Data Analysis Report

# **Overview**

## **Biometrics**

Biometrics are body measurements and calculations related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. A biometric recognition system can run in two different modes: identification or verification.

## **Identification**

Identification is the process of trying to find out a person’s identity by examining a biometric pattern calculated from the person’s biometric features.

In the identification case, the system is trained with the patterns of several persons. For each of the persons, a biometric template is calculated in this training stage. A pattern that is going to be identified is matched against every known template, yielding either a score or a distance describing the similarity between the pattern and the template. The system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns (in this case all patterns of persons not known by the system) from being correctly identified, the similarity has to exceed a certain level. If this level is not reached, the pattern is rejected.

## **Verification**

In the verification case, a person’s identity is claimed a priori. The pattern that is verified only is compared with the person’s individual template. Similar to identification, it is checked whether the similarity between pattern and template is sufficient to provide access to the secured system or area.

# **Aims and Objectives**

## **Aim**

Analyzing Performance metrics of Face Recognition System.

## 

## **Objective**

To estimate the pose of the face by Face landmarks(left eye, right eye, nose, left mouth, right mouth and chin) and analyzing performance metric by varying the threshold values.

# **Work Stages**

## **Face Detection**

The camera will detect and recognize a face.

## 

## **Face Analysis**

A photo of the face is captured and analyzed. Most facial recognition relies on 2D images rather than 3D because it can more conveniently match a 2D photo with public photos or those in a database. Distinguishable landmarks or nodal points make up each face.

## 

## **Converting An Image to Data**

The analysis of your face is then turned into a mathematical formula. These facial features become numbers in a code. This numerical code is called a faceprint. Similar to the unique structure of a thumbprint, each person has their own faceprint.

## 

## **Finding a Match**

Your code is then compared against a database of other faceprints. This database has photos with identification that can be compared.



Performance Metrics

## 

## **True Acceptance Rate (TAR)**

Measure of the chance that a system (correctly) verifies a true claim of identity.

TAR =

## **False Acceptance Rate (FAR)**

Measure of the chance that a user who should be rejected is accepted by the system.

FAR =

## **True Rejection Rate (TRR)**

Measure of the chance that a system (correctly) rejects a false claim of identity. It is also known as recall.

TRR =

## **False Rejection Rate (FRR)**

Measure of the chance that a user who should be accepted is rejected by the system.

TAR =

## **Accuracy**

Accuracy (ACC) is calculated as the number of all correct predictions divided by the total number of the dataset.

ACC =

## **Precision**

Precision (PREC) is calculated as the number of correct positive predictions divided by the total number of positive predictions.

PREC =

## **F1 Score**

It combines precision and recall into a single measure. Mathematically it’s the harmonic mean of precision and recall.

F1 Score =

## **Misclassification Rate**

It tells you what fraction of predictions were incorrect. It is also known as Classification Error.

ACC =

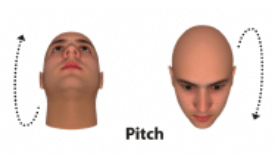
## **Equal Error Rate (EER)**

The rate at which both acceptance and rejection errors are equal.

# **Head Pose Estimation**

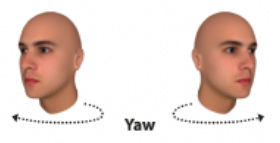
## **Pitch**

Rotation around the side-to-side axis is called pitch.



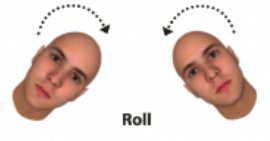
## **Yaw**

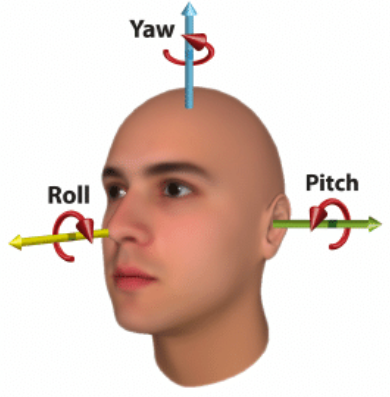
Rotation around the vertical axis is called yaw.



