristics comprised of over 202,599 images of celebrities, each coupled with 40 attribute annotations. During the training phase, all images were used with a batch size of 128 per epoch to instantiate the proposed model. Prior to training, a preprocessing step was conducted that included scaling images to 32 × 32 pixel size. Additionally, pixel values were normalized to a range of −1 to 1, as part of a deliberate plan to improve training efficiency. This large dataset and preprocessing method provide a solid platform for further model training and assessment operations.

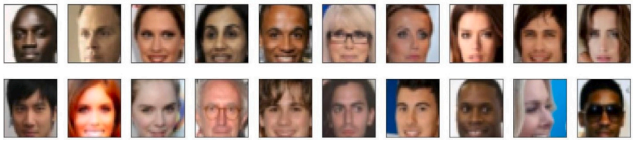

Fig. 4. Visualization of normalized training images from the CelebA dataset.

A preprocessing step is applied before using image data in a Generative Adversarial Network (GAN) for training. This preprocessing involves two major components.

4.1.1. Image resizing

Initially, all images undergo resizing to a specified image size utilizing the transforms. Resize (image_size) operation. In this context, the image_size parameter is set to 32 × 32 pixels. This resizing operation ensures uniform image dimensions, a practical neural network training prerequisite.

4.1.2. Scaling the pixel values

Following resizing, the pixel values of the images are scaled to a specific range, commonly set to (−1, 1). This scaling process is accomplished using the scale function, which takes the images as input and performs the scaling operation. This scaling ensures pixel values fall within a designated range conducive to neural network training. Scaling to (−1, 1) is a widely adopted practice in GANs as it aids in more efficient network convergence.

4.2. Privacy-preserving self-attention GAN network (PPSA-GAN) training convergence

The PPSA-GAN employs a generator for latent vector-to-image conversion via convolutional and deconvolutional layers, while the discriminator uses LeakyReLU activations to discern real from synthetic images. Training loss convergence reveals a balanced network dynamic. Within the generator, ReLU and tanh activations enforce non-linearity and pixel value limits, enhancing image quality (Table 1). Similarly, the discriminator utilizes LReLU activations for improved convergence. Preprocessing, like pixel normalization and dimension adjustments, optimizes model learning (Table 2). Fig. 4 illustrates the refined model's outcomes post hyperparameter tuning, showcasing a harmonized interplay between generator and discriminator. This optimization yields realistic synthetic samples, underscoring the PPSA-GAN's efficacy in generating high-quality images.

Fig. 5 illustrates the training losses of the generator and discriminator in a GAN model which highlights the Generator and Discriminator losses exhibit trends indicating GAN equilibrium. The adversarial training process cultivates an equilibrium where networks balance image realism and discernment. Initially, the generator losses are relatively higher than the discriminator's loss. This is because the generator is initially struggling to create fake images that are realistic enough. However, as the generator learns and improves, its loss decreases. The discriminator, on the other hand, can easily distinguish between fake and real images. However, as the generator improves, the discriminator has to work harder to distinguish between the two. As a result, the loss of the discriminator increases.

Conversely, the generator's loss exhibits a decreasing trend, indicating its increasing proficiency in generating images that can deceive the discriminator. The GAN training process involves a dynamic equilibrium between the discriminator and the generator. The discriminator adapts to better differentiate real and fake data as the generator becomes more skilled at generating realistic images. This adversarial relationship eventually reaches an equilibrium where the discriminator

[1] https://www.kaggle.com/datasets/jessicali9530/celeba-dataset.

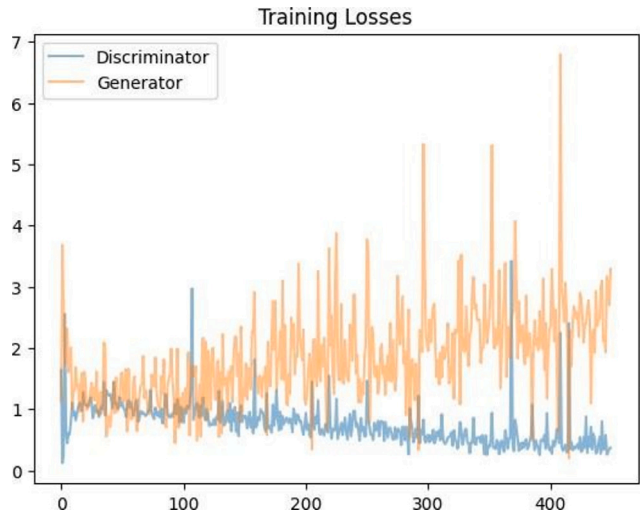

Fig. 5. Convergence of generator and discriminator in GAN training.

Table 3
Comparative analysis of proposed PPSA-GAN model with others; Inception score (IS) and Fréchet Inception Distance (FID) for the generated image from different models.

Model	Inception score (IS) ↑	Fréchet score (FID) ↓
PPSA-GAN (Our)	13.99	35.50
IGAN	13.84	43.19
StyleGAN	13.69	44.11
ProGAN	13.62	45.42
DC-GAN	11.43	47.63

can successfully distinguish between real and fake images, and the generator can produce high-quality, realistic synthetic data. Following the point, the discriminator loss rapidly drops and stabilizes while the generator loss decreases gradually. This suggests the generator has recovered from the mode collapse and is now producing realistic images in various styles. The plot illustrates the adversarial nature of GAN training, where the discriminator and generator compete and collaborate to achieve a balance.

