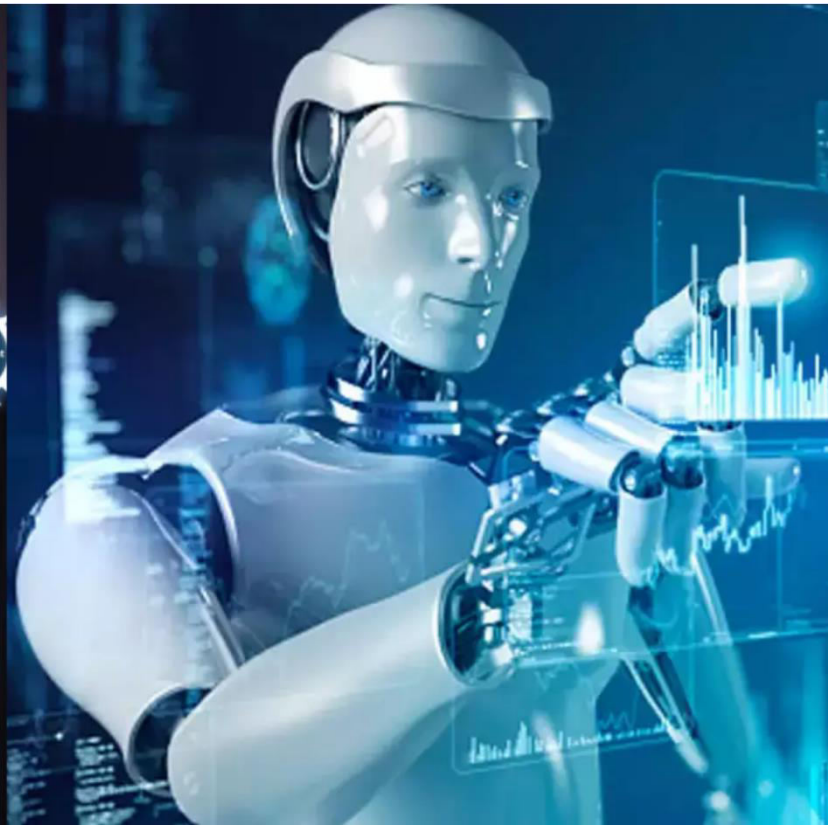
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503226|

Intelligent Face Detection and Preprocessing System: A Review

Priyanka Subhash Gurav, Prof.A.D.Gujar

Department of Computer Engineering, TSSM's Bhivarabai Sawant College of Engineering and Research, Narhe, Pune, India

ABSTRACT-The rapid expansion of facial image datasets, protecting individual privacy while maintaining data utility has become a critical challenge. Traditional anonymization techniques often degrade image quality or fail to effectively conceal identity. This study proposes a hybrid face anonymization framework that integrates Face Latent Anonymization (FLA) and Face Feature Anonymization (FFA). The latent space modification disrupts identity-related attributes, while semantic mask-guided feature anonymization preserves essential non-identity characteristics such as pose, expression, and age. The combined approach ensures realistic image generation with strong identity obfuscation. Experimental evaluation on CelebA-HQ and LFW datasets demonstrates superior performance compared to existing GAN-based anonymization methods. Results confirm that the proposed model achieves a balanced trade-off between privacy protection and data usability for downstream machine learning applications.

KEYWORDS- Face Anonymization, Latent Space, Feature Space, StyleGAN, Privacy Preservation.

I. INTRODUCTION

The rapid advancement of artificial intelligence and deep learning has significantly increased the use of facial image datasets in applications such as surveillance, healthcare, authentication, and social media analytics. While these datasets enable powerful recognition and analysis systems, they also raise serious privacy concerns. Facial images contain unique biometric identifiers that can reveal an individual's identity without consent. Regulatory frameworks such as GDPR emphasize strict protection of personal data, creating the need for reliable anonymization techniques. However, removing identity information without damaging the image's analytical value remains a complex challenge. Traditional masking or blurring approaches often degrade image quality and reduce usability for further tasks like attribute prediction or detection.