## **Roll**

Rotation around the front-to-back axis is called roll.





# **False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics**

## 

## **What is false acceptance rate or FAR?**

As the number of false acceptances (FAR) goes down, the number of false rejections (FRR) will go up and vice versa (see the figure below). The point at which the lines intersect also has a name: the Equal Error Rate (EER). This is where the percentage of false acceptances and false rejections is the same

**What is false rejection rate or FAR?**

The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system’s FRR typically is stated as the ratio of the number of false recognitions divided by the number of identification attempts.

## 

## **Relation between FAR, FRR and EER**

As the number of false acceptances (FAR) goes down, the number of false rejections (FRR) will go up and vice versa (see the figure below). The point at which the lines intersect also has a name: the Equal Error Rate (EER). This is where the percentage of false acceptances and false rejections is the same.

#### How does this affect the security level and user convenience?

If you try to reduce the FAR to the lowest possible level, the FRR is likely to rise sharply. In other words, the more secure your access control, the less convenient it will be, as users are falsely rejected by the system. The same also applies the other way round. Do you want to increase user convenience by reducing the FRR? In this case the system is likely to be less secure (higher FAR).

**Configuring the FAR and FRR in the software**

The FAR and FRR can usually be configured in a security system’s software by adjusting the appropriate criteria so that they are more or less strict. We can conclude from the information above that this will result in a system that is more secure (but less user-friendly) or less secure (but more user-friendly).

**Problem linked to this**

There are only a few systems on the market that allow a high level of security to be achieved in combination with user-friendly access control. If an organisation does not opt for such a system, it will often prioritise user convenience over security.

You can imagine the thinking behind this: “We don’t want people to have to queue up at the door because the system is not working properly. They may already have spent all morning stuck in traffic and not yet had a coffee.”

In some situations, of course, prioritising convenience in this way may be acceptable to users. However, that is clearly not the case in situations where they expect a high level of security. And that is the problem: often the user has no insight into exactly how the software has been configured. This can create a false sense of security.

**Visibility of the FAR and FRR**

Like many security experts, we take the view that the FAR and FRR should not be changed invisibly. We believe that the visibility of these aspects should be part of a system’s configuration. In any case, this is something to bear in mind when selecting your access security system!

# **Thresholding (False Acceptance / false recognition)**

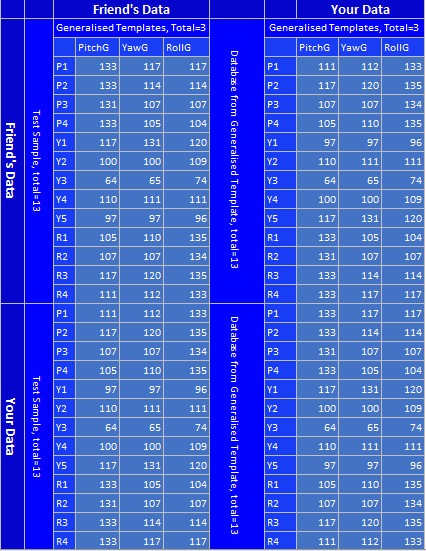
# **What is Thresholding**

We use scores (also called weights) to express the similarity between a pattern and a biometric template. The higher the score is, the higher is the similarity between them. As described in the preceding section, access to the system is granted only, if the score for a trained person (identification) or the person that the pattern is verified against (verification) is higher than a certain threshold.

**Example**

In this table we can see the score of a train person (Your Data) and a test person ( Friend Data) being compared. The score is higher where

patterns are similar and low where patterns are dissimilar. We will call it **general matrix**.



