# Automatic Signature Stability Analysis and Verification using Local Features

Team Name: Jai Ballaya
Team Members:

- Teja Sai Dhondu (20171075, CSE)
- Swetanjal Dutta  (20171077, CSD)
- Nishant Sharma (20171079, CSE)

TA Mentor: Prathyakshun Rajashankar

Repo URL: https://github.com/swetanjal/Automatic-Signature-Stability-Analysis-And-Verification-Using-Local-Features/

# Abstract

- Present a novel algorithm for a ***fully automatic offline*** system to classify between ***Genuine*** and ***Forged*** signatures even in ***presence of Disguised*** signatures
- Achieved an ***equal error rate of 15%*** on the ***4NSigComp2010*** Dataset, the most well known publicly available dataset for forensic signature verification competition
- ***Local features*** of signature is used instead of global features

# What is unique about this paper...

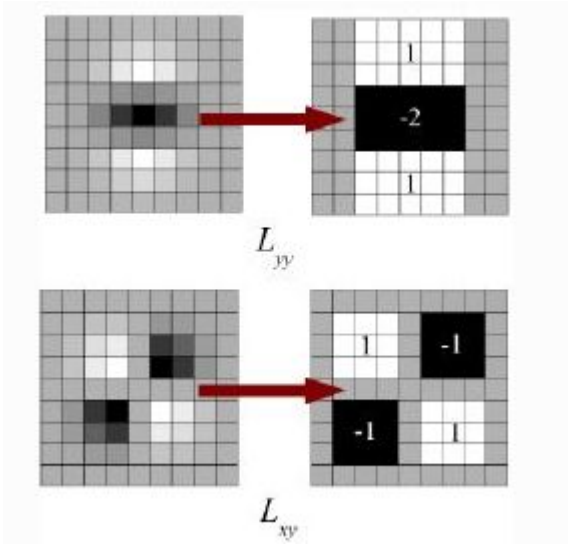
- Using local SURF features to perform stability analysis
- Offline system
- Achieves a low Equal Error Rate even in the presence of **DISGUISED** Signatures
- Equal Error Rate of 15% on 4NSigComp2010 Dataset. Best team in the competition achieved an EER of 55%

# What unique did we do...

- Our main focus was to implement the paper as there was no publicly available implementation of this paper
- Applied our knowledge of writing vectorised codes to make our implementation efficient
- We used threading to achieve a super fast implementation of the code

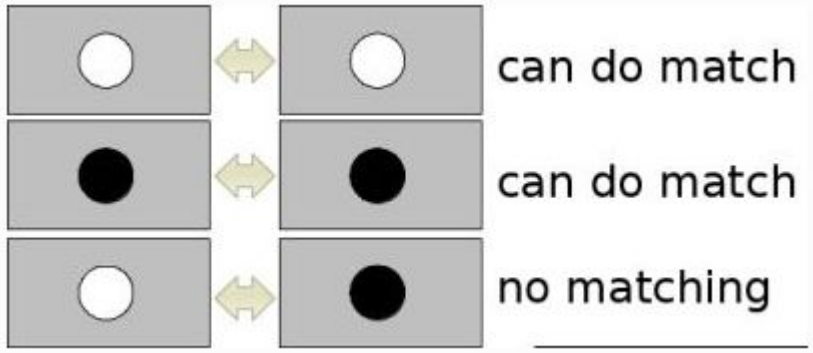
# SURF

- Task: Look for locally distinct points
- In SIFT, Lowe approximated Laplacian of Gaussian with Difference of Gaussian for finding scale-space
- SURF goes a little further and approximates LoG with Box Filter
- Convolution with box filter can be easily calculated with the help of integral images
- SURF rely on determinant of Hessian matrix for both scale and location
- For orientation assignment, SURF uses wavelet responses in horizontal and vertical direction for a neighbourhood of size 6s



