A SECURE BANKING BY FACE RECOGNITION METHOD

A.Porselvi, M.E, Anusha S, Meena P, Nishitha K

Department of Computer Science & Engineering,

Panimalar Institute of Technology, Chennai, Tamil Nadu, India

---***---

Abstract -*There is associate degree imperative want for rising security in banking region. This project we have a tendency to discusses concerning banking transactions exploitation facial identification. The target of this project is to develop a strong automatic formula for transacting cash in higher level security purpose with high recognition rates in varied setting. The biometric authentication code with banking code is a lot of typical ways. The processed info passes through the info of banks and payment systems. Once facial identity is matched then dealings can finished. Haarcascade based mostly formula has been applied for quick and easy face detection from the input image. The result show that the planned formula has able to train a lot of quantity of information and high accuracy.*

***Key Words*: Authentication, payment, face detection ,high accuracy, security**

1.INTRODUCTION

Machine learning (ML) is that the scientific study of algorithms and math models that computer systems use to perform a selected task whereas not victimization specific directions, hoping on patterns and inference instead. It's seen as a group of engineering science. Machine learning algorithms build mathematical model supported sample data, known as "training data", to make predictions or decisions whereas not being expressly programmed to perform the task. In net, there square measure many chances of intruders' gaining contraband access. Machine learning algorithms square measure utilized in a good sort of applications, like email filtering and laptop vision, wherever it's troublesome or unfeasible to develop a traditional algorithmic rule for effectively performing arts the task.

Over the last decade, we've seen a rise within the use of technology in several business sectors to alter and higher interact customers. This can be very true within the banking and finance sector. Since the beginning of the digital revolution face recognition has been gaining prominence over bit and kind based mostly interactions thanks to the convenience it offers while not compromising on the protection of transactions. Despite a rise within the use of EMV cards (Europe, MasterCard, Visa) including watchword creation policies, there has been a surge in banking fraud cases. As a results of the billions that square measure lost by major banking establishments, there has been a decision to modify to biometric face recognition to curb this issue. It implies that banking software package can deem face scans that it then compares with similar ones that were uploaded by the bank's personnel into their system therefore on verify the customer's identity. The aim is to evidence the identity and solely enable a dealings to travel through if the account owner's identity is completely known. This client ID authentication method is thought as KYC (Know Your Customer).

We add machine learning algorithms to observe the facial identification. We can use machine learning technology, opencv,sqllite info and neural network algorithmic rule .

2.RELATED WORK:

2.1. The face key recognition technology performs the following tasks:

Locates a moving object at intervals the camera browse

- Determines if the moving object is face
- Compares live faces with samples from the info
- Face recognition technology can work with every low-resolution USB
- Cameras and low or high-resolution CCTV cameras

2.2Biometric Authentication process involves:

The matching of the extracted feature with the sample feature already holds on in information. once the user provides a sample of the same nature i.e., face scan, etc. with its PIN in the ATM system, then the system sends grid points of the user's face to information as a rule of numbers through a network to the server. On the server aspect, the user's current sample is matched when decipherment and compared with the one hold on in information. As soon as, the sampled pictures match the present image, the user is allowed to proceed additional as associate degree genuine user for dealing, deposit, transfer, etc., else user is taken into account as an invalid user, and session is terminated.

2.3.Surface Texture Analysis:

The most superior method is Surface Texture Analysis (STA). STA does not examine the entire face but a patch of membrane on it. This patch is divided into separate blocks. The skin surface, the pore on the skin, and other face characteristics are converted to a code. This code is used for comparison.

2.4. Eigen faces for Recognition:

- By considering theory, relevant information in an exceedingly} very face footage unit of measurement extracted and compare one face writing with an information of models.
- Find the principal components of the distribution of faces, or the eigenvectors of the variance matrix of the set of face footage. A simple approach to extract the data contained in an exceedingly} image of a face is to somehow capture the variation in an exceedingly very assortment of face footage, freelance of any judgment of choices, and use this information to jot down in code and compare individual face footage.
- The number of potential Manfred Eigen faces is adequate the quantity of face pictures within the coaching set.
- However we will conjointly represent the faces by approximating these by the simplest Eigenfaces having largest Eigen-values that successively account for the foremost variance inside the set of face pictures. This will increase the procedure potency**.**
- (i) Initialization: The training set of face images is acquired and Eigen faces are calculated which define the face space;
  (ii)When a new face is encountered, a set of weights based on input image and Eigen faces is calculated by projecting the input image onto each of the Eigen faces;
  (iii)The image is determined to be face or not by checking if it is sufficiently close to face Space; and
  (iv)If it is a face, the weight patterns are classified as either a known person or an unknown one.

2.5.DBN(deep belief network)

DBN learning is to estimate hidden and visual weights in very given coaching information. At the start, an associate initial estimate of the parameters is calculated mistreatment associate unsupervised bottom-up learning strategy.

2.6 Steganography :

Text-Based Steganography: It makes use of options of English language like grammatical relation, fastened ordination and use of periphrases for activity information instead of mistreatment properties of an announcement .

