IMAGE PRIVACY PRESERVATION USING COMPUTER VISION TECHNIQUE

Project Submitted to the
SRM University AP, Andhra Pradesh
for the partial fulfillment of the requirements to award the degree of

Bachelor of Technology
in
Computer Science & Engineering
School of Engineering & Sciences

submitted by

Faiyajuddin Shaik(AP20110010363)

Nikhith Reddy Devalapalle(AP20110010368)

Jagadeesh Pamulapati (AP20110010386)
Jaya Prakash Kadiyala(AP20110010403)

Under the Guidance of

Prof Swagata Samanta and Prof Pradyut Kumar Sanki

Department of Computer Science & Engineering
SRM University-AP
Neerukonda, Mangalgiri, Guntur
Andhra Pradesh - 522 240
May 2024

DECLARATION

Declaring that this project report, **IMAGE PRIVACY PRESERVATION USING COMPUTER VISION TECHNIQUE**, is a legitimate work completed by me under the guidance of Prof Swagata Samanta and Prof Pradyut Kumar Sanki , it fulfills a portion of the requirements for the award of a Bachelor of Technology degree in the Computer Science & Engineering, SRM University-AP.

I have expressed my opinions in this work using my own words, but I have correctly and appropriately attributed the original sources wherever I have used someone else's words or thoughts. I further attest that I have adhered to the standards of academic honesty and integrity and have not altered or manipulated any data, notion, idea, fact, or source in my work. I understand that violating any of the aforementioned could lead to disciplinary action from the institution or organization as well as legal action from uncited or improperly obtained sources. Using this study as the basis, no degree or other honor has ever been awarded.

Place	:	Date	: June 6, 2024
Name of student	: Faiyajuddin Shaik	**Signature**	: .....
Name of student	: Nikhith Reddy Devalapalle	**Signature**	: .....
Name of student	: Jagadeesh Pamulapati	**Signature**	: .....
Name of student	: Jaya Prakash Kadiyala	**Signature**	: .....

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

SRM University-AP

Neerukonda, Mangalgiri, Guntur

Andhra Pradesh - 522 240

CERTIFICATE

This is to certify that the report entitled **IMAGE PRIVACY PRESERVATION USING COMPUTER VISION TECHNIQUE** submitted by **Faiyajuddin Shaik, Nikhith Reddy Devalapalle, Jagadeesh Pamulapati , Jaya Prakash Kadiyala** to the SRM University-AP a genuine record of the project work completed with my/our assistance and supervision serves as a partial fulfillment of the requirements for the award of a Master of Technology degree in This report, in any format, has not been sent, for any reason, to any other university or institute.

Project Guide	**Head of Department**
Name : Prof Swagata Samanta and Prof Pradyut Kumar Sanki	**Name** : Prof. Niraj Upadhayaya
Signature:	**Signature**: .....

ACKNOWLEDGMENT

I want to express my gratitude and debt of gratitude to everyone who assisted me in properly preparing and presenting this project report, which is named **IMAGE PRIVACY PRESERVATION USING COMPUTER VISION TECHNIQUE**

We would like to sincerely thank our mentor in charge, Prof Swagata Samanta and Prof Pradyut Kumar Sanki sir, and also thank Prof. Niraj Upadhayaya, Head of Department of Computer Science & Engineering for their encouragement. We were able to overcome numerous challenges that arose during every stage of this project thanks to her immense knowledge and patience. We had an absolutely incredible experience working on this project overall. We learned a lot of facts about numerous topics about which we had always been intrigued when we were under her guidance. There is no supervisor we could have asked for better.

ABSTRACT

With the increasing concerns surrounding privacy in digital imagery, this research project presents a novel approach to address these issues through the utilization of face obfuscation for detection and median blur for image anonymization. The project workflow begins with the implementation of a face obfuscation algorithm, which efficiently identifies and localizes faces within images without the need for complex deep learning models. Leveraging image processing techniques and heuristic rules, this algorithm achieves reliable face detection across diverse. Once faces are detected, a median blur algorithm is applied to the corresponding regions to effectively anonymize individuals while preserving the overall structure and context of the image. Unlike traditional blurring methods, median blur offers a balance between effectiveness and computational efficiency, making it suitable for real-time applications and large-scale image processing tasks.

