Safeguarding Identities with GAN-based Face Anonymization

Mahmoud Ahmad Al-Khasawneh
School of Computing, Skyline University College, University City Sharjah, 1797, Sharjah, UAE | Jadara University Research Center, Jadara University, Jordan
mahmoud@outlook.my

Marwan Mahmoud
The Applied College, King Abdulaziz University, Saudi Arabia
mmamahmoud@kau.edu.sa

Received: 17 April 2024 | Revised: 6 May 2024 | Accepted: 8 May 2024

 DOI: https://doi.org/10.48084/etasr.7527

ABSTRACT

Effective anonymous facial registration techniques are critical to address privacy concerns arising from facial recognition technology. This study presents an intelligent anonymity platform that incorporates blockchain with advanced privacy and uses a CIAGAN-powered approach. This solution addresses the immediate need for privacy in facial recognition technology. The proposed system uses advanced techniques to anonymously generate highly realistic and effective facial images. The widespread use of facial recognition systems places greater emphasis on privacy concerns, emphasizing the need for strong enrollment mechanisms. The proposed system uses CIAGAN to address this challenge and generate facial images while preserving important attributes. Blockchain storage ensures that data integrity and security are maintained. The process begins with detailed image preprocessing steps to improve data quality and eliminate unwanted noise. CIAGAN can generate anonymous face images with important facial attributes to complicate the recognition of specific objects. A dataset of 202,599 facial images was used. Performance metrics such as PSNR and SSIM indicate image quality and uniformity. The PSNR obtained was 35.0516, indicating a unique image anonymization process.

Keywords-blockchain; facial recognition; CIAGAN

I. INTRODUCTION

Today, with the rapid development and deployment of technology, facial anonymization has become a matter of urgency [1-4]. This problem has been intensified by the numerous digital devices that create and transmit visual content almost uncontrollably, many times without a person's awareness or consent. The essence of sufficient protection is embodied in privacy and security concerns, such as cyberbullying and fraud [5-8]. GDPR is the result of private data security being a major concern. Data quality can be compromised by strict laws that complicate explicit consent to data use [9-11]. Privacy issues on human image data have become a serious problem. GANs can generate images that look very almost real and ensure that private details are well protected. Facial masking is the procedure to anonymize faces in images. Such systems can transform facial data in images or videos to distort identities. However, the distorted data must not contain unrelated image data [12]. Facial anonymization techniques should establish security and higher privacy in the digital media world. The primary task is to use deep learning to avoid revealing unique facial appearance features that can lead to identification [13]. These approaches aim to make any attempt at facial recognition ineffective [14]. Above all, anonymized photos must meet their purpose and, at the same time, meet the highest standards of privacy and quality [15].

It is necessary to create a standard to evaluate the adequacy, quality, and privacy protection of anonymized photos. Masking human identity is very important in many domains, including surveillance, social networks, medical imagery, research, and education [16, 17]. The remarkable advances have improved the performance and efficiency of such processes [18]. Generative adversarial networks (GANs) have paved the way for solving privacy problems. GAN technology is highly valued for its widely used generating capabilities and is used for the development of many complex products. With the advantages provided by GAN optimization strategies and their ability to resolve numerous privacy and security issues, GANs have gained the attention of the academic and industrial communities [19, 20]. In essence, a GAN has two neural networks that cooperate but operate in a duality manner: the generator and the discriminator. The generator aims to produce fake data or inputs that mimic the genuine with the ultimate goal of defeating the discriminator [19]. The discriminator is a deep learning-based algorithm designed to distinguish between genuine and fake data after learning. In general, the generator attempts to fool the discriminator. This allows the generation of

synthetic data that resemble real-world scenarios [20, 21]. GAN [22] is an important aspect of image generation, involving a generator network to produce synthetic images that are indistinguishable from real-life photos by deceiving the discriminator. This study examines the weaknesses of previous face anonymization techniques and proposes a face anonymization method that increases the privacy and data utility of images. In [23], the foundation for contemporary approaches to privacy protection was established. This study aimed to safeguard against re-identification by guaranteeing that individuals within a dataset remain indistinguishable. Facial photographs were anonymized by taking an average of k photos from a certain collection, ensuring privacy protection. However, the k-same technique has some disadvantages, especially when addressing ghosting artifacts resulting from image misalignment. These artifacts weaken image privacy by modifying the original quality [24]. The study in [25] focused on eliminating privacy concerns about the participation of people in remote video conferences. This study focused on the efficient use of blur filters for video calls.

Deep learning is an advanced subfield of machine learning that works similarly to the human brain[26]. In [27], a new method was proposed for face de-identification, subtly mixing some facial features by interchanging faces and applying K-anonymity without altering the sketch of the images. In [28], an approach focusing on de-identifying the entire body was proposed, surpassing the simple obscuring of facial regions. This method combined the Viola-Jones face detector, a deep convolutional GAN, and the graph cut segmentation algorithm. In [29], a synthesis-based approach was proposed, aiming to enhance privacy by enabling the transfer of facial attributes. This method used an encoder-decoder network structure and allowed better preservation of distinct facial features and simultaneous concealing of identities by transferring them from image to image. In [30], a variational GAN was used to obtain image representations that kept the expression as the facial feature with identity privacy. The Conditional Identity Anonymization Generative Adversarial Network (CIAGAN) model [31] is an advanced solution specifically designed to anonymize images and videos. This model provides a new swapping-face strategy, taking advantage of the encoder-decoder architecture and employing adversarial training. This model applies sophisticated landmark extraction procedures to precisely identify and conceal given facial features in photos. Such territories are substituted with other, artificially made, to maintain the confidentiality of services and information. This model stands out from traditional approaches by ensuring both anonymization and diversity. In [32], blockchain was used with image anonymization. Blockchain is an electronically distributed database shared by all nodes within a specific network, where blocks are linked together, resembling a linked list. It serves as a digital database ensuring secure storage of data and swift access for authorized users. Blockchain consists of two main components: transaction records of actions among network nodes and the recording of all transactions, traceable back to the first block. The important security aspects of blockchain pertinent to facial image security are immutability, instant availability, integrity, transparency, audibility, and anonymity [33]. Table I shows a comparative analysis of state-of-the-art approaches.