BPCS Steganography: the data activity capability of a real color image is around five hundredth . A sharpening operation on the dummy image will increase the embedding capability quite an bit. organisation of the key information by a compression operation makes the embedded information additional intangible. The steganography program for every user is straightforward. It more protects against eavesdropping on the embedded data. it's most secured technique and provides high security.

2.7Image segmentation:

The planned work is employed as a building block by a additional advanced image process systems such localization of craniofacial landmarks of the lateral bone X-ray image for image segmentation. mistreatment the live of fuzzy entropy we'll outline 3 linguistic variables specifically black, grey and white sculptures by 3 fuzzy subsets B, G and W severally **.**

2.8 IRIS AND FINGERPRINT DETECTION :We have existing application to spot the ID of associate object exploitation barcode and QR code. For additional security purpose it's additional vital to spot objects exploitation bio-metrics which has Fingerprint recognition, Iris recognition and Face detection modules. once it involves security problems fingerprints are often manipulated by exploitation colloid and alternative means that. however it's tedious to steal iris recognition of someone. This application is specifically created for parcel or messenger services so as to avoid deliver. It are often majorly enforced in extremely confidential areas like military, government functions so on. we tend to ar attending to implement of these modules in a very single application and thence it used as utile machine mobile app exploitation biometry.

3. IMPLEMENTATION WORK:

Facial Recognition code incorporates a bodily property detection that stops hackers from using a image of the consumer for impersonation functions. the popularity system conjointly permits customers to access their bank accounts from computers. we tend to use face of user for the dealing and authentication, that the would like of OTP isn't needed. the advance in information sources, combined with new analytical capabilities supported machine learning models, permits United States of America to provide every client customized service. With reduced uncertainty due to a additional correct risk assessment supported a wider client digital footprint. this method uses real time face detection it reduces the danger of obtaining hacked by unauthorized folks over the web. we've used our face as AN authentication key therefore there's no would like of Arcanum problems here . It reduces the danger of obtaining misused once user registers mobile is lost.

Facial recognition is one in every of various ways in which banks will decrease friction in their customers' expertise and increase potency and accessibility. Haar Cascade primarily based formula has been applied for fast and straightforward face detection from the input image. The face image is then being regenerate into gray scale image. Haar options will simply be scaled by increasing or the scale of component cluster being examined. this permits options to discover options on specific gestures. The variances of contrasts between the component teams square measure accustomed confirm relative lightweight & dark areas .

After that, the iris candidates square measure extracted from the intensity valleys from the detected face. costs of each iris candidates square measure calculated. Finally the iris candidates square measure paired up and so the worth of each possible pairing is computed by a mixture of mathematical models.

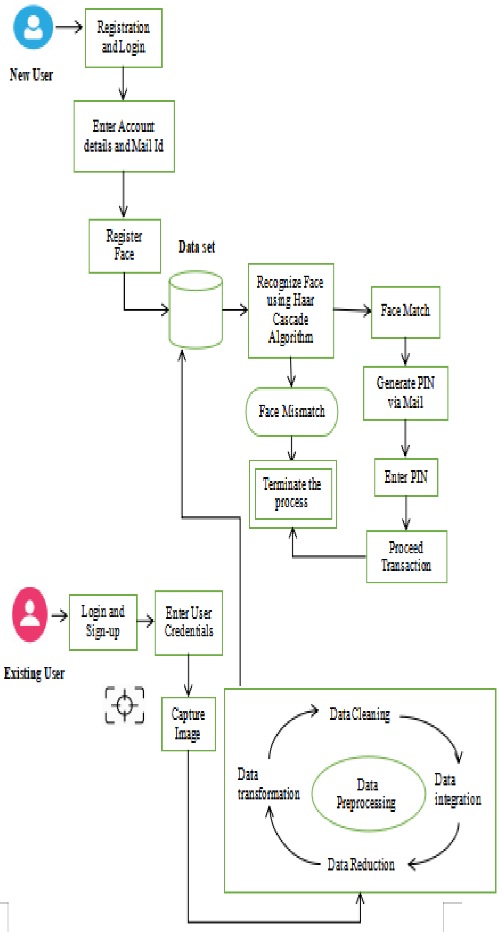

Fig 1. Flow of diagram. [2]

4. MODULES:

4.1. Registration:

In this module new user should register their face to get account number. For that they need to fill their personal details like Username, Password and Mail ID.

4.2. Face Detection:

Face detection may be a great tool which will be utilized in completely different fields like security and human resources. OpenCV provides the Haar Feature-based Cascade Classifiers for face detection. This technique apply series of classifiers to each sub window of input image, the primary one classifier eliminates an outsized range of non-faces examples with little process. The opposite classifiers eliminate extra negatives however need extra computation. Once many stages of process the amount of sub-windows has been reduced radically. Filters square measure accustomed thirty eight extract options from image, and people filters became a lot of and a lot of complicated in every stage from one to n

4.3. Face Recognition:

Identity verification could be a manner of recognizing a personality's face through technology. An identity verification system uses countenance from a photograph or video. It compares the data with a dataset of known faces to search out a match.

