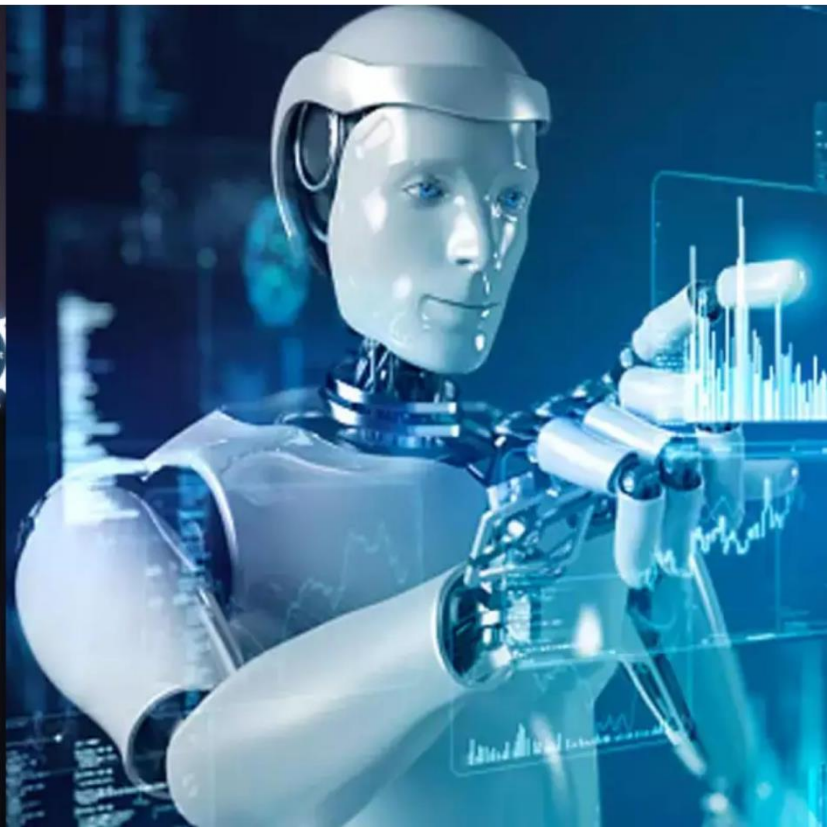
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 4, April 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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

Privacy-Preserving Face Detection and Anonymization System

Priyanka S. Gurav, Prof. A. D. Gujar

P. G. Student, Department of Computer Engineering, TSSM's BSCOER, Narhe, Pune, Maharashtra, India

Assistant Professor, Department of Computer Engineering, TSSM's BSCOER, Narhe, Pune, Maharashtra, India

ABSTRACT: This paper presents a Privacy-Preserving Face Detection and Anonymization System that compares traditional image-processing and deep learning-based techniques for protecting facial identity. The system uses an end-to-end pipeline with face detection (YOLOv8 and Haar Cascade) and evaluates five anonymization methods using metrics like SSIM, PSNR, and Privacy Score. Results show a trade-off between privacy and image quality, where traditional methods offer stronger privacy but reduce usability, while deep learning approaches maintain better image clarity with moderate privacy. The study concludes that adaptive and neural-based methods provide an effective balance, making them suitable for real-world, privacy-compliant applications.

KEYWORDS: Face Detection, Face Anonymization, Deep Learning, YOLOv8, Image Processing.

I. INTRODUCTION

The rapid growth of computer vision technologies has significantly impacted applications such as public safety, smart cities, and retail analytics, where accurate human detection and identification are essential. However, the large-scale collection of visual data, particularly human faces, raises serious privacy concerns. Facial data is considered sensitive under regulations like GDPR, CCPA, and the DPDP Act, making its processing without consent legally challenging.

To address these issues, various face anonymization techniques have been developed, including traditional methods like Gaussian blur and pixelation, as well as advanced deep learning-based approaches. While these techniques help protect identity, they often degrade image quality and reduce the effectiveness of downstream AI tasks.

This project focuses on the critical trade-off between privacy preservation and model performance. It proposes a comprehensive benchmarking framework to evaluate multiple anonymization methods using modern detection models such as YOLOv8. The aim is to identify approaches that ensure privacy while maintaining the utility of computer vision systems, enabling compliance with legal standards.

