hackerearth

Makeathon 2023

Idea Submission

TEAM NAME & MEMBER DETAILS

Team Name- Optimizers

Mallika

Apurva Chaudhary

Jyoti Singh

Shivangi Singh

THEME: Facial Recognition for transactions or OTP

PROBLEM STATEMENT

Ecommerce is growing in leaps and bounds in today's time.With increase in the feasibility of online transactions crime and fraudulent activities are also increasing. To aid user authorization and identification, various two-factor authentications such as OTP along with device identification methods are being used. Since passwords and OTPs are vulnerable (Mazar BOT virus in android system [1]), we propose to enhance the security with Facial recognition.

During the transaction, the system will verify the user’s face and enter the OTP. If it matches the transaction will be a success. If the face does not matches, The user needs to use the OTP sent to the device along with transaction password which is well known and set by the user in the bank. Using facial recognition we are not leveraging present available security authentication methods, instead we are adding an extra security method which is more feasible to user.

There are many issues which need to be addressed when using Facial Recognition such as Identity Theft / Fraudulent activities prevention, model accuracy, User Feasibility and Privacy

Facial recognition is susceptible to identity theft as fraudsters can use a photo of the user and fool the system. Moreover all the facial recognition methods involve user image to be added to a dataset for model training. Security breaching attacks by fraudsters can be done on the dataset or collection of user images, to avoid this issue we need to add encryption on the image dataset.Our main aim is to develop a system which takes in consideration all the stated issues and increase the accuracy of facial recognition.

How it Helps to Solve the Problem

- Facial recognition integration with transactions is a tedious task which involves various Security issues

- Using the following approach we are tackling identity theft, ensuring User Privacy & User Feasibility and interoperability

- This Low cost solution does not require any high sensors or high definition camera and can be implemented by smart android devices

- The model used are ensured to give a higher accuracy.In case the model is unable to recognize the image, There is no leverage of existing OTP and Secure password method

Framework/Technology Stacks

- REST API/ WCF framework for formulation of Recognition page
- Encryption/Decryption -> AES/RSA or PCA
- Face Detection using HaarCascade + ADABOOST
- Face Recognition- MobilenetV2
- Database - Shivangi

Impact Metrics

- Accuracy
- Confidence
- F1 Score
- Precision
- Recall
- Time Complexity
- Cost of Implementation

SOLUTION

REST API FACE RECOGNITION

To ensure Interoperability we can build face recognition model using REST API. Base64 encoding is used in Json Response

i)DATASET CREATION & TRAINING MODEL

- **Data Preprocessing -**

The unwanted noise, blur, varying lightening condition, shadowing effects can be remove using pre-processing techniques .once we have fine smooth face image then it will be used for the feature extraction process.

- **Face Detection -Haar Cascade**

Using Haar Cascade Model for Face Detection, This model has a higher accuracy. Images will be stored with an ID assigned

- **Training of images Haar Cascade can be combined with ADA boost (similar to Viola algorithm) to increase speed**

ii) Image Encryption

Image embedding using PCA and RSA/AES. It helps in ensuring image breach during transmission

iii) Anti-spoofing Dataset with liveliness detection

Training Dataset = Real + Spoof images

- Accessing Dataset
- Data Preprocessing
  Libraries -> Numpy, cv2, matplotlib, shutil
- Model Selection
  MobilenetV2 (MobileNetV2 outperforms MobileNetV1 and ShuffleNet (1.5) with comparable model size and computational cost), Activation Function ReLU
- Accuracy Check

Database Creation

- Database is created using PostgreSQL to design a database schema that accommodates the specific needs of banking applications, stores user data in the form of tables and allows binary data storage like image files.
- Once database is set up after importing data, it is used in banking application to store and retrieve user data and image.

- Visual tool is used to interact with database directly or PostgreSQL can be integrated with banking application using API.
- Securing sensitive data in a banking database is crucial for ensuring the privacy and safety of customer's information. Some ways to secure database in banking sector -
- Encryption can help protect sensitive data from unauthorised access using techniques like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) to encrypt data.
- Access controls can be implemented to ensure only authorised users can access sensitive data by implementing role based access control approved by the administration and management.
- Use of firewalls, intrusion detection and prevention systems to prevent unauthorised access in network systems
- Implementing monitoring and auditing for any modification, unauthorised access or deletion of sensitive data.
- Regularly update and patch the database software and OS to ensure any vulnerabilities are addressed.

Facial Recognition

i) Extract the facial features of the user input face and the user stored faces from the database using a deep neural network using MobileNetV2
The features are typically represented as high-dimensional vectors.

ii) After that calculate the cosine similarity between both faces using the following formula:
cosine_similarity = dot_product(user_input_features, user_stored_features) / (norm(user_input_features) * norm(user_stored_features))
where dot_product is the dot product between the user input features and user stored features, and norm is the L2-norm of the feature vector.

iii)The cosine similarity score ranges from -1 to 1, with 1 indicating a perfect match and -1 indicating a complete mismatch.
A similarity score above a certain threshold is considered a match, and the identity of the user stored face corresponding to the highest similarity score is returned as the recognition .