## 

## **How to differ between clients and impostors**

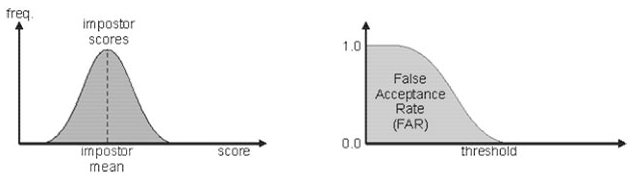
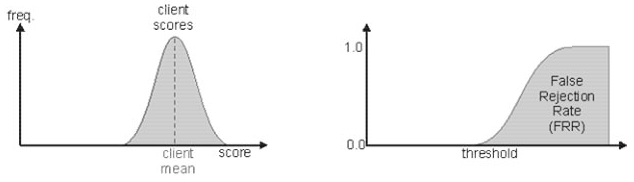
In theory, client scores (scores of patterns from persons known by the system) should always be higher than the scores of impostors. If this would be true, a single threshold, that separates the two groups of scores, could be used to differentiate between clients and impostors.

## **Problems in Classification**

Due to several reasons, this assumption isn’t true for real world biometric systems. In some cases impostor patterns generate scores that are higher than the scores of some client patterns. For that reason it is a fact that however the classification threshold is chosen, some classification errors occur.

## **Choice of Threshold**

The choice of the threshold value becomes a problem if the distributions of the client and the impostor scores overlap, as shown in the next image on the left. On the right, the corresponding false acceptance and false recognition rates are displayed.



## **Comparing biometric systems**

In order to compare two biometric systems both FARs FRRs values should be specified of both the systems. If the manufacturers of the systems just specify a single value for the FARs of them, then it is not sufficient to compare the systems. But also when the values for FAR and FRR are given, there still exists the problem that those values are threshold-dependent. Assuming that the threshold of the systems is adjustable, there is no reasonable way to decide if a system with a higher FAR and a lower FRR performs better than a system with a lower FAR and a higher FRR value.

**Confusion Matrix of Sample Data**

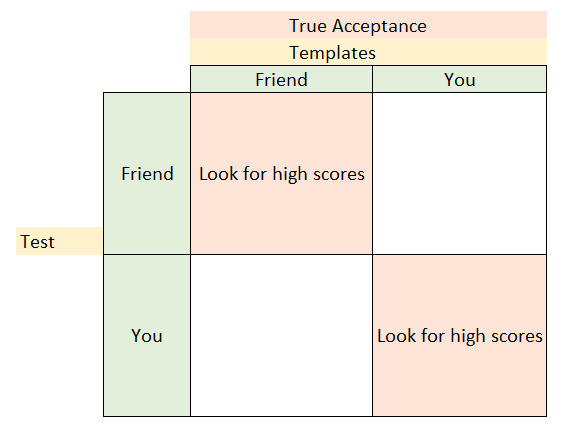
A confusion matrix, also known as an error matrix, is a specific table layout that allows visualization of the performance of an algorithm, typically a supervised learning one.

It is a special kind of contingency table, with two dimensions ("actual" and "predicted"), and identical sets of "classes" in both dimensions (each combination of dimension and class is a variable in the contingency table).



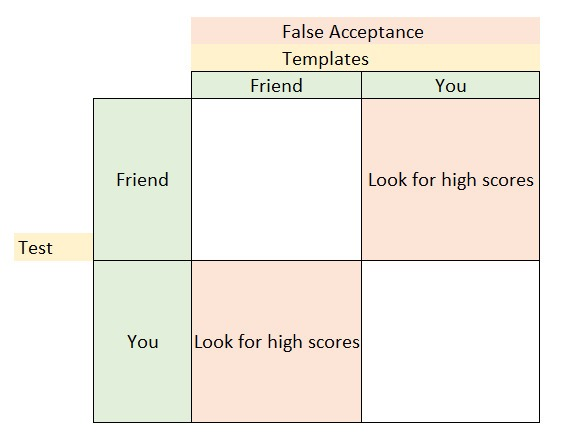
**True positive (TP)**

True Positive is the number of cases correctly identified as true.



