OPEN ACCESS
Vietnam Journal of Computer Science
Vol. 9, No. 2 (2022) 187–202

DOI: 10.1142/S2196888822500105

World Scientific
www.worldscientific.com

In Your Face: Person Identification Through Ratios and Distances Between Facial Features

Mohammad Alsawwaf

School of Electrical and Data Engineering
University of Technology Sydney
15 Broadway Ultimo, NSW 2007, Australia

College of Comp. Science and Information Tech.
Imam Abdulrahman Bin Faisal University
King Faisal Road, Dammam 34212, Saudi Arabia
mohammad.alsawwaf@uts.edu.au; malsawwaf@gmail.com

Zenon Chaczko

School of Electrical and Data Engineering
University of Technology Sydney
15 Broadway Ultimo, NSW 2007, Australia

Marek Kulbacki

R&D Center, Polish-Japanese Academy of
Information Technology
Warszawa, Poland, DIVE IN AI, Wroclaw, Poland

Nikhil Sarathy

School of Electrical and Data Engineering
University of Technology Sydney
15 Broadway Ultimo, NSW 2007, Australia

Received 14 June 2020
Accepted 11 August 2021
Published 17 November 2021

These days identification of a person is an integral part of many computer-based solutions. It is a key characteristic for access control, customized services, and a proof of identity. Over the last couple of decades, many new techniques were introduced for how to identify human faces. This approach investigates the human face identification based on frontal images by producing ratios from distances between the different features and their locations. Moreover, this extended version includes an investigation of identification based on side profile by extracting and diagnosing the feature sets with geometric ratio expressions which are calculated into feature vectors. The last stage involves using weighted means to calculate the resemblance.

The approach considers an explainable Artificial Intelligence (XAI) approach. Findings, based on a small dataset, achieve that the used approach offers promising results. Further research could have a great influence on how faces and face-profiles can be identified. Performance of the proposed system is validated using metrics such as Precision, False Acceptance Rate, False Rejection Rate, and True Positive Rate. Multiple simulations indicate an Equal Error Rate of 0.89. This work is an extended version of the paper submitted in ACIIDS 2020.

Keywords: Biometrics; geometric ratios; pixel segmentation; DNN; XAI; identification; feature extraction; human recognition; feature vector.

1. Introduction

1.1. *Background*

Identification of humans based on facial characteristics is a widely used access control technique. Nowadays, the technique is seen in almost all electronic devices like tablets and smartphones. It is also used widely in identity proof applications and even in obtaining access to physical locations like research facilities, labs and pharmacies. Some smart homes also implement security systems that use facial features to enter or grant access to different facilities.[1]

There are multiple steps involved in the facial recognition process.[2] The flow of these steps varies based on the system that they are part of. Generally, the first step is face detection where the system tries to locate a face in a given image or video stream. If a face is found, extraction of the features usually follows. Then, based on the chosen method of identification and verification, an algorithm is applied to get the final results. Figure 1 shows the general flow diagram of these steps.

There are also multiple approaches to the face detection procedure. Some of these approaches are referred to as feature-based while others are referred to as image-based. Figure 2 shows a visual taxonomy of different face detection techniques. From these different approaches, Neural Networks (NN), more specifically Convolutional Neural Networks (CNN's), is one the of best and most successful due to the greatly improved results it produces over other methods.[3] CNN's are based on

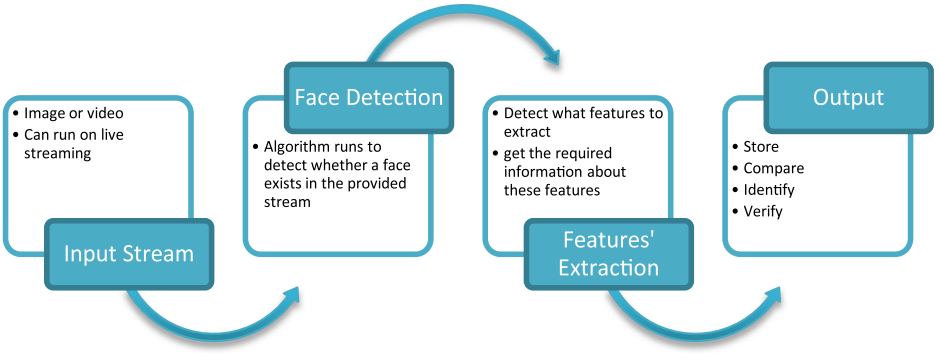

Fig. 1. Generic face recognition steps.

