FACIAL IMAGE SUPPRESSION TO MAINTAIN DATA PRIVACY

A Project Report

for the fulfilment

of

J-Component Project

of the course

Network and Information Security – ITE4001

By

SOUBHIK SINHA (19BIT0303)

TUSHAR KUMAR B P (19BIT0358)

Under the guidance of

Dr. (Prof.) USHA DEVI G

HoD (Information Technology)

Slot : E1+TE1

VIT®

Vellore Institute of Technology

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

Fall Semester , 2022-2023

Facial Image Suppression to Maintain Data Privacy

Soubhik Sinha[1] , Tushar Kumar B P[2]

[1,2] Department of Information Technology, School of Information Technology and Engineering (SITE), VIT University , Vellore, Tamil Nadu – 632014, India

***Abstract* – Facial-based identification is utilised in a variety of contexts, from the identification of a person based on still photographs in a passport or identity card to the identification of a person based on face images taken by a surveillance system without the individual's consent. Privacy may be violated in many application contexts, particularly in video surveillance. Contrary to other body parts, the face may easily be recognised in photographs. Traditional methods of face picture de-identification are ineffective in concealing identity or lower the quality of education. In this paper, a technique for suppressing original face photos using blended facial composites was devised. With this technique, the original face's key features may be seen but its identity is hidden. There is a need for the research and development of multimodal concealing methods that simultaneously hide, remove, or replace various types of personal identifiers (face, gesture, gait) from multimedia content due to recent advancements in multi-sensor acquisition and recording devices and remote surveillance systems. Multimodal suppression is a problem that hasn't been fully solved.**

***Keywords* – de-identification , identifiers , multi-sensor acquisition**

I. INTRODUCTION

In the most recent years, there has been a dramatic increase in the amount of data shared online. With the advent of the Internet, it has become necessary to stop hackers and other adversaries from accessing private information. In this research, we want to put into practise a way for applying de-identification techniques to anonymize facial images. There are several ways to do this, including blurring the image, obscuring certain facial traits, and altering facial features by adding noise calculated by removing average values of specific face attributes, including skin colour and shape. To lessen the granularity of our image data, we'll use modified averaging over images. Additionally, we will compare our approach an industry standard—black-boxing—on the basis of image de-identification. The Kaggle Face Recognition Dataset is what we 've utilising. Facial recognition technology has recently been used by a large number of software MNCs for services like surveillance, photo tagging, preserving identification data, etc. Therefore, the topic of whether our identities are secure from sensitive data leaks and if the firms are adhering to adequate safety requirements has emerged. With Facebook's (now Meta) implementation of tagging individuals in uploaded photos, the government's installation of surveillance cameras, CCTV cameras in banks and other institutions, etc., image recognition has become an essential component of any organization's operations. Therefore, it is necessary to privatise the data in order to safeguard it from unreliable sources.

II. LITERATURE REVIEW

[1] Compression Independent Reversible Encryption for Privacy in Video Surveillance : Privacy rights are starting to become more important as video monitoring becomes a crucial component of our security architecture. The main issue is the fact that video surveillance devices are being used to monitor ordinary people who are not suspects and store those recordings. This approach of recording everything and processing it afterwards has significant privacy problems. Similar privacy concerns occur when highway traffic is frequently filmed by surveillance cameras while car tags are being read. Security professionals may have a valid reason to study the footage, thus the solution of blurring or blackening the sections of the film is not acceptable to them. Contrarily, it is an invasion of privacy to leave films featuring identifiable individuals and cars out in the open. The issue can be solved by selectively encrypting the video's elements that reveal identity (such as faces and

vehicle tags) in surveillance applications. A video can have portions that can be encrypted for privacy while still allowing decryption for future legitimate security needs.

[2] Facial expression preserving privacy protection using image melding : Social networking sites like Meta presently allow for the sharing of a huge number of photographs. These images typically show persons, and if they are shared without their consent, they may breach their right to privacy. Blurring is one form of visual privacy protection that is applied to people's faces without their consent in order to address this privacy risk. However, this may also ruin the context of the image if some persons are filtered while others are not. Missing facial expressions makes it harder to understand the image.

[3] Say cheese! Privacy and facial recognition : There is a need to develop rules for handling data and securing it because there are so many photographs uploaded online and so many businesses using this data for their services. The many rules covered by European data protection legislation are discussed in this essay.