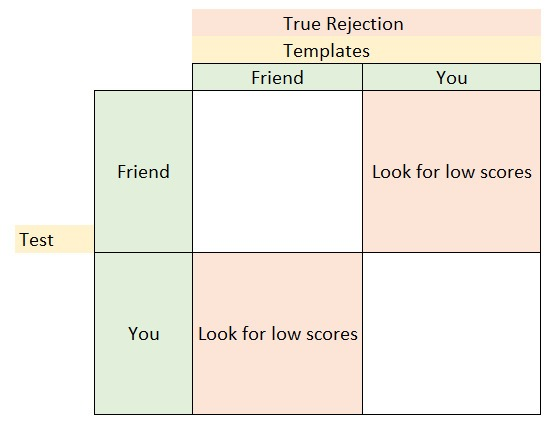
**False Positive (FP)**

False Positive is the number of cases incorrectly identified as true.

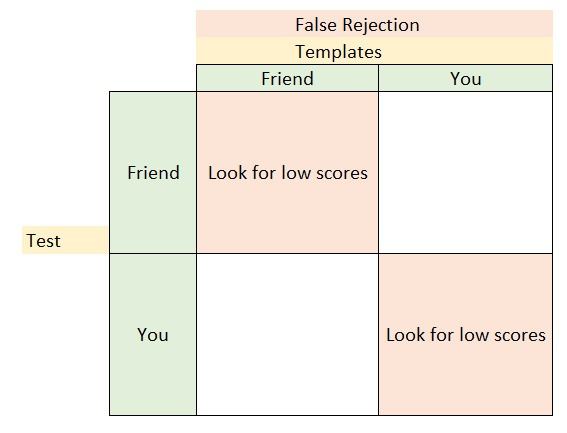


**True negative (TN)**

True negative is the number of cases correctly identified as False.



**False negative (FN)**

False negative is the number of cases incorrectly identified as False.

# **Example**

On the example table introduced in the thresholding portion, we will apply thresholding with threshold value = 120.

## **Acceptance Matrix**

In the acceptance matrix, the score greater than threshold in the general matrix corresponds to 1 and the score less than threshold corresponds to 0.

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

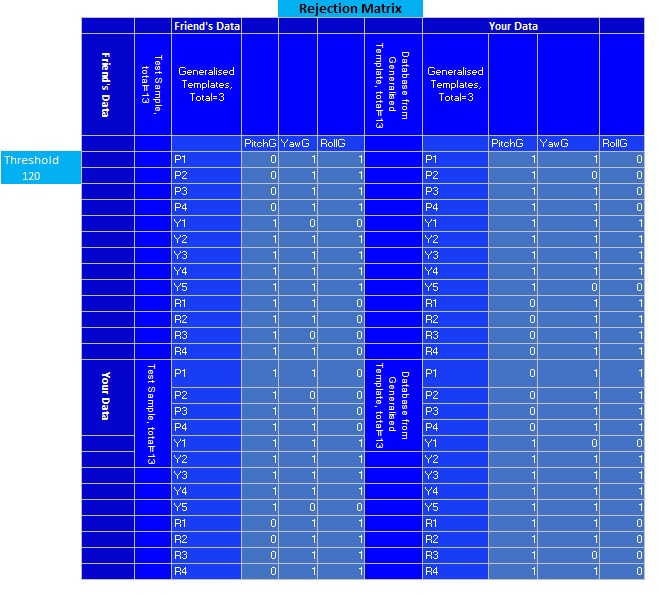
## 

## 

## 

## **Rejection Matrix**

In the acceptance matrix, the score greater than threshold in the general matrix corresponds to 0 and the score less than threshold corresponds to 1.



## 

## 

## 

## 

## 

## 

## 

## 

## **True Positive**

The True Positive matrix for the given general matrix is as follows.

