# DE-IDENTIFICATION OF DATA FOR DATA PRIVACY

*to be submitted in partial fulfilling of the requirements for the course on*

**Information Security Management – CSE3502 (F1)**

*By*

**Dipesh Balani – 19BIT0354**

**Tushar Kumar B P – 19BIT0358**

**Utkarsh – 19BIT0402**

*Under guidance of*

**Prof. John Singh K**

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

# ABSTRACT

Data is biggest asset for any organization in this century. It defines everything from their current marketing strategy to long-term plans. Every consumer deposits valuable pieces of their information online. Advances in information technology make the storage, cataloging, and use of such information trivial. This project aims to preserve the sensitive information of users by applying de-identification algorithms.  There are numerous techniques such as blurring out, masking facial features such as skin and shape and encrypting passwords. Pictures of faces, unlike other body parts, are very easily identifiable. Conventional techniques of de-identification aren't capable of concealing the identity. Thus, there is a requirement for masking facial features which help improve data privacy.

# INTRODUCTION

Face-based identification is used in various application scenarios - from identification of a person based on still images in passport or identity card to identification based on face images captured by a surveillance system without the cooperation of the person. In many application scenarios, especially in video surveillance, privacy can be compromised.

Photographs of the face, unlike those of other body regions, are readily identifiable. Traditional methods of facial image de-identification decrease educational quality or fail to adequately conceal identity. In the present study, a method that uses blended facial composites to de-identify original facial images was developed. This method allows significant components of the original face to be visualized while concealing its identity. Due to recent advances in multi-sensor acquisition and recording devices and remote surveillance systems, there is a need for the research and development of multimodal de-identification methods that simultaneously hide, remove or substitute different types of personal identifiers (face, gesture, gait) from multimedia content. The solution to the problem of multimodal de-identification is still a major challenge.

# MOTIVATION

In recent times, many software MNCs have implemented facial recognition software for services like surveillance, photo-tagging, maintaining identity records, etc. So, the question has arisen whether our identity is safe from leaks of sensitive data and are the companies following proper safety guidelines. Image recognition has become an integral part of any organization's operations such as Facebook implementing tagging people in uploaded pics, the government installing surveillance cameras, CCTV cameras in banks and other institutions, etc. Thus, there is a need to protect this info from untrusted sources by privatizing the data.

# OBJECTIVES

The main objective of this project is to design a new methodology by modifying the averaging method with which we will be able to de-identify the facial imaged and recover them successfully with maximum accuracy possible, compared to the existing methods.

# PROBLEM STATEMENT

The amount of data shared over the internet has increased drastically in these recent years with the advent of the Internet. With this, comes the need of preventing hackers/adversaries from accessing sensitive information. In this project, we aim to implement a method of anonymizing facial images using de-identification techniques. Several methods are available to implement this as blurring out the image, hiding certain facial features, modifying the facial features by adding some noise calculated by taking out average values of certain facial features, such as skin colour, shape.

# EXISTING SYSTEMS

## Compression Independent Reversible Encryption for Privacy in Video Surveillance [1]

With video surveillance becoming an integral part of our security infrastructure, privacy rights are beginning to gain importance. The key concern is the fact that private citizens, who are not suspects, are being recorded and recordings archived through the use of video surveillance systems. Such a record-everything-and-process-later approach has serious privacy implications. Similar privacy issues arise when surveillance cameras routinely record highway traffic as vehicle tags are recorded. The solution of removing the identities by blurring/blackening the portions of the video is not acceptable to security personnel as they may have a legitimate need to review the videos. On the contrary, leaving the videos with the identities of people and vehicles in public is a breach of privacy. A solution to the problem is selective encryption of portions of the video that reveal identity (e.g., faces, vehicle tags) in surveillance applications. Regions of a video can be encrypted to ensure privacy and still allow decryption for legitimate security needs at any time in the future.

## Facial expression preserving privacy protection using image melding [2]

An enormous number of images are currently shared through social networking services such as

Facebook. These images usually contain the appearance of people and may violate people's privacy if they are published without permission from each person. To remedy this privacy concern, visual privacy protection, such as blurring, is applied to facial regions of people without permission. However, in addition to image quality degradation, this may spoil the context of the image: If some people are filtered while others are not, missing facial expressions makes comprehension of the image difficult.

**Say cheese! Privacy and facial recognition [3]**

With many images being shared over the internet and many companies utilizing this data for their services comes the need of implementing guidelines for dealing with data and protecting it. This paper discusses various guidelines under European data protection laws.

**Efficient Privacy-Preserving Facial Expression Classification [4]**

This paper proposes an efficient algorithm to perform privacy-preserving (PP) facial expression

classification (FEC) in the client-server model. The server holds a database and offers the classification service to the clients. The client uses the service to classify the facial expression (FaE) of the subject. It should be noted that the client and server are mutually untrusted parties and they want to perform the classification without revealing their inputs to each other. In contrast to the existing works, which rely on computationally expensive cryptographic operations, this paper proposes a lightweight algorithm based on the randomization technique. The proposed algorithm is validated using the widely used JAFFE and MUG FaE databases. Experimental results demonstrate that the proposed algorithm does not degrade the performance compared to existing works. However, it preserves the privacy of inputs while improving the computational complexity by 120 times and communication complexity by 31 percent against the existing homomorphic cryptography-based approach.

**Privacy-Preserving Face Recognition [5]**

Biometric techniques have advanced over the past years to a reliable means of authentication, which are increasingly deployed in various application domains. In particular, face recognition has been a focus of the research community due to its unobtrusiveness and ease of use: no special sensors are necessary, and readily available images of good quality can be used for biometric authentication. The development of new biometric face-recognition systems was mainly driven by two application scenarios.

- To reduce the risk of counterfeiting, modern electronic passports, and identification cards contain a chip that stores information about the owner, as well as biometric data in the form of a

fingerprint and a photo. While this biometric data is not widely used at the moment, it is

anticipated that the digitized photo will allow to automatize identity checks at border crossings or even perform cross-matching against lists of terrorism suspects.

- The increasing deployment of surveillance cameras in public places sparked interest in the use of face recognition technologies to automatically match the faces of people shown on surveillance images against a database of known suspects. Despite massive technical problems that render this application currently infeasible, automatic biometric face recognition systems are still high on the agenda of policymakers.

The ubiquitous use of face biometrics raises important privacy concerns; particularly problematic are scenarios where a face image is automatically matched against a database without the explicit consent of a person (for example in the above-mentioned surveillance scenario), as this allows to trace people against their will. The widespread use of biometrics calls for a careful policy, specifying to which party biometric data is revealed, in particular, if biometric matching is performed at a central server or in partly untrusted environments.

**Privacy and Data Protection at the time of Facial Recognition: Towards a new right to Digital Identity [6]**

Indicators of the state of 'health' of the users' rights in the digital world, the new Facebook's default privacy settings, and its facial recognition functionality will be discussed in the first part

of this paper. The Facebook case constitutes also an example of the use of special categories of personal data (biometrics) by a social networking site, having legal implications in terms of data protection, privacy, and user's management of digital identity. Based in particular on the findings of the Eurobarometer (EB)

on users' attitudes as regards personal data and identity protection), on 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), the analysis contained in the second part of the paper will highlight some of the shortcomings of the current data protection legal framework that the recent Proposal of the European Commission for a Regulation on Data Protection seems only partially apt to solve.

**Preserving Privacy by De-identifying Facial Images, Elaine Newton Latanya Sweeney Bradley Malin [7]**

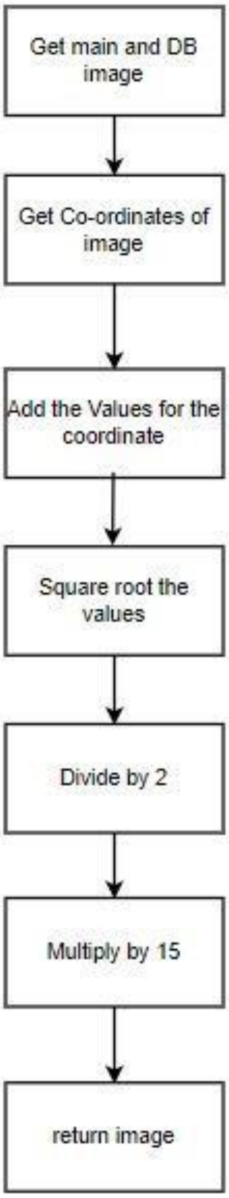
In the context of sharing video surveillance data, a significant threat to privacy is face recognition software, which can automatically identify known people, such as from a database of drivers’ license photos, and thereby track people regardless of suspicion. This paper introduces an algorithm to protect the privacy of individuals in video surveillance data by de-identifying faces such that many facial characteristics remain but the face cannot be reliably recognized. A trivial solution to de-identifying faces involves blacking out each face. This thwarts any possible face recognition, but because all facial details are obscured, the result is of limited use. Many ad hoc attempts, such as covering eyes or randomly perturbing image pixels, fail to thwart face recognition because of the robustness of face recognition methods. This paper presents a new privacy-enabling algorithm, named k-Same, that scientifically limits the ability of face recognition software to reliably recognize faces while maintaining facial details in the images. 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 (k-Same-Pixel) or eigenvectors (k-Same-Eigen).

# PROPOSED METHODOLOGY

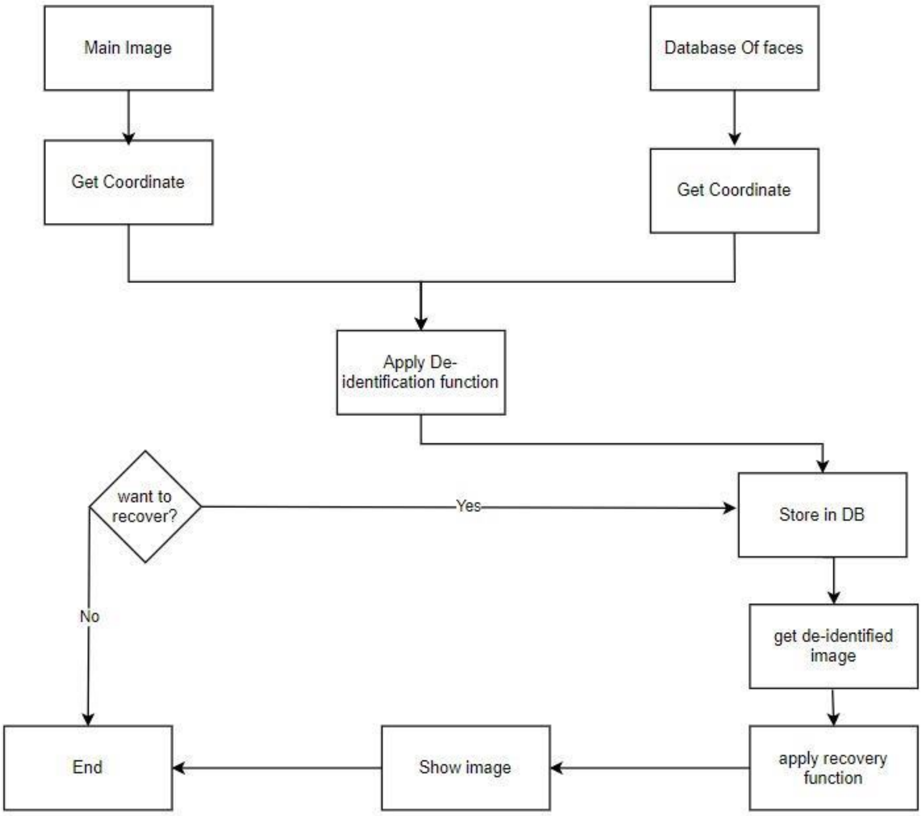
Our method includes modified averaging over images. In this method we will take an Image as the Main image and use this image for de-identification of images in the Database by using the De-identification function. Modified Averaging works on the principles of moving averages. It is also deployed in the FinTech world where prices of equity change every second. This algorithm works dynamically by computing on the basis of the last modified value and not the original value. We will then store these de-identified images in the database of deidentified images.

The flow of our project is shown in the architecture diagrams below.