TABLE I. STATE-OF-THE-ART APPROACHES FOR FACE ANONYMIZATION

Algorithm	Anonymization technique	Data Type		Privacy guaranty	Test dataset
		Video	Image		
Traditional Method	[23]	No	Yes	Yes	[34]
	[25]	Yes	No	No	N/A
	[35]	Yes	Yes	No	N/A
	[36]	Yes	No	No	IHD
	[37]	Yes	No	No	IHD
	[38]	Yes	Yes	No	[39]
	[40]	Yes	Yes	No	[41]
Machine Learning	[22]	N/A		X	MNIST, TFD, [42]
Deep Learning	[27]	No	Yes	Yes	[43]
	[28]	Yes	Yes	No	[44]
	[29]	Yes	Yes	No	[45], [55]
	[46]	Yes	Yes	No	[45], [46]
	[31]	Yes	Yes	No	DALY, [47], [49]
	[48]	Yes	Yes	No	MOTS, [49], [50],
		Yes	Yes	Yes	[51] and others
Proposed		Yes	Yes	Yes	[50]

This study:

- Introduces a cutting-edge framework that uses blockchain and the CIAGAN model for intelligent face anonymization, effectively addressing the growing concerns around privacy.
- The proposed model generates incredibly lifelike and anonymous facial images while also incorporating blockchain to improve data security. This technique ensures improved data quality and eliminates noise, thus improving the effectiveness of face anonymization.
- Implements a thorough evaluation protocol using PSNR and SSIM to evaluate the quality of anonymized images.

II. INTELLIGENT BLOCKCHAIN-ENABLED GAN-BASED FACE ANONYMIZATION MODEL

The proposed method uses GANs for image anonymization, encompassing pre-processing input images to isolate sensitive facial regions and recognizable background objects, generating anonymized images through GAN training, and securely storing anonymized images in blockchain for increased security and access control. Image resizing, fine-tuning, and loss functions were used to improve the method's performance and the level of realism in the images produced. The main focus was to optimize the anonymized image to achieve three key objectives: maintain privacy and image quality, and secure the data.

A. Problem Statement

Facial image anonymization aims to develop a robust model to effectively balance privacy preservation, image utility, and security. Let I_{orig} represent the original facial image and I_{anon} denote the generated anonymized one. Primary

objectives can be measured using the Structural Similarity Index (SSIM) and the Peak Signal-to-Noise Ratio (PSNR).

1) Privacy Preservation Objective

This objective aims to minimize the loss of structural information in the anonymized image compared to the original image. This objective is quantified by maximizing the SSIM between I_{orig} and I_{anon}. SSIM is a perceptual metric that considers changes in structural information, luminance, and contrast. A higher SSIM indicates greater similarity to the original image, thus preserving privacy by retaining important visual features without revealing sensitive information.

$$PrivacyPreservationObjective = max\ SSIM(I_{orig}, I_{anon}) \quad (1)$$

2) Image Utility Objective

This objective ensures that the anonymized image maintains high visual quality, making it useful for various computer vision tasks such as detection and recognition. This objective is measured by the PSNR between I_{orig} and I_{anon}. PSNR quantifies the relationship between the maximum possible power of a signal and the power of noise that affects its representation. A higher PSNR indicates better image quality, suggesting that the anonymized image retains sufficient detail and clarity for practical applications.

$$ImageUtilityObjective = \max(PSNR(I_{orig}, I_{anon})) \quad (2)$$

3) Security Objective

The security objective focuses on reducing the risk of privacy breaches by minimizing the vulnerability of the anonymized image to re-identification attacks. This objective is measured by a custom vulnerability metric that assesses the susceptibility of the anonymized image to adversarial attacks and re-identification techniques. Factors that influence this metric include the robustness of the anonymization method, the strength of encryption techniques, and the ability of the model to withstand adversarial attacks. Blockchain ensures the integrity and authenticity of the anonymized images. Blockchain's decentralized nature provides an immutable ledger for storing image data, ensuring that any unauthorized attempts to tamper with the anonymized images are easily detectable. This integration significantly reduces the risk of re-identification and improves the overall security of the anonymization process.

$$Security\ Objective = \min(Risk(I_{anon}) \quad (3)$$

B. Proposed Intelligent Face Anonymization Model

Figure 1 shows the proposed image privacy model, which is seamlessly integrated with the blockchain. The model incorporates a generator and discriminator framework and the blockchain architecture. The model has six essential stages: data collection, image preprocessing, integration with blockchain, processing using GANs, output generation, and blockchain validation. Each step ensures the coordination of a crucial element of the data flow and seamless transition while upholding robust protection. The procedure commences with the identification of facial landmarks, followed by the generation of background images for masks. Subsequently, cropping and scaling techniques are employed in the input photographs. Afterward, the modified photographs are stored in arrays, which are subsequently uploaded to a blockchain. A CIAGAN is used to achieve anonymization. The procedure initializes the generator and discriminator neural networks within the CIAGAN, followed by training over multiple epochs. During the training, the discriminator evaluates both genuine and counterfeit photographs, while the generator develops the ability to produce genuine counterfeit images to mislead the discriminator. The trained GAN is used to produce the final anonymized images.

