DISSERTATION

ON

Unconstrained Face Identification using Rank Level Fusion

A Thesis submitted in Rank Level fusion
for the Degree of

Bachelor of Technology In

Computer Science and Technology

stream of

Information Technology

Sayan Pandey
15/ IT/21

Under the Supervision of

Dr. Dakshina Ranjan Kisku

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
National Institute of Technology Durgapur
M.G. Avenue, A-Zone, Durgapur – 713209
West Bengal, India

April 2019

Department of Computer Science and Engineering
National Institute of Technology Durgapur, Durgapur – 713209

Certificate of Recommendation

This is to certify that **Sayan Pandey** has completed the dissertation entitled **"Unconstrained Face Identification using Rank Level Fusion"** under the supervision and guidance of **Dr. Dakshina Ranjan Kisku**, National Institute of Technology, Durgapur. We are satisfied with his work, which is being presented for partial fulfillment of the degree of **Bachelor of Technology in Computer Science and Engineering**, National Institute of Technology Durgapur.

Dr Dakshina Ranjan Kisku
Asst. Professor, Dept. of CSE
National Institute of Technology
Durgapur – 713209, INDIA

Dr. Tandra Pal
Professor, Dept. of CSE
National Institute of Technology
Durgapur – 713209, INDIA

Department of Computer Science and Engineering
National Institute of Technology Durgapur, Durgapur – 713209

Certificate of Approval

The foregoing thesis is hereby approved as a creditable study of B.Tech in Computer Science and Engineering an presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or any statement made, opinion expressed or conclusion therein but approve this thesis only for purpose for which it is submitted.

BOARD OF THESIS EXAMINERS

1.______________________________ 2. ______________________________

3.______________________________ 4. ______________________________

5.______________________________ 6. ______________________________

Declaration of Originality and Compliance of Academic Ethics

We hereby declare that this thesis contains literature survey and original research work by the undersigned candidate, as a part of his Bachelor of Technology in Computer Science and Engineering. All information in this document has been obtained and presented in accordance with academic rules and ethical conduct, we have fully cited and referenced all material and results that are not original to this work.

Name: Sayan Pandey
Exam Roll No: 15/IT/21
Thesis Title: Rank Level Fusion
Signature with Date:

ACKNOWLEDGEMENTS

We would like to thank our adviser Dr. Dakshina Ranjan Kisku. We have been extremely fortunate to benefit from his supervision. His work ethics and dedication to ensuring the success of the students is certainly exceptoional.

Unconstrained Face Identification using Rank Level Fusion

ABSTRACT

Biometrics is the technical term for body measurements and calculations. However, in modern day we have digital platform to propose the biometric calculations to a greater extent. Today we use biometrics to identify and classify human beings. **Finger prints, facial recognition, retina and iris identification** etc. have now become a part and parcel of everyone's life.

Biometric Match is the name given to the decision that a biometric sample and a reference template stored in a biometric database comes from the same human source, based on their high level of similarity. The device that performs this match is called **Biometric Matcher**. There is an innate ability of this matchers to provide dissimilarity scores based on comparisons made between samples; the lower the score the higher the match.

The technology is fascinating. But as a greater number of biometric matchers and a greater number of samples the more is the complexity to determine an individual's identity. Since matchers may not have a universal rules and units to generate and assign scores respectively, a person's identity based on scores from different matchers can be confusing to determine and we may end up mismatching someone's biometric match with other.

Rank Level Fusion here comes in handy. Every subject is given a unique rank based on the matching scores generated by a particular matcher. Lower the score lower the rank. Rank Level Fusion works on the ranks generated based on matching scores. With efficient Rank Level Fusion Algorithms, a **consolidated fused rank table** is generated which is finally used for identification.

CONTENTS

Chapter 1

Introduction

Our world is progressing technologically in a very efficient and fast pace. From identity cards to bank accounts to our personal smartphones everything is digitalized and everything it needs is our **identification**. But with more and more people it becomes more complex to handle biometric data. For security purposes

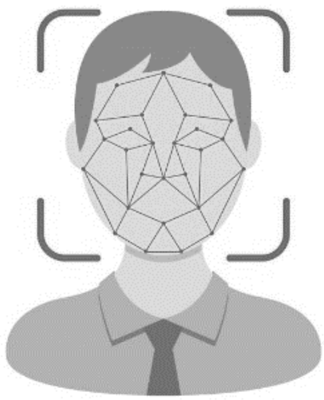
Identification, is a very important aspect in order to keep imposters away from acessing illicit properties and information. Hence mishandling and mis-classification of this crucial data can lead to disasters. Biometric aspects live **facial recognition, fingerprint recognition , retina and iris recognition** are today's building blocks of **Biometric Identification.**

It is indeed quite obvious that two people won't have same biometric data and their match results will be different. However in special cases like in *twins*, most likely they will have *same faces*. So biometrics based on just faces won't work. Here is a catch; We make use of *multiple biomtric matchers* to clearly identify a person's identity. That being said multiple matchers will produce multiple *dissimilarity scores* and hence tackling them will be time consuming and may be error prone.

This paper deals with proper study, use and deployment of the algorithms that are crucial in handling this vast data from different biometric matchers. The work is to make a consolidated table of *identifiacation ranks*. This table will subsequently help us recognise and identify each and every indiviadual with a good amount of surity. The widely used technique is ***Rank Level Fusion.*** With this technique each and every individuals are ranked based on the dissimilarity scores and finally with efficient fusion algorithms like *Highest Rank Method, Borda Count Method, Weigthed Borda Count Method and Bayes Fuse Method* we develop a consolidated rank table ready and capable of uniquely identifying subjects with ease and efficiency.

This research paper is based on *facial recognition* explaied in detail in the next section.

1.1 Introduction to Face Identification



A **facial recognition** system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. It is also described as a *Biometric Artificial Intelligence* based application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape.

While initially a form of computer application, it has seen wider uses in recent times on mobile platforms and in other forms of technology, such as robotics. It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Although *the accuracy of facial recognition system as a biometric technology is lower than iris recognition and fingerprint recognition*, it is widely adopted due to its contactless and non-invasive process. Recently, it has also become popular as a commercial identification and marketing tool. Other applications include advanced human-computer interaction, video surveillance, automatic indexing of images, and video database, among others.

1.2 Approaches for Face Identification

There are many approaches for face identification and recognition which are widely used and are in the field of biometrics for a long time. Let us illustrative some of these approaches one by one.

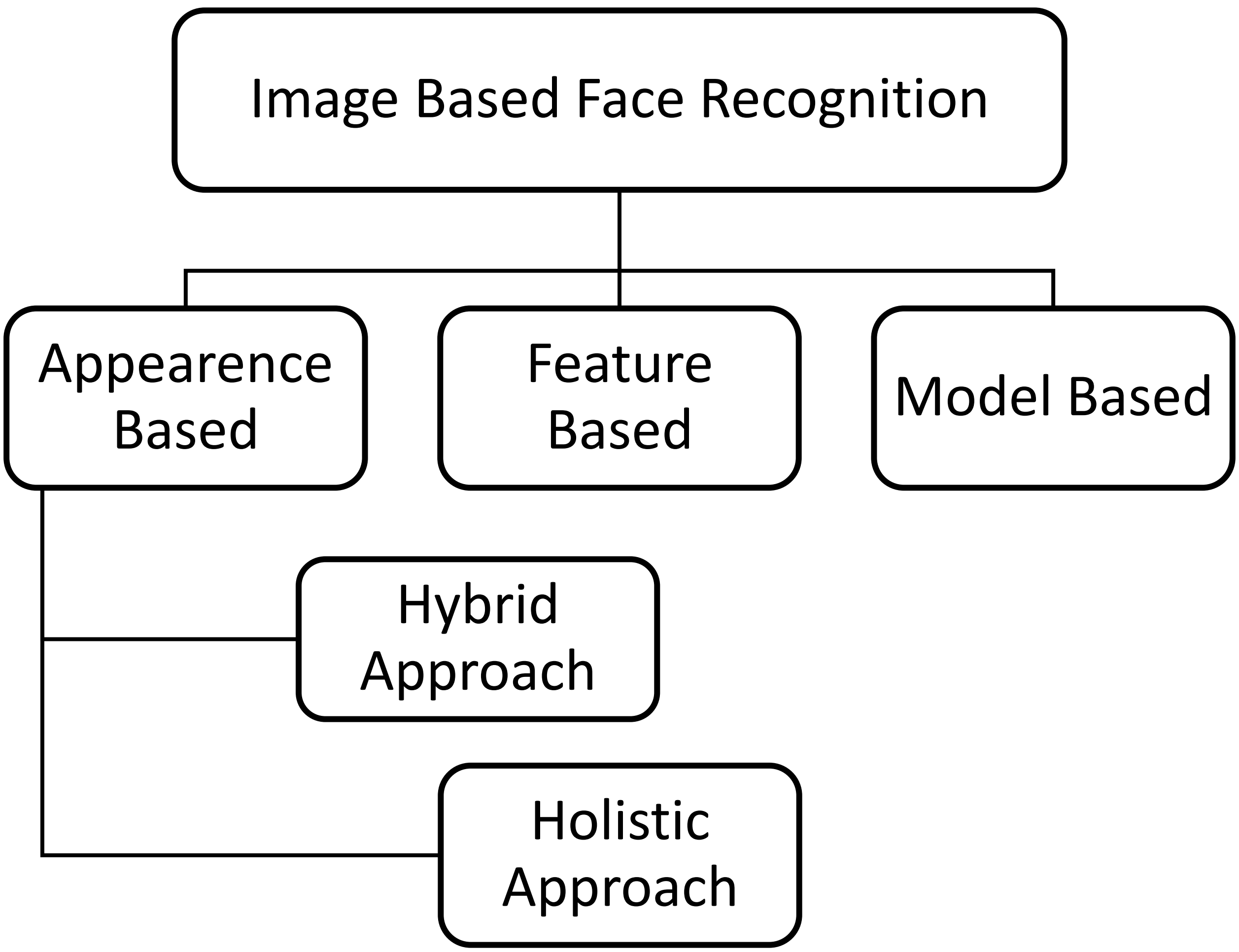


Fig 1: Approaches for Face Recognition/Identification

1.2.1 Appearance based

Appearance based face recognition techniques have received significant attention from a wide range of research areas such as biometrics, pattern recognition, computer vision and machine mining. Although humans can recognize faces easily, building automated face recognition systems remains a great challenge in computer-based automated recognition research. To have a clear and high-level categorization, instead follow a guideline suggested by the psychological study of how humans use holistic and local features. Specifically, they have the following categorization: **Holistic approaches and Hybrid approaches.**

- **Holistic Methods**: In this approach, the complete face is considered as a single feature for detection and recognition. It compares the similarities of whole face, ignoring individual features like eyes, mouth, nose etc. These schemes are characterized into two parts as shown in Figure 2:

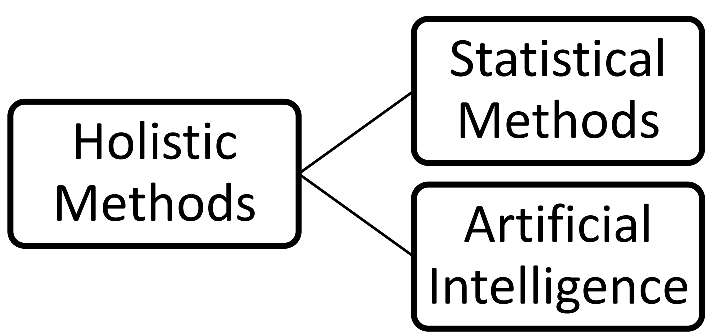


Fig 2: Holistic Face Recognition Methods

Statistical Approach:

The face image density is calculated and the density set values are compared with the density values of database images. This calculation is very expensive and directly suffering under the usual gap’s pathways, such as face orientation scaling and illuminations. To cope with this problem, dimensions, it has been suggested that many other diagrams, use ways to reduce the size and statistical stay ahead of the most obvious dimensions before recognition performance. Some of them are as follows:

A. Sirovich and Kirby were first getting the benefit of PCA for economically represent face images. They represent facial images. They showed that in any particular, can effectively represent time eigen pictures coordinate space, and that each region can modernize with only a small photos own collection and appropriate expectations ("Transactions") along each Eigen pictures.
B. Pentland et. al. expanded the Turk and Pentland capabilities of the system in several ways and proposed “Multiple Observer” technique to deal with pose variations.
C. Sharif M. et. al. Proposed another technique for illumination normalization, results shows that proposed technique produced better recognition accuracy.
D. Hashing technique is used in for fast face recognition.

Artificial Intelligence Approach:

Artificial Intelligence approach with tools such as neural networks and automatically recognizes the faces of learning techniques.

A. Samaria and Harter applied one-dimensional HMM and get 87% accuracy rate on ORL database.
B. Sharif et al produced a survey on HMM, Eigen face, geometric based and template matching approach.
C. Nefian and Hayes III also used the same database and recorded 98% recognition and compared the results with embedded HMM and also claimed that their mechanism was much intelligent than that of Samaria.

Fig 3: Artificial Intelligence based face recognition (2nd image)

- **Hybrid Approach:** Hybrid approaches are considered as the best approaches. Face recognition by means of using the nose tip for the main attribute of feature extraction phase. Then a hybrid 3D model is used for the recognition purpose. A research work is done on the face recognition with the help of the Gabor filter approach and the normalization approach. With the *combination of holistic and feature based, a hybrid method* was proposed in using Markov Random Field, in which facial images were sub divided into patches. The IDs were allocated and compared using BP algorithm. A research work done, introduced a much faster method of face recognition using basis coordinates of nose tip, its slope and fusion of different dependent regional classifier with the 3D face classifier. Results show 99% identification and 94.6% verification rate. Proposed LSP descriptor to overcome the problems of illumination and pose variations. Further SRC was applied to extract 3D depth information. Color image used and concept of tensor discriminant color space (TDCS) was introduced in 2D fast Face recognition approach based on wavelet network was proposed by. The technique is the combination of training algorithm of face image and comparing it from training set. Moreover, to increase performance, Levenberg Marquardt method was implemented. Another novel face recognition method Sp-Tensor was proposed using sub-pattern technique. The performance of the Sp-Tensor has better recorded than the Tensor Face. For 3D face recognition, proposed an Insensitive to noise and resolution invariant-based method.

