UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Technology

Maris Popens

Privacy preserving using face replacement-based image anonymisation tool

Bachelor's Thesis (12 ECTS)

Curriculum Science and Technology

Supervisors:
Doğuş Karabulut

Prof. Gholamreza Anbarjafari

Tartu 2020

Privacy preserving using face replacement-based image anonymisation tool

Abstract:

The General Data Protection Regulation that was implemented in 2018 put increased stress on online privacy of people. This increased the pressure on social media platforms to protect privacy and follow the new set of guidelines. Currently, the only possible tool for preserving personal privacy is censorship, which either covers up or blurs out a part of an image that could potentially conceal vital details. This thesis proposes a proof of concept for a solution that could keep the image undisrupted while preserving the privacy of the person. This potential solution replaces the face with a generated face that lacks distinguishing features. This thesis describes the steps required to carry out face replacement. It takes advantage of precise facial detection in combination with a face collage that was generated by averaging copious amounts of facial images. The result is an image that still has all its details while preserving the privacy of the person.

Keywords: face replacement, censorship, image processing, artificial intelligence, convolutional neural networks, privacy

CERCS: P176 - Artificial intelligence, T111 - Imaging, image processing, P170 - Computer science, numerical analysis, systems, control

Privaatsuse säilitamine kasutades näovahetusel põhinevat pildi anonüümseks muutmise tööriista

Lühikokkuvõte:

Isikuandmete kaitse üldmäärus, mis võeti kasutusele aastal 2018, rõhutas inimeste privaatsust veebis. See nõudis, et sotsiaalmeedia kanalid peavad kaitsma inimeste privaatsust ja järgima uusi suuniseid. Hetkel ainuke vahend eraelu privaatsuse säilitamiseks on tsensuur, mis katab või hägustab osa pildist, kuid võib potentsiaalselt varjata tähtsaid detaile. Selles lõputöös esitletakse lahenduse kontseptsioon, mis ei moonda pilti, kuid säilitab inimese privaatsuse. See potentsiaalne lahendus asendab inimese näo genereeritud näoga, millel puuduvad eristatavad iseärasused. Selles lõputöös kirjeldatakse vajalikke etappe, et teostada näovahetust. See kasutab täpset näotuvastust koos näokollaažiga, mis loodi mitmete nägude kokku ühtlustamise teel. Tulemuseks on pilt, mis sisaldab kõiki vajalikke detaile, kuid säilitab inimese privaatsuse.

Võtmesõnad:

Näovahetus, tsensuur, pilditöötlus, tehisintellekt, konvolutsiooniline närvivõrk, privaatsus

CERCS: P176 - Tehisintellekt; T111 – Pilditehnika, P170 - Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

TABLE OF CONTENTS

TERMS, ABBREVIATIONS AND NOTATIONS

- AI – Artificial Intelligence
- CNN – Convolutional Neural Network
- DL – Deep Learning
- EU – European Union
- GAN – Generative Adversarial Network
- GDPR – General Data Protection Regulation
- HOG – Histogram of gradients
- MIT – Massachusetts Institute of Technology
- ML – Machine Learning
- NN – Neural Network

INTRODUCTION

With the newly implemented General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 in the European Union (EU) there is an increased emphasis on the privacy of European citizens. The fact that this regulation is implemented in the EU, it is not limited to just European companies. (Dean and Nigl, 2019.) Due to the global reach provided by the internet, companies found in the United States are affected by this, as a result of EU citizens being serviced by them. This forces everyone who wants to service EU citizens to follow the guidelines. And most of the companies are following the guidelines, as they do not want to lose 500 million clients. (Tankard and Pathways, 2016)

The main point of GDPR is privacy protection. For social media, where images are shared privacy is a sensitive topic, as images can hold massive quantities of personal data and in the modern times of advancing biometric authentication, facial images are becoming increasingly looked for and abused wrongfully. As a result of this, it is important to protect facial image data from unwanted exposure. That would be people, who are not in the circle of acquaintances, as these people already know the facial features of this person and potentially are already in the hold of such image in their private photo library. Because of this, the focus should be put on strangers, whose intentions are unknown and do not know them personally. (Senthil Kumar, Saravanakumar and Deepa, 2016)

Problem Definition

Currently available method for image privacy protection is image blurring or covering a part of the image, in other words, censorship. This is an effective method for protecting privacy as parts of images are obstructed. This is an effective way for identity concealment, but for it to achieve that purpose, it needs to ruin an image. (Gutta *et al.*, 2005). This method is acceptable when the integrity of the image is not a priority and the result is important. For social media, such a method will not be of the best use, as in social media image posting is meant to share the content of the image. The solution proposed in this thesis is the face anonymisation utilizing face replacement. This results in an image, that keeps its contextual integrity while at the same time preserves the privacy of the person.

Over the last 20 years, face detection has gone a long way and it has improved both in performance and accuracy. Also, following the development of Artificial Intelligence (AI), this process has been further improved. The improvement in face detection motivates its use in a more precise censorship method. (Bitouk *et al.*, 2008) Thanks to these advancements, it has become easier and more promising to use face replacement for face anonymisation. For this thesis, the aim is to create a proof of concept technology for automated face replacement. The idea behind this method is to replace the face of the person in the image with a face collage that is generated without specific facial features and details. (Mahajan, Chen and Tsai, 2017) This results in a face that does not contain personal facial data that can be used against the person, as a mean to steal identity or to gain access to data that is protected by facial biometric authentication. (Harding, 2019) (Bruce and Young, 1986)

Aim of the Thesis

In this thesis, the primary technology for face replacement has been presented, tested, and evaluated. The structure of this work is presented as follows. The beginning step is a literature overview of the background knowledge and specific concepts required to understand and develop the technology for face replacement. Afterwards, the methods that are used in this thesis, that include face detection, age and gender detection, creation of the face collage and the face-swapping, are introduced and explained. This section is followed by the presentation and discussion of the results which are further summarized in the conclusion in the perspective of further applications.

1 LITERATURE REVIEW

In 2018 a new regulation took place of earlier Data Protection directive to protect living persons concerning handling and processing of their data and the free movement of that data. Regulation is called the General Data Protection Regulation, also known as GDPR. This brought a lot of potential distress to social media platforms, as they are purely focused on handling personal data, as a result, creating unfamiliar problems and challenges that had to be overcome. One of such challenges is privacy related to photo sharing and displaying. (Wieringa *et al.*, 2019)

A potential solution for this problem is the usage of automatic facial anonymisation using automated image processing tools. This results in facial privacy preservation, without disrupting the quality of the imagery. The goal of this literature review is to cover the technology, that makes up the process of face detection and face replacement – all the steps required to effectively preserve the identity of the person. (Mansfield-devine, 2016)

1.1 Image processing.

The first part of doing any image modification digitally is image processing. When dealing with digital computer images, even the most basic actions require image processing. To start, I will layout basic terms, that are needed in the perception of the current topic and literature behind it. Image is an array or a matrix of square pixels (from the word picture element) arranged in columns and rows. Pixel is the smallest element that makes up a digital image.

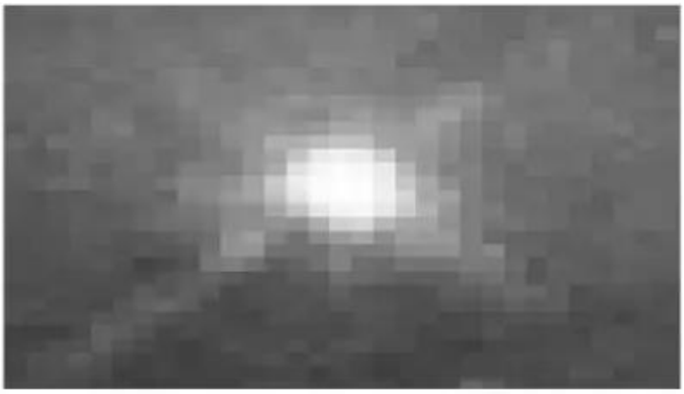

Figure 1.1. An image – array of pixels. (Saroha *et al.*, 2013)

Image processing is the method of converting image into digital form and performing some operations on it. Converting an image into digital form is done by either picture scanning or digital picture creation, that is a digital camera or some device of such kind. Digitally image is treated as a two-dimensional signal, it does not have depth and on these two dimensions – width and height, operations are performed. Operations include image enhancement or just displaying the created image. According to the article (Saroha *et al.*, 2013), image processing can be divided into three steps:

1. Creating digital image either by an optical scanner or digital photography
2. Analysing and manipulating image
3. Output, either of modified image or image analysis data.

1.2 Face detection

The main part of the face anonymisation is face detection. A fundamental part of it is the perception of the face. Humans are capable of recognizing familiar people or human faces with ease. This ability is so advanced in humans, that we tend to recognize facial features in objects, that are non-human or even non-living. (Nirkin *et al.*, 2018) This phenomenon was researched by Ichikawa and his colleagues. The results gathered proved that for humans if the object has eyes-like features, then it is perceived as a face-like object. Examples of some such objects can be seen in figure 1.2.

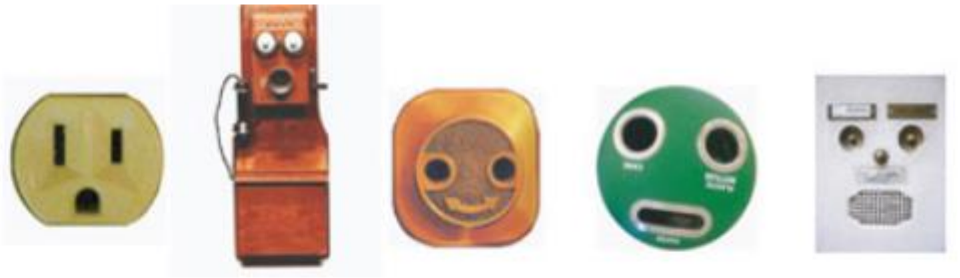

Figure 1.2. Non-living face-like objects. (Ichikawa, Kanazawa and Yamaguchi, 2011)

This ability of humans is impressive. For computers, this is not innately achievable. For a computer to recognize a human face, it has to be taught, what is a human face. Over many years, this has proved to be a complex task to complete. In the last 20 years, the first big breakthrough that was made on face detection was the usage of Haar-like features. This was done by Paul Viola and Michael Jones in the year 2001. In their experiment, they proposed the usage of Haar-like features for face detection. They also started using an integral image for face detection. Integral image is a method of creating an average of the image without losing details. This lightens the technical requirements for processing the image. This and the usage of Haar-like features made it possible for almost real-time face detection on computers in the year of 2001. When their article was released, this was a leap forward for face detection in computer vision.