C. Data Acquisition

The CelebA dataset [50] is a well-known source for facial attribution assignments, containing 202,599 celebrity photos covering a range of characteristics. Each image has a resolution of 178×218 pixels. 162,000 images were used for training, 20,000 for validation, and 20,599 for testing. The collection contains extensive information about many elements of the celebrities' appearances, covering forty unique attributes. For the training process, the images were standardized to 128×128 pixels to balance computational efficiency and model performance, cropping them to a square aspect ratio, and then downscaling them to the desired dimensions. This step facilitated the consistent image processing by the CIAGAN model, ensuring that it could effectively learn the relevant features while maintaining computational efficiency.

D. Image Preprocessing

The images were landmarked to annotate significant facial features that can include private information. The image background was masked to eliminate it and highlight the primary subject. The images were cropped to successfully hide prominent facial features while maintaining image utility. The intended result was achieved by employing cropping, region of interest selection, face detection, and facial landmark detection. In the end, image resizing was used to change the dimensions of the images while preserving their use and anonymity.

E. Blockchain-enabled Face Anonymization

The blockchain network was used to address privacy, security, and accountability issues. Blockchain's use of cryptographic hashing methods improves security and ensures the integrity of anonymized facial data. Furthermore, as blockchain transactions are visible, users may thoroughly examine and verify data transactions. Blockchain enhances auditing and accountability by facilitating the tracking of data sources and monitoring data usage through its audit trail features. This promotes transparency and accountability in all aspects of data management. Furthermore, the application of blockchain removes the need for middlemen by enabling direct peer-to-peer sharing of data among authorized institutions.

F. Proposed GIAGAN-based Face Anonymization Model

This study uses the CIAGAN model to translate input photos, landmarks, representations of masked faces, and stated IDs. The generator uses the one-hot encoded identification data processed after the encoder effectively translates complex visual properties into a lower-dimensional environment. The decoder produces output images by amalgamating the input data. The discriminator diligently analyses these synthesized

images, skillfully differentiating between genuine and artificial ones. Noise vectors are employed to produce counterfeit images that exhibit a high degree of realism. The discriminator examines the collection of photos, highlighting and identifying any instances of false attempts. The detected photos are sent back to the generator for further improvement, creating an iterative process that aims to produce difficult-to-identify counterfeit images. Finally, the generator produces real images that are accepted as genuine. These images are then stored on the blockchain to ensure security and preservation. Until the generator produces output with the appropriate degree of authenticity and quality, the aforementioned iterative process continues. Figure 2 shows the detailed process.

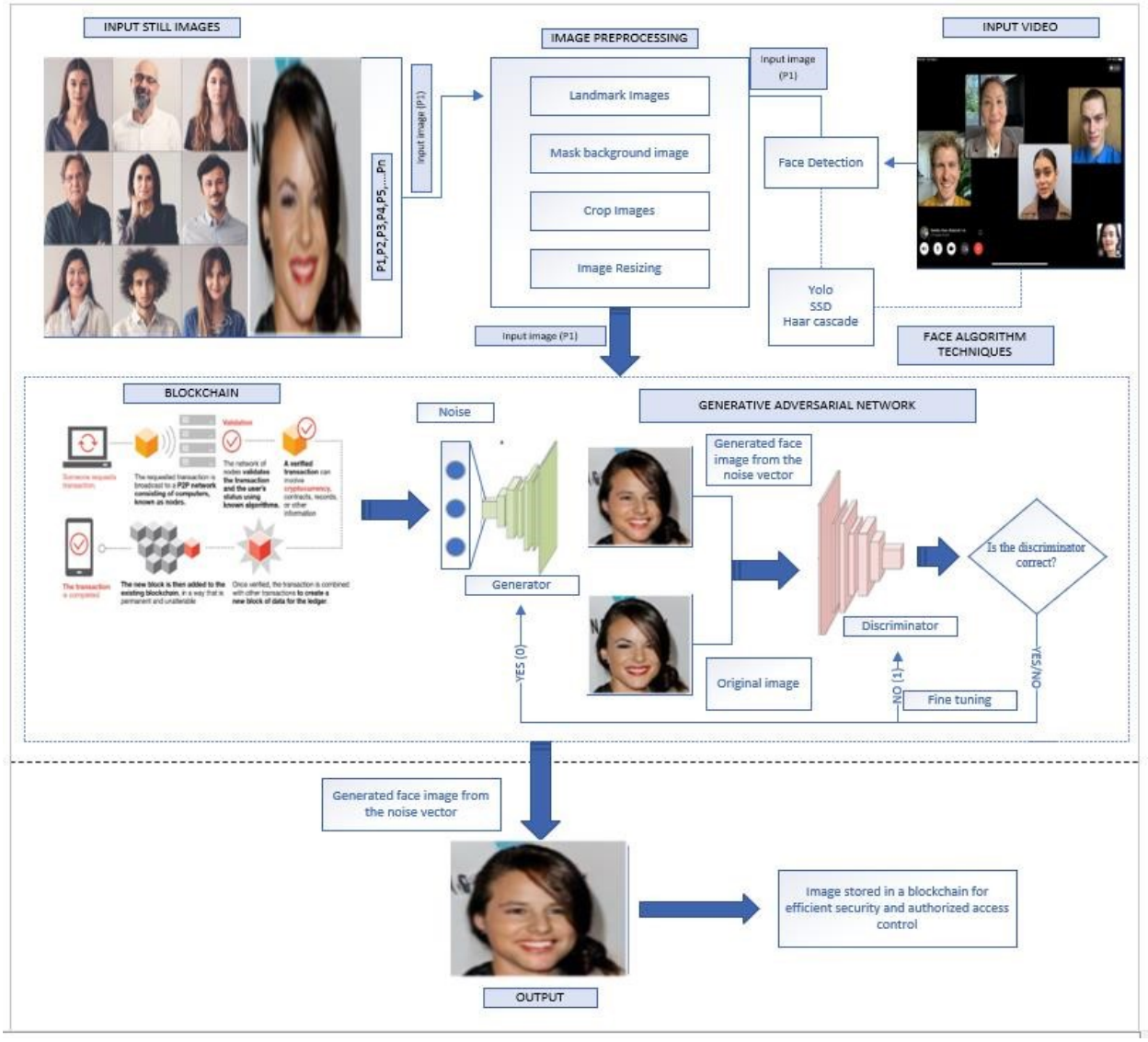

Fig. 1. Diagram of the proposed intelligent model.