1.2.2 Feature based

Opposite to holistic, feature based approach consider individual feature of the face like eyes, nose, mouth, mole, ears and match the similarity between the images. Another approach in the domain of face recognition includes face recognition by means of hexagonal features detection. The approach works on the bases of edge detection for the sake of face detection and recognition using the hexagonal facial features. Face recognition by means of using the heuristic parameters and storing them in the database before searching can be analyzed in. This approach mainly focused on nose portion of the acquired images followed by gray scale conversion and transformation of intensity. Another research work in which the face recognition is done by the help of edge information refined by the help of reduced sample size. Low dimension space for face images is done by DCT. The color feature in terms of HSV color space of the images of the facial portion is considered. The skin region is detected using the hue and saturation attributes. The SVD (single value decomposition) method is used in the face recognition in which the DWT (discrete wavelet transforms) and DCT (discrete cosine transforms). Skin feature of the face is used, this research methodology uses the techniques like block approach and the RGB color space. Fiscal features like eyes, nose and mouth were taken as point and Gabor filter applied for feature extraction. Another method introduced mid frequency values method for feature extraction, covariance matrix was computed on the basis of DCT & PCA. SIFT is another feature extraction tool.

Scale-invariant feature transform (aka. SIFT)

The **scale-invariant feature transform** (**SIFT**) is a feature detection algorithm in computer vision to detect and describe local features in images. It was patented in Canada by the University of British Columbia. and published by David Lowe in 1999. Applications include object recognition, robotic mapping and navigation, image stitching, 3D modeling, gesture recognition, video tracking, individual identification of wildlife and match moving.

SIFT key points of objects are first extracted from a set of reference images and stored in a database. An object is recognized in a new image by individually comparing each feature from the new image to this database and finding candidate matching features based on ***Euclidean distance*** **of their feature vectors**. From the full set of matches, subsets of key points that agree on the object and its location, scale, and orientation in the new image are identified to filter out good matches. The determination of consistent clusters is performed rapidly by using an efficient hash table implementation of the generalized Hough transform. Each cluster of 3 or more features that agree on an object and its pose is then subject to further detailed model verification and subsequently outliers are discarded. Finally, the probability that a particular set of features indicates the presence of an object is computed, given the accuracy of fit and number of probable false matches. Object matches that pass all these tests can be identified as correct with high confidence.

Features: The detection and description of local image features can help in object recognition. The SIFT features are local and based on the appearance of the object at particular interest points, and are invariant to image scale and rotation. They are also robust to changes in illumination, noise, and minor changes in viewpoint. In addition to these properties, they are highly distinctive, relatively easy to extract and allow for correct object identification with low probability of mismatch. They are relatively easy to match against a (large) database of local features but, however, the high dimensionality can be an issue, and generally probabilistic algorithms such as k-d trees with best bin first search are used. Object description by set of SIFT features is also robust to partial occlusion; as few as 3 SIFT features from an object are enough to compute its location and pose. Recognition can be performed in close-to-real time, at least for small databases and on modern computer hardware.

Fig 4: Features by SIFT

Main stages

Scale-invariant feature detection

Lowe's method for image feature generation transforms an image into a large collection of feature vectors, each of which is invariant to image translation, scaling, and rotation, partially invariant to illumination changes and robust to local geometric distortion. These features share similar properties with neurons in primary visual cortex that are encoding basic forms, color and movement for object detection in primate vision. Key locations are defined as maxima and minima of the result of difference of Gaussians function applied in scale space to a series of smoothed and resampled images. Low-contrast candidate points and edge response points along an edge are discarded. Dominant orientations are assigned to localized key points. These steps ensure that the key points are more stable for matching and recognition. SIFT descriptors robust to local affine distortion are then obtained by considering pixels around a radius of the key location, blurring and resampling of local image orientation planes.

Feature matching and indexing

Indexing consists of storing SIFT keys and identifying matching keys from the new image. Lowe used a modification of the k-d tree algorithm called the **best-bin-first search** method that can identify the nearest neighbors with high probability using only a limited amount of computation. The BBF algorithm uses a modified search ordering for the k-d tree algorithm so that bins in feature space are searched in the order of their closest distance from the query location. This search order requires the use of a heap-based priority queue for efficient determination of the

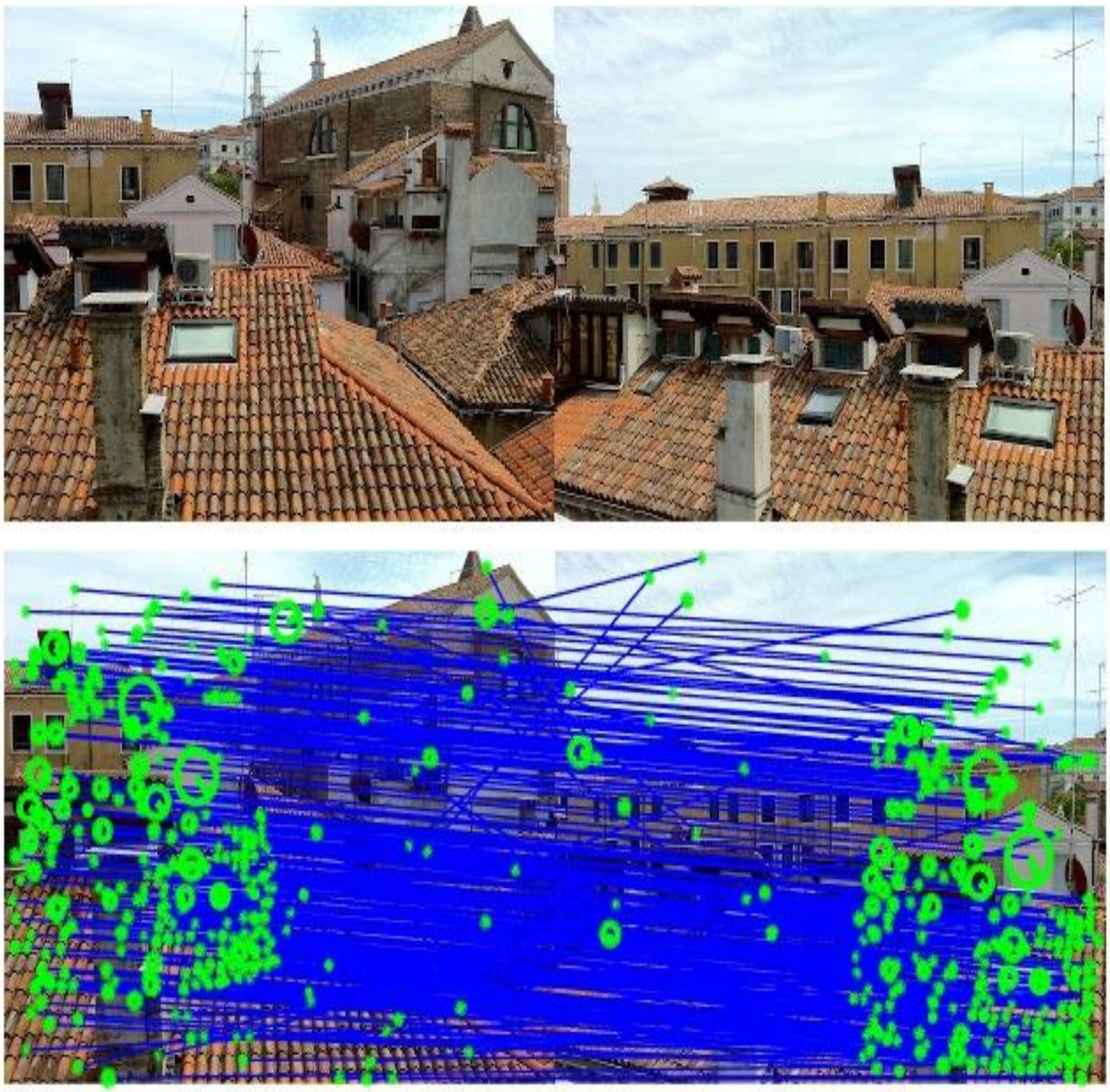


Fig 5: Features matching by SIFT

search order. The best candidate match for each key point is found by identifying its nearest neighbor in the database of key points from training images. The nearest neighbors are defined as the key points with minimum **Euclidean distance** from the given descriptor vector. The probability that a match is correct can be determined by taking the ratio of distance from the closest neighbor to the distance of the second closest. Lowe rejected all matches in which the distance ratio is greater than 0.8, which eliminates 90% of the false matches while discarding less than 5% of the correct matches. To further improve the efficiency of the best-bin-first algorithm search was cut off after checking the first 200 nearest neighbor candidates. For a database of 100,000 key points, this provides a speedup over exact nearest neighbor search by about 2 orders of magnitude, yet results in less than a 5% loss in the number of correct matches.

Cluster identification by Hough transform voting

Hough transform is used to cluster reliable model hypothesis to search for keys that agree upon a particular model pose. Hough transform identifies clusters of features with a consistent interpretation by using each feature to vote for all object poses that are consistent with the feature. When clusters of features are found to vote for the same pose of an object, the probability of the interpretation being correct is much higher than for any single feature. An entry in a hash table is created predicting the model location, orientation, and scale from the match hypothesis. The hash table is searched to identify all clusters of at least 3 entries in a bin, and the bins are sorted into decreasing order of size.

Each of the SIFT key points specifies 2D location, scale, and orientation, and each matched key point in the database has a record of its parameters relative to the training image in which it was found. The similarity transform implied by these 4 parameters is only an approximation to the full 6 degree-of-freedom pose space for a 3D object and also does not account for any non-rigid deformations. Therefore, Lowe used broad bin sizes of 30 degrees for orientation, a factor of 2 for scale, and 0.25 times the maximum projected training image dimension (using the predicted scale) for location. The SIFT key samples generated at the larger scale are given twice the weight of those at the smaller scale. This means that the larger scale is in effect able to filter the most likely neighbors for checking at the smaller scale. This also improves recognition performance by giving more weight to the least-noisy scale. To avoid the problem of boundary effects in bin assignment, each key point match votes for the 2 closest bins in each dimension, giving a total of 16 entries for each hypothesis and further broadening the pose range.

Model verification by linear least squares

Each identified cluster is then subject to a verification procedure in which a linear least squares solution is performed for the parameters of the affine transformation relating the model to the image. The affine transformation of a model point $[x\ y]^T$ to an image point $[u\ v]^T$ can be written as below

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} m1 & m2 \\ m3 & m4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} tx \\ ty \end{bmatrix}$$

where the model translation is $[tx\ ty]^T$ and the affine rotation, scale, and stretch are represented by the parameters m1, m2, m3 and m4. To solve for the transformation parameters the equation above can be rewritten to gather the unknowns into a column vector.

$$\begin{bmatrix} x & y & 0 & 0 & 1 & 0 \\ 0 & 0 & x & y & 0 & 1 \\ \dots & & & & & \\ \dots & & & & & \end{bmatrix} \begin{bmatrix} m1 \\ m2 \\ m3 \\ m4 \\ tx \\ ty \end{bmatrix} = \begin{bmatrix} u \\ v \\ . \\ . \end{bmatrix}$$

This equation shows a single match, but any number of further matches can be added, with each match contributing two more rows to the first and last matrix. At least 3 matches are needed to provide a solution. We can write this linear system as

$$A\hat{\mathbf{x}} \approx \mathbf{b},$$

where *A* is a known *m*-by-*n* matrix (usually with *m* > *n*), **x** is an unknown *n*-dimensional parameter vector, and **b** is a known *m*-dimensional measurement vector.

Therefore, the minimizing vector is a solution of the **normal equation**

$$A^T A\hat{\mathbf{x}} = A^T \mathbf{b}.$$

The solution of the system of linear equations is given in terms of the matrix ,
called the pseudoinverse of *A*, by

$$\hat{\mathbf{x}} = (A^T A)^{-1} A^T \mathbf{b}.$$

which minimizes the sum of the squares of the distances from the projected model locations to the corresponding image locations.

Outlier detection

Outliers can now be removed by checking for agreement between each image feature and the model, given the parameter solution. Given the linear least squares solution, each match is required to agree within half the error range that was used for the parameters in the Hough transform bins. As outliers are discarded, the linear least squares solution is re-solved with the remaining points, and the process iterated. If fewer than 3 points remain after discarding outliers, then the match is rejected. In addition, a top-down matching phase is used to add any further matches that agree with the projected model position, which may have been missed from the Hough transform bin due to the similarity transform approximation or other errors.

The final decision to accept or reject a model hypothesis is based on a detailed probabilistic model. This method first computes the expected number of false matches to the model pose, given the projected size of the model, the number of features within the region, and the accuracy of the fit. A *Bayesian probability* analysis then gives the probability that the object is present based on the actual number of matching features found. A model is accepted if the final probability for a correct interpretation is greater than 0.98. Lowe's SIFT based object recognition gives excellent results except under wide illumination variations and under non-rigid transformations.