# 

## 

## 

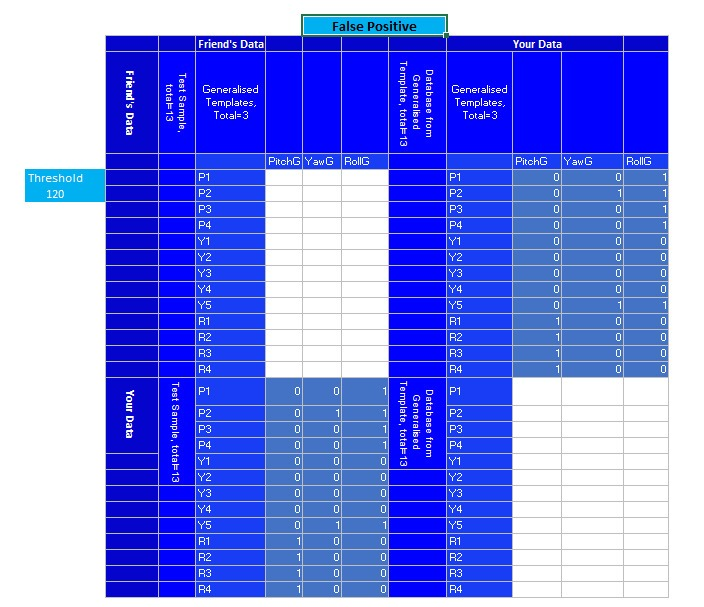
## 

## 

## 

## **False Positive**

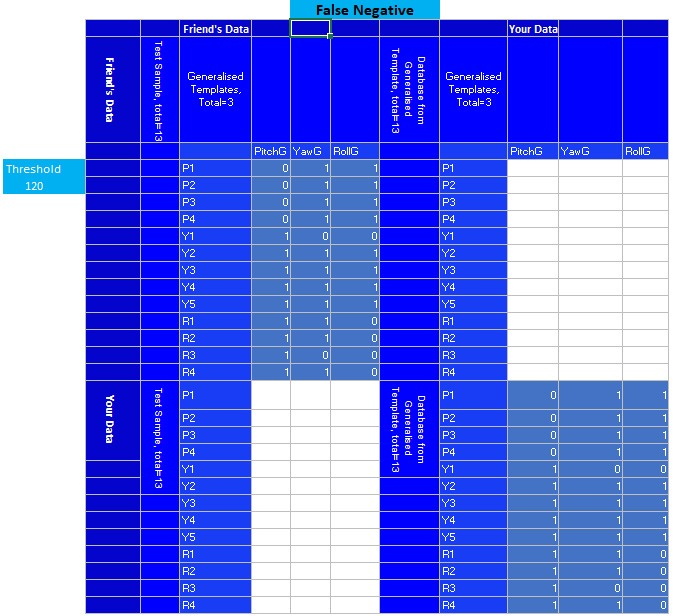
False Positive matrix for the given general matrix is as follows.



## 

## **False Negative**

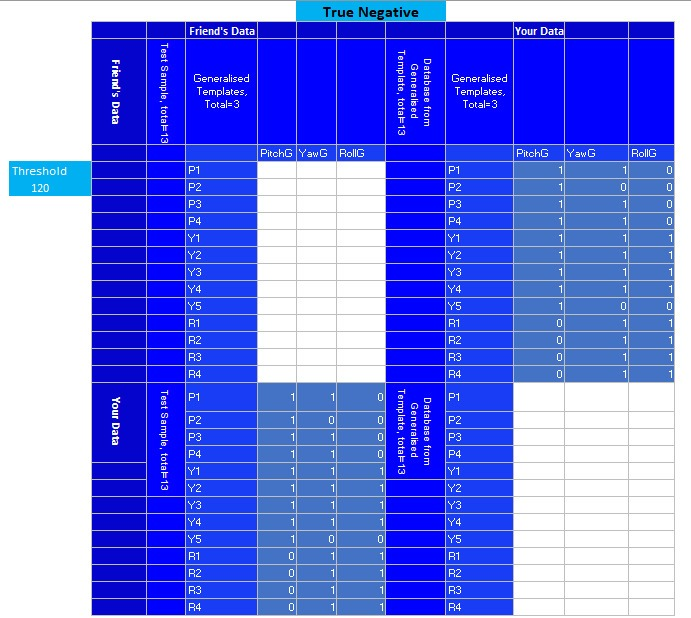
False Negative matrix for the given general matrix is as follows.