4.4Steps Involved

1. An image of your face is captured from a photograph or video. Your face would possibly seem alone or during a crowd. Your image might show you trying straight ahead or nearly in profile.

2. Identity verification software package reads the pure mathematics of your face. Key factors embrace the gap between your eyes and also the distance from forehead to chin.

3. Your facial signature — a mathematical formula — is compared to a dataset of renowned faces.

4. A determination is created. Your face print might match that of a picture during an identity verification system dataset.

4.4. Pin Generation:

In this module pin will be generated face security purpose. Initially we will set our pin we can transact amount through pin or face. If the pin matches transaction will be done.

4.5. Transaction:

In this module transaction will be done user need to enter their details like from account, to account, Amount then face recognition will be done if the face matched then it will be authorized user or transaction will not be done.

5. HARDWARE REQUIREMENTS:

Processor : Pentium iv

RAM : 8 GB

Processor : 2.4 GHZ

Main memory : 8GB RAM

Processing speed : 600 MHZ

Hard disk drive : 1TB

Keyboard :104 keys

6. SOFTWARE REQUIREMENTS:

IDE: Anaconda navigator

Front end: Python.

Operating system :Windows 10

Dataset: Image

Library's : numpy, pandas, openCV

7. CONCLUSION

In this paper main focus is safety our cash and our dealings. Victimization biometric authentication implies that the banking client has only 1 face which may permit them access to all or any their bank accounts. Haar cascade-based algorithmic rule has been applied for quick and straightforward face detection from the input image. Face Detection module analyses every captured frame and extracts valid faces from every frame.

Face Identification deals with face recognition and verification of the detected face. As a result of the technology grows day nowadays, there's a unit innumerable changes happening throughout the complete system and considerably security for each component is crucial.

8. FUTURE WORK:

Face Identification deals with face recognition and verification of the detected face. In Future any fraudulent access by the fake user is eliminated with the help of radio frequency identification card

REFERENCES:

[1] DeepaMalviya, “Face Recognition Technique: Enhanced Safety Approach for ATM”,International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.

[2] Ramapriyadharshini M1 , Sakthi Bala K.S2 ,Subalakshmi J3 , Mr Anand Joseph Daniel D4” Bank transaction using facial identification” IJARIIE-ISSN(O)-2395-4396 Vol-6 Issue-2 2020.

[3] Aru, OkerekeEze, IhekweabaGozie,”Facial Verification Technology for Use In Atm Transactions”,Volume-02, Issue-05, pp-188-193.

[4]FatemaA.Albalooshi,MaxSmithCreasey”,Face Recognition System For Secured Mobile Banking”,Conference Paper Scientific and Research Publication,oct-2018.

[5]SudarshanDumbre,ShamitaKulkarni,DevashreeDeshpande,Prof P.V.Mulmule”,Face Detection and Recognition for Bank Transaction”,Journal of Emerging Technologies and Innovative Reseach(JETIR),Volume-3,Issue 5,May 2016.

[6]OlutolaFagbolu,OlumideAdewaleBonifaceAleseandOsuolaleFestus”,Secured Banking Transaction with Face Based Automation Teller Machine”,IJISET - International Journal of Innovative Science,Engineering& Technology, Vol. 1 Issue 10, December 2014 .

[7]MohsinKarovaliya,SaifalKarediab,SharadOzac, Dr.D.R.Kalbanded “Enhanced security for ATM machine with OTP and Facial recognition features”MohsinKarovaliya et al. / Procedia Computer Science 45 (2015) 390 – 396.

[8]Janani.S.R,Sivaparthiban.C.B,LekhaT.R“Secured Credit Card Transactions Using Webcam"(IJEAT),eISSN:0056,P:2395-0072,Volume-3,Issue-4,April2016.

[9]TisonVarghese,vidyaNambiar,PushkarDandekar “Authentication Of Credit Card Using Facial Recognition “International Journal of Latest Technology in Engineering, Management & Applied Science(IJLTEMAS) Volume 7,Issue 6,April 2018,ISSN 2278-2540.

[10]P. Muniasamy , S. JoneyBabayal,”Securing ATM by Facial Recognition Authentication”,International Journal of Scientific Engineering and Research (IJSER),Volume 5 Issue 7, July 2017.

[11] Mrs.D.MURUGESWARI, KN.SANGEETHA , M.SRIVANI” Secure e-pay using text based steganos and visual cryptography” International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015 .

[12]S. Raja , S. Sankar, S. Saravanakumar and M. Padmarasan” Simulation and Mathematical Modeling of Image Segmentation” Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 6 November 2013

[13] P. Sheelarani , K.Anushree, N.Gayathri , S.Saranya ”Multipurpose machine learning mobile application using biometrics” International Journal of Pure and Applied Mathematics Volume 118 No. 20 2018, 4267-4272