CS/RBE 549 Computer Vision, Fall 2021
Project Report
Team [REDACTED]

Member	Signature	Contribution (%)
Vedhas Vinjamuri		33
Shreyansh Goyal		34
Monika Sri Vyshnavi Nagalla	N.M.S.Vyshnavi	33

Grading:	Approach	_____/15
	Justification	_____/5
	Analysis	_____/15
	Testing & Examples	_____/15
	Documentation	_____/10
	Difficulty	_____/10
	Professionalism	_____/10
	Presentation	_____/20
	Total	_____/100

Table of contents

Table of figures

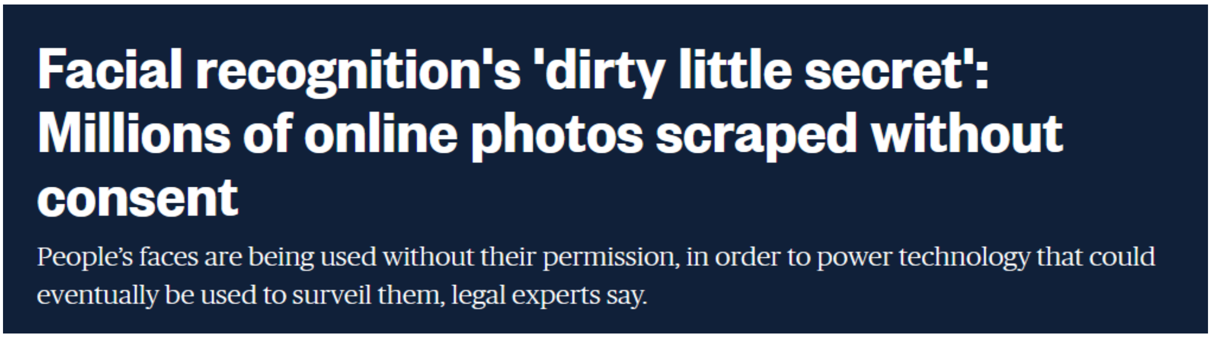
Abstract

In today’s technological world, where we have search engines like Clearview just for facial recognition, it is important to restrict the accessibility to our faces and ensure the fundamental right to privacy. This project is to work towards the anonymization of the faces present in any live feed, captured videos, and photos. This was achieved by first detecting the faces using the Haar Cascade algorithm and then turning the detected faces into a small block for the data to be lost permanently and finally resizing it. Face Detection using Haar feature-based cascade classifiers is an effective detection method used even today in various places. The anonymization process is invariant to the movements and therefore, can keep the face anonymous if it is in the frame.

The project presents a good scope in the future where this can be used as a built-in camera feature. This will come in handy for investigative journalists and protect the identities of the witnesses and victims of crime. This can also help people to ensure they are not constantly surveyed without any warrant by the law enforcement agencies.

Introduction

Our faces have never been more vulnerable. Facial recognition algorithms have made it easy to identify individuals from a single snap, a fact that's particularly relevant with the victims, witnesses, and protestors. As the technology advances, real-time facial recognition which involves the constant scanning of live video feeds to match moving faces with a database of still images is starting to spread. Police in China are reportedly using it to pick suspects out of crowds, and retailers there are using it to identify customers and their buying preferences. U.S. security agencies are testing the technology in some airports and border crossings. And now systems are being designed for use by local police. China has gone further than any society to expand facial recognition, using it to create a national surveillance state in which the technology is used to shame jaywalkers and find criminal suspects in the crowds of sporting events. The algorithms must be fed hundreds of thousands of images of a diverse array of faces. Increasingly, those photos are coming from the internet, where they're swept up by the millions without the knowledge of the people who posted them, categorized by age, gender, skin tone, and dozens of other metrics, and shared with researchers at universities and companies.

