VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Face Anonymization in Video

Review 3

Submitted by

18BCI0224 - Rajarshi Saha
19BCE0511 - Aradhana Ghosh
20BCT0123 - P. Meghana Srilekha

Group - 4

Course Code: CSE4015
Course Title: Human Computer Interaction

Table of Contents

Acknowledgement

With due regards, we would like to thank our professor, Dr. Joshva Devadas T (School of Computer Science and Engineering) whose immense guidance helped us in completing this project. We wish to express our sincere thanks to the Honourable Chancellor, Dr. G. Viswanathan, and respected Vice-chancellor, Dr. Rambabu Kodali, for providing us the proper ambience to carry out our project work successfully. We would like to express our gratitude and appreciation for our team members, who have collectively contributed their work to help our project reach completion and succeed.

ABSTRACT

The aim of our project is to anonymize faces of humans in a recorded video to preserve the privacy of individuals who appear in videos containing sensitive contexts or wish to conceal their identities before sharing on social media platforms to avoid cyber bullying, cyber stalking and other problems caused by the trend of viral videos in today's social climate. We implement automatic face detection and blurring for processing the video. This project has been developed as a web application currently but we wish to extend it as a web extension for social media applications too in the future.

1. INTRODUCTION

Concerning the protection of observed people's privacy, smart video surveillance implies both risk and chance. The systems' increasing capabilities can be misused if we do not deploy suitable counter-measures. AI Based video surveillance systems are privacy aware and powerful. These systems help operators identify incidents by focusing attention to events detected by intelligent algorithms. Videos are released anonymously to protect privacy. The idea behind smart video surveillance designs is to prevent unjustified intrusions into people's privacy. Situation assessment is meant for what someone is doing and not for who it is. In our project, we investigated various anonymization techniques available in the present day and implemented the best one as a smart surveillance method for videos.

1.1 Face Recognition

Face recognition is a major feature in smart surveillance. This feature helps in protecting the privacy of a person and also in surveillance of a situation. Core challenge of face recognition is to create a robust model that can remove all privacy-sensitive information and also generate a new, realistic face for data visual integrity. Individuals in pictures differ widely in terms of poses, backgrounds and other appearance features. So, the solution should cope with all conditional information accordingly.

1.2 Image Blurring

Image blurring protects the identity of a person on screen and also often helps in preventing companies from misusing the identity of the person for ads without their consent. In blurred images, the part of the image under consideration is "smoothed", which means that edges are not observed in it which makes it difficult to detect the original features in the image. One of the filters used for blurring is low pass filter that allows low frequency to enter and stops high frequency. Here, frequency means the change of pixel value. Around edges, pixel values change rapidly as the blur image is smooth so high frequency should be filtered out.

1.3 Video Processing

Video processing covers most of the image processing methods, but also includes methods where the temporal nature of video data is exploited.

1.4 Image Analysis

Here, the goal is to analyze the image with the purpose of first finding objects of interest and then extracting certain parameters of these objects that we wish to modify.

1.5 Face Detection

Face detection is a computer technology that determines the locations and sizes of human faces in images. It detects facial features and ignores everything else. In detection, the task is to find the locations and sizes of all objects in an image that belong to a given class. Face detection can be regarded as a more general case of face localization. The task is to find the locations and sizes of a known number of faces. One usually does not have this additional information.

Early face-detection algorithms focused on the detection of human faces at the forefront. Newer algorithms attempt to solve the more general and difficult problem of multi-view face detection. That is, the detection of faces that are either rotated along the axis from the face to the observer or rotated along the vertical or left-right axis.

2. REQUIREMENT ANALYSIS

We collected some data through a small-scale survey. The survey questioned the following:

- Do you consider yourself a socially active person?
- Do you use any social media platform?
- Can you name any sensitive/controversial social topic?
- Would you like to raise your voice and give any opinion about it publicly?
- If you have replied with "No" in the previous question, give reasons on why you don't want to speak about the sensitive topic?
- Would you speak about it, if you were anonymous?
- Do you think anonymity would help people be more free/independent?

Some of the noteworthy observations have been provided below:

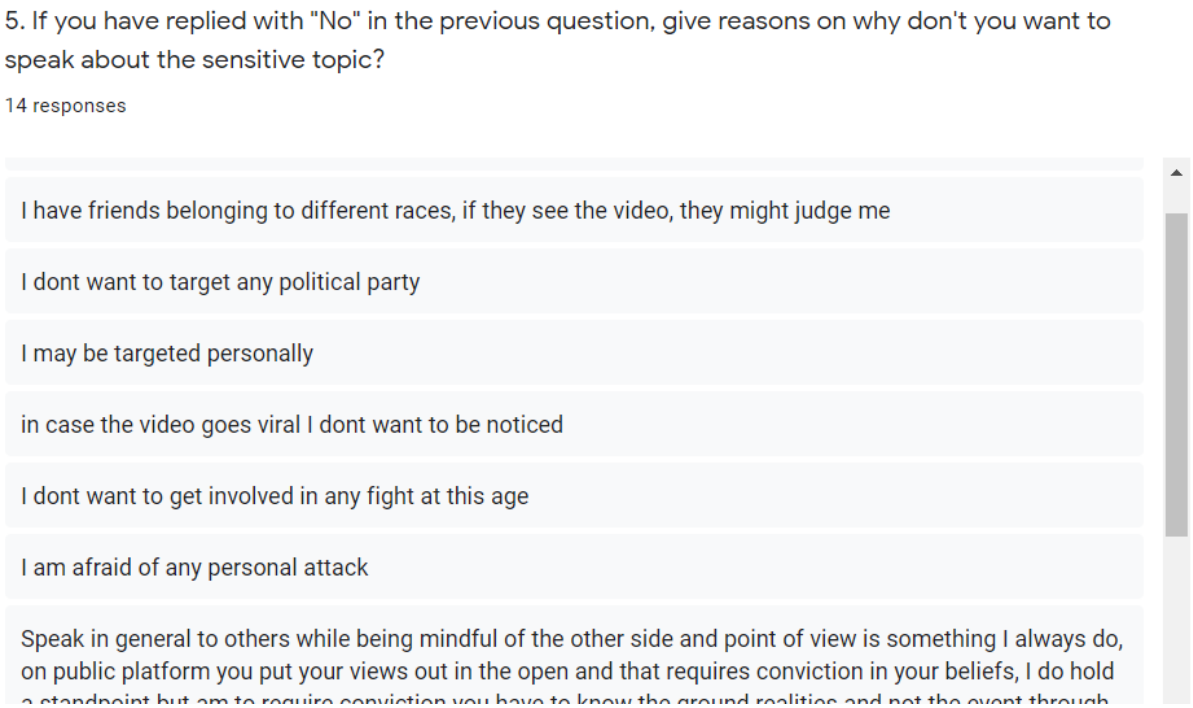

Figure 1. Collected responses to the fifth question in a circulated questionnaire.