1.2.3 Model based

Model based facial recognition is another approach. 3D facial model can be acquired using both active and passive means. Extensively used active 3D image acquisition technique is infrared input which project laser beam onto an object and records its reflection resulting best and accurate 3D models recognition. Stereo Imaging is the passive technique for the acquisition of 3D model in which two or more cameras simultaneously capture a scene from different angles. Depth information is acquired using disparity information from different angles. In 3D to 2D face recognition method was presented, using SRC and CCA for face recognition, results show a better performance with low computational cost. A new model

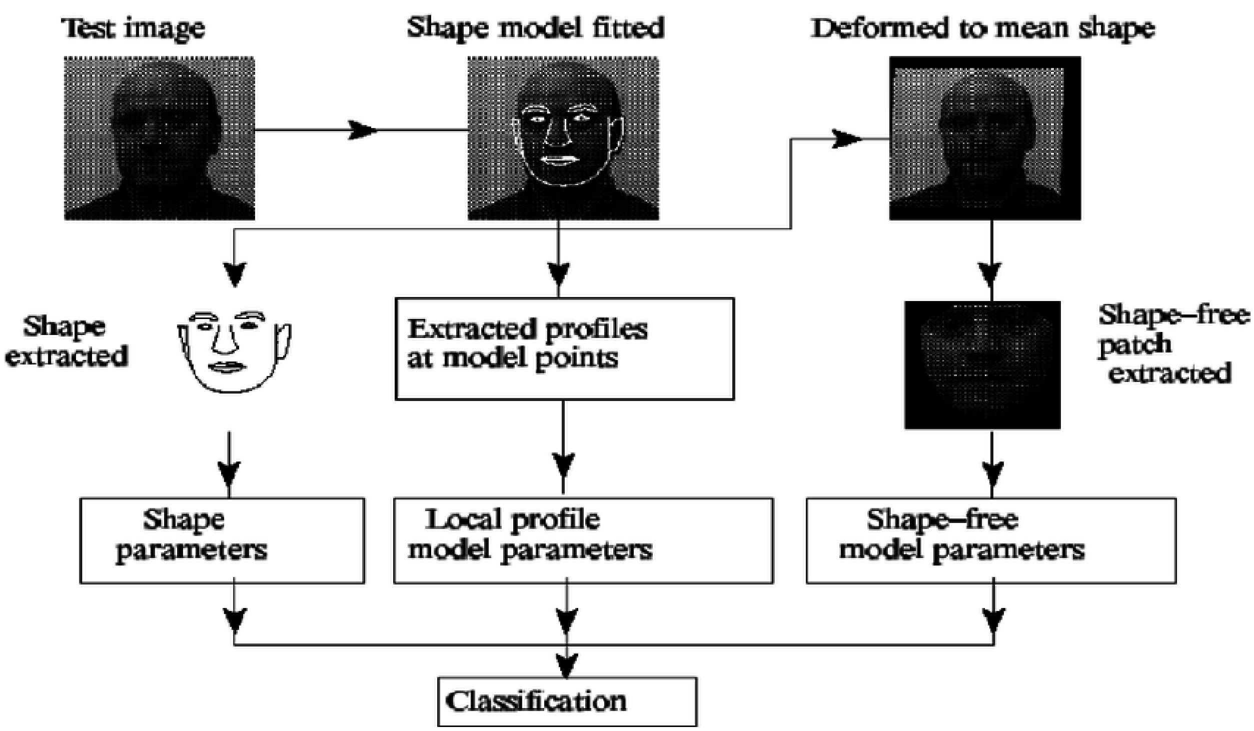


Fig 5: Flexible Appearance Model Based Face Recognition Scheme

“Associate-Predict” (AP) was introduced by to eliminate pose, illumination and expression variations. AP method effectively handled the personal variations. presented a discriminative model to overcome age variation problem in face recognition, using *scale invariant feature transform (SIFT) and multi-scale local binary patterns for local descriptors and introduced multi-features discriminant analysis (MFDA)* algorithm to analyze the local descriptors, resulting face recognition improvement in aging factor.

1.3 Challenges of Face Identification

Over the last decade, academic computer vision researchers and commercial product developers have improved the performance of automated face recognition algorithms on a variety of challenging face recognition tasks. Because humans currently perform face recognition tasks in most real-world security situations, it is unclear whether the use of algorithms improves security or puts it at greater risk. The real challenge in face detection and recognition technologies is the ability to handle all those scenarios where subjects are non-cooperative and the acquisition phase is unconstrained. There are numerous factors that cause the appearance of the face to vary. These sources of variation in the facial appearance can be categorized into two groups: **Intrinsic factors and Extrinsic ones**.

A) **Intrinsic factors: -** are due purely to the physical nature of the face and are independent of the observer. These factors can be further divided into two classes: **intrapersonal and interpersonal**. Intrapersonal factors are responsible for varying the facial appearance of the same person, some examples being age, facial expression and facial paraphernalia (facial hair, glasses, cosmetics, etc.). **Interpersonal factors**, however, are responsible for the differences in the facial appearance of different people, some examples being ethnicity and gender.

B**) Extrinsic factors: -** cause the appearance of the face to alter via the interaction of light with the face and the observer. These factors include illumination, pose, scale and imaging parameters (e.g., resolution, focus, imaging, noise, etc.).

Following are the common problems and challenges that a face recognition system can have while detecting and recognizing faces:

1.3.1 Automatically locate the Face

Locating or detecting a face in an image or video is the first step in a face recognition system. It is not always possible that in an image sequence the position of the head is stationary. For example, in a Video Surveillance System at a crowded place, it is a difficult task to detect a face as there is always some motion. Second, the background is very complex that makes detection more challenging.

Fig 6: Locating Face in a crowded place

1.3.2 Illumination

Illumination means light variations. Illumination changes can vary the overall magnitude of light intensity reflected back from an object, as well as the pattern of shading and shadows visible in an image. Indeed, varying the illumination can result in larger image differences than varying either the identity or the viewpoint of a face. The same individual imaged with the same camera and seen with nearly the same facial expression and pose may appear dramatically different with changes in the lighting conditions. The problem of face recognition over changes in illumination is widely recognized to be difficult for humans and for algorithms. The difficulties posed by variable illumination conditions, therefore, remain a significant challenge for automatic face recognition systems. It is found that the difference between two images of the same person taken under varying illumination is greater than the difference between the images of two different persons under same illumination. The variation in illumination changes the appearance of the face drastically as shown in figure.

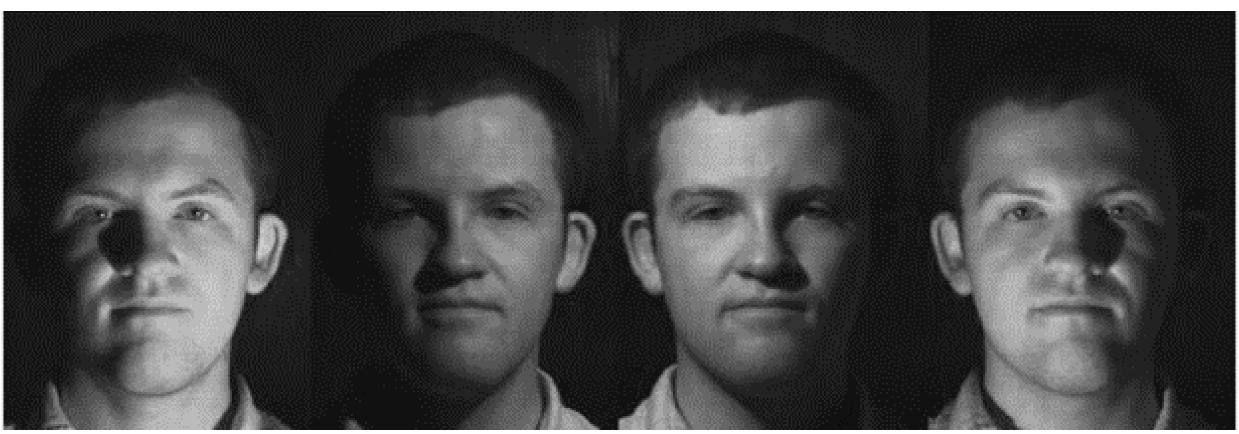


Fig 7: Variation in Illumination

1.3.3 Pose

Pose variations in an image is also a matter of concern in face recognition. The pose of a face changes with viewing angle of the observer &rotation in the head position. These changes in the posture strike a serious problem for the identification of the input image. A Face Recognition System can tolerate cases with small rotation angles, but it becomes a challenge when rotation angle goes higher and the available image in the database may have only the frontal view of the face which may differ in pose with the input image and that misleads the system result in faulty identification or no recognition.

Fig 8: Variation in Pose

1.3.4 Expressions

Face is one of the most important human's biometrics which due to its unique characteristics plays a major role in conveying human identity and emotion. Because of these emotions human mood varies and results in different facial expressions. With this make-up and hair style also changes the facial expressions. These differences in facial expressions change the appearance of the face and it becomes difficult for a Face Recognition System to match the accurate face stored in the database as shown in figure.

Fig 9: Variation in Expressions

1.3.5 Ageing

The human face is not a unique, rigid object. Everything changes with time, so with the increasing age the appearance of a person also changes which affect the face recognition system as shown in figure.

Fig 10: Variation with age

1.3.6 Occlusion

Occlusion means blockage. When in a Face Recognition System, the whole face is not available as input Occlusion means blockage. When in a Face Recognition System, the whole face is not available as input image or image sequence, then it is termed as Occlusion. It is one of the important challenges of the face recognition as shown in the figure. This is due to presence of various occluding objects such as glasses, beard, moustache etc. on the face and when an image is captured from a surveillance camera; the face lacks some parts. In real world applications also, it is very common situation to acquire persons talking on the phone or wearing glasses, scarves, hats, etc. or for some reasons having their face covered with hands. Such a problem can severely affect the classification process of the recognition system.

Fig 11: Variation in occlusion

1.3.7 Low Resolution

Low resolution problem occurs in a face recognition system when resolution of the face image to be recognized is lower than 16x16. This problem happens in many surveillance applications, such as small-scale standalone camera applications in supermarkets and banks, CCTV in public streets, etc. where images taken from a surveillance camera generally consists of very small face area and cannot provide enough resolution of face for recognition. As the person face is not close to the camera, the face region will be smaller than 16x16. Such a low-resolution face image consists of very limited information as most of the details are lost. This can drop down the recognition rate drastically.

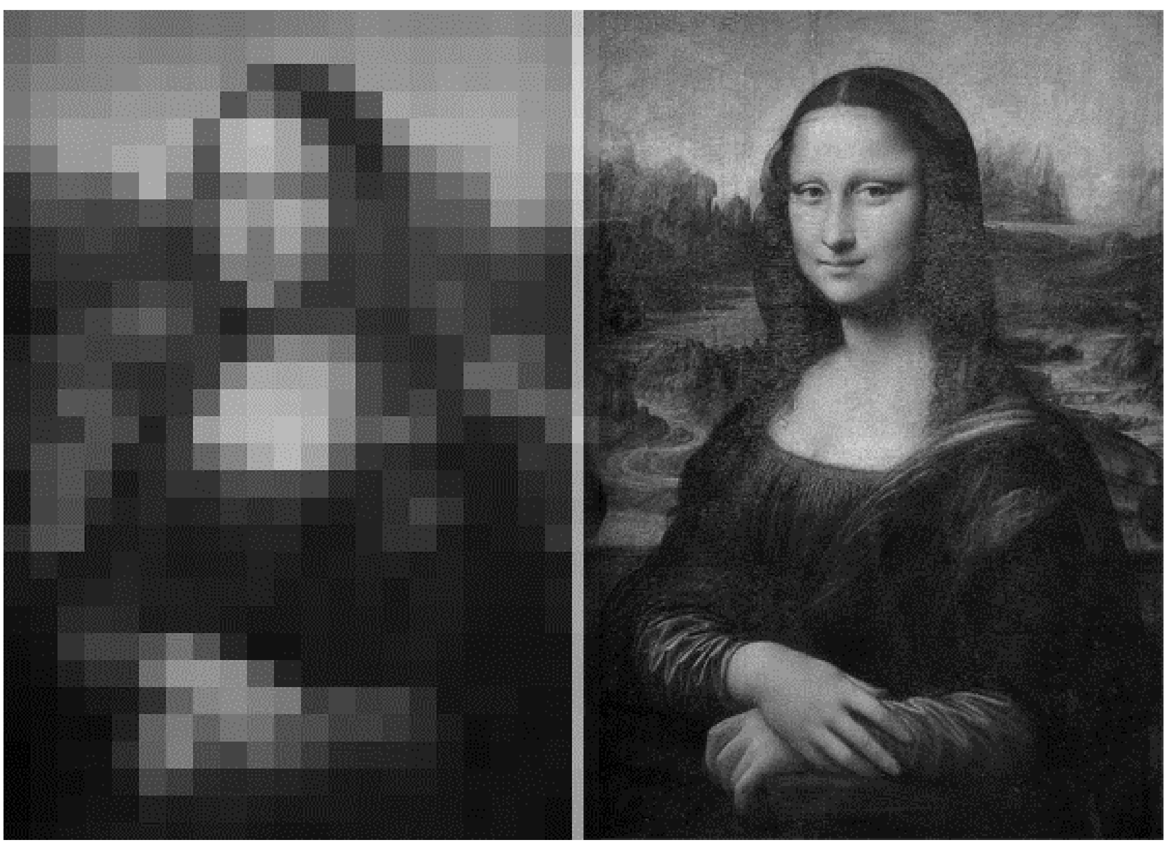


Fig 12: Variation in resolution, low vs high resolution

1.3.8 Similar Faces

Different persons may have similar appearance that sometimes it is impossible for a human to identify them. So, it is very difficult for a recognition system to identify them.

Fig 13: Similar face detection

1.4 Advantages of Face Identification

There are innumerable advantages of face recognition. From security to health care to finances; every where it can be used with accuracy. Some of the advantages are listed below.

1 The Improvement of Security Level

A face biometric system greatly improves your security measures. All corporation's premises would be protected since you'll be able to track both the employees and any visitors that come into the area. Anyone who doesn't have access or permission to be there will be captured by the recognition system that alerts you instantly about the trespassing.

2 Easy Integration Process

Most of the time, integration of facial recognition tools work pretty flawlessly with the existing security software that companies have installed. And they're also easy to program for interaction with a company's computer system.

It doesn't require to spend additional money and time on redeveloping your own software to make it suitable for FRT integration. Everything will be already adaptable.

3 High Accuracy Rates

These days, the success level of face tracking technology became higher than ever before. Thanks to the assistance of 3D facial recognition technologies and infrared cameras the process of identification happens to be incredibly accurate and showing great results. It’s possible but difficult to fool such system, so you can be sure that an FR digital security software will successfully track every aspect of attendances to provide a better level of protection for your facilities.