**Low Level Diagram**



## High Level Diagram



The flow starts by taking an image from the database and applying the de-identification function and storing the resulting image. Here, we will be providing an option for recovery. If the recovery is needed, then we will extract the image from the database and recover the original image in grayscale form.

The proposed methodology contains three modules, one for identification of the facial features, the second for de-identification of the facial features for data privacy, and the last module for recovery of the original image from the de-identified image.

### Module 1: Identification of Facial Features

In this module, we will be extracting the main features of the face that normally define a face. We will be using a facial landmark detector which is included in a Python dlib Library. This will produce 68 co-ordinates that will map the special, rather, the main features of a face, which include eyes, nose, ears, mouth, jaws and eyebrows.

**The facial features are indexed by python indexing as follows:-**

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].

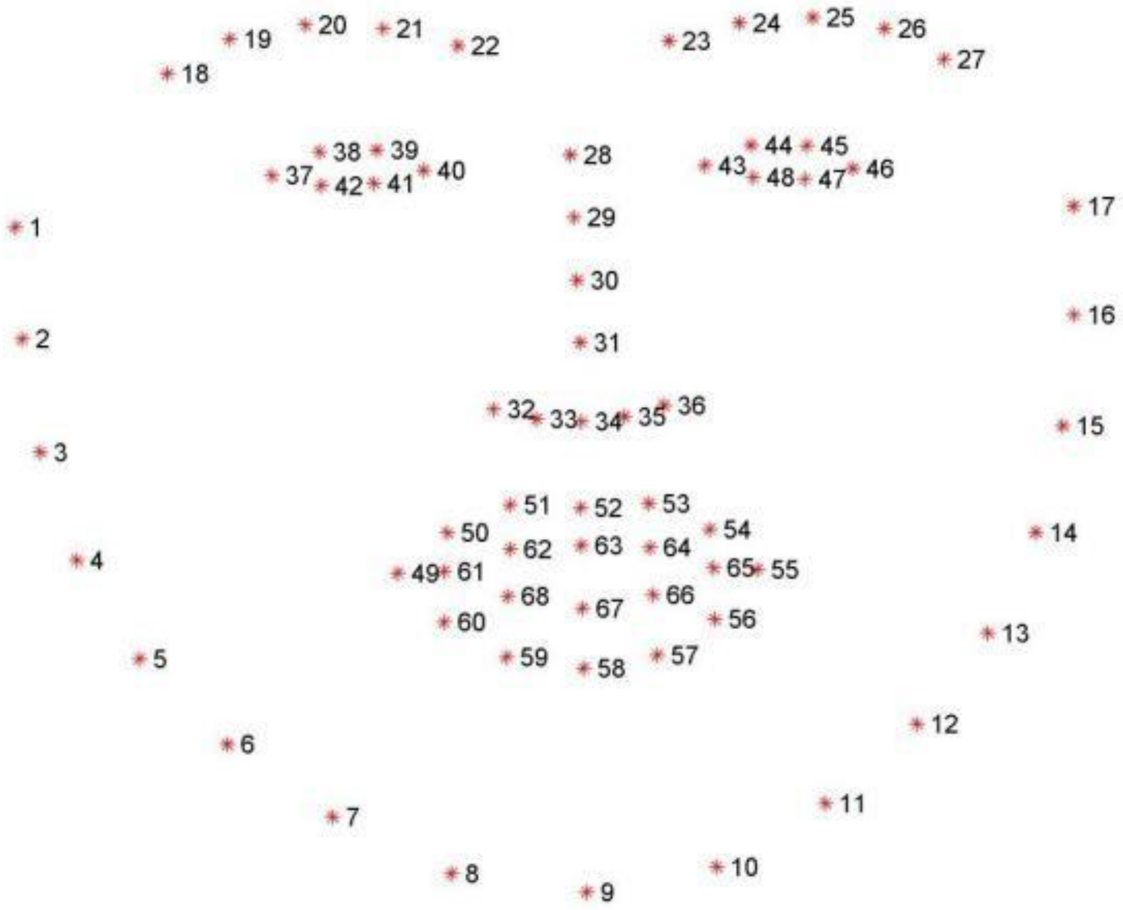
4. The right eye using [36, 42].

5. The left eye with [42, 48].

6. The nose using [27, 35].

7. The jaw via [0, 17].

**The picture below shows how the 68 co-ordinates the facial features.**



There are various set of functions from the library that have been used to achieve this process.

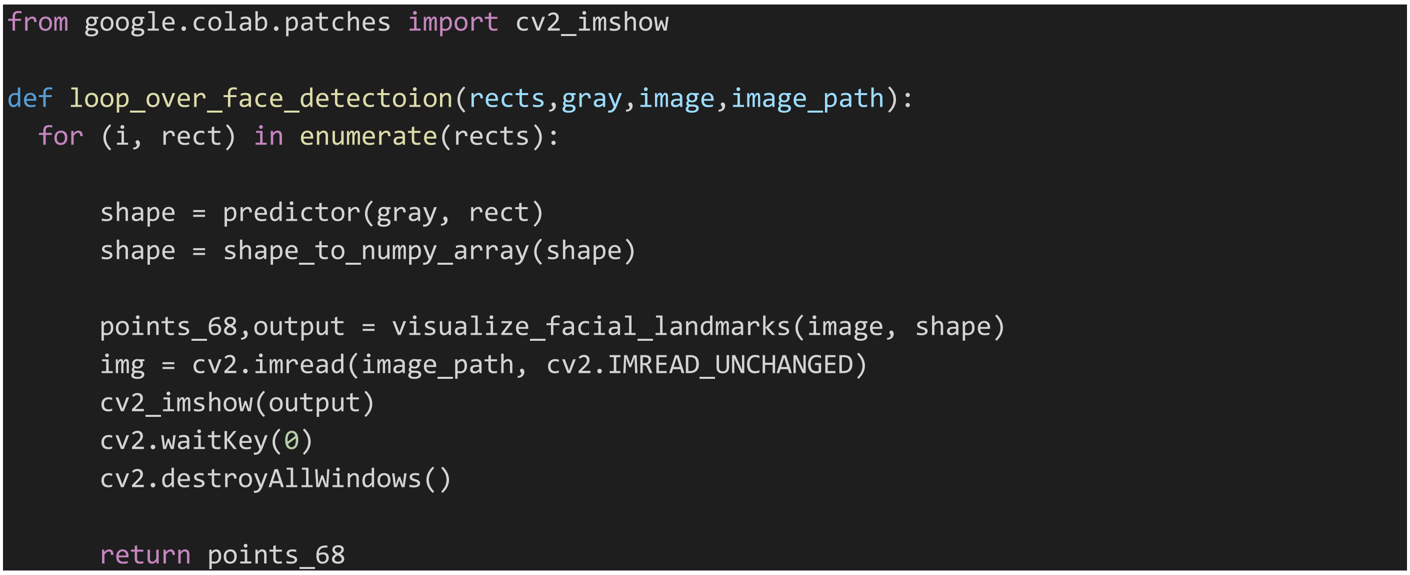
**A Function to convert the shape of the image into numpy array**

```
def shape_to_numpy_array(shape, dtype="int"):

    coordinates = np.zeros((68, 2), dtype=dtype)


    for i in range(0, 68):
        coordinates[i] = (shape.part(i).x, shape.part(i).y)


    return coordinates
```

## A function to colour the facial features that have been mapped

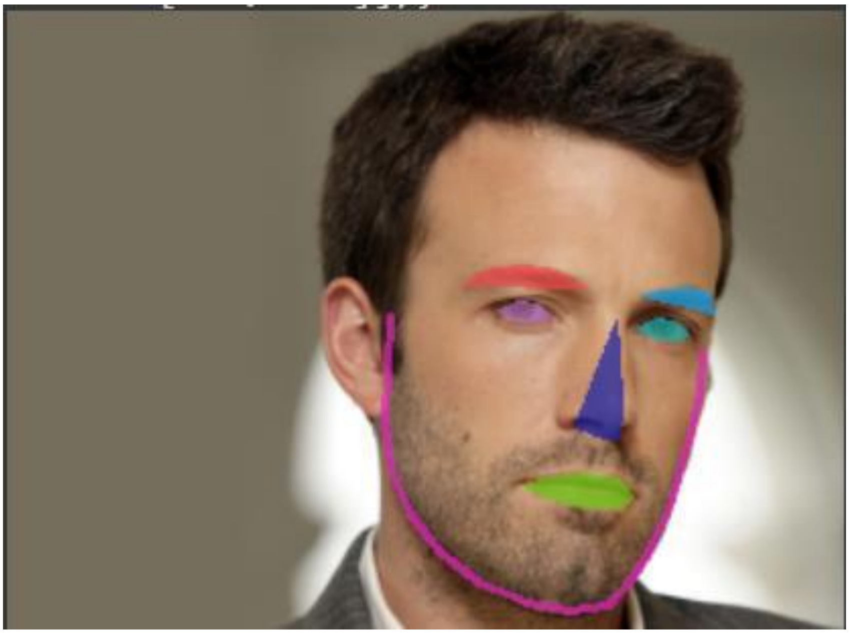
```
def visualize_facial_landmarks(image, shape, colors=None, alpha=0.75):

    overlay = image.copy()
    output = image.copy()


    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)]


    for (i, name) in enumerate(FACIAL_LANDMARKS_INDEXES.keys()):

        (j, k) = FACIAL_LANDMARKS_INDEXES[name]
        pts = shape[j:k]
        facial_features_cordinates[name] = pts


        if name == "Jaw":

            for l in range(1, len(pts)):
                ptA = tuple(pts[l - 1])
                ptB = tuple(pts[l])
                cv2.line(overlay, ptA, ptB, colors[i], 2)


        else:
            hull = cv2.convexHull(pts)
            cv2.drawContours(overlay, [hull], -1, colors[i], -1)


    cv2.addWeighted(overlay, alpha, output, 1 - alpha, 0, output)


    return facial_features_cordinates,output
```

**A function to detect the facial features and apply it to the above two functions**



```
from google.colab.patches import cv2_imshow

def loop_over_face_detectoion(rects,gray,image,image_path):
  for (i, rect) in enumerate(rects):

      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.waitKey(0)
      cv2.destroyAllWindows()

      return points_68
```

**After performing all the above operations, the output looks like the image shown below.**



This is the completion of the first step, rather, first module which involves the identification of the facial features in the given picture.

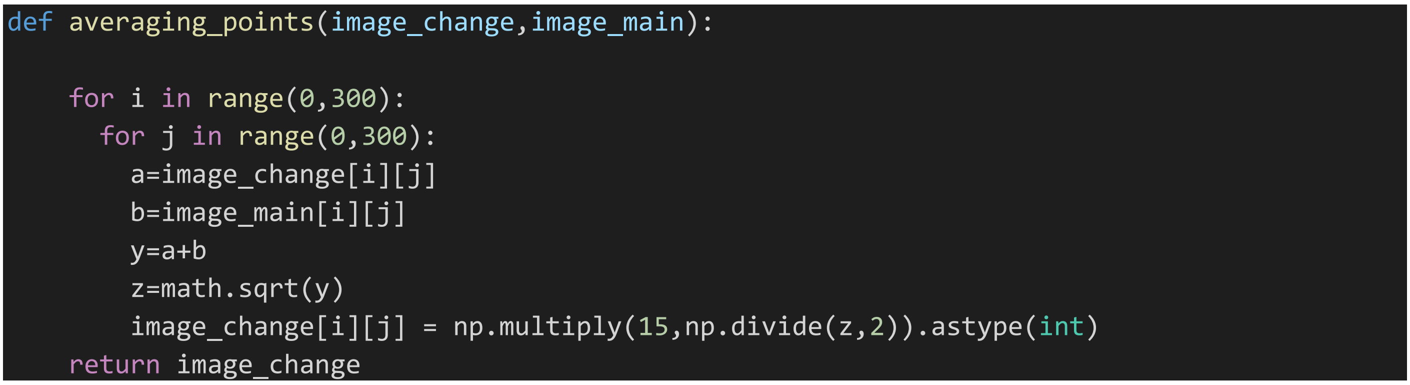
**Module 2: De-identification of facial features for privacy**

In the second module, we take the main image which we used and an image from the database of equal size. Now, the next step contains adding the values of each co-ordinate of the images and then square-rooting it. The result will be divided by 2 and multiplied with 15.