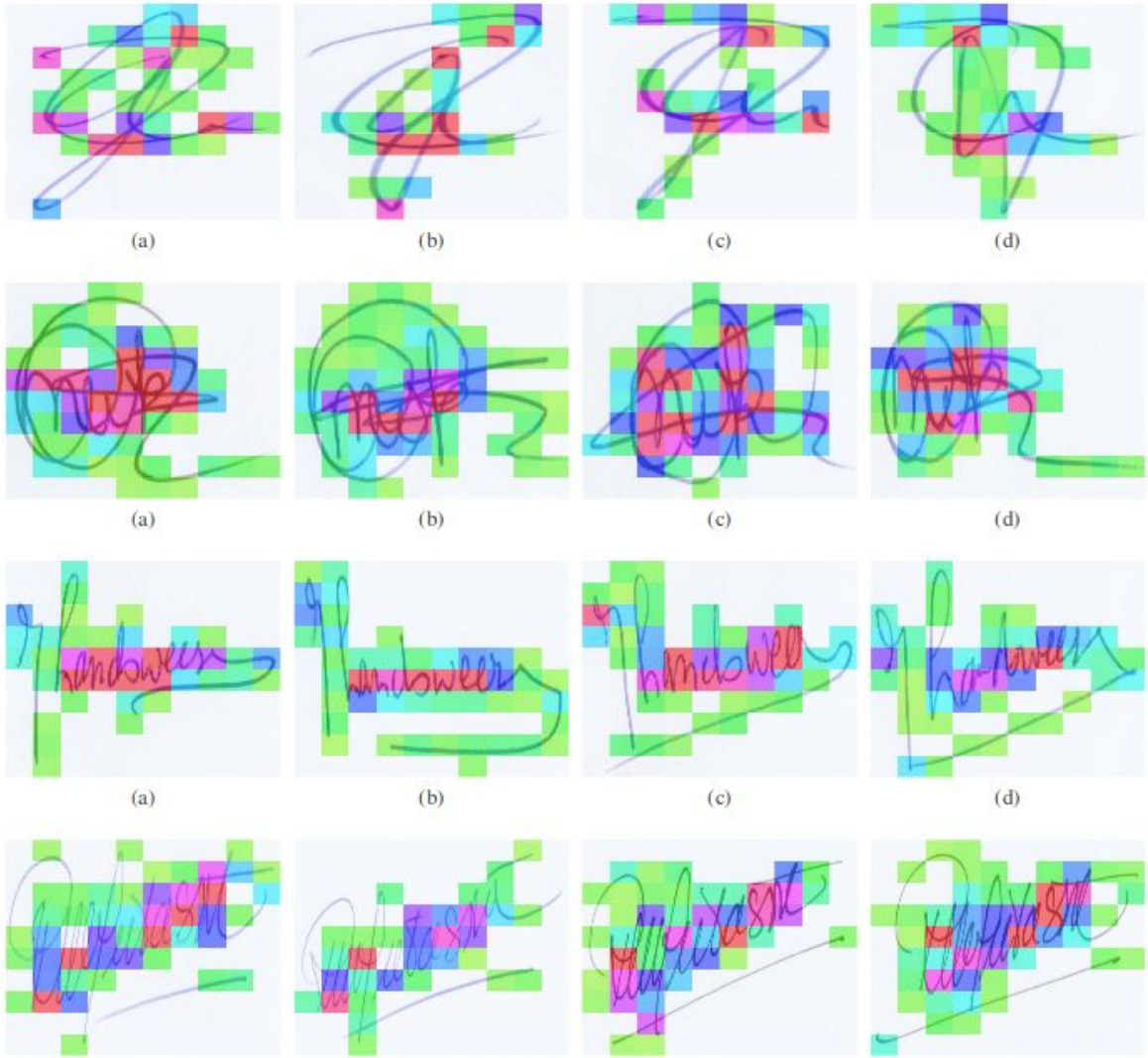
# SURF(continued)

- For feature description, SURF uses Wavelet responses in horizontal and vertical direction
- The sign of the Laplacian distinguishes bright blobs on dark backgrounds from the reverse situation.
- In the matching stage, we only compare features if they have the same type of contrast