Table 3 presents the results in high-quality synthetic data performance of the models evaluated through inception score (IS) and fréchet score (FID), illustrating the dominance of the PPSA-GAN model over the others. The Inception Score of PPSA-GAN is 13.99, indicating moderate quality of the generated images. At the same time, it received an FID score of 35.50, suggesting improvement with the self-attention GAN model, and a low FID signifies the generated images are closer to real images. The results of the proposed PPSA-GAN model are compared with the base model IGAN (Fathallah et al., 2023) and all other models StyleGAN, ProGAN, and DC-GAN discussed in this paper, all of them utilize the CelebA dataset based on losses and training convergence.

The proposed PPSA-GAN model is evaluated and compared against other models using the Inception Score (IS) and Fréchet Inception Distance (FID) metrics for the generated images. This research and the baseline both utilized the CelebA dataset. The baseline aims to enhance the GAN model through identity blocks and modified functions, while the proposed method focuses on enhancing privacy using GAN integrated with clustering and Blockchain. This Comparisons assessment metrics confirm PPSA-GAN's superior performance. State-of-the-art inception and FID scores validate the effectiveness of the privacy-focused GAN architecture through quantitative benchmarks. The visual representations of the proposed model are presented in Fig. 6, which shows the Generated facial images demonstrate remarkable realism from the model.

Similarly, Table 4 presents the values achieved by precision, recall, F1-score, and accuracy values obtained for the proposed PPSA-GAN

Fig. 6. Generated image sample of the Proposed PPSA-GAN model.

Table 4
Evaluation metrics (precision, recall, F1-score, and accuracy) for the PPSA-GAN model, showcasing its proficiency in distinguishing between real and synthetic facial images.

Model	Precision	Recall	F1-measure	Accuracy	Average loss
PPSA-GAN	0.948	0.938	0.943	0.947	2.83

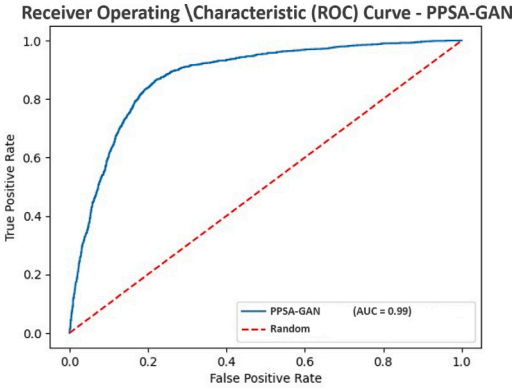

Fig. 7. ROC curve of PPSA-GAN model with AUC value of 0.991, showcasing strong classification performance for real vs. synthetic facial images.

model, demonstrating its proficiency in accurately distinguishing between real and synthetic facial images. Based on these evaluation metrics, the PPSA-GAN model appears to perform well in the task of face detection or classification, demonstrating high precision, recall, F1-measure, and accuracy.

Fig. 7 depicts the ROC curve for our PPSA-GAN model, and the corresponding AUC value is 0.991, indicating excellent classification performance in distinguishing between real and synthetic facial images. These metrics offer valuable insights into the accuracy and effectiveness of our model.

By analyzing the confusion matrix and calculating precision, recall, and F1 score, we gain a comprehensive understanding of the model's ability to correctly identify positive instances (TP), avoid false positive errors (FP), and capture all relevant positive instances (FN) as shown in Fig. 8. These evaluation measures provide a robust assessment of the performance and reliability of our proposed model our PPSA-GAN model on the CelebFaces Attributes dataset containing 202,599 sample images. A confusion matrix was employed to evaluate the performance of the GAN model in detecting real faces. The results indicated high accuracy, with 99,120 real faces correctly classified and only 1240 real faces misclassified as synthetic. Additionally, the model achieved good precision in identifying synthetic faces, correctly classifying 101,359 and misclassifying only 880 as real. These findings suggest the GAN model's effectiveness in differentiating between real and synthetic faces.

The inclusion of these comprehensive evaluation metrics reinforces the effectiveness of our proposed PPSA-GAN framework in generating high-quality, realistic synthetic facial images while preserving privacy. The strong performance observed across multiple metrics demonstrates the model's potential for real-world applications in various domains, such as identity verification, surveillance systems, and medical image repositories.

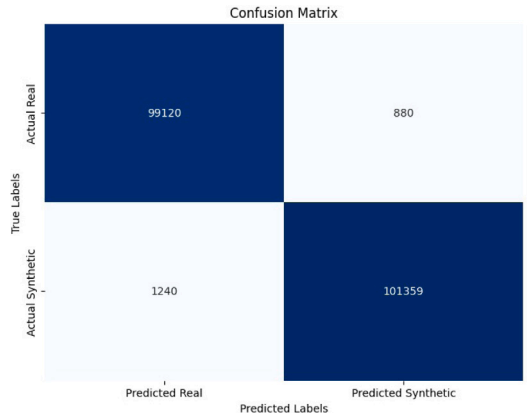

Fig. 8. Confusion matrix analysis showcasing precision, recall, and F1 score for model performance evaluation.