So the formula for **de-identification will be**

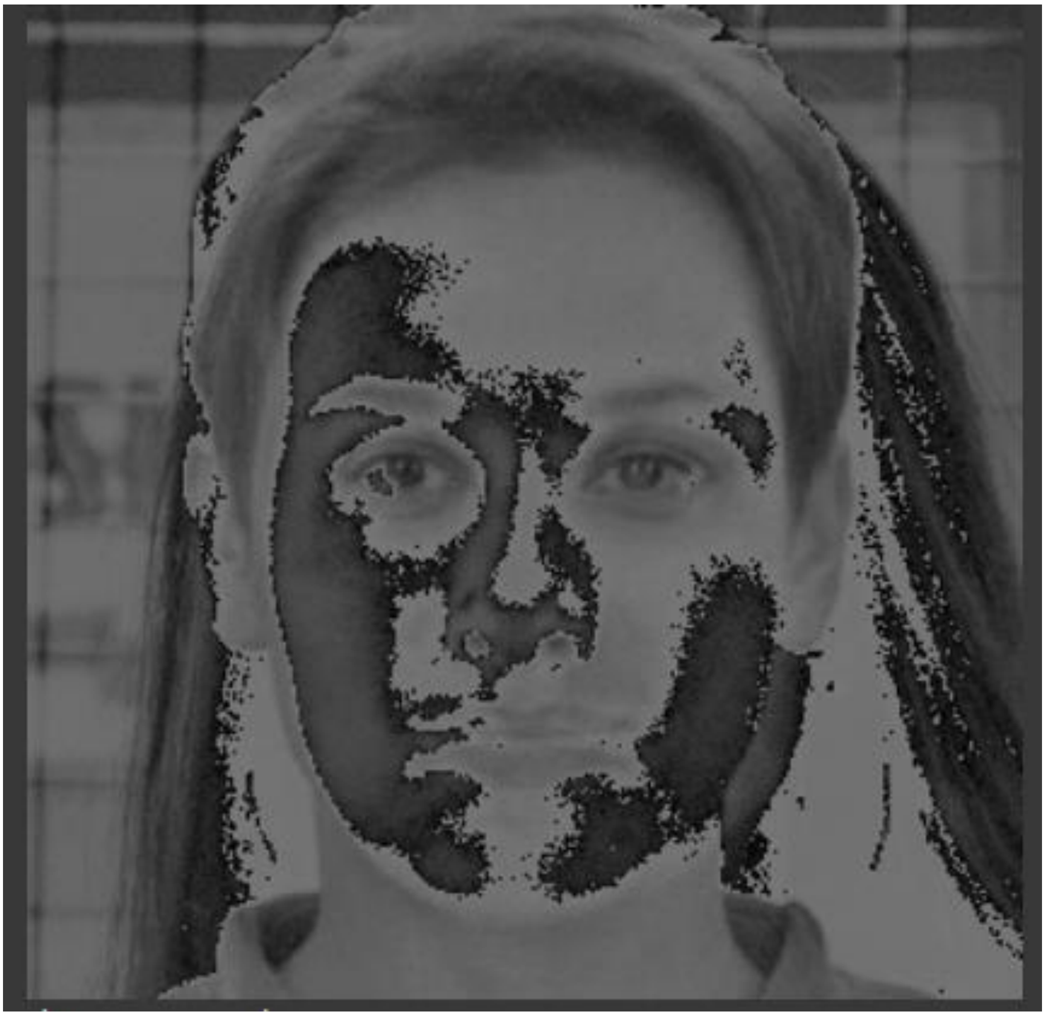
**De-Identify = ((srt(Main_img[i][j]+DB_img[i][j]/2)*15)**

The function to **de-identify the image**



```
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
```

Running this code fragment with the image will give us the following image as the output.



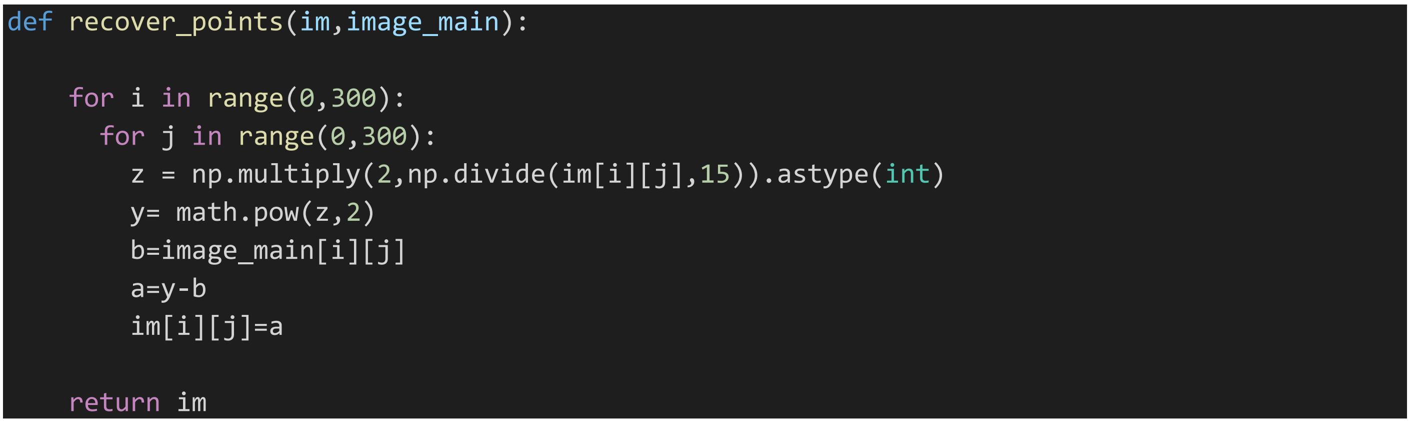
### Module 3: Recovery of Original Image form the De-Identified Image

In this module, we will take the main image and the de-identified image from the database of equal size. The values of the co-ordinate will be multiplied by 2 and divide them by 15 and then we will take the square of the result. This result will be subtracted with the values of the main image with the same co-ordinates.

The formula for this procedure will be as follows

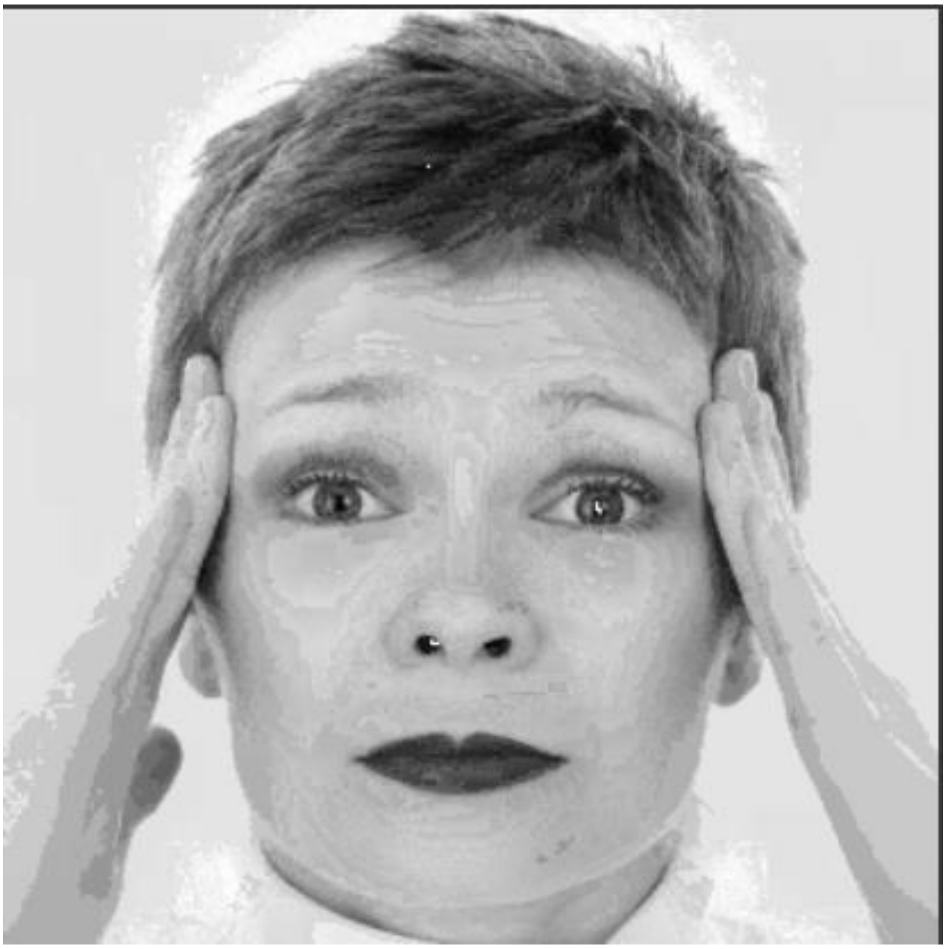
**Recover = ((2*(deidentified_img[i][j]))/15)$^{2}$ – main_img[i][j]**

The function to **recover the image**



```
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
```

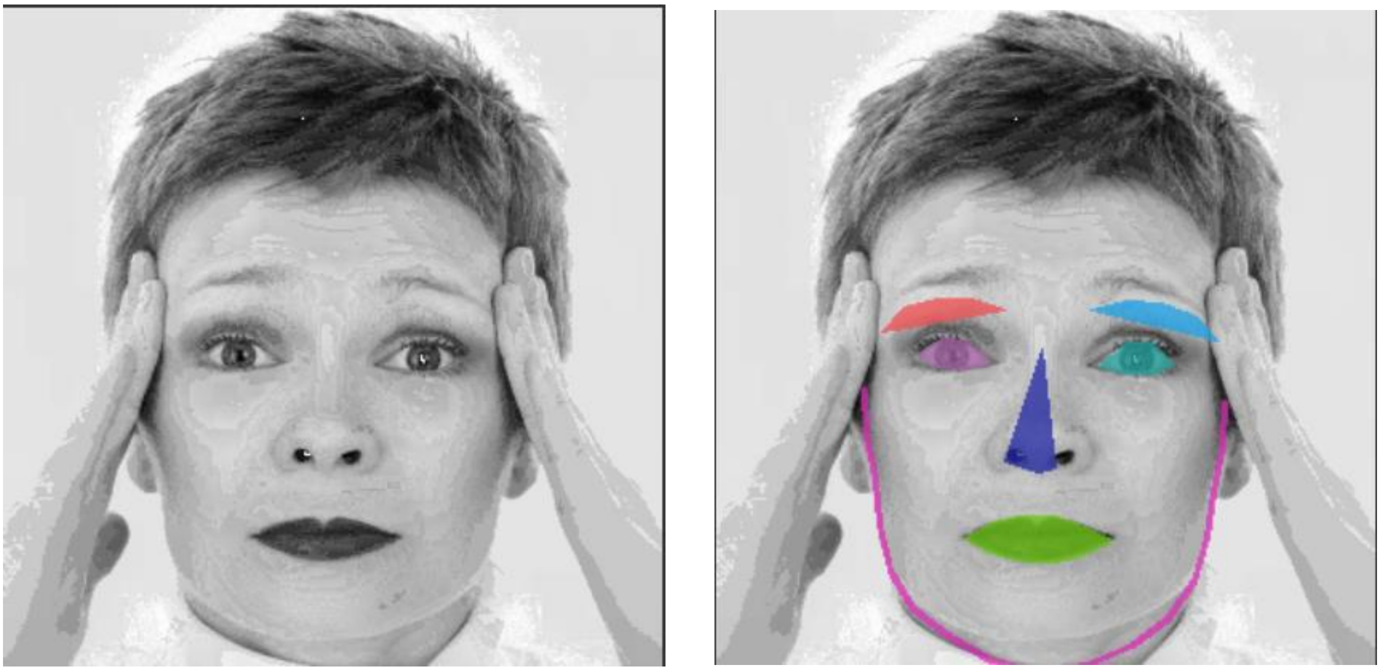
The resulting image will be as shown below



## RESULT AND DISCUSSION

Here, we will be discussing about how our model is able to recover the images properly. The method we proposed helped us to identify all the facial features properly with the help of dlibs facial feature detector.