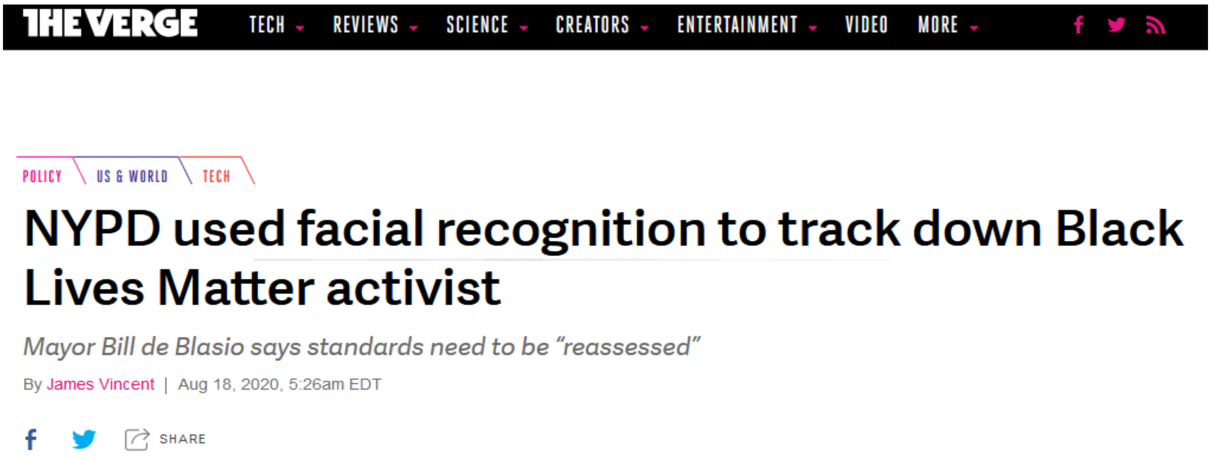


Facial recognition's 'dirty little secret': Millions of online photos scraped without consent

People's faces are being used without their permission, in order to power technology that could eventually be used to surveil them, legal experts say.

Figure 1 Legal experts have been long worried about the photos which end up in the database without consent of the people

Despite "real-time" facial recognition's dazzling potential for crime prevention, it is also raising alarms of the risks of mistakes and abuse especially in countries with authoritarian governments. There isn't anyone to oversee the misuse of technology even in democratic nations. There have already been multiple reports of the technology being used by the police departments in various states in the US. Protestors have been arrested using the facial recognition methods on the videos and pictures of the event posted on the internet or being shown on the news.



NYPD used facial recognition to track down Black Lives Matter activist

Mayor Bill de Blasio says standards need to be "reassessed"

By James Vincent | Aug 18, 2020, 5:26am EDT

Figure 2 : NYPD Used Facial recognition to track down Black Lives Matter Activist: The Verge

Therefore, with these technological advancements, we also need to ensure that the individual's right to privacy is ensured. As facial recognition technology becomes more sophisticated, it can be one of the gravest privacy threats of our time. It has the potential to remove the anonymity we expect in crowds and most public places. Unrestricted use of new surveillance technologies can shift the constitutional implications of the right to privacy.

With these implications in mind, we started to work on ways to anonymize any face which appears in live or captured video and photos. For that, our first goal was to detect the faces which appear in the frame using a face-detection algorithm and then work on how we can anonymize the faces for the data to be lost permanently to protect the identities of the individuals.

Related Work

To achieve the task of face detection and to successfully implement it with the knowledge of the feature extraction learned in the class we choose to use Haar features. A classifier based on Haar features and attention cascade with Adaboost is the first-ever classifier to detect faces. The Haar features are sensitive to change in the contrast values between adjacent rectangular groups of pixels. Hence, they are good at detecting the lines and edges. The figure depicts the original Haar features used in the original paper by Viola Jones. Using the below features we could detect facial structures like eyes, eyebrows, lips.

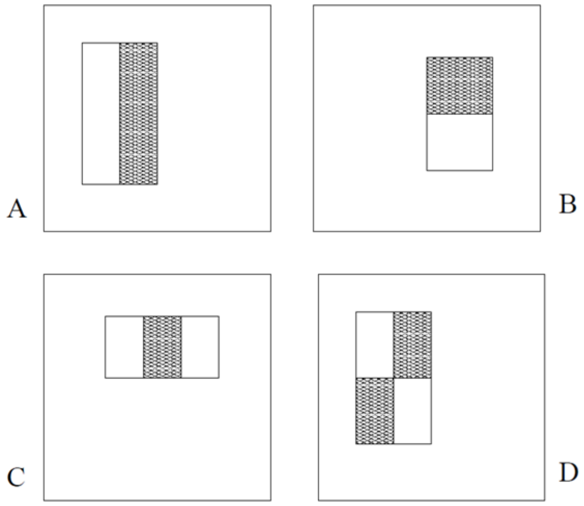


Figure 3: Haar features (rectangle features) defined in the research paper by Viola and Jones[1]

Figure 4 describes how a line rectangle feature can detect the eye which has a top area darker than the underneath. We could observe that even though the image is slightly blurred the line feature is able to detect the eye. As a later stage out of all the features detected over a training image, we need to select the best features that describe a face. For this purpose, a boosting technique called Adaboost is used to separate the weak learners. It is to be remembered that the dataset contains both positive images i.e., the images containing the faces, and the negative images without any faces. Similarly, using the above Haar features we could detect structures like lips, eyes, and eyebrows as shown in figure 5.