II. LITERATURE SURVEY

Facial data anonymization has become an important research area due to increasing concerns about privacy protection in computer vision and surveillance systems. Computer Vision and Artificial Intelligence based applications require methods that can protect personal identity while preserving image usability.

Bensaid et al. [1] presented a facial dataset anonymization framework that focused on balancing privacy and utility. The authors compared different anonymization techniques and evaluated their impact on facial recognition accuracy and image quality. Their study highlighted that stronger anonymization improves privacy but reduces the usefulness of images for AI applications.

De Coninck et al. [2] proposed a privacy-preserving visual analysis system for video applications. The authors developed obfuscation models that protect sensitive information without requiring sensitive labels during training. Their work demonstrated that deep learning-based anonymization can preserve important visual information while reducing identity leakage.

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

Sonkar [3] discussed recent innovations in AI privacy and emphasized the importance of protecting user data in machine learning systems. The study reviewed modern AI-based privacy techniques, including anonymization, encryption, and privacy-aware learning models, showing the growing demand for secure AI applications.

Kaur et al. [4] explored advanced data anonymization techniques for secure and privacy-preserving data sharing in big data environments. The authors explained multiple anonymization strategies and highlighted the challenges of maintaining data utility while ensuring privacy protection. Their work showed the importance of adaptive anonymization methods for modern digital systems.

Jain et al. [5] introduced the fundamentals of biometric recognition systems and explained the role of facial features in identity recognition. The study provided a strong foundation for understanding how facial recognition systems operate and why anonymization is necessary to prevent unauthorized identity exposure.

Chen et al. [6] evaluated the impact of data anonymization on image retrieval systems. Their research analyzed how anonymization affects image matching and retrieval accuracy. The results indicated that heavy anonymization improves privacy but can reduce system performance in computer vision tasks.

From the literature survey, it is observed that existing research mainly focuses on balancing privacy protection and image usability. Traditional anonymization methods provide strong privacy but degrade image quality, while deep learning approaches maintain better visual quality with moderate privacy protection. Based on these observations, the proposed work develops a Privacy-Preserving Face Detection and Anonymization System that combines face detection techniques with multiple anonymization methods and evaluates them using privacy and utility metrics for real-world applications.

III. METHODOLOGY

The proposed Privacy-Preserving Face Detection and Anonymization System is designed as a modular benchmarking pipeline that ensures reproducibility, transparency, and measurable privacy–utility trade-offs. The architecture consists of the following interconnected blocks as shown in fig. (a)

