Blockchain E-Voting System Using Face Recognition

Biometric System (AY 2023/24)

SAPIENZA
UNIVERSITÀ DI ROMA

Weidong Cai – 1836167
Elena Jiang – 1846716

Related Work

Biometrics-Generated Private/Public Key Cryptography for a Blockchain-Based E-Voting System

- scan the **fingerprints** of authorised voters and collect the biometric data;
- data is used to generate unique **secret and public keys** for each voter ;
- cryptographic keys are imported into **MetaMask** ;
- interaction with **DApps**, a web 3.0 application;
- voters use these keys to interact with the voting DApp to cast their votes

Proposed System

- an advanced e-voting system that leverages **mobile technology**
- **face recognition** for biometric identification;
- system uses collected facial data to generate a **unique ID**, RFC4122 UUID;
- all the transaction is send by the fund

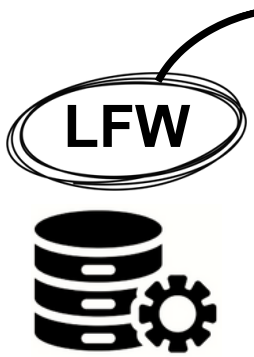
Evaluation Face Recognition

The evaluation of the face recognition system involves an **open set identification** task.

GhostFaceNet: declared score of **99.7%**.

The model was trained on the **MS1MV2 dataset** and it was tested on the **Labeled Faces in the Wild (LFW) dataset**

Enrolled: a person has more than three images and select up to six valid photos.
Not enrolled: a person has three or fewer images.



The **final dataset** is structured as follows:

- Enrolled entities: 100
- Genuine Probes: 437
- Impostors: 100
- Impostor Probes: 115

Performance evaluation

Using an **ALL-against-ALL approach:** comparisons between each probe and all the templates in the gallery

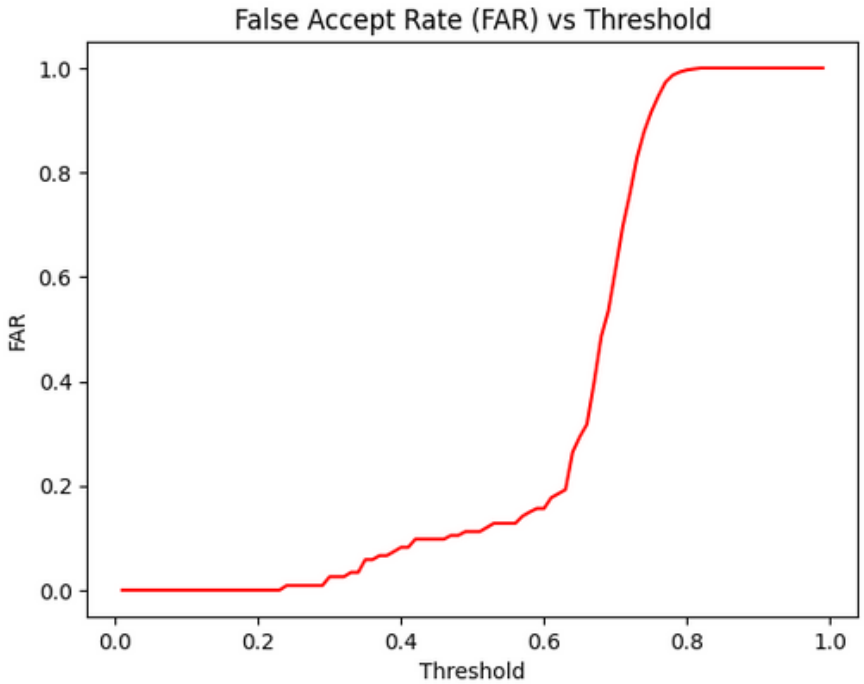
The face recognition was performed using **deepface** with **cosine distance**. (Distance between similar vectors should be low)

Using a threshold range of **0.01 to 0.99**, with a step of 0.01.