# Local Stability Analysis

- Humans generally show the intra-writer or within writer variations when they write signatures
- Hence, we cannot afford to use all regions for verification purposes as it will lead to a large number of false negatives
- The figure on the right are heat maps of some example specimen (genuine) signatures from four different authors (one genuine author in each row)
- Green regions are most stable while red regions are least stable parts



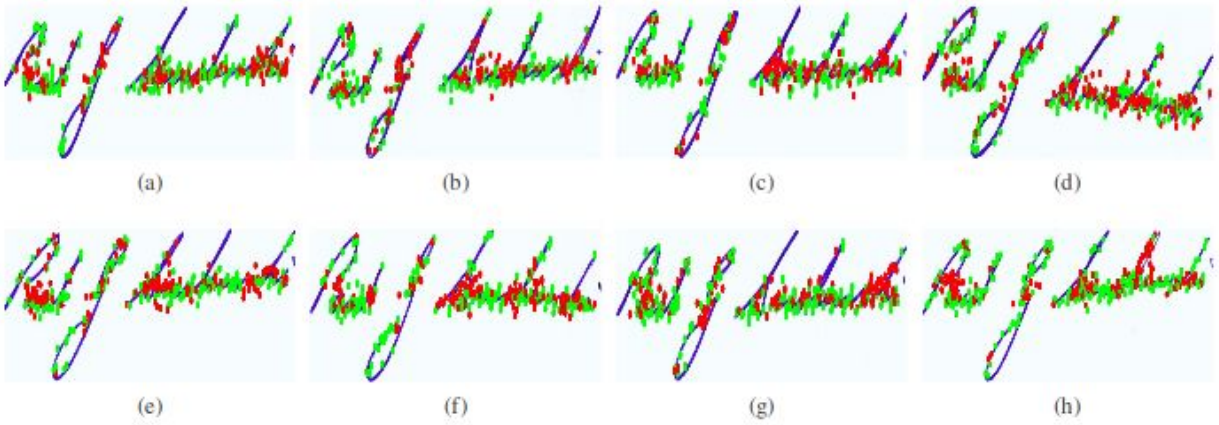
# Algorithm:

Creating a database of stable keypoint descriptors

- Compute SURF keypoint descriptors from all reference signatures except one signature and store in a temporary database(tmp_DB)
- Compute SURF keypoint descriptors from the left out signature and find the distance of each keypoint to the nearest descriptor present in tmp_DB

# Algorithm(contd...)

- Find average distance(d) and eliminate all keypoints having distance greater than d. Descriptors having distance less than or equal to d are added to final database(DB)
- Repeat the above steps in LOO fashion to generate the final database(DB) of keypoint descriptors




The points in red have distance > d, indicating unstable regions. The points in green have distance <= d, indicating stable regions and hence can be used for classification

# Algorithm:

Classification of unseen Signatures

- Extract SURF descriptors from queried signature
- Match each of these 128 dimensional feature vectors with the descriptors in final database(DB)
- If distance between 128 dimensional vector and matched descriptor in DB is less than empirically determined threshold, we consider it as a match

- Depending on percentage of matched points, we proceed with the classification of genuine or forged based on the metrics in the following slides