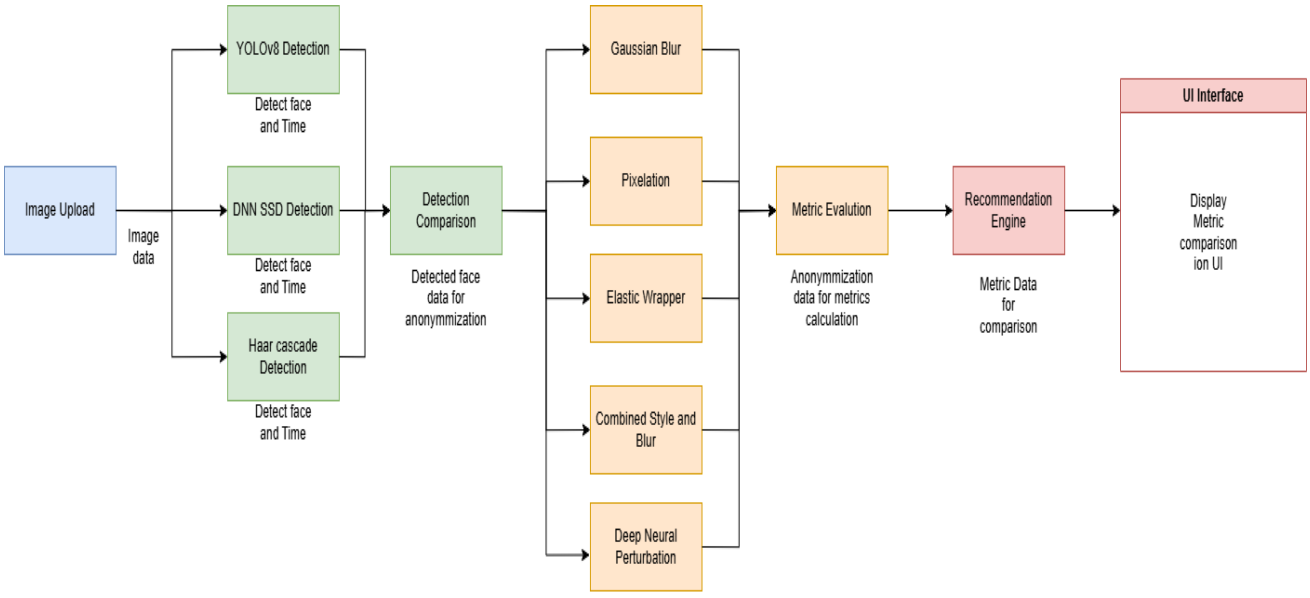


fig.(a) System Architecture

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

1. Image Upload Block
   - Entry point for the workflow.
   - Accepts a single image to maintain controlled benchmarking and reproducibility.

2. Face Detection Blocks (YOLOv8, DNN SSD, Haar Cascade)
   - Three parallel detectors analyze the image.
   - YOLOv8 offers speed and accuracy, DNN SSD balances precision with efficiency, and Haar Cascade provides a lightweight classical option.

3. Each outputs bounding boxes and detection time.
Detection Comparison Block
   - Compares detectors based on accuracy and processing time.
   - Selects the most efficient detector for the given image.
   - Passes chosen bounding box coordinates to segmentation.

4. Face Segmentation Block
   - Isolates the facial region of interest (ROI).
   - Ensures only sensitive areas are anonymized while preserving contextual integrity.

5. Anonymization Blocks
Five anonymization methods applied to the ROI:
   - Gaussian Blur (simple, legally compliant)
   - Pixelation (clear privacy shield)
   - Elastic Warp (distorts geometry, breaks identity)
   - Stylization + Blur (natural, aesthetic anonymization)
   - Deep Neural Perturbation (CNN-based feature noise injection for strong privacy with minimal utility loss).

6. Metrics Evaluation Block
   - Computes quantitative measures: SSIM, PSNR, MSE, Sharpness Retained, Detection Evasion, Re-identification detectability, and Irreversibility.
   - Provides a comprehensive privacy–utility assessment.

7. Recommendation Engine Block
   - Synthesizes metrics to recommend the optimal detector and anonymization method.
   - Ensures compliance with privacy regulations (GDPR, CCPA, DPDP Act) while maintaining operational usability.

Algorithm:
The system operates in a sequential pipeline:
1. Image Upload – User provides a single image for reproducible benchmarking.
2. Face Detection – YOLOv8, DNN SSD, and Haar Cascade run in parallel, outputting bounding boxes, counts, and processing times.
3. Detection Comparison – Results are compared; the best detector is selected based on speed–accuracy trade-off.
4. Segmentation – The chosen bounding box isolates the facial ROI, preserving background context.
5. Anonymization – Five methods (Blur, Pixelation, Elastic Warp, Stylization+Blur, Deep Neural Perturbation) anonymize the ROI independently.
6. Metrics Evaluation – Outputs are assessed using fidelity (SSIM, PSNR, MSE), utility (sharpness, detection evasion), and privacy (re-identification, irreversibility).
7. Recommendation – Metrics aggregated into a Privacy–Utility Balance Score (60% privacy, 40% utility). Best detector and anonymization method are identified.
8. Output – UI displays detection comparison, anonymized results, metrics dashboard, and final recommendation.