For each threshold calculate: DI, FA, GR, FR, DIR, FRR, FAR, GRR

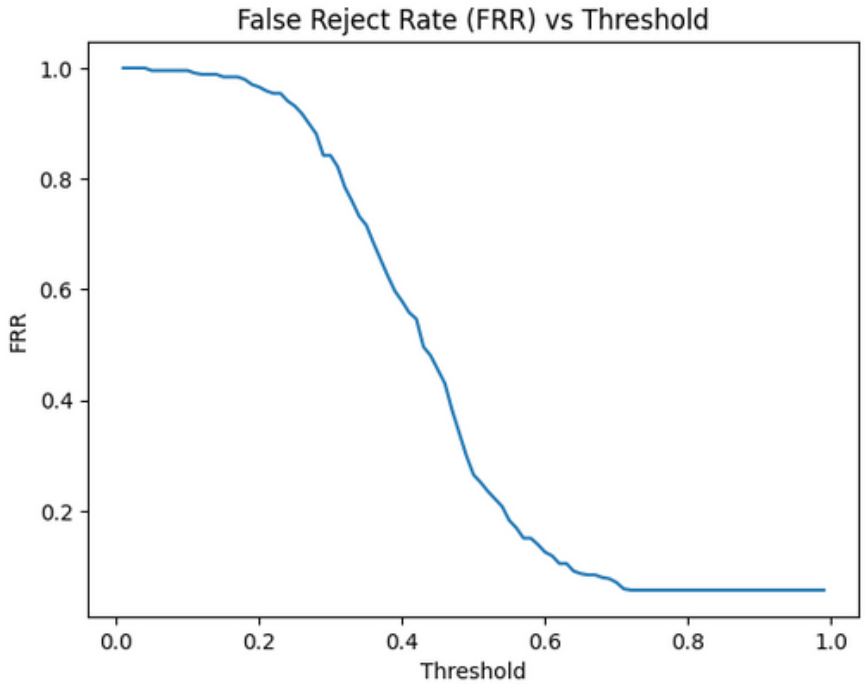
False Accepts Rate

the percentage of recognitions where someone is wrongly recognised (false acceptance)



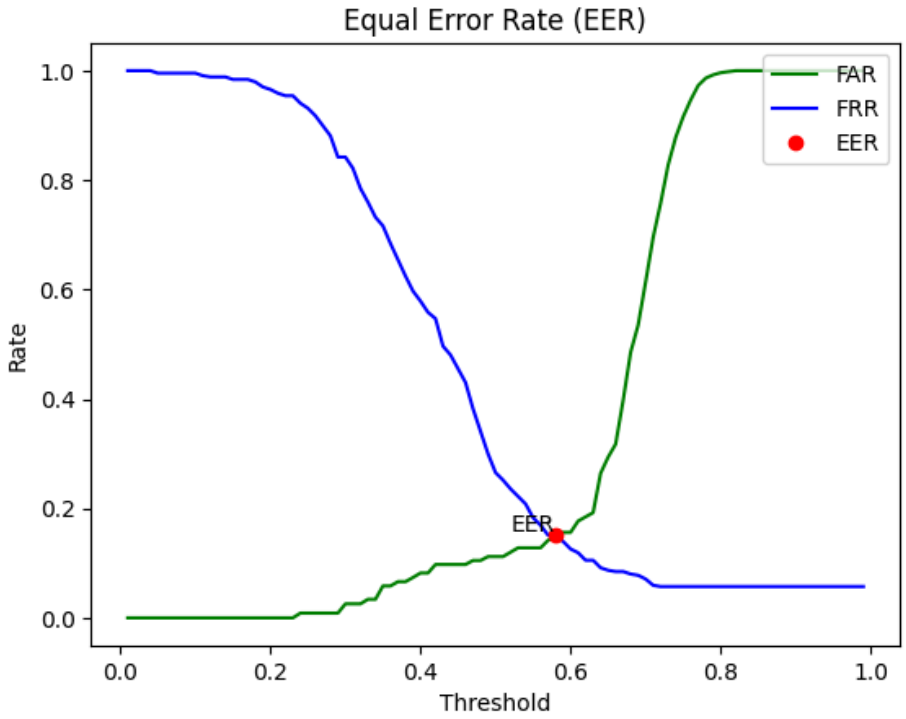
False Reject Rate

the percentage of recognitions where someone is wrongly not recognised (false rejection)