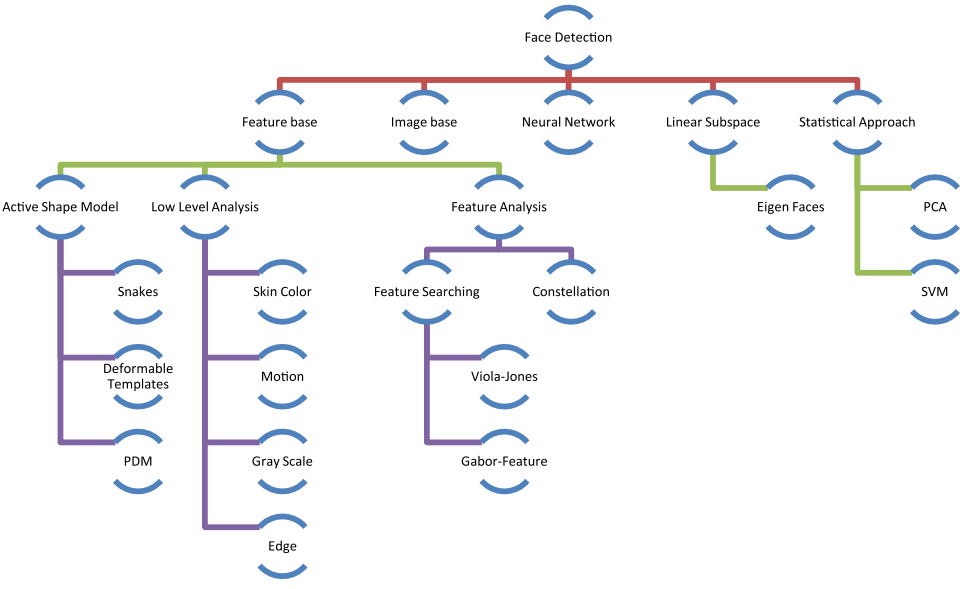

Fig. 2. Taxonomy of face detection techniques. Adopted from Ref. 5

deep learning and considered the current state-of-the-art in terms of accuracy and benchmarking.

Facial recognition, like other computer systems, has many challenges. Currently adopted approaches face difficulties with obstacles, expressions that are not defined, lightning, and even noise.[4] Additionally, identity morphing and theft attacks are becoming more aggressive which is another challenge that needs consideration.[5]

On top of these challenges, there are concerns regarding (1) privacy when storing peoples' faces on databases, (2) storage capacity as these databases can grow and consume a lot of storage space when storing comparison templates,[6] (3) how fast can results be calculated, and most importantly (4) how these calculations are completed and is it possible for a user of the system to understand why a certain result has been reached. In many deep learning approaches, it is very difficult, sometimes impossible, to understand why the system concluded that a match is in place or why not.

This paper aims to present an innovative explainable method for facial recognition from images for the purpose of access control. The proposed method uses advanced segmentation to extract the relevant facial features. The extracted features are then used to produce feature-based vectors that are utilized to complete the recognition process.

1.2. *Paper structure*

Two proposed experiments took place consecutively in this paper. The first experiment uses the python open-source face detection library to detect a face in an input image or moving in the view field of the camera. Then, the first algorithm is applied

to calculate different distances between the relevant chosen points of interest. The second experiment is for face profile and it uses deep learning models for the detection part of the features. Then another explainable feature vector comparison takes place for the identification. In each experiment section, an overview, setup, and discussion subsections are provided. Finally, a conclusion with potential future work is given.

2. Experiment 1: Frontal Face

2.1. *Overview and setup*

This experiment refers to python's open source face recognition library by Ref. 7 which is based on dlib.[8] Dlib is a C++ toolkit written with support for python along with examples of how to use it. The toolkit contains algorithms that use machine learning for a variety of applications, one of which is the face detection. This face detection part is adopted in this paper to offer a complete solution for the access control. But it is not the focus of this paper or the proposed solution. However, it is important to introduce how the face detection works to move on to the next parts.

In this python library, the face detection algorithm extracts and displays the pixel coordinates of each detected face in a given image. It follows a face template that contains 68 different landmarks and if a match is found, then a face has been detected and the coordinates are printed. Figure 3 shows the Face Landmarks Template used in dlib.

This approach is intended to identify a person based on detecting the face from a camera live feed, save the face image in order to process it, compare the results to the enrolled subjects in the database, and finally either grant access to that person or

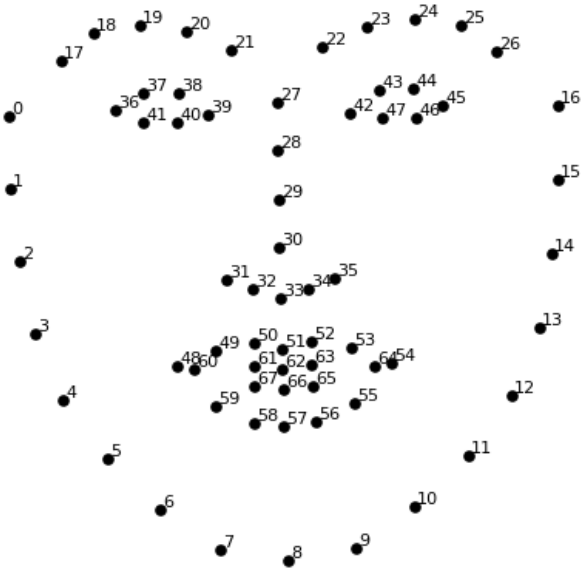

Fig. 3. Face Points Template extracted from dlib.[7]

deny it. Alternatively, the proposed system accepts an image as an input and checks if it contains a face in order to move on to the processing stage.