The performance of our system is evaluated through rigorous experimentation and analysis. Quantitative metrics such as detection accuracy and processing speed are measured to assess the effectiveness of the face obfuscation algorithm. Additionally, subjective evaluations are conducted to evaluate the quality of the anonymization process and its impact on image clarity and aesthetics.

Overall, our research project provides a practical and efficient solution for addressing privacy concerns in digital imagery. By leveraging face obfuscation and median blur techniques, our system offers a lightweight yet effective approach to safeguarding individual privacy in various applications, including social media platforms, surveillance systems, and personal privacy tools.

ABBREVIATIONS

GDPR – General Data Protection Regulation

OPENCV – Open-Source Computer Vision Library

API – Application Programming Interface

CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION TO THE PROJECT

Deep learning plays an important role in our life. As we can use our faces to do many things which is also a part of our privacy, using that we can protect our mobile by face detection and find other missing people. The usage of camera technology is increasing day by day which results to today's reality. The vast data provided by machine learning algorithms are increasingly from the usage of users. They also require the protection of those people's privacy.

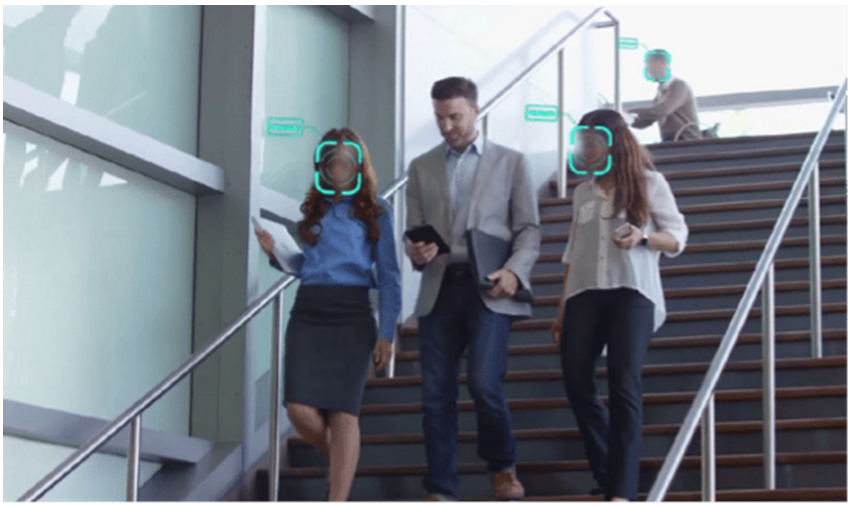

Figure 1.1: Image

The GDPR states that, "Personal data is always personal and privacy where we should use that wisely and limitly. Some people use this as their weapon and do some ridiculous things to others privacy details." Many approaches have been significantly developed for animalising visual data. Out of all approaches face blurring is the most appropriate and effective

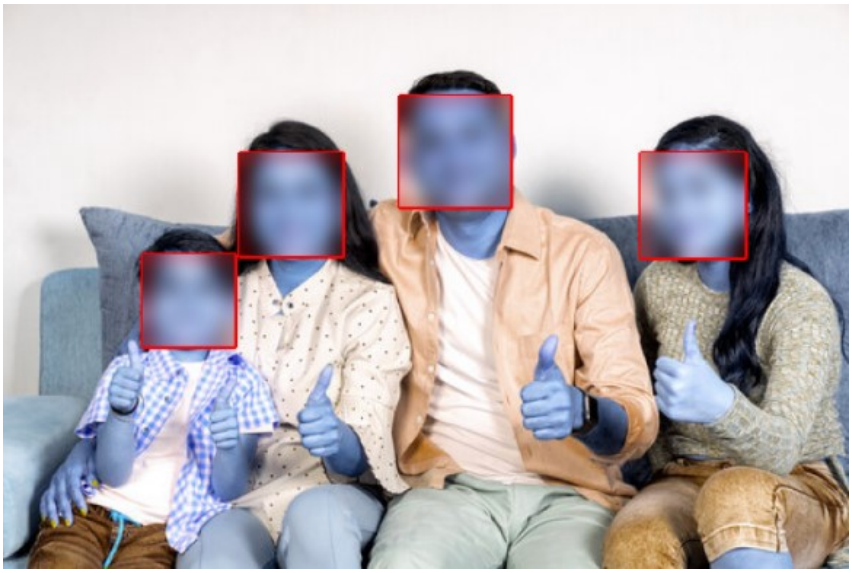

Figure 1.2: image 2

techniques. This technology allows us to share the data with other world while maintaining our privacy intact and others privacy like pictures and videos Using deep learning technology face blur technology can detect faces at any real time video presence. And when it is done an additional layer of "blurring or pixelation "is added on top to conceal the face. In this procedure video's other features remain unchanged none is affected

