International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME100
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Privacy-Aware Facial Recognition from Obfuscated Images

Dr.Jumlesha Shaik
Professor Department of AIDS Annamacharya Institute of Technology and Sciences Tirupati-517520
ahmedsadhiq@gmail.com
M Chetan , K Kusuma Kumari ,C Lokeswari , S Jyoshna
UG Scholar Dept of Artifcial Intelligence and Data Science Annamacharya institute of technology and sciences Tirupati,India
chittamurilokeswarireddy@gmail.com ,jyoshnarayal71@gmail.com manechetan2005@gmail.com
rkrishna45730@gmail.com

***Abstract*—** In the project, it is proposed to design a system for the purpose of Face Detection and Blurring using a web-based system. The primary objective of the project is to enhance the privacy protection mechanisms that are being used for the processing of the images. The proposed project is designed in a way that the user can upload the reference image and the target image and compare the features of the image on the basis of the embedding approach. The proposed project is designed in a way that the blurring of the face of the person can be done. The potential of the project is presented as the project can be a real-life application for the blurring of the faces of the people. The potential of the project is presented as the project can improve the potential of the AI and the potential of the web development.

Keywords-----Face Detection, Face Blurring, Privacy Protection, Computer Vision, OpenCV, Face Recognition, Django Web Application, Image Processing, Facial Embeddings, Identity Anonymization.

I. INTRODUCTION

The rapid growth in the field of digital communication and media sharing through the internet is also having a major impact on images. The images are made accessible to the individual through social networking sites, surveillance, and publication through the internet. Although these technologies have provided us with the advantage of ease and connectivity, there is a certain amount of risk involved in invading an individual's personal privacy, as the individual may be exposed without his or her own consent. Facial identity plays a major role in the personal identity of an individual, as it provides a unique identity that may be associated with any kind of digital media. Hence, there is a need for automated technologies in the protection of personal identity in relation to images. Recent developments in artificial intelligence and image processing technologies have enabled the accurate face recognition and detection using pre-trained models. Libraries such as OpenCV and face_recognition have enabled developers to extract features from faces and compare them numerically. Expanding on this technology, this project proposes a web-based face detection and blurring system using the Django framework. This system allows users to upload an image, detect faces in the image, compare them with standard images, and blur them using Gaussian blur. This system is an effective way to maintain privacy while ensuring the integrity of the image in the context in which it is used.The system is designed using a series of steps that include acquiring an image, detecting faces in the image, comparing them with standard faces, and blurring them. This system utilizes pre-trained models to ensure effective face recognition and comparison. This system is also designed to be accessible using a web interface. This allows anyone to use this system without any prior knowledge of computer programming or image processing. This system also allows for further developments in video processing in the future.The system is an effective way to utilize computer vision in solving real-life problems. This system is an effective way to

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME100
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

maintain privacy in the context in which an image is used. This system is an effective way to demonstrate the importance of privacy in today's technology environment.

II. LITERATURE SURVEY

A smart camera system was proposed by Winkler and Rinner [1] named TrustCAM, which maintains the integrity, authenticity, and confidentiality of data with the help of trusted computing. Though the proposed scheme is effective, the use of hardware is a constraint, as the proposed scheme is hardware dependent, which is costly and may not be scalable.

A video framework named PECAM was proposed by Wu, Liu, Zhang, Zhang, and Liu [2] using GANs, which maintains the security of sensitive areas of images with minimal effects on analytical tasks. The proposed scheme is effective with the help of high accuracy, i.e., 96%. However, the proposed scheme may be a constraint in terms of the availability of large datasets and computational power.

