R.A. Jamadar, 2023, 11:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Face Anonymization Using Haar Cascade

Prof. R.A. Jamadar, Om Garje, Gourav Reshi, Ritik Bhat, Shreyash Ware
Department of IT,
All India Shri Shivaji Memorial Society's,
Institue of Information Technology
Pune, India
riyaz.jamadar@aissmsioit.org, omgarje35@gmail.com, gouravreshi09@gmail.com, ritikbhat2@gmail.com, captainjacky3@gmail.com

Abstract- After gaining knowledge of several computer vision concepts and creating our own facial detection algorithms, we were captivated by the concept of face anonymization and the ability to conceal an individual's identity. We decided to focus our project on face obfuscation, which involves making something obscure and unclear. To achieve this, we developed an algorithm that blurs out faces and places a colored bar over the eyes to anonymize individuals. Our model can balance recognition utility and appearance anonymization by modifying various facial attributes based on practical demands, producing diverse results.

Keywords- Obfuscation, Face anonymization, Facial detection.

I. INTRODUCTION

Computer Vision is a challenging and fascinating task in Artificial Intelligence. It serves as a bridge between computer software and the visuals that we encounter in our environment, enabling the software to understand and learn about the visuals.

For instance, determining a fruit based on its color, shape, and size. This may be a simple task for the human brain, but in the Computer Vision pipeline, it involves data collection, processing, and training the model to differentiate between fruits based on their characteristics. The goal is to identify and comprehend images and provide new images that are useful in various fields.

Face detection is a form of computer vision that aids in detecting and visualizing facial features in pictures or videos. This type of object detection technique detects instances of semantic artifacts of a given class (such as people, cars, and houses) in digital pictures and videos. With technology advancement, face recognition has become increasingly important in areas such as photography, defense, and marketing.

However, the mass availability of monitoring devices has recorded an enormous amount of facial image data, which has raised privacy concerns as AI-based computer vision technologies are used to mine personal information at a large scale. To avoid the abuse of privacy data, some restrictive laws and regulations, e.g., the General Data Protection Regulations (GDPR), require consent from individuals for the use of their personal data. However, facial image data leakage occurs frequently worldwide. Moreover, users' facial images stored in databases, even if not exposed, are still vulnerable to third-party users or applications.

Hence, face anonymization has become a crucial step for many facial applications. Face de-identification aims to preserve facial attributes like gender, age, and race while de-identifying face images, which have evolved over time.

II. RELATED WORK

Earlier face de-identification works relied mainly on naive transformation methods. These approaches are commonly used in everyday life, such as obfuscating facial sensitive parts through masking, pixelization, blurring, and other methods. However, these simple and direct occlusion methods seriously affect data availability. Moreover, these methods have been proven to be ineffective with deep learning-based face recognition. Another commonly used method is the k-same algorithm based on exploiting the average face of k-closest faces to replace the given face, resulting in face recognition accuracy less than

International Journal of Science, Engineering and Technology

An Open Access Journal

1/k. To improve data utility and average face naturalness, several variants have been proposed. More recently, new techniques and mechanisms have been applied to enhance facial privacy, such as adding adversarial perturbations to implement de-identification.

GANs have inspired a new vein of face de-identification techniques, which can be divided into two categories: those that adopt the conditional in painting-based technique and those that manipulate facial representations. Deep Privacy uses a GAN-based head in painting technique to generate obscured faces while removing privacy-sensitive information from the original face.

Sun et al. extract attribute features from the input face and then generate anonymous faces. Gafni et al. generate high-level representations from face images that minimize identity associations while keeping the perceptions unchanged. CIAGAN leverages a vector to control the fake identity of the generated images. Identity DP combines differential privacy mechanisms with deep neural networks to achieve adjustable privacy control.

III. SYSTEM ARCHITECTURE

1. Haar Cascade:

Haar Cascade is an effective method for detecting objects. It's a machine-learning-based method in which a cascade of actions is learned from many positive and negative images. It becomes used to seeing things in different frames. Fig. shows the Haar cascade classifier.

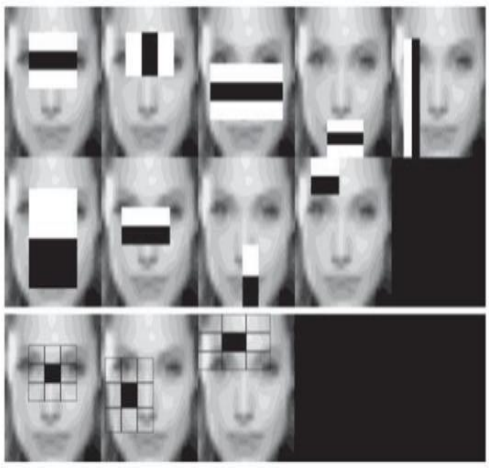

Fig 1. View of Haar Cascade Classifier.

