ONLINE BANKING USING TWO – FACTOR AUTHENTICATION

P. Selvi Grija, Balakrishnan Nandhini Devi, Jeevitha.D, Seethalakshmi.R

Abstract- Internet is progressively employed by banks as a channel for receiving delivering their product and services to their customers. However, it continues to gift challenges to the monetary security and private privacy. Security problems like phishing, spywares, faux emails purporting to be send from bank, use worm programs (key Loggers) to capture user IDs and passwords. Therefore we offer a solution that focuses on the person's distinctive physical attribute noted as Biometrics- facial feature recognition using Eigenface. It's a biometric technology which will be applied to the assorted fields in terms of human identity. This experiment of face recognition system uses fifty facial images as test images. Test images and training images are taken directly with the camera with a distance of face shooting is sixty cm.

Keywords- *Phishing, Spyware, Face Recognition, Eigen face, Threshold, Face Detection.*

I. INTRODUCTION

Banks have historically been within the forefront of harnessing technology to boost their merchandise, services and potency. They have, over an extended time, been exploitation electronic and telecommunication networks for delivering a good vary important extra merchandise and services. The delivery channels embrace direct dial – up connections, non-public networks, public networks etc. and therefore the devices embrace telephone, Personal Computers together with the machine Machines, etc. With the recognition of PCs, easy accessibility to World Wide net (WWW), is progressively utilized by banks as a channel for receiving directions and delivering their merchandise and services to their customers. This way of banking is mostly know as net banking, though they vary in merchandise and services offered by completely different banks vary wide each in their content and class. One in all the largest attractions of net as Associate in nursing electronic medium is its openness and freedom. It's a property right and there's no restriction on who will use it as long collectively adheres to its technical parameters. This has additionally given rise to considerations over the safety of information and knowledge transfer and privacy. These considerations are common to any network together with closed user cluster networks. However over the web, the scale of risk are larger whereas the management measures are comparatively fewer.

Humans acknowledge one another consistent with their numerous characteristics for ages.

Identity verification (authentication) in PC has been historically supported one thing that one has (key, magnetic or chip card) or one is aware of (PIN, password). Things like keys or cards, however, tend to induce taken or lost and passwords are typically forgotten. To attain a lot of reliable verification or identification we must always use one thing that basically characterizes the given person. Statistics provide machinedriven strategies of identity verification or identification on the principle of measurable physiological or behavioral characteristics.

Biometric systems will be employed in two completely different modes. Identity verification happens once the user claims to be already registered within the system (presents an ID card or login name); during this case the verification biometric information obtained from the user is compared to the user's information already keep within the information. Identification (also known as search) identification happens once the identity of the user could be a priori unknown.

During this case the user's biometric information is matched against all the records within the information because the user will be anyplace within the info or he/she truly doesn't have to be there in any respect. Before the user will be with success verified or identified by the system, he/she should be registered with the biometric system. User's biometric information is captured, processed and stored.

Eigen face recognition approaches can be classified in an appearance-based method, because the eigenface face recognition use information from the raw pixel image which is used for training and classification of image identity. The idea of this method is projecting an image of a face that can be seen as a vector. To produce the eigenface, the digital image of human faces take at the same lighting conditions, then normalized into a grayscale image. The image is processed in the same resolution and then used as the vector dimension where the components are derived from the pixel value of the image.

Basically human face recognition procedure consists of two stages. The first stage is where the face detection process takes place very rapidly in humans except in certain circumstances where the object is located at a far distance. The second stage is recognition stage which is recognizing the face as individuals face. To solve a spread of issues, face recognition ought to be applied within the sensible and versatile devices.

II. RELATED WORK

Video-To-Video Face Authentication System Robust to Pose Variations

High-quality still-to-still (image-to-image) face authentication has shown success under controlled conditions in many safety applications. They propose a video-to-video face authentication system that is robust to pose variations by making use of synthesized frontal face appearance that contains both texture and shape information. To obtain the appearance, we first reconstruct 3D face shape from face feature points detected from the video using active shape model (ASM). Conventional ASM algorithms cannot handle large pose variations and fast head movement exhibited in video sequences. To address these problems, they present a novel prediction-assisted approach that is capable of providing an accurate shape initiation as well as automatically switching on multi-view models for ASM. Then we can generate frontal shape mesh from the reconstructed 3D face shape. Based on the mesh, we synthesize frontal face appearance with the ASM-detected faces in video. For authentication they proposed 2-directional 2-dimensional client specific fisher's linear discriminant algorithm. The proposed algorithm is a variant of fisher's linear discriminant (FLD) and directly computes eigenvectors of image scatter matrices in row and column direction without matrix-to-vector conversion.