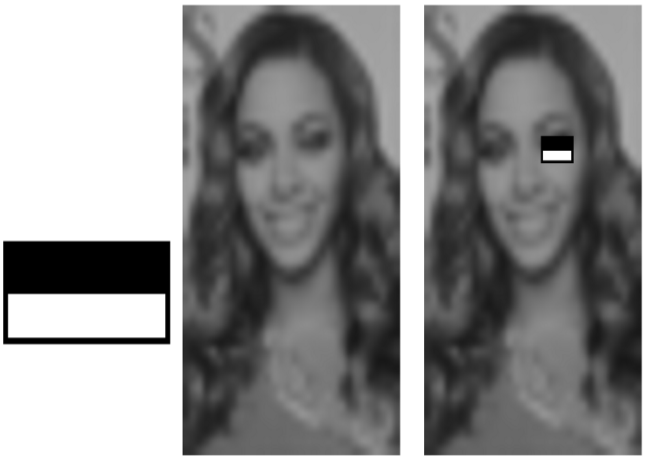


Figure 4: Using the Haar line feature, the eye in the picture of Beyoncé is detected.

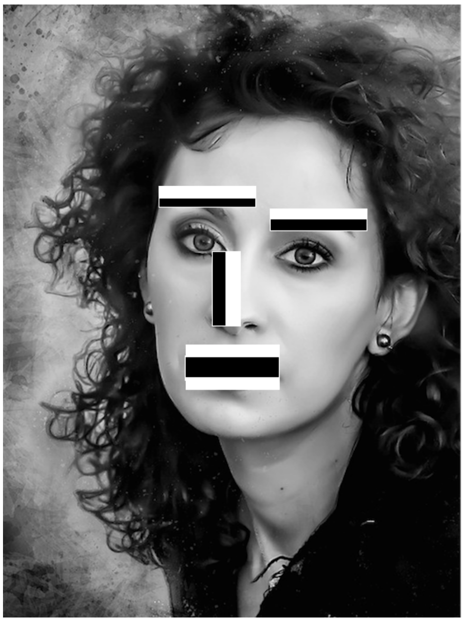


Figure 5: Facial structures detected in the image by Haar features.

After applying Adaboost the feature set would drastically be reduced from 180,000 to 6000. These 6000 features [1] are to be passed to each training image over a window size of 24×24 to detect the location of the face. To reduce this complexity an attentional cascade was implemented. The main idea of this cascade is that not all features have to be run over all the 24×24 windows. When a feature fails in a window, it is to be assumed that there are no facial features in that window. Hence, the computation complexity and the time are reduced. With this knowledge on Haar cascade classifiers let us move to the methodology.

Methodology

We begin by accessing the camera live feed using CV2, an OpenCV package for Python. Next, using the Haar feature-based cascade classifier, faces are detected, and bounding boxes are created. The feature sets for the classifier are in the XML format and the window size for the attentional cascade is set as 24x24. The training data consists of both positive and negative images meaning the images that contain the faces and the images without any faces.

After identifying the bounding box, the next task is to blur out the face component of the image, which is within the box. The first option was to use blurring algorithms available in the CV2 module. However, these are easily reversible, since they are based on hard algorithms, and can be brute-forced to reconstruct the faces within. This poses a risk to security and goes against the core aim of the project.