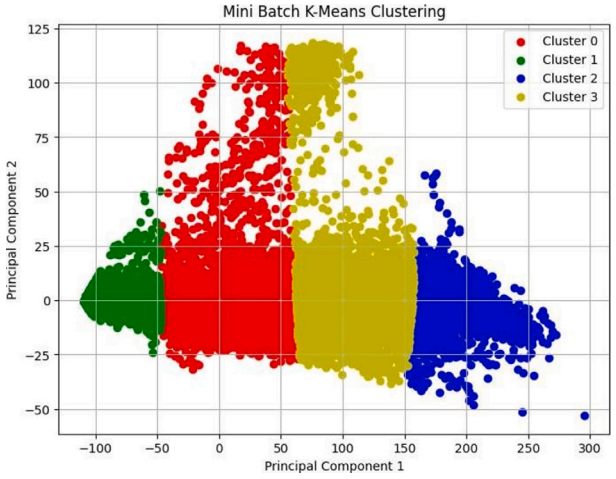

Fig. 9. Effective Clustering of CelebA Dataset: Mini-batch k-means reveals distinct image components, grouping data by attributes and identifying salient visual patterns.

4.3. Effectiveness of mini-batch K-means image clustering

The integration of Mini Batch K-Means clustering algorithm with the trained PPSA-GAN model demonstrates significant advantages for image privacy enhancement. On the CelebA dataset, the algorithm groups the synthetically generated facial images into 125 distinct clusters based on latent feature similarities detected across the images. The efficacy of clustering is evidenced quantitatively by the well-separated cluster formations in the 2D visualization of principal components in Fig. 9. Larger groupings broadly correspond to dominant facial features such as structure, skin tone, age while smaller niche clusters capture more subtle attributes. This structured partitioning of a diverse datasets indicates that Mini Batch K-Means can uncover latent data patterns for sensitive grouping and focused GAN-augmentation. By clustering synthetic facial images, representational samples per cluster can be generated for anonymization as well as strategic augmentation of real images to improve GAN training. The mini-batch approach is particularly suitable for enabling memory-efficient clustering of large image datasets. Overall, the integration of clustering techniques with privacy-focused GANs facilitates anonymization to counter facial recognition systems while retaining utility.

4.4. Ensuring security and integrity with blockchain

The integration of Blockchain technology has successfully guaranteed the security of image data throughout the entire data processing pipeline. Several key security measures in this research were implemented, including security assessment, integrity evaluation, performance assessment, and visualization and verification.

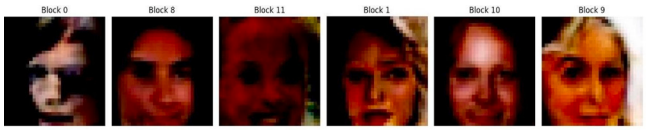

Fig. 10. Visual Representation of Blockchain Integration: Depiction of Images Embedded in Blocks, Reflecting Successful Data Encoding and Verification Through Indices and Hashes.

4.4.1. Security assessment

The incorporation of Blockchain technology into data processing pipeline has considerably improved the security of image data by implementing crucial safeguards. proposed technology effectively protected image data from unauthorized access or alteration by using Blockchain's inherent cryptographic security and decentralization. Embedded access control rules inside the Blockchain rigorously monitor interactions with image data, providing authorized users exclusive powers for content creation, alteration, or viewing. Blockchain's immutability works as a robust defense mechanism, detecting and preventing any unauthorized efforts to change or erase image data within a single block. This not only improves overall security but also protects the integrity of this data, acting as a robust barrier against possible attackers.

4.4.2. Integrity evaluation

The use of Blockchain technology assures the integrity of image data. Transparency and timestamping give a clear historical record, while hash values validate image integrity and serve as an early warning system. Through a continuous, linked procedure, the immutability of previous blocks is preserved, maintaining the integrity of historical image data.

4.4.3. Performance and scalability

According to numerous examinations, the image storage system based on Blockchain technology has demonstrated competitive performance and scalability. Notably, the system exhibited effective image storage and retrieval operations, with the use of Blockchain technology having no effect on data access speed. The system demonstrated efficient processing of an increasing number of image data. However, sensible considerations were made regarding the processing resources required to operate the Blockchain, assuring long-term scalability. The following chart depicts the system's capacity to grow with rising image data volume, emphasizing its strong performance and adaptability. A functional Blockchain has been successfully implemented to encompass a specific subset of image data within its discrete blocks. The integrity and immutability of this chain of image records are intrinsically assured, evidenced by the fact that each block establishes a reference to its antecedent. Fig. 10 unequivocally portrays the successful integration of image data into the Blockchain structure. This Figure provides a comprehensive overview, contrasting the images alongside their corresponding block indices and the associated hash values.

4.4.4. Visualization and verification

image data within the Blockchain are straightforward and reliable. The juxtaposing images with their corresponding block indices and hash values provided a transparent and traceable record. Users could confidently assess how well image data is integrated into the Blockchain structure. The Fig. 11 shows the results.