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

IV. EXPERIMENTAL RESULTS

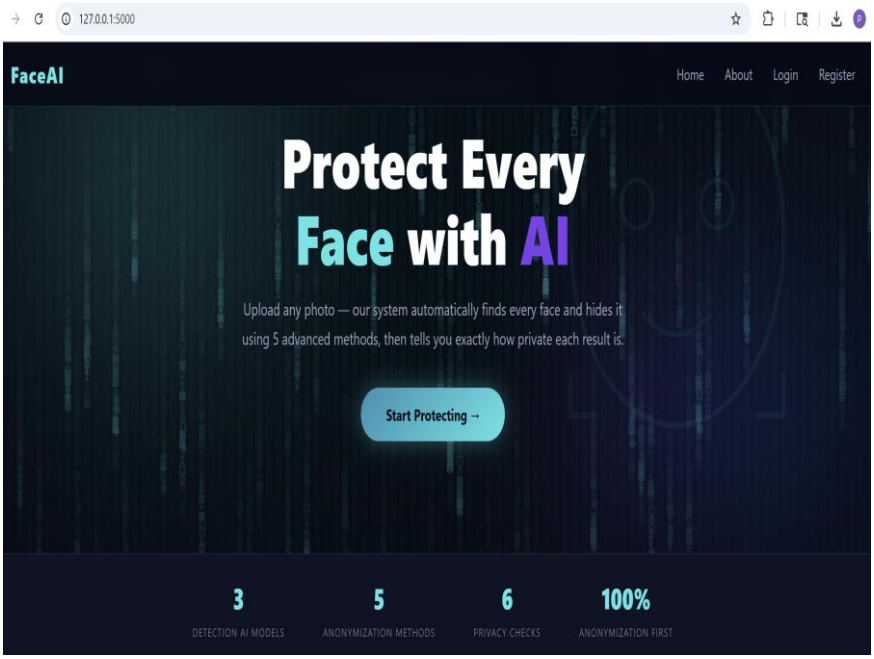


Fig.(a)

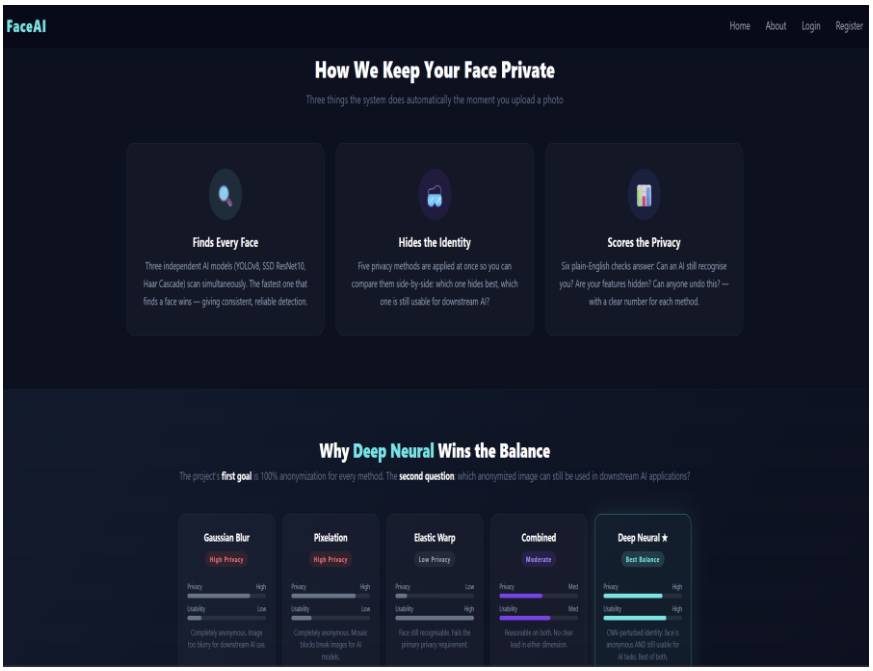


Fig.(b)