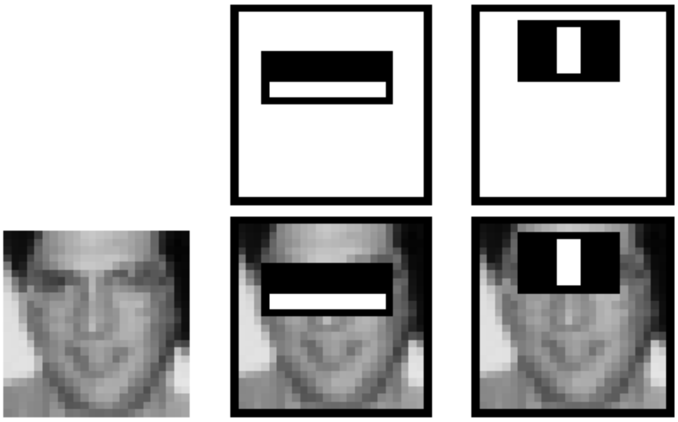

Figure 1.3. Application of Haar-like features on face detection. (Viola and Jones, 2001)

As can be seen in figure 1.3. Haar-like features are a method of finding facial features based on predefined Haar-like objects, objects that detect features in a region of interest based on the difference between adjacent pixels in the image. This proved to be computationally effective while maintaining high accuracy. (Viola and Jones, 2001) (Mita, Kaneko and Hori, 2005)

10 years later a newer method was developed, that has improved accuracy on the cost of a higher computational requirement, but the performance of computers also has increased over time, so it is possible to run computationally more demanding methods of facial detection compared to 2001. This next step in the detection of the face was made in the early 2010s and it was based on the histogram of oriented gradients. This method was already used before for general object detection, but in 2011 (Déniz *et al.*, 2011) this method was applied to face recognition. (Zafaruddin and Fadewar, 2018)

Histogram of gradients, also known as HOGs, are image descriptors are not sensitive to a two-dimensional rotation. They work based on edge detection. Human face and objects, in general, are recognizable and defined because of the edges that are visible within them. For a face, eyes, nose, mouth, and other facial features create local edges.

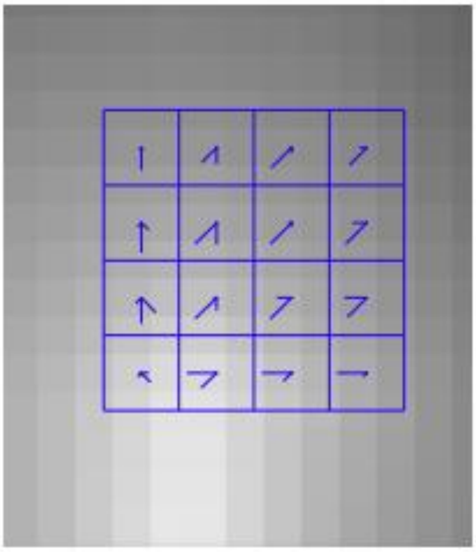

Figure 1.4. Example of histogram of gradients in an 8 by 8 grid. (Déniz *et al.*, 2011)

The example that can be seen in figure 4 shows the working principle of HOG’s. They show the direction in which the light changes from lighter to darker. Thanks to this, it is capable of effectively detecting the face, including in a non-front or partially obstructed situation, either by an obstacle or facial accessories.

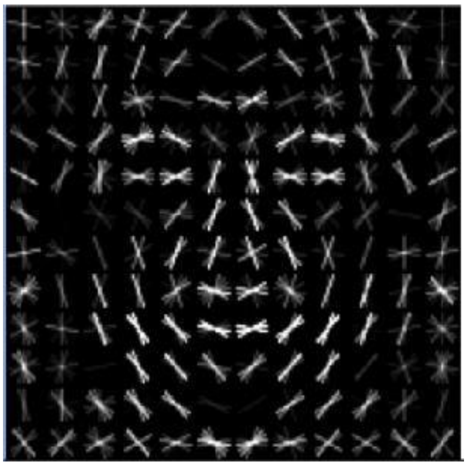

Figure 1.5. Histogram of oriented gradients face representation generated from a large quantity of face image data. (Déniz *et al.*, 2011)

As can be seen in figure 1.5., the lines create an approximate representation of the face, which is used in the detection of the face. This representation is flexible, in the sense that it can be rotated for detecting faces that are upside down or in a different rotation. It also works impressively on the partly turned face, which is an important part of face recognition, since not all images "in the wild" are perfect frontal portraits. Therefore, it is important to cover as variable data as possible for face detection. In a practical comparison between these two methods for facial recognition, HOG-based method proved to be marginally more precise.

"*Based on the experiment before the system can classify and detect the face in many cases and conditions. With six types of condition and five times of trial, obtain the accuracy by 75,33% by using V-J and 80,22% by using HOG. V-J algorithm can detect frontal face very well in images, regarding of their scale, pose, makeup, expression, and illumination, but rather difficult to detect the face who have occlusions like using helm, eyeglass, and mask (...) The HOGs more accurate than V-J for face detection, it can represent local appearance very well.*" (Rahmad *et al.*, 2020)

1.3 Age and gender classification

Another requirement for quality facial anonymisation is to replace the faces with faces of correct age and gender. This will improve the visual quality and integrity of the final image. Therefore, it is important to detect the age and gender of the person represented in the image accurately, to avoid obstructions in the form of incorrect age and/or gender face replaced on to the person in the image. Any analysis and image processing of facial image data is based on the quality of facial detection. If the face is detected correctly, the following tasks done on that data are going to be more exact. In the case of this thesis, the facial detection method chosen is effective and highly right, therefore, this is going to cause a minor problem if any.

Age and gender detection of a person based on their face is not an easy task. Humans are not capable of precise predictions, however, computers are capable of more advanced pattern recognition than humans, if taught properly. Currently, the most effective way for a computer to learn on an image dataset is using convolutional neural network. To begin with, convolutional neural networks are neural networks that have at least a single layer of a mathematical operation called convolution. Result of this is a decrease for data that has to be processed by the image. Convolution helps to achieve this by compressing image data, meaning, that it is capable of decreasing the size of the image without losing essential information about an image. This is important in the cases when there is a limited computational resource and usually, it is limited.

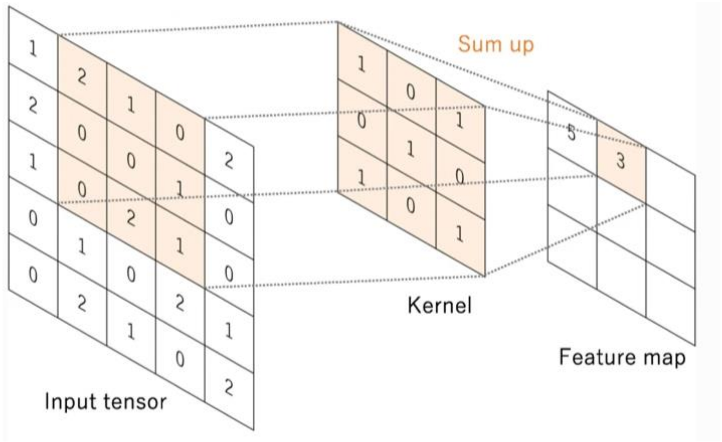

Figure 1.6. Representation of a convolution layer. (Yamashita *et al.*, 2018)

As it can be seen in the example of a convolutional layer in figure 6, one convolution compresses information about 9 pixels into a single pixel. This decreases the amount of data that needs to be processed nine times and amount of convolution layers can be more than one, therefore, we can significantly decrease the amount of time required for the process of learning.

Thanks to the convolutional neural network (CNN) age and gender classification can be done quite efficiently. If there are copious amounts of data available with people of different ages and genders, neural networks can accurately learn different patterns including hidden ones. For a human, this is not an easy task, as we are not capable of processing that many images with such detail. For a computer, where a neural network is built similar to a human brain, meaning, each neuron handles a certain part of an image. To account for the enormous size of images, there are copious amounts of neurons, which, in the manner of a convolutional layer are connected to further neurons. Such a neural network results in an efficient and accurate result of the desired form. (Indolia *et al.*, 2018)

In the age and gender classification experiment by Levi and Hassner (2015), the application of CNN to such task can significantly improve the accuracy of classification, even with a much smaller size of available images. Levi and Hassner (2015) mentioned that it is possible to still significantly improve the results, with a dataset of a larger size. The accuracies that they reported in their article were ~86% for gender classification and 50%

for exact age classification, but with the possible mistake of 1-off, the reported accuracy is ~85%. Such results are impressive, taking into account, that the validation of the results was done on images, which quality was far from perfect – image out of focus, washed-out face in the image or face is not straight at the camera, which creates difficulties with the characterisation of facial features. (Levi and Hassncer, 2015)

1.4 Face collage

For the face replacement to be effective as a tool for facial anonymisation, it must swap the face with a face that does not exist or a face that does not hold details of another person. Multiple available solutions are capable of achieving such results. One of such would be a using a Generative Adversarial Network (GAN). This is a neural network, that is used to generate images.