Equal Error Rate

the point at which the FAR and FRR are equal

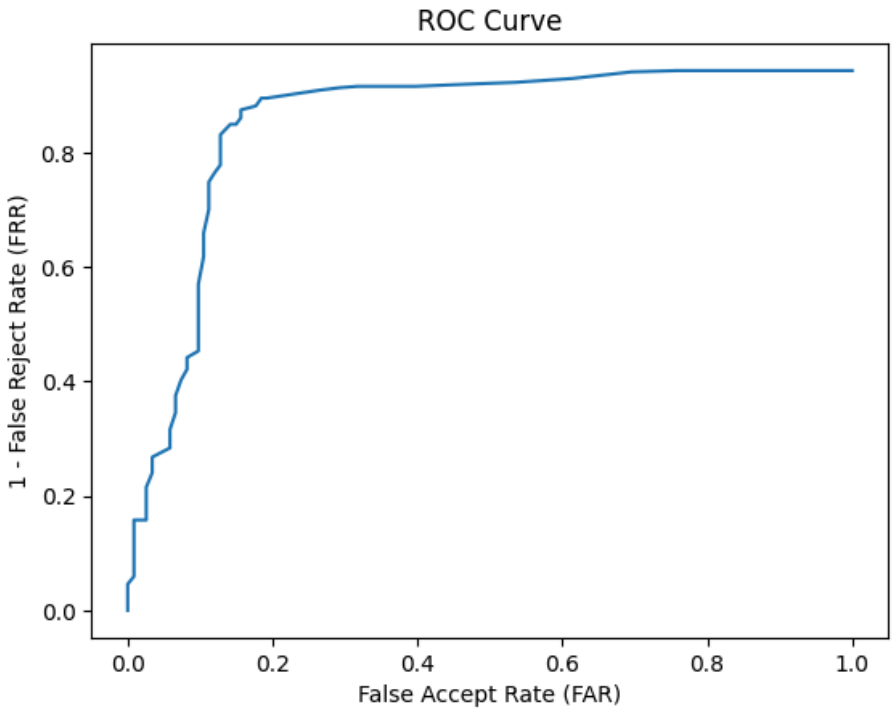


The EER corresponds to a threshold value of approximately 0.58.

Threshold	0.58
Detection Rate (DI)	371
False Acceptance (FA)	19
Genuine Attempts (GR)	108
False Rejection (FR)	58
Detection and Identification Rate (DIR)	0.8489702517162472
False Rejection Rate (FRR)	0.15102974828375282
False Acceptance Rate (FAR)	0.14960629921259844
Genuine Rejection Rate (GRR)	0.8503937007874016