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

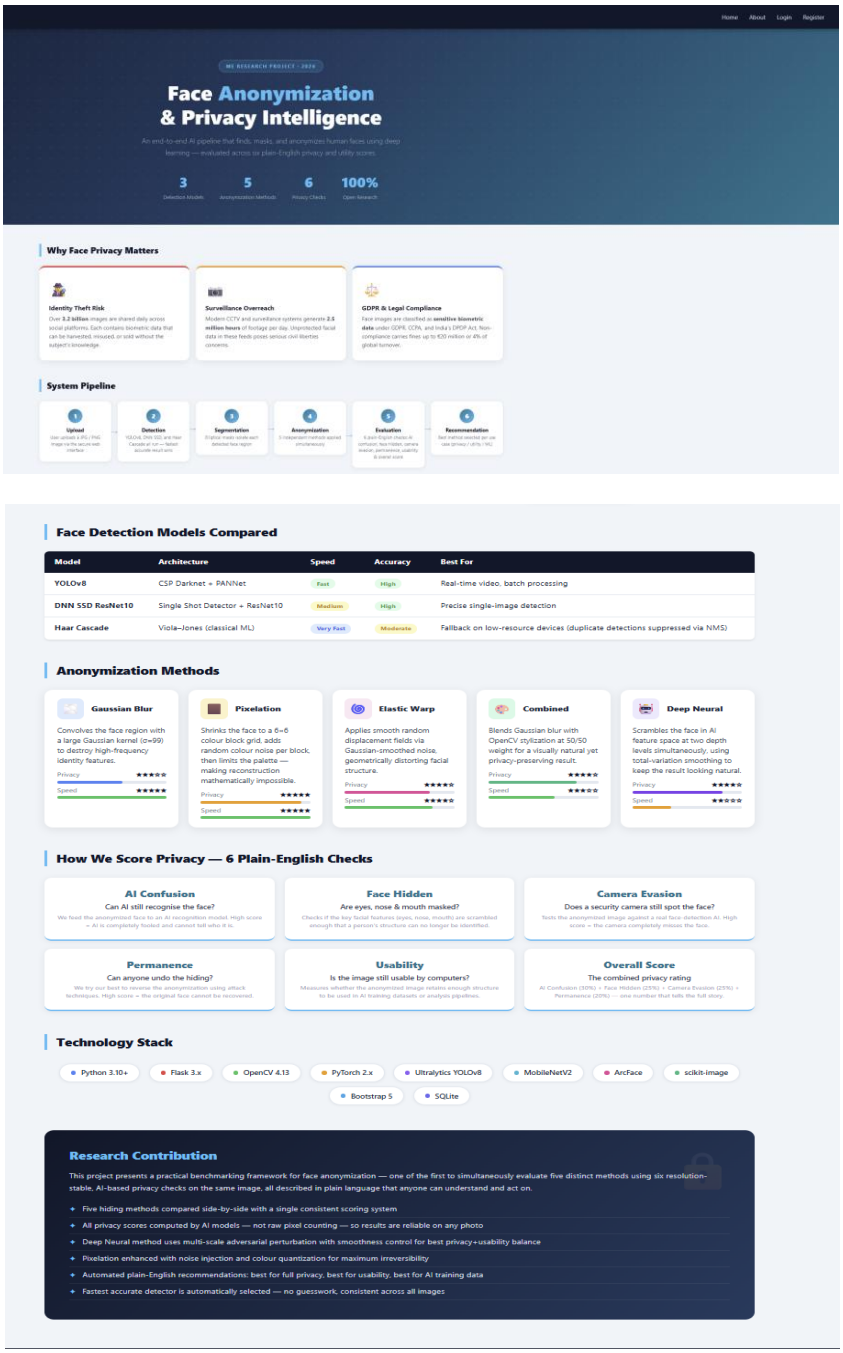


fig.(c)

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

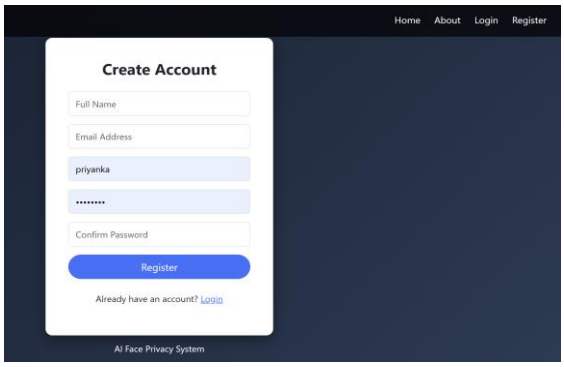


Fig. (d)

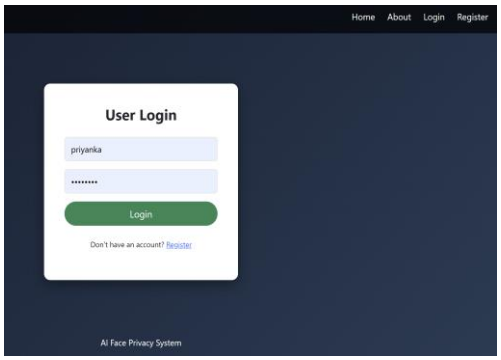


fig. (e)