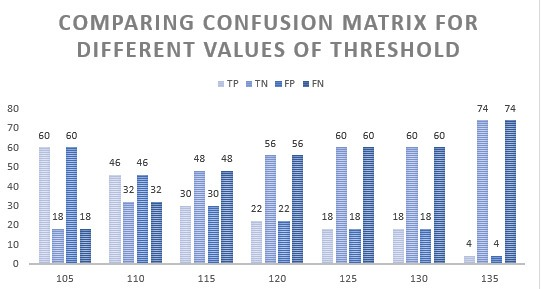


## 

## **True Negative**

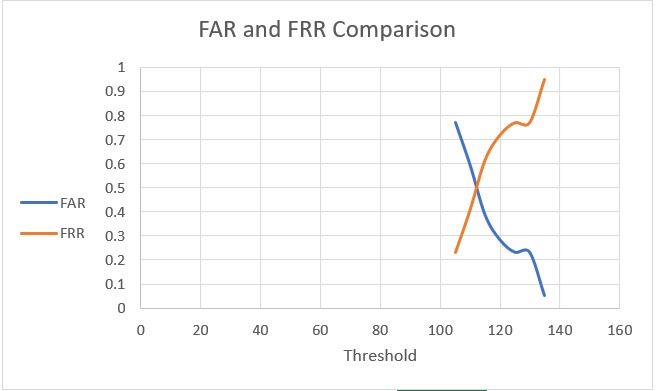
The True Negative matrix for the given general matrix is as follows.