2. Live Feed Blur Architecture:

After successfully loading cascade file for face detection, we then access the camera to capture the live the feed. Once the live feed has been captured then we detect faces. We then take the coordinates (x,y,h,w) from the live feed, then we apply blurring algorithm using starting point as x-coordinate and ending point as y-coordinate. Then we display the blurred frames in a window.

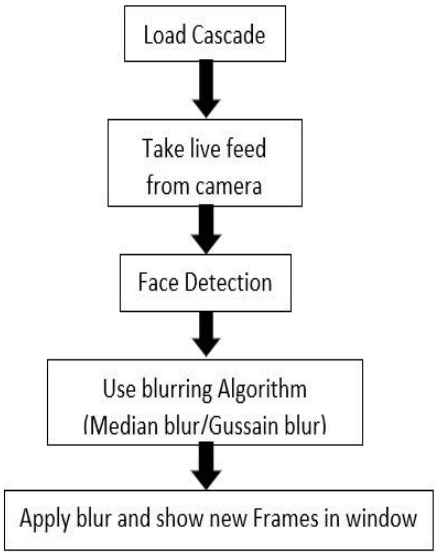

Fig 2. Live Feed Blur.

IV. LITERATURE REVIEW

Tomoya Muraki, Shintaro Oishi, MasatsuguIchino, Isao Echizen, Hiroshi Yoshiura. "Anonymizing Face Images by Using Similarity Based Metric" [1] A similarity-based method for face anonymization that has provable security and trade-off controllability in the situation. Only uses grey-scale images. Uses only 68 points on the face contour and various parts of the face (e.g., eyebrows, eyes, nose, and mouth) as face image feature points.

Jingzhi Li1, Lutong Han, Ruoyu Chen, Hua Zhang, Bing Han, Lili Wang, Xiaochun Cao. "Identity Preserving Face Anonymization via Adaptively Facial Attributes Obfuscation" [2] The method can adaptively discover the identity-independent visual attributes, and then conditioned on these visual attributes the privacy preserving face is generated. Uses Identity-aware activation heat maps to localize the identity-related facial parts. Uses the face parser to divide the face image into five parts and select the corresponding facial attributes.

International Journal of Science, Engineering and Technology

An Open Access Journal

Ramadan TH. Hasan, Amira Bibo Sallow. "Face Detection and Recognition Using OpenCV" [3] It only detects the face and objects in the image. It does not modify or blur the face.

Erich-Matthew Pulfer "Different Approaches to Blurring Digital Images and Their Effect on Facial Detection" [4] Analyzing the usage of multiple images blurring techniques and determining their effectiveness in combating facial detection algorithms. Does not change facial Attributes detecting facial landmark.

V. CONCLUSION

Our team has developed a unique framework to safeguard the privacy of face images within monitoring systems. Our approach involves a new face anonymization model that blends the strong generative abilities of stargan with exceptional facial attribute indicators we discovered. We have proven that our model can produce a broad range of facial appearance variations while preserving identity.

Through our experiments, we have verified that our method maintains the recognition accuracy of different face recognition systems and effectively anonymizes facial features. Our model also offers precise edit controls, allowing users to specify desired attributes such as a large nose. Moving forward, we aim to investigate the capability of our model to protect other facial attributes like age, race, and emotions.

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to the faculty to allow us to do this wonderful informative project on the topic "Face Anonymization Using Haar Cascade" which also helped us in doing a lot of research and we came to know about so many new things for which I am thankful them.

We would like to extend my sincere thanks to Prof. R.A. Jamadar for their guidance and constant supervision as well as for providing necessary information regarding the project and for their support in completing the project.

REFERENCES

[1] Razvan Viorescu et al. 2018 reform of eu data protection rules.

[2] European Journal of Law and Public Administration, 4(2):27–39, 2017.

[3] Oran Gafni, Lior Wolf, and Yaniv Taigman. Live face de-identification in video. In Proceedings of the IEEE International Conference on Computer Vision, pages 9378–9387, 2019.

[4] HanxiangHao, David Güera, Amy R Reibman, and Edward J Delp. A utility preserving gan for face obscuration. arXiv preprint arXiv:1906.11979, 2019.

[5] Tao Li and Lei Lin. Anonymousnet: Natural face de-identification with measurable privacy. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2019.

[6] XiuyeGu, Weixin Luo, Michael S Ryoo, and Yong Jae Lee. Passwordconditioned anonymization and deanonymization with face identity transformers. In European Conference on Computer Vision, pages 727–743, 2020.

[7] Zhenyu Wu, Haotao Wang, Zhaowen Wang, HailinJin, and Zhangyang Wang. Privacy-preserving deep action recognition: An adversarial learning framework and a new dataset. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020.

[8] Maxim Maximov, Ismail Elezi, and Laura Leal-Taixé. Ciagan: Conditional identity anonymization generative adversarial networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 5447– 5456, 2020.