[4] Efficient Privacy-Preserving Facial Expression Classification : In this research, an effective method for client-server facial expression classification (FEC) with privacy preservation (PP) is proposed. The server maintains a database and provides the clients with a classification service. The customer employs the service to classify the subject's facial expression (FaE). The client and server are both mutually untrustworthy parties, and they desire to carry out the classification without disclosing their inputs to one another. The current works, which rely on computationally expensive cryptographic operations, are contrasted with the lightweight methodology proposed in this paper, which is based on the randomization method. The popular JAFFE and MUG FaE databases are utilised to validate the proposed algorithm. Experimental findings show that the suggested method performs similarly to earlier research in terms of performance. In contrast to the current homomorphic cryptography-based technique, it protects input privacy while increasing computational complexity by 120 times and communication cost by 31%.

[5] Privacy-Preserving Face Recognition : Over the last several years, biometric methods have developed into a trustworthy method of authentication that is increasingly used in a variety of application domains. Due to its unobtrusiveness and usability, face recognition in particular has attracted the attention of the research community. No special sensors are required, and easily accessible, high-quality photos may be utilised for biometric authentication. Two application situations served as the primary motivators for the creation of new biometric face-recognition systems - Modern electronic passports and identity cards have a chip that saves information about the owner as well as biometric data in the form of a fingerprint and a picture to lower the danger of counterfeiting. While currently not extensively utilised, the digital photo is anticipated to enable automated identification checks at border crossings and potentially cross-matching against databases of terrorist suspects, AND Interest in using facial recognition technology to automatically match the faces of persons seen on surveillance photographs against a database of known suspects has increased as surveillance cameras are being placed in more public areas. Despite significant technical issues that make this application now unworkable, governments continue to place a high priority on automatic biometric face recognition systems. Face biometrics are widely used, which raises significant privacy concerns. Particularly troubling are situations where a face image is automatically matched against a database without a person's explicit consent (such as in the aforementioned surveillance scenario), as this enables the tracking of individuals against their will. The widespread use of biometrics necessitates a strict policy that specifies to whom biometric information is revealed, especially if biometric matching is carried out at a central server or in otherwise highly untrusted situations.

[6] Privacy and Data Protection at the time of Facial Recognition: Towards a new right to Digital Identity : In the first section of this article, we will cover the new Facebook's default privacy settings, facial recognition technology, and indicators of the "health" of users' rights in the digital world. The Facebook case is an

illustration of a social networking site using biometrics as a specific category of personal data, which has legal ramifications for data security, privacy, and user control over their digital identity. Specifically based on data from the Eurobarometer (EB), The analysis contained in the second paragraph of the paper will highlight some of the flaws in the current legal framework for data protection that the recent proposal of the European Commission for a Regulation on Data Protection seems only to pave over. These flaws include users' attitudes toward personal data and identity protection, recent opinions of the Article 29 Working Party (Art29 WP), and the recent report of the UN Special Rapporteur, Frank La Rue, on freedom of expression (2011).

[7] Preserving Privacy by De-identifying Facial Images : Face recognition software is a significant threat to privacy in the context of sharing video surveillance data since it may monitor people independent of suspicion by automatically identifying known individuals, such as from a database of driver's licence photographs. This work offers a method for de-identifying faces in video surveillance data so that many facial characteristics are retained but the face cannot be reliably identified. De-identifying faces is easily accomplished by simply blacking out each face. This blocks any potential face recognition, but the outcome is only partially useful because all facial details are hidden. Due to the resilience of facial recognition techniques, many ad hoc attempts to prevent it, including hiding eyes or randomly shifting picture pixels, fail. This work introduces a novel privacy-enabling algorithm called k-Same, which restricts the accuracy of face recognition software while preserving facial details in the images. The algorithm compares faces using a distance metric to assess how similar they are, and it then generates new faces by averaging image elements, such as the original picture's pixels (k-Same-Pixel) or eigenvectors (k-Same-Eigen).