**Image Recovery of our model using dlibs facial feature detector**



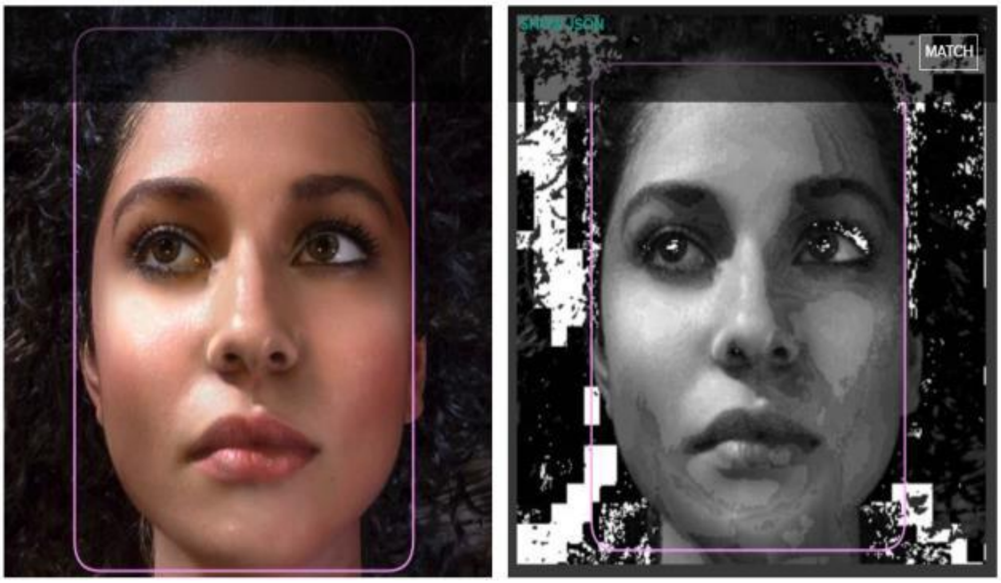
Here we have also shown a **metric** for face recognition.
In this we use an online face recognition tool and match the recovered image with the original image.

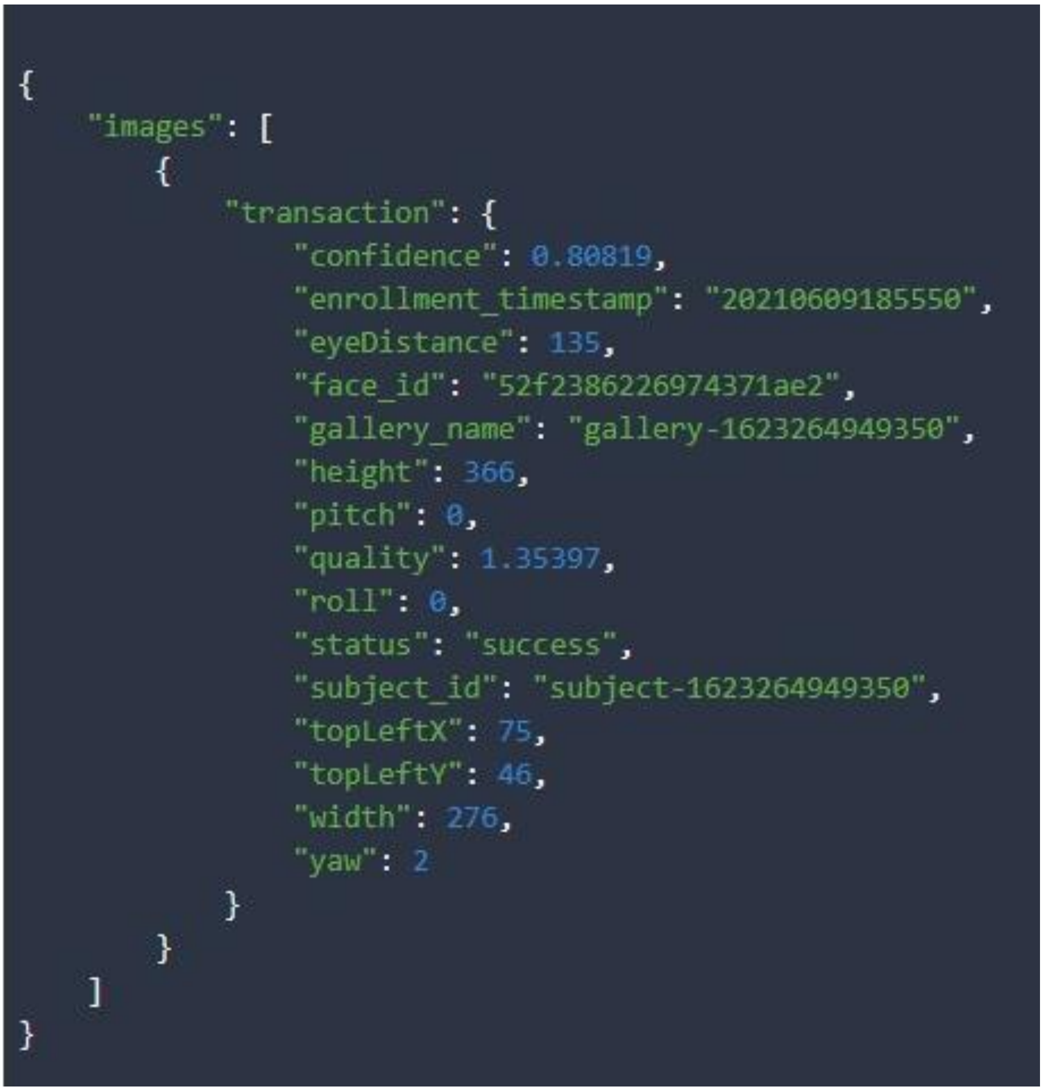
| | |
|---|---|
| And the metric used is confidence. Which means how sure the face recognition software is in matching the two faces **Metric** | **Average confidence of 10 randomly recovered images** |
| **Recovery rate of the target image based on confidence of algo** | **85.8%(avg)** |

**Confidence** is a statistic showing how sure the software is that the recovered and original image is alike.
The tool we are using is **KAIROS**

Link: https://www.kairos.com/demos

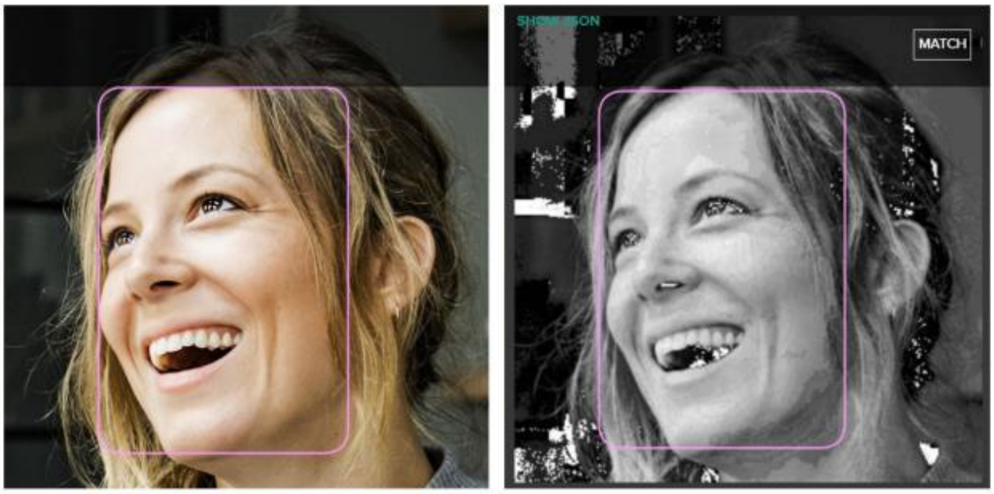
# Image 1

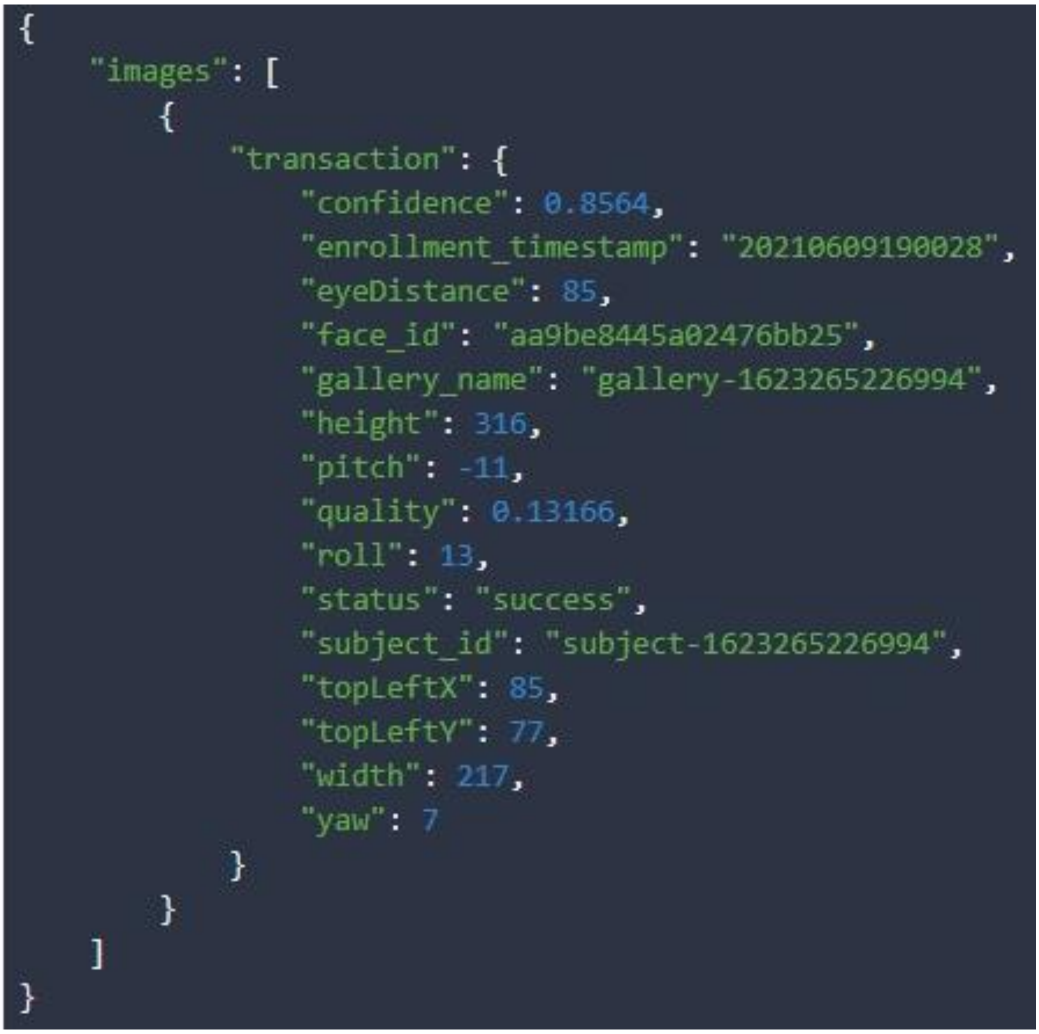




```
{
    "images": [
        {
            "transaction": {
                "confidence": 0.80819,
                "enrollment_timestamp": "20210609185550",
                "eyeDistance": 135,
                "face_id": "52f2386226974371ae2",
                "gallery_name": "gallery-1623264949350",
                "height": 366,
                "pitch": 0,
                "quality": 1.35397,
                "roll": 0,
                "status": "success",
                "subject_id": "subject-1623264949350",
                "topLeftX": 75,
                "topLeftY": 46,
                "width": 276,
                "yaw": 2
            }
        }
    ]
}
```