Chapter 2

MOTIVATION

Growing Privacy Concerns:

As digital imaging has become more widely used, the quantity of private visual data exchanged online has skyrocketed. Photos are included in this as well as recordings made by security cameras in public areas, sent over messaging applications, and posted to social media sites. Sharing this kind of material can promote social interactions and communication, but it also poses privacy issues.

Example: For instance Imagine a situation where someone shares a picture of their buddies during a party on social media. Although it might not seem like much, the picture might unintentionally divulge private information about people's travels, pursuits, or interpersonal connections. This information could be used by hostile actors for harassment or stalking if appropriate security measures aren't in place.

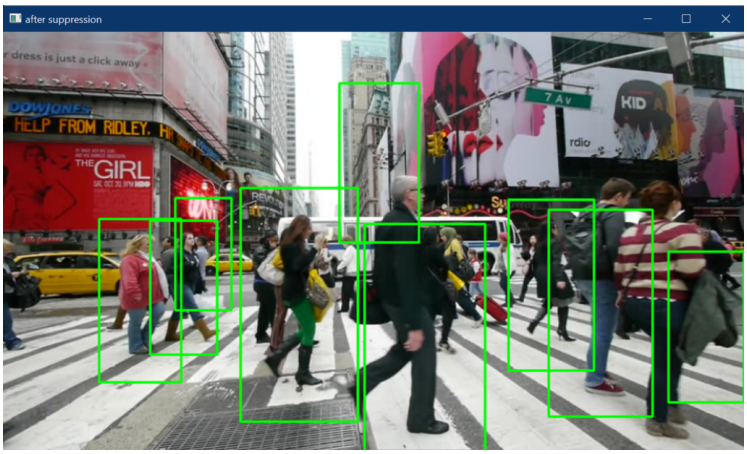

Figure 2.1: Computer Vision

Legal and Ethical Considerations:

As technology advances quickly, there are now more difficult ethical problems around the use of visual data. Talks about the appropriate management of personal visual data center on topics like permission, data ownership, and the right to privacy. Laws and regulations pertaining to data protection, for example, also regulate the gathering, archiving, and distribution of visual data.

Example: As an illustration Let us say a business creates a facial recognition system for security reasons, but neglects to get the people whose photos the system uses to identify them to give their informed consent. Due to the possibility that the business is breaking privacy rules that demand express authorization before collecting and using biometric data, this could have legal ramifications.