G. Security As A Service (SECaaS) for Intelligent Face Anonymization

SECaaS is a method to provide a wide range of services through cloud infrastructure. This approach integrates SECaaS to enhance the security and privacy of GIAGAN-generated anonymized facial images. Once the anonymized images are produced, SECaaS provides robust encryption to protect the data from unauthorized access. The encrypted images are then securely recorded on a blockchain, ensuring tamper-proof storage and maintaining an immutable record of the anonymization process. SECaaS also enforces strict access controls and continuous monitoring to detect and respond to security threats in real time. Additionally, it offers auditing capabilities to ensure compliance with data protection regulations. SECaaS ensures that the entire process, from anonymization to data storage and access, is secure and transparent, protecting individuals' privacy and maintaining data integrity. Figure 3 shows the full SECaaS architecture.

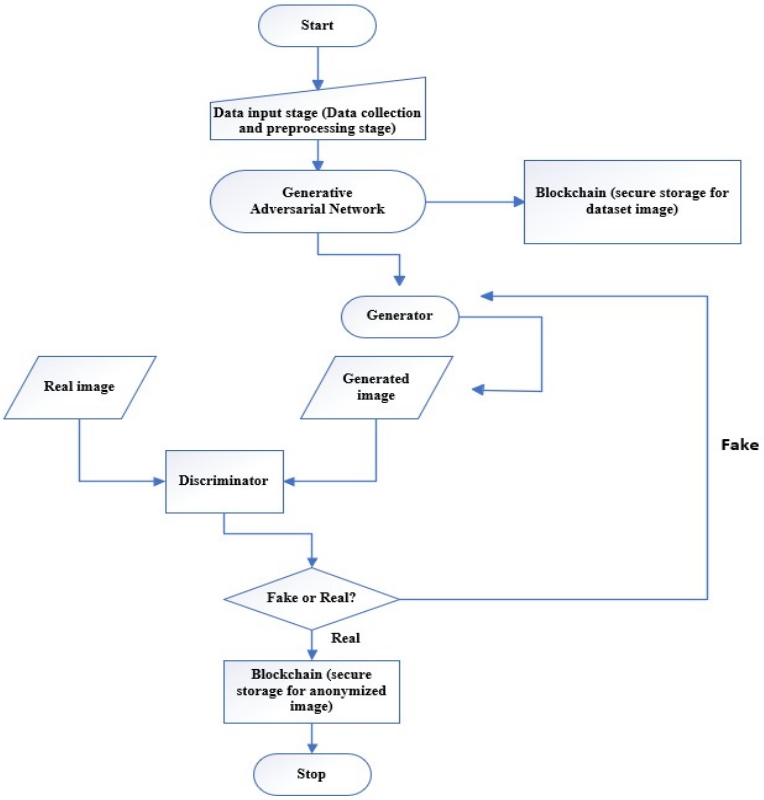

Fig. 2. Flowchart of the proposed intelligent face anonymization model.

III. DEVELOPMENT

A. Tool and Technologies

Table II details the software tools used to develop the proposed method. The codebase for training and producing anonymous photos and movies was largely developed using Python libraries and modules. Given its extensive use in machine learning and deep learning, as well as its interoperability with popular environments such as Google Colab and VS coding, Python 3 was selected as the programming language [51, 52]. Python also helped optimize resources thanks to its open-source nature, small memory footprint, and support for GPU acceleration to speed up training. By including TensorFlow and PyTorch libraries, the model's capabilities were further increased. PyTorch stood out due to its user-friendly interface and strong support for intricate neural network designs.

TABLE II. RESOURCES AND LIBRARIES USED FOR DEVELOPMENT

Tool	Specification
Pandas	To generate a data frame for the dataset.
PyTorch	For deep learning and image processing
OpenCV (cv2)	For computer vision and image processing
CUDA v12.0	NVIDIA API for GPU acceleration
Matplotlib	For data visualization
NumPy	To generate a random image for test data
Kaggle API	To fetch the CelebA dataset
DeepFace	API for facial recognition
Dlib	Used for facial landmark detection

B. Training Strategy

CIAGAN was implemented using the TensorFlow and PyTorch frameworks. The CelebA dataset was preprocessed, with images resized to 128×128 pixels to ensure consistency. The Least Squares Generative Adversarial Network (LSGAN) framework was integrated to enhance training stability and image quality by modifying the traditional GAN loss function. Specifically, the LSGAN loss function minimizes the Pearson χ^2 divergence, resulting in more stable training dynamics. The generator and discriminator were optimized using the Adam optimizer with a learning rate of 0.0001. The performance of CIAGAN was evaluated using PSNR and SSIM to ensure high-quality and similar anonymized images. Blockchain was used to store and manage the anonymized images securely. This integration provides a comprehensive solution for facial image anonymization, maintaining privacy while ensuring the usability and security of the anonymized data.