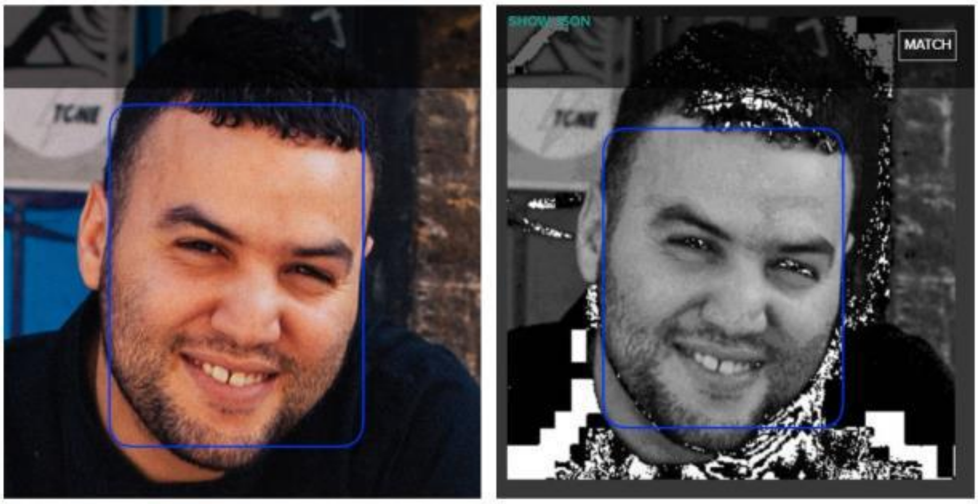
## Image 2

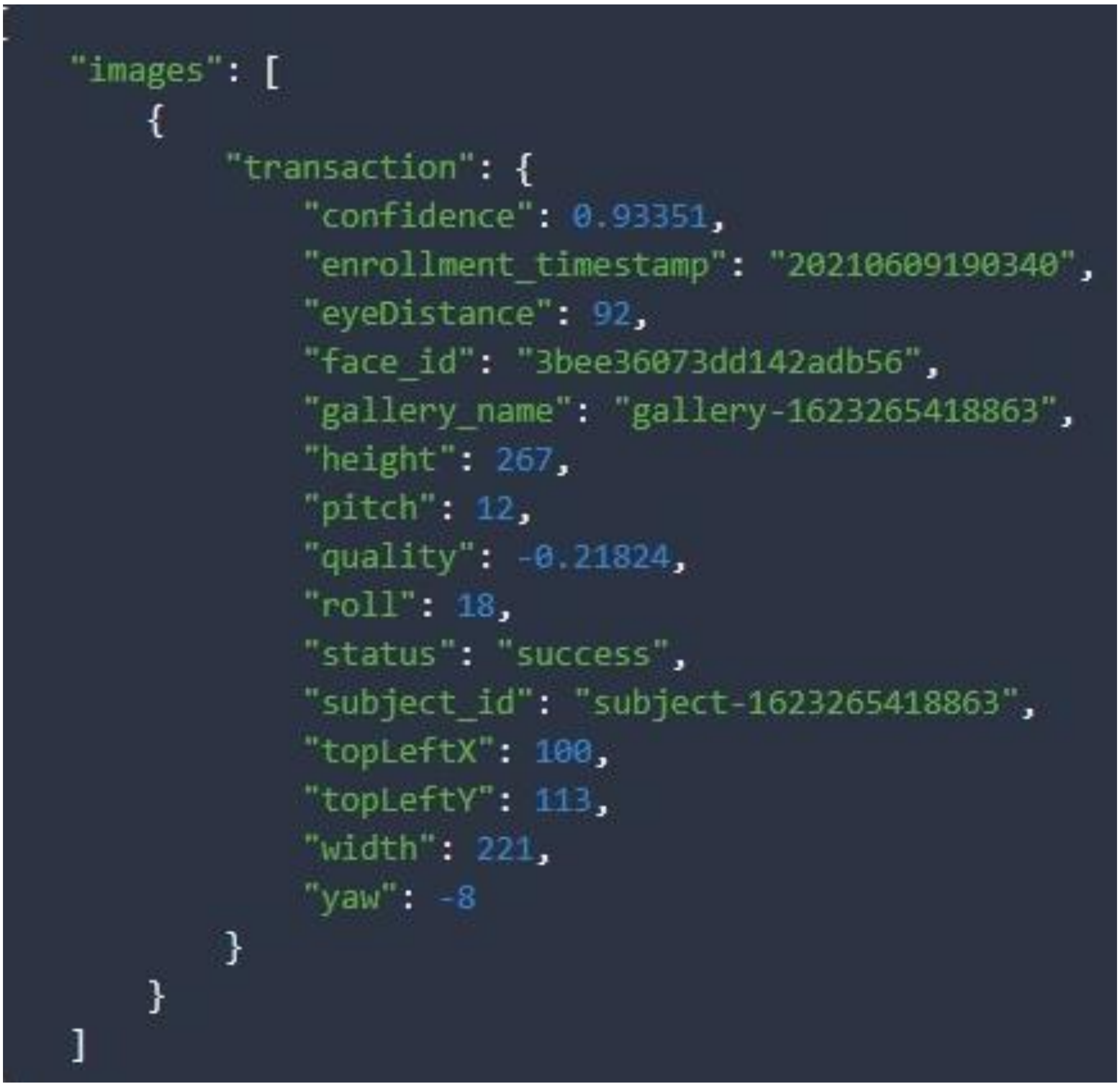




```
{
    "images": [
        {
            "transaction": {
                "confidence": 0.8564,
                "enrollment_timestamp": "20210609190028",
                "eyeDistance": 85,
                "face_id": "aa9be8445a02476bb25",
                "gallery_name": "gallery-1623265226994",
                "height": 316,
                "pitch": -11,
                "quality": 0.13166,
                "roll": 13,
                "status": "success",
                "subject_id": "subject-1623265226994",
                "topLeftX": 85,
                "topLeftY": 77,
                "width": 217,
                "yaw": 7
            }
        }
    ]
}
```

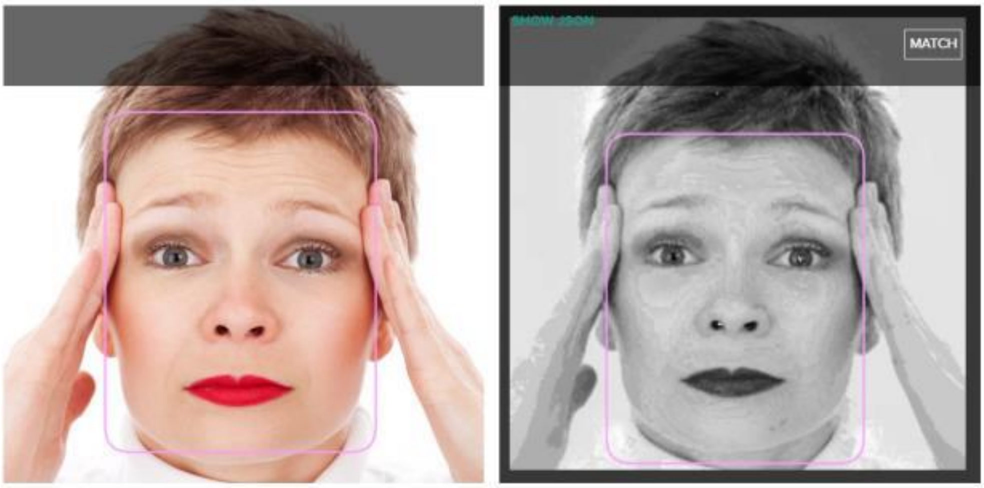
## Image 3

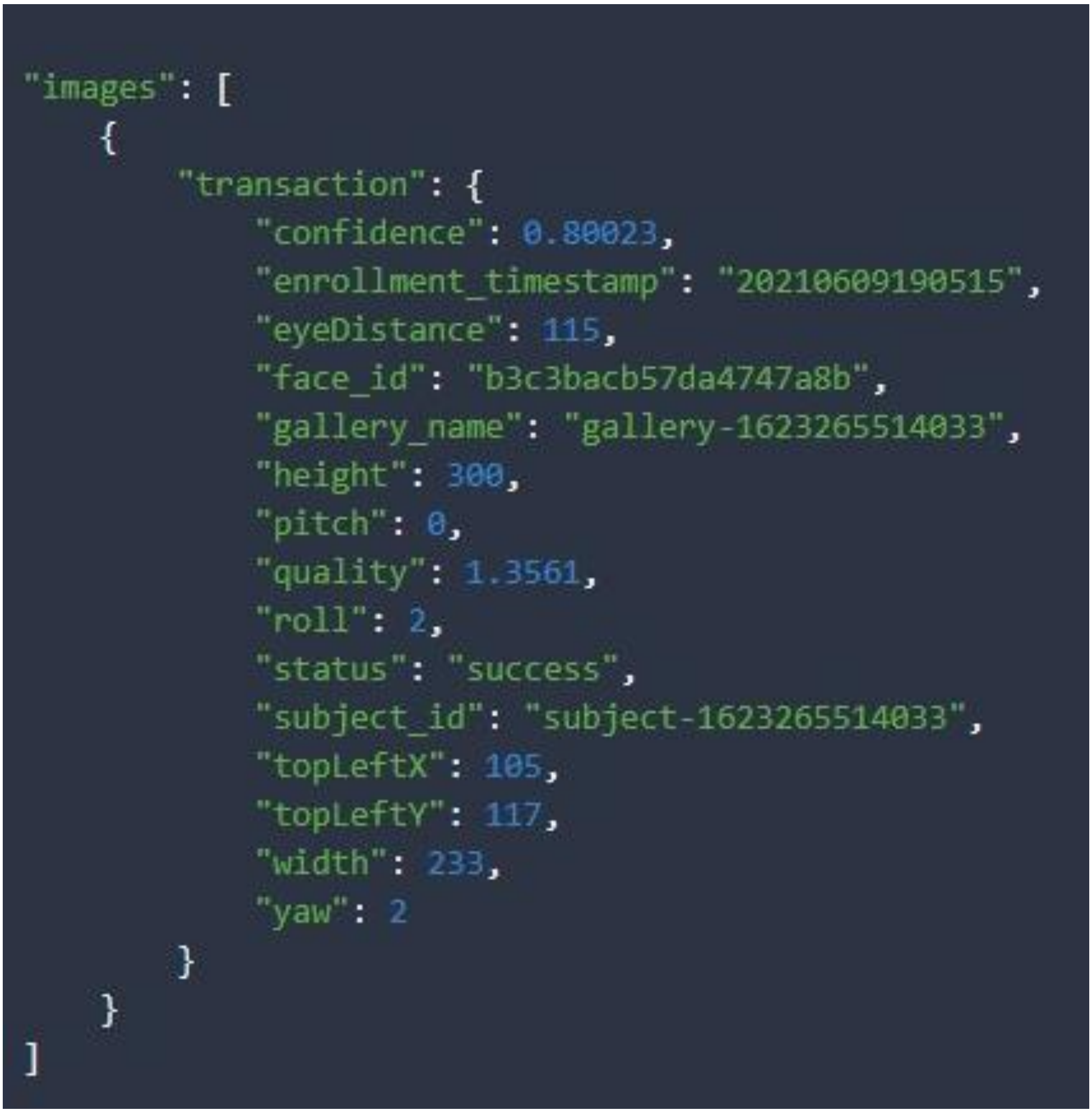




```
  "images": [
      {
          "transaction": {
              "confidence": 0.93351,
              "enrollment_timestamp": "20210609190340",
              "eyeDistance": 92,
              "face_id": "3bee36073dd142adb56",
              "gallery_name": "gallery-1623265418863",
              "height": 267,
              "pitch": 12,
              "quality": -0.21824,
              "roll": 18,
              "status": "success",
              "subject_id": "subject-1623265418863",
              "topLeftX": 100,
              "topLeftY": 113,
              "width": 221,
              "yaw": -8
          }
      }
  ]
```