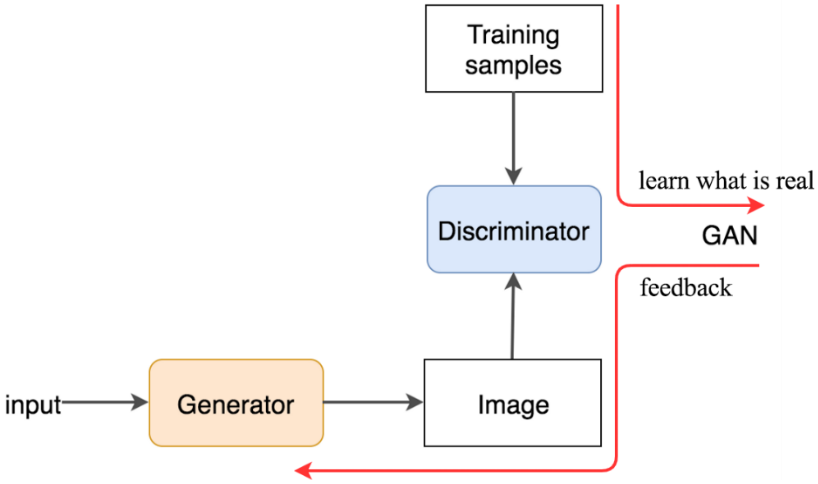

Figure 1.7. Schematic of a Generative Adversarial Network.[1]

The whole functional structure of GAN can be seen in figure 1.7. The main part of such a network is the discriminator. It receives training samples which are real images and compares them to the image generated by the generator. In this comparison discriminator "chooses" which image is real. If the real image is chosen as a real, then the generator gets feedback on its generation and adapts to generate images that look more real. If the generated images are chosen as a real, then it means, that generated image is good. The expected result of such a network is a convergence between generated and natural images – a point when it

[1] https://medium.com/@jonathan_hui/gan-whats-generative-adversarial-networks-and-its-application-f39ed278ef09

is impossible to distinguish which image is naturally taken and which is generated. (Karras, Laine and Aila, 2019)

This method is an extremely effective one. It can potentially lead to a generated face image that looks like a real person, which creates a probability for this system to be potentially ineffective, in the case it generates a face that looks like a real person. The second issue brought by this method is the high computational resource requirement, as it is a neural network, that needs to be taught based on a large facial image dataset. This results in it being ineffective if the result is needed as soon as possible. The third problem would be the requirement for a large quantity for facial image data. If the amount is too small, then it will start to generate images that look like the images from the dataset. These issues of high computational requirement, a large amount of required data and the potential infectivity makes this method of problematic use when under limited computational and time resources, but if these problems are overcome, it can prove to be most effective for use in face replacement, as it will generate faces that look normal, but these faces do not exist meaning they will not breach the privacy of a real person. (Karras *et al.*, 2019)

An alternative method that is capable of creating anonymous faces is facial averaging of substantial amounts of face images. This generates a face without specific details of individual faces. Such a method requires a copious quantity of facial images, but the requirement is not as high as for GANs. This method is also computationally lighter as there is no machine learning involved. This method also proves to be more effective than currently used censorship of eyes. Facial recognition algorithms have become so advanced, that covering eye does not obstruct the capabilities of facial detection and recognition. The facial averaging of facial image features is done on the basis metric distances and the higher amounts of the image are used, the less distinct the details in the resulting average faces

"The algorithm determines the similarity between faces based on a distance metric and creates new faces by averaging image components, which may be the original image pixels." (Newton, Sweeney and Malin, 2005)

1.5 Face Replacement

The last step of automatic facial anonymisation is the replacement of the face. A crucial part of this step is the detection of the face. This is a crucial step because face replacement is done based on face detection, namely, the facial features. Most people's faces are different, as a result, for a successful face replacement we have to warp the position of facial features – eyes, brows, nose, mouth to be at the same location as the target. This is done using 68 facial landmarks. Such a number of landmarks is a standard for facial feature definition. It was chosen due to its popularity and support from the community. Another key factor was that this standard of facial is not the most computational resource-heavy while still maintaining detailed description of facial features. They precisely and efficiently represent the shape of the face and on this basis fitting of one face to another is done. (Zhang, Song and Park, 2014)

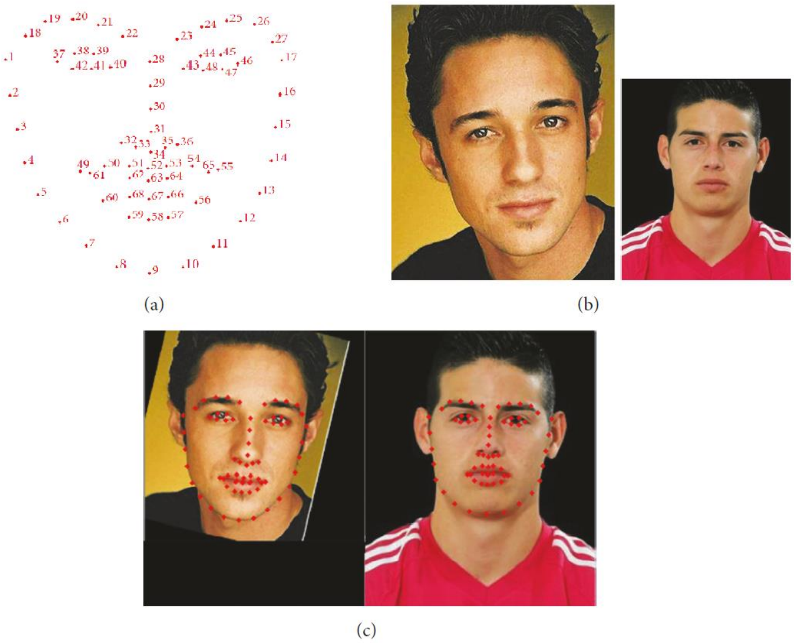

Figure 1.8. Results of applying facial landmarks. (Chen *et al.*, 2019)

As can be seen from figure 1.8., it is possible to align facial landmarks with the face of any position and based on that align different faces to each other. To apply one face on to another, the face we want to warp, according to the coordinates of the landmarks, gets modified – increased or decreased, stretched to be of the same size as the face we are replacing our face on. After face warping has been done, the face replacement is not finished. There are people of different races, there are also different lighting conditions in images. Therefore, it is important to do colour correction in all cases. Since the face that is warped is of the same shape as the base face, it is possible to just average the colour of the base face and the face that we are replacing with. When the face is replaced, the resulting face looks normal and without prior knowledge, it is hard to notice that a change has been made. (Bailer, 2019)

2 Methodology

This thesis proposes an application-based approach to the problem of facial feature anonymisation. This solution is designed to solve the problem of the remaining image content integrity after the censorship that has been performed on the image. By replacing only the substantial facial features instead of creating obstructions for a whole segment of the image, the person's facial features would be hidden, but the picture would not become obscure. The functional scheme of this process can be seen in figure 2.1.

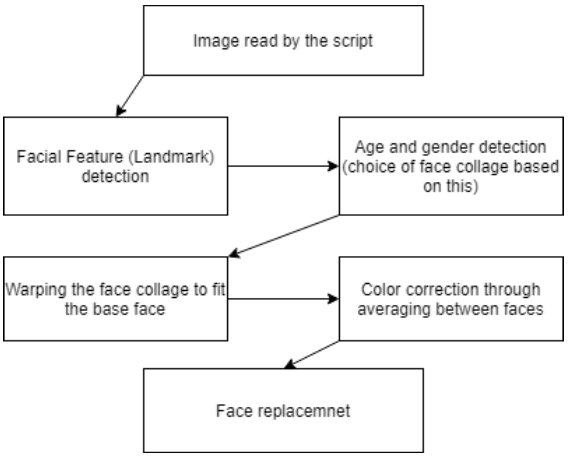
Image read by the script
Facial Feature (Landmark) detection
Age and gender detection (choice of face collage based on this)
Warping the face collage to fit the base face
Color correction through averaging between faces
Face replacemnet

Figure 2.1. The working principle of the automated face anonymisation tool proposed in this thesis.

The order in which the calculations are conducted in the proposed solution can be seen in figure 2.1. The first step for an image to be processed is the loading of this image into the programming environment. Once this task is accomplished the following steps are performed. First, using the facial detection algorithm which utilizes histogram of oriented gradients with the standard of 68 facial landmarks, the coordinates of these facial features are detected and stored for each face separately in a list. After this step, the processing is done on a face by face basis. For each face detected in the image the age and gender is predicted, warping and colour correction between the base face and the face collage is performed and the face collage is applied to the image. These steps are repeated for each face separately and once all faces have been replaced, the anonymised image is returned.

The Python scripts that were used for age and gender detection and face collage creation were taken from the publicly available GitHub repositories. Github is a hosting service for Git version control, which allows for an effective storing and handling of the code. The codes used in this thesis are available under Massachusetts Institute of Technology

(MIT) license and GNU General Public License meaning that this code is provided under no warranty and there are no limitations to possibilities of use of it. For the purposes of this work, it means that the source code can be modified, integrated and adapted for any type of use without limitations.

2.1 Face detection using histogram of oriented gradients (HOG)

The facial detection method used in this thesis was taken from the Python library DLib[2]. Dlib provides a frontal face detector function that utilizes histogram of oriented gradients (HOG). The availability of such a tool inside the library simplifies the application of this method for this thesis.

Histogram of oriented gradients (HOG) has proven to be effective as a descriptor for object recognition in general and its application for facial recognition proved their efficiency in this particular field as well. Previously available methods, that were created and extensively used at the end of the twentieth century assumed that a face can be reconstructed with a linear combination of the calculation descriptions. This approach allowed for the low-performance requirement and acceptable effectivity of the method, but with the advancements of technology and the expansion of available computational resources, such an economic approach to facial recognition was not as necessary. These methods that can be considered classical are still in use because of their good performance both in the detection and in the computational requirement, but there is still room for improvement.

Histogram of oriented gradients is a feature-based method for facial recognition as it detects the face using facial components such as eyes, nose mouth and others. The process of facial recognition using HOG can be divided into three steps. These three steps are scale-space extrema detection, orientation assignment and finally the descriptor extraction. (Albiol *et al.*, 2008)

The first step is done to achieve the invariance towards the scale of the image. This method accomplishes this goal by the means of comparing each point with its neighbours on the same scale and a smaller scale. If the value of this point is either maximum or minimum of all these points then this point is an extrema, meaning, that it is a point where the features of the image change, extrema being the brightest pixels out of all, minima meaning the

[2] http://dlib.net/

darkest pixels. Since the necessary information about the image is left, scale invariance is achieved as the main features of the image are kept while minimal details that would complicate the measurements are stripped away.

The second step is aimed at achieving the orientational invariance of the image. This is done following the extrema from the previous step. Dominant orientation of the image is detected using image gradient information and following this, all image gradients are made relative to this dominant orientation.

The third and the final step is the extraction of the HOG descriptors. In (Albiol *et al.*, 2008) the method for HOG descriptor extraction was based around 25 facial landmarks researchers used. Such a method is effective, but it is heavily dependent on facial landmark localization. This method is very susceptive to occlusions, strong illuminations and a change of the position of the face. In (Déniz *et al.*, 2011) the proposed alternative is to perform the normalization of the image in advance before performing the HOG descriptor extraction. Another important point the authors mentioned is that the use of different sized grids for HOG descriptors can lead to a different amount of details in different points, for example, a smaller sized grid with a higher amount of grids around the eye region would more precisely describe the facial features there. At the same time, a larger grid with fewer grids around the mouth region would still precisely describe the mouth feature, while not requiring such high amounts of computational resources.