Accuracy ensures that there won’t be any misunderstandings and uncool awkwardness that comes from bad face recognition software. With high levels of accuracy, you’d sure that the right person will be recognized at the right time.

4 Full Automation

Instead of manual recognition, which is done by security guards or the official representatives outside of company’s premises, the facial recognition tech automates the identification process and ensures its flawlessness every time without any halting. You won’t even need an employee to monitor the cameras 24/7.

Automation means convenience and reduces the expenses too. Therefore, any entrepreneur would be fond of the fact that image identification systems are fully automated.

5 Forget the Time Fraud

One of the big benefits that facial recognition technology companies offer is the time attendance tracking that allows excluding the time fraud among the workers. No more buddy favors from securities for staff members, since everyone now has to pass a face scanning device to check-in for work. And the paid hours begin from this moment till the same check-out procedure. And the process will be fast due to the fact that employees don’t have to prove their identities or clock in with their plastic cards.

It’s crucial for businessmen to trust their workers but keep an eye on them just in case. Unfortunately, time fraud is one of the most common violations of the work ethics, but the facial identification tech will spare you a headache regarding this matter.

1.5 Applications of Face Identification

Facial recognition is being used in many businesses. Used in unlocking your door with a key, but maybe not with your face. As strange as it sounds, our physical appearances can now verify payments, grant access and improve existing security systems. Protecting physical and digital possessions is a universal concern which benefits everyone, unless you're a cybercriminal or a kleptomaniac of course. Facial biometrics are gradually being applied to more industries, disrupting design, manufacturing, construction, law enforcement and healthcare.

1. Payments

It doesn't take a genius to work out why businesses want payments to be easy. Online shopping and contactless cards are just two examples that demonstrate the seamlessness of postmodern purchases. However, customers wouldn't even need their cards. In 2016, MasterCard launched a new selfie pay app called MasterCard Identity Check. Customers open the app to confirm a payment using their camera, and that's that. Facial recognition is already used in store and at ATMs, but the next step is to do the same for online payments. Chinese ecommerce firm Alibaba and affiliate payment software Alipay are planning to apply the software to purchases made over the Internet.

2. Access and security

As well as verifying a payment, facial biometrics can be integrated with physical devices and objects. Instead of using passcodes, mobile phones and other consumer electronics will be accessed via owners' facial features. Apple, Samsung and Xiaomi Corp. have all installed face recognition in their phones. This is only a small-scale example, though. In future, it looks like consumers will be able to get into their cars, houses, and other secure physical locations simply by looking at them. Jaguar is already working on walking gait ID – a potential parallel to facial recognition technology. Other corporations are likely to take advantage of this, too. Innovative facial security could be especially useful for a company or organization that handles sensitive data and needs to keep tight controls on who enters their facilities.

3. Criminal identification

If Facial Recognition can be used to keep unauthorized people out of facilities, surely it can be used to help put them firmly inside them. This is exactly what the US Federal Bureau of Investigation is attempting to do by using a machine learning algorithm to identify suspects from their driver's licenses. The FBI currently have a database which includes half of the national population's faces. This is as useful as it is creepy, giving law enforcers another way of tracking criminal across the country. AI equipped cameras have also been trailed in the UK to identify those smuggling contraband into prisons.

4. Advertising

The ability to collect and collate masses of personal data has given marketers and advertisers the chance to get closer than ever to their target markets. Facial Recognition could do much the same, by allowing companies to recognize certain demographics – for instance, if the customer is a male between the ages of 12 and 21, the screen might show an ad for the latest FIFA game.

5. Healthcare

Instead of recognizing an individual, medical professionals could identify illnesses by looking at a patient's features. This would alleviate the ongoing strain on medical centers by slashing waiting lists and streamlining the appointment process. The question is, would you really want to find out you had a serious illness from a screen? If it's a choice between a virtual consultation or a month long wait for an appointment, then maybe so. Another application of facial biometrics within healthcare is to secure patient data by using a unique patient photo instead of passwords and usernames.

With a predicted worth of $15 billion by 2025, biometrics is an industry worth watching. It's clear that facial biometrics are a helpful tool for finance, law enforcement, advertising and healthcare, as well as a solution to hacking and identity theft. Of course, Facial Recognition is by no means foolproof. Gaining access to possessions using physical traits could even be counterintuitive for security. A face, as social robots like Nadine have shown us, is easily replicated. And when it comes to public adoption, some people are reluctant to switch to contactless cards, let alone abandon them completely. For the most part, though, facial recognition technology seems to be encouraging a more seamless relationship between people, payments and possessions.

Chapter 2

Rank Level Fusion

The majority of biometric system deployed use feature extraction from a single biometric modality and a particular classification procedure to determine the identity on an individual. The perfect solutions for user identification are often difficult to achieve, mainly due to the large number of user classes and the imperfection in the feature extraction process. Therefore, the improvement in the user identification results using the simultaneous extraction of features and classifiers of different types has been investigated. The combination of potentially conflicting decisions in multimodal or unimodal biometric system employing different classifiers can be achieved in several ways: at feature, score and decision level. In general, the improvement in identification accuracy is achieved by selecting combination mechanism that can take advantage of strengths of individual classifiers while suppressing their weakness. Any biometric recognition system is capable of generating matching scores for the input user with those of the enrolled possible identities. The set of all the possible user identities can be ranked by sorting the matching scores in the descending order.

Thus, a biometric system can identify an unknown user by generating ranks, i.e., integer numbers for each of the possible user identity. The rank level fusion refers to the mechanism of combining such output ranks from the various biometrics matchers (subsystems), to consolidate the combined output ranks in order to establish the identity of an individual with higher confidence. The matching score contains more information than ranks and therefore matching score level fusion schemes are believed to be more flexible. However, the rank level fusion schemes do not require transformation of ranks from various biometrics matchers into a common domain and are simpler to implement. Several decision level fusion schemes only use top choice (rank) from each of the biometric classifiers which is likely to be sufficient for biometric systems with small number of users. However, with the increase in number of enrolled identities or users, the correct rate for top choices drops, the secondary choices often contain near misses that should not be overlooked and are made use of in the rank level fusion.

2.1 Modes of Combining Ranks

The voting techniques proposed by different researchers for consolidating rank output from the different biometric matchers will now be introduced. Given the ranked list of user identities returned by M different biometric matchers, let **ri(k)** be the rank assigned to the user k by the **i^{th}** matcher. The user identity for kth user is assigned by computing the fused rank score **m_k** from all the M matchers

2.1.1 Highest Rank Method

In highest rank method, the user identity is ascertained from the highest ranks returned by the individual matchers. Each of the possible user identity receives M ranks, each from the M matchers. The fused rank score m_k for every possible user identity k is computed from the minimum (highest) of these M ranks. The user identities are then sorted in the order of fused rank scores to obtain the combined or new ranking from all M matchers. Any ties in the fused rank scores (m_k) are randomly broken to obtain linearly ordered combined ranking. These ties are due to a number of user identities sharing the same combined ranks and depend on the number of employed matchers. The chances of the occurrences of such ties will be smaller if the number of enrolled user identities are large and the number of matchers employed in the fusion are small. The advantage of this method lies in the utilization of strength of each of the biometric matchers. However, large number of matchers can result in more ties in the combined ranking which is the major problem with this method. Therefore, this method is considered useful in biometric systems combining small number of matchers with large number of enrolled users.

2.1.2 Borda Count Method

The Borda count is the generalization of majority vote and the most commonly used method for **unsupervised** rank level fusion. It is the voting method in which each matcher gives priority to all possible user identities. Each matcher ranks the fixed set of possible user identities in the order of its preference. For every matcher, the top ranked user identity is given N votes, the second ranked candidate identity is given N-1 votes and so on. Then for every possible user identity, the votes from all the matchers are added. The user identity that receives the highest number of votes is assigned as the winner or the true user identity.

$$m_k = \sum_{i=1}^{M} r_i(k) \qquad \forall\ k, k = \{1, 2, \dots N\}$$

The Borda count score m_k represents strength of agreement among different biometric matchers. The Borda count method assumes statistical independence, i.e., ranks assigned to a given user by different matchers are independent. This assumption is often made in practice but it may not be true. The Borda count method is particularly considered suitable for combining the biometrics matchers with large number of user identities that often generate the correct user identities near the top of list (ranks) but not at the top. This method is efficient, simple and does not require any training. However, it assumes that all matchers are equally correct. This may not be the case when some matchers are more likely to be correct than others. Therefore, weighted Borda count method has been suggested to utilize the strength of individual matchers.

2.1.3 Weighted Borda Count Method

The performance of different biometric matchers is not uniform, for example a biometric matcher using iris images is expected to perform better than those matchers using hand geometry or face images. Therefore, modification of Borda count method by assigning corresponding weights to the ranks produced by individual matchers has been suggested. The fused rank scores in weighted Borda count method are computed as follows

$$m_k = \sum_{i=1}^{M} w_i r_i(k)$$

where the wi represents the weights assigned to the **ith** matcher. The weight wi are assigned to reflect the significant of each matcher and can be computed from the overall assessment of the performance. The weights are computed during the training phase using logistic or using more sophisticated machine learning techniques.

2.1.4 Bayes Fuse

The Bayes fuse is the supervised rank level fusion method based on Bayesian inference. Each of the possible user identity is ranked according to the fused rank scores computed as follows:

$$m_k = \sum_{i=1}^{M} \log \frac{\Pr[m_k(i) \mid gennuine]}{\Pr[m_k(i) \mid imposter]}$$

where *$P_r[m_k(i)|$ imposter]* is the probability that an imposter user would be ranked to m_k (i) by the i^{th} matcher and *P_r [m_k (i)| genuine]* is the probability that a genuine user would be ranked to m_k (i) by the i^{th} matcher. These two likelihood probabilities are computed from the training data during training phase. The above equation is easily derived from the estimation of two posterior probabilities, each for the genuine and imposter class, using Bayes rule. The combined ranks generated using makes a common naïve Bayes assumption, i.e., individual ranks assigned to the user identities by M matchers are independent. The training phase in Bayes fuse method required the collection of simple statistics about the distribution of ranks among various user identities. The rank level fusion using Bayes fuse was originally introduced for information retrieval but is equally useful in biometrics fusion.

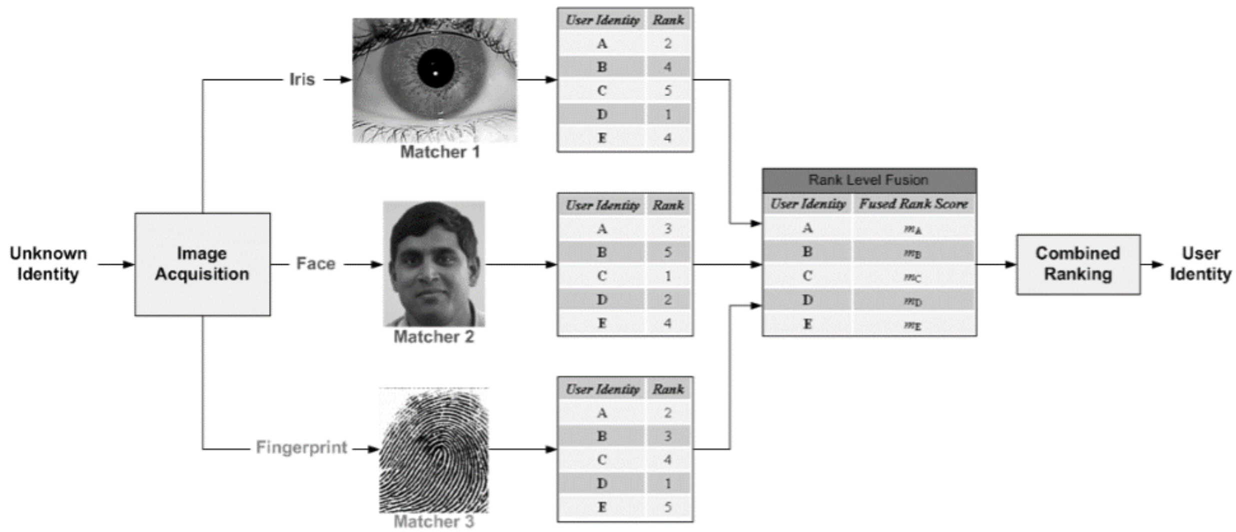


Fig 14: Rank Level Fusion

2.2 Applications of Rank Level Fusion

Rank Level Fusion is solely used as a better way of combining ranks and making an identification table. Rank Level Fusion is a technique which deals with formation of a consolidated rank table for Identification of a person. There are lot of benefits let us state some of them:

Handling Scores from different Domains

Since we know humans have different ways of generating biometric data, may be from *fingerprint, iris, palms or faces* however due to variation of brands and lack of *universal standards of score generation* and techniques to identify; Rank Level Fusion has now become a must. For example: A person has three biometric data scores from three different or similar biometric matchers. It is quite evident from this fact that biometric data from different matchers will prove to show different types of results depending on its own functioning and dataset. Fingerprint matchers will show a set of scores and ranking that in most cases will vary from iris or facial identification matchers. In this scenario we fail to identify a person by his or her biometrics which is not desirable. Rank level fusion unites these scores and makes identification table that can lead us to accurately Identifying a person. Through the efficient fusion algorithms, we can generate a final consolidated table leading to proper functioning of biometric match.

Ease of operation

It is worth mentioning that handling huge amount of data is not a good deal because it may cause error and flaws in operation. When the number of matchers and number of subjects becomes huge handling huge amount of data can be a source of misclassification and irreversible errors. For example, what if while handling data someone placed someone else biometric data to someone other. This will lead the other person biometric data to be used without his/her knowledge.

Shorter Computation Time

If too many candidates or subjects along with huge biometric data is present from different matchers then establishing identity of a person will take huge lot of time. Comparing and establishing identity from all data available data is truly very costly in computation time hence making a consolidated table will let us combine all the data from all ranks from different matchers and help us get a consolidated table. This consolidated table will now help us getting identification ranks and get identity of a person in shortest time possible.