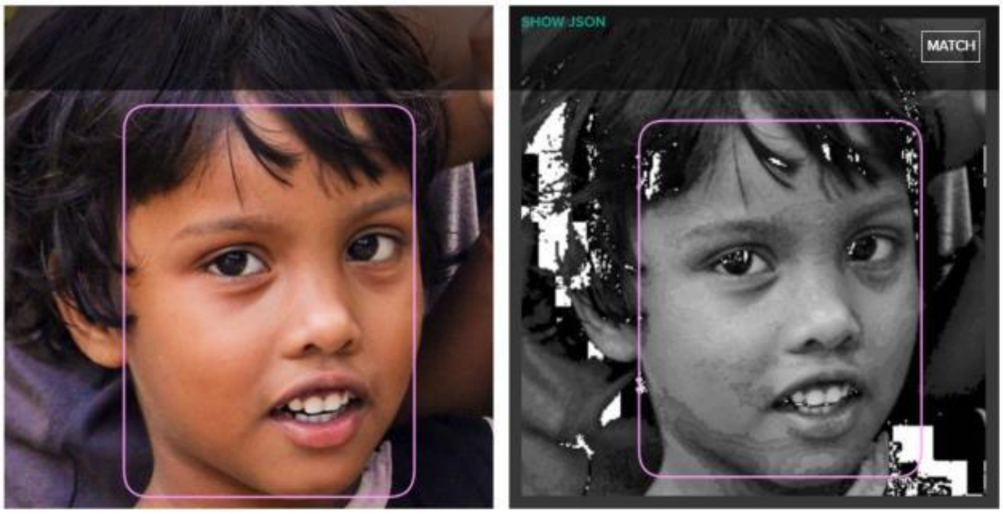
**Image 4**

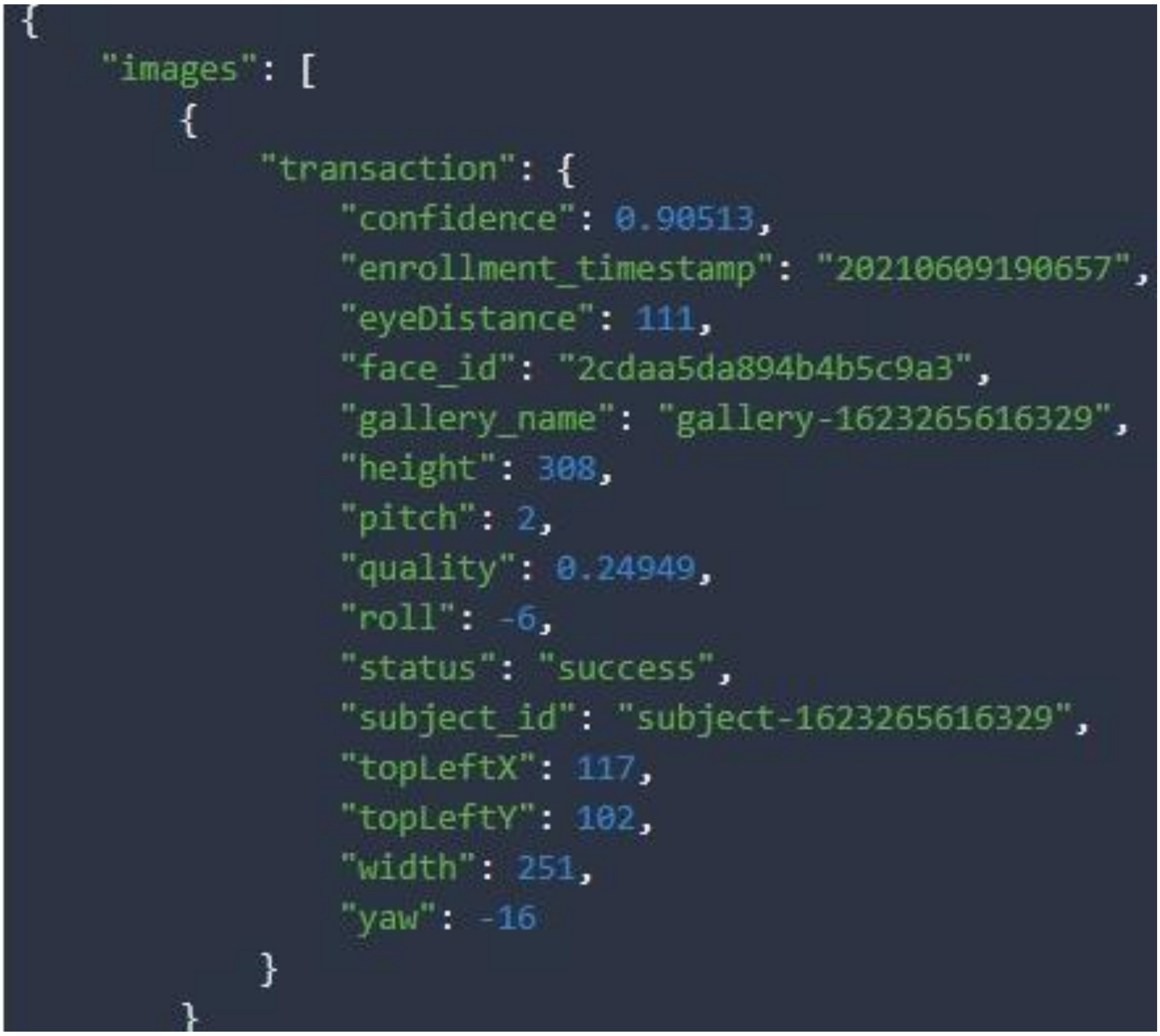




```
"images": [
    {
        "transaction": {
            "confidence": 0.80023,
            "enrollment_timestamp": "20210609190515",
            "eyeDistance": 115,
            "face_id": "b3c3bacb57da4747a8b",
            "gallery_name": "gallery-1623265514033",
            "height": 300,
            "pitch": 0,
            "quality": 1.3561,
            "roll": 2,
            "status": "success",
            "subject_id": "subject-1623265514033",
            "topLeftX": 105,
            "topLeftY": 117,
            "width": 233,
            "yaw": 2
        }
    }
]
```

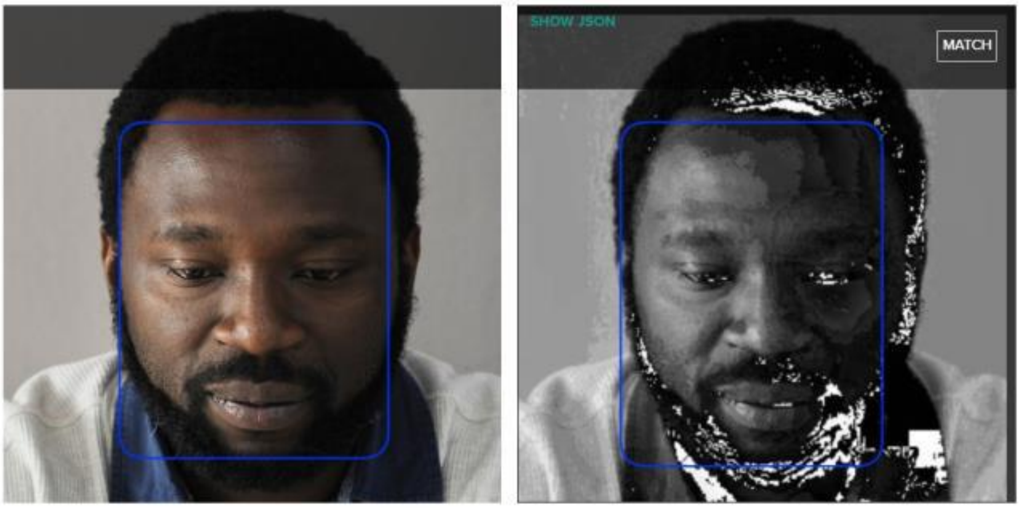
## Image 5

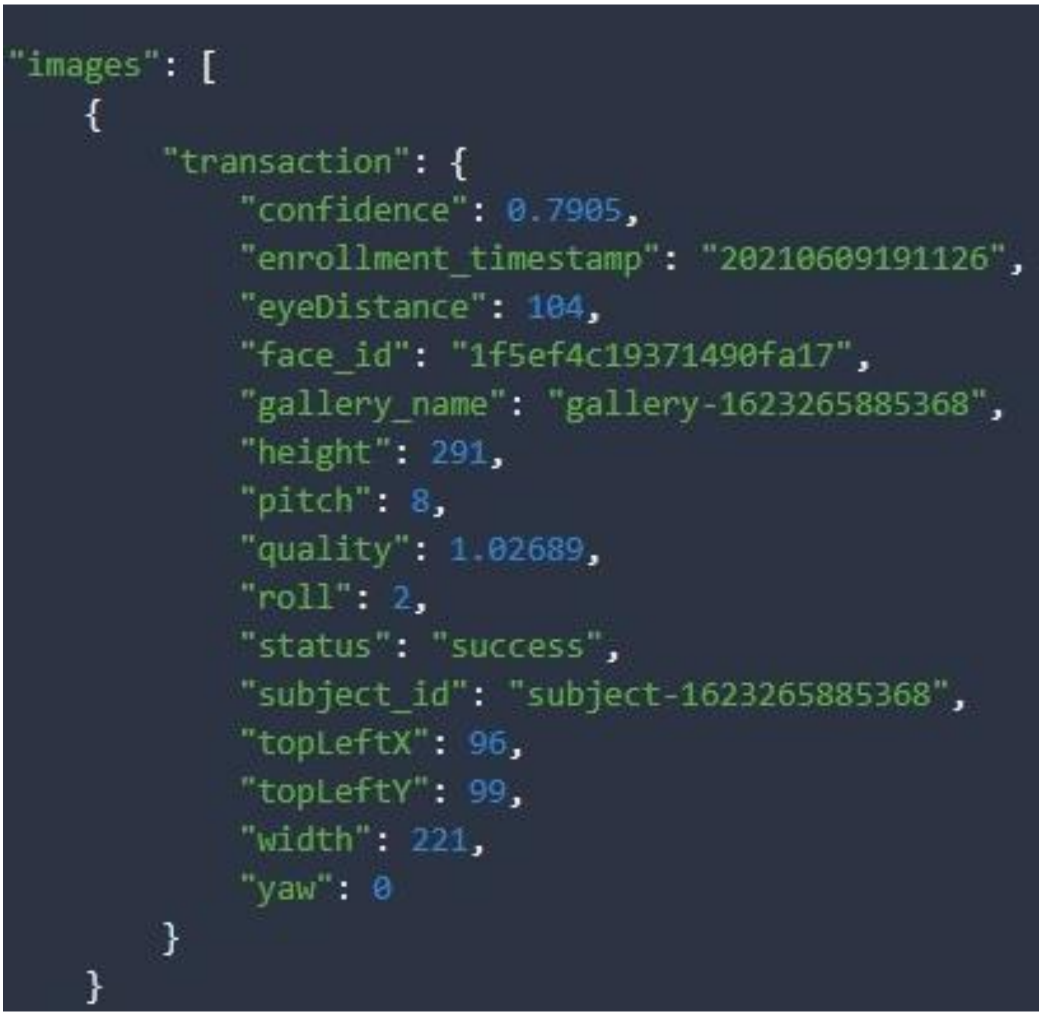




```
{
    "images": [
        {
            "transaction": {
                "confidence": 0.90513,
                "enrollment_timestamp": "20210609190657",
                "eyeDistance": 111,
                "face_id": "2cdaa5da894b4b5c9a3",
                "gallery_name": "gallery-1623265616329",
                "height": 308,
                "pitch": 2,
                "quality": 0.24949,
                "roll": -6,
                "status": "success",
                "subject_id": "subject-1623265616329",
                "topLeftX": 117,
                "topLeftY": 102,
                "width": 251,
                "yaw": -16
            }
        }
```