Their conclusion was a uniform sampling of HOG descriptors and reduced dimensionality of these descriptors resulted in a significant increase of in facial recognition performance – up to 13% increase. (Déniz *et al.*, 2011)

2.2 Face collage creation

For the creation of a face collage the method of averaging was used. To recall, the face detection method returns the coordinates of facial features. Consequently, the facial image averaging is done by the means of averaging copious amounts of facial image feature coordinate data. The facial feature coordinate data for each corresponding coordinate is arithmetically averaged between all the supplied facial images. Result of this is a facial image that does not contain specific details of a distinct face which allows the face replacement to be done with a face that preserves privacy[3].

[3] https://github.com/alyssaq/face_morpher

2.3 Age and gender detection

Age and gender play an important role in interactions between people. These social interactions are also present in social media. In the case of this thesis, it was important for a face replacement to take place based on age and gender as even minimal differences in this aspect change the perception of people in the eyes of other people around them. (Lynch, 1998) For this reason, it is important to accomplish face replacement on the base of age and gender. Also, a supportive factor is the avoidance of the phenomenon called, uncanny valley, as an improper facial replacement could result in a feeling of discomfort based on inappropriate face swap.

Machine Learning (ML) techniques play a paramount role in the context of pattern recognition for age and gender detection. The latest advances in Graphics Processing Units (GPUs) and the resulting accelerated computation capabilities enabled ML research community to conduct their studies using rather sophisticated artificial Neural Networks (NNs), such as Convolutional Neural Networks (CNNs). The main virtue of CNNs in image processing settings is their contributions to obviating the necessity of performing pre-processing tasks such as smoothing and sharpening, which is due to the convolutions carried out in the course of applying them. A convolution operator finds the relationship between a given number of neighbouring pixels. For each image enhancement technique, a specific convolution kernel needs to be used, which is not required by CNNs, as they are capable of learning and creating the required kernels, in example filters, on their own.

The estimation of age and gender is done by means of a convolutional neural network. The architecture used in the neural network, as can be seen in figure 2.2. , contains 3 convolutional layers and 2 fully connected layers.

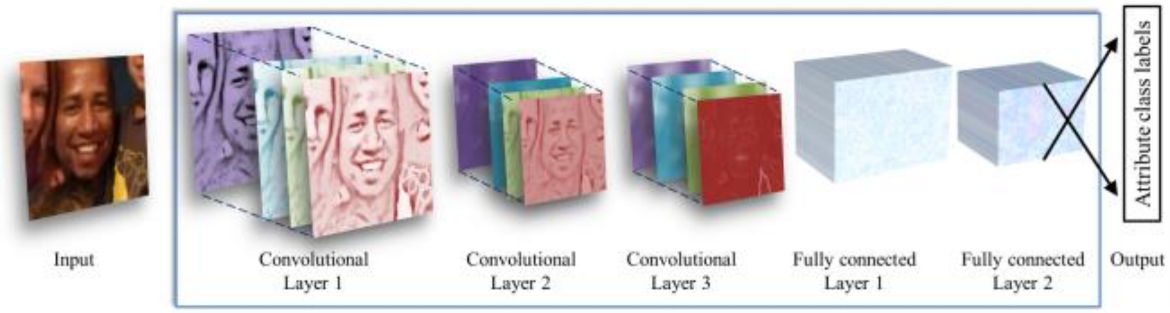

Figure 2.2. The architecture of Convolutional Neural Network used for age and gender classification (Levi and Hassncer, 2015)

One of the many problems that were encountered throughout the development of a CNN for age and gender estimation is the gathering of a large labelled image training set. An easy solution mentioned in the article would be to gain access to private social image repositories, as there is available information about the person gender and age. The problem of this solution is the fact that usually, such images are either private or as it happens on the internet, they are unlabeled. This would force copious amounts of work to be done by manual labelling. Therefore datasets for age and gender detection form real-world images are limited and lacking in size and amounts of data. In the case of using a small dataset on ML, it presents another problem and it is called overfitting. Overfitting occurs when the training dataset is small in size and the neural network does not learn anything from it, but just remembers the data it has processed. This results in potentially high or even perfect accuracy of future predictions when measured on the used dataset, but accuracy drastically declines when applied to the images outside the training dataset. Therefore it is important to take necessary measures in order to avoid overfitting as overfitting makes the resulting model unusable.

The architecture of the network that is used for the age and gender detection is simple: five layers in total out of which there are 3 convolutional layers. Such simplicity in the architecture is justified by the small amount of available labelled data. For a simple architecture, the risk of overfitting is lower. Another aspect was the nature of classifiable data. Instead of tens of thousands of attributes generated by the neural networks used for facial detection, for this task, only 8 classes for age attribute and 2 classes for gender attribute were used.

The measurement of the accuracy of age estimation was done by analysing the accuracy it gives for the exact age-group and when the model predicts the age-group to be 1-off, that is, the true result would be either immediately older or immediately younger group.

For gender estimation the accuracy reported is around ~79%. For age estimation exact prediction resulted in ~45% accuracy, but with a 1-off method of measurement, the reported accuracy reached ~80%. Such result is not a bad one and the explanation provided in the paper is that the main source of mistakes made by the system is an extremely challenging state of the images, such as lighting conditions, low-resolution image, blurred images or make-up on the person. All of these conditions and especially the last one are capable of changing the perception of the human face and therefore the perception of their gender and age, as make-up is often used to improve appearance on the face and masking signs of ageing.

2.4 Face replacement

The method used for face replacement is based on the standard of 68 facial landmarks that define the facial features required for the definition of the face. These facial features are located for both base face that we want to anonymize and the face collage that we are using to cover the base face. Variety of 2D transformations: translation, rotation, scaling and sheering, are used to change the shape of a face collage to fit the base face. This is done to make the shapes of the faces corresponding to each other and place the face collage onto the base face. After the shapes have been matched the final step that needs to be carried out is colour correction. It is done by using gaussian averaging between the face collage and base face. This results in an image where the colour of the face collage fits the base face. In situations where the image contains multiple faces, the face replacement is done to each face separately.

3 Experimental Results and Discussion

3.1 The FairFace dataset

The dataset that was used in this thesis project is the FairFace dataset. (Kärkkäinen and Joo, 2019)[4] This dataset was created to address the problem that most of the existing databases have a strong bias towards Caucasian faces. There is a large amount of data available, but most existing datasets are not balanced when non-Caucasian races are considered. In their research the authors of the mentioned article detected the significant underrepresentation of other races, such as Latinos, etc.. Such a serious bias has previously caused disruptive errors in the software that was trained based on it. Examples of this are the situations when the digital cameras produced by Nikon detected a blink in a group of Asian users due to the characteristic shape of their eyelid. Another example would be the cases of recognition of African American faces as gorillas by the Google Photos algorithm. (Yavuz, 2019)

Contrary to that, the FairFace dataset was designed to avoid any discrimination. The FairFace dataset contains hundred and eight thousand five hundred and one image primarily gathered from the YFCC-100M Flickr dataset (Thomee *et al.*, 2016). The Flicker dataset contains images that are available on internet sources such as Twitter and online newspapers. The FairFace dataset used the racial division into seven categories – White, Black, Indian East Asian, Southeast Asian, Middle East and Latino. (Kärkkäinen and Joo, 2019) The result of such division was an extensive work for quality classification of images towards the list of different races. Kärkkäinen and Joo utilised Amazon Mechanical Turk (MTurk)[5] for labelling of the available dataset as it did not contain the required attributes for the desired image division. The method they used required that 2 out of 3 workers label the image as the corresponding race for it to be accepted as the ground truth, which means that it is the true label of the image. This extensive process resulted in a face attribute collection with the balance concerning race, gender and age.

This dataset was chosen for this project due to the goal of creating an automated all-inclusive face anonymisation tool. For this tool to be effective on a large variety of people of most races, ages and gender it is required to cover as many different cases as possible. It

[4] https://github.com/joojs/fairface

[5] https://www.mturk.com/

was necessary to filter facial image data by age and gender for the generation of average face collages with the goal of similar age and gender replacement. It was a necessity for the dataset needed to cover these attributes. The FairFace dataset covered many attributes including these, which contributed to the choice of the dataset being in favour of FairFace.

This dataset was used for average face collage creation. It was done with the idea of generating a face that would be maximally fitting for all people to the extents of the possibility. If the average face is made from people of all races in a balanced manner, then by containing features of all races the resulting face will discard all of these details. This removal of details is beneficial to the aim of this thesis as face anonymisation is improved in the case of the removal of facial details, be that facial expression or racial features.

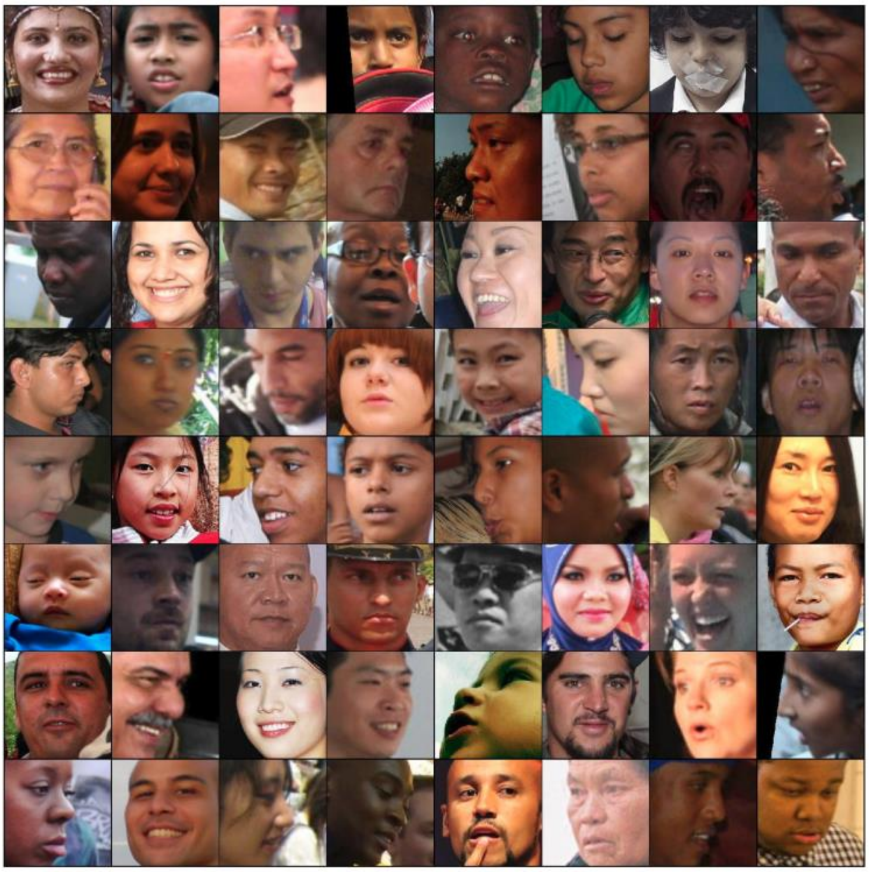

Figure 3.1 Example of the FairFace dataset facial images. (Kärkkäinen and Joo, 2019)

The FairFace dataset contains a high diversity of facial images, both in quality of the image and the face of the people. This can be observed in figure 3.1. In this figure, people from all the aforementioned seven races. Such diversity in quality and faces is beneficial as it allows for the generation of faces with even fewer details. It is important to have balance in the quality of images, otherwise, the resulting average face might be removed of details to such extent it would result in a face that would not look human-like and that would cause a different kind of problem during face replacement, it would cross the line and delve into the uncanny valley.