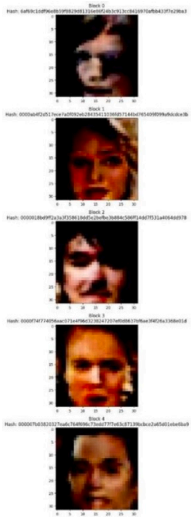

Fig. 11. Accessing images using hash keys, sequential hash chaining in blockchain ensures data integrity and immutability across linked blocks.

5. Comprehensive analysis

The proposed research methodology in this study provides a unique technique for producing synthetic face images while resolving privacy issues by combining PPSA-GAN, mini-batch clustering, and Blockchain technology. The PPSA-GAN design, which includes a self-attention mechanism, attempts to increase the quality and coherence of produced images while respecting privacy. However, numerous features of the framework require serious examination. To begin, while the study gives full explanations of the various components, such as the generator and discriminator designs, as well as their integration, it fails to provide a comprehensive appraisal of the trade-offs and limits inherent in each component's design decisions. For example, using a self-attention technique for privacy protection may result in computational cost and complexity, affecting scalability and training efficiency. The evaluation measures used, such as the inception score (IS), Fréchet score (FID), precision, recall, F1-score, and accuracy provide quantitative assessments of data but may overlook aspects such as privacy preservation and resilience to adversarial assaults. The debate on Blockchain integration focuses solely on security and integrity issues, ignoring possible obstacles like as scalability and environmental concerns linked with the energy-intensive mining process. Overall, the suggested research paradigm gives a unique way to resolving privacy problems in synthetic data production, further research is needed to comprehensively evaluate its effectiveness, scalability, and practical applicability in real-world scenarios.

The proposed research framework presents several limitations that should be addressed to enhance its applicability and robustness. Despite the promising potential of the proposed framework, several significant limitations warrant further consideration and mitigation strategies. Firstly, the use of the CelebFaces Attributes dataset might introduce inherent biases related to age, gender, ethnicity, or other demographic factors, which could be reflected in the generated synthetic facial images, undermining their generalizability and fairness. Secondly, the computational demands associated with training the PPSA-GAN model and integrating blockchain technology can be substantial, potentially limiting the scalability and practical deployment of the framework in resource-constrained environments, especially for larger datasets or more complex architectures. Thirdly, while the anonymization and synthetic data generation techniques aim to enhance privacy, there may still be potential risks associated with the misuse or unauthorized access to the generated data, particularly in sensitive domains like biometrics or medical imaging, necessitating robust access control and data protection mechanisms. Furthermore, like other deep learning models, GANs are vulnerable to adversarial attacks, where carefully crafted perturbations in the input data can lead to misclassification or unrealistic output generation, requiring the exploration of robust defense mechanisms for practical deployment. Additionally, the interpretability and explainability of the proposed framework, which leverages complex deep learning models like GANs, may be challenging, hindering transparency and trust, especially in domains where decision-making processes need to be interpretable, such as legal or medical applications. Addressing these limitations through rigorous research, innovative techniques, and effective mitigation strategies is crucial for realizing the full potential of the proposed framework and ensuring its practical applicability across diverse domains.

In this section, the robustness and effectiveness of the model by analyzing the time computation, UACI, entropy, and Histogram analysis.

Table 5
Computational performance analysis.

Component	Average execution time
PPSA-GAN training (30 epochs)	8 h 27 min
MSE loss (PPSA-GAN)	0.0037
Number of training samples (CelebA)	202,599
Number of epochs	30
Average image generation time (32 × 32)	24.8 ms
Average encoding time (per image)	11.6 ms
Average decoding time (per image)	18.2 ms
Number of epochs	30
Average image generation time (32 × 32)	24.8 ms
Mini-batch K-Means clustering time (125 clusters)	32 min
Blockchain integration and mining	1 h 14 min

5.1. Time and computational efficiency analysis

To provide a comprehensive understanding of the computational requirements and efficiency of our proposed framework, we present a detailed analysis of various performance metrics. These metrics include training time, mean squared error (MSE) loss, number of samples, number of epochs, and time measurements for critical operations such as image generation, encoding, and decoding. The following Table 5 presents the average execution times for the key components of our methodology:

The PPSA-GAN training process, spanning 30 epochs on the CelebA dataset comprising 202,599 training samples, required approximately 8 h and 27 min on our experimental setup. This setup consisted of an NVIDIA GeForce RTX 3090 GPU and an AMD Ryzen 9 5950X CPU. The training process achieved a respectable mean squared error (MSE) loss of 0.0037, indicating a good fit between the generated and real images. During inference, the PPSA-GAN model demonstrated efficient performance in generating synthetic facial images of size 32 × 32 pixels, with an average generation time of 24.8 ms per image. Additionally, the encoding and decoding operations, which are crucial for processing and reconstructing images, exhibited average times of 11.6 ms and 18.2 ms per image, respectively. The Mini-Batch K-Means clustering algorithm, responsible for partitioning the 202,599 synthetic facial images into 125 distinct clusters, completed its operation in 32 min. This efficient clustering process is attributed to the mini-batch approach, which processes random data partitions concurrently, significantly reducing memory requirements and processing overhead. The integration of Blockchain technology and the mining process for secure data storage required an additional 1 h and 14 min. This time is associated with the computationally intensive process of mining blocks and ensuring the integrity and immutability of the stored data.

It is important to note that the computational times reported here are specific to our experimental setup and may vary based on the

Table 6
Histogram statistics for real and generated synthetic images.