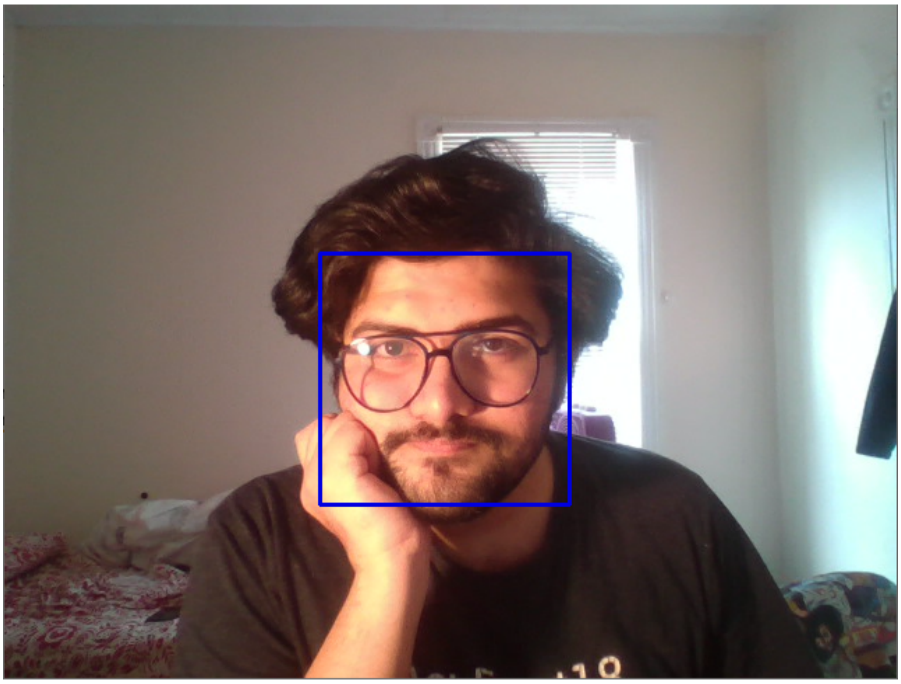


Figure 6: Bounding Boxes using Haar Cascade Classifier.

The best way to truly ensure anonymity is to make sure that the faces within cannot be reconstructed. To do this, one solution is to use a blurring method that loses enough data that reconstruction becomes close to impossible. To ensure sufficient data loss, the section of the image inside the bounding box is transformed into an 8×8 image, and then changed back to its original resolution, and stitched to the original image.
Since the process of reduction to an 8×8 image causes the loss of over 90% of the data in the face structure, when stitched back into the image, this becomes a blur that is barely recognizable and cannot be reconstructed into faces.

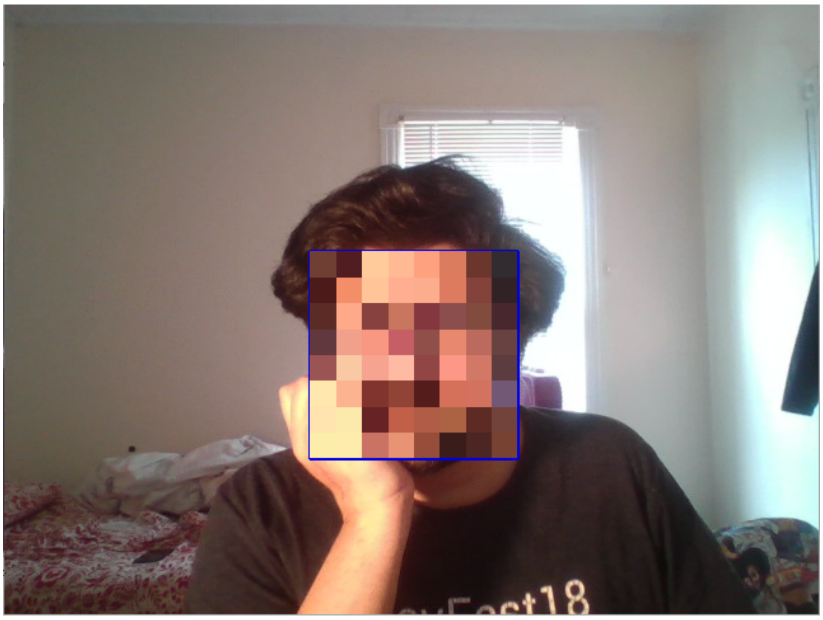


Figure 7: Blurring of a face using the 8×8 method.

This method allows for proper anonymization of faces, with a lower chance of reconstruction. Additionally, it is robust enough to work under various light sources, different-sized faces, and multiple faces in the same frame. By using the Haar Cascade and a manual blurring method, the program becomes a lightweight and compatible solution, with the capability to be deployed easily and deliver accurate results quickly.

Results

A Face Anonymizer is successfully created. It successfully detects the face and anonymizes it with great efficiency. The system is invariant to scale which means even when a face moves near or away from the camera the anonymization process is not hindered. As shown in the figure below, the anonymizer successfully detects the multiple faces which are present on and off the phone screen. This proves the efficiency of the classifier used.