„The uncanny valley (UV) effect refers to an eerie feeling of unfamiliarity people get while observing or interacting with robots that resemble humans almost but not quite perfectly.“ (Palomäki *et al.*, 2018)

This effect is observable not only in the field of robotics but to the field of visual representation of human and their faces, therefore it is important to not cross this line for the generation of the average face collage.

3.2 Automated face anonymisation results

The main goal of the solution developed in the scope of this thesis was achieved as a result. These results are not always perfect, but in most situations, the result is quite satisfactory.

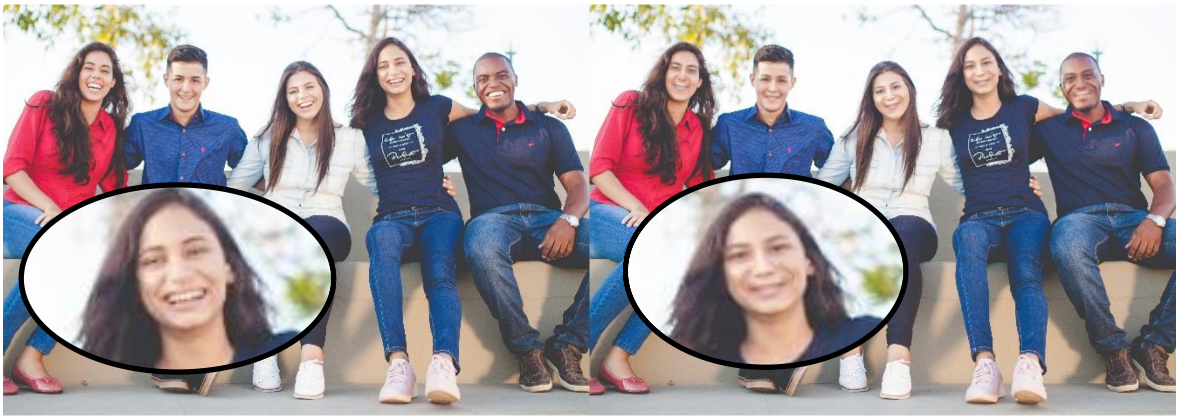

Figure 3.2. Comparison of the original image (on the left) (Photo by Naassom Azevedo on Unsplash) and the resulting anonymised image (on the right side).

As can be deduced from figure 3.2. the processed image has face replacement applied, without ruining the appearance of the image. On the image on the right, the facial expressions have been removed and most of the facial features – eyes, mouth and brows replaced. For this image, the desired result has been achieved. Face replacement-based image anonymisation without disrupting the content of the image.

In cases of a good image such as the image in figure 3.2, where people are looking towards the camera the quality of face replacement is positive. Not all images fall under the category of a good image.

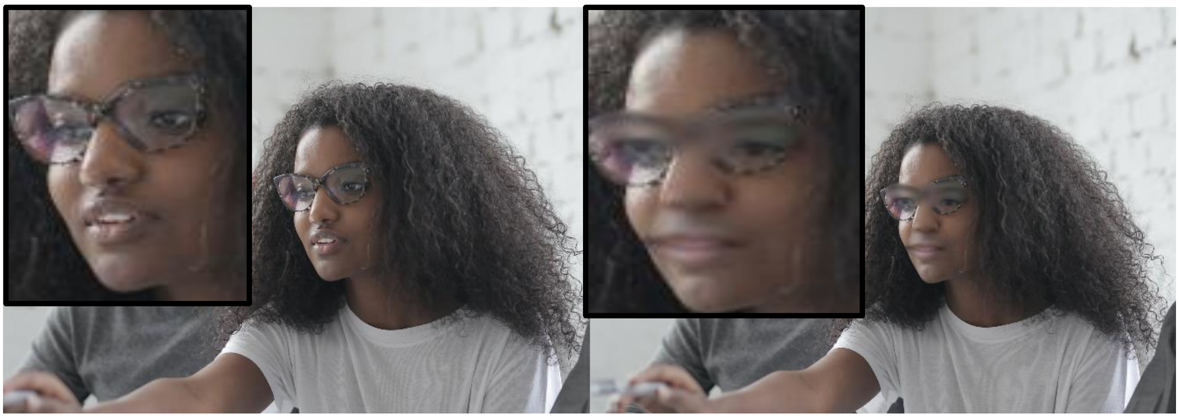

Figure 3.3. Comparison of the original image (on the left) (Photo by Andrea Piacquadio from Pexels) and the resulting anonymised image (on the right side).

The resulting image can be seen in figure 3.3. on the right side in the case of a bad face replacement. The person on the right is not facing towards the camera and there is an obstruction on their face in the form of eyeglasses. Their face was detected, as the eyes can be seen through the glasses and the face replacement was made, but the result is not the best. Especially following the fact, that a part of their eye is still visible even with the face replacement. This is not the worst possible case, as there might be cases resulting in the face not being detected, such as bad lighting conditions or angle of the face towards the camera is too high. Such cases are highly probable in the real-world situations, but figure 3.3 works as a visualisation of what could cause problems and what a bad case looks like, even if the case is not the worst possible in the wild.

3.3 Automated face anonymisation effectivity

The main analysis was to measure the effectiveness of automated facial anonymisation usage for the preservation of the persons' privacy. For measuring such effectiveness a small dataset of 50 images was collected. Dataset covered 10 people with commonly recognizable faces with 5 facial images of each. 4 images were used as a test comparison and 1 image was used as a facial identification base. That face was afterwards replaced to see if there was a change in ability for technology-driven methods to recognize the face. The method used for facial comparison is Amazon Rekognition, which provides an

AI-driven face comparison to determine what is the possibility in percentage that the face belongs to the person in the image.

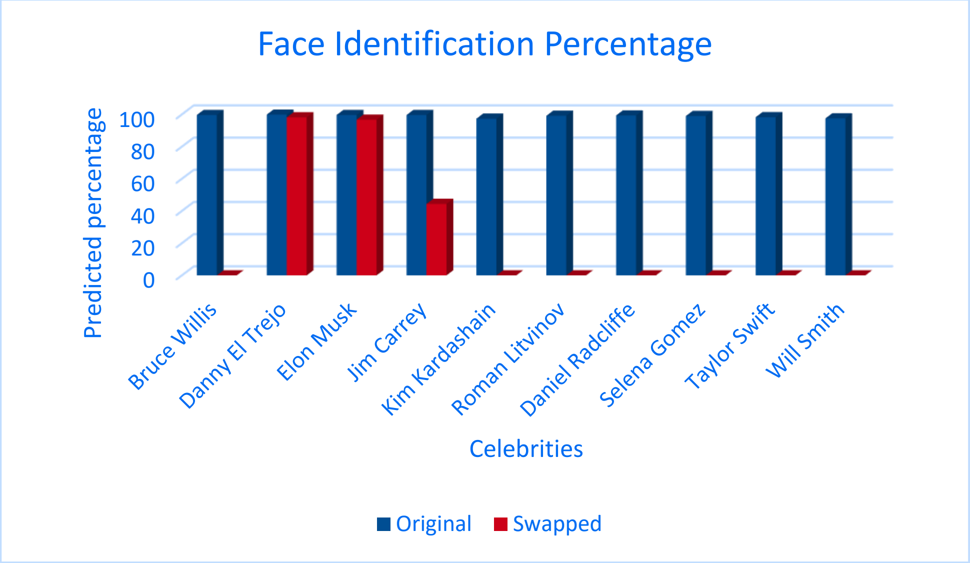

Figure 3.4. Graph of face identification prediction percentage

The graph in figure 3.4 contains data about the confidence that the face shown in an image corresponds to the person whose face is given as base. On the y-axis is the graph the percentage can be seen. On the x-axis in the graph, the people whose faces were analysed can be seen. For each person, there are two bars in the graph. Dark blue bar corresponds to the confidence that the person's real face is that persons real face. Red bar corresponds to the confidence that the persons swapped face are the person real face. In the results, except for 3 celebrities – Danny El Trejo, Elon Musk and Jim Carrey, swapped faces were not detected as a face of the celebrity. In the case of Jim Carrey in 2 images out of 4, his face was detected when comparing to the swapped face. In the 2 cases when the face was detected, confidence value was below 90%. For Danny El Trejo and Elon Musk, the face replacement did not fully cover the features of the original face, resulting in a detection of the original face. The dataset used for this analysis is located in the appendix as Figure 4.1

3.4 Created face collage similarity

Next analysis that was done was on the generated face collages. The idea behind this analysis is that the average faces would be most similar between age and gender groups, as the approximate location of facial features around which the averaging is done stay the same. These features would be eyes, nose and mouth. If large enough quantity of facial images, then all details about the face are lost and face collages will end up looking the same. Face collages can be seen in the appendix as Figure 4.2

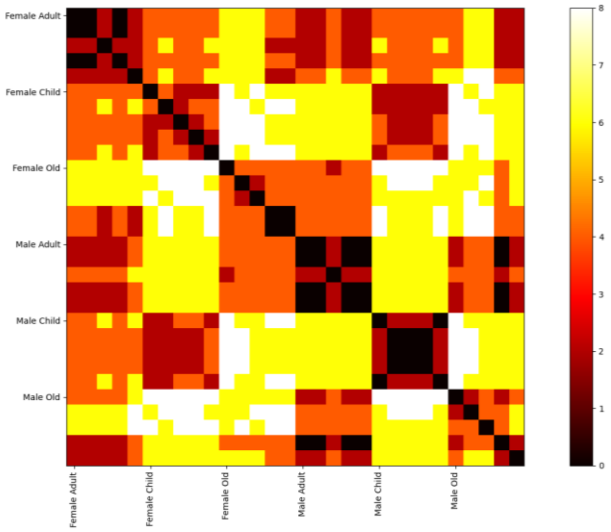

Figure 3.5. Heatmap showing the similarities between all face collages.