Technology Selection

01	REST API	Ensures interoperability, lightweight
02	Haar Cascade	According to Research Studies of MUCT Dataset, face detection by Haar Cascade is more accurate but slow and takes a lot of training time
03	ADABOOST	To Improve the processing speed of Haar Cascade Adaboost is used to increase the processing speed
04	MobileNetV2	High efficiency CNN due to channeled bottleneck. Much faster on mobile devices
05	LDA analysis using XOR and Pixel Substitution	Strong Encryption and Decryption

METHODOLOGY

- *Register users for availing the facility of transaction by Facial Recognition*

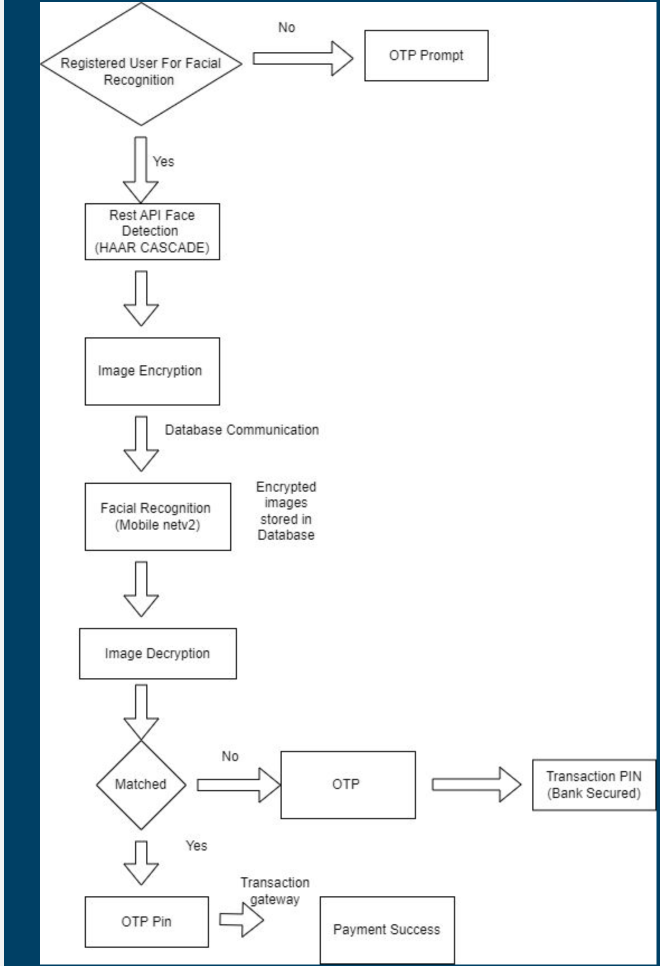
- *During transaction , Users will be provided a Rest API page along with Payment gateway which includes Face detection*

  .

- *The extracted features using Haar Cascade are encrypted and sent to the database for recognition.*

- *If recognition is a success generate OTP and move forward to the payment gateway.*

hackerearth

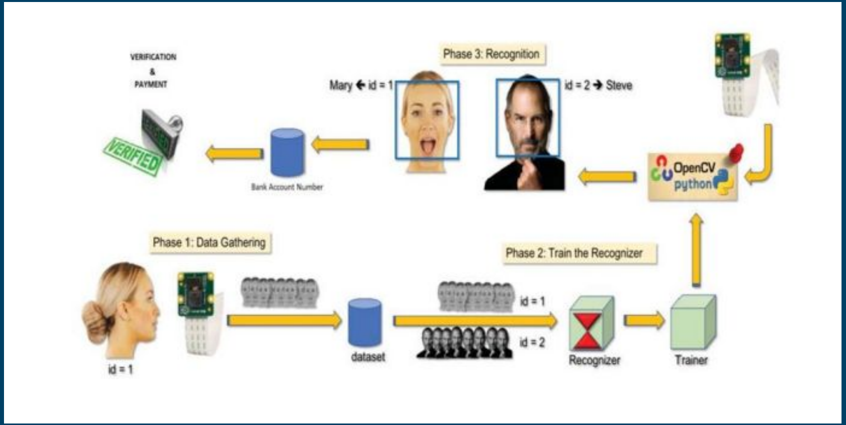

Registered User For Facial Recognition
No
OTP Prompt
Yes
Rest API Face Detection (HAAR CASCADE)
Image Encryption
Database Communication
Facial Recognition (Mobile netv2)
Encrypted images stored in Database
Image Decryption
Matched
No
OTP
Transaction PIN (Bank Secured)
Yes
OTP Pin
Transaction gateway
Payment Success

hackerearth

METHODOLOGY

- *Facial Recognition involves anti-spoof detection and liveness analysis to prevent identity theft.*

  .
- *Encryption Decryption of Images is done to secure Database repository and secure transfer of image using (Pixel Substitution and Scalar automata for Scrambling).*



Ref - *International Journal for Research in Applied Science & Engineering Technology (IJRASET) Online Transaction Security Using Face Recognition: A Review by*
Dr. Ankita Karale , Aman Tiwari , Anay Wadkar , Aditi Patil, Diptesh Waghulde Associate Professor, Department of Computer Engineering, Sandip Institute of Technology and Research Center, Nashik, India

hackerearth

SOCIETAL IMPACT/ NOVELTY

Due to availability of a secure solution it will help in mitigating the fraudulent activities during transaction.

Using Facial recognition will help in improving user feasibility

FUTURE SCOPE

- *Integration of Facial Recognition with Government ids such as Adhar*
- *Tracking history of transactions and detecting Fraudulent activities*
- *Improving Accuracy of the model*

THANK YOU