Early anonymization techniques relied on simple image processing operations such as pixelation, masking, or blurring. Although these methods obscure visible identity details, they significantly distort important facial attributes. As a result, anonymized images become unsuitable for advanced machine learning applications. With the emergence of Generative Adversarial Networks (GANs), more sophisticated face replacement and inpainting approaches were introduced. These techniques generate synthetic faces to replace original identities, producing more realistic outputs. However, many GAN-based methods either fail to preserve subtle facial attributes or struggle to ensure complete identity obfuscation. Some methods focus only on latent space manipulation, leaving feature-level identity traces intact.

To address these limitations, a more comprehensive anonymization strategy is required. Effective facial anonymization must ensure strong identity protection while preserving non-sensitive attributes such as age, pose, and expression. Maintaining this balance is essential for keeping anonymized datasets useful for research and model training. Therefore, integrating both latent space transformation and feature space modification provides a promising direction. By combining these techniques, it becomes possible to produce realistic, high-quality images that protect privacy while retaining analytical utility.

II. MOTIVATION

The growing availability of publicly accessible facial datasets increases the risk of identity misuse and privacy violations. Existing anonymization methods either compromise visual realism or fail to fully conceal identity-related features. There is a strong need for a system that can guarantee privacy protection without reducing dataset utility. The

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503226|

motivation behind this work is to develop a hybrid anonymization framework that effectively hides identity while maintaining structural and semantic facial attributes required for machine learning applications.

III. GAP ANALYSIS

Existing anonymization techniques primarily focus on either latent space manipulation or feature-level modification, but rarely both. Latent-only approaches may leave identifiable visual cues in the feature space, while feature-based methods may not sufficiently disrupt identity embeddings used in recognition systems. Additionally, many GAN-based techniques introduce artifacts, distort facial geometry, or reduce attribute consistency. Therefore, there is a research gap in developing an integrated approach that simultaneously ensures strong anonymization, high image quality, and attribute preservation.

IV. LITERATURE SURVEY

EmreOzen [1], In this study, a comprehensive methodology and system implementation are proposed for concurrent face detection, landmark extraction, quality assessment, and face recognition directly at the edge, without relying on external resources. The approach integrates cutting-edge techniques, including the utilization of the Extended YOLO model for face detection and the ArcFace model for feature extraction, optimized for deployment on embedded devices. By leveraging these models alongside a dedicated recognition database and efficient software architecture, the system achieves remarkable accuracy and real-time processing capabilities.

MAHMOODULHAQ [2], In this paper, we have developed an augmented reality cricket broadcasting application that uses player face recognition during play to display player personal data. The system utilizes the AdaBoost algorithm for player and player face detection, employing a PAL based face recognition model to recognize the faces of players on the field.

HATEF OTROSHI SHAHREZA [3], The results on different benchmarking real face recognition datasets demonstrate the superiority of SynthDistill compared to training on previous synthetic datasets, achieving a verification accuracy of 99.52% on the LFW dataset with a lightweight network. The results also show that SynthDistill significantly narrows the gap between real and synthetic data training. The source code of our experiments is publicly available to facilitate the reproducibility of our work

ZIQILIU [4], this paper proposes an innovative coverless steganography framework for face recognition images based on diffusion model. The framework firstly extracts face features and generates masks containing these features. Then, combined with conditional diffusion model and text key, a deterministic Denoising Diffusion Implicit Model (DDIM) is used to sample coverless steganography images. Secret images can also be recovered in high quality with DDIM Inversion technology.

JHON I. PILATAXI [5], Facerecognition(FR)isoneofthemostwidelyusedbiometricmethodsforidentityauthentica tion. Although most of the recently proposed methods demonstrate remarkable performance on high-quality datasets, such as LFW, their effectiveness is limited when assessed on low-resolution images. To address this challenge, knowledge distillation and super-resolution techniques have been applied, primarily using the ResNet architecture.