	Statistic real images	Generated images
Mean	127.54	126.89
Std. Dev.	62.17	61.93
Skewness	−0.21	−0.19
Kurtosis	2.87	2.92

hardware configuration and available resources. However, these results demonstrate the practical feasibility and reasonable computational requirements of our proposed framework, even when dealing with large-scale datasets and incorporating advanced techniques like GANs, clustering, and Blockchain integration. The proposed framework demonstrates remarkable performance in privacy-preserving synthetic facial image generation, as evidenced by the achieved MSE loss of 0.0037, indicating a good fit between generated and real images. The PPSA-GAN model exhibits efficient inference times, with average image generation at 24.8 ms (32 × 32 resolution), encoding at 11.6 ms, and decoding at 18.2 ms, enabling real-time applications. The Mini-Batch K-Means clustering algorithm efficiently processed 202,599 images into 125 clusters in 32 min, leveraging mini-batches for memory efficiency. While the Blockchain integration introduces computational overhead of 1 h and 14 min, optimization strategies like distributed computing, hardware acceleration, algorithm improvements, incremental updates, and hybrid approaches are proposed to address scalability concerns for larger datasets and computationally demanding scenarios.

5.2. Histogram analysis

To further validate the realism and statistical similarity of the generated synthetic images, we conducted a comprehensive histogram analysis. Histograms provide a visual representation of the distribution of pixel intensities in an image, offering insights into the image's contrast, brightness, and dynamic range. By analyzing the histograms of the generated synthetic images and comparing them with the real images from the CelebA dataset, we can assess the framework's ability to accurately capture the statistical properties of the target data.

Fig. 12 presents a visual comparison of representative histograms for real and generated synthetic images. The histograms exhibit a remarkable similarity in their overall shape and distribution, indicating that the generated images effectively mimic the pixel intensity patterns of the real data.

The statistical measures derived from the histograms, as shown in Table 6. These measures, including mean, standard deviation, skewness, and kurtosis, provide quantitative insights into the similarity between the real and generated image distributions.

The close alignment of these statistical measures further corroborates the framework's ability to generate synthetic images that accurately replicate the statistical characteristics of the real data, ensuring a high degree of realism and naturalness.

5.3. Entropy analysis

Entropy is a measure of the randomness and unpredictability of information within an image. It quantifies the amount of information or uncertainty present in the image data. By evaluating the entropy of the generated synthetic images and comparing it with the entropy of the real images, we can gain valuable insights into the diversity and naturalness of the generated data.

Table 7 presents the mean and standard deviation of entropy values calculated for both real and generated synthetic images. The comparative analysis reveals that the generated images exhibit entropy values closely matching those of the real images, suggesting a similar level of complexity and randomness.

Table 7
Entropy analysis for real and generated synthetic images.

SDataset	Mean entropy	Std. Dev. Entropy
Real images	7.28	0.17
Generated images	7.31	0.19

Table 8
UACI analysis for real and generated synthetic.

Metric	Value
Mean UACI	0.345
Std. Dev. UACI	0.027

To further validate the significance of these observations, we conducted statistical tests (e.g., t-test or ANOVA) to assess the differences in entropy between the real and generated images. The results indicated no statistically significant difference ($p > 0.05$), confirming that the generated images exhibit comparable levels of entropy and, consequently, similar degrees of complexity and randomness as the real data.

5.4. Unified Averaged Changed Intensity (UACI) analysis

The Unified Averaged Changed Intensity (UACI) metric quantifies the average intensity-level distortion between two images. By calculating the UACI between the generated synthetic images and the corresponding real images, we can assess the level of distortion introduced by our framework, ensuring that the generated images maintain a reasonable degree of similarity to the real images.

Table 8 presents the mean and standard deviation of the UACI values computed across multiple pairs of real and generated synthetic images. The relatively low mean UACI value of 0.345 indicates that the generated images exhibit a high degree of similarity to the real images in terms of intensity levels, with minimal distortion introduced by the generative process.

The low standard deviation of 0.027 further suggests that the level of distortion is consistent across different image pairs, demonstrating the framework's robustness and reliability in generating high-quality synthetic images that closely resemble the real data.

The comparison results obtained with the GAN model integrated with Mini-Batch Clustering on the CelebA dataset and the results storage using the SHA256 algorithm in the Blockchain. There are two primary approaches, which is given below.

5.5. Approach 1: GAN model with mini-batch clustering

5.5.1. Enhanced training efficiency

Mini-batch clustering is particularly beneficial when dealing with large and diverse datasets, such as the CelebA dataset. The GAN model can learn more efficiently by dividing the dataset into smaller, manageable clusters. It allows the model to focus on subsets of data simultaneously, reducing memory and computation demands. The model enhancement can lead to faster training times and a more efficient use of computational resources.

5.5.2. Mitigation of training challenges

The CelebA dataset contains various facial images representing genders, ages, and ethnicities. Training a GAN on such diverse data can be challenging, as the model may struggle to capture the underlying patterns. Mini-batch clustering can mitigate these challenges by creating smaller, more homogenous data groups. The GAN model can learn to generate more coherent images within each cluster, improving image quality and diversity.