Chapter 3

Literature Survey

This segment includes the existing and established theory in Rank Level Fusion on an *Unconstrained Face Identification using Rank Level Fusion.* Some related works on feature extraction and matching by SIFT.

3.1 Rank Level Fusion

As already explained in **Chapter 2** about detailed functioning of Rank level Fusion. It is the Process of consolidating various ranks from scores generated by different biometric matchers and creating the Identification table.

The research paper that paved the way for Rank Level Fusion on unconstrained face identification is made by

"Ajay Kumar Indian Institute of Technology Delhi Hauz Khas, New Delhi 110016, India.

This book chapter appears in Encyclopedia of Biometrics, pp.607-611

Stan Z. Li (Eds), Springer, August 2009"

3.2 Score Generation

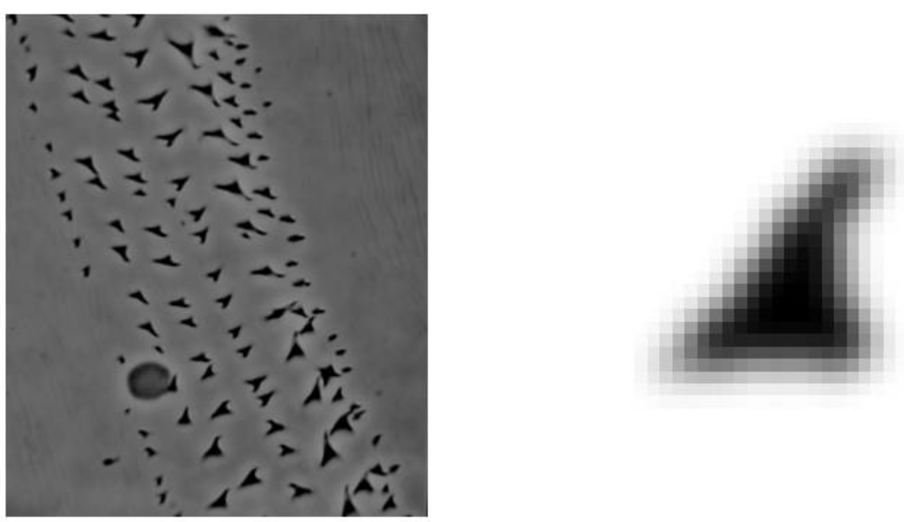
This section discovers the techniques used for score generation for the various image-based matcher. Predominantly the score generation is based on face data hence three used techniques are used

3.2.1 Feature Matching Score (by SIFT)

This part is discussed in **Section 1.2.2.** This uses features extracted from different images and by using Euclidian distance generates matching scores with logic less the score more the match.

3.2.2 Correlation Scores

Correlation is the technique to find similarity between two images. The image in figure 15(a) shows a detail of the ventral epidermis of a fruit fly embryo viewed through a microscope. Biologists are interested in studying the shapes and arrangement of the dark, sail-like shapes that are called denticles. A simple idea for writing an algorithm to find the denticles automatically is to create a template T, that is, an image of a typical denticle. Figure 15(b) shows a possible template, which was obtained by blurring (more on blurring later) a detail out of another denticle image. One can then place the template at all possible positions (r,c) of the input image I and somehow measure the similarity between the template T and a window W(r,c) out of I, of the same shape and size as T. Places where the similarity is high are declared to be denticles, or at least image regions worthy of further analysis.



(a) (b)

Fig 15: (a) Denticles on the ventral epidermis of a Drosophila embrio. Image courtesy of Daniel Kiehart, Duke University. (b) A denticle template.

3.2.3 Empirical mode decomposition

Image empirical mode decomposition (IEMD) is an empirical mode decomposition concept used in Hilbert–Huang transform (HHT) expanded into two dimensions for the use on images. IEMD provides a tool for image processing by its special ability to locally separate superposed spatial frequencies. The tendency is that the intrinsic mode functions (IMFs) other than the first are low-frequency images. In this study we give an overview of the state-of-the-art methods to decompose an image into a number of IMFs and a residue image with a minimum number of extrema points, together with the use of the method. Ideas and open problems are presented.

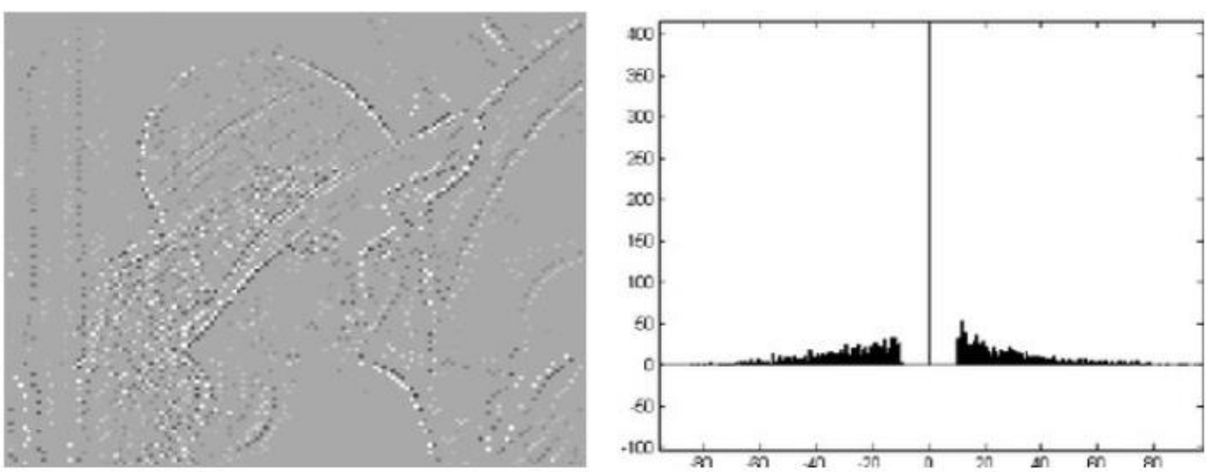


Fig 16: EMD equivalent of a image

3.3 Identification and CMC Curve

Identification is done based on the highest frequency of a particular rank that has occurred for a particular subject in majority of the fused rank tables. *That Rank's percentage of occurrence in the called to be the percentage accuracy of that rank and that rank is the subject's identity.*

3.3.1 CMC Curve

Each probe biometric sample is compared against all gallery samples. The resulting scores are sorted and ranked. Determine the rank at which a true match occurs. True Positive Identification Rate (TPIR): Probability of observing the correct identity within the top K ranks. CMC Curve: Plots TPIR against ranks. A typical CMC Curve: Rank-based metric is given below.

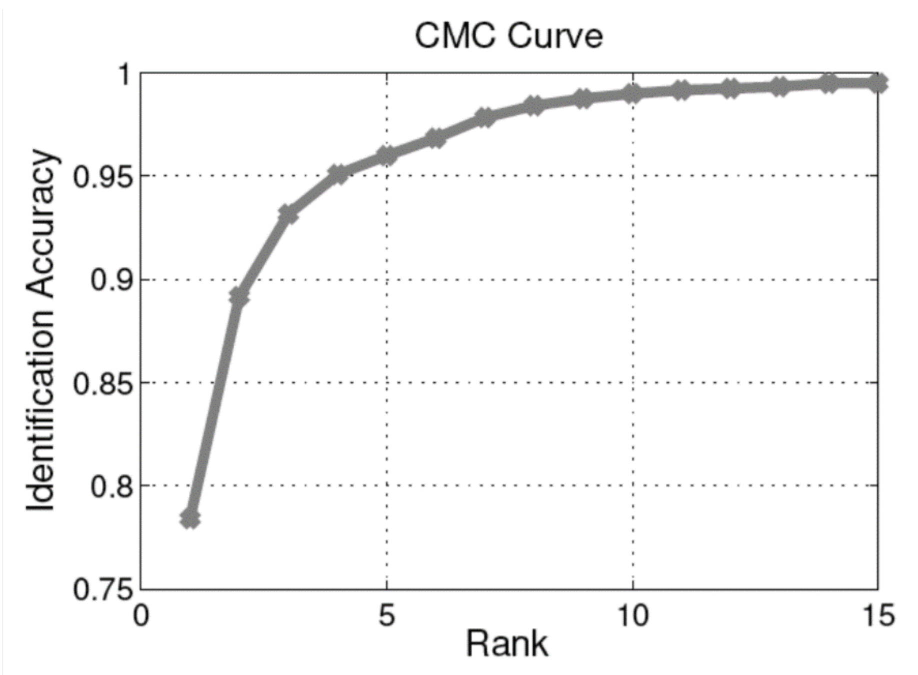


Fig 17: Typical CMC Curve

Chapter 4

Proposed Work

This segment includes proposed work, the algorithms, the dataset and all the techniques and technologies used included. This work was done on the *Unconstrained Face Identification using Rank Level Fusion.*

4.1 Overview

The Technique used is fairly simply but very efficient which is explained in later sections. We also take some of the starter algorithms that we have used to establish a suitable facial database for our functioning.

4.2 Dataset

LFWcrop is a cropped version of the Labeled Faces in the Wild (LFW) dataset, keeping only the center portion of each image (i.e. the face). In the vast majority of images almost all of the background is omitted.

LFWcrop was created due to concern about the misuse of the original LFW dataset, where face matching accuracy can be unrealistically boosted through the use of background parts of images (i.e. exploitation of possible correlations between faces and backgrounds).

For each LFW image, the area inside a fixed bounding box was extracted. The bounding box was at the same location for all images, with the upper-left and lower-right corners being (83,92) and (166,175), respectively. The extracted area was then scaled to a size of 64x64 pixels. The selection of the bounding box location was based on the positions of 40 randomly selected LFW faces.

As the location and size of faces in LFW was determined through the use of an automatic face locator (detector), the cropped faces in LFWcrop exhibit real-life conditions, including mis-alignment, scale variations, in-plane as well as out-of-plane rotations.

4.3 Sorting Images

Since LFWcrop database had variety of images that are somehow different in pose, lighting and most importantly in *frequency.* As there is variable frequency of a person's image it turned out to be an urgent necessity to sort the images according to the frequency and consider only those people who have more than one image in the database as shown below.

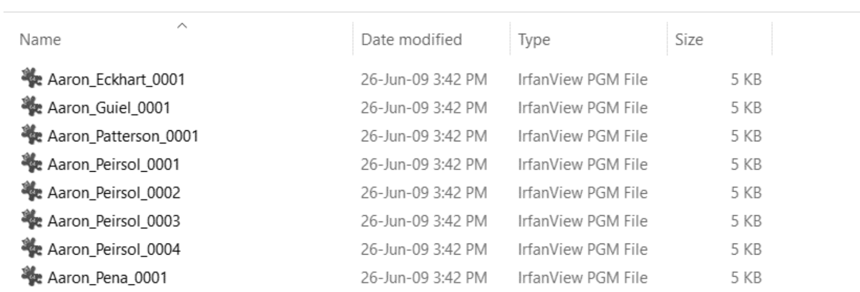


Fig 18: Before Sorting

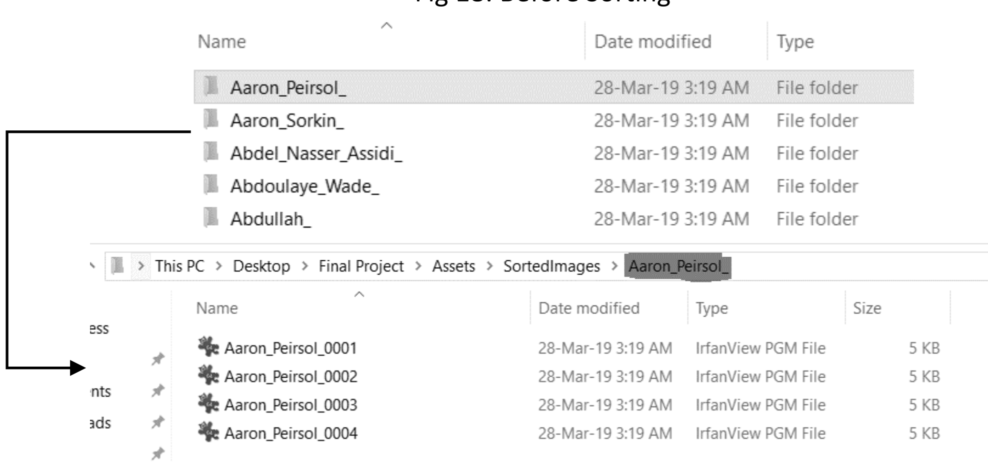


Fig 19: After Sorting

The algorithm used is fairly simply as it functioning is given by the following pseudocode.

```
while (counter < Size_of_Directory) {

       I = Read_Image_Name(counter++);

       /*
          if a person has image name as:
          Sayan_Pandey_0001.pgm

          Name = Sayan_Pandey_
          ImgId = 0001.pgm
        */

              Name = Crop_Name_front(I)
              ImgId = Crop_Name_back(I)

              /* Master List stores the end parts for a particular person
                 masterList = { 0001.pgm, 0002.pgm, .....}
              */
              masterList.insert(ImgId)

              /*
                sortedList is a map<string,vector<string>>
                stores Name of the person with a list of ends of all his
                image names.
              */

              sortedList.insert(Name, masterList)

}
```

After the map has been created, we check the number of images per person and then create a folder named by him. Then iterate from begin to end of its respetctive vector of Image Ids (ImgId) then keep copying/moving those images into that folder.

4.4 Generating Scores

After we are done with all the sorting, we then move to MATLAB for generating image scores based on *SIFT, Correlation and EMD operations.*

The Process is taken control by the following steps:

- Each subject is compared with rest all other subjects.
- The three ways of generating scores is operated.
- Score values for a particular subject is stored temporarily.
- Finally, a separate CSV file is created by that person's name storing scores of all the three operations *(SIFT, Correlation and EMD)* for every other individual in a form of a table.