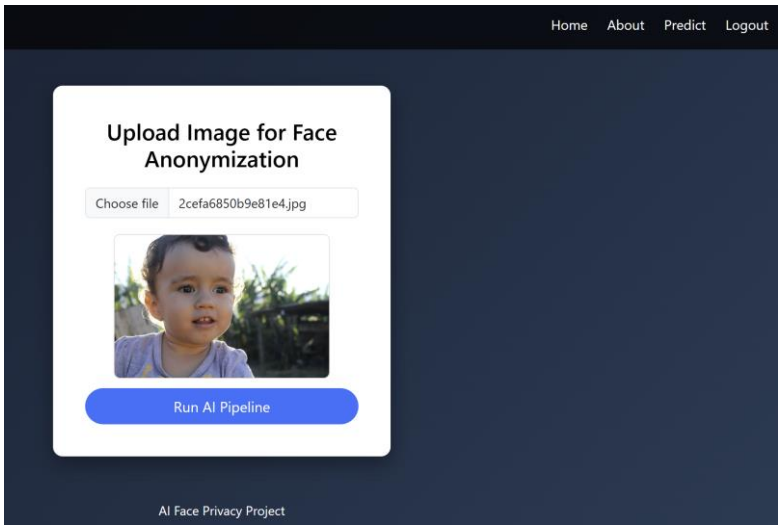
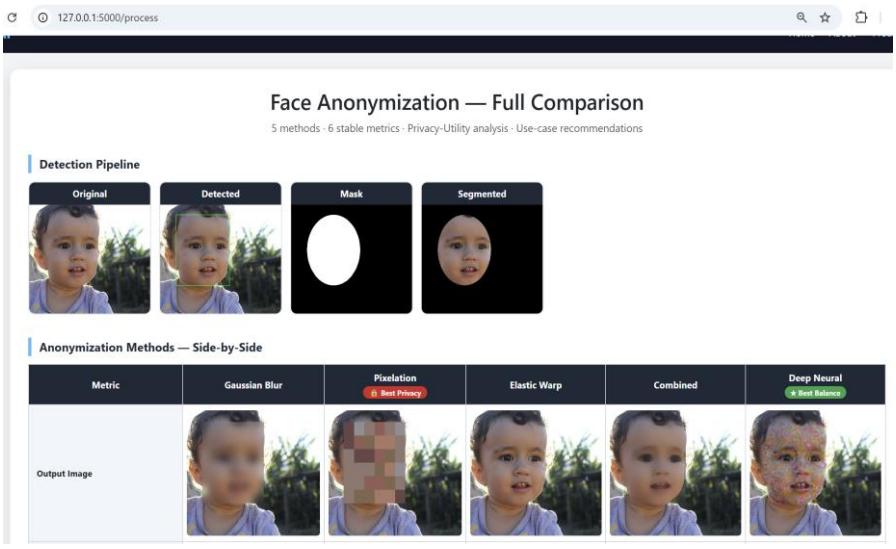


Fig.(f)



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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