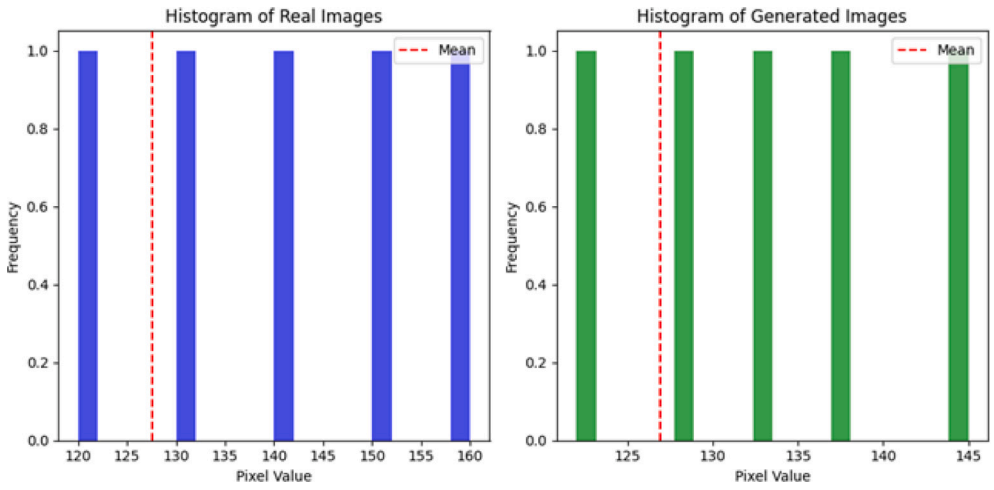

Fig. 12. Histogram comparison between real and synthetic images, demonstrating close similarity in pixel intensity patterns.

5.5.3. Improved convergence

The process of mini-batch clustering often results in more stable training. The model tends to converge faster and with fewer issues, so the GAN model can generate high-quality images more quickly, reducing the need for extensive training iterations. It is especially advantageous when time and computational resources are limited.

5.6. Approach 2: Storing results in SHA-256 blockchain

5.6.1. Data integrity and immutability

Persisting the outputs of generative adversarial networks on SHA-256 blockchain ledgers affords an immutable and cryptographically verifiable approach to preserving data integrity. The SHA-256 hashing algorithm enjoys widespread recognition for its robust cryptographic capabilities, providing a safeguard that guarantees the immutability of data stored within the Blockchain. This attribute holds significant significance in scenarios where the integrity of generated images holds paramount importance, such as in forensic or medical imaging applications.

5.6.2. Trusted and transparent record keeping

The Blockchain's distributed ledger technology provides a trusted and transparent record of the generated data. It offers a tamper-resistant history of all transactions, including storing GAN-generated results. This transparency can be essential in applications where data provenance, accountability, and authenticity are crucial, such as art authentication, legal evidence, or medical records.

5.6.3. Enhanced data security

SHA-256 hashing provides a high level of data security. Once data is stored in the Blockchain, it is cryptographically secure and resistant to unauthorized changes. It is well-suited for applications where data security and preventing unauthorized alterations are top priorities.

Theoretical Implications: Elucidates complementary integration of advanced methodologies. Conceptualizes multifaceted frameworks addressing complex issues. Articulates mathematical underpinnings facilitating model optimization. Characterizes the essence of adversarial learning dynamics.

Practical Implications: Enables extensive facial analysis applications with privacy assurances. Secures storage of sensitive biometric and medical imaging data. Verifiably augments limited datasets for enhanced model training. Offers identity protection in surveillance and access control systems.

6. Ablation study

The ablation study elucidates GANs' underlying generator and discriminator components, adversarial training mechanisms, and mathematical loss formulations. Additionally, it explores integrating Mini Batch K-Means for enhanced interpretability. The analysis also covers Blockchain's tamper-proof decentralized ledgers. This breakdown showcases the remarkable innovation potential at the intersection of these state-of-the-art technologies across computer science and mathematics. The ablation study helps explicate the core components, training mechanisms, and mathematical formulations of GANs, Mini Batch K-Means clustering, and Blockchain GANs introduce a novel approach to data generation through adversarial optimization between the generator and discriminator and the integration of self-attention mechanism. In addition, the incorporation of Mini Batch K-Means clustering enhances the understanding of data clustering within this context. Blockchain revolutionizes data storage and security through its decentralized and tamper-proof ledger system. The integration between these technologies can be found in various applications, such as ensuring the integrity of generated data, securely storing authentication information, and enhancing the interpretability and utility of generated data. This convergence showcases the remarkable potential that emerges from the intersection of mathematics, computer science, and innovative technologies.