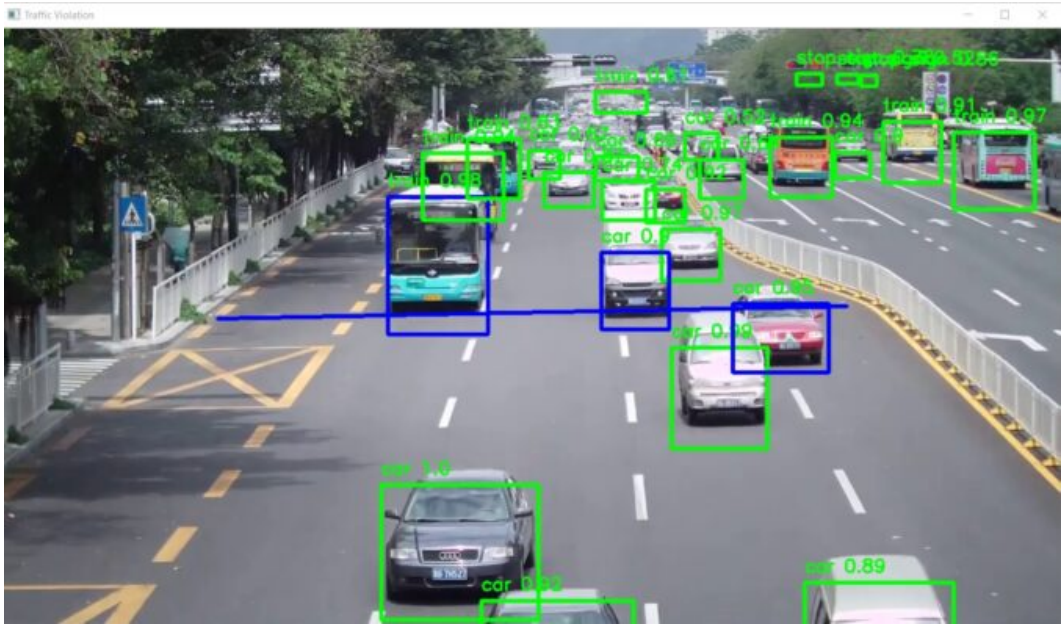

Figure 2.2: Computer Vision

Chapter 3

LITERATURE SURVEY

An summary of the previously published works on a topic is what a literature review is. The phrase can be used to describe an entire academic document or a specific portion of a book, essay, or other scholarly work. In any case, the goal of a literature review is to give the audience and the researcher/author a broad overview of the body of information that already exists on the subject at hand. A thorough literature assessment can guarantee that the right theoretical framework, research methodology, and/or research question have been selected. More specifically, a literature review gives the reader context by placing the current work within the corpus of pertinent literature. In these situations, the review typically comes before the methodology and and results sections of the work.

In the process of preparing a thesis, dissertation, or journal article, graduate and post-graduate students frequently have to produce a literature review. Reviews of the literature are also frequently included in research proposals and prospectuses, which are authorised documents that students submit before starting their dissertations or theses.

A review article can take the form of a literature review. A literature review is, therefore, an academic work that summarises the state of the art on a given subject, encompassing theoretical and methodological advancements as well as significant discoveries. Review of the literature is a secondary source; it does not report newly conducted or unique experimental work. most frequently connected to scholarly writing.

Chapter 4

DESIGN AND METHODOLOGY

4.1 IS PRIVACY PRESERVING IN AI USEFUL ?

Because of some unpredicted accuracy od deep learninf techniques , some Ai applications have creatred As a result,The companies can collect a lot of data from the user as the amount of data used for training gives the accuracy for deep learning . In that result user's personal and private data are stored indefinently which is not shown publicaly . Many facts proprietors, as an example, clinical institutions that want to apply deep getting to know techniques on sensitive information including medical records, are hindered by means of privateness and confidentiality troubles. As a result, the improvement of privateness-preserving large-scale deep studying has enormous blessings for a couple of packages.

Giving authorized access for sensitive information in private database is being more important matter nowadays.

Face obfuscation is used to mitigate privateness troubles based totally on face pics. item detection research normally assumes get right of entry to to complete, unobfuscated pics. In visual datasets, even supposing most classes are commonly no longer humans classes, many incidental people appear inside the pix, and their privateness is a difficulty

Figure 4.1: image 2

4.2 WHAT DO YOU MEAN BY VIDEO BLURRING BASED ON COMPUTER VISION

Applications based on Computer vision are formed by the un forgettable precision made by deep learning techniques. As the amount of data used for training is closely related to effictiveness of algorithms in deep learning, businness manager can use a huge amount of data from user. Face obfuscation is develeoped mainly to reduce face photos privacy which concerns more. All unobscured images have entire access to majority of object detection research work.

For blurring the faces in videos we use the recent technology of artificial intelligence. This would be a useful advantage for many security resaons and peoples privacy. In the market there are many face blurring technologies based on Ai in which each of them differ a little bit. When an image is appeared in screen as soon as possible image is blurred similar to real time video based.

Chapter 5

IMPLEMENTATION

5.1 HOW DOES FACE BLUR IN VIDEO WORK

There are numorous methods which can apply to create face blur in videos. In these methods one of the algorithm is used to detect and identify the image in data frame , then that image part is send to blurring filter . This can apply in real time at the time of video shot itself . Or else you can the filter after the video was prepared or viceversa.

Median blur is one of the most popular face blurring methods. Using the bounaries of images the filter will blur the face edges and recognize who's is whom .The filters like motion blur is also possible for real time video.