When a face is detected and the processing phase starts, the proposed algorithm uses the face template provided to calculate the distances between points of interest as follows: (1) the near ends of the eyes which correspond to points 39 and 42 in Fig. 3, (2) ear-to-ear which correspond to points 0 and 16, (3) nose-top to bottom of the nose which are points 27 and 33, and (4) nose-top to the chin which are points 27 and 8 in the same figure. These computations produce the face length and width resulting in complete face ratios. Based on the calculated ratios, a unique identifier is issued per image. This identifier is the base advantage of this first proposed approach. It is also what will be tested for use as identification for access control.

In some face identification systems, an actual photo of the subject being identified is registered in the database. When access control is needed, the image is retrieved and the matching is conducted. The notion of using unique identifiers results in various advantages. It omits the need for comparing the new and the registered pictures. Rather, only numbers are registered and matched every time the identification is needed. Hence, making the identification process much faster. Additionally, there is an exclusion of the fact that the operation invades privacy. This is accomplished by storing only the unique identifier and not the actual image of the face. Finally, there is a significant amount of storage that can be freed because no photos are required to be saved anymore.

This proposed method assumes the following:

- Frontal face pictures or a live feed with a person passing showing frontal face are used.
- Pictures are illuminated enough around the face to show the features.
- Full faces show in the pictures and live feed.

The approach locates the coordinates of each given point. For example, point 39 in the template is demonstrated in Table 1. The algorithm obtains the x and y coordinates of each relevant point. Table 1 also shows the list of relevant points needed in the algorithm:

Then, use the following formula to find the distance between the eyes:

$$\text{Distance} = \sqrt{(X_i - X_{i-1})^2 + (Y_i - Y_{i-1})^2}, \tag{1}$$

where X_i is representing x_2 in Table 1 which is the x-axis coordinate of the second point in "near ends of eyes" in the table (left eye). Similarly, X_{i-1} is representing x_1

Table 1. Distances calculated on facial features and their corresponding points from Fig. 3.

No.	Description	Corresponding points in Fig. 3
1	Near ends of eyes	$39(x_1, y_1) - 42(x_2, y_2)$
2	Ear to ear	$0 - 16$
3	Nose length	$27 - 33$
4	Nose to chin	$27 - 8$

in Table 1 which is the x-axis coordinate of the first point in "near ends of eyes" (right eye). The same applies to the Y_i and Y_{i-1} which represent the y_2 and y_1 consecutively in the same table. These formulas are applied on all listed points in Table 1. Then the following formulas are applied to find the ratios for the face length and width:

$$\text{Ratio}_{\text{width}} = \frac{D_{\text{Between eyes}}}{D_{\text{Between ears}}}, \tag{2}$$

$$\text{Ratio}_{\text{length}} = \frac{D_{\text{Nose Length}}}{D_{\text{Nose to Chin}}}. \tag{3}$$

2.2. *Analysis and results*

The software is given an image, batch of images, or a live video stream as input. After some modifications and tweaks to the face detection part of the python library, the software is capable to detect faces and apply the facial template to them.

A test set with two siblings' has been created using the same settings for the photo shoot. With both of the siblings, the camera was 120 cm away from them and it was placed at line-of-sight in terms of height. Captures occurred at the same time to ensure the same surrounding illumination. Both siblings were requested to perform three different postures, smiling, mouth open, and neutral. The captured photos are displayed in Fig. 4.

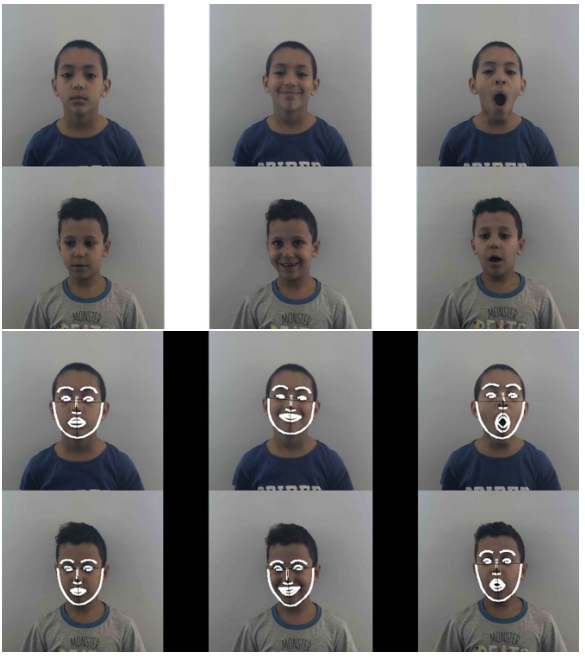

Fig. 4. Two siblings' photos taken with identical situations: Row 1 Subject (1) with three stances, Row 2 Subject (2) with three stances — Owned Pictures.