IV. EXPERIMENTAL RESULTS

A. Performance Metrics

SSIM and PSNR are classic performance metrics to evaluate pictures. PSNR compares the produced images to their source and yields a quality score by calculating the peak signal power ratio to the power of picture differences. The PSNR formula is as follows:

$$PSNR = 10 \cdot log10P(\frac{Max^2}{MSE}) \quad (9)$$

where *Max* is the highest 8-bit value that a picture can have. Averaging the squared discrepancies between adjacent pixels can determine the Mean Squared Error (MSE) between the produced and source images. In general, a PSNR between 30 and 50 dB is considered to indicate good picture quality. SSIM evaluates picture quality by considering structure, brightness, and contrast. SSIM measures the degree to which the produced images structurally resemble the original. A siamese network architecture was used to enhance the model's capability to distinguish between similar and dissimilar images. The siamese network was trained using a contrastive loss function, encouraging the network to minimize the feature distance between images of the same identity and maximizing the distance between different images. This training strategy enables the siamese network to learn discriminative features that facilitate effective facial recognition and similarity assessment. SSIM is given by:

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (10)$$

where the compared images are denoted by x and y, μ represents their mean values, σ^2 represents their variance, and σ their dispersion. Finally, the division with a weak denominator can be stabilized by using the tiny constants C_1 and C_2. An SSIM value close to 1 means that the original and generated images are very similar, a value of -1 indicates perfect anti-correlation, and a value of 0 means that there is no resemblance. The experimental results showed that the images produced had a high-quality output with a PSNR of 35.0516 and an SSIM score of 0.8898.

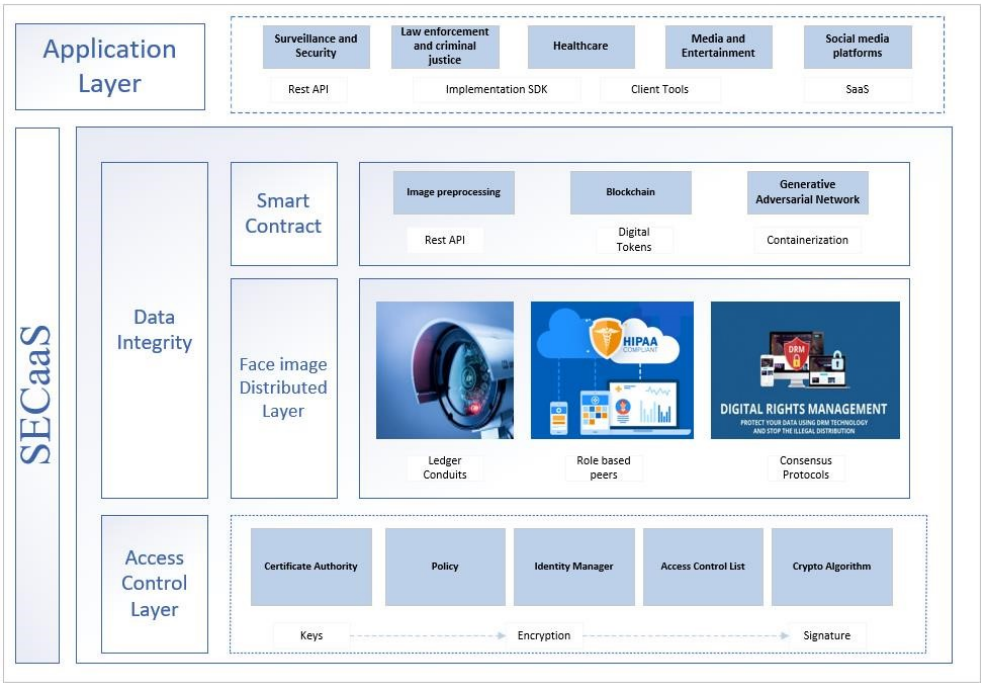

Fig. 3. SECaaS diagram of proposed intelligent face anonymization model.

B. *Quantitative Results*

Figure 4 displays the model's loss convergence, illustrating the patterns for the discriminator (Critic), Generator, and the siamese network. The presence of a noticeable plateau in both the discriminator and generator curves indicates the achievement of a stable condition, suggesting that the generator regularly produces images of sufficient quality to deceive the discriminator into classifying them as authentic. In contrast, the curve of the siamese network demonstrates a pattern of decreasing loss as the number of repetitions increases, indicating a consistent improvement in the network's capacity to differentiate between similarities and differences across images during training. This pattern highlights the network's ability to acquire knowledge and enhance its image categorization skills through greater exposure to training data.

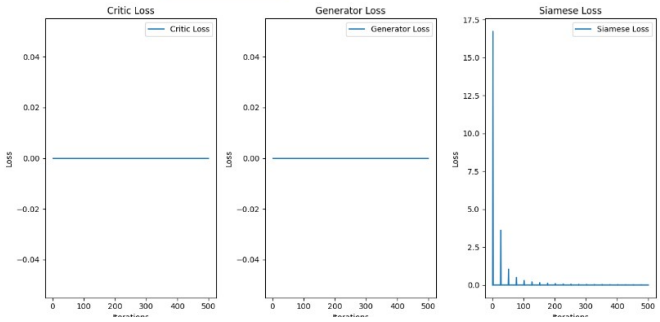

Fig. 4. Convergence loss for the proposed model.

Figure 5 shows a comparison of a picture processed using blurring and the proposed model. Unlike typical blurring techniques that indiscriminately cover visual information, the

proposed model uses complex algorithms to enable successful anonymization while maintaining the subject's original attitude. Blurring, particularly in the context of computer vision applications, has some limits when it comes to tasks like tracking and identification. The shortcomings of conventional blurring techniques in terms of adjusting to and learning from sample photographs were described in [31], which impedes their effectiveness in image de-identification. However, the proposed model produces excellent anonymized photographs, demonstrating its remarkable performance and ability to preserve original features while enhancing privacy.