5.2 USAGE OF FACE BLUR

It has been demonstrated that face obfuscation, such as facial blurring, is beneficial for preserving privacy. However, entire, undecorated images are frequently used for object recognition, object detection, and image segmentation. In order to blur faces in the Image, the following steps were used.

5.3 1. DETECT FACES WITH FACE ANNOTATION

Faces are frequently found , even for pictures that aren't explicitly people categories, proving the importance of privacy-aware face recognition for . Face segmentation model to obscure sensitive picture portions using pixels Object identification, scene recognition, object detection, and face attribute categorization are a few examples of downstream computer vision tasks Face detection is the first step in face obfuscation. As a result, all faces are identified and annotated using face detectors.

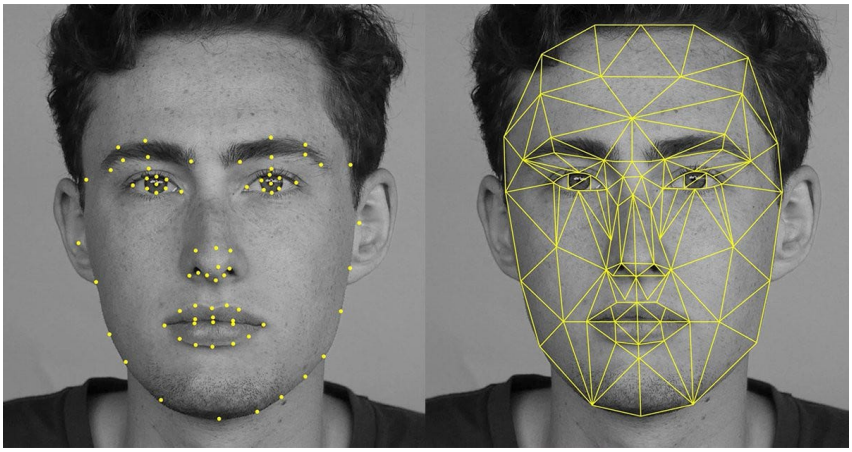

Figure 5.1: image 4

Figure 5.2: image 4

5.4 BLUR DETECTED FACES FOR FACE OBFUSCATION

here are numerous methods which can apply to create face blur in videos.

One algorithms from these methods is used to detect and identify the face in that image, then that part is send to blurring filter.

Median Blur is one of the most popular face blurring methods. Using the boundaries of images, the filter will blur the face edges and recognize who's is whom. Obfuscation of faces has a negligible effect on the precision of recognition models. On face-blurred photos, bench marking with various deep neural networks revealed that the total recognition accuracy just minimally (0.68 **Effects of Face Blur on Computer Vision Tasks** Several different

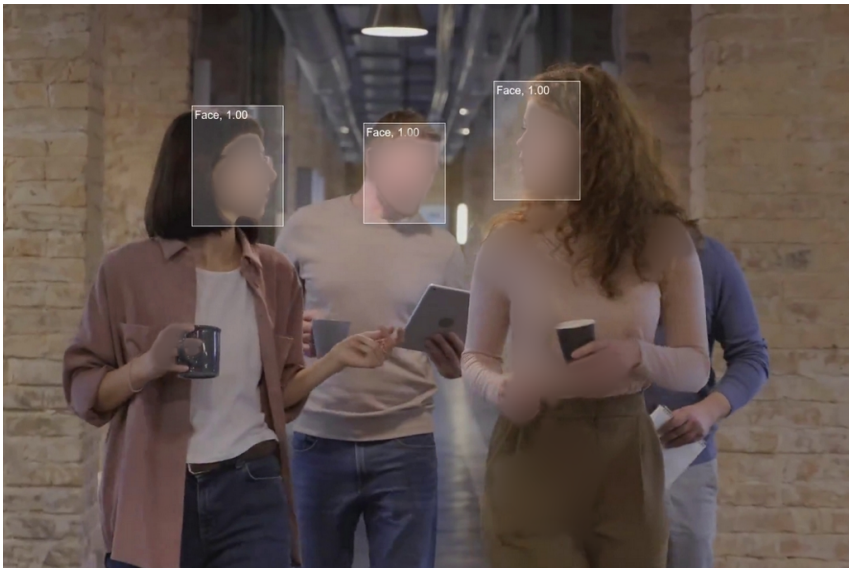

Figure 5.3: image 5

computer vision tasks benefit from the use of visual features discovered . Computer vision techniques were tested on face-blurred images, and the results showed that face obfuscation gives privacy protection with little loss of accuracy.