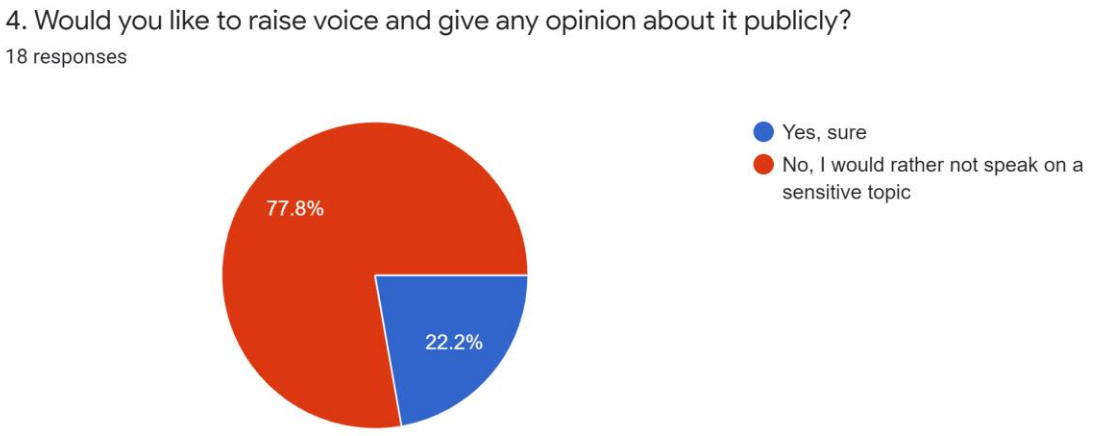

Figure 2. A pie chart analysis of the answers to the fourth question in the circulated questionnaire.

The data we collected through the questionnaire and the poll shows that people are quite wary of discussing a sensitive topic publicly. What we understood by their reasoning is that they are hesitant to reveal their identity publicly, especially when it comes to controversial topics. The observation in Figure 2 shows that about 78% of online social media users restrict their public view because of the fear of getting identified and targeted.

We also observed that around 72% of these hesitant people are using social media (Figure 4) and 85% of them consider themselves to be socially active (Figure 3).

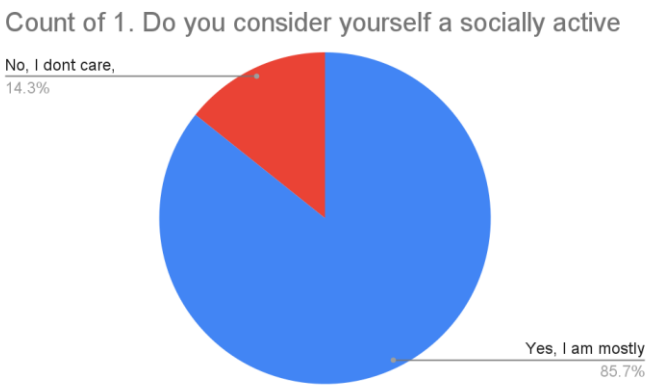

Figure 3. A pie chart analysis of the answers to the first question in the circulated questionnaire.

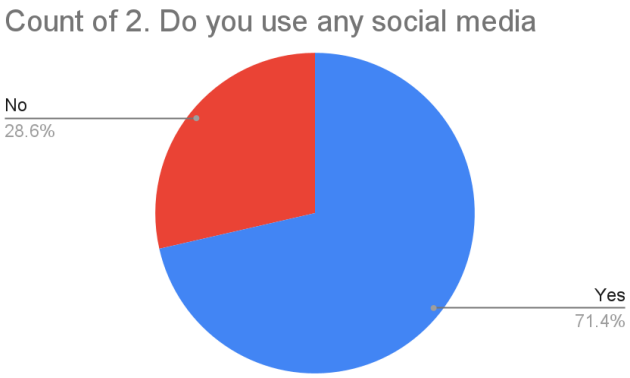

Figure 4. A pie chart analysis of the answers to the second question in the circulated questionnaire.

With this survey, we assume that getting identified for controversial or sensitive topics on the Internet or mass media is an issue. To further confirm our assumption, we conducted one more generalized survey using a poll to investigate whether people feel safe to post their pictures and videos on the Internet.

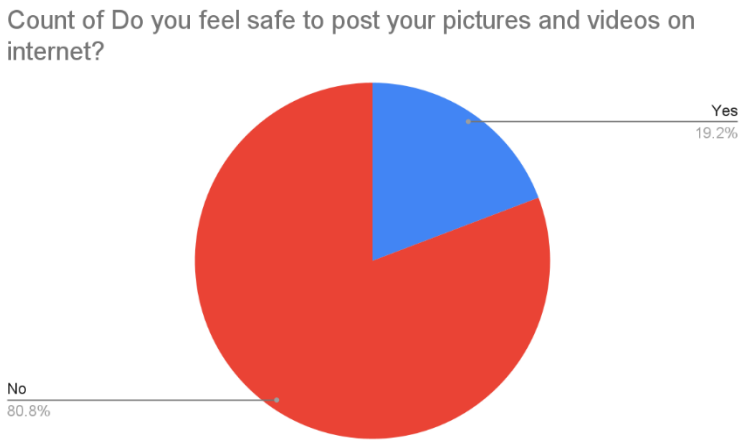

Figure 5. A pie chart analysis of the collected responses to the circulated poll.

The results shown in Figure 5 demonstrate that almost 81% of the surveyed people do not feel safe about posting their personal pictures or videos on the Internet.