# Important Metrics: FAR, FRR, EER

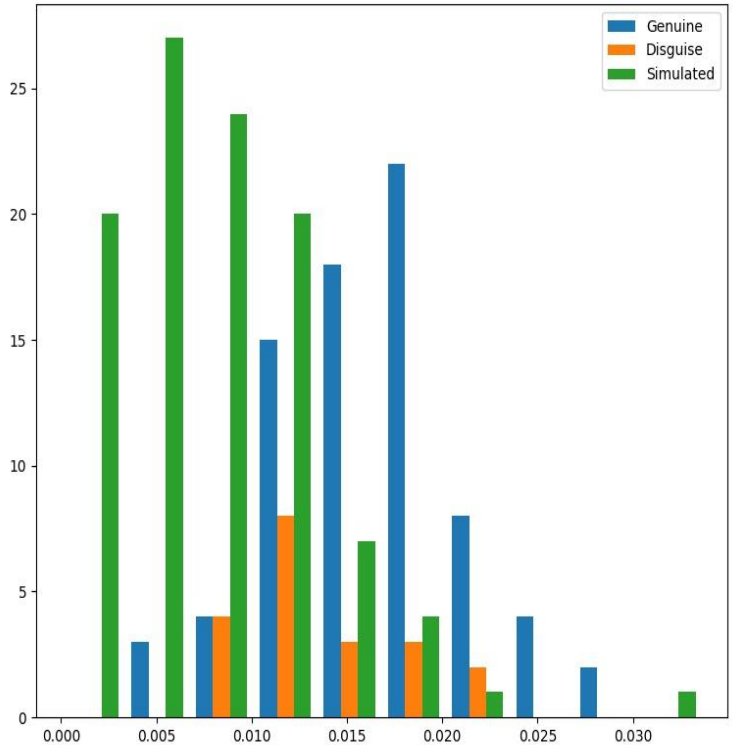
1. False Acceptance Rate(FAR) : Measure of the likelihood that forged signature will be *incorrectly classified as genuine*.
2. False Rejection Rate(FRR) : Measure of the likelihood that genuine or disguised signature will be *incorrectly classified as forged.*
3. Equal error rate (EER): When the above error rates are equal, the common value is referred to as the equal error rate.