Jianyu Xiao [6], The Face Anti-Spoofing (FAS) methods plays a very important role in ensuring the security of face recognition systems. The existing FAS methods perform well in short-distance scenarios, e.g., phone unlocking, face payment, etc. However, it is still challenging to improve the generalization of FAS in long-distance scenarios (e.g., surveillance) due to the varying image quality.

SiddhikaPokharkar [7], This paper presents a dual-factor authentication system that integrates face recognition and Personal Identification Number (PIN) verification to improve ATM transaction security. Utilizing a Convolutional Neural Network (CNN) for real-time face recognition, the proposed system significantly reduces the risk of unauthorized access.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503226|

SudhaV [8], The review also analyses research gaps and future directions in areas like multimodal fusion, explainable AI, collaborative learning, online adaptation etc. Overall, this review provides useful insights into the capabilities and limitations of existing literature which can guide future research on secure face recognition systems for attendance marking.

Jiankang Deng [9], In this paper, we first introduce an Additive Angular Margin Loss (ArcFace), which not only has a clear geometric interpretation but also significantly enhances the discriminative power. Since ArcFace is susceptible to the massive label noise, we further propose sub-centerArcFace, in which each class contains K sub-centers and training samples only need to be close to any of the K positive sub-centers.

ROLAND STENGER [10], In this work, we investigate the influence of different image-based subject anonymization methods on the performance of the three common computer vision (CV) tasks: keypoint detection, instance segmentation, and face detection. We compare the anonymization methods on how much they affect the performance of the CV tasks, as well as their degree of anonymization. Furthermore, a re identification attack scenario is applied.

EMNA BENSAID [11], This paper introduces a new two-stage anonymization method that combines Deep Face Latent space Anonymization (FLA) with Face Feature space Anonymization (FFA) guided by semantic masks. In the first stage, FLA hides identity by modifying the latent space of facial images. In the second stage, FFA uses semantic masks to preserve important facial features like expressions and head poses while still hiding identity.

HELENA MONTENEGRO [12], In this work, we leverage cold diffusion to decompose superimposed images, empirically demonstrating that it is possible to obtain two or more identically-distributed images given their average. We propose novel sampling strategies for this task and show their efficacy on three datasets. Our findings highlight the risks of averaging images as an anonymization technique and argue for the use of alternative anonymization strategies.

V. ARCHITECTURE

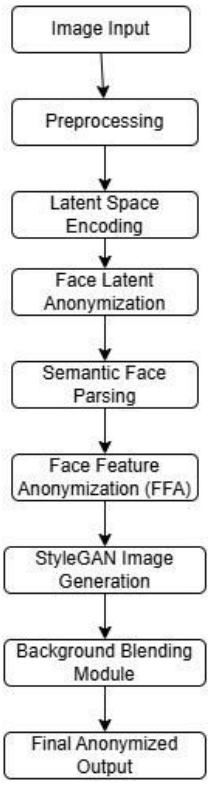


Figure 1.Block Diagram

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503226|

VI. EXISTING SYSTEM

Current face anonymization systems include traditional image obfuscation methods such as blurring and pixelation, as well as GAN-based face replacement models like DeepPrivacy and CIAGAN. While GAN-based approaches improve visual realism, they often depend heavily on landmark detection and may distort facial attributes. Some methods modify only the latent space of generative models, which may not fully prevent identity leakage from feature representations. These limitations reduce anonymization effectiveness or compromise downstream usability.

VII. PROPOSED SYSTEM

The proposed system introduces a hybrid face anonymization framework that integrates Face Latent Anonymization (FLA) and Face Feature Anonymization (FFA) within a StyleGAN-based generative architecture. First, the input facial image is encoded into the W+ latent space using a pSp encoder, which captures identity and non-identity attributes such as pose, expression, and lighting. The Face Latent Anonymizer then modifies identity-sensitive latent dimensions using an encoder–decoder structure supported by residual blocks and attention mechanisms. During training, Identity Loss is maximized to ensure strong identity alteration, while Attribute Loss is minimized to preserve non-identity facial characteristics. This balanced optimization enables the system to effectively conceal identity while maintaining realistic facial structure and semantic consistency.