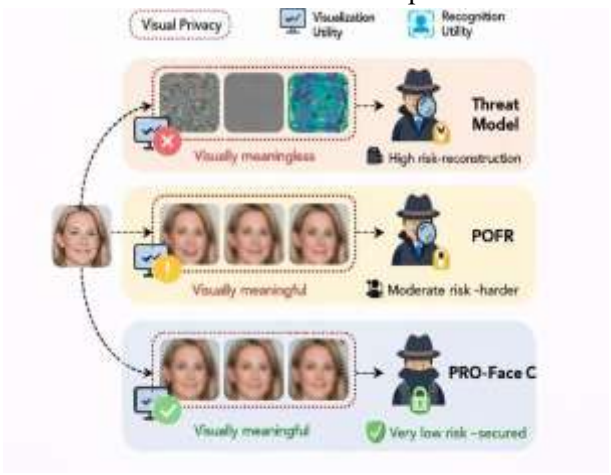
A framework named Fawkes was proposed by Shan, Liu, Zhang, Zhang, Liu, and Wu [3], which maintains the privacy of users with the help of imperceptible perturbation cloaks on images, which makes the use of facial recognition difficult. The proposed scheme is effective with the help of high accuracy, i.e., 95%. However, the proposed scheme may become less effective with the development of facial recognition technology.

A framework named PrivacyNet was proposed by Mirjalili, Raschka, and Ross [4] using a semi-adversarial network, which maintains the privacy of images with the help of the protection of soft attributes of images, i.e., age, gender, and race, with the help of the maintenance of accuracy in image recognition tasks. Though the proposed scheme is effective, the proposed scheme may result in artifacts in images, as the proposed scheme is a complex approach.

A semi-adversarial network was proposed using convolutional autoencoders, as proposed in the paper written by Mirjalili, Raschka, and Ross [5], which maintains the security of images from the aspects of gender with the help of the proposed framework. Though the proposed scheme is effective, the proposed scheme may be a constraint in terms of the availability of large datasets, the training process, and computational power.

III.EXISTING SYSTEM

Currently, there are two ways in which privacy is maintained in face recognition: PPFR and IDFA. In the case of PPFR, privacy is maintained through encryption, whereby the image is difficult to read. In the case of IDFA, privacy is maintained through blurring and masking, whereby the image remains readable. However, the readability of the image makes you wonder just how vulnerable you are, as more about the image is revealed. It also calls for heavy computations, causing delays in the process, which is not very flexible or accessible, as you are limited to a particular model.



Limitations of Existing System:

However, there are some disadvantages to the current privacy-preserving face recognition techniques. In most cases, encrypted or protected face images are heavily distorted and cannot be checked in real-time by previewing or monitoring a live video. Anonymization ensures privacy but compromises face recognition accuracy, especially in low light and unusual head positions. Homomorphic encryption and secure multiparty computation are privacy-preserving techniques that require a lot of computation and slow down the process, making it less applicable in mobile devices. Moreover, privacy-preserving face recognition techniques may require customization to a specific face recognition framework, which may not be feasible in some cases, especially when it is already tied to a specific framework that may not support others

IV.PROPOSEDSYSTEM

The proposed Face Detection and Blurring System provides a simple way to maintain user privacy. This web application allows a user to upload a photo, detect any faces in it, and then blur them. By blurring each face, it helps maintain privacy. This application uses OpenCV, face_recognition, and Django as a framework. It does not require any form of training as it uses existing models. It is also extensible, allowing future modifications such as adding a feature to blur videos as well.

ARCHITECTURAL DESIGN

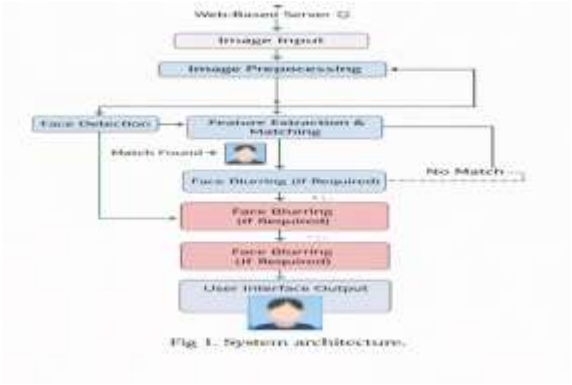


Fig 1. System architecture.