The process of anonymizing videos using the proposed intelligent model involved the execution of a series of steps. At first, the video feed was divided into separate image frames to make it easier to process. Following the initial stages, subsequent procedures were followed to isolate and crop facial regions from each frame. Then, these regions were subjected to anonymization procedures to obscure identifiable features. After removing personal information, these facial segments were reinserted into their corresponding video sequences, guaranteeing thorough anonymization of facial data while maintaining the overall authenticity of the visual content, as shown in Figures 7 and 8.

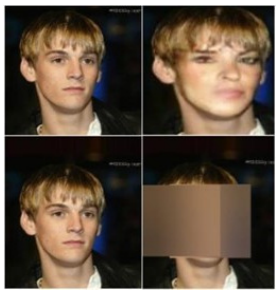

Fig. 5. A test image processed using blurring and the proposed method.

Fig. 6. The first and third columns show the original images, while the second and fourth present their anonymized counterparts.

Fig. 7. Faces extracted from the test video.

Fig. 8. Faces in the test video after anonymization

C. Performance Evaluation of Face Anonymization

The model's performance was comprehensively evaluated using multiple measures, as shown in Table III and Figure 9. The Fréchet Inception Distance (FID) scores, which measure the similarity between generated and genuine images, were consistently low in all subsets. The testing subset had the lowest FID value of 15.05, indicating a higher degree of similarity to real images. The precision, recall, and F1-score metrics measure the accuracy of the model in classifying and detecting features. These measures consistently show high values, indicating strong performance.

TABLE III. FACE EVALUATION METRICS RESULT

	FID	**Precision**	**Recall**	**F1-score**	**mAP @0.5**	**mAP @0.5:0.95**
Training	18.82	0.817	0.614	0.701	0.349	0.349
Validation	19.01	0.829	0.595	0.692	0.346	0.341
Testing	15.05	0.802	0.620	0.705	0.349	0.345

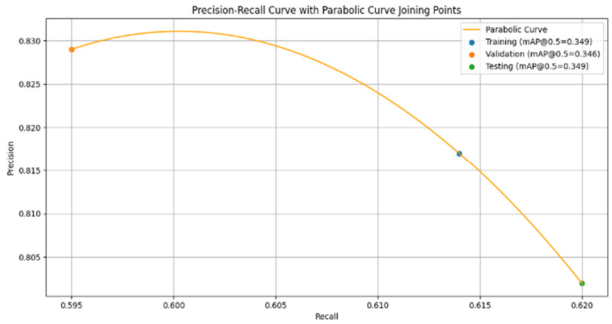

Fig. 9. Precision over recall curve.

V. COMPARATIVE ANALYSIS

A. Baseline Approach vs. Proposed Anonymization Model

Conventional techniques for blurring faces are inadequate in facilitating the identification and monitoring of faces in computer vision tasks. In addition, the provision of limited anonymity is observed due to the ease with which blurred regions can be reversed using widely used image filtering algorithms. Figure 5 shows that the intelligent model outperforms the baseline blurring method when it comes to keeping users' identities hidden while still preserving important visual details.

B. Proposed Model vs AnonymousNet

AnonymousNet [52] employs a GAN model to achieve image de-identification. However, the produced images frequently display inconsistencies, such as variations in hair

color, compared to the original images. The proposed method for image anonymization protects privacy while preserving the authenticity of the original images. Unlike AnonymousNet, which has the potential to introduce inconsistencies in anonymized images, CIAGAN guarantees a higher level of precision in replicating essential characteristics by integrating facial landmarks and utilizing advanced image processing methods. After comparing the two models, as shown in Table IV, it is clear that the proposed Intelligent Model outperformed AnonymousNet in various important metrics. The SSIM score of 0.8898 indicates a higher degree of similarity to the source images, and the PSNR value of 35.0516 indicates less noise and improved fidelity in the generated images. The results validate the superiority of the proposed model in producing high-quality images, showcasing its efficacy and reliability in practical situations.

TABLE IV. PERFORMANCE METRICS RESULT COMPARISON

Model	PSNR	SSIM
AnonymousNet [52]	20.07	0.7894
Proposed Model	35.0516	0.8898

VI. CONCLUSIONS

This study presents a comprehensive framework for facial image anonymization. Combining CIAGAN and blockchain, this study addresses privacy concerns associated with facial popularity structures. The proposed technique demonstrated excellent results in balancing first-class image privacy, as verified by extensive experimentation and evaluation with AnonymousNet. CIAGAN enables the introduction of stunning anonymized images with minimal loss of quality, as evidenced by the PSNR and SSIM metrics. The proposed method provides a compelling strategy to address the growing need for privacy and facial recognition in unique application domains. It also provides certain safe and responsible use, meeting the growing demands. In the future, additional research efforts are needed to enhance the efficiency and scalability of the proposed framework. Effectively managing large datasets and dealing with the complexities of real-time deployment are critical. Furthermore, exploring advanced strategies such as federated knowledge or differential privacy could significantly improve the privacy properties of this framework.

REFERENCES

[1] M. Haider AbdAlkreem, R. Sadoon Salman, and F. Khiled Al-Jibory, "Detect People's Faces and Protect Them by Providing High Privacy Based on Deep Learning," *Tehnički glasnik*, vol. 18, no. 1, pp. 92–99, Feb. 2024, https://doi.org/10.31803/tg-20231210183347.

[2] Y. Said, M. Barr, and H. E. Ahmed, "Design of a Face Recognition System based on Convolutional Neural Network (CNN)," *Engineering, Technology & Applied Science Research*, vol. 10, no. 3, pp. 5608–5612, Jun. 2020, https://doi.org/10.48084/etasr.3490.