In parallel, the Face Feature Anonymizer operates in the image feature space using semantic masks generated through face parsing. These masks segment facial regions such as eyes, nose, mouth, and hair, allowing selective modification of identity-related regions while preserving structural alignment. A randomly generated identity is blended with the original semantic layout to maintain pose and expression consistency. The anonymized latent and feature representations are then injected into the StyleGAN generator to synthesize a high-quality anonymized image. Finally, a blending mechanism preserves the original background to ensure visual coherence. This dual-space anonymization strategy provides stronger privacy protection while maintaining high image quality and usability for downstream machine learning tasks.

VIII. CONCLUSION

This study presents a hybrid face anonymization framework that balances privacy protection and data utility. By combining latent space and feature space anonymization techniques, the proposed system effectively conceals identity while preserving important facial attributes. Experimental results demonstrate superior performance compared to existing methods in terms of image quality and anonymization strength. The framework enables anonymized facial datasets to remain suitable for machine learning applications such as detection and attribute classification. Overall, the proposed approach offers a practical and reliable solution for privacy-preserving facial image analysis in real-world scenarios.

REFERENCES

[1]. EmreOzena, FikretAlima, SefaBurakOkcua, EnesKavaklia, and CevahirCiglaaaAselsan Inc., Yenimahalle, Ankara, T¨urkiye” Real-Time Face Recognition System at the Edge”, April 2024.
[2]. MAHMOODULHAQ SADIQUE AHMAD 1,MUHAMMADATHARJAVEDSETHI,” Automatic Player Face Detection and Recognition for Players in Cricket Games” March 2024.
[3]. HATEF OTROSHI SHAHREZA AND SÉBASTIEN MARCEL,” Knowledge Distillation for Face Recognition Using Synthetic Data With Dynamic Latent Sampling” December 2024.
[4]. YUAN GUO ANDZIQILIU,” Coverless Steganography for Face Recognition Based on Diffusion Model”, October 2024.
[5]. JHON I. PILATAXI 1,2, (Graduate Student Member, IEEE), JUAN P. PEREZ1,2, CLAUDIO A. PEREZ,” Neuroevolutionary Convolutional Neural Network Design for Low-Resolution Face Recognition”, May 2025.
[6] Jianyu Xiao 1, Wei Wang,” AMobileFaceNet-Based Face Anti-Spoofing Algorithm for Low-Quality Images”, uly 2024.
[7] Siddhika Pokharkar1, BhagyashriBhalerao,” A Real Time Face Detection & Security System for ATM Machine.”, May 2025.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503226|

[8] Sudha V, Sangeetha S, Ganesh Shankar S, Arun A, Durga Ram R," FACE RECOGNITION-BASED ATTENDANCE SYSTEMS USING ANTI-SPOOFING METHODS", 2024e-ISBN: 978-93-6252-750-9 IIP Series, Volume 3, Book 4, Part 1.

[9] Jiankang Deng, JiaGuo, Jing Yang, NiannanXue," ArcFace: Additive Angular Margin Loss for Deep Face Recognition", arXiv:1801.07698v4 [cs.CV] 4 Sep 2022.

[10] ROLAND STENGER AND SEBASTIAN FUDICKAR 1,STEFFEN BUSSE 2,JONAS SANDER," Evaluating the Impact of Face Anonymization Methods on Computer Vision Tasks: A Trade-Off Between Privacy and Utility", December 2024.

[11] EMNA BENSAID 1,(Member, IEEE), MOHAMED NEJI1,2, (Senior Member, IEEE), HABIB CHABCHOUB," Facial Dataset Anonymization: Striking the Balance Between Privacy and Utility", December 2024.

[12] HELENA MONTENEGRO 1,2 (Graduate Student Member, IEEE) AND JAIME S. CARDOSO," Leveraging Cold Diffusion for the Decomposition of Identically Distributed Superimposed Images", July 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details