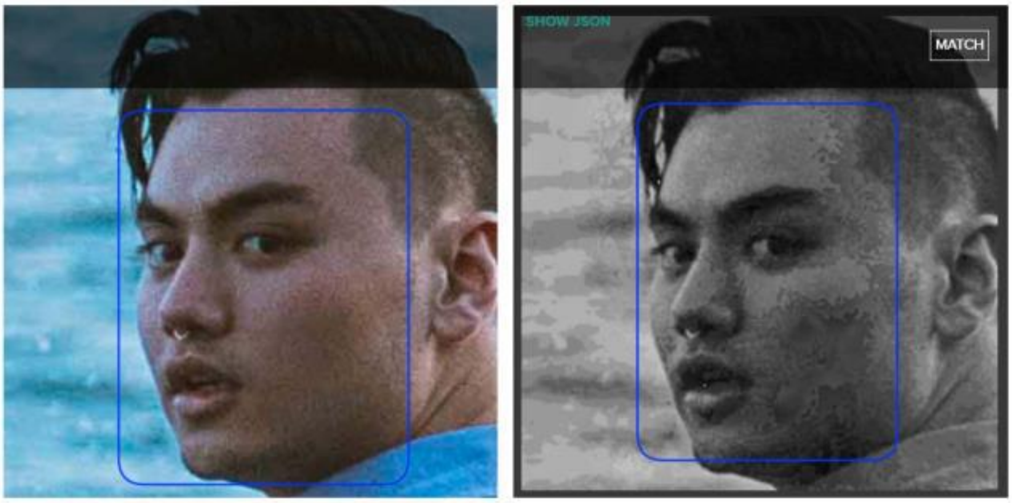
## Image 6

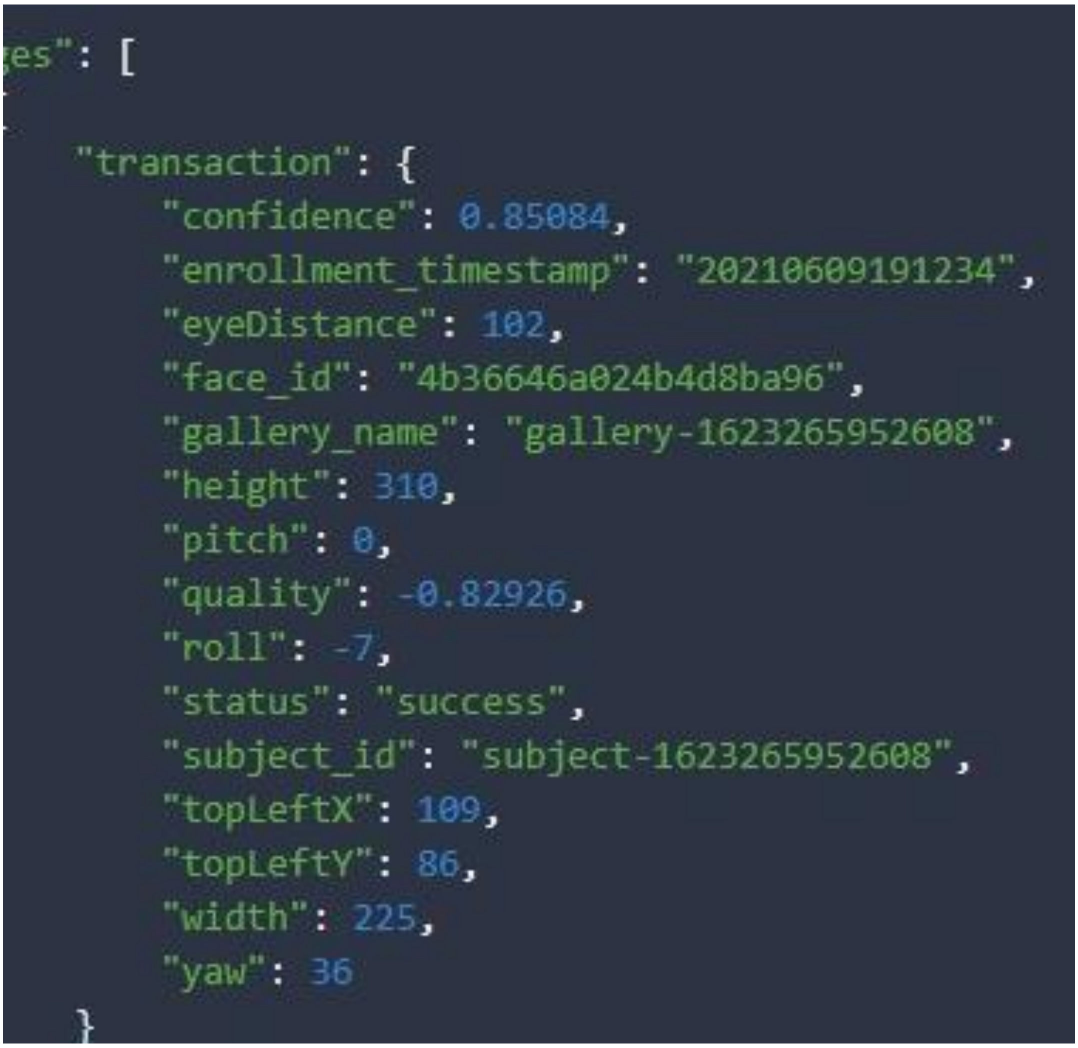




```
"images": [
    {
        "transaction": {
            "confidence": 0.7905,
            "enrollment_timestamp": "20210609191126",
            "eyeDistance": 104,
            "face_id": "1f5ef4c19371490fa17",
            "gallery_name": "gallery-1623265885368",
            "height": 291,
            "pitch": 8,
            "quality": 1.02689,
            "roll": 2,
            "status": "success",
            "subject_id": "subject-1623265885368",
            "topLeftX": 96,
            "topLeftY": 99,
            "width": 221,
            "yaw": 0
        }
    }
```

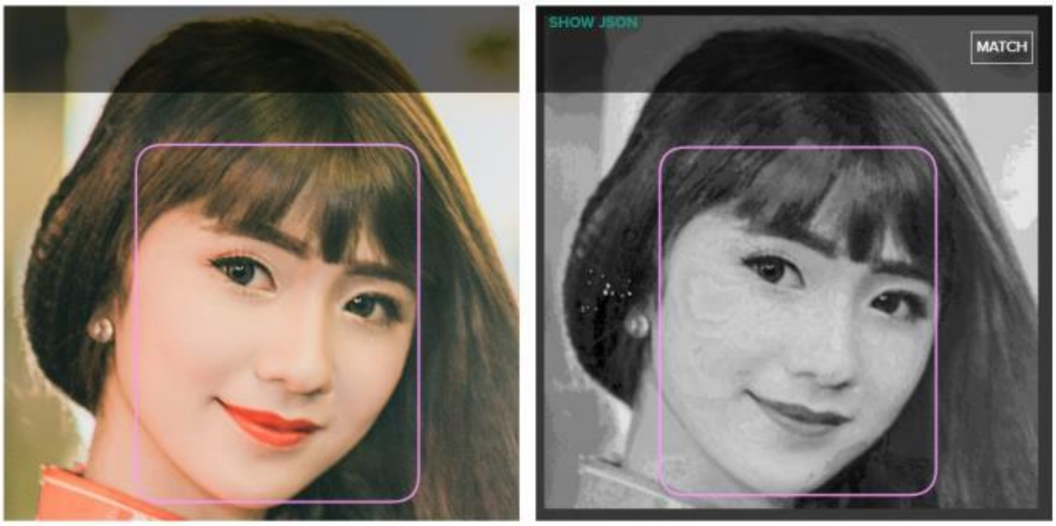
## Image 7

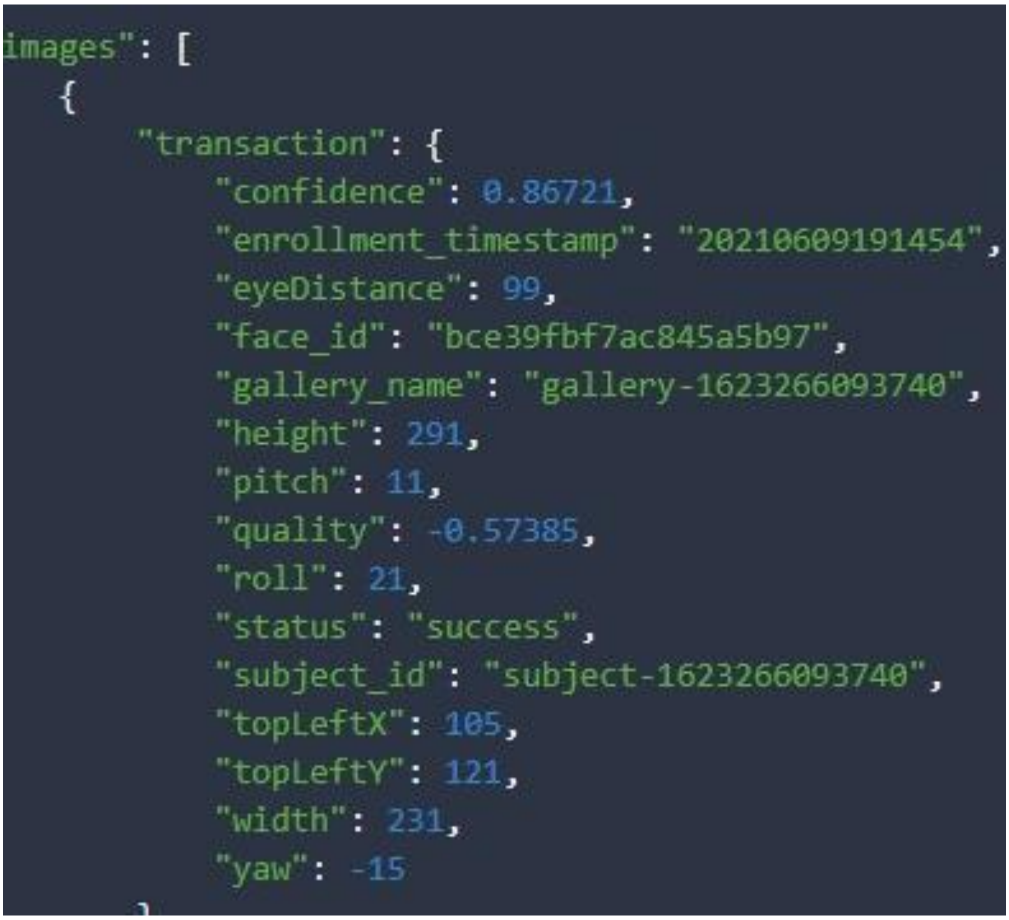




```
es": [

    "transaction": {
        "confidence": 0.85084,
        "enrollment_timestamp": "20210609191234",
        "eyeDistance": 102,
        "face_id": "4b36646a024b4d8ba96",
        "gallery_name": "gallery-1623265952608",
        "height": 310,
        "pitch": 0,
        "quality": -0.82926,
        "roll": -7,
        "status": "success",
        "subject_id": "subject-1623265952608",
        "topLeftX": 109,
        "topLeftY": 86,
        "width": 225,
        "yaw": 36
    }
```