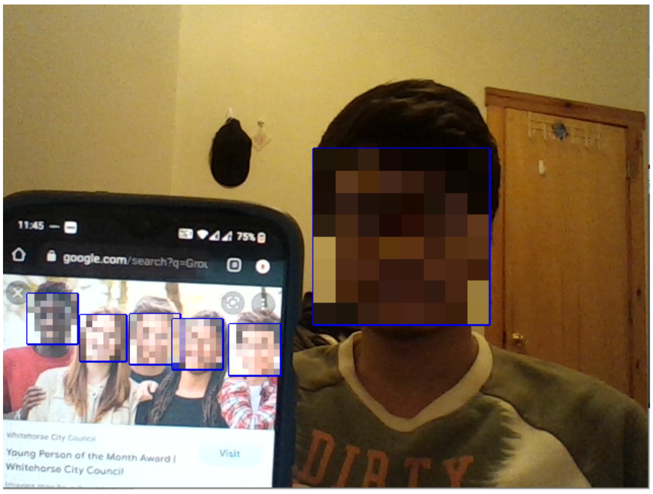


Figure 8: Operation under different lighting, face sizes, and multiple faces simultaneously.

The results are invariant to the lighting situation and works perfectly even in the different backgrounds. The system works with ~90% accuracy, and ensures proper face blurring, with a near-zero chance of reconstruction which was one of our main objectives while starting this project.

The results are disrupted when an individual turns the face sideways which proves that this classifier isn't rotation-invariant. As shown in the figure below, the classifier is unable to anonymize the whole face and sometimes doesn't even detect the face which beats its whole purpose. This is one aspect of our project that we would like to work on in the future.

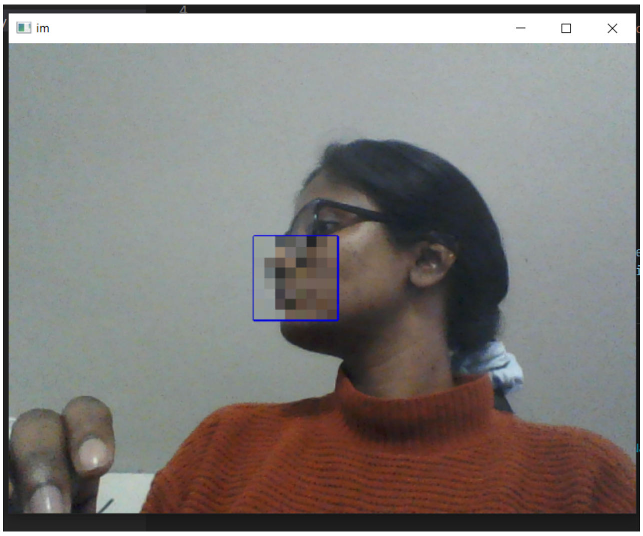


Figure 9: Face when turned sideways from the camera is not fully detected

Conclusion

We started this project with concerns around the privacy of individuals when their photos end up being online and used by facial recognition tools. Our main goal was to create a barrier for recognition by anonymizing these faces present in the frame in such a way that the facial data can’t be retained. We used Haar-Cascade classifiers to detect the faces whose concept was first published in 2001. These classifiers were trained to detect the faces present in the frame. The detected faces were then resized to 8×8 blocks for the data to be lost sufficiently and then resized again. This process allows the data to be lost permanently. The classifier makes the anonymization scale-invariant which will come in handy in real-life applications.

For future work, we would like to make this anonymizer rotation-invariant as well which will make it perfect to use this project as a built-in function in a camera. We used the Haar-Cascade algorithm mainly because it requires less memory (in KB). Other algorithms like YOLO or CNN require larger training datasets than the Haar-Cascade. This will widen the scope of application of this project to places that have less memory available.

Appendix

The languages and libraries used:

- Python
- CV2
- Numpy

The link to the code:

https://github.com/vvedhas/FaceAnonymizer

References

1. Paul Viola & Michael Jones(2001) “Rapid Object Detection using a Boosted Cascade of Simple Features”.
2. Facial recognition's 'dirty little secret': Millions of online photos scraped without consent
3. Cops across the US are using facial recognition tech to arrest protestors
4. Face Detection with Haar Cascade. Exploring a bit older algorithm which… | by Girija Shankar Behera | Towards Data Science
5. Rapid Object Detection using a Boosted Cascade of Simple Features
6. Coding Robin Train Your Own OpenCV Haar Classifier