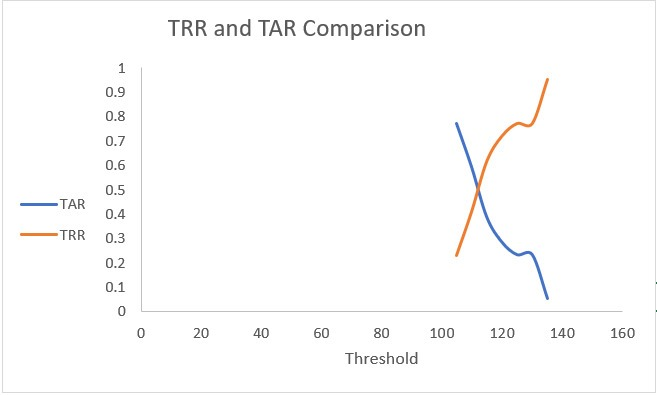


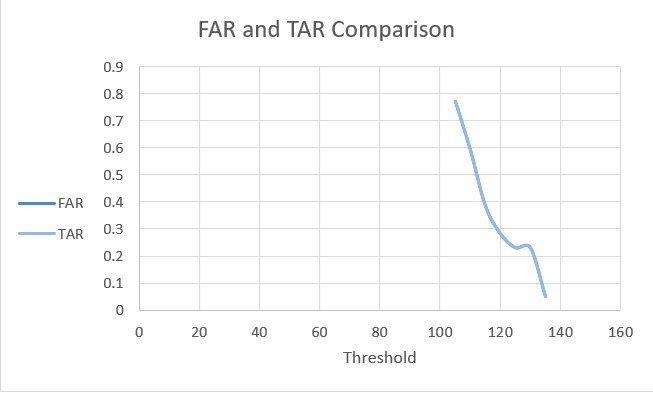
# 

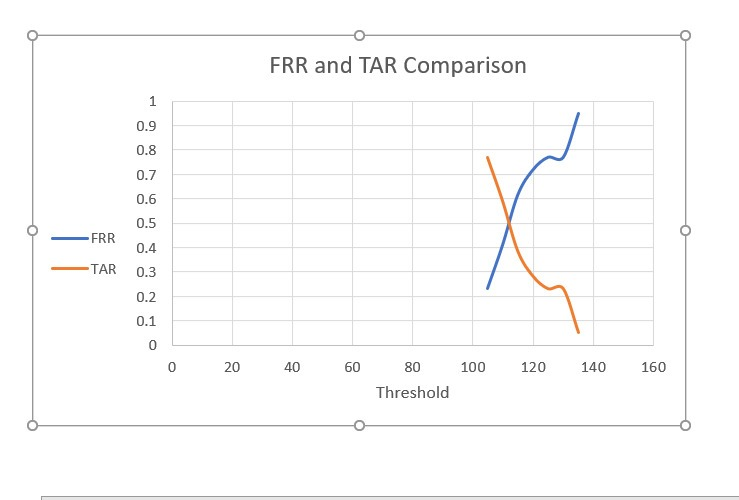
# **Comparison among TAR TRR FRR FAR**

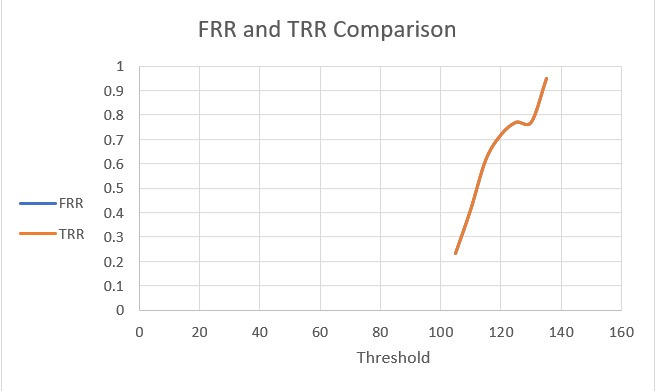


The point at which the FAR and FRR curve intersects is known as the Equal Error Rate (EER). This is where the percentage of false acceptances and false rejections is the same. In our case, EER = 0.5.







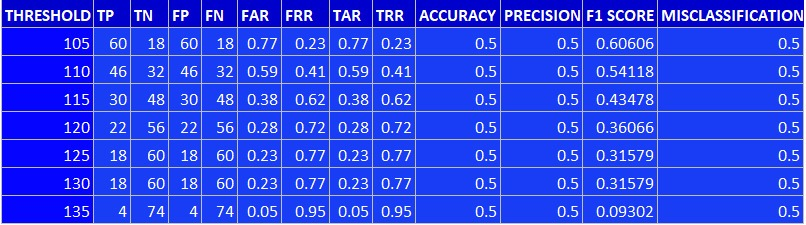


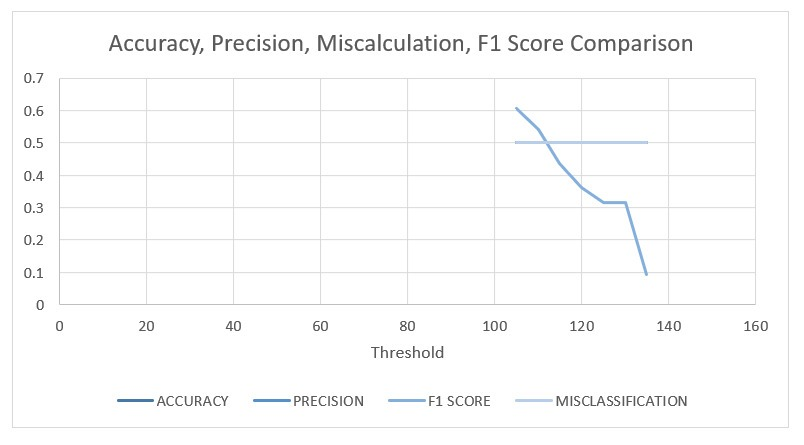


# 

**Performance Metrics**

Following table shows the performance of our system for different values of threshold.