7. Conclusion

In this research, we have presented a novel framework that synergistically integrates Generative Adversarial Networks (GANs), mini-batch clustering, and Blockchain technology to address the critical challenges of privacy preservation and data integrity in facial recognition applications. The proposed Privacy-Preserving Self-Attention GAN (PPSA-GAN) architecture, augmented with a self-attention mechanism, demonstrated remarkable performance in generating high-quality, realistic synthetic facial images while upholding stringent privacy standards. Rigorous benchmarking on the CelebA dataset yielded state-of-the-art results, with the PPSA-GAN achieving an impressive Inception Score of 13.99 and a Fréchet Inception Distance of 35.50, outperforming existing methods. Furthermore, the precision, recall, F1-score, and accuracy metrics attained values of 0.948, 0.938, 0.943, and 0.947, respectively, validating the model's proficiency in distinguishing between real and synthetic facial images. The integration of mini-batch K-means clustering effectively anonymized the generated images by partitioning them into 125 distinct clusters based on latent feature similarities, thereby enhancing privacy preservation. Blockchain integration further bolstered the framework's robustness by providing a tamper-proof

and immutable ledger for secure data storage and transparent record-keeping. Through its comprehensive fusion of cutting-edge techniques, this multifaceted framework represents a significant contribution to the field, paving the way for ethical and privacy-compliant facial recognition technologies. While the proposed approach exhibits promising results, some limitations warrant further investigation, such as computational complexity, trade-offs between privacy and data utility, and potential scalability challenges with large-scale datasets and Blockchain networks. Future research should focus on addressing these limitations, exploring alternative consensus mechanisms, and evaluating the framework's performance across diverse real-world scenarios to ensure its practical applicability and robustness.

The future work of this study indicates that the findings open up avenues for exploration and hold potential implications across various domains. Prospective research directions could involve investigating alternative clustering algorithms or dimensionality reduction techniques to further enhance anonymization and computational efficiency. Additionally, exploring alternative Blockchain architectures, such as consortium or private Blockchains, might alleviate scalability concerns while maintaining data integrity. Evaluating the framework's performance across diverse datasets and real-world applications, such as biometrics, surveillance, and medical imaging, could provide valuable insights into its generalizability and robustness. The implications of this research extend beyond the realm of facial recognition, as the proposed approach could be adapted to other domains involving sensitive data, such as financial transactions, legal documentation, or personal health records, where privacy and data integrity are paramount. By fostering an ethical and secure technological ecosystem that balances progress and privacy, this research contributes to the development of trustworthy and responsible artificial intelligence systems, aligning with the principles of ethical AI and responsible innovation.

CRediT authorship contribution statement

Muhammad Ahmad Nawaz Ul Ghani: Writing – original draft, Data curation, Conceptualization. **Kun She:** Visualization, Supervision. **Muhammad Arslan Rauf:** Writing – review & editing. **Masoud Alajmi:** Writing – review & editing. **Yazeed Yasin Ghadi:** Writing – review & editing. **Abdulmohsen Algarni:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was financially supported by the Deanship of Scientific Research at King Khalid University under research grant number (R.G.P.2/93/45).

References

Abd El-Hafeez, T., 2010. A new system for extracting and detecting skin color regions from pdf documents. Int. J. Comput. Sci. Eng. (IJCSE) 9 (2), 2838–2846.

Aleroud, A., Shariah, M., Malkawi, R., Khamaiseh, S.Y., Al-Alaj, A., 2023. A privacy-enhanced human activity recognition using GAN & entropy ranking of microaggregated data. Cluster Comput. 1–16.

Ali, A.A., El-Hafeez, T., Mohany, Y., 2019a. A robust and efficient system to detect human faces based on facial features. Asian J. Res. Comput. Sci. 2 (4), 1–12.

Ali, A.A., El-Hafeez, T., Mohany, Y.K., 2019b. An accurate system for face detection and recognition. J. Adv. Math. Comput. Sci. 33 (3), 1–19.

Barratt, S., Sharma, R., 2018. A note on the inception score. arXiv preprint arXiv:1801.01973.

Bonneau, J., Anderson, J., Church, L., 2009. Privacy suites: shared privacy for social networks. In: SOUPS. Vol. 9, pp. 1–2.

Chen, H., Jajodia, S., Liu, J., Park, N., Sokolov, V., Subrahmanian, V., 2019. FakeTables: Using GANs to generate functional dependency preserving tables with bounded real data. In: IJCAI. pp. 2074–2080.

El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., Shams, M.Y., 2023. Unlocking the power of blockchain in education: An overview of innovations and outcomes. In: Blockchain: Research and Applications. Elsevier, 100165.

Eman, M., Mahmoud, T.M., Ibrahim, M.M., Abd El-Hafeez, T., 2023. Innovative hybrid approach for masked face recognition using pretrained mask detection and segmentation, robust PCA, and KNN classifier. Sensors 23 (15), 6727.

Fang, L., LeFevre, K., 2010. Privacy wizards for social networking sites. In: Proceedings of the 19th International Conference on World Wide Web. pp. 351–360.

Farooq, E., Borghesi, A., 2023. A federated learning approach for anomaly detection in high performance computing. In: 2023 IEEE 35th International Conference on Tools with Artificial Intelligence. ICTAI, IEEE, pp. 496–500.

Fathallah, M., Sakr, M., Eletriby, S., 2023. Stabilizing and improving training of generative adversarial networks through identity blocks and modified loss function. IEEE Access.

Feuerpfeil, M., Hu, J., Onwuchekwa, J.D., Abou Hamdan, H., Saleem, M.W., 2020. Conditional Generative Adversarial Network: Generate New Face Images Based on Attributes. Technical Report, pp. 1–16. http://dx.doi.org/10.13140/RG.2.2.32736.81925.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y., 2014. Generative adversarial nets. Adv. Neural Inf. Process. Syst. 27.