After analyzing the collected data, we can safely conclude that getting identified on mass media for controversial or sensitive topics does cause a privacy breach. Hence, we have developed a web application that helps people anonymize their faces in a video, so that they can enjoy their privacy on the Internet without worrying about cyberbullies recognizing them in shared videos.

3. DATA FLOW

The hierarchical task analysis (HTA) for our project has been displayed in Figure 6 below:

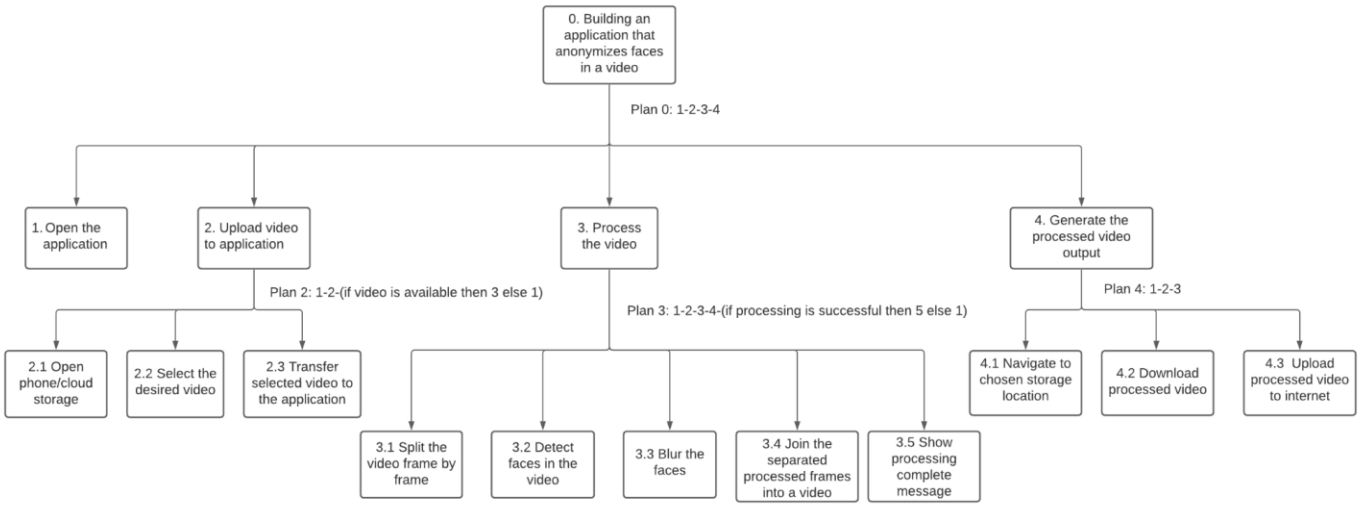

Figure 6. Hierarchical Task Analysis of our video anonymization project.

The Storyboard for our project has been displayed in Figure 7 below:

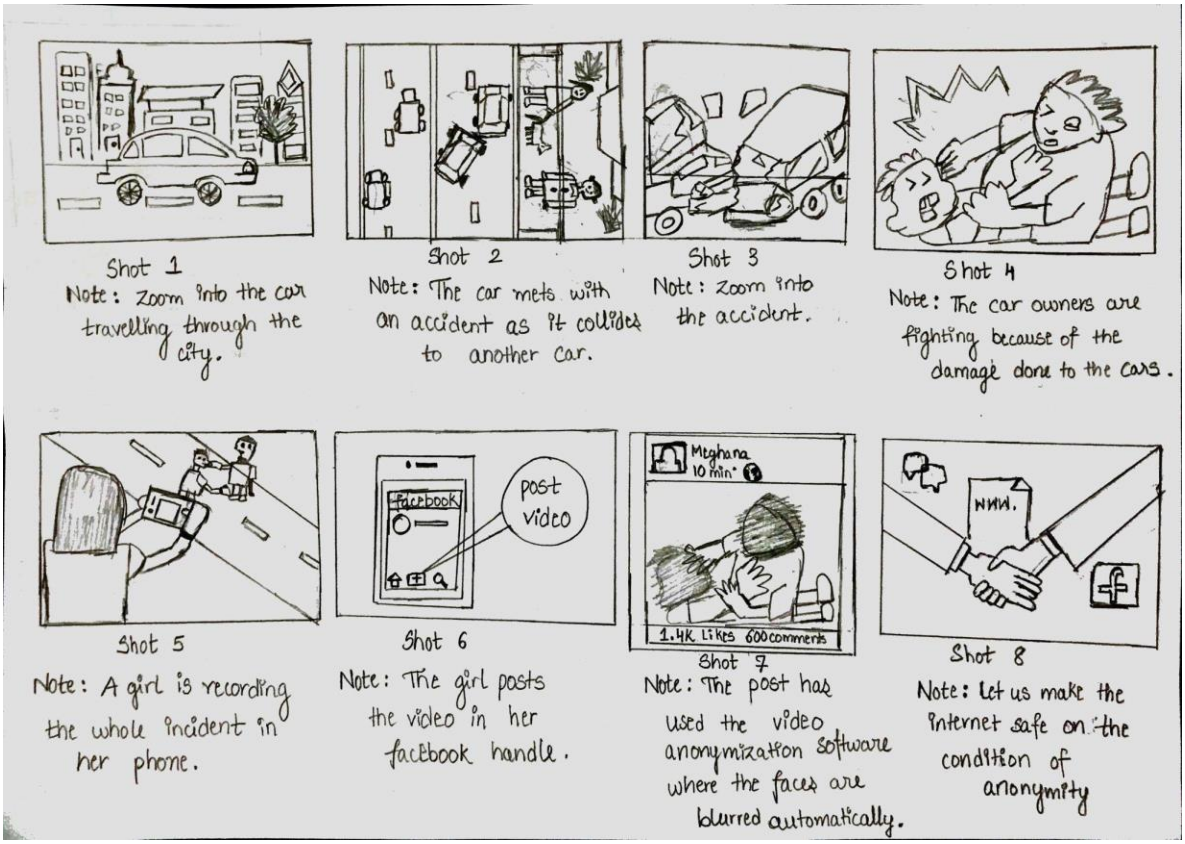

Figure 7. A storyboard demonstrating a situation where our program can be used.

4. PROJECT MODULES

Our project comprises five modules that have been detailed in the following sub-sections.