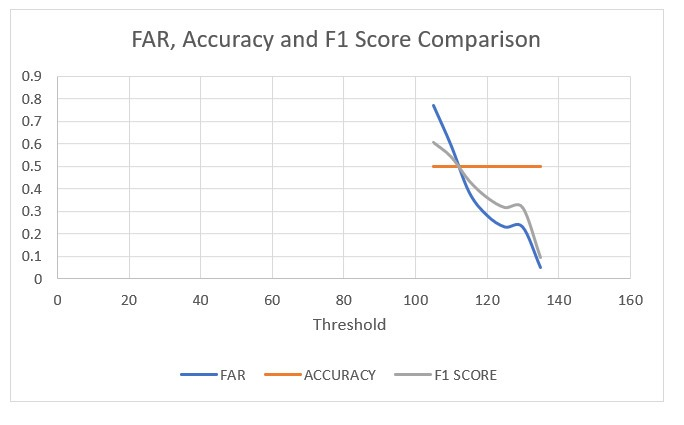
## 

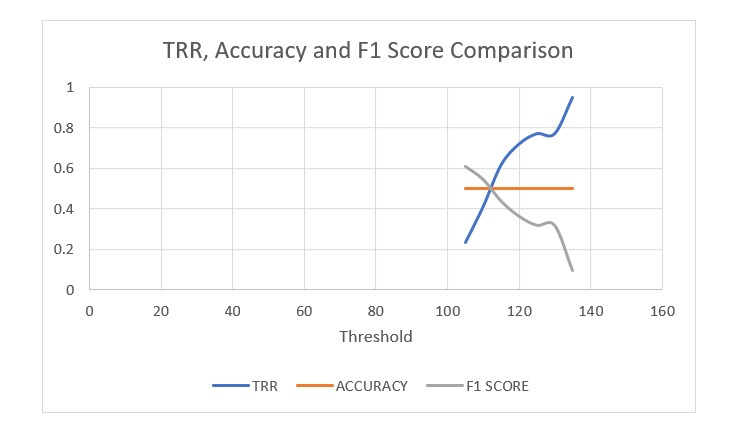
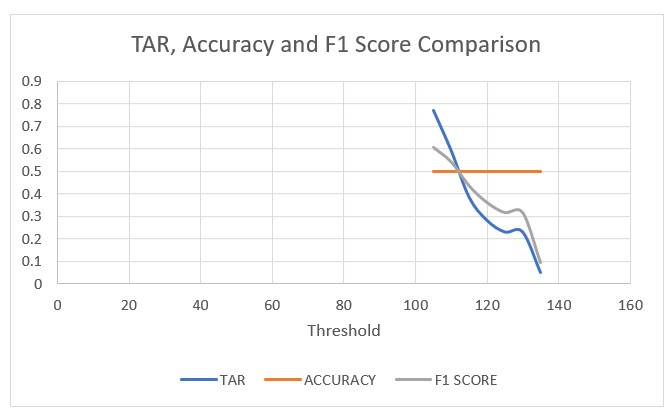
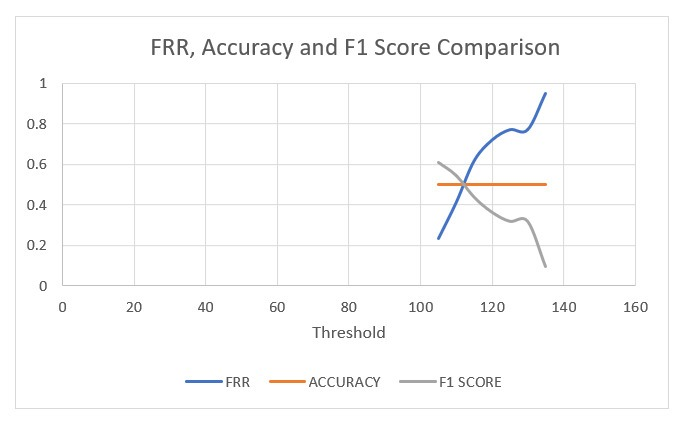
## 

## 

## 

## TRR, TAR, FAR, FRR comparison with Accuracy and F1 Score





# **Conclusion**

These days there is a lot of emphasis on FAR (False Acceptance Rate).

However, FAR only provides half the information. When selecting a biometric solution, we need to find out what the false recognition Rate (FRR) is at the said FAR.

So when a biometric solution provider claims to have a very low FAR, it is very important to find out what the FRR is at this ‘low’ FAR. Then depending upon the application one needs to evaluate whether the FAR & FRR ratio is acceptable for the application.

In a practical scenario a low FAR & a high FRR would ensure that any unauthorized person will not be allowed access. It would also mean that the authorized people will have to reveal their face from different angles or maybe they would have to remove their glasses before they are allowed access.

Therefore, it is good to have a very low FAR, but if this low FAR is coming at the cost of high FAR then the solution needs to be re-evaluated.