# Tuning Hyperparameters

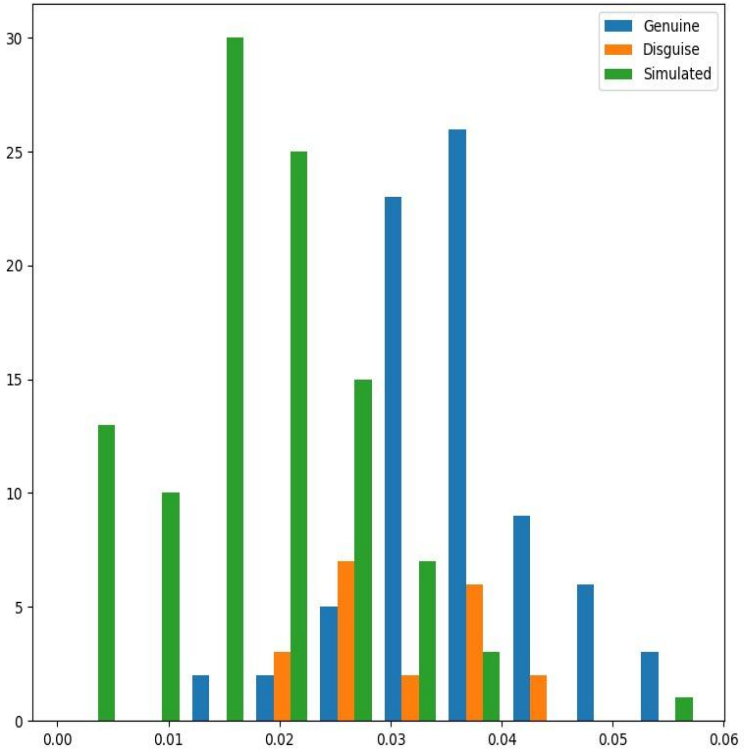

Threshold: Euclidean Distance for deciding matching points

Theta: Percentage matched points for deciding genuine vs forged signature

# Matched Points Percentage VS Threshold

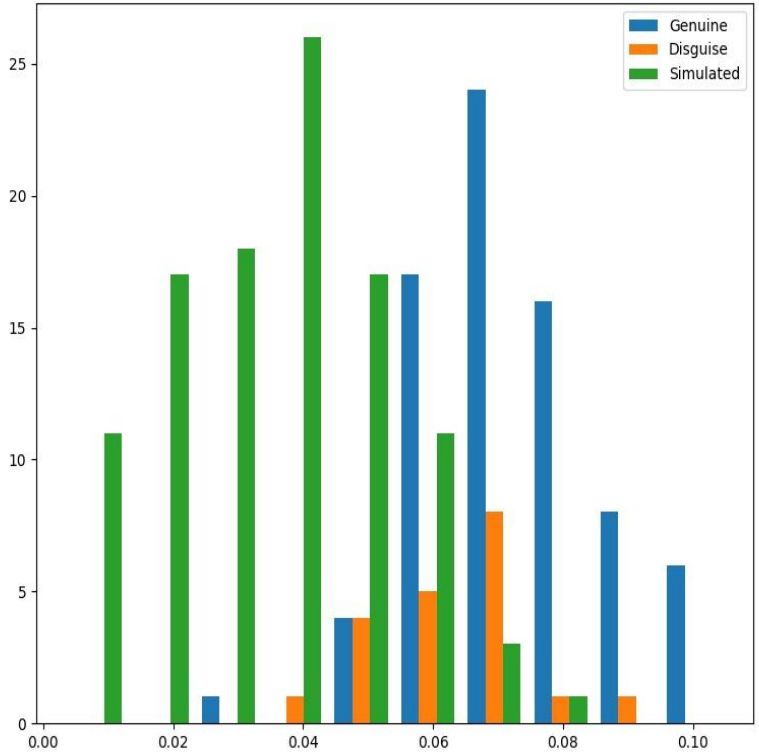



Threshold = 0.10

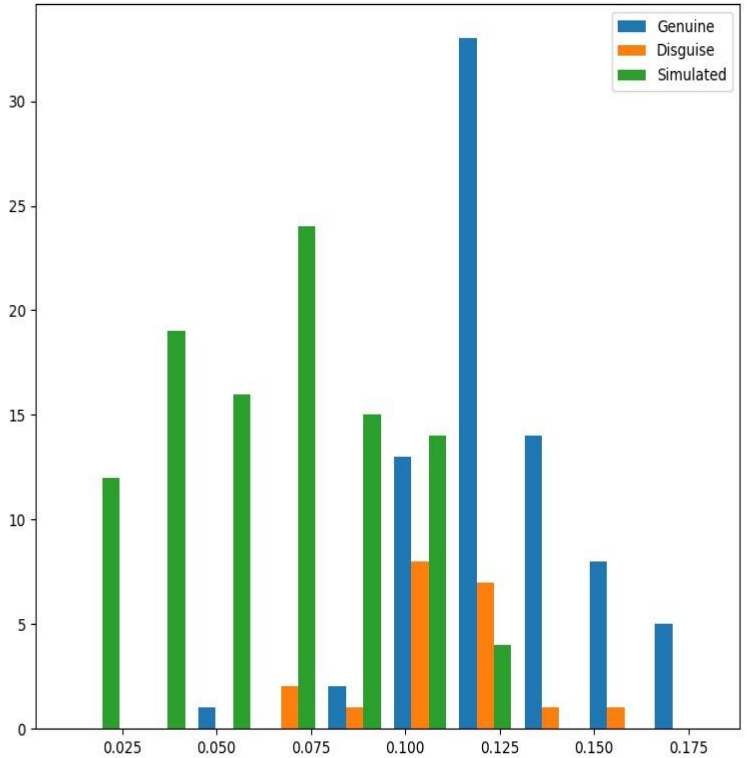



Threshold = 0.11

# Matched Points Percentage VS Threshold

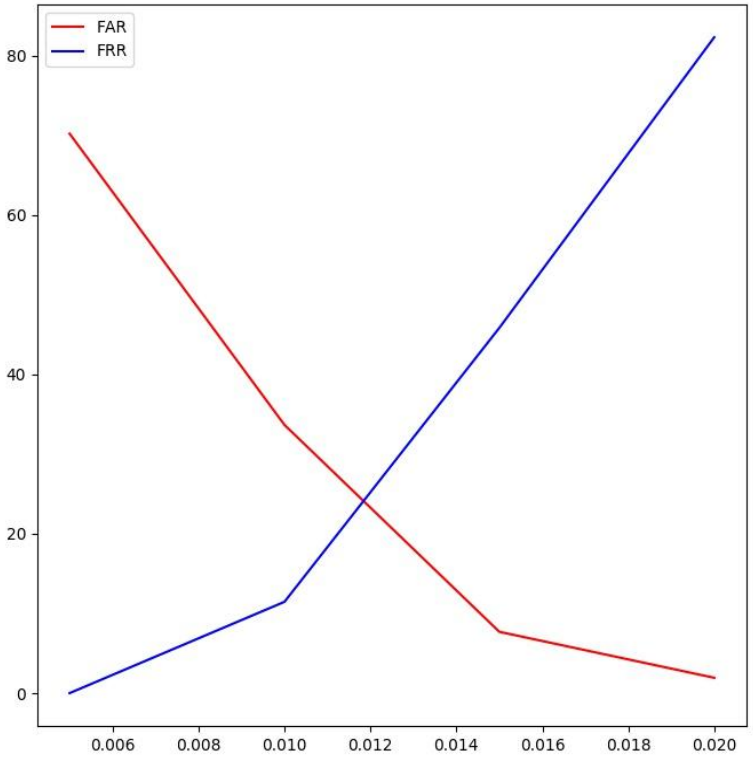