Figure 5.4: image 6

5.5 ALTERNATIVE METHODS TO ANONYMIZE FACES

From merely obscuring the face using frequently unpleasant ocluders, like black boxes or mosaics, to more sophisticated systems that produce natural images, numerous ways of visual identity obfuscation have developed.

1. Face covering. Examples of face-blurring-like face anonymisation techniques include masking the facial area with ocluders like mosaic or a black strip. These strategies continue to be the most often used ones for hiding visual information in images or movies.

2. Face replacement. By replacing heads in photographs, a novel technique masks identities while maintaining a high degree of likeness to the content of the original image.

3. Removing of moving people. A technique to automatically remove and inpaint faces and licence plates . In order to create a realistic output image, a moving object segmentation technique was utilised to detect, delete, and inpaint moving objects with information from other perspectives View

Chapter 6

HARDWARE/ SOFTWARE TOOLS USED

Hardware tools :

1. Computer
2. Camera or Imaging device

Software tools :

1. OpenCV
2. MATLAB
3. Median blur
4. Gaussian blur
5. Jupyter Notebook

Chapter 7

RESULTS & DISCUSSION

7.1 IDENTIFICATION SUCCESS

The findings of the identification process utilising the single detection strategy are summed up below. hit (the target is present and the answer is correct), miss (the target is present and the response is incorrect or ”None of above”), true alarm (the target is absent and the response is present), and false alarm (the target is absent but the response is present) are the options available. Face blurring is 49, however total identification success is 74 for all instances.

Figure 7.1: Image 7

7.2 IDENTIFICATION SELF ASSURANCE

Total correctness is represented by both hit and correct rejection.because both a false alert and a miss indicate complete error. In the event of a strike, proper rejection, or false alarm, the variations between the outcome and face blurring are marginal and not statistically significant (p¿0.5). The confidence rating of the result for overall wrongness is higher than that of face blurring with p¡0.1. Finally, the confidence ratings are ¿= 4, independent of the result of the identification.

Table 1. Successful identification by filter

		Privacy Filters	
		As is	Face blurring
Identification Success	All cases	74%	49%
	Target present	76%	69%
	Target absent	69%	24%

Figure 7.2: Image 7

Standard error of the mean is shown by the error bars in the identification self-assurance suggested values.

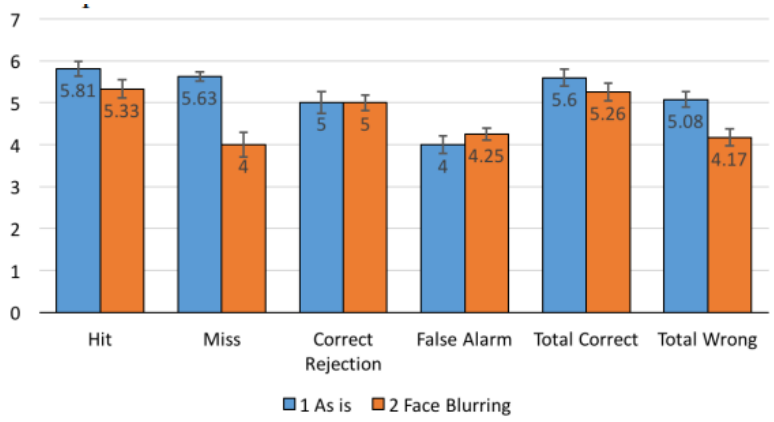

Figure 7.3: image 8

Likeability was shown to be higher in photographs that did not have the privateness filter applied than those that did. t(46) = 1.24, p =.22 suggests

that there may not be a difference in the likeability between face blurring and as is, even though the suggestion of as is is marginally better.

Table 2. Photo satisfaction, information sufficiency, photo enjoyment, social presence, and likeability means for *as is* vs. *face blurring*.

	Privacy Filters			
	As is	Face blurring	t	df
Satisfaction	5.0(0.23)	4.15(0.23)	3.74***	46
Information Sufficiency	5.43(0.22)	4.30(0.22)	5.61***	46
Photo Enjoyment	4.77(0.22)	4.0(0.23)	3.79***	46
Social Presence	5.06(0.22)	4.60(0.22)	2.57*	46
Likeability	4.83(0.28)	4.40(0.28)	1.24	46

Note. * = p < .05, *** = p < .001. Standard Error of the Mean appear in parentheses below means.