Heatmap in figure 3.5 shows data about the similarity between all face collages. A comparison was also done for a face collage against itself, the diagonal from top left to bottom right is the darkest colour, as the image itself is identical to itself. On y and x-axis, the images are divided into groups of 5, as there were 5 images per each age and gender group. In the heatmap, white corresponds to the least similarity and darkest colour corresponds to identical images.

3.5 Automated face anonymisation algorithm complexity

The complexity of the algorithm shows how much the time required for calculations increases with the increase of data to be processed. This is an important characteristic for any algorithm as it shows its effectivity and how well it scales for large-scale applications. Analysis of algorithm complexity was done by increasing face quantity and increasing the scale of the image. Example of the images for determining the algorithm complexity can be seen in the appendix as figure 16

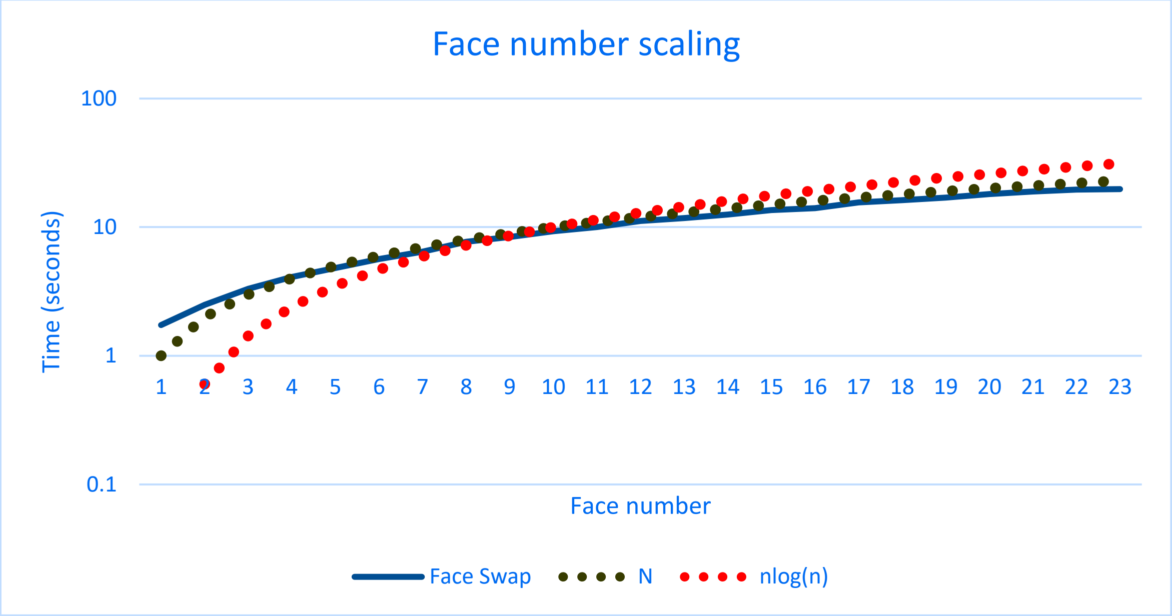

Figure 3.6. Graph of calculation time increase over the increase of face quantity.

The graph in figure 3.6 contains data about the time required for the automated face replacement solution to process an image against the number of faces in the image. The y-axis in the graph is in logarithmic scale and it corresponds to the time required for the processing of a single image. The x-axis is the number of the face in the image. In the graph, there are 3 lines. The full line is the line corresponding to the solution proposed in this project. Dotted lines are used for determination of algorithm complexity – how much the calculation time increases with the increase of processed data. By comparing the full line with the dotted line, it can be deduced that the complexity of the algorithm is linear, as the dotted line corresponding to N is overlapping with the full line.

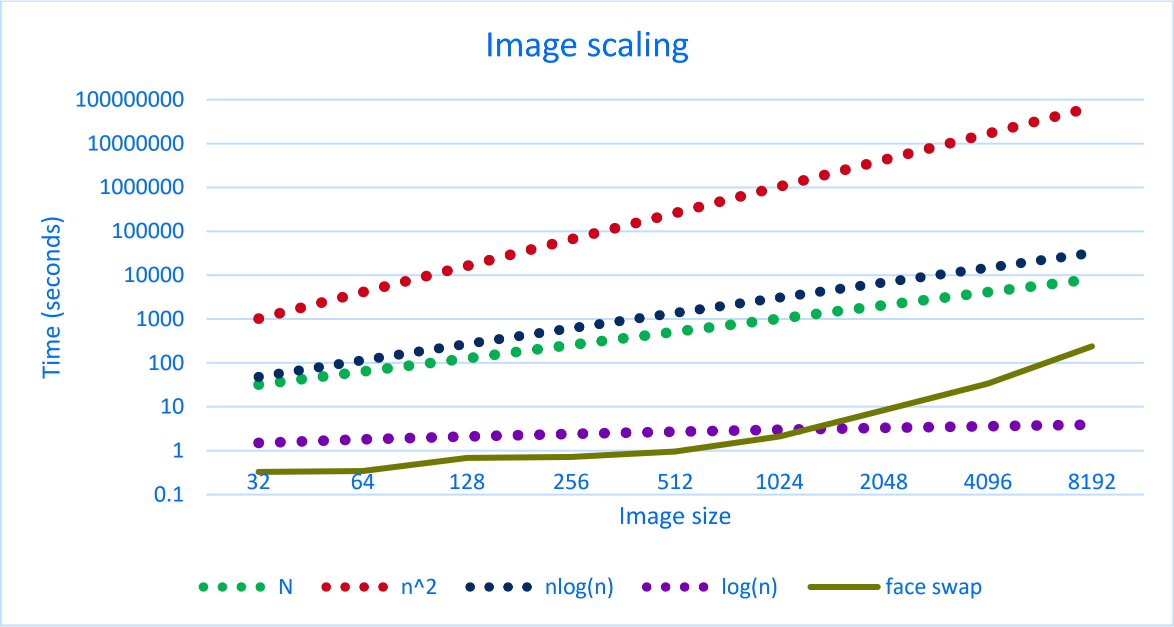

Figure 3.7. Graph of calculation time increase over the increase of image resolution.

The graph in figure 3.7 contains data about the time required for the automated face replacement solution to process an image against an increase in the resolution of the image to be processed. The y-axis in the graph is in logarithmic scale and it corresponds to the time required for the processing of a single image. The x-axis is the resolution of the image. For testing, it ranged from 32x32 to 8192x8192. There are 5 lines can be seen in the graph. The full line is the line corresponding to the solution proposed in this project. Dotted lines are used for determination of algorithm complexity – how much the calculation time increases with the increase of processed data. By comparing the full line with the dotted line, it can be deduced that the complexity of the algorithm varies according to the size of the image. In the beginning, the slope of the full line is approximately the same as log(n) line, after 512x512 the slope of the line increases to be corresponding to the slope of the line n^2. This leads to the complexity of the algorithm being logarithmic until 512x512, afterwards it is to the power of 2.

3.6 Discussion

The solution that was made in this thesis gave impressive results in visual analysis. The visual part of the image is only a small part of the social media privacy problem. As social media profiles are exposed to data mining networks it is important to test the effectiveness of the solution computationally, that is by using facial recognition and comparison tool. Following the frontend part of the solution, which is the received result, it is also important to measure the performance of the algorithm, to analyse its efficiency and possibly detect computational issues that could arise in the case of unexpected situations.

As can be seen from the main test for the effectiveness of the face anonymisation tool in the graph in figure 3.4, in most cases the method proposed in this thesis proves to be effective. In some cases, it gave a minute result. Judging from the celebrity image with the face swapped, in the case of Danny El Trejo and Elon Musk the face swap did not work perfectly, as some part of the eyelids and other important facial features was left and that could provide identification basis for the facial comparison technology. Overall, the result proved to be effectively working in more than 70% of the cases.

The following test was done on the visual similarity of average face collages. Looking at figure 3.5, the conclusion that can be drawn from heatmap is that face collages in the same age and gender group are highly similar to each other and images of the same age or gender group are more similar to each other than images of other age or gender group.

Analysis of the algorithm complexity was the following task. It was done in 2 parts. To test the algorithm effective response to an increase in the number of faces and an increase in the resolution of the image. As shown in figure 3.6, the complexity of the face anonymisation algorithm over the increase of face quantity is linear, as can be seen from the comparison with the dotted line N. This shows that the code is effective when it comes to an increasing amount of faces with the complexity of *O(n)*. This means that the functionality will not drastically slow down when given large amounts of faces.

Looking at the graph in figure 3.7, the complexity of the face anonymisation algorithm over the increase of image resolution can be divided into two stages. The first stage until image size 512x512, during which the complexity angle wise corresponds to *log(n)* dotted line. After 512x512, the second stage can be observed, during which the angle of the face swap line increases to be the same as n^2 dotted line. This means that the algorithm complexity when it comes to image resolution increase is *O(log(n))* until the image size of 512x512, afterwards the complexity is $O(n^2)$, showing a drastic increase in requirement of computation resources. Potential causes of this could be the performance of the computer used to conduct this test. When it reached its computational limit, the time required for computations increased, as it was not capable of processing such high amounts of data in the available processing power or handling such amounts of data in the memory.

4 Conclusion and Future Work

4.1 Conclusions

The problem of privacy on social media is an everlasting challenge, as people are required to balance between hiding all information and sharing too much, which can lead to dire consequences. One of the important aspects of privacy challenges on social media is image sharing. It can lead to unwanted exposure or a leak of confidential data by means of abusing facial features, that might be used for biometric authentication.