Table 2. Identifiers for the test set of siblings.

Subject	Stance	Width ratio	Length ratio	Identifier
1	Neutral	0.270701	0.418404	0.2707 : 0.4184
2	Neutral	0.251650	0.431787	0.2483 : 0.4317
1	Open mouth	0.267701	0.342805	0.2677 : 0.3428
2	Open mouth	0.236177	0.363249	0.2361 : 0.3632
1	Smiling	0.281542	0.413448	0.2815 : 0.4134
2	Smiling	0.252807	0.428302	0.2528 : 0.4283

Now, the system is provided with the captured photos to detect faces and apply the template. Then the calculations are applied to get the results and produce the unique identifier for each image as per Table 2.

The above results can be very valuable to this research as the subjects are siblings with significant similarities in appearance and they are very close in age but not twins. These results show enough difference to distinguish between these two siblings when looking at the identifiers. For subject 1, in the width ratio, it can be observed that there is a maximum of 0.014 difference between the different stances for the width ratio. However, if we compare both subjects to each other, we find that the minimum difference is 0.015.

This means that it is possible to set a threshold between the two siblings for face width to identify one over the other for access control. Moreover, by looking at the face width identifier for both subjects, it can be observed that subject one's face width ratio appears to be greater than subject two's face while subject two's face length ratio appears to be greater.

For this experiment, the Labeled Faces in the Wild (LFW) dataset has been utilized with 13,233 tagged pictures for 5749 individuals with 1680 of them with 2 or more images. This dataset is used because it was designed for "studying the problem of unconstrained face recognition" and developed by the University of Massachusetts, Amherst.[9] The size of this library allows for it to be used in research without suffering from storage space or using it with high-performance computing power. Besides, it is utilized widely for benchmarking by many works of literature making it ideal for this experiment.

Since this frontal face method is divided into two parts, mainly detection and identification, the 10-fold cross-validation was used to benchmark the detection part of the approach. This result is adopted to show that the system as whole is consistent even though this is not the main focus on this method. Using this K-fold technique eliminates the "too optimistic" results and makes them more realistic.[10] However, the identification part, which is the main contribution in this method, was benchmarked using the Equal Error Rate due to the statistical nature of the identification algorithm.[11]

Using the 10-fold cross-validation for the detection of faces, an accuracy of 99.38% has been reported (see Table 3). This means that out of the 13,233 images, faces were correctly detected and landmarked in 13,150 of them.[7]

Table 3. Statistics of publicly available academic benchmark datasets.

Dataset	Purpose	No. of images	Accuracy
LFW[9]	Testing	13,233	99.38%

Table 4. Performance comparison on LFW dataset.

Algorithm	Accuracy	EER
HoG + Sub-SML	88.34	11.45
LBP + Sub-SML	83.54	16.00
FV + Sub-SML	91.30	8.85
Deep features	99.38	0.62
This approach	93.30	6.85

Out of the detected pictures, the identification algorithm populated ratios for subjects with more than one image for a total of 1680 individuals. However, after recording all of these ratios for the 1680 subjects, the actual matching step ran on 100 images and achieved the outcomes in Table 4. The table also benchmarks this approach with other identification approaches on the same dataset.

Even though this approach's results have a lower accuracy than the current state-of-the-art, deep features, this is being compensated by providing very high explainability which other approaches are unable to provide. Higher explainability means that a system admin can know why, why not, and how a subject is given access. Thus, allowing for enhancement of the accuracy while maintaining the explainability.

This is a step to try and solve issues like pinpointing why a system using deep learning has granted access to a subject's identical twin for example which is a growing concern. By increasing the explainability and basing the identification on a glass box calculations, where everything is clear, system developers can know why these issues are happening and how to attempt to fix them.

3. Experiment 2: Face-Profile

3.1. *Overview and setup*

Face-profile identification is harder than frontal and more complicated because less information can be extracted with less features. In this case, it means that only half of the features are visible and not from a frontal view. Therefore, extracting the contour and identifying prominent features is a key step.