[3] D. Virmani, P. Girdhar, P. Jain, and P. Bamdev, "FDREnet: Face Detection and Recognition Pipeline," *Engineering, Technology & Applied Science Research*, vol. 9, no. 2, pp. 3933–3938, Apr. 2019, https://doi.org/10.48084/etasr.2492.

[4] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face Recognition Systems: A Survey," *Sensors*, vol. 20, no. 2, Jan. 2020, Art. no. 342, https://doi.org/10.3390/s20020342.

[5] H. M. Al-Dabbas, R. A. Azeez, and A. E. Ali, "Two Proposed Models for Face Recognition: Achieving High Accuracy and Speed with Artificial Intelligence," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13706–13713, Apr. 2024, https://doi.org/10.48084/etasr.7002.

[6] S. Jana, A. Narayanan, and V. Shmatikov, "A Scanner Darkly: Protecting User Privacy from Perceptual Applications," in *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, Feb. 2013, pp. 349–363, https://doi.org/10.1109/SP.2013.31.

[7] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," *Journal of Information Security and Applications*, vol. 82, May 2024, Art. no. 103748, https://doi.org/10.1016/j.jisa.2024.103748.

[8] E. Kavoliūnaitė-Ragauskienė, "Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union," *Journal of Human Rights Practice*, Jan. 2024, https://doi.org/10.1093/jhuman/huad065.

[9] L. Yang *et al.*, "Exploring the role of computer vision in product design and development: a comprehensive review," *International Journal on Interactive Design and Manufacturing (IJIDeM)*, Mar. 2024, https://doi.org/10.1007/s12008-024-01765-7.

[10] R. K. Shukla and A. K. Tiwari, "Security Analysis of the Cyber Crime," in *The Ethical Frontier of AI and Data Analysis*, IGI Global, 2024, pp. 257–271.

[11] G. Kaur *et al.*, "Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime," *Engineering Proceedings*, vol. 62, no. 1, 2024, Art. no. 6, https://doi.org/10.3390/engproc2024062006.

[12] A. Kammoun, R. Slama, H. Tabia, T. Ouni, and M. Abid, "Generative Adversarial Networks for Face Generation: A Survey," *ACM Computing Surveys*, vol. 55, no. 5, Sep. 2022, Art. no. 94, https://doi.org/10.1145/3527850.

[13] S. Arman, T. Yang, S. Shahed, A. Mazroa, A. Attiah, and L. Mohaisen, "A Comprehensive Survey for Privacy-Preserving Biometrics: Recent Approaches, Challenges, and Future Directions," *Computers, Materials & Continua*, vol. 78, no. 2, pp. 2087–2110, 2024, https://doi.org/10.32604/cmc.2024.047870.

[14] H. Albalawi, "Human Recognition Theory and Facial Recognition Technology: A Topic Modeling Approach to Understanding the Ethical Implication of a Developing Algorithmic Technologies Landscape on How We View Ourselves and Are Viewed by Others," Ph.D. dissertation, University of Central Florida, 2023.

[15] L. Arbuckle and K. E. Emam, *Building an Anonymization Pipeline: Creating Safe Data*. Sebastopol, CA, USA: O'Reilly Media, Inc., 2020.

[16] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, vol. 57, 2010, Art. no. 1701.

[17] R. H. Weber and U. I. Heinrich, *Anonymization*. Springer Science & Business Media, 2012.

[18] T. Li and L. Lin, "AnonymousNet: Natural Face De-Identification With Measurable Privacy," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Long Beach, CA, USA, Jun. 2019, pp. 56–65, https://doi.org/10.1109/CVPRW.2019.00013.

[19] D. Saxena and J. Cao, "Generative Adversarial Networks (GANs): Challenges, Solutions, and Future Directions," *ACM Computing Surveys*, vol. 54, no. 3, Feb. 2021, Art. no. 63, https://doi.org/10.1145/3446374.

[20] V. Asokan, "Handling Class Imbalance Using Generative Adversarial Network (GAN) and Convolutional Neural Network (CNN)," University of Reading, UK, Sep. 2021.

[21] W. Zhang, "Generating Adversarial Examples in One Shot With Image-to-Image Translation GAN," *IEEE Access*, vol. 7, pp. 151103–151119, 2019, https://doi.org/10.1109/ACCESS.2019.2946461.

[22] I. Goodfellow *et al.*, "Generative Adversarial Nets," in *Advances in Neural Information Processing Systems*, 2014, vol. 27.

[23] E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," *IEEE Transactions on Knowledge and Data*

Engineering, vol. 17, no. 2, pp. 232–243, Oct. 2005, https://doi.org/10.1109/TKDE.2005.32.

[24] R. Gross, E. Airoldi, B. Malin, and L. Sweeney, "Integrating Utility into Face De-identification," in *Privacy Enhancing Technologies*, 2006, pp. 227–242, https://doi.org/10.1007/11767831_15.

[25] C. Neustaedter, S. Greenberg, and M. Boyle, "Blur filtration fails to preserve privacy for home-based video conferencing," *ACM Transactions on Computer-Human Interaction*, vol. 13, no. 1, pp. 1–36, Nov. 2006, https://doi.org/10.1145/1143518.1143519.

[26] W. M. S. Yafooz, E. A. Hizam, and W. A. Alromema, "Arabic Sentiment Analysis on Chewing Khat Leaves using Machine Learning and Ensemble Methods," *Engineering, Technology & Applied Science Research*, vol. 11, no. 2, pp. 6845–6848, Apr. 2021, https://doi.org/0.48084/etasr.4026.

[27] H. Chi and Y. H. Hu, "Face de-identification using facial identity preserving features," in *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Sep. 2015, pp. 586–590, https://doi.org/10.1109/GlobalSIP.2015.7418263.