4.1 User interface

Front-end technology has been implemented in this module to develop the user interface of our web application using JavaScript, HTML and CSS.

4.2 Connecting the user interface to the backend

In this module, the front-end of the user interface has been connected to the backend developed using Flask. The video uploaded by the user on the client-side is sent to the server for processing. After the faces have been detected and blurred successfully on the server-side, the processed video is downloaded on the client-side for the user. Error handling scenarios like empty submission and attempts to upload a video greater than or equal to 200MB are implemented in this module.

4.3 Face detection

Automatic face detection in the uploaded video is implemented in this module. The OpenCV open-source library is a popular and powerful tool used for image processing and computer vision applications. The functions available in this library were used to automatically detect faces in the video uploaded by the user before blurring them. The video is converted to grayscale mode to make the video processing task easier.

4.4 Blurring faces

After the faces have been successfully detected, the video is split into numerous frames. The Gaussian blur technique is then applied to the detected faces in each video frame. The OpenCV library has been utilized to perform these tasks.

4.5 Export

When all the faces in each video frame have been blurred successfully, the modified frames are re-joined into the new processed video. This processed video is exported to the same path as the original video so that the user can find and access it easily.

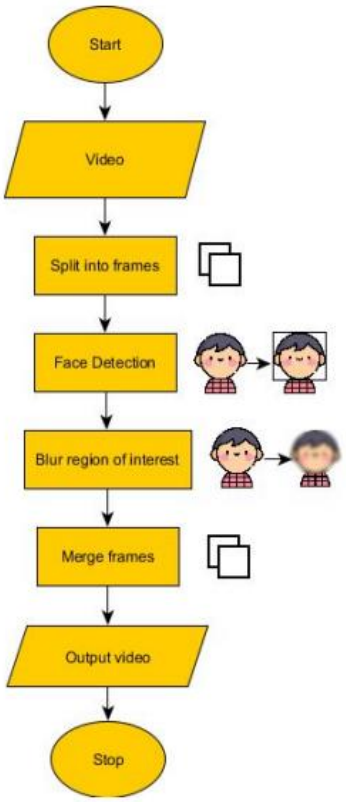

Figure 8. A flowchart depicting the process of face anonymization in a video.

5. DESIGN SCREENSHOTS

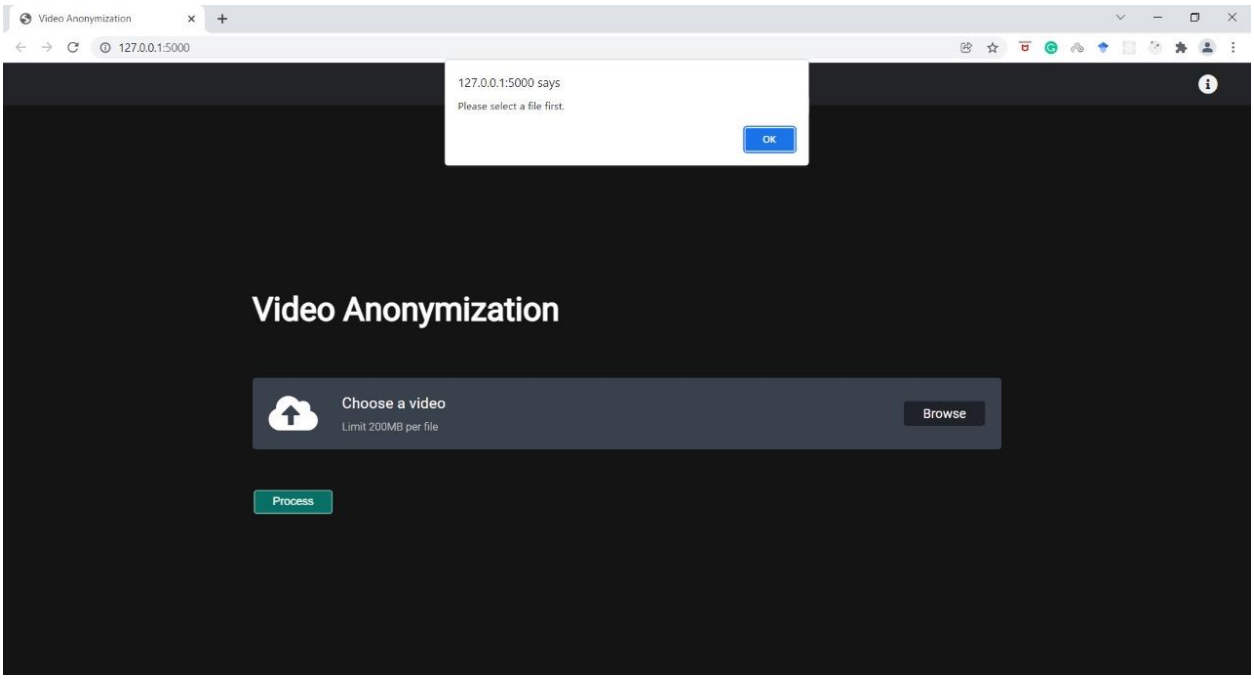

Figure 9. Error message for empty submission.