[8] Face de-identification using facial identity preserving features : A crucial piece of technology for privacy-preserving social media and intelligent surveillance applications is automated human face picture de-identification. In contrast to the typical face blurring methods, in this work, we propose to achieve facial anonymity by subtly altering existing facial images into "averaged faces" to make it harder to determine the related identities. This strategy protects privacy while maintaining the aesthetics of the facial images. In particular, we investigate facial identity-preserving (FIP) characteristics based on deep learning. The FIP features, in contrast to conventional face descriptors, can dramatically decrease intra-identity variation while maintaining inter-identity differences. We achieve the goal of k-anonymity face picture de-identification while maintaining desirable utility by suppressing and fiddling with FIP features. We successfully show that the resultant "averaged faces" will nevertheless maintain the beauty of the original photographs while eluding facial image identification verification using a face database.

[9] “All the better to see you with, my dear”: Facial recognition and privacy in online social networks : An overview of the ethical and legal issues raised by facial recognition technology used by online social networks looks at ways to control the implications for privacy, specifically from the standpoint of protecting European data.

[10] Robust human face hiding ensuring data privacy : Video monitoring of individuals today must protect their privacy. In this study, we provide a seamless solution to that issue, which maintains individual anonymity, by masking faces in video sequences. Two modules make up the system. First, a face detection analysis module locates and tracks areas of interest (ROIs). Second, in order to limit the accurate portrayal of human faces, the JPEG 2000 encoding module compresses the frames while maintaining the ROIs in a distinct data layer. Face detection and tracking are combined in the analysis module in order to find faces in the picture and follow them seamlessly through time. Combining these two techniques increases resilience since tracking may be able to identify faces in subsequent frames even when face identification algorithms are unable to. Additionally, the identification of faces keeps the target from being lost during tracking. The JPEG data corresponding to the recognised ROIs is downshifted by the encoding module to the code stream’s lowest quality layer. The human faces will then be decoded with lesser visual quality, up to invisibility where necessary, when the transmission bandwidth is constrained.

[11] The De-identification Dilemma : A Legislative and Contractual Proposal, Fordham Intellectual Property : One way to protect privacy while allowing other uses for private information is through de-identification. De-identified data, however, is typically still capable of being re-identified. The main goal of this article is to offer a legally-based practical solution for the sharing of de-identified personal information while also offering privacy protections. The legal framework enables a knowledge discloser and a knowledge recipient to engage into a voluntary agreement that specifies obligations and provides compensation for aggrieved parties.

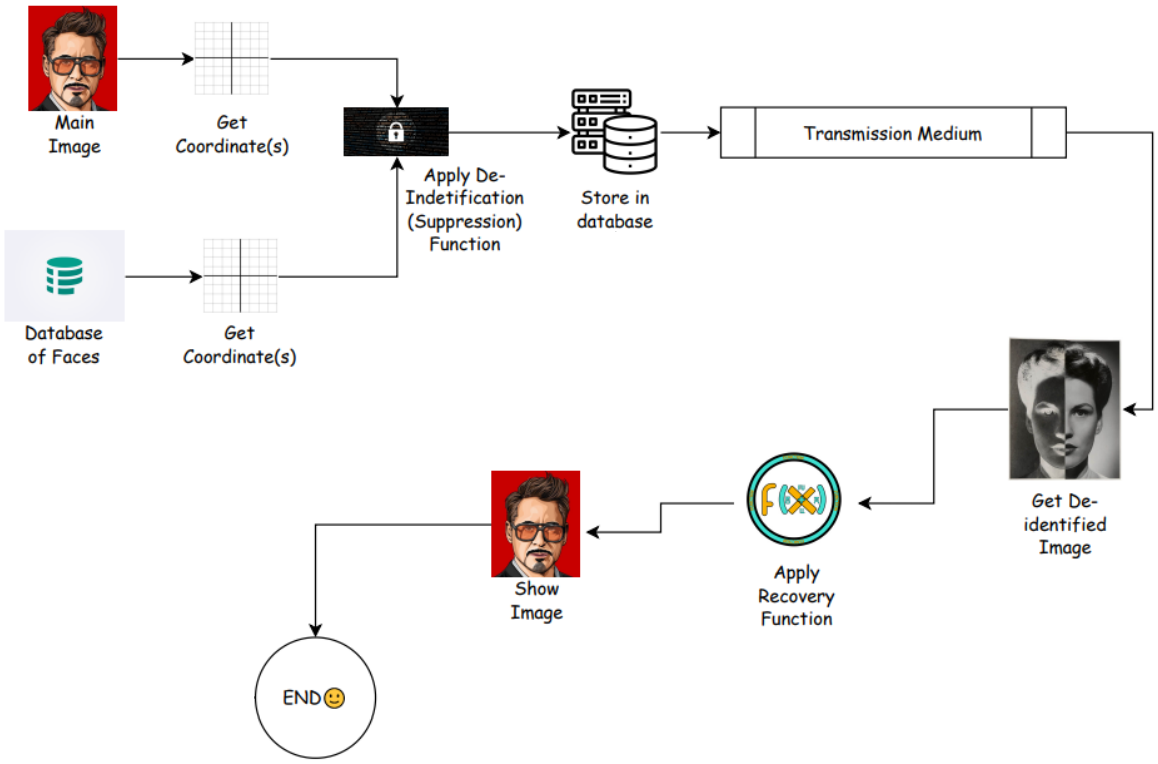
[12] Retaining Expressions on De-identified Faces, Proceedings of the session on Biometrics, Forensics, De-identification, and Privacy Protection : The de-identification methods for physiological, behavioural, and soft-biometric identifiers in multimedia documents, as well as non-biometric identifiers, are summarised in this article.