Also, finding relations between these extracted features that could potentially lead to an identifying combination is also important. Thus, the experiment in this section will explain how this approach is attempting to extract the needed information and features. Figure 5 shows the process diagram of the face profile

recognition. The following assumptions have been observed in the experiment of the face-profile identification:

- Input images are taken with good lightning where facial features are visible.
- The SiblingsDB dataset consisting of 420 side profiles of different subjects have been used for training and validation of the network-based prediction model. For the system performance measurement, five subject's same face side photos were used.
- All the faces considered for the experiment have minimal or no rotation.
- Final validation images are segmented manually for the purpose of the experiment results, while on the other hand, a deep learning model has been trained to segment the relevant features automatically including the ear.

3.1.1. *Facial feature detection: Deep learning models*

In the first stage towards extraction of the face-profile features, two deep learning approaches are considered, YOLO V2 and pixel-based segmentation. First, YOLO v2 was used, employing deep neural networks (DNN) model. A custom model was prepared for training using 400 face-profile images from publicly available datasets.[12] A loss convergence rate of around 3.0 was found. This delivered reasonably suitable bounding box results for the relevant facial features. These features are ear, nose, forehead, eyes, mouth, and chin.

The second approach, also employing DNNs, is the pixel-based segmentation using Mask R-CNN model.[13] In this model, a subset of face-profile images was used for the training. The aim was to primarily analyze two specific outputs — the pixel boundary coordinates and the overall correctness of the feature pattern points. Manual annotation was done in this stage using the image annotator tool for reasons highlighted in the assumption section.[14]

A dataset consisting of around 50 images of face-profile for five different subjects with a fixed resolution was used. The next step, after obtaining the detected features, focuses on extracting the contour points for each feature.[15] The limitation faced was in dealing with clustered points. In many instances, out-liers were present, which made the construction of an accurate polygon to represent the features precisely harder to achieve.

3.1.2. *Geometric ratio vectors: Inter-feature properties*

Feature detection occurs following the construction of the polygon contour, which is constructed from the outline points of the feature. The created contour is inserted into a set of equidistance points that vary from 30 to 50 points depending on the feature. These points serve as inputs to the vector function. This is performed to enable point-to-point distance and derive angular variations among sets of features.

To exemplify this, consider the distance between each point on the ear to all points on the nose. This is a set to be considered in the calculations. Other examples

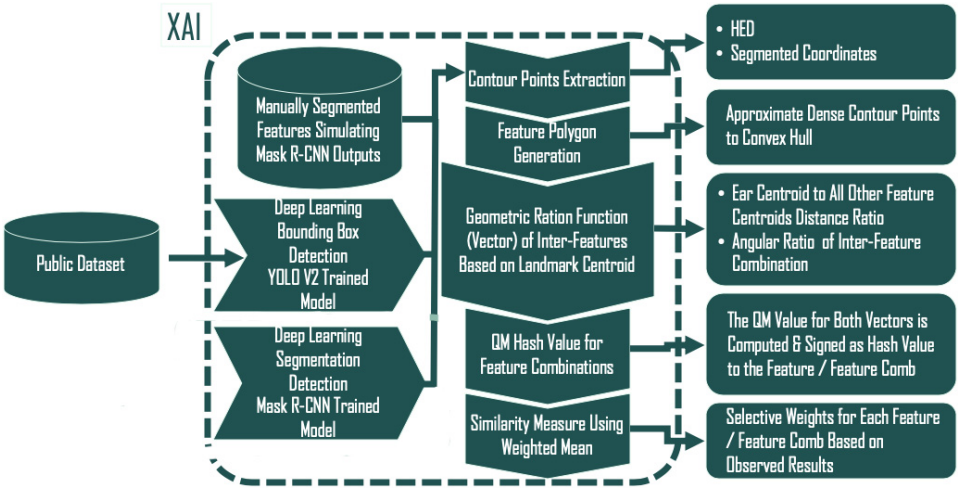

Fig. 5. Explainable Face-Profile Recognition Algorithm Flow: This process diagram shows the different steps in the methodology — facial feature extraction, geometric vector construction and similarity measure.

include ear to forehead and forehead to nose. These computations are very crucial in obtaining the geometric signature for the considered feature. This signature is hypothesized to be unique for each feature and also for inter-feature patterns as well.[16]

In the experiments, two geometric functions have been considered for calculating the feature vectors: 1. Distance ratio functions and 2. Angular functions. Ratios and angular criteria have been widely used in facial recognition. However, in this experiment, the application of functions on a large set of points strongly employs the distinctive inter-feature linking. As a brief instance, this paper will discuss only a distinct case of interval ratio function, which is the ear-chin-nose correlation. The contributed algorithm uses several inter-feature combinations repeated on all points of the contours. To be more precise, a feature-set consisting of 15 and 9 is used sequentially for the distance ratio and angular computations. The following formulas (4) and (5) define the creation of a distance ratio feature vector.