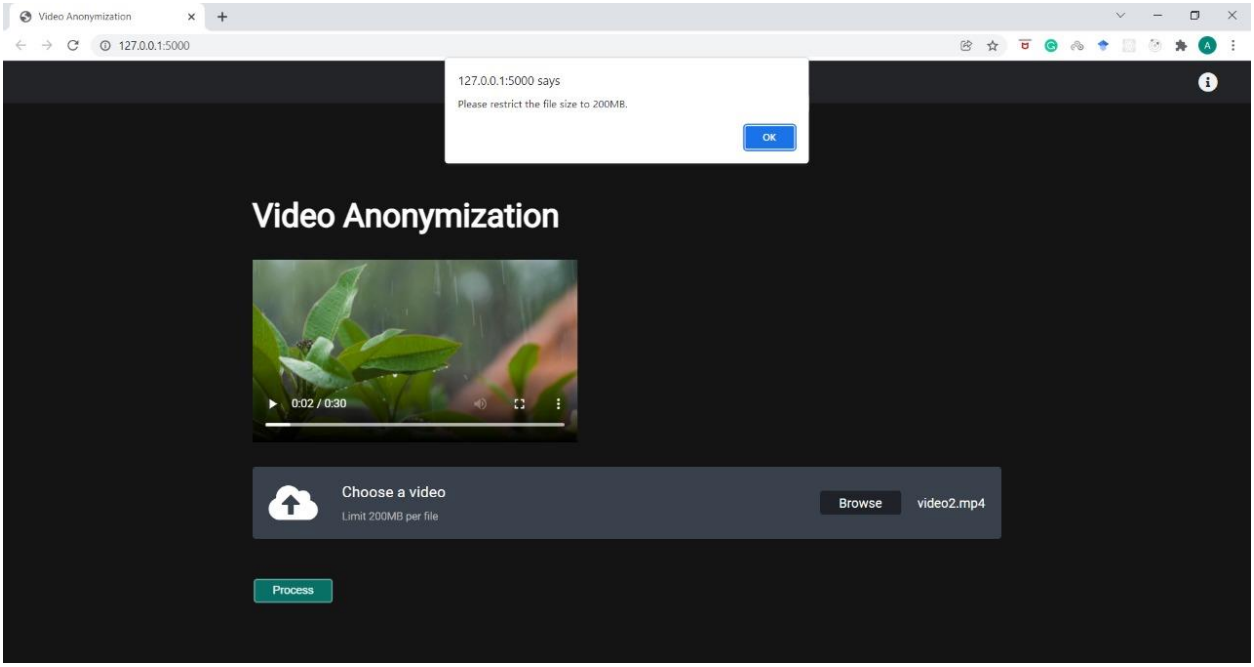

Figure 10. Error message for video file size >= 200MB.

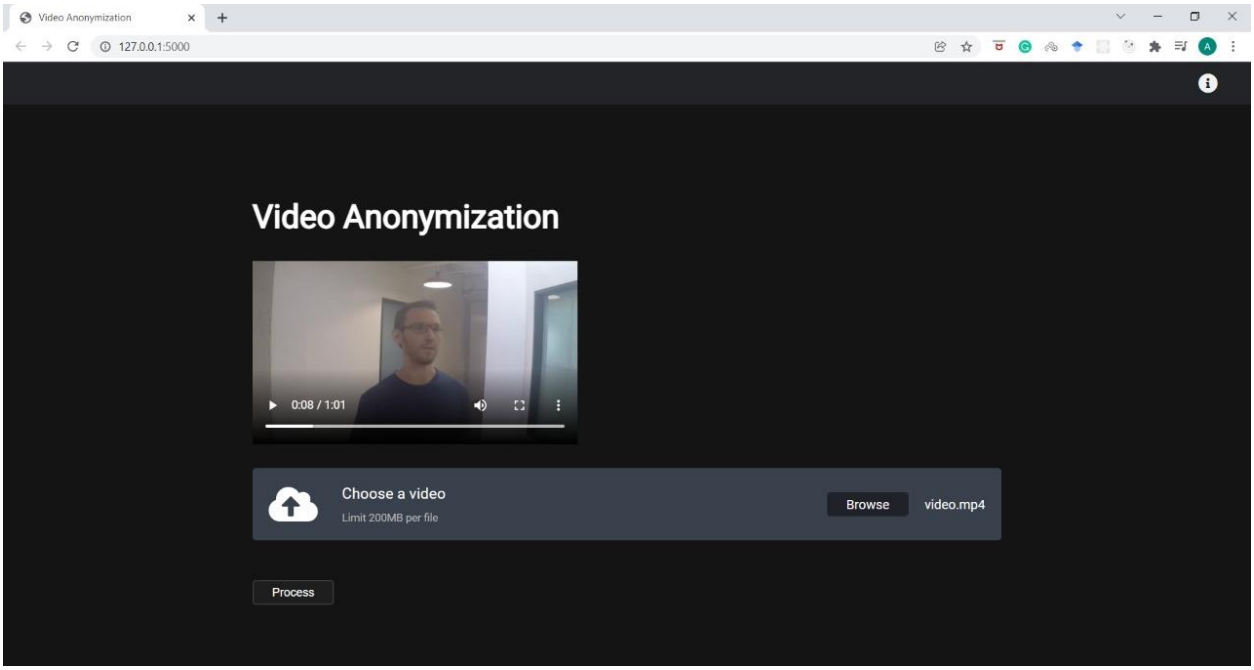

Figure 11. Successful video upload along with its preview.