[13] Real-time and Multi-View Face Tracking on Mobile Platform, IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) : The Android Studio and OpenCV libraries are used to implement the face detection and tracking that the article proposes, and the Sony Xperia Z2 Android Lollipop smartphone is used for testing. These tests demonstrate that optical flow with regular features produces face tracking results that are more accurate and efficient than optical flow with fast corner features.

[14] Person De-Identification in Videos, IEEE Transactions on Circuits and Systems for Video Technology : This article describes the situations in which de-identification is necessary and, consequently, the problems such situations raise. a method for removing people's identities from videos. Our method entails monitoring and segmenting individuals over a conservative voxel space that takes into account time, x, and y. Using voxels, a de-identification modification is conducted every frame to hide the identity. Face, silhouette, and other features are hidden. The outcomes of our method for various films and different changes.

[15] An Approach to the De-Identification of Faces in several Poses, Proceedings of the session on Biometrics, Forensics, De-identification, and Privacy Protection : The overview of techniques, approaches, and fixes for face de-identification in still images and films is presented in this study. Privacy is frequently violated in many application contexts, particularly in video surveillance. One method for protecting privacy is de-identification, which is the process of hiding or removing personal identifiers from personal information captured in multimedia content or replacing them with substitute personal identifiers to prevent disclosure and use of knowledge for purposes unrelated to the one for which the knowledge was initially acquired.

III. PROPOSED NETWORK SECURITY MODEL



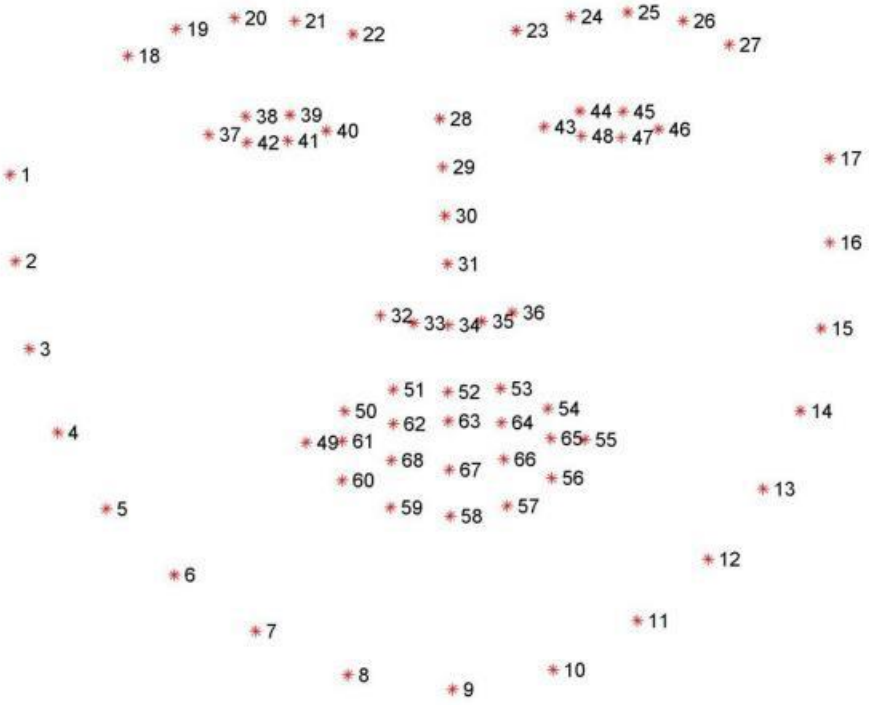
The general layout of our project will be as follows: Here, we grab the primary image and an additional image from the database, de-identify them, and then save them. We will retrieve the original grayscale image by extracting the image from the database. Our approach uses a modified average across pictures. Using the De-identification function, we will utilise one picture as the main image in this technique to de-identify other photos in the Database. These de-identified photographs will thereafter be kept in the database of de-identified images.