$$f_{\text{chin}-\text{nose}_i} = \frac{d_{i-C_{\text{ear}}}}{d_{i-C_{\text{nose}}} * \cos\theta}, \tag{4}$$

where $f_{\text{chin}-\text{nose}_i}$ denotes the point function of the specific feature combination, in this case chin is centroid to point i on the nose contour and $d_{i-C_{\text{ear}}}$ and $d_{i-C_{\text{nose}}}$ denote the distances between a contour point i and the respective feature centroid for ear and nose.

$$\mathcal{V}_{\text{chin}-\text{nose}} = \{\underset{i=1}{\overset{i=n}{}} f_{\text{chin}-\text{nose}_i}\}, \tag{5}$$

where $\mathcal{V}_{\text{chin}-\text{nose}}$ denotes the feature vector for the specific combination in this case chin to nose.

The geometric combinations used for the vector representation follows a specific order on the polygon. In turn, this ensures that vectors of similar features from different subjects are comparable. This approach of feature vector computations is similar to early attempted research.[17] However, it is significantly distinct in the way the vectors are created by utilizing several geometric functions that compare the features using corresponding centroids.

3.1.3. *Feature hash value and similarity measures*

After conducting multiple tests using the acquired vectors, encouraging results were observed. Preliminary trials to estimate the similarity of two comparable feature vectors (ex: ear-nose distance ratio vector, ear-frontal features angular ratio vector) using cosine similarity and Euclidean and Minkowski distances yielded inconsistent results. Particularly, few false positives and false negatives. Suggesting that even when matching feature vectors of the same subject in different stances, a notable variation in corresponding features was seen.

In contrast, the overall shape and positional characteristics of the features seem similar. Hence to overcome these concerns, this research adopted a simpler and explainable technique. It is mainly concentrating on comparing the derived quadratic mean (QM) of two related vectors. These values showed distinctive and consistent results for different feature combinations of a specific person. Therefore, the QM of the vectors has been accepted as the "hash" value. This is performed to describe the various features and their combinations numerically. The formulation of QM is given as follows:

$$\mathrm{QM} = \sqrt{\frac{\sum_{i=1}^{i=n} \mathcal{R}_i^2}{n}}. \tag{6}$$

After attributing the features with the hash value (QM) in formula (6), the final step is calculating the overall similarity. A similarity score of two comparable vectors of feature combinations is computed and is displayed as the percentage difference. Formula (7) denotes the calculation of the similarity using QM.

$$\mathcal{S}_{\text{similarity}}(\mathcal{QMV}1, \mathcal{QMV}2) = \frac{|\mathcal{QMV}1 - \mathcal{QMV}2|}{\max(\mathcal{QMV}1, \mathcal{QMV}2)}. \tag{7}$$

Table 5 compares the QM value of the distance ratio vector ($\mathcal{V}$) for various inter-feature combinations of a specific subject against the prediction of different images — Subject 1. Each of the shown five combination's geometric computations are with respect to the ear's centroid.

Table 6 compares the QM value of the angular ratio vector ($\mathcal{V}$) for the five side facial features of a specific subject against the prediction of different images — Subject 3. The angular feature vector is constructed using a combination of point to point as well as point to centroid angles in radians.

Table 5. QM (hash values) of the various inter-feature combinations of Subject-1.

	Picture ID of the Same Subject		
Feature ID	Pic1	Pic2	Pic3
Eye-to-Nose	4.5175	5.1894	4.3468
Eye-to-Forehead	21.5947	19.1717	20.5560
Eye-to-Chin	2.2930	2.3617	2.2964
Nose-to-Nose	44.1705	45.1848	41.0454
Nose-to-Forehead	18.0604	17.0112	16.0835

Table 6. QM (hash values) of the facial features of Subject-3 derived from the angular vector.

	Picture ID of the same subject			
Feature ID	Pic1	Pic2	Pic3	Pic4
Ear	0.5578	0.5617	0.5435	0.5549
Eyes	0.7768	0.7324	0.7327	0.7214
Nose	0.5736	0.5838	0.5775	0.5836
Forehead	0.5618	0.6398	0.6280	0.6215

3.2. *Analysis and results*

Obtained results from the conducted experiments exhibit compelling findings of the geometric characteristics of the face-profile features. Moreover, the common challenges confronted while extracting the feature contours and consequent calculations in inter-feature measurements can unlock new perspectives for future research in this area. Finally, conventional performance benchmark techniques have been used for the validation of similarity.

Table 7 shows the performance metrics of the system achieved during the trials conducted. The threshold values outline the probabilistic degree of similarity between two given face-profile images. The difference in the False Acceptance Rate (FAR) and False Rejection Rate (FRR) drops with the increase of the threshold. On the other hand, the True Positive Rate (TPR) starts decreasing. It can be stated here that the average similarity score between two images of the same subject is around

Table 7. Performance metrics of the xFPR algorithm based on multiple simulations.