Figure 7.4: image 9

The error bars show the standard error of the mean for the mean values of the photo satisfaction, information sufficiency, photo enjoyment, social presence, and filter likeability.

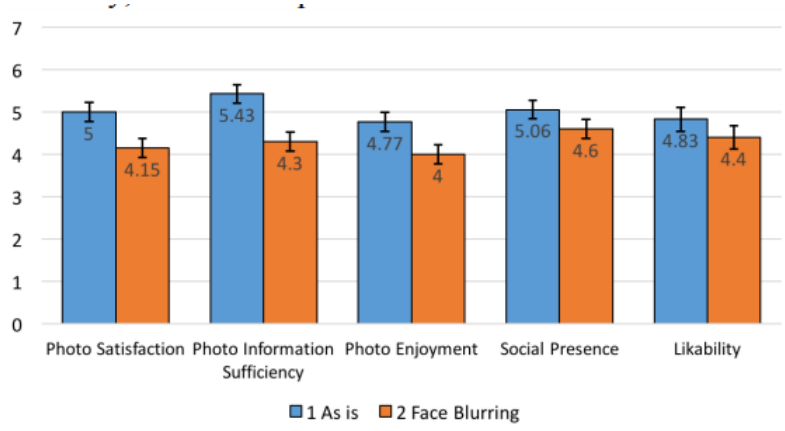

Figure 7.5: image 10

Chapter 8

CONCLUSION

In conclusion, our project introduces a novel approach to addressing privacy concerns in digital imagery using computer vision techniques. .

The project workflow begins with a face obfuscation algorithm that efficiently identifies and localizes faces within images without the need for complex deep learning models. Leveraging image processing techniques and heuristic rules, this algorithm achieves reliable face detection across diverse inputs. Once faces are detected, a median blur algorithm is applied to the corresponding regions to effectively anonymize individuals while preserving the overall structure and context of the image.

Unlike traditional blurring methods, median blur offers a balance between effectiveness and computational efficiency, making it suitable for real-time applications and large-scale image processing tasks. The performance of the system is evaluated through rigorous experimentation and analysis, including quantitative metrics such as detection accuracy and processing speed, as well as subjective evaluations to assess the impact on image clarity and aesthetics.

Overall, this project provides a practical and effective solution for addressing privacy concerns in digital imagery. By leveraging face obfuscation and median blur techniques, the proposed system offers a lightweight yet robust approach to safeguarding individual privacy in various applications, including social media platforms, surveillance systems, and personal privacy tools.

REFERENCES

[1] **G. O. Young**, Synthetic structure of industrial plastics, in *Plastics*, 2nd Ed., Vol.3, J.Peters, Ed. New York: McGraw Hill, 1964, 15-64

[2] **Bradshaw, P.**, An Introduction to Turbulence and its Measurement, Pergamon Press, 1971.

[3] **J. U. Duncombe**, Inrared navigation – Part I : An Assessment of feasibility, *IEEE Trans. Electron Devices*, Vol. ED-11, No.1, 34-39, Jan 1959

[4] Oxygen absorption in the earths

[5] **Bradshaw, P.**, An Introduction to Turbulence and its Measurement, Pergamon Press, 1111.

[6] **E. E. Reber, R. L. Michell and C. J. Carter**, Oxygen absorption in the earths atmosphere, Aerspace Corp., Los Angeles, CA, Tech. Rep. TR-0200 (4230-46)-3, Nov 1988.

LIST OF PUBLICATIONS

[1] **Andrews, G.E and D.Bradley** (1972) The Burning Velocity of Methane-Air Mixtures, *Combustion & Flame*, 19, 275-288.

[2] **J. U. Duncombe**, Inrared navigation – Part I : An Assessment of feasibility, *IEEE Trans. Electron Devices*, Vol. ED-11, No.1, 34-39, Jan 1959

[3] **Lefebvre, A. H.**, (1965) Progress and Problems in Gas Turbine Combustion, *10th Symposium (International) on Combustion*, The Combustion Institute, Pittsburg, 1129- 1137.