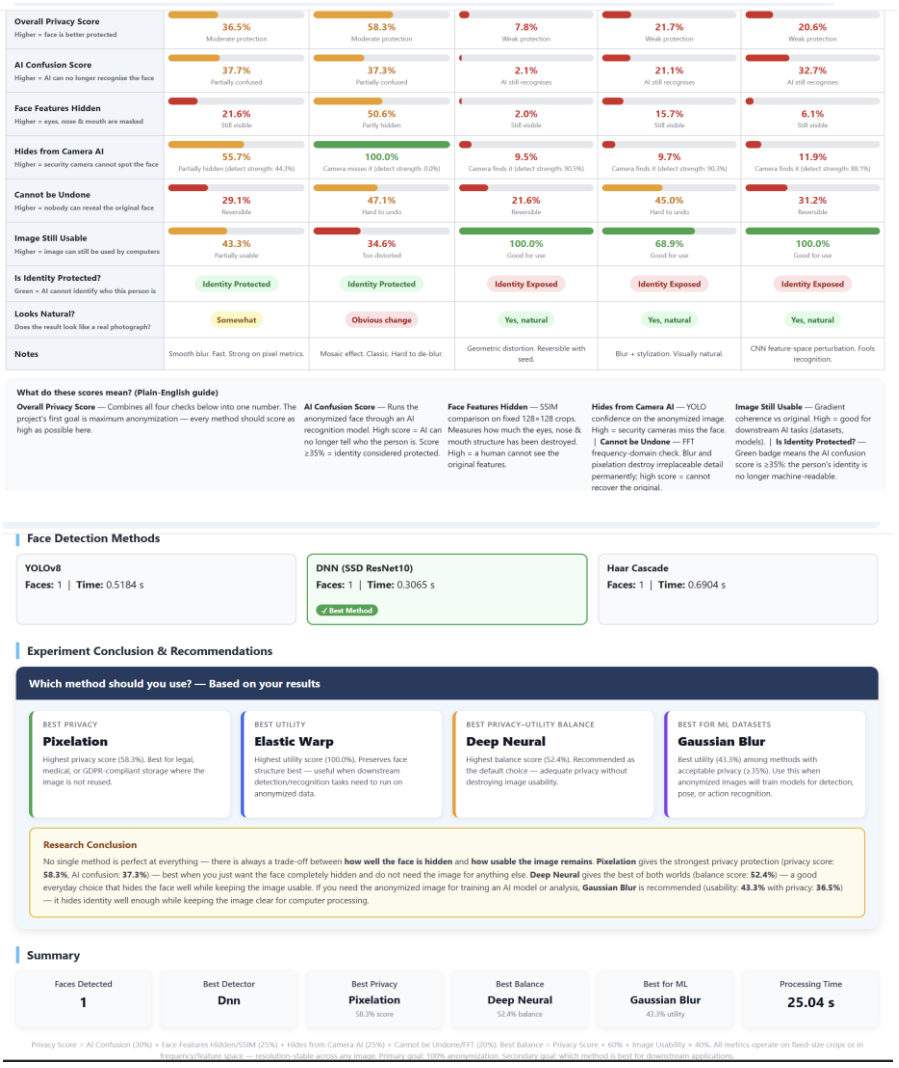


Fig.(g)

Fig. (b) Home page (c) About page (d) User Registration Page (e) User Login Page (f) Browse window(for image upload) (g) Face Anonymization Comparison Results

V. CONCLUSION

This paper presented a Privacy-Preserving Face Detection and Anonymization System that combines face detection techniques with multiple anonymization methods to protect facial identity. The system evaluated traditional and deep learning-based approaches using privacy and image-quality metrics such as Privacy Score, SSIM, and PSNR. Experimental results showed that traditional methods provide stronger privacy protection but reduce image usability, while neural-based methods preserve better image quality with moderate privacy. Overall, adaptive and deep learning-based anonymization achieved the best balance between privacy and utility, making the system suitable for real-world privacy-preserving applications such as surveillance, public monitoring, and AI datasets.

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504270|

REFERENCES

[1] E. Bensaid, M. Neji, H. Chabchoub, K. Ouahada, and A. M. Alimi, "Facial Dataset Anonymization: Striking the Balance Between Privacy and Utility," IEEE Access, vol. 12, pp. 180830–180841, 2024.
[2] S. De Coninck, W.-C. Wang, S. Leroux, and P. Simoens, "Privacy-preserving visual analysis: training video obfuscation models without sensitive labels," Applied Intelligence, vol. 54, pp. 6041–6052, 2024.
[3] S. Sonkar,"Recent Innovations in AI Privacy: Protecting Data in the Age of Machine Learning," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 2, pp. 611–619, 2025.
[4] R. Kaur, S. Rani, S. Jambhorkar, and C. Desai,"Advancing Data Anonymization Techniques for Secure and Privacy-Preserving Data Sharing in the Era of Big Data," International Journal of Engineering and Computer Science, vol. 13, no. 9, pp. 26468–26476, 2024.
[5] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004
[6] M. Chen, M. Eberhardinger, and J. Maucher, "Evaluating the Impact of Data Anonymization on Image Retrieval," IEEE Access, vol. 12, 2024.
[7] E. Ozen, F. Alim, S. B. Okcu, E. Kavakli, and C. Cigla, "Real-Time Face Recognition System at the Edge," 2024.
[8] M. S. Ahmad, M. A. J. Sethi, M. A. Elaffendi, and M. Asim, "Automatic Player Face Detection and Recognition for Players in Cricket Games," 2024.
[9] H. O. Shahreza and S. Marcel, "Knowledge Distillation for Face Recognition Using Synthetic Data With Dynamic Latent Sampling," 2024.
[10] Y. Guo and Z. Liu,"Coverless Steganography for Face Recognition Based on Diffusion Model," 2024.
[11] J. I. Pilataxi, J. P. Perez, and C. A. Perez, "Neuroevolutionary Convolutional Neural Network Design for Low-Resolution Face Recognition," 2025.
[12] J. Xiao, W. Wang, L. Zhang, and H. Liu,"A MobileFaceNet-Based Face Anti-Spoofing Algorithm for Low-Quality Images," 2024.

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