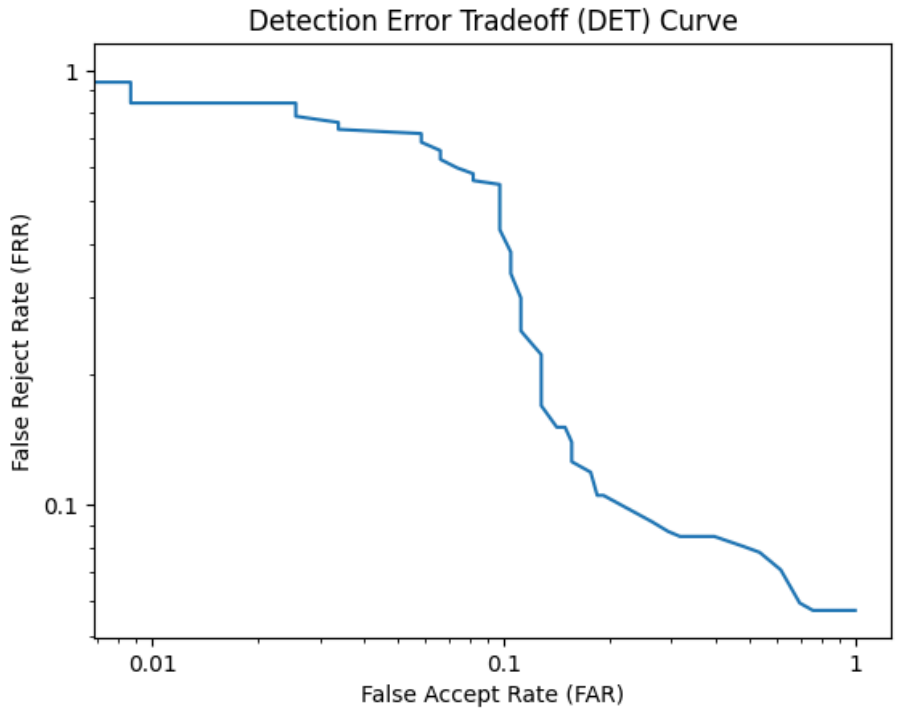
Receiver Operating Characteristic

1 - FRR vs FAR



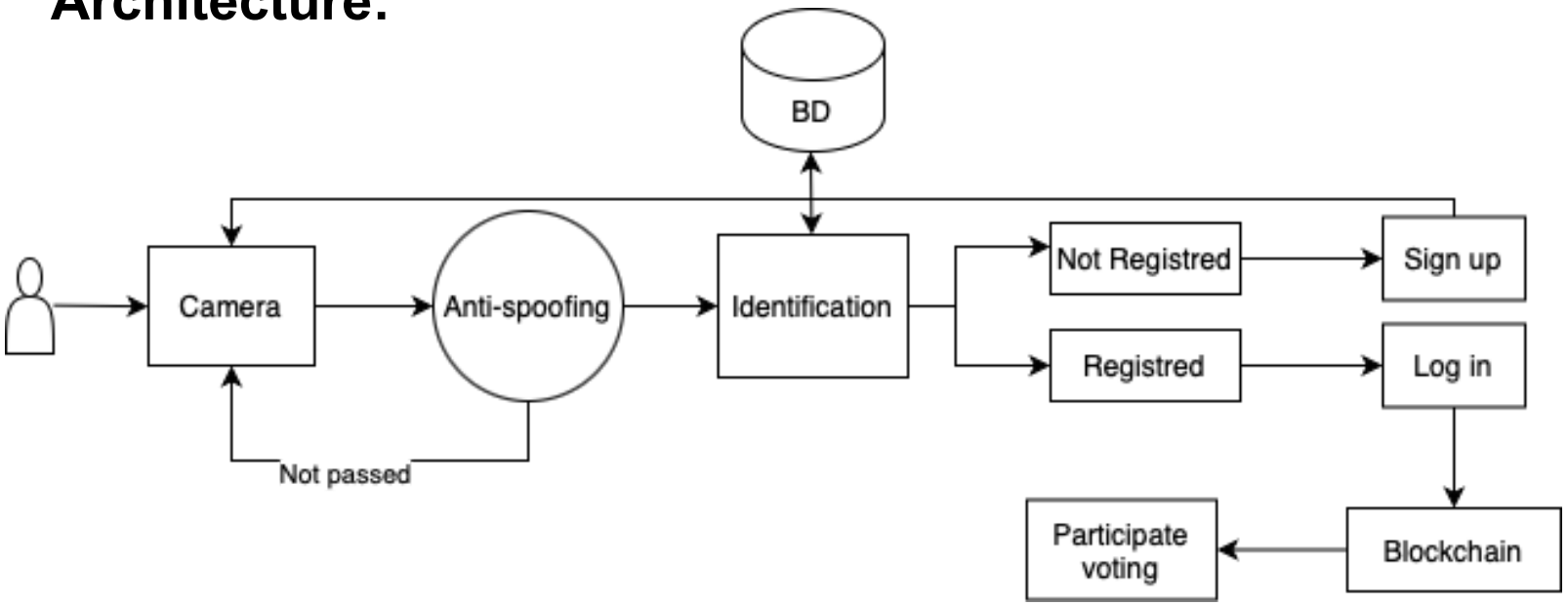
Detection Error Tradeoff