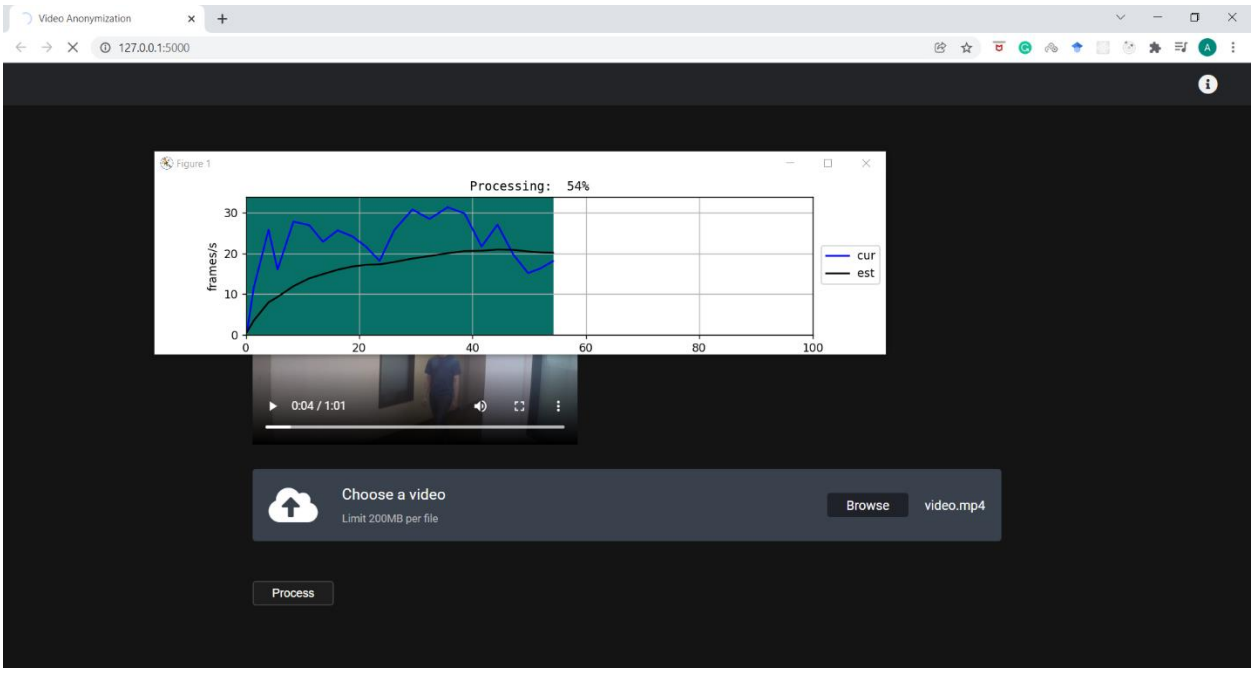

Figure 12. A dynamic progress bar to indicate that the video is being processed.

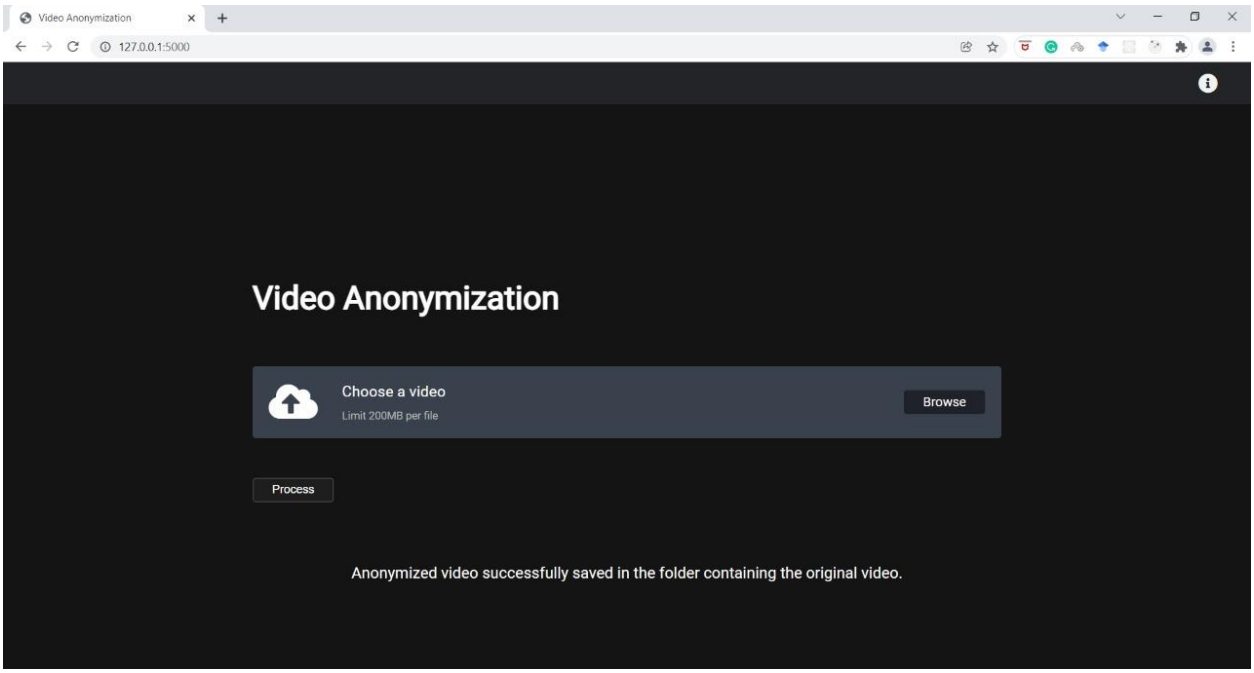

Figure 13. Video has been successfully processed and downloaded at the same location as the original video.

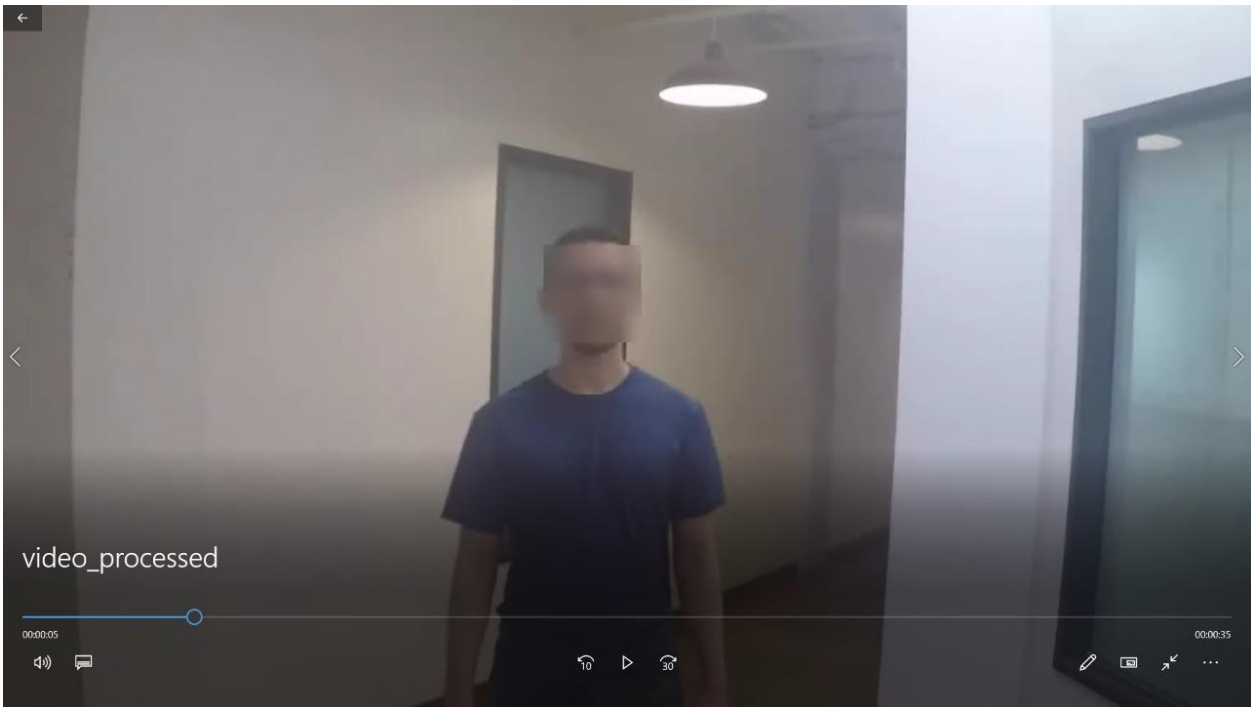

Figure 14. Downloaded processed video with successfully blurred faces.