The solution proposed in this thesis is to use face replacement to preserve the privacy of images shared online. The technology required to power this solution has been advancing at an increased pace which motivates its usage for such solutions. Automated face anonymisation is potentially more effective than currently existing censorship methods, as they change all the important facial features, not just eyes, but also nose and mouth. Such a method is also potentially less obstructive towards the contents of the image, by not blurring out or hiding parts of the image, but just replacing certain parts, which could prove to be a privacy leak.

The results of the proposed solution were measured both in the effectiveness of the method and in the efficiency of the solution. According to the measurements done on facial recognition and comparison before and after facial anonymisation, the effectivity of the code is higher than 70% at the current state. This means that it is effective at keeping the privacy of the person whose face was anonymized. A potential solution for increasing the effectiveness would be applying the solution twice to increase the effectiveness of the solution.

The efficiency of the code was estimated through measuring the time required to run the code with the increase of the number of the faces and also the time required to run the code with the increase of the resolution of the image. Increase of the amount of the faces proved the complexity of the algorithm to be linear, that is, the time required to run the solution increases linearly based on the amount of the faces in the image. For the increase of the resolution of the image, while the resolution of the image was not too big, the time required almost did not increase and when the resolution became too high, the limit of computational resources was hit and time required to run the code increase by the power of 2, meaning, that if the dimensions of each side increase 2 times, the time required increases

4 times. A potential solution for this would be using a more powerful computational machine, which would not hit its limit so early.

4.2 Future Work

Future aspects of this solution that could improve the effectiveness of current solution would be using a different method for face detection. The current method is bound to 68 points and it must have all 68 points for the face to be detected. The improvement would be to use a more versatile solution that detects the face more effectively and is not based around a certain amount of point. This would lead to it being more effective in a larger quantity of cases, instead of just frontal faces, as well as improving other modules of the solution which are based on facial detection, such as face replacement and age and gender detection. Another way to improve the code would be to use facial image generation for face anonymisation instead of averaging massive quantities of the facial images. This improvement would create a large diversity of faces to swap and if properly configured on a powerful machine it could generate faces real-time as soon as there is a request for face anonymisation. If such improvements were implemented, this method would change the world of censorship and it would be impossible to know if the face on the image is original or anonymised.

REFERENCES

Grey, Dean and Nigl, Alfred. (2019). The Impact of New Privacy Laws (GDPR) on Social Media Platforms.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Harding, D., 2019. Facial Recognition: When Convenience and Privacy Collide. [online] Securitymagazine.com. Available at: <https://www.securitymagazine.com/articles/90533-facial-recognition-when-convenience-and-privacy-collide> [Accessed 14 May 2020].

Albiol, Alberto *et al.* (2008) 'Face recognition using HOG-EBGM', *Pattern Recognition Letters*, 29(10), pp. 1537–1543. doi: 10.1016/j.patrec.2008.03.017.

Bailer, W. (2019) 'Face Swapping for Solving Collateral Privacy Issues in Multimedia Analytics', in Kompatsiaris, I. et al. (eds) *MultiMedia Modeling*. Cham: Springer International Publishing, pp. 169–177.

Bitouk, D. *et al.* (2008) 'Face swapping: Automatically replacing faces in photographs', *ACM Transactions on Graphics*, 27(3). doi: 10.1145/1360612.1360638.

Bruce, V. and Young, A. (1986) 'Understanding face recognition', *British Journal of Psychology*, 77(3), pp. 305–327. doi: 10.1111/j.2044-8295.1986.tb02199.x.

Chen, D. *et al.* (2019) 'Face swapping: Realistic image synthesis based on facial landmarks alignment', *Mathematical Problems in Engineering*, 2019, pp. 1–12. doi: 10.1155/2019/8902701.

Déniz, O. *et al.* (2011) 'Face recognition using Histograms of Oriented Gradients', *Pattern Recognition Letters*, 32(12), pp. 1598–1603. doi: 10.1016/j.patrec.2011.01.004.

Gutta, S. *et al.* (2005) 'United States patent 6,959,099 B2 - METHOD AND APPARATUS FOR AUTOMATIC FACE BLURRING', 2(12).

Ichikawa, H., Kanazawa, S. and Yamaguchi, M. K. (2011) 'Finding a face in a face-like object', *Perception*, 40(4), pp. 500–502. doi: 10.1068/p6926.

Indolia, S. *et al.* (2018) 'Conceptual Understanding of Convolutional Neural Network- A Deep Learning Approach', *Procedia Computer Science*. Elsevier B.V., 132, pp. 679–688.

doi: 10.1016/j.procs.2018.05.069.

Kärkkäinen, K. and Joo, J. (2019) ‘FairFace: Face Attribute Dataset for Balanced Race, Gender, and Age’. Available at: http://arxiv.org/abs/1908.04913.

Karras, T. *et al.* (2019) ‘Analyzing and Improving the Image Quality of StyleGAN’. Available at: http://arxiv.org/abs/1912.04958.

Karras, T., Laine, S. and Aila, T. (2019) ‘A style-based generator architecture for generative adversarial networks’, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2019-June, pp. 4396–4405. doi: 10.1109/CVPR.2019.00453.

Levi, G. and Hassncer, T. (2015) ‘Age and gender classification using convolutional neural networks’, *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2015-Octob, pp. 34–42. doi: 10.1109/CVPRW.2015.7301352.

Lynch, S. A. (1998) ‘Who supports whom? How age and gender affect the perceived quality of support from family and friends’, *Gerontologist*, 38(2), pp. 231–238. doi: 10.1093/geront/38.2.231.

Mahajan, S., Chen, L. J. and Tsai, T. C. (2017) ‘SwapItUp: A face swap application for privacy protection’, *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 46–50. doi: 10.1109/AINA.2017.53.

Mansfield-devine, S. (2016) ‘The battle for privacy’, *Network Security*. Elsevier Ltd, 2016(6), pp. 11–15. doi: 10.1016/S1353-4858(16)30058-7.

Mita, T., Kaneko, T. and Hori, O. (2005) ‘Joint Haar-like features for face detection’, *Proceedings of the IEEE International Conference on Computer Vision*, II(May 2014), pp. 1619–1626. doi: 10.1109/ICCV.2005.129.

Newton, E. M., Sweeney, L. and Malin, B. (2005) ‘Preserving privacy by de-identifying face images’, *IEEE Transactions on Knowledge and Data Engineering*, 17(2), pp. 232–243. doi: 10.1109/TKDE.2005.32.

Nirkin, Y. *et al.* (2018) ‘On face segmentation, face swapping, and face perception’, *Proceedings - 13th IEEE International Conference on Automatic Face and Gesture Recognition, FG 2018*, pp. 98–105. doi: 10.1109/FG.2018.00024.

Palomäki, J. *et al.* (2018) ‘Evaluating the replicability of the uncanny valley effect’, *Heliyon*, 4(11). doi: 10.1016/j.heliyon.2018.e00939.

Rahmad, C. *et al.* (2020) ‘Comparison of Viola-Jones Haar Cascade Classifier and Histogram of Oriented Gradients (HOG) for face detection’, *IOP Conference Series: Materials Science and Engineering*, 732(1), pp. 0–8. doi: 10.1088/1757-899X/732/1/012038.

Saroha, R. *et al.* (2013) ‘Review paper on Overview of Image Processing and Image Segmentation’, *International Journal of Research in Computer Applications and Robotics*, 1(7), pp. 1–13.

Senthil Kumar, N., Saravanakumar, K. and Deepa, K. (2016) ‘On Privacy and Security in Social Media - A Comprehensive Study’, *Physics Procedia*. Elsevier Masson SAS, 78(December 2015), pp. 114–119. doi: 10.1016/j.procs.2016.02.019.

Tankard, C. and Pathways, D. (2016) ‘What the GDPR means for businesses’, *Network Security*. Elsevier Ltd, 2016(6), pp. 5–8. doi: 10.1016/S1353-4858(16)30056-3.

Thomee, B. *et al.* (2016) ‘YFCC100M: The new data in multimedia research’, *Communications of the ACM*, 59(2), pp. 64–73. doi: 10.1145/2812802.

Viola, P. and Jones, M. (2001) ‘Rapid object detection using a boosted cascade of simple features’, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 1(February). doi: 10.1109/cvpr.2001.990517.

Wieringa, J. *et al.* (2019) ‘Data analytics in a privacy-concerned world’, *Journal of Business Research*. Elsevier, (May), pp. 0–1. doi: 10.1016/j.jbusres.2019.05.005.

Yamashita, R. *et al.* (2018) ‘Convolutional neural networks: an overview and application in radiology’, *Insights into Imaging*. Insights into Imaging, 9(4), pp. 611–629. doi: 10.1007/s13244-018-0639-9.

Yavuz, C. (2019) ‘Machine Bias Artificial Intelligence and Discrimination Master of Laws in International Human Rights Law View project Master of Laws View project’, (June). doi: 10.13140/RG.2.2.10591.61607.

Zafaruddin, G. M. and Fadewar, H. S. (2018) ‘Face recognition using eigenfaces’, *Advances in Intelligent Systems and Computing*, 810, pp. 855–864. doi: 10.1007/978-981-13-1513-8_87.

Zhang, X., Song, J. and Park, J. Il (2014) ‘The image blending method for face swapping’, *Proceedings of 2014 4th IEEE International Conference on Network Infrastructure and Digital Content, IEEE IC-NIDC 2014*, pp. 95–98. doi: 10.1109/ICNIDC.2014.7000272.