FAR vs FRR in logarithmic form



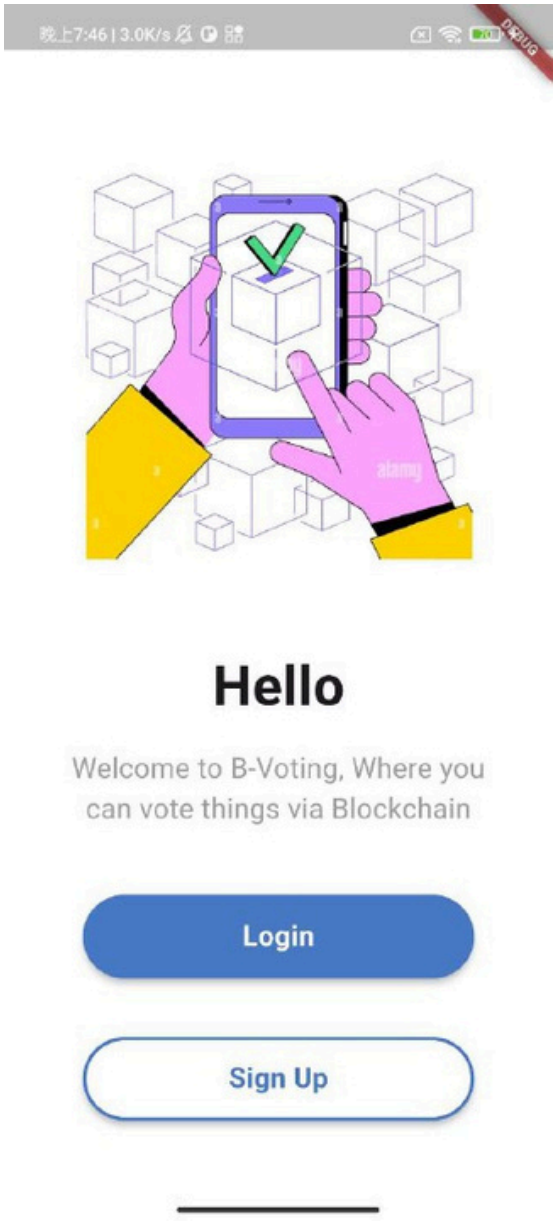
Demo (mobile application)

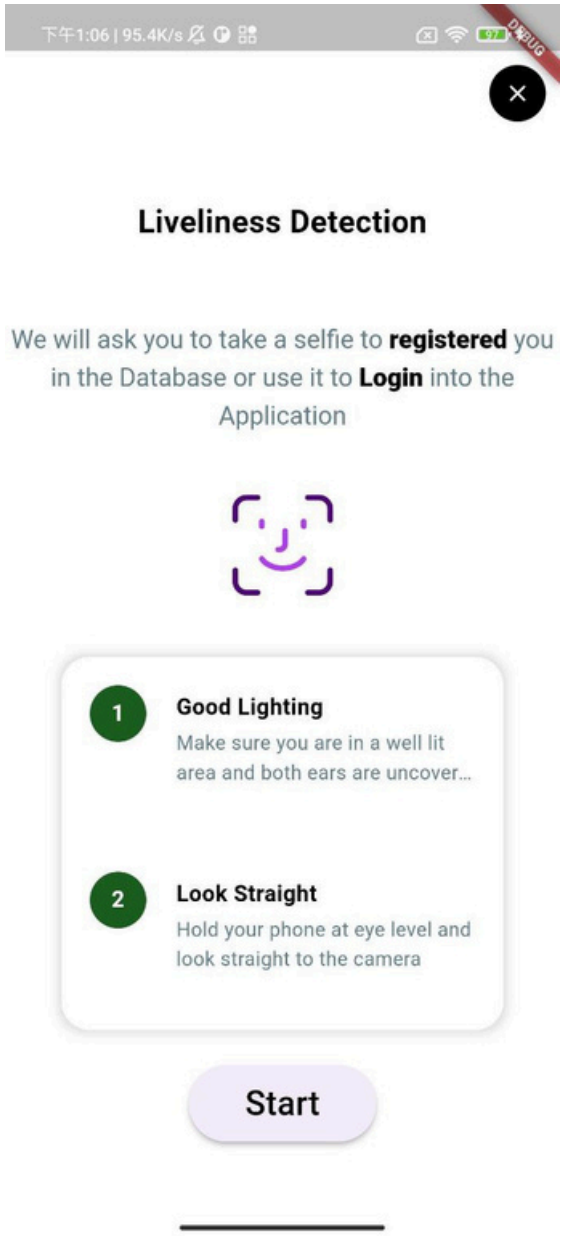
Architecture:



Enabling Technologies:

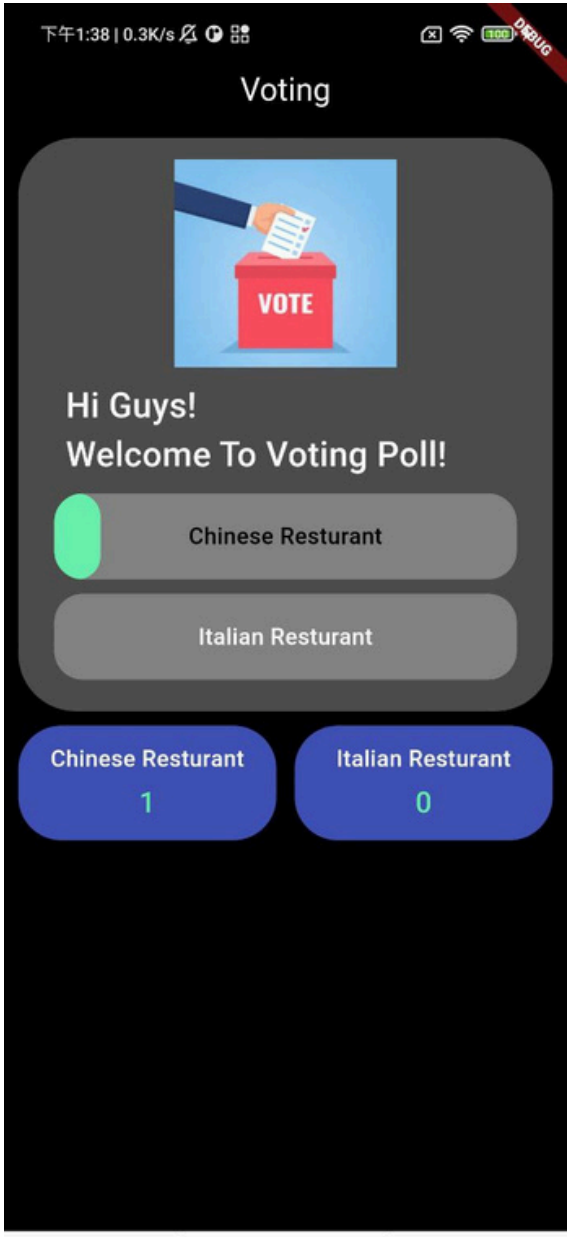
- Flutter
- Solidity
- Sepolia testnet
- Firebase - Firestore Database





Sign up and Login

- **30s time limit** for anti-spoofing checks using **m7_liveliness_detection**
- captured face image of the user will be saved in **base64 format** in the **Firebase** database.
- use **deepface** to check if the user is already registered in db.



Blockchain

- all transactions are sent by the fund based on the ID of voter
- voting process are executed via blockchain
- unique ID is saved in the blockchain
- Smart Contract is deployed on the **Sepolia testnet**
- system utilizes the **web3dart** package
- All transactions within the Vote Protocol are managed by **a single Ethereum account**

THANK YOU

for watching