Face Anonymization Using Haar Cascade

***Abstract*—** After being introduced to many computer vision concepts and designing our own facial detection algorithms, we were intrigued with the idea of face anonymization and being able to conceal your identity. So, we decided to do our project on face obfuscation. Obfuscation is the action of making something obscure and unclear. So, we have implemented an algorithm to blur out faces and place a colored bar over the eyes to anonymize an individual. Our model can achieve a balance between recognition utility and appearance anonymizing by modifying different numbers of facial attributes according to practical demands and provide a variety of results.

***Keywords*—** Obfuscation, Face anonymization, Facial detection.

I. INTRODUCTION

Computer Vision is one of the most fascinating and challenging tasks in the field of Artificial Intelligence. Computer Vision serves as a link between computer software and the visuals we see around us. It enables computer software to comprehend and learn about the visuals in its environment. As an example: The fruit is determined by its color, shape, and size. This job may seem simple for the human brain, but in the Computer Vision pipeline, we first collect data, then conduct data processing operations, and then train and educate the model to learn how to differentiate between fruits based on size, shape, and color. The main goal is to identify and comprehend the images and offer new images that are more useful for us in different life fields. Face detection is a form of computer vision that aids in detecting and visualizing facial features in captured pictures or real-time 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. Face recognition has become increasingly important as technology has advanced, especially in fields such as photography, defense, and marketing. The mass availability of monitoring devices has recorded an amount of facial image data, and many AI-based computer vision technologies are used to mine personal information at a large scale. Thus, privacy concerns are growing as the tremendous progress on computer vision technologies. To avoid the abuse of privacy data, some restrictive laws, and regulations, e.g., the General Data Protection Regulations (GDPR), require the consent from the individual for any use of their personal data. However, the leakage of facial image data is occurring frequently in the world. Moreover, user's facial images stored in the database, even if they are not exposed, are still vulnerable to third-party users or applications. Therefore, face anonymization has become one of the critical steps for many facial applications.

II. RELATED WORK

Face de-identification focuses on preserving facial attributes like gender, age, and race while deidentifying face images, which have evolved over time. Earlier works on face de-identification are mainly naive transformation based. These approaches are the most used in our daily life, and they obfuscate facial sensitive parts through masking, pixelization, blurring and other methods. However, these simple and direct occlusion methods seriously harm the data's availability. What was worse, these methods have been shown to be ineffective with deep learning-based face recognition. Another representative method is the k-same algorithm based. These algorithms exploit the average face of k-closet faces to replace the given face, which make the face recognition accuracy less than 1/k. Many variants were proposed to improve the data utility and the naturalness of average face. More recently, new techniques and mechanisms have been applied to enhance face privacy. Some researchers implement de-identification by adding adversarial perturbations. GANs inspire a new vein of face de-identification techniques. They can be divided into two categories: those that adopt the conditional inpainting-based technique, and those that manipulate facial representations. Deep Privacy uses GAN-based head inpainting technique to generate obscured faces, ensuring privacy-sensitive information is thoroughly removed from the original face. Sun et al. extracts attributes features from the input face, and then generates anonymous faces. Gafni et al. generate high-level representations from face images that minimize identity associations, while keeping the perceptions (pose, illumination, and expression) unchanged. CIAGAN leverages a vector to control the fake identity of the generated images. IdentityDP combines differential privacy mechanisms with deep neural networks to achieve adjustable privacy control. Specifically, for the identity representation the differential privacy perturbation is added, whereas for the attribute representation is unchanged.

III. SYSTEM ARCHITECTURE

· *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.

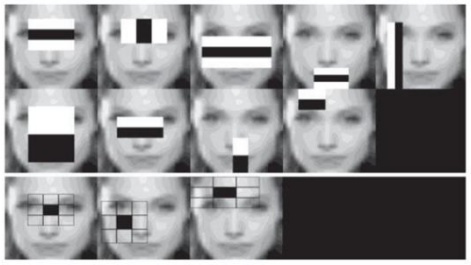

Fig. 1: View of Haar Cascade Classifier

· ***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.

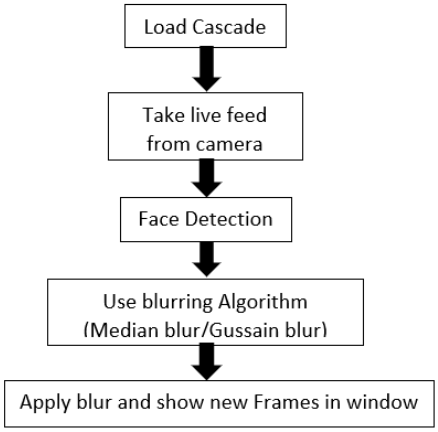

Fig.2: Live Feed Blur

IV. Literature Review

(1). *Tomoya Muraki, Shintaro Oishi, Masatsugu Ichino, Isao Echizen, Hiroshi Yoshiura.*

"Anonymizing Face Images by Using SimilarityBased 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, mouth) as face image feature points.

(2). 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 heatmaps 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.

(3). *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.

(4). *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 combatting facial detection algorithms. Does not change facial Attributes detecting facial landmark.

V. Conclusion

We develop a novel framework for protecting the privacy of face images in monitoring system. We introduce a novel face anonymization model, which combines the strong generative powers of stargan with the discovered extraordinary facial attribute indicators. We have shown that our model can generate wide appearance variations of face images with identity-preserving. experimental results demonstrate that our method can preserve the recognition utility for distinct face recognizers, and effectively anonymize the facial appearance. We have also demonstrated that our method provides fine- grained edit controls, such as specifying a desired attribute e.g., big nose. In the future, we will explore our model's ability to protect other facial attributes, e.g., race, age, emotion, etc.

VI. 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.

VII. References

[1] Razvan Viorescu et al. 2018 reform of eu data protection rules. European Journal of Law and Public Administration, 4(2):27–39, 2017.

[2] 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.

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

[4] 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.

[5] Xiuye Gu, 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.

[6] Zhenyu Wu, Haotao Wang, Zhaowen Wang, Hailin Jin, 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.

[7] 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.