	Performance metric of the algorithm			
Decision threshold	Recall/TPR	Precision	FAR	FRR
0.9610	0.91	0.70	0.14	0.10
0.9620	0.89	0.72	0.12	0.11
0.9630	**0.89**	**0.74**	**0.11**	**0.11**
0.9640	0.88	0.75	0.10	0.12

0.96. In contrast, the score of images of different subjects tends to range between 0.85 and 0.93. This indicates that examining side faces using geometric computations requires high precision as there are only slight differences in the human side profile under the discussed experimental setup and assumptions. Figure 6 shows the EER diagram of the results achieved.

3.2.1. *Pixel segmentation-based DNN model for side face contours*

The two procedures that have been used to derive the specific contour points from the face profile present a good insight into feature extraction. Although the HED-based DNN model in combination with the YOLO-v2 deep learning model was effective in extracting explicit contour points, the limitations inflicted by the outliers points (from neighboring features) inside the bounding box ultimately impacted the precision of the comparison measures. The challenges can nevertheless be overcome to a degree by using more advanced DNN models such as YOLO v3 and Single Shot Detector (SSD). Moreover, custom clustering approaches specific to a feature pattern such as ear can increase the precision of the feature vectors created using approximated polygons. Consequently, it is believed that this method has scope to be further enhanced and have a potential contribution to facial feature extraction techniques inflicted.

In the second technique that uses the manual pixel segmentation of features, extraction of a particular set of contour points was achieved. This has inspirited our future work toward using advanced DNN models such as Mask R-CNN. Experiments implementing this are currently undergoing. The segmented pixels approach has a high advantage over the bounding box technique since the "region of interest" becomes a lot more specific generating far fewer outliers. We propose the pixel segmentation-based DNN model as an effective technique for

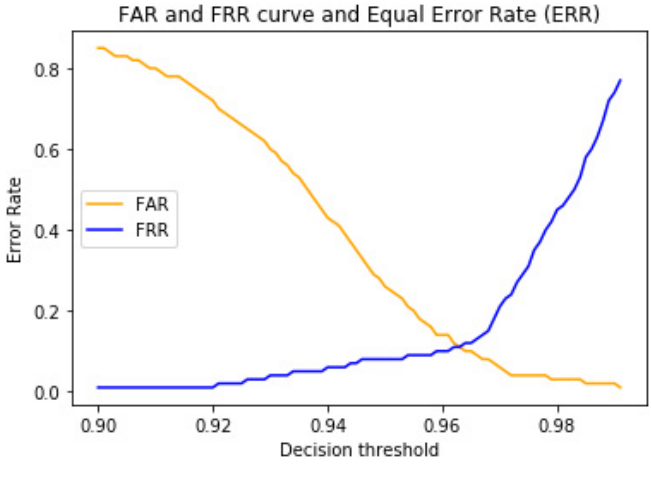

Fig. 6. This graph depicts the performance of the system under multiple simulations. The FAR and FRR curve meet at the error rate value of 0.11 and the EER is calculated as 0.89.

feature extraction with particular stress on the full side face and other facial feature analysis.[18]

3.2.2. *Distinctive geometric properties of the side face*

Findings from our experiments show that geometric values acquired from the feature vectors for each feature such as ear, nose, and forehead and also other feature to feature combinations are unique. These geometric values have been perceived to be consistent and within a distinctive range for each feature to feature combinations across various images of the same subject's face profile. Accordingly, this implies that the face profile features of humans can be geometrically exploited to produce a set of distance and angular ratios that are specific to a person.

Feature vectors can then be created using these point functions to associate values for the face profile. Previous efforts that have applied the notion of geometric properties such as the golden ratio have proved that it is a useful approach for analyzing and classifying human features. As exhibited from the execution of the suggested approach (ERR rate of 0.89), it can be inferred that the technique adopted is a useful augmentation in the field of facial recognition research.

4. Advantages and Drawbacks

4.1. *Advantages and drawbacks of the thr approach used in Experiment* 1

The developed software tool for the experiment can accept multiple input formats. It is able to process images and video streams. This approach is built on top of an existing face recognition solution in the python library. It is worth mentioning that the calculations completed of the distances between features are useful in understanding how simple ratios between features can play a role in similarity comparisons between faces. It is also important to note that the calculations completed offer very high explainability to the user as why two faces are similar. The low accuracy provided by this approach is contrasted with the high explainability. It is very important to develop the research further to increase the accuracy while maintaining the high explainability because this is the main goal of the research.