IV. IMPLEMENTATION

We use a facial landmark detector included within the Python dlib module to extract the key facial traits that typically characterise a face. 68 of the results from this detector correspond to certain face features, including the jawline, eyes, ears, nose, mouth, and eyebrows. The jaws, eyes, ears, nose, mouth, and eyebrows are among the specific facial features that can be identified using the following python coordinates that map to them. The following is how Python indexing organises the facial features :

1. The mouth can be accessed through points [48, 68].
2. The right eyebrow through points [17, 22].
3. The left eyebrow through points [22, 27].
4. The right eye using [36, 42].
5. The left eye with [42, 48].
6. The nose using [27, 35].
7. The jaw via [0, 17].

We can see what each of these 68 coordinates correspond to below :



The following are the methods used to identify facial features –

A. Function to transform an image's shape into a numpy array :

```
def shape_to_numpy_array(shape, dtype="int"):
    # initialize the list of (x, y)-coordinates
    coordinates = np.zeros((68, 2), dtype=dtype)

    # loop over the 68 facial landmarks and convert them
    # to a 2-tuple of (x, y)-coordinates
    for i in range(0, 68):
        coordinates[i] = (shape.part(i).x, shape.part(i).y)

    # return the list of (x, y)-coordinates
    return coordinates
```

B. Function to color-code the mapped facial features :

```
def visualize_facial_landmarks(image, shape, colors=None, alpha=0.75):
    # create two copies of the input image -- one for the
    # overlay and one for the final output image
    overlay = image.copy()
    output = image.copy()

    # if the colors list is None, initialize it with a unique
    # color for each facial landmark region
    if colors is None:
        colors = [(19, 199, 109), (79, 76, 240), (230, 159, 23),
                  (168, 100, 168), (158, 163, 32),
                  (163, 38, 32), (180, 42, 220)]

    # loop over the facial landmark regions individually
    for (i, name) in enumerate(FACIAL_LANDMARKS_INDEXES.keys()):
        # grab the (x, y)-coordinates associated with the
        # face landmark
        (j, k) = FACIAL_LANDMARKS_INDEXES[name]
        pts = shape[j:k]
        facial_features_cordinates[name] = pts
```

```
     # check if are supposed to draw the jawline
     if name == "Jaw":
         # since the jawline is a non-enclosed facial region,
         # just draw lines between the (x, y)-coordinates
         for l in range(1, len(pts)):
             ptA = tuple(pts[l - 1])
             ptB = tuple(pts[l])
             cv2.line(overlay, ptA, ptB, colors[i], 2)

     # otherwise, compute the convex hull of the facial
     # landmark coordinates points and display it
     else:
         hull = cv2.convexHull(pts)
         cv2.drawContours(overlay, [hull], -1, colors[i], -1)

 # apply the transparent overlay
 cv2.addWeighted(overlay, alpha, output, 1 - alpha, 0, output)

 # return the output image
 #print(facial_features_cordinates)
 return facial_features_cordinates,output
```

C. Function to recognise facial features and use it in conjunction with the previous two functions :

```
# loop over the face detections
from google.colab.patches import cv2_imshow

def loop_over_face_detectoion(rects,gray,image,image_path):
  for (i, rect) in enumerate(rects):
      # determine the facial landmarks for the face region, then
      # convert the landmark (x, y)-coordinates to a NumPy array
      shape = predictor(gray, rect)
      shape = shape_to_numpy_array(shape)

      points_68,output = visualize_facial_landmarks(image, shape)
      img = cv2.imread(image_path, cv2.IMREAD_UNCHANGED)
      cv2_imshow(output)
      # cv2_imshow("Image", output)
      cv2.waitKey(0)
      cv2.destroyAllWindows()

      return points_68
```

We select the primary image as well as an identically sized image from the database. Next, we square root the result after adding values to each image's coordinate. Later, we multiply it by 15, then divide it by 2.