Threshold = 0.12

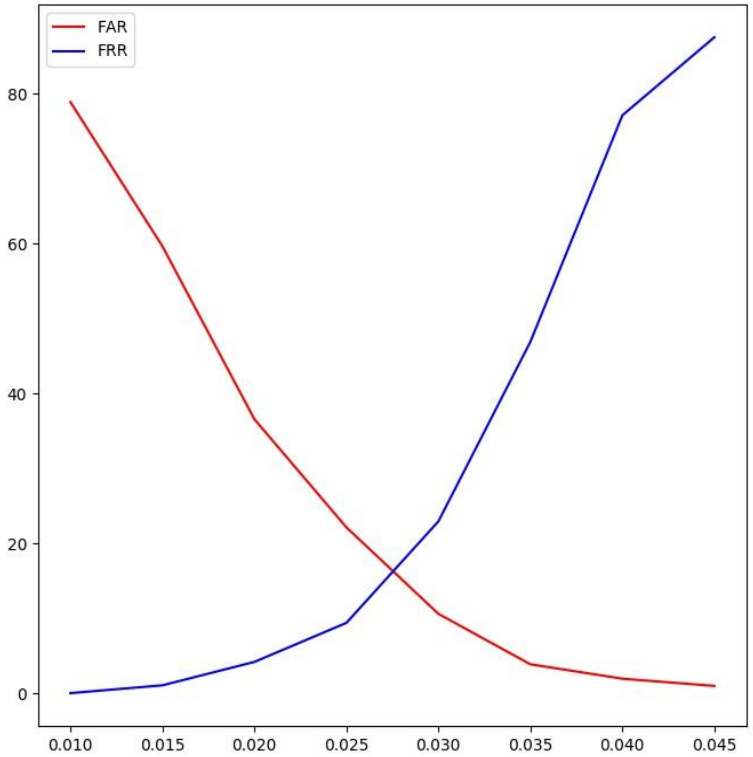



Threshold = 0.13

# EER VS Theta

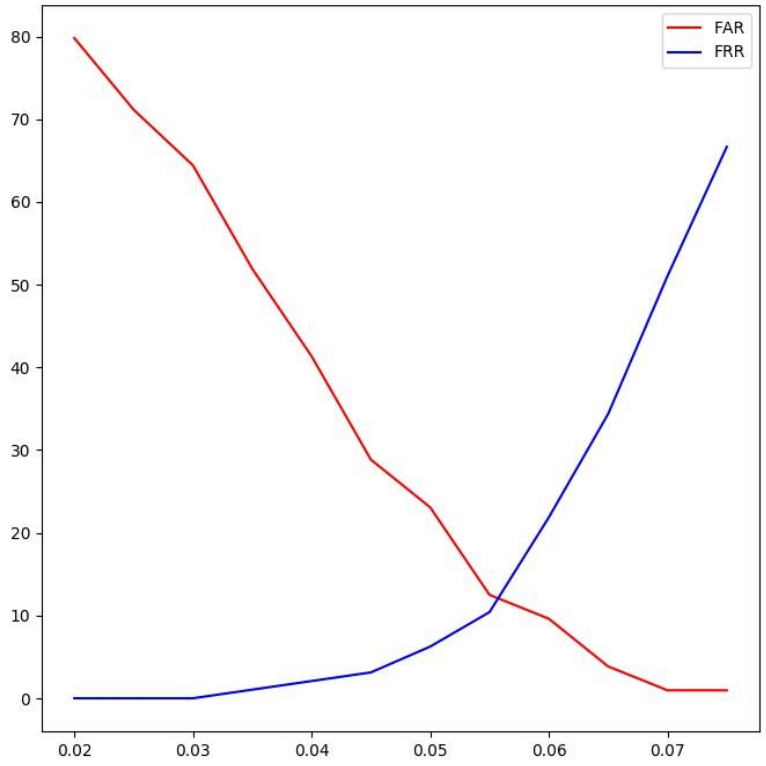



Threshold = 0.10

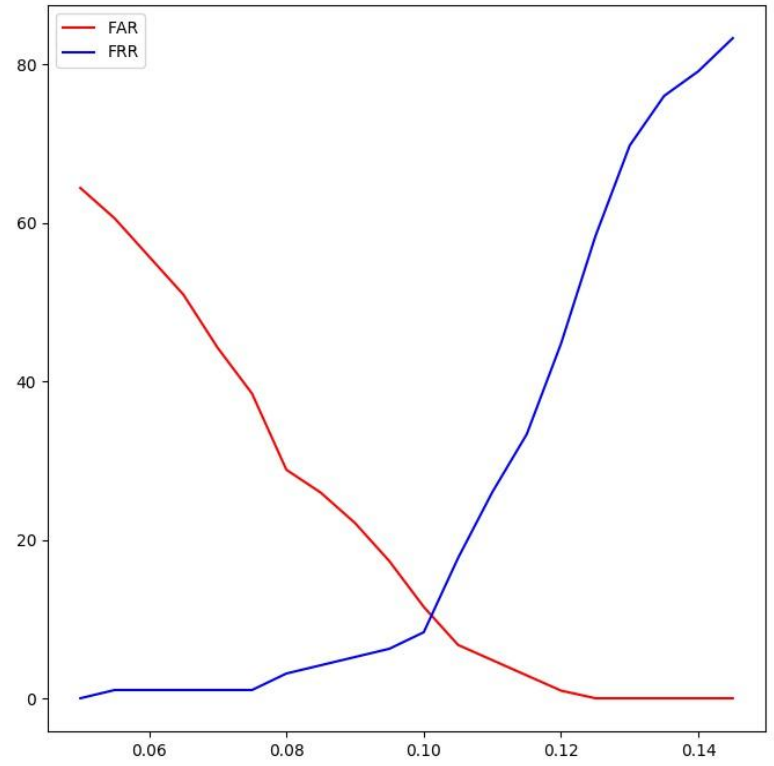



Threshold = 0.11

# EER VS Theta




Threshold = 0.12




Threshold = 0.13

# Confidence Matrix

Best Threshold = 0.11, Theta = 0.0275

| | Genuine | Forged |
|---|---|---|
| Genuine | 68 | 8 |
| Disguised | 12 | 8 |
| Forged | 15 | 89 |

# EER: 16%

# Work Division

"Alone we can do so little, together we can do so much"

- Teja:
  - Vectorised and threaded implementation of algorithm
  - Generate plots, report results
  - Create demo
- Swetanjal:
  - Unoptimised implementation of algorithm
  - Project Proposal
  - Presentation slides
- Nishant:
  - Rough implementation of algorithm
  - Testing
  - Documentation