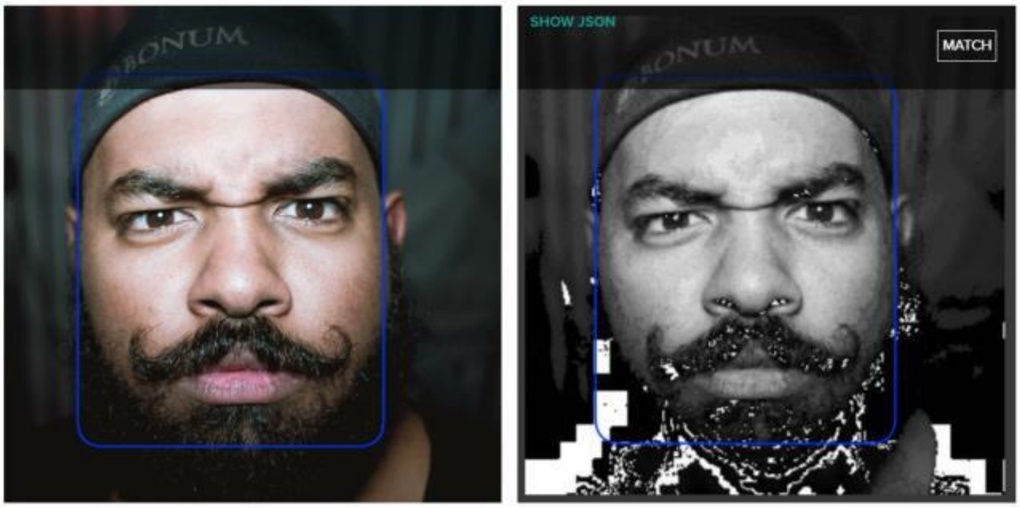
## Image 8

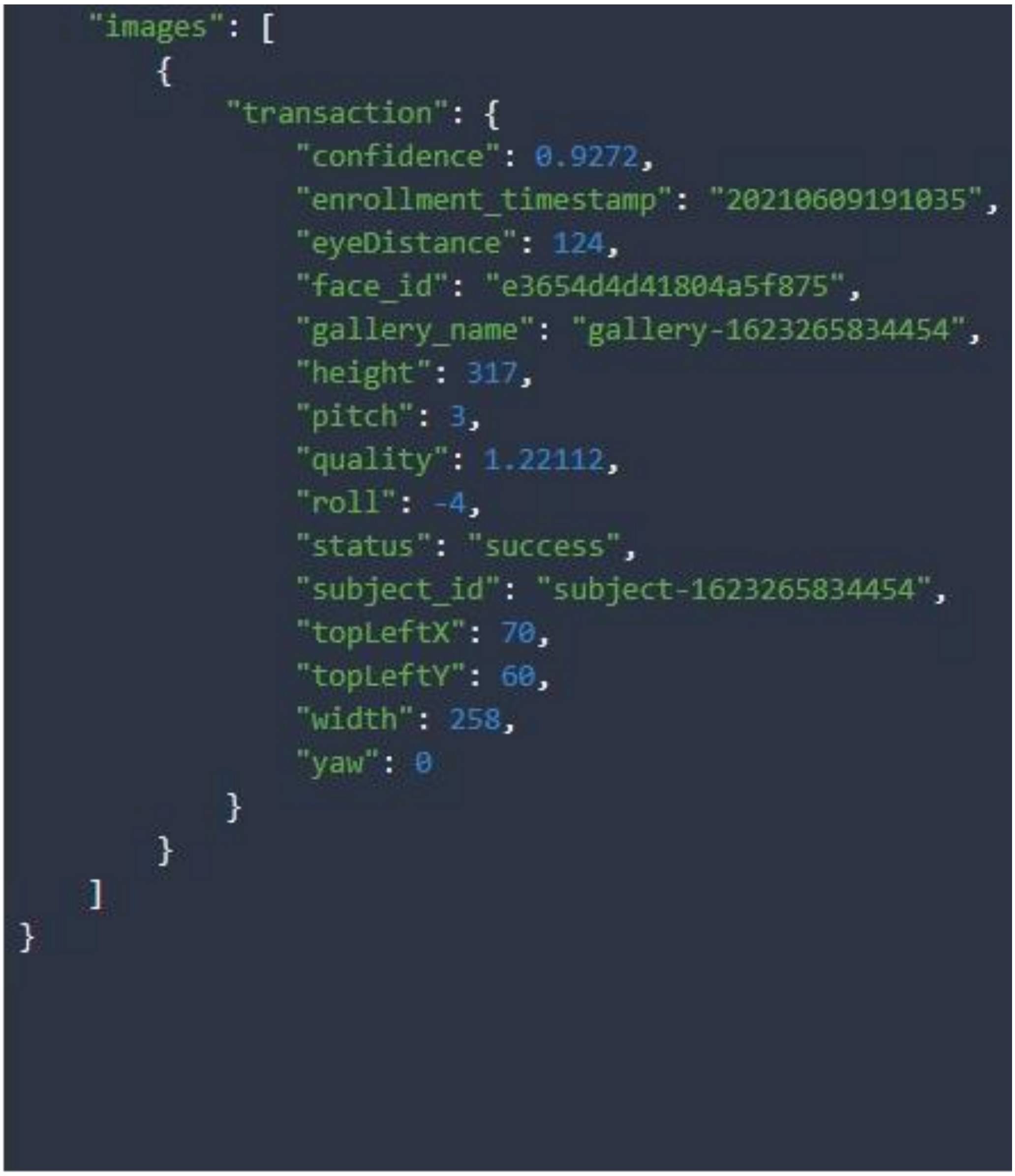




```
images": [
  {
      "transaction": {
          "confidence": 0.86721,
          "enrollment_timestamp": "20210609191454",
          "eyeDistance": 99,
          "face_id": "bce39fbf7ac845a5b97",
          "gallery_name": "gallery-1623266093740",
          "height": 291,
          "pitch": 11,
          "quality": -0.57385,
          "roll": 21,
          "status": "success",
          "subject_id": "subject-1623266093740",
          "topLeftX": 105,
          "topLeftY": 121,
          "width": 231,
          "yaw": -15
      }
```

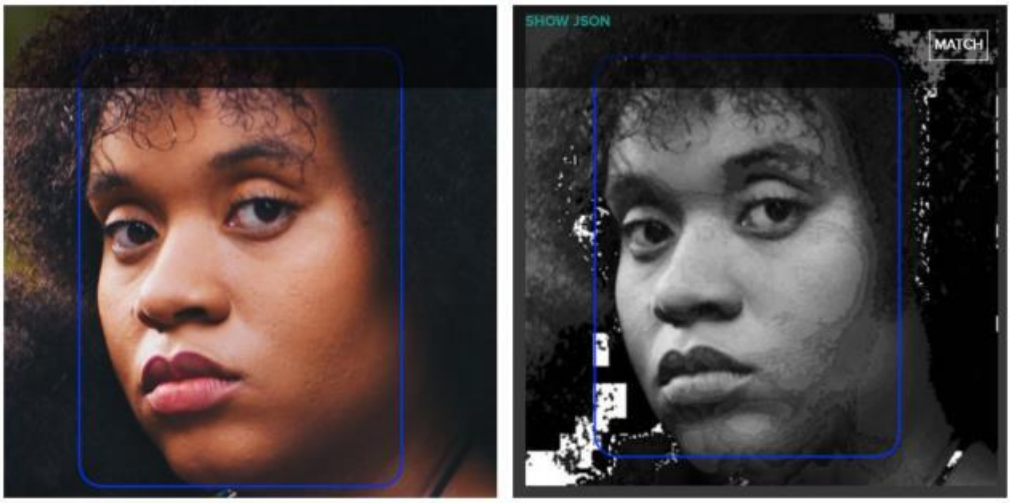
## Image 9

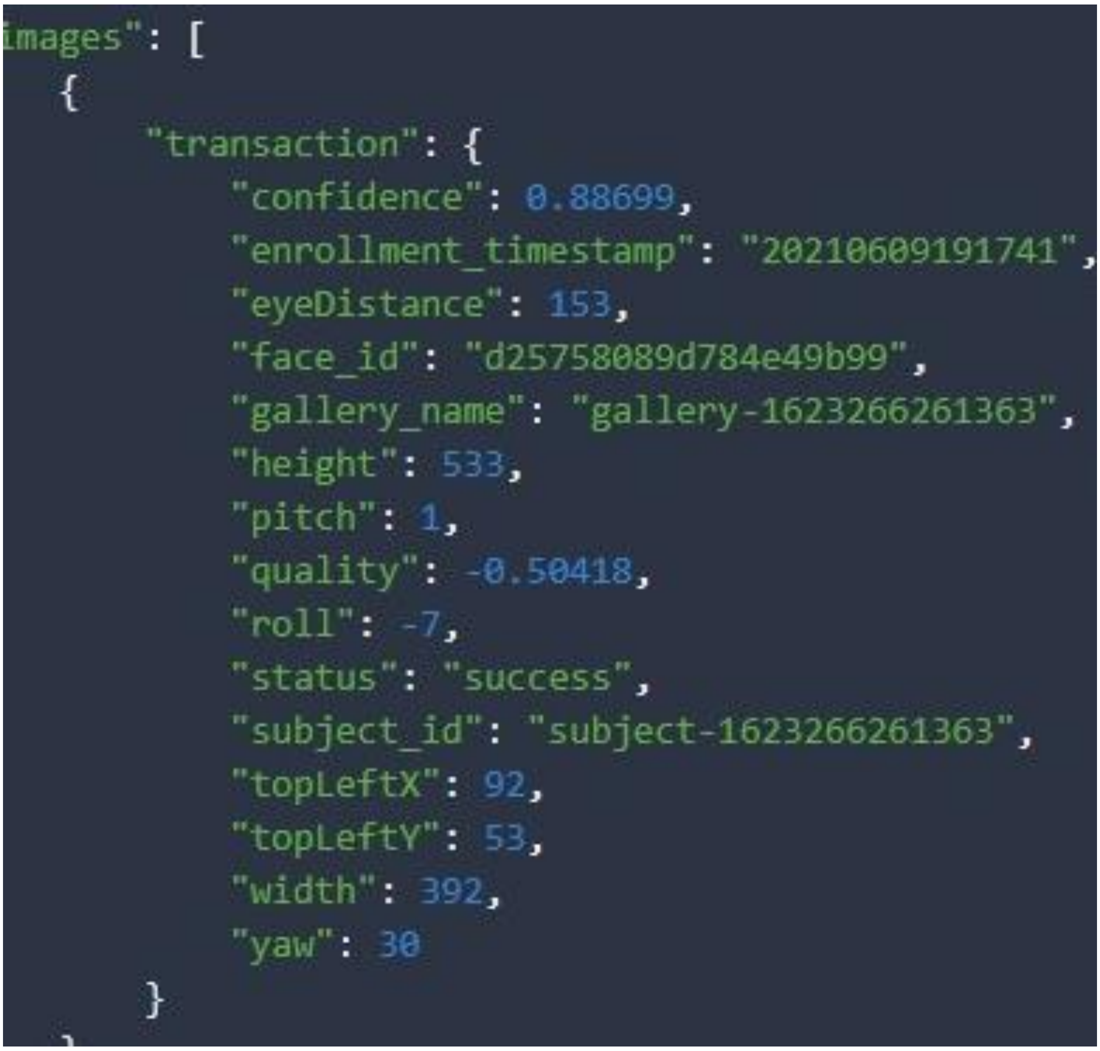




```
    "images": [
        {
            "transaction": {
                "confidence": 0.9272,
                "enrollment_timestamp": "20210609191035",
                "eyeDistance": 124,
                "face_id": "e3654d4d41804a5f875",
                "gallery_name": "gallery-1623265834454",
                "height": 317,
                "pitch": 3,
                "quality": 1.22112,
                "roll": -4,
                "status": "success",
                "subject_id": "subject-1623265834454",
                "topLeftX": 70,
                "topLeftY": 60,
                "width": 258,
                "yaw": 0
            }
        }
    ]
}
```

## Image 10





```
images": [
    {
        "transaction": {
            "confidence": 0.88699,
            "enrollment_timestamp": "20210609191741",
            "eyeDistance": 153,
            "face_id": "d25758089d784e49b99",
            "gallery_name": "gallery-1623266261363",
            "height": 533,
            "pitch": 1,
            "quality": -0.50418,
            "roll": -7,
            "status": "success",
            "subject_id": "subject-1623266261363",
            "topLeftX": 92,
            "topLeftY": 53,
            "width": 392,
            "yaw": 30
        }
    }
```

We also compared our proposed method with two other traditional methods, black box and blurring.

| **Metric** | **Black box** | **Blurring** | **Our method** |
|---|---|---|---|
| **Accuracy rate of non detection of face and facial points after image is de-identified** | **20%** | **20%** | **80%** |

## CONCLUSION AND FUTURE ENHANCEMENT

Thus, we can conclude that we are able to de-identify the images successfully with an accuracy of 80% as mentioned in the comparative analysis. Our modified averaging over images method was able to de-identify and recover the images successfully. The facial recognition software were able to match the recovered images with the original or main images with a confidence level of 85.08%. Our model was also able to out-perform the traditional methods and overcome the drawbacks of the traditional methods.

## 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.

The link below is for the code implemented for de-identification as well as comparison with the two traditional methods

**https://colab.research.google.com/drive/1YERTgzUhkzE77E6PJRcQyiWOgt25Pn_e?usp=sharing**