The formula will be **De-identify=((sqrt(Main_img[i][j]+DB_image[i][j])/2)*15**

Function(s) to Suppress –

```
#de-identification function
def averaging_points(image_change,image_main):

    for i in range(0,300):
      for j in range(0,300):
        a=image_change[i][j]
        b=image_main[i][j]
        y=a+b
        z=math.sqrt(y)
        image_change[i][j] = np.multiply(15,np.divide(z,2)).astype(int)
    return image_change
```

We select the largest primary picture and de-identified image from the database. The values for each coordinate in the deidentified picture are then multiplied by 2, divided, and squared. Later, using the same coordinates, we deduct the value of the primary picture.

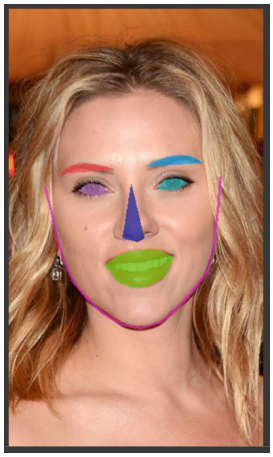
The formula will be **recover=((2*(Deidentified_image[i][j]))/15)2 - Main_img[i][j]**

Function(s) to recover –

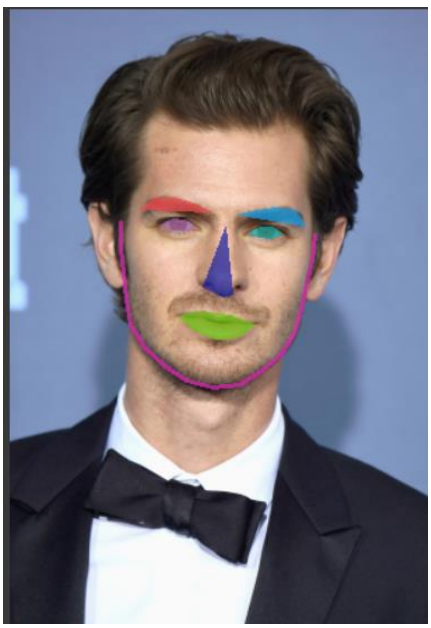
```
#recovery of images
def recover_points(im,image_main):

    for i in range(0,300):
      for j in range(0,300):
        z = np.multiply(2,np.divide(im[i][j],15)).astype(int)
        y= math.pow(z,2)
        b=image_main[i][j]
        a=y-b
        im[i][j]=a

    return im
```

V. RESULTS AND DISCUSSION

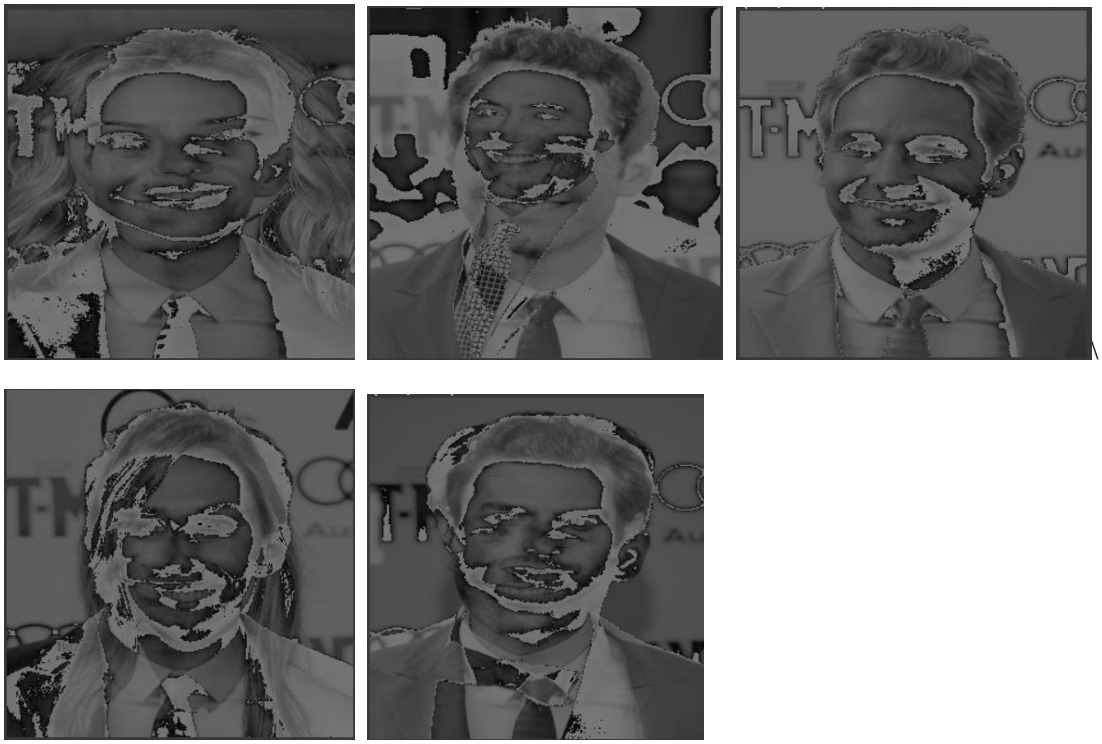
This is how the picture / pictures appears after our project has identified facial features –