[28] K. Brkic, I. Sikiric, T. Hrkac, and Z. Kalafatic, "I Know That Person: Generative Full Body and Face De-identification of People in Images," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Honolulu, HI, USA, Jul. 2017, pp. 1319–1328, https://doi.org/10.1109/CVPRW.2017.173.

[29] Y. Li and S. Lyu, "De-identification Without Losing Faces," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, Paris, France, Apr. 2019, pp. 83–88, https://doi.org/10.1145/3335203.3335719.

[30] J. Chen, J. Konrad, and P. Ishwar, "VGAN-Based Image Representation Learning for Privacy-Preserving Facial Expression Recognition," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Salt Lake City, UT, USA, Jun. 2018, pp. 1651–165109, https://doi.org/10.1109/CVPRW.2018.00207.

[31] M. Maximov, I. Elezi, and L. Leal-Taixé, "CIAGAN: Conditional Identity Anonymization Generative Adversarial Networks," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Seattle, WA, USA, Jun. 2020, pp. 5446–5455, https://doi.org/10.1109/CVPR42600.2020.00549.

[32] H. Choudhury, B. Goswami, and S. K. Gurung, "CovidChain: An Anonymity Preserving Blockchain Based Framework for Protection Against Covid-19," *Information Security Journal: A Global Perspective*, Sep. 2021, https://doi.org/10.1080/19393555.2021.1921315.

[33] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, Aug. 2019, https://doi.org/10.1016/j.future.2019.02.060.

[34] *Face Recognition Technology (FERET)*, NIST. [Online]. Available: https://www.nist.gov/programs-projects/face-recognition-technology-feret.

[35] T. E. Boult, "PICO: Privacy through Invertible Cryptographic Obscuration," in *Computer Vision for Interactive and Intelligent Environment (CVIIE'05)*, Lexington, KY, USA, Aug. 2005, pp. 27–38, https://doi.org/10.1109/CVIIE.2005.16.

[36] D. Chen, Y. Chang, R. Yan, and J. Yang, "Protecting Personal Identification in Video," in *Protecting Privacy in Video Surveillance*, A. Senior, Ed. London, UK: Springer, 2009, pp. 115–128.

[37] R. Cucchiara, A. Prati, and R. Vezzani, "Advanced video surveillance with pan tilt zoom cameras," in *Proceedings of the 6th IEEE International Workshop on Visual Surveillance*, 2006, pp. 334–352.

[38] A. Melle and J. L. Dugelay, "Scrambling faces for privacy protection using background self-similarities," in *2014 IEEE International Conference on Image Processing (ICIP)*, Paris, France, Jul. 2014, pp. 6046–6050, https://doi.org/10.1109/ICIP.2014.7026220.

[39] D. Kasikrit, "AT&T Database of Faces." https://www.kaggle.com/datasets/kasikrit/att-database-of-faces.

[40] M. Xuan and J. Jiang, "Video Security Algorithm Aiming at the Need of Privacy Protection," in *2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery*, Tianjin, China, Dec. 2009, vol. 5, pp. 473–477, https://doi.org/10.1109/FSKD.2009.391.

[41] S. Barattin, C. Tzelepis, I. Patras, and N. Sebe, "Attribute-Preserving Face Dataset Anonymization via Latent Code Optimization," in *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Vancouver, BC, Canada, Jun. 2023, pp. 8001–8010, https://doi.org/10.1109/CVPR52729.2023.00773.

[42] "cifar10 | TensorFlow Datasets." https://www.tensorflow.org/datasets/catalog/cifar10.

[43] "The CMU Multi-PIE Face Database." https://www.cs.cmu.edu/afs/cs/project/PIE/MultiPie/Multi-Pie/Home.html.

[44] S. Alver, "chokepoint-bbs." 2022. https://github.com/alversafa/chokepoint-bbs.

[45] "FERG-DB." https://grail.cs.washington.edu/projects/deepexpr/ferg-2d-db.html.

[46] Z. Ren, Y. J. Lee, and M. S. Ryoo, "Learning to Anonymize Faces for Privacy Preserving Action Detection," presented at the Proceedings of the European Conference on Computer Vision (ECCV), 2018, pp. 620–636, Accessed: May 25, 2024.

[47] H. Jhuang, J. Gall, S. Zuffi, C. Schmid, and M. J. Black, "JHMDB Dataset." http://jhmdb.is.tue.mpg.de/.

[48] A. E. Yahya, A. Gharbi, W. M. S. Yafooz, and A. Al-Dhaqm, "A Novel Hybrid Deep Learning Model for Detecting and Classifying Non-Functional Requirements of Mobile Apps Issues," *Electronics*, vol. 12, no. 5, Jan. 2023, Art. no. 1258, https://doi.org/10.3390/electronics12051258.

[49] M. Kawulok, M. E. Celebi, and B. Smolka, "Labeled Faces in the Wild." University Of Massachusetts, 2016.

[50] Z. Liu, P. Luo, X. Wang, and X. Tang, "Large-scale CelebFaces Attributes (CelebA) Dataset." Available: https://mmlab.ie.cuhk.edu.hk/projects/CelebA.html.

[51] S. I. Alqahtani, W. M. S. Yafooz, A. Alsaeedi, L. Syed, and R. Alluhaibi, "Children's Safety on YouTube: A Systematic Review," *Applied Sciences*, vol. 13, no. 6, Jan. 2023, Art. no. 4044, https://doi.org/10.3390/app13064044.

[52] T. Li and L. Lin, "AnonymousNet: Natural Face De-Identification With Measurable Privacy," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Long Beach, CA, USA, Jun. 2019, pp. 56–65, https://doi.org/10.1109/CVPRW.2019.00013.