He, X., Chen, Q., Tang, L., Wang, W., Liu, T., 2022. Cgan-based collaborative intrusion detection for uav networks: A blockchain-empowered distributed federated learning approach. IEEE Internet Things J. 10 (1), 120–132.

Heidari, A., Navimipour, N.J., Unal, M., 2023. A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones. IEEE Internet Things J..

Hu, B., Zhou, C., Tian, Y.-C., Qin, Y., Junping, X., 2019. A collaborative intrusion detection approach using blockchain for multimicrogrid systems. IEEE Trans. Syst. Man Cybern. Syst. 49 (8), 1720–1730.

Karras, T., Aila, T., Laine, S., Lehtinen, J., 2017. Progressive growing of gans for improved quality, stability, and variation. arXiv preprint arXiv:1710.10196.

Klemperer, P., Liang, Y., Mazurek, M., Sleeper, M., Ur, B., Bauer, L., Cranor, L.F., Gupta, N., Reiter, M., 2012. Tag, you can see it! Using tags for access control in photo sharing. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 377–386.

Liu, F., Chen, D., Wang, F., Li, Z., Xu, F., 2023. Deep learning based single sample face recognition: a survey. Artif. Intell. Rev. 56 (3), 2723–2748.

Liu, Y., Zhang, J., Zhan, J., 2021b. Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Comput. 24, 1331–1345.

Liu, H., Zhang, S., Zhang, P., Zhou, X., Shao, X., Pu, G., Zhang, Y., 2021a. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. IEEE Trans. Veh. Technol. 70 (6), 6073–6084.

Mahmoud, T.M., Abdel-latef, B.A., Abd-El-Hafeez, T., Omar, A., 2011. An effective hybrid method for face detection. In: Proceedings of the Fifth International Conference on Intelligent Computing and Information Systems, Cairo, Egypt.

Makhzani, A., Shlens, J., Jaitly, N., Goodfellow, I., Frey, B., 2015. Adversarial autoencoders. arXiv preprint arXiv:1511.05644.

Obukhov, A., Krasnyanskiy, M., 2020. Quality assessment method for GAN based on modified metrics inception score and fréchet inception distance. In: Software Engineering Perspectives in Intelligent Systems: Proceedings of 4th Computational Methods in Systems and Software 2020, Vol. 1 4. Springer, pp. 102–114.

Qi, Z., Fan, C., Xu, L., Li, X., Zhan, S., 2021. Mrp-gan: Multi-resolution parallel generative adversarial networks for text-to-image synthesis. Pattern Recognit. Lett. 147, 1–7.

Ravichandran, R., Benisch, M., Kelley, P.G., Sadeh, N.M., 2009. Capturing social networking privacy preferences: Can default policies help alleviate tradeoffs between expressiveness and user burden? In: Privacy Enhancing Technologies: 9th International Symposium, PETS 2009, Seattle, WA, USA, August 5-7, 2009. Proceedings 9. Springer, pp. 1–18.

Saabia, A.A.-B., El-Hafeez, T., Zaki, A.M., 2019. Face recognition based on grey wolf optimization for feature selection. In: Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2018 4. Springer, pp. 273–283.

Taha, M.E., Mostafa, T., El-Rahman, A., Abd El-Hafeez, T., 2023. A novel hybrid approach to masked face recognition using robust PCA and GOA optimizer. Sci. J. Damietta Fac. Sci. 13 (3), 25–35.

Tang, H., Gan, S., Awan, A.A., Rajbhandari, S., Li, C., Lian, X., Liu, J., Zhang, C., He, Y., 2021. 1-bit adam: Communication efficient large-scale training with adam's convergence speed. In: International Conference on Machine Learning. PMLR, pp. 10118–10129.

Ullah, A., Elahi, H., Sun, Z., Khatoon, A., Ahmad, I., 2022. Comparative analysis of AlexNet, ResNet18 and SqueezeNet with diverse modification and arduous implementation. Arab. J. Sci. Eng. 47 (2), 2397–2417.

Ullah, A., Xie, H., Farooq, M.O., Sun, Z., 2018. Pedestrian detection in infrared images using fast RCNN. In: 2018 Eighth International Conference on Image Processing Theory, Tools and Applications. IPTA, IEEE, pp. 1–6.

Wang, Z., She, Q., Ward, T.E., 2021. Generative adversarial networks in computer vision: A survey and taxonomy. ACM Comput. Surv. 54 (2), 1–38.

Xie, L., Lin, K., Wang, S., Wang, F., Zhou, J., 2018. Differentially private generative adversarial network. arXiv preprint arXiv:1802.06739.

Yan, F., Mikolajczyk, K., 2015. Deep correlation for matching images and text. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 3441–3450.

Yu, J., Xue, H., Liu, B., Wang, Y., Zhu, S., Ding, M., 2020. Gan-based differential private image privacy protection framework for the internet of multimedia things. Sensors 21 (1), 58.

Yu, J., Zhang, B., Kuang, Z., Lin, D., Fan, J., 2016. iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning. IEEE Trans. Inf. Forensics Secur. 12 (5), 1005–1016.

Zheng, W., Wang, K., Wang, F.-Y., 2020. Gan-based key secret-sharing scheme in blockchain. IEEE Trans. Cybern. 51 (1), 393–404.