After suppression, the o/p image will be comparable to the below result :

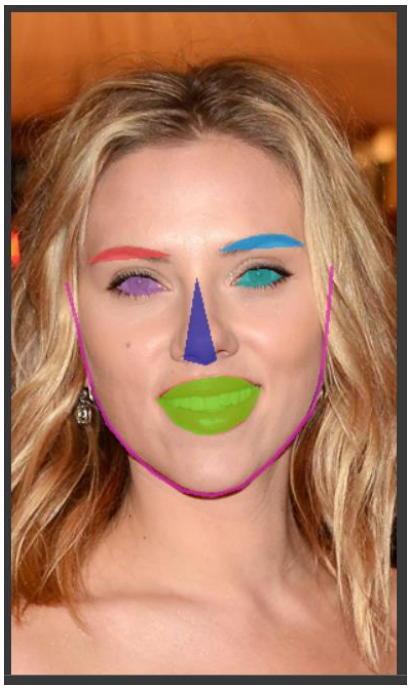


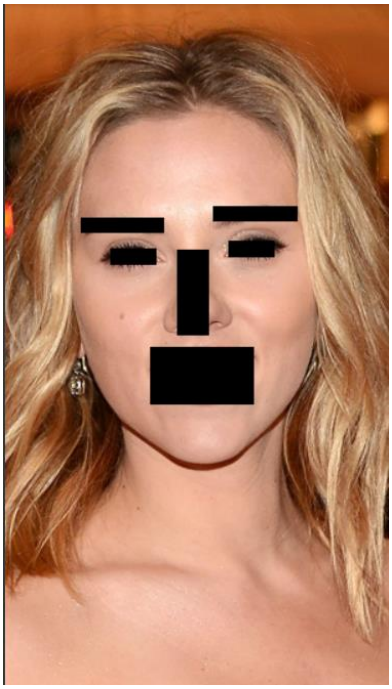
After feeding the o/p image to the recovery function – we will get the below output :

V(A). COMPARSION STUDY WITH RESPECT TO TRADITIONAL METHODS

BLACK BOX

One of the earliest techniques used here involves simply replacing the facial region with a black or white (rectangular, elliptical, or circular) cover. The human eye might find this technique useful, but facial recognition software won't.





If a human eye had examined it, the methods mentioned above would have been successful, but a recognition programme would identify it right away. Parrot recognition, a straightforward technique, was frequently employed. Here, parrot recognition compared de-identified images with the gallery image instead of comparing the disoriented image to the original one. This made the task much easier and decreased the level of privacy protection.

V(B). COMPARATIVE ANALYSIS

Using online face recognition and face detection software, we will compare the black-box algorithm with our suggested approach by choosing a few random images and their de-identified images.

Metric	Black-Box	Proposed Method
Accuracy rate of non-detection of face and facial points after image is suppressed.	**20%**	**80%**

The metric used here (see above in the table), indicates that the face in the de-identified image is not likely to be detected by face detection software. We have the BETAFACE tool for this.