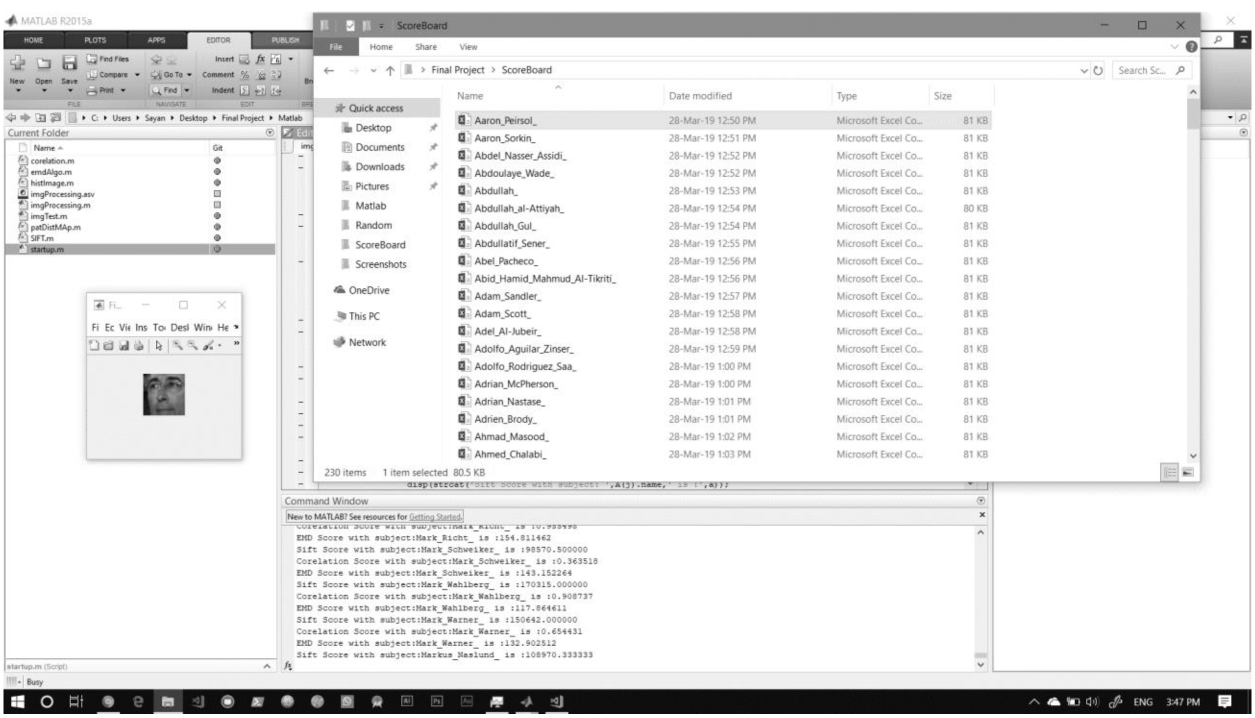
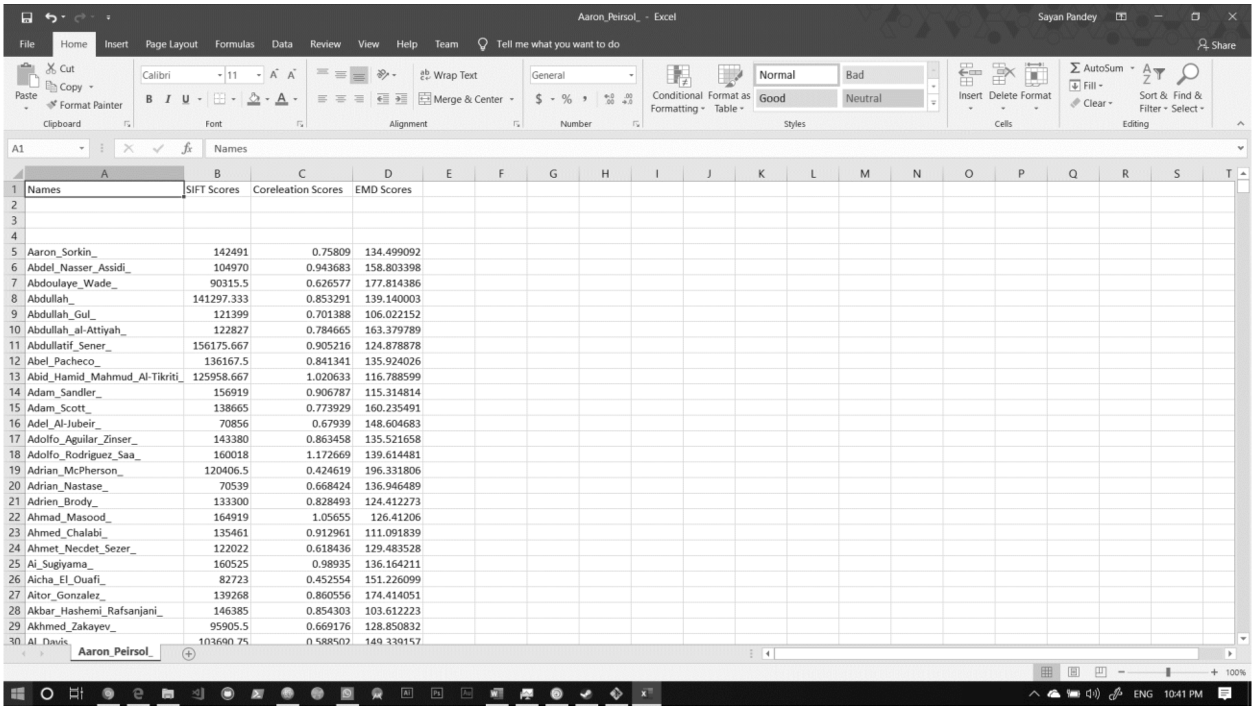


Fig 20: Screenshot showing scores and CSV files for every Individual



	Names	SIFT Scores	Coreleation Scores	EMD Scores
1	Names	SIFT Scores	Coreleation Scores	EMD Scores
2				
3				
4				
5	Aaron_Sorkin_	142491	0.75809	134.499092
6	Abdel_Nasser_Assidi_	104970	0.943683	158.803398
7	Abdoulaye_Wade_	90315.5	0.626577	177.814386
8	Abdullah_	141297.333	0.853291	139.140003
9	Abdullah_Gul_	121399	0.701388	106.022152
10	Abdullah_al-Attiyah_	122827	0.784665	163.379789
11	Abdullatif_Sener_	156175.667	0.905216	124.878878
12	Abel_Pacheco_	136167.5	0.841341	135.924026
13	Abid_Hamid_Mahmud_Al-Tikriti_	125958.667	1.020633	116.788599
14	Adam_Sandler_	156919	0.906787	115.314814
15	Adam_Scott_	138665	0.773929	160.235491
16	Adel_Al-Jubeir_	70856	0.67939	148.604683
17	Adolfo_Aguilar_Zinser_	143380	0.863458	135.521658
18	Adolfo_Rodriguez_Saa_	160018	1.172669	139.614481
19	Adrian_McPherson_	120406.5	0.424619	196.331806
20	Adrian_Nastase_	70539	0.668424	136.946489
21	Adrien_Brody_	133300	0.828493	124.412273
22	Ahmad_Masood_	164919	1.05655	126.41206
23	Ahmed_Chalabi_	135461	0.912961	111.091839
24	Ahmet_Necdet_Sezer_	122022	0.618436	129.483528
25	Ai_Sugiyama_	160525	0.98935	136.164211
26	Aicha_El_Ouafi_	82723	0.452554	151.226099
27	Aitor_Gonzalez_	139268	0.860556	174.414051
28	Akbar_Hashemi_Rafsanjani_	146385	0.854303	103.612223
29	Akhmed_Zakayev_	95905.5	0.669176	128.850832
30	Al_Davis	103690.75	0.588502	149.339157

Fig 21: Screenshot showing scores table for Aaron_Piersol

4.5 Reading and Fusing Scores

Then we read these scores from the CSV files and finally we go for fusion. The important steps for this approach are given below:

- Fused Scores are read and stored into temporary tables.
- Each Table for each individual is ranked according to the score following the logic – 'The lower the score the Higher the Rank'.
- These scores are then ranked and made ready for fusion.
- All Three operators' scores are ranked.

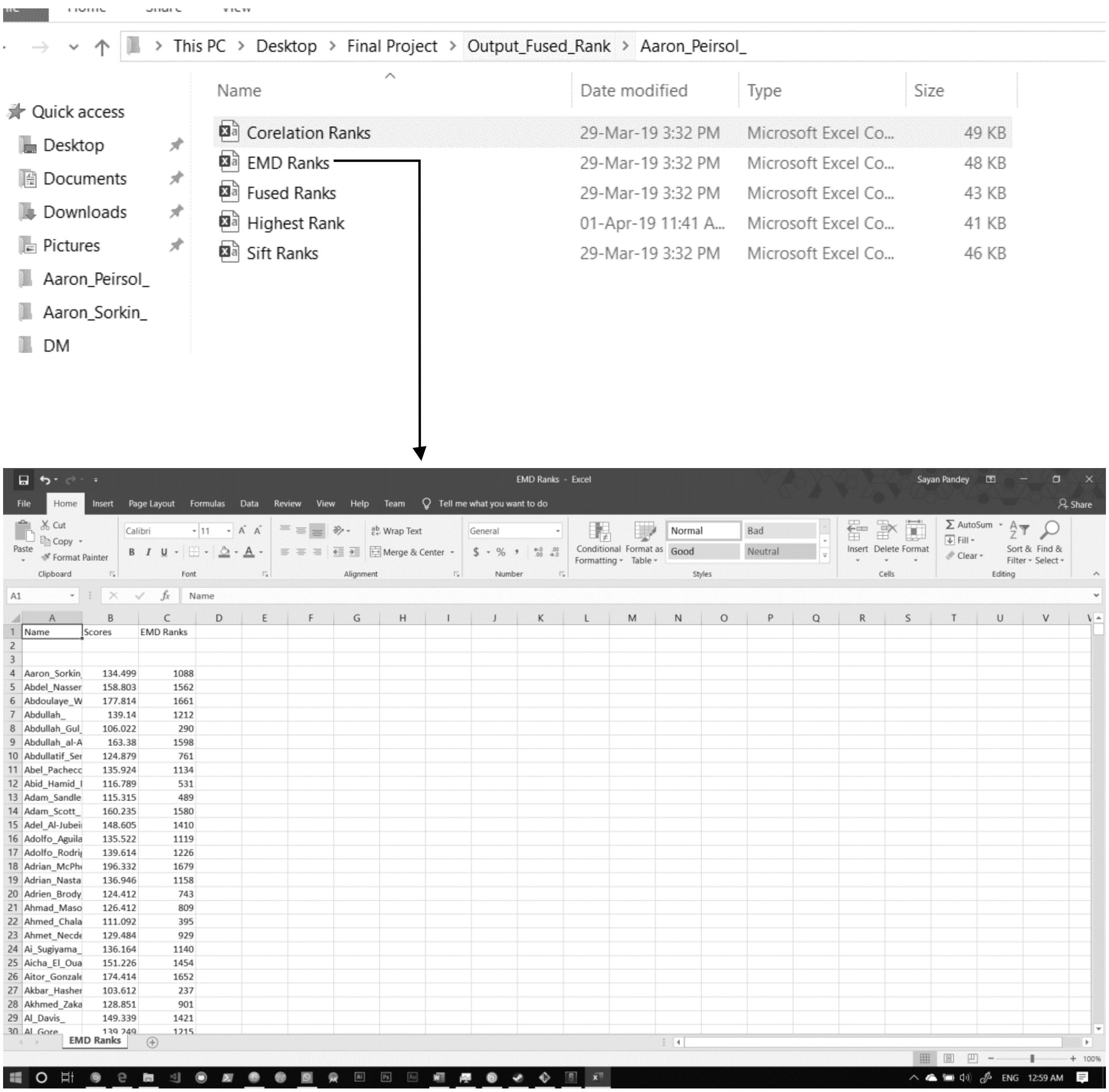
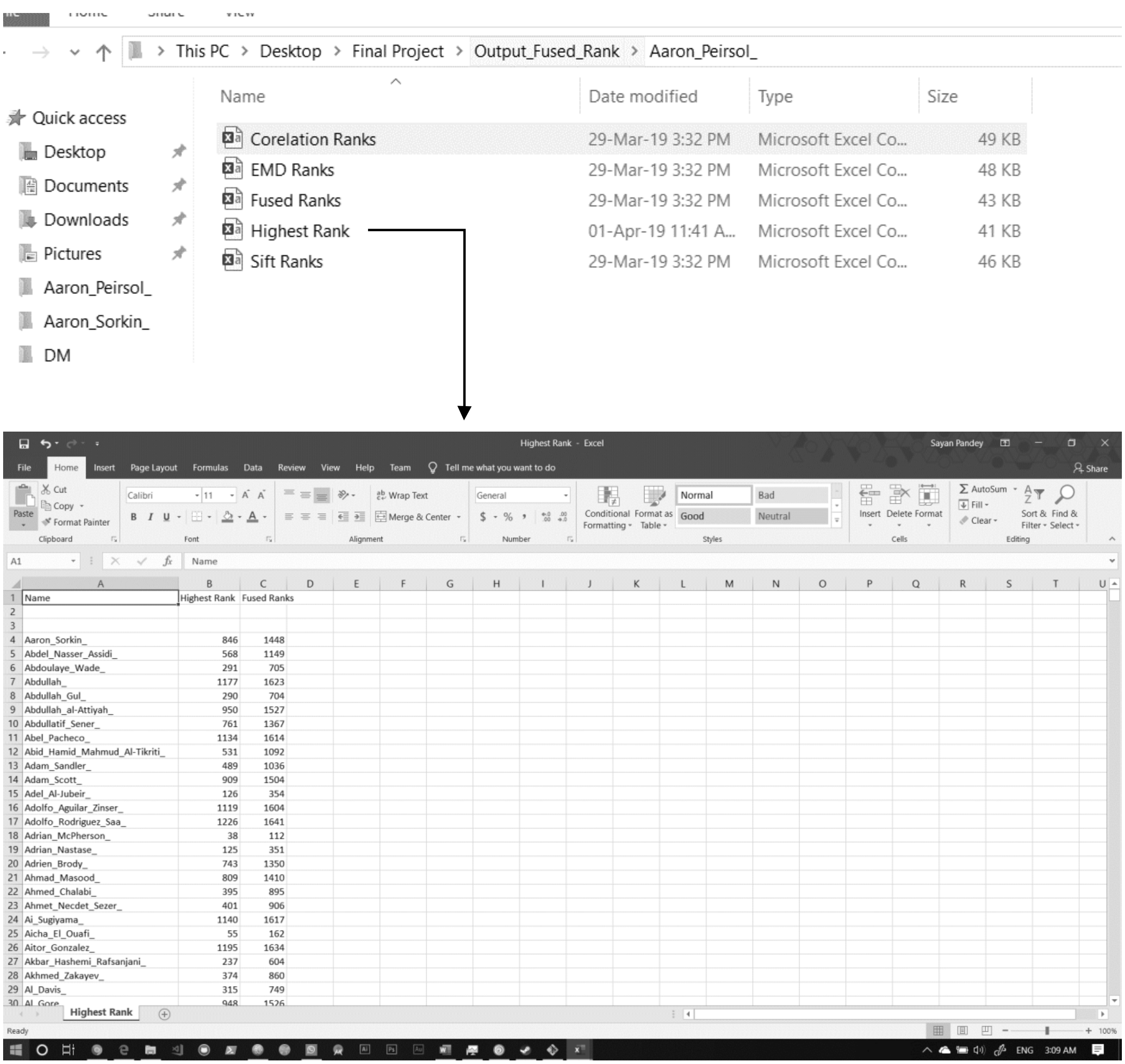