4.2. *Advantages and drawbacks of the thr approach used in Experiment* 2

Being able to identify someone based on face-profile is a very important research. It is huge step into providing flexibility into face recognition. Identifying relevant features based on geometrical vectors is both scientific and explainable. Moreover, automating the segmentation is a big development in the approach used in Experiment 2. Accuracy again is decreased when explainability is a priority. But it is important to

enlarge the datasets and simulations to find ways to increase the accuracy so that this approach can be enhanced and achieve better results.

5. Conclusion and Future Work

We are in the process of expanding our experiments and obtaining benchmark results against different state-of-the-art methods using industry standards. One way we aim to do this is by expanding the datasets used and include other approaches in the benchmarking process. There are many advantages to the proposed approach including sustaining privacy using a unique identifier per person instead of storing pictures. This further helps in saving storage space. Additionally, faster computations are achieved due to comparing numbers. Lastly, this approach is done in an explainable matter using a glass-box approach rather than a black-box in which it is unclear how the identification results are obtained.

Investigation of the findings from the second approach recommended and its novel methodology offer reassuring outcomes. Considering the benchmark for performance in the field of facial profile identification, the system is able to achieve a high level of prediction passing 0.89 precision. The suggested new algorithm can be enhanced further in the following areas:

- The automation of the pixel segmentation using deep learning models such as Mask R-CNN and SSD.
- Exploring more combinations of inter-feature relationship.
- Implementing the algorithm in the context of frontal face features.
- Future versions should include simulations using larger datasets.

References

1. A. Bud, Facing the future: The impact of apple FaceID, *Biometric Technol. Today* **2018** (1) (2018) 5–7.
2. M. Iqbal, M. S. I. Sameem, N. Naqvi, S. Kanwal and Z. Ye, A deep learning approach for face recognition based on angularly discriminative features, *Pattern Recogn. Lett.* **128** (2019) 414–419.
3. G. Cheng, J. Han, P. Zhou and D. Xu, Learning rotation-invariant and fisher discriminative convolutional neural networks for object detection, *IEEE Trans. Image Process.* **28**(1) (2019) 265–278.
4. A. Kumar, A. Kaur and M. Kumar, Face detection techniques: A review, *Artif. Intell. Rev.* **52**(2) (2019) 927–948.
5. U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt and C. Busch, Face recognition systems under morphing attacks: A survey, *IEEE Access* **7** (2019) 23012–23026.
6. J. Liu, W. Liu, S. Ma, M. Wang, L. Li and G. Chen, Image-set based face recognition using K-SVD dictionary learning, *Int. J. Mach. Learn. Cybern.* **10**(5) (2019) 1051–1064.
7. A. Geitgey, Machine learning is fun! part 4: Modern face recognition with deep learning, Medium Corporation (2016) (accessed on 6 October 2019).
8. D. E. King, Dlib-ml: A machine learning toolkit, *J. Mach. Learn. Res.* **10** (2009) 1755–1758.

9. G. B. Huang, M. Ramesh, T. Berg and E. Learned-Miller, Labeled faces in the wild: A database for studying face recognition in unconstrained environments, Technical Report 07-49, University of Massachusetts, Amherst (2007).
10. T.-T. Wong, Performance evaluation of classification algorithms by k-fold and leave-one-out cross validation, *Pattern Recogn.* **48**(9) (2015) 2839–2846.
11. Soumyadip Sengupta, Jun-Cheng Chen, Carlos Castillo, Vishal M Patel, Rama Chellappa, and David W Jacobs. Frontal to profile face verification in the wild, *2016 IEEE Winter Conf. Applications of Computer Vision (WACV)* (IEEE, 2016), pp. 1–9.
12. T. F. Vieira, A. Bottino, A. Laurentini and M. De Simone, Detecting siblings in image pairs, *Vis. Comput.* **30**(12) (2014) 1333–1345.
13. K. He, G. Gkioxari, P. Dollár and R. Girshick, Mask r-cnn, in *Proc. IEEE Int. Conf. Computer Vision* (2017), pp. 2961–2969.
14. A. Dutta and A. Zisserman, The vgg image annotator (via) (2019), *arXiv:1904.10699*.
15. S. Suzuki *et al.*, Topological structural analysis of digitized binary images by border following, *Comput. Vis., Graphics, Image Process.* **30**(1) (1985) 32–46.
16. D. Zhang, Q. Zhao and F. Chen, Quantitative analysis of human facial beauty using geometric features, *Pattern Recogn.* **44**(4) (2011) 940–950.
17. X. Jia and M. S. Nixon, Extending the feature vector for automatic face recognition, *IEEE Trans. Pattern Anal. Mach. Intell.* **17**(12) (1995) 1167–1176.
18. D. Shailaja and P. Gupta, A simple geometric approach for ear recognition, *9th Int. Conf. Information Technology (ICIT'06)* (IEEE, 2006), pp. 164–167.