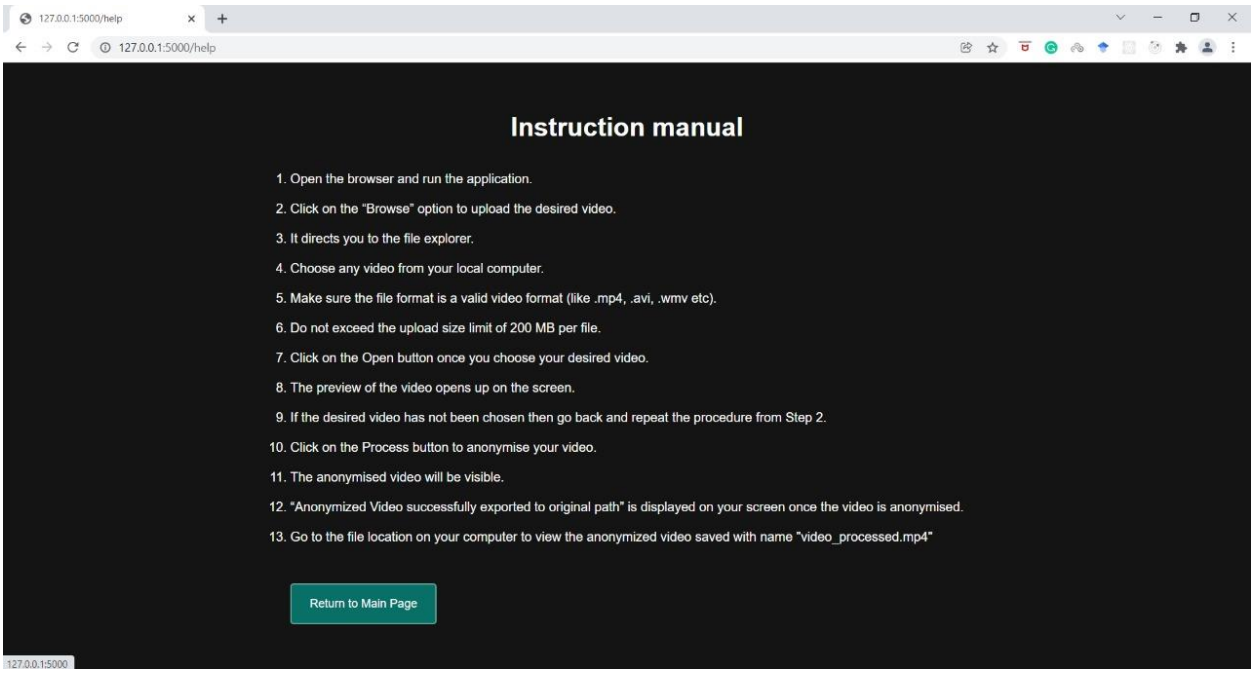

Figure 15. An instruction manual to explain to the user how to use the web application.

6. TEN HEURISTIC EVALUATION

H2-1: Visibility of system status

A preview of the uploaded video is shown to the user to indicate successful upload. The original video preview along with the video name is displayed on the screen to let the user check whether the desired video only has been uploaded instead of any other video. A progress bar is displayed to let the user know how much of the video processing has been completed. When the progress bar concludes, the user understands that the processing is complete. A message is also shown on the screen letting the user know where the processed video has been saved.

H2-2: Match between system and the real world

The Home page, error messages, instruction manual, buttons, video upload bar and all other content appearing on the web application screen speak the users' language with words, phrases and concepts familiar to the user. Any user with a rudimentary knowledge of how to use a website and the English language can use this web application.

H2-3: User control and freedom

All actions are reversible and mistakes can easily be rectified. If the user erroneously picks the wrong video file, the Browse button provides the flexibility to go back to the file explorer and choose the desired video again. If the user opens the instruction manual then they can click on the "Return to Main Page" button to return to the home screen. The user can also simply reload the

page to process another video. Video controls consisting of pause/play, volume, full screen/normal mode, control playback speed, picture-in-picture and download are also available on the video preview to let the user control how to interact with the preview.

H2-4: Consistency and Standards

The user interface of the web application follows a consistent theme including the font style, background and navigation bar. After every page reload or new visit, there is no change in the user interface. The label provided for every button and hyperlink is self-explanatory and does exactly what it conveying. For example, the “Process” starts the video processing and the “Browse” button allows the user to browse for videos to be processed.

H2-5: Error prevention

If the user clicks on the “Process” button without uploading any video, an error message is displayed to the user explaining that a video has to be uploaded prior to processing. If the user uploads a video which exceeds the file size limit of 200MB, an error message conveys this issue to the user and provides the solution of uploading a smaller video.

H2-6: Recognition rather than recall

All the actions and options of the interface have been developed in a clear and organized manner. There are no hidden areas in the user interface so that the user can find the functionalities that she/he is looking for easily. Every feature of the web application can be easily accessed by a button click with each button and hyperlink possessing a self-explanatory, precise label. Hence, there is no need for the user to memorize any features of the application interface. Important information regarding the features can easily be retrieved when required. A preview of the chosen video is displayed so that the user doesn’t have to recall what video was uploaded.

H2-7: Flexibility and efficiency of use

The navigation of the page is made accessible by allowing tab navigation so that the user does not have to reach for the mouse every time a particular part of the interface needs to be accessed. All the main features are front and center so no separate keyboard shortcut is needed. Clicking on a button is enough to upload, process and download the video as well as access the instruction manual.

H2-8: Aesthetic and minimalist design

No irrelevant and unnecessary information is shown to the user. It is aesthetically pleasing with a video preview provided. It has a minimalistic design which provides easy access to everything the user requires.