Fig 21: Screenshot showing scores (EMD) and respective rankings

Then we read these scores from the CSV files and finally we go for fusion. For Fusion we Apply *'Highest Rank Method'* and find the fused rank table for each and every individual. The sample of the table is given below.



Name	Highest Rank	Fused Ranks
Aaron_Sorkin_	846	1448
Abdel_Nasser_Assidi_	568	1149
Abdoulaye_Wade_	291	705
Abdullah_	1177	1623
Abdullah_Gul_	290	704
Abdullah_al-Attiyah_	950	1527
Abdullatif_Sener_	761	1367
Abel_Pacheco_	1134	1614
Abid_Hamid_Mahmud_Al-Tikriti_	531	1092
Adam_Sandler_	489	1036
Adam_Scott_	909	1504
Adel_Al-Jubeir_	126	354
Adolfo_Aguilar_Zinser_	1119	1604
Adolfo_Rodriguez_Saa_	1226	1641
Adrian_McPherson_	38	112
Adrian_Nastase_	125	351
Adrien_Brody_	743	1350
Ahmad_Masood_	809	1410
Ahmed_Chalabi_	395	895
Ahmet_Necdet_Sezer_	401	906
Ai_Sugiyama_	1140	1617
Aicha_El_Ouafi_	55	162
Aitor_Gonzalez_	1195	1634
Akbar_Hashemi_Rafsanjani_	237	604
Akhmed_Zakayev_	374	860
Al_Davis_	315	749
Al_Gore_	948	1526

Fig 22: Screenshot showing fused scores and rankings

4.6 Identification

To understand identification in a convincing way let us use an analogy to make things clear and finally we will show the actual logic behind identification ranks.

4.6.1 Identification Analogy

To make it interesting let assume we are playing a game and the name of the game is ***'Guess the Age'***. The game deals with guessing the age of a person. The rules are simple, suppose there are 10 people playing this game and each player will guess the age of other player or the age of the player in a range of five years except his or her own age as definitely one must be knowing his/her age. Suppose someone can guess the age of another person to be 20 – 25 years. When every player is considered rational, honest and in sound mind, we will get 90 such guessing results clear and authentic based on the players' speculation. If we note down the results and for a particular player then we find max frequency of occurrence of an age group among all guessed by others we can claim that to be his age group by some percentage chance. For example, if a person X is guessed to lie in an age group of 30-35 years 7 times, 25-30 years and 45-50 years once each by 9 other players, we can claim person X is in age group of 30-35 years by a probable percentage of

$$\frac{7}{9} * 100 = 77.78\%$$

4.6.2 Identification Logic

Since the analogy is quite clear so we can move forward with our logic of identifying the subjects from our fused table. Like the analogy for every single person we find number of times a rank is issued to him in all the tables which are not fused. In other words, a person can lie in a table in different rank position for different person for different matchers. Our task is to mine that person’s name in all the tables available and create a frequency table for each and every individual as shown in the figure.

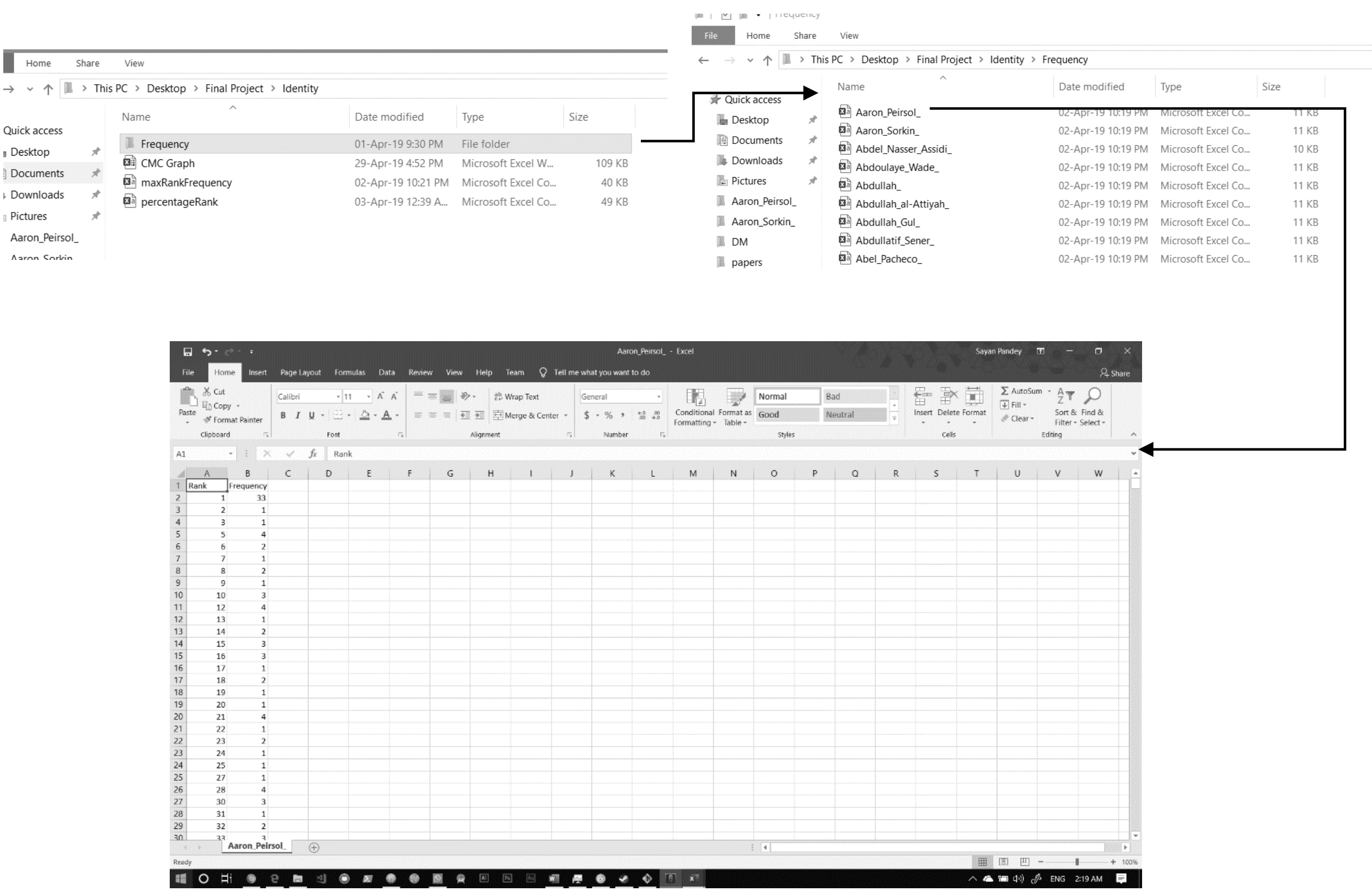


Fig 23: Screenshot showing Frequency of occurrence of Ranks

Again, after mining all the frequency tables we finally find the *Rank with maximum frequency of occurrence* for each individual. This rank will serve us as the purpose for identification.

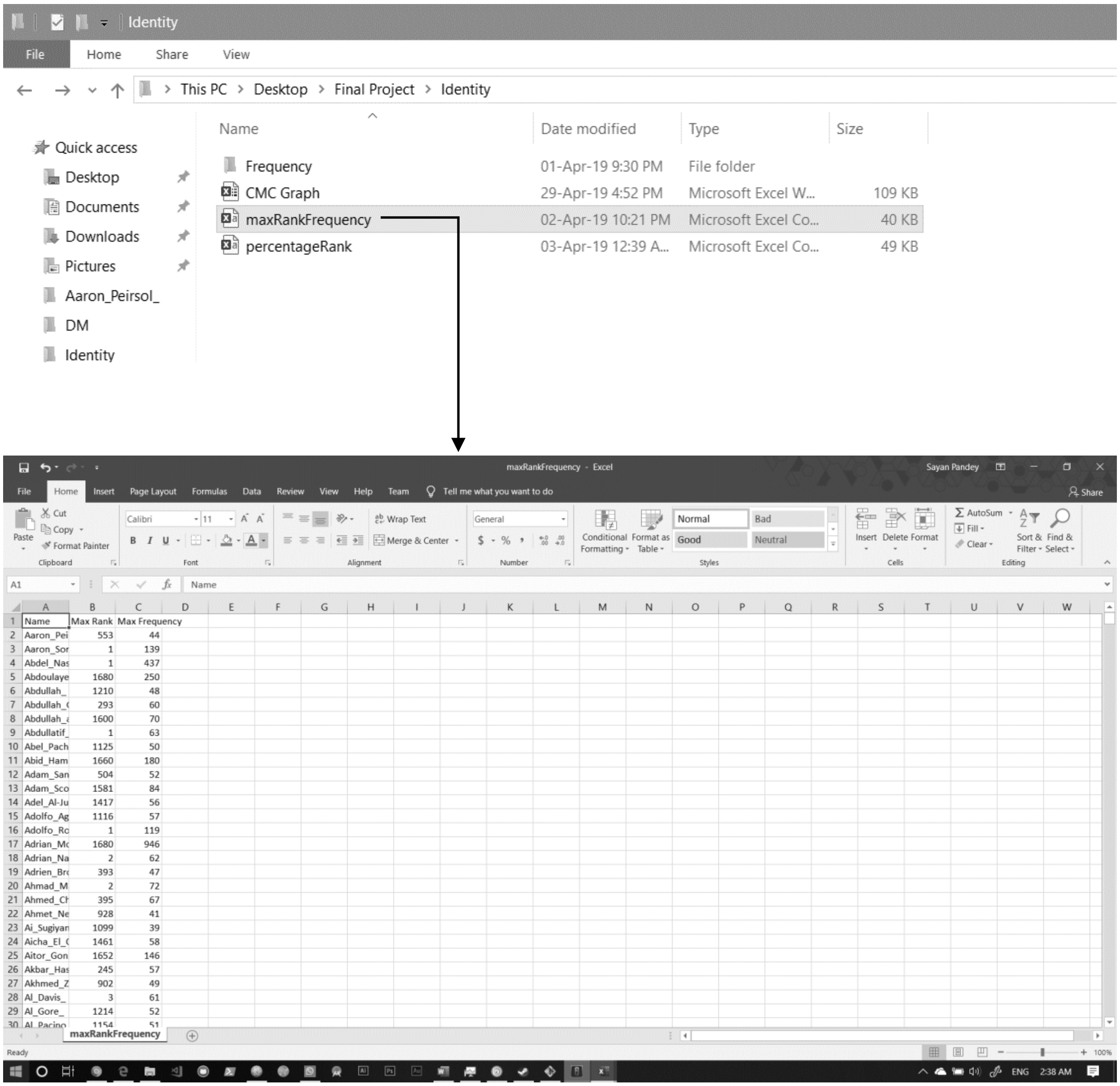


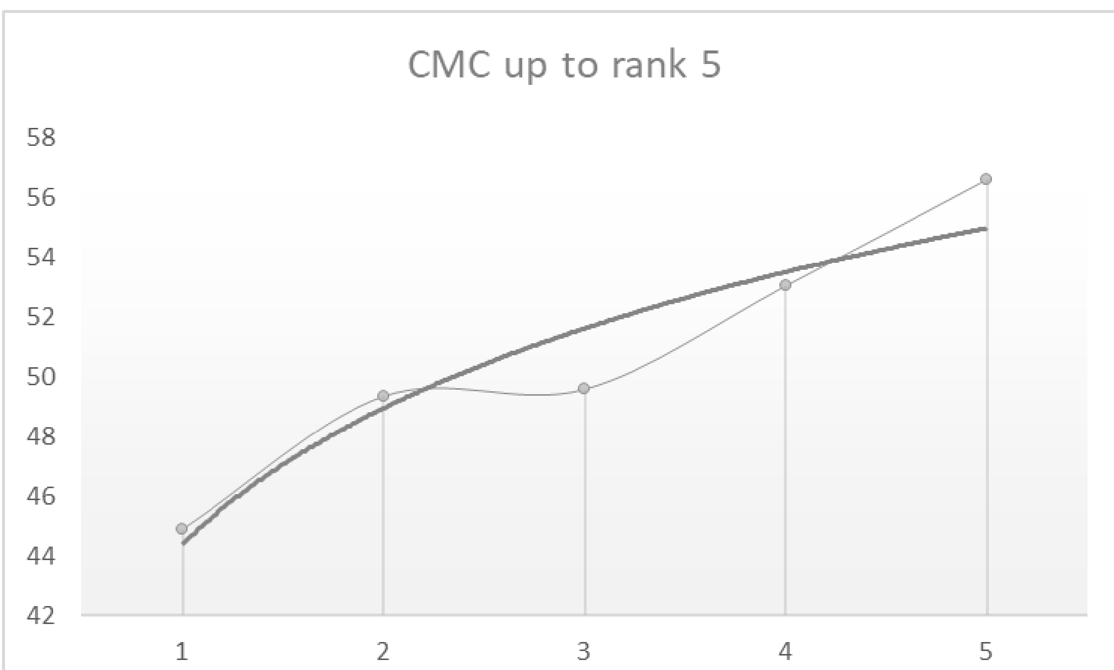
Fig 24: Screenshot showing Maximum Frequency of occurrence of Ranks

Finally, we find the occurrence of this *Maximum Frequency Rank* in all the fused tables and find out how many times that maximum Frequency Rank has occurred and calculate its percentage.