Face collage creation technology – face averaging: https://github.com/alyssaq/face_morpher

What is a Generative Adversarial Network: https://medium.com/@jonathan_hui/gan-whats-generative-adversarial-networks-and-its-application-f39ed278ef09

MIT license: https://mit-license.org/

Appendix

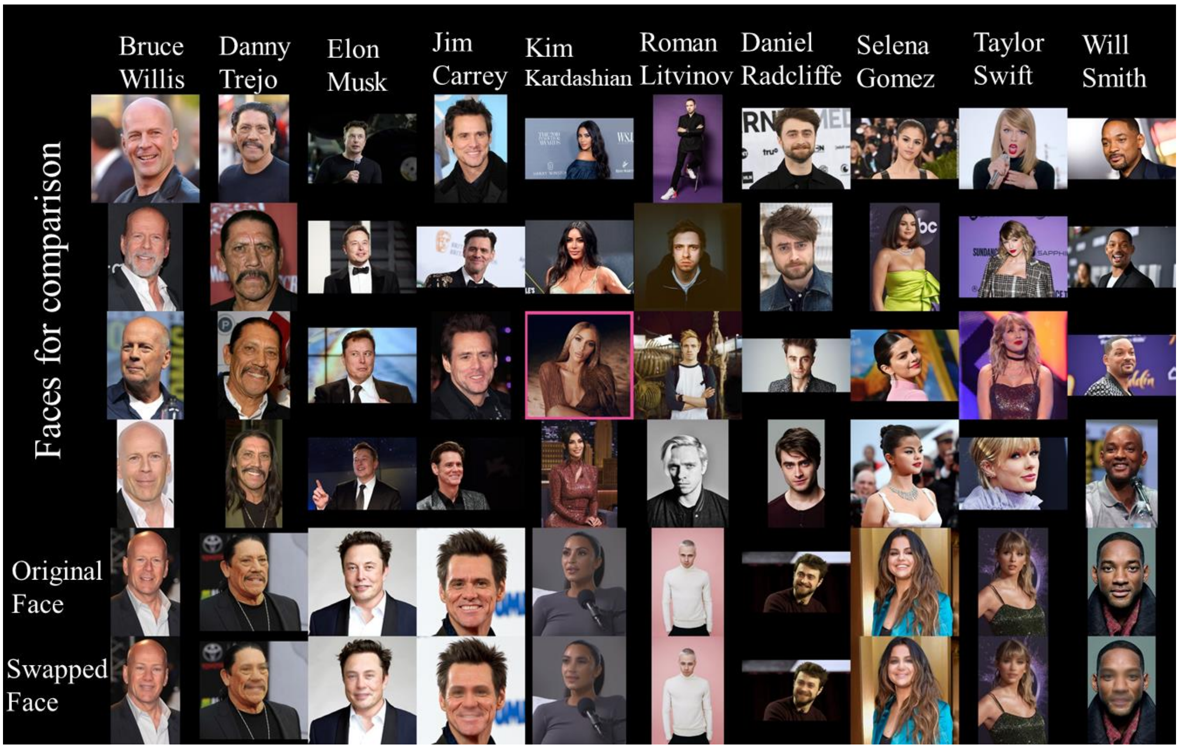

Figure 4.1 – Identity test dataset collage

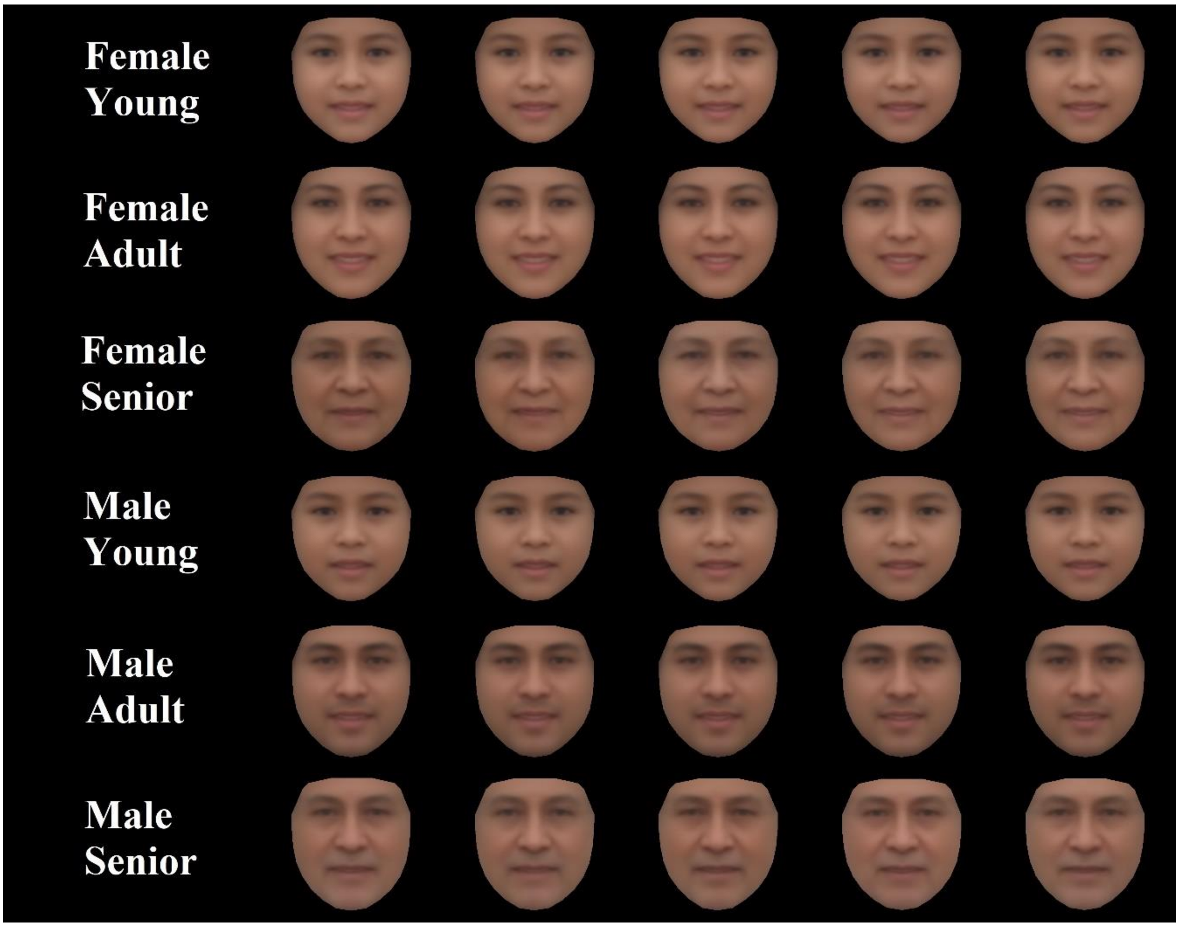

Figure 4.2 – Face collage dataset collage

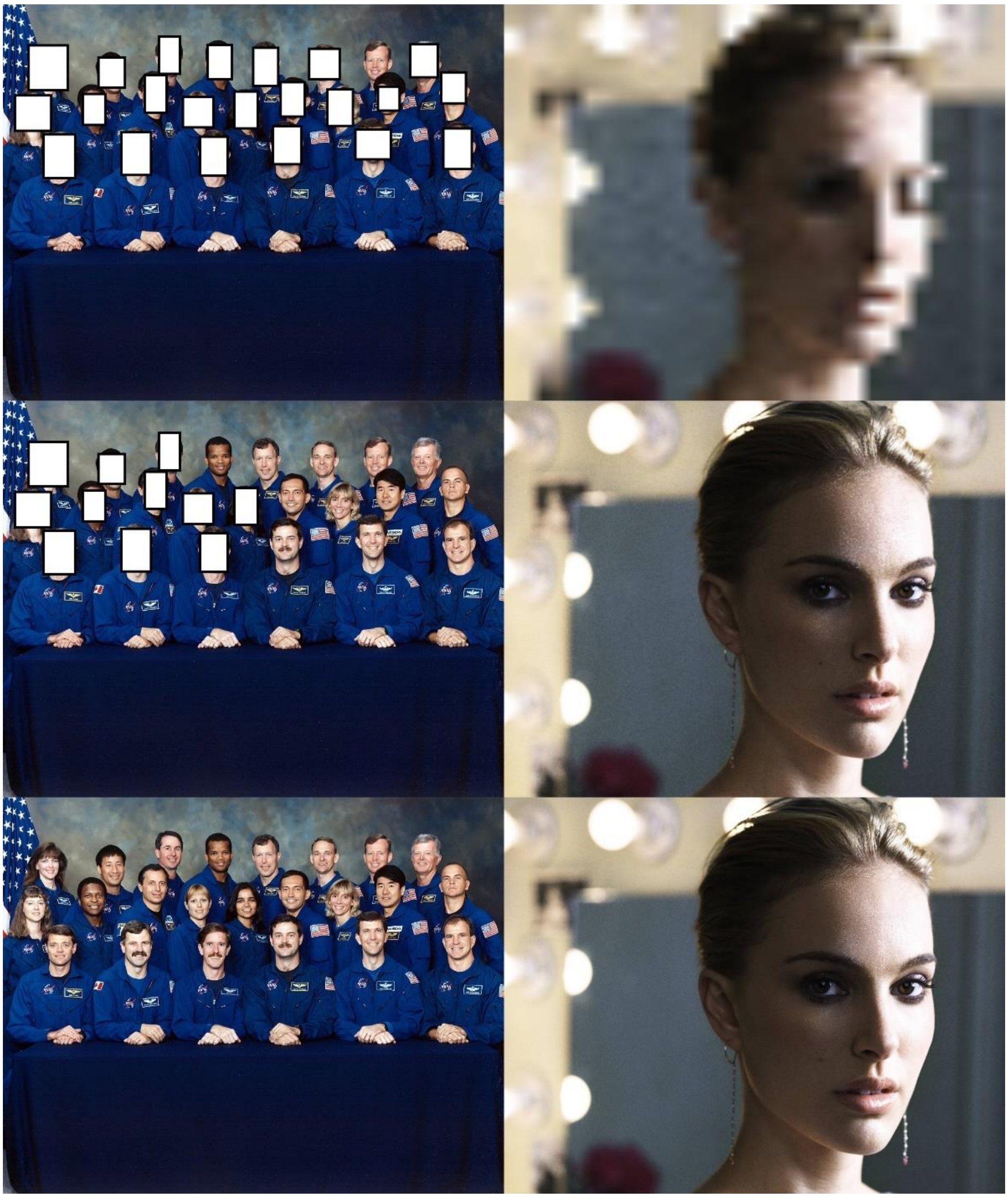

Figure 4.3 – Examples of images used for algorithm complexity testing

NON-EXCLUSIVE LICENCE TO REPRODUCE THESIS AND MAKE THESIS PUBLIC

I, Maris Popens,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

Privacy preserving using face replacement-based image anonymisation tool,

(*title of thesis*)

supervised by Doğuş Karabulut & Prof. Gholamreza Anbarjafari.

(*supervisor's name*)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Maris Popens

20/05/2020