H2-9: Help users recognize, diagnose and recover from errors

Error messages are provided for every action done wrong. They are in simple and plain language so that the user can easily understand the mistake that has been committed. The error message for file size exceeding 200MB is given as “File size must be smaller than 200 MB” and when a user clicks the “Process” button before selecting a video, the error message shown is “Please select a file first.”. It not only recognizes the errors precisely for the user but also helps them recover from it by providing a solution.

H2-10: Help and documentation

An easy to understand and access instruction manual is available to the user with detailed steps to achieve the task successfully. It is not displayed on the home page to avoid a cluttered interface but an information icon is provided at the navigation bar that will redirect the user to the instruction manual.

7. TESTING

Three testing methods are used to test the application.

7.1 Usability testing

It involves all the GUI components, dealing with how the user handles the app components. We have made sure that the upload and download features are working properly and users do not face any kind of problem while using both features.

7.2 Interface testing

This component does not require the user, it helps proper communication between two software systems. In our case, it is Python in the backend and HTML in the frontend with Flask along with JavaScript acting as a medium to connect the two.

7.3 Acceptance testing

This helps the end-user determine whether the system is working for the given specification requirement. In our case, if all the faces in the original video are successfully blurred and processed video is made available to the user by downloading it on the client-side system, then the objective of protecting the users’ privacy through face anonymization in a video is achieved.

One usability problem that some users are facing is that they are finding the process to be slightly lengthy, i.e., to first convert the video to an anonymized video and then again uploading the video to any social media site. In this process, the users have to upload a video twice and also download the anonymized video on their computers, which takes up their time and memory on their devices.

To solve this multistep process, we can make a browser extension for social media sites like Facebook or YouTube, where users will be able to upload directly to social media using our plugin as discussed in Section 8.

7.4 Test case report

Test Case ID	Test Scenario	Test Steps	Test Data	Expected Results	Actual Results	Pass/ Fail
1	Check video upload and change path.	1. Select a video 2. Choose another video to change the path	Video .mp4 classr oom. mp4	Successfull y selected	Successfully selected	Pass
2	Check if any other file format is allowed to be selected by default.	1. Select a file with audio format	hello. mp3	Can't find the file	Can't find the file	Pass
3	Check if the form is not accepting responses with blank input.	-	-	Alert box Showing “Field required” and form Not submitting	Alert box Showing “Field required” and form Not submitting	Pass
4	Check if the form is accepting video up to the given limit (200MB).	Upload a video with a file size above 200 MB	-	Alert: File size exceeded	Alert: File size exceeded	Pass
5	Check if the user can view the converted video.	Press the Process button	-	<Video Playing>	<Video playing>	Pass
6	Check if the user can download the processed video.	Press on the downloaded button	-	<Video downloaded >	<Video downloaded>	Pass
7	Check whether the data from the HTML form is going to Python for processing.		-	<Video Playing>	<Video Playing>	Pass

8	Check if the form accepts another input on page reload.	Press Refresh and upload a video again	-	<Video Playing>	<Video Playing>	Pass
9	Check if the privacy of the people in the video is protected.	-	-	<The output video should have blurred faces>	<The output video is having blurred faces>	Pass
10	Check if all the faces in the given video are being anonymized.		-	<All the faces are being blurred out>	<All the faces are being blurred out>	Pass

8. CONCLUSION AND FORESEEABLE ENHANCEMENTS

This project aims to protect and preserve the privacy of individuals who appear in videos with sensitive contexts. This web design would reduce the annual number of cyberbullying cases and lend a hand in making the social media platforms safe, secure and constructive. This application is very efficient as it provides sufficient anonymization to protect the user's identity and this is available to the users for free.

For foreseeable enhancements, we plan to implement our project as a web extension too for social media applications so that users can directly post the processed video on social media. We also intend to reduce the video processing time using multithreading in the future.

REFERENCES

[1] T. Muraki, S. Oishi, M. Ichino, I. Echizen and H. Yoshiura, "Anonymizing Face Images by Using Similarity-Based Metric," 2013 International Conference on Availability, Reliability and Security, 2013, pp. 517-524, doi: 10.1109/ARES.2013.68.

[2] Natacha Ruchaud, Jean-Luc Dugelay. Automatic Face Anonymization in Visual Data: Are we really well protected?. Electronic Imaging, Feb 2016, San Francisco, United States. ffhal-01367565f

[3] A. J. Colmenarez and T. S. Huang, "Face detection and recognition," *NATO ASI Series F Computer and Systems Sciences*, vol. 11, no. 2, pp. 208–218, 1998.

[4] L. H. Koh, S. Ranganath, and Y. V. Venkatesh, "An integrated automatic face detection and recognition system," *Pattern Recognition the Journal of the Pattern Recognition Society*, vol. 35, no. 6, pp. 1259–1273, 2002.

[5] H. Lee, M. U. Kim, Y. Kim, H. Lyu and H. J. Yang, "Development of a Privacy-Preserving UAV System With Deep Learning-Based Face Anonymization," in IEEE Access, vol. 9, pp. 132652-132662, 2021, doi: 10.1109/ACCESS.2021.3113186.

[6] Girshick, R.B., Donahue, J., Darrell, T., Malik, J.: Rich feature hierarchies for accurate object detection and semantic segmentation. In: CVPR (2014)

[7] Ledig, C., Theis, L., Huszar, F., Caballero, J., Aitken, A.P., Tejani, A., Totz, J., Wang, Z., Shi, W.: Photo-realistic single image super-resolution using a generative adversarial network. CoRR (2016)

[8] H. Proença, "The UU-Net: Reversible Face De-Identification for Visual Surveillance Video Footage," in IEEE Transactions on Circuits and Systems for Video Technology, doi: 10.1109/TCSVT.2021.3066054.

[9] E.M. Newton, L. Sweeney, and B. Malin. Preserving privacy by de-identifying face images. IEEE Transactions on Knowledge and Data Engineering, 17(2):232– 243, 2005.

[10] Nakamura, T., Sakuma, Y., & Nishi, H. (2019, November). Face image anonymization as an application of multidimensional data K-anonymizer. In 2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW) (pp. 155-161). IEEE.