4.6.3 CMC Curves

When this Identification percentages are placed in a cumulative order, we get a special type of graph called the CMC graph. This graph shows us how efficiently we are able to identify a group of people under a range of rank. The more is the percentage amount the more is accuracy. Below are the graphs which show the accuracy percentage in a range of rank.

NOTE: X axis denotes Range of Ranks Y axis denotes percentage accuracy.



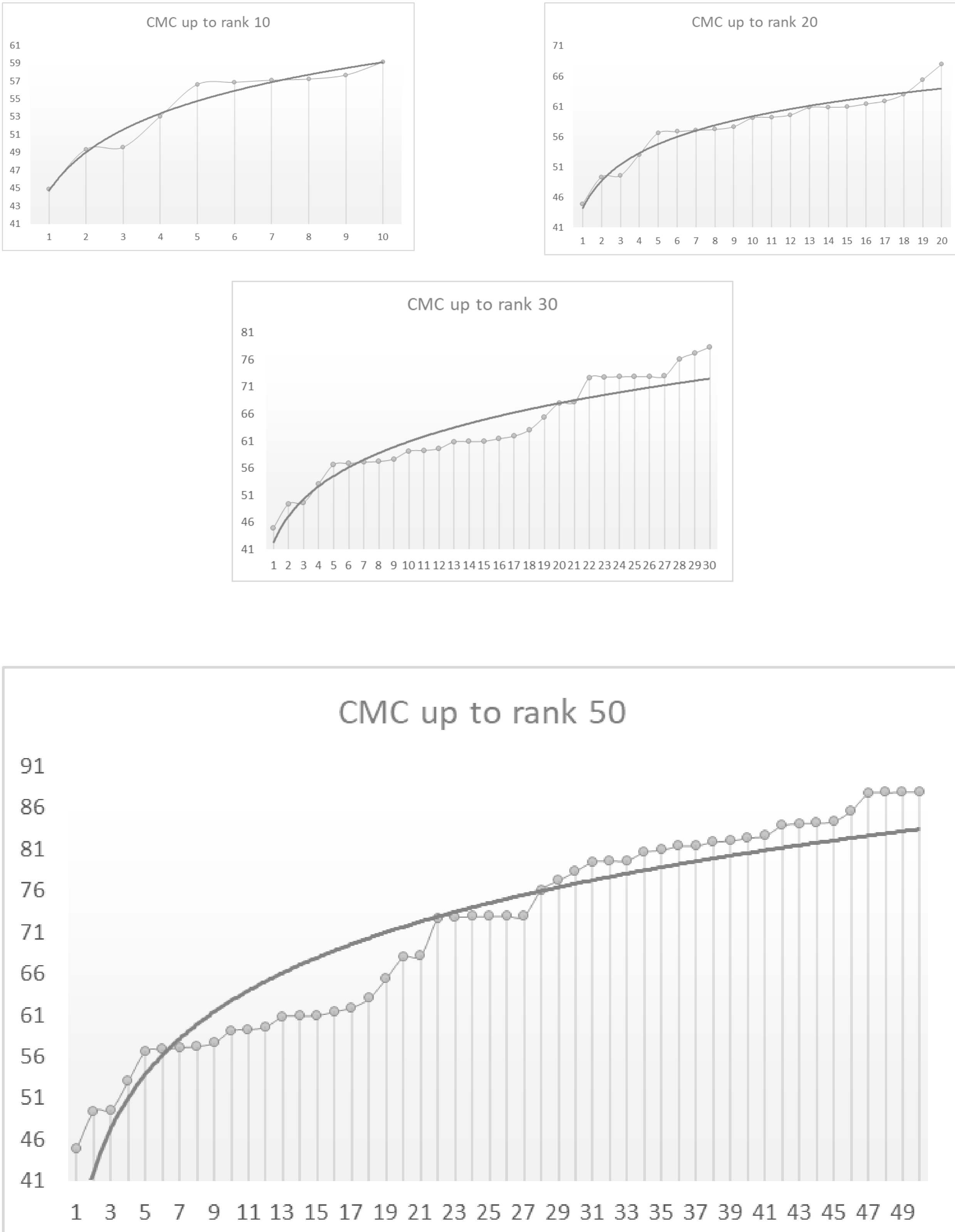


Fig 25: CMC Graphs up to rank 50 shows more than 86% accuracy

4.7 CPU Times

The computer used for the operation has the following specifications:

- **CPU:** Intel Core i7-5500U @ 2.50Ghz auto overclock @ 3.00Ghz
- **RAM:** 16.0 GB
- **System Type:** 64- bit Windows 10 Professional
- **GPU:** Nvidia GeForce 920M DDR5 4GB graphics memory
- **Secondary Storage:** 2TB
- **Connectivity:** Intel Dual Band Wireless-AC 3160 and 10/100 Ethernet port

The whole process took a lot of time to compute however the majority of time consumption was done in **MATLAB score generation and Visual Studio 2017 console operations** consisting of reading files and fusion operations and then writing files. Below is a screenshot of typical CPU usage during the operation.

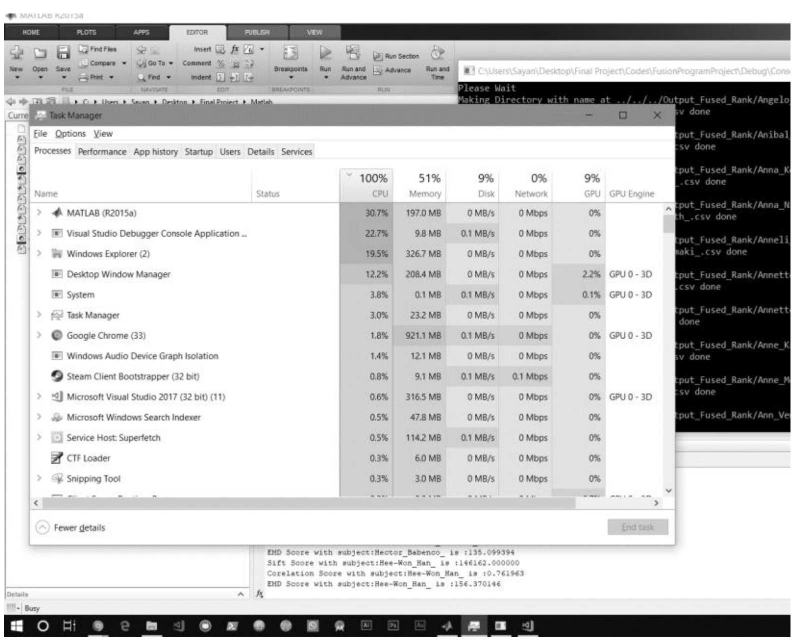


Fig 26: CPU usage during operation

The process is hugely CPU and memory intensive even with **100% use of CPU and 51% use of primary memory (RAM),** the process of generating scores and fusion itself took more than **24 hours** on non-stop operation. The average operation of time is about **52 seconds** over all 1680 individuals. Minimum time taken is **37.37 seconds** for subject *'Nancy_Demme_'* and maximum time taken is **313.828 seconds** for subject *'Queen_Elizabeth_II_'.* The following screenshot shows computation times.

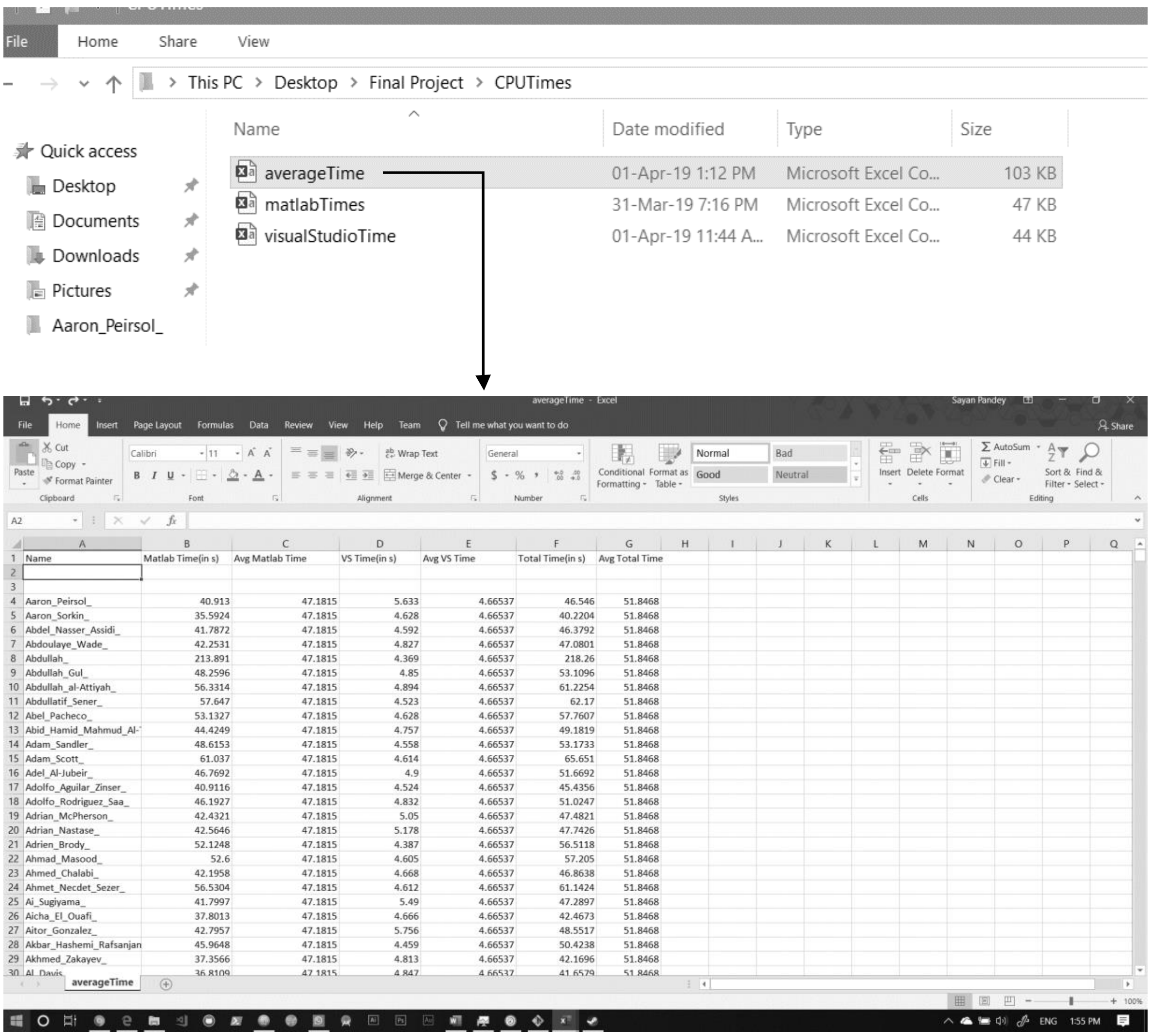


Fig 27: Screenshot showing computation times for each subject

Chapter 5

Conclusion and Future Works

This segment includes the conclusive results of our work and its future aspects and scopes. This work was done on the *Unconstrained Face Identification using Rank Level Fusion.*

5.1 Summary and Conclusion

Combining multimodal data proves to be a very promising trend, both in experiments and in real-life biometric authentication applications. Multimodal biometric systems can overcome some of the limitations of unimodal systems. For example, the problem of non-universality is addressed since multiple traits can ensure sufficient population coverage. Also, multimodal biometric systems make it difficult for an intruder to simultaneously spoof the multiple biometric traits of a registered user. The key to multimodal biometrics is the **fusion of various biometric data**. Fusion can occur at various levels, the most popular one is the score level where the scores output by the individual modalities are integrated. However, in our Experiment we have used the concept of *Rank Level Fusion.* Hence ranking all the scores into ranks and then fusing them.

5.2 Future Works

Despite reasonable improvements in the performance shown, the biometric authentication systems still pose a variety of challenges under different scenarios. Following are the few considerations of future works that can be extended or implemented for the biometric authentication system.

- The authentication results presented in this thesis should be validated using other public multimodal real-user databases. Specifically, it would be necessary to measure the performance of the suggested approaches with a larger dataset, containing more individuals.

- The proposed techniques in this thesis can also be applied with other kinds of biometrics like hand geometry and palm veins in conjunction with fingerprint where all the unimodal inputs can be taken using a single sensor.
- Investigating further methods for evaluating the quality of the testing data will be an important aspect of the future work. The distance between a reference model and the model associated with a claimant can be useful for evaluating the quality of testing data.
- Most Rank-level fusion rules assume that the scores pertaining to all the matchers are available prior to fusion. Hence, if there are some missing matching scores they are not well equipped to deal with this problem. So future work can be considered on missing scores.