V(C). RESULTS

Here, we discuss the correct image recovery capabilities of our model. Using dlibs facial feature detector, we were able to accurately identify all of the face characteristics. Here, we have also demonstrated a facial recognition measure. In this case, we compare the recovered image with the original image using an online facial recognition programme. And confidence is the employed measure. This refers to how confident the two faces are in matching the facial recognition programme.

Metric	Average confidence of 5 randomly recovered images
Recovery rate of the target image based on confidence of algorithm.	85.5%

A statistic called **confidence** demonstrates how confident the software is that the recovered and original image are identical. Tool used for measuring confidence : **KAIROS.**

VI. CONCLUSION

As a result, we draw the conclusion that, as stated in the comparison study, we can effectively de-identify photos with an accuracy of 80%. De-identification and picture recovery were accomplished using our modified averaging across images technique. With a confidence level of 85.08%, facial recognition software was able to match our recovered photographs with the original ones. Additionally, our model outperformed one of the conventional approaches and was able to do so while avoiding their shortcomings. Future work shall include the inculcation of transmission medium where the sender side will be responsible for suppressing the images and the receiver side will recover the original image through the recovery function. The same transmission medium shall be used to store the de-identified & recovered image (DUO) for future enhancement of the model for further de-identification of other images.

VII. REFERENCES

[1] Paula Carrillo, Hari Kalva, “Compression Independent Reversible Encryption for Privacy in Video Surveillance”, EURASIP Journal on Information Security, Volume 2009, Article ID 429581, 2009.

[2] Yuta Nakashima, Tatsuya Koyama, Naokazu Yokoya, Noboru Babguchi, “Facial expression preserving privacy protection using image melding”, IEEE International Conference on Multimedia and Expo (ICME), Aug.6, 2015.

[3] Ben Buckley Matt Hunter, “Say cheese! Privacy and facial recognition”, Elsevier Ltd., December 2011.

[4] Yogachandran Rahulamathavan, Muttukrishnan Rajarajan, “Efficient Privacy-Preserving Facial Expression Classification”, IEEE Transactions on Dependable and Secure Computing, Volume 14, issue 3, 08 July 2015.

[5] Zekeriya Erkin, Martin Franz, Jorge Guajardo, Stefan Katzenbeisser, Inald Lagendijk, Tomas Toft, “Privacy-Preserving Face Recognition”, PETS 2009, pp 235-253, 2009

[6] Shara Monteleone, ” Privacy And Data Protection At The Time Of Facial Recognition: Towards A New Right To Digital Identity?”, 2012.

[7] Elaine Newton, Latanya Sweeney, Bradley Malin, “Preserving Privacy by De-identifying Facial Images”, IEEE Transactions on Knowledge and Data Engineering, Volume 7, issue 2, March 2003.

[8] Hehua Chi, Yu Hen Hu, “Face de-identification using facial identity preserving features”, IEEE Global Conference on Signal and Information Processing (GlobalSIP), 25 February 2016.

[9] Norberto Nuno Gomes de Andrade, Aaron Martin, Shara Monteleone, "All the better to see you with, my dear: Facial recognition and privacy in online social networks”, IEEE Security and Privacy Magazine 11, 14 February 2013.

[10] Isabel Martínez-Ponte, Xavier Desurmont, Jerome Meessen and Jean-François Delaigle, “Robust Human Face Hiding Ensuring Privacy”, Citeseer, 2005.

[11] R. Gellman, "The Deidentification Dilemma: A Legislative and Contractual Proposal, Fordham Intellectual Property", Media and Entertainment Law Journal, vol.21, issue 1, pp. 33-61, 2011.

[12] L. Meng, Z. Sun, A. Ariyaeeinia, K. L. Bennett, "Retaining Expressions on De-identified Faces", Proceedings of Special Session on Biometrics, Forensics, De-identification, and Privacy Protection BiForD 2014, pp. 27-32, 2014.

[13] L. Xu, J. Li, K. Wang, "Real-time and Multi-View Face Tracking on Mobile Platform", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1485-1488, 2011.

[14] P. Agrawal and P. J. Narayanan, "Person De-Identification in Videos", IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 3, pp. 299-310, March 2011.

[15] B. Samarzija, S. Ribaric, "An Approach to the De-Identification of Faces in Different Poses", Proceedings of Special Session on Biometrics, Forensics, De-identification and Privacy Protection BiForD 2014, pp.21- 26, 2014.