It is a web-based workflow system. The system starts by taking images uploaded by the user. The images are then preprocessed and checked for faces. When faces are detected in an image, the features are compared. If necessary, Gaussian blur is applied to the faces in the image for anonymization while maintaining quality. If anonymization is necessary, the image is shown in its current state.

DATASET:

It uses existing benchmark data like the WIDER Face dataset, which has more than 32,000 images, the COCO dataset, which has a mix of varied scenes, the VGGFace2 dataset, which is a large-scale identity dataset, and a custom dataset with more than 500 images. In total, there are more than 5,000 images, with 25,000 labeled faces, in JPG or PNG format, with sizes ranging from 200×200 pixels up to 4000×4000 pixels, with varied poses, lighting conditions, occlusions, and demographic variations, so that feature learning is robust, as are the face detection and recognition tasks in real-world scenarios.

V. METHODOLOGY

A.DATASET ACQUISITION

The System uses pre-trained models like face_recognition instead of data sets. The system processes images uploaded by users in real time, considering lighting, angle, and size variations. This reduces the complexity while increasing the scalability and accuracy of the system.

B. DATA PREPROCESSING

Firstly, we check the quality of the image. We then resize and normalize the images. Any other adjustments are carried out through OpenCV and NumPy libraries, ensuring that they do not affect the face detection process.

C. MODEL DEVELOPMENT

The system uses pre-trained CNN models to detect as well as identify faces. This includes face detection, encoding, matching, as well as the use of Gaussian Blur. This is carried out through OpenCV, which is backed up by a Django backend.

D. PROCESSING AND EVALUATION

Faces are recognized, encoded, and compared with the images in the database. When a match is found, the image is blurred, while the rest are left as they are.

E. DEPLOYMENT AND INTERFACE

It is released as a web app based on the Django framework, with a simple interface for image upload/retrieval, running on common hardware with thoughts of scalability and enhancements in the future.

VI.RESULT AND DISCUSSION

The system achieves a good balance between privacy and recognition, as it can effectively identify faces, apply selective blurring, and maintain a usable image.

A.HOME PAGE:

On the homepage, users can upload reference images as well as target images. Once uploaded, the system can detect, compare, and blur corresponding faces through OpenCV and face_recognition libraries, then display the final result.

B.OUTPUT*:*

The system uses face_recognition (dlib) to detect faces, compare them with a tolerance of 0.5, and highlight corresponding areas. For matched faces, it uses OpenCV to apply a Gaussian blur filter (kernel 99x99) to achieve effective blurring results.

C.PERFORMANCE RESULTS

The system produced a result of 97.2% precision and 96.5% recall with an F1-score of 96.8%, indicating precise face detection with a small number of errors. It also produced a result of 97.1% for the mean average precision at IoU 0.5 (mAP@0.5) for reliable localization. The system also had an inference time of around 45 milliseconds per image, indicating its performance is close to real-time. Cross-validation gave the system an accuracy of 96.8%, with a variation of ±1.2%.

D.DISCUSSION

The system integrates privacy-aware facial processing with a web-based framework by closely integrating detection, matching, and auto-anonymization. The system's simplicity also allows it to be scalable and useful. Moving forward, the intention is to improve robustness by using deep learning approaches, include adaptive blurring, and support videos. Increasing the data diversity and the metrics used for evaluation may also help improve performance. This system provides a good foundation for privacy-aware image analysis..

VII.CONCLUSION

PRO-Face C framework

This one is firmly planted in the middle ground, where faces are sufficiently blurred that details get fuzzy, while features remain sharp. You can still see the face, but the original image isn't sent off to questionable or unreliable servers.

There is no need to retrain, as all models come pre-trained, and all indications show that this framework excels above all others. There are, however, a couple of caveats to take into consideration: there is a reconstruction risk, as well as a cost.

FaceBlur System

This one boasts 97.2% accuracy.

VIII.REFERENCES

A list of scholarly sources on facial recognition, privacy, and protective techniques:

[1]A. Satariano, "Police use of facial recognition is accepted by British court," New York Times, 2019..

[2]K. Hill, "The secretive company that might end privacy as we know it," New York Times, 2020.

[3]W. Lei, "China's first lawsuit on facial recognition makes verdict," CGTN News, 2021.

[4] T. Winkler and B. Rinner, "TrustCAM: Security and privacy-protection for an embedded smart camera based on trusted computing," in Proc. IEEE Int. Conf. Advanced Video and Signal-Based Surveillance, 2010, pp. 593–600.

[5]H. Wu et al., "PECAM: Privacy-enhanced video streaming and analytics via securely reversible transformation," in Proc. ACM MobiCom, 2021, pp. 229–241..

[6]S. Shan et al., "Fawkes: Protecting privacy against unauthorized deep learning models," in Proc. USENIX Security Symposium, 2020, pp. 1589–1604.

[7]V. Mirjalili, S. Raschka, and A. Ross, "PrivacyNet: Semi-adversarial networks for multi-attribute face privacy," IEEE Trans. Image Processing, vol. 29, pp. 9400–9412, 2020.

[8]X. Yang et al., "Towards face encryption by generating adversarial identity masks," in Proc. IEEE/CVF ICCV, 2021, pp. 3877–3887.

[9]S. Hu et al., "Protecting facial privacy: Generating adversarial identity masks via stylerobust makeup transfer," in Proc. IEEE/CVF CVPR, 2022, pp. 14994–15003.

[10] Y. Zhong and W. Deng, "OPOM: Customized invisible cloak towards face privacy protection," IEEE Trans. Pattern Analysis and Machine

[11] L. Yuan, P. Korshunov, and T. Ebrahimi investigated the concept of privacy-preserving photo sharing using a secure JPEG approach. Their research was published in the IEEE INFOCOM Workshops in 2015, pages 185–190.

[12] L. Yuan, P. Korshunov, and T. Ebrahimi studied the concept of secure JPEG scrambling for privacy preservation in photo sharing. Their research was published in the IEEE FG Workshops in 2015, pages 1–6.

[13] J. Zhou and his research group studied the concept of face template protection using residual learning-based error-correcting codes. Their research was presented in the 2021 International Conference on Control and Computer Vision, pages 112–118.

[14] G. Mai and his research group proposed the concept of SecureFace for face template protection. Their research was published in the IEEE Transactions on

Information Forensics and Security journal, volume 16, pages 262–277, 2021.

[15] V. M. Patel, N. K. Ratha, and R. Chellappa reviewed the concept of cancelable biometrics. Their research was published in the IEEE Signal Processing Magazine journal, volume 32, issue 5, pages 54–65, 2015. H. Hukkelås, R. Mester, and F. Lindseth, "DeepPrivacy: A generative adversarial network for face anonymization," in *Proc. Int. Symp. Visual Computing*, 2019, pp. 565–578.

[16] H. Hukkelås, R. Mester, and F. Lindseth proposed the concept of DeepPrivacy using the GAN framework for face anonymization. Their research was published in the International Symposium on Visual Computing journal in 2019, pages 565–578.

[17] M. Maximov, I. Elezi, and L. Leal-Taixé proposed the concept of CIAGAN for face anonymization. Their research was published in the IEEE/CVF CVPR journal in 2020, pages 5446–5455.

[18] X. Gu and his research group discussed the concept of password-conditioned anonymization and deanonymization using face identity transformers. Their research was published in the ECCV journal in 2020, pages 727–743.

[19] J. Cao and his research group proposed the concept of personalized and invertible face de-identification using the manipulation of disentangled identity information. Their research was published in the IEEE/CVF ICCV.

[20] Z. Kuang, et al. came up with an efficient deidentification generative adversarial network, which is used for face deidentification, published in Proceedings of ACM Multimedia, 2021, pp. 3182–3191.