Smart Application for AMS Using Face Recognition

Attendance Management System (AMS) can be made into smarter way by using face recognition technique, where we use a CCTV camera to be fixed at the entry point of a classroom, which automatically captures the image of the person and checks the observed image with the face database using android enhanced smart phone. It is typically used for two purposes. Firstly, marking attendance for student by comparing the face images produced recently and secondly, recognition of human who are strange to the environment i.e. an unauthorized person. For verification of image, a newly emerging trend 3D Face Recognition is used which claims to provide more accuracy in matching the image databases and has an ability to recognize a subject at different view angles. [8]

Person authentication from neural activity of face- specific visual self- representation

They propose a new biometric system based on the neurophysiological features of face-specific visual self-representation in a human brain, which can be measured by ElectroEncephaloGraphy (EEG). They devise a novel stimulus presentation paradigm, using self-face and non-self-face images as stimuli for a person authentication system that can validate a person's identity by comparing the observed trait with those stored in the database (one-to-one matching). Unlike previous methods that considered the brain activities of the resting state, motor imagery, or visual evoked potentials, there are evidences that the proposed paradigm generates unique subject-specific brain-wave patterns in response to self- and non-self-face images from psychology and neurophysiology studies. They also devise a method for adaptive selection of EEG channels and time intervals for each subject in a discriminative manner. This makes the system immune to forgery since the selected EEG channels and time intervals for a client may not be consistent with those of imposters in terms of the latency and amplitude of the brain-waves.

There are various technical issues in online banking which may affect the user data and password. [4] The concept of biometrics is also used in various android phones, to prevent an intruder from stealing their secret passwords or information.[7]

III. EXISTING WORK

In the existing system we have a tendency of using keyboard and key pads to type the pin number or passwords. These can be easily hacked by software called key-loggers which are installed in user PC without their knowledge. Also through session time, IP address, the account can be hacked. By using numeric or alpha numeric password, if it revels to third party it can be misused.

The security attacks which take place in client side are phishing and Trojan attacks, at network the attacks may include DNS spoofing, network interception, and at bank side web application attack, server attacks are possible. The attack at bank can be detected using session hijacking attacks or transaction verification/user profiling. For networks attacks we can use second channel or secured channel mechanism which is used for sending verification using other channel such as SMS and enters data on an external device which contains a secret key and cannot be controlled by Trojans. For client side security we can use virtual operating system on host system, bootable CD-ROM/USB stick, read information from screen and decrypt on external devices etc.

Disadvantages in existing system

- Password may easily reveled to third party.
- Hacking possible using key loggers.
- IP address the account can also be hacked using online banking facilities.

IV. PROPOSED WORK

To achieve more reliable verification or identification in online banking we should use something that really characterizes the given person. Hence the proposed system uses the concept of Biometrics through which the user can be identified unique and cannot be hacked by the hackers. So we proposed the Eigen face recognition technique.

Eigen face recognition approaches can be classified in an appearance-based method, because the eigenface face recognition use information from the raw pixel image which is used for training and classification of image identity. The idea of this method is projecting an image of a face that can be seen as a vector. To produce the eigenface, the digital image of human faces take at the same lighting conditions, then normalized into a grayscale image.

The image is processed in the same resolution and then used as the vector dimension where the components are derived from the pixel value of the image. Basically human face recognition procedure consists of two stages. The first stage is where the face detection process takes place very rapidly in humans except in certain circumstances where the object is located at a far distance. The second stage is recognition stage which is recognizing the face as individuals face.

Advantages in the proposed system

- Unique identity.
- Complex in hacking.
- Highly secured form to use online services.

SYSTEM ARCHITECTURE

A system that adopts our face authentication system Fig. 1 consists of following parts: acquisition, a database, and a matching routine.

Acquisition: When a user wants to be authenticated in a system that adopts our scheme, he/she offers his/her face image and their enrollment details. The acquisition routine consists of an optical device for obtaining the user's facial image and a key pad for the enrollment details.

Database: Stores the enrollment details along with the user template which is send to the matching process for authentication.

Matching: here the user input face is compared with probe image that is the image stored in the database. Comparison of the templates is done by eigenface process.

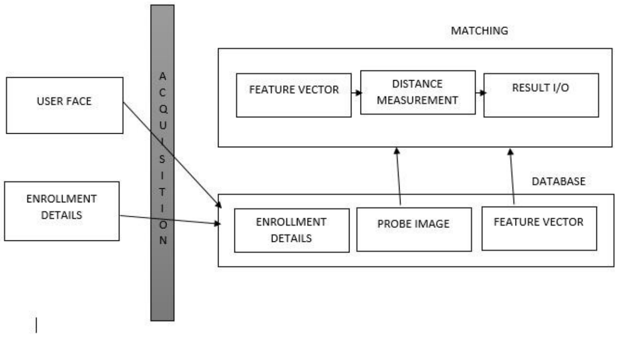

Fig: 1 Face-Authentication system

The flow diagram of our system Fig. 2, depicts the enrollment and authentication process. In the enrollment process the user face along with other enrollment details are acquired from user and stored in the database. In the authentication process again the user face is acquired from user is compared with the probe image (user face which is already stored in the database) using eigenface methodology. After computing, the distances between the feature vector and all the stored feature vectors are compared. The matching routine returns 1 when the distances are lower than a certain threshold value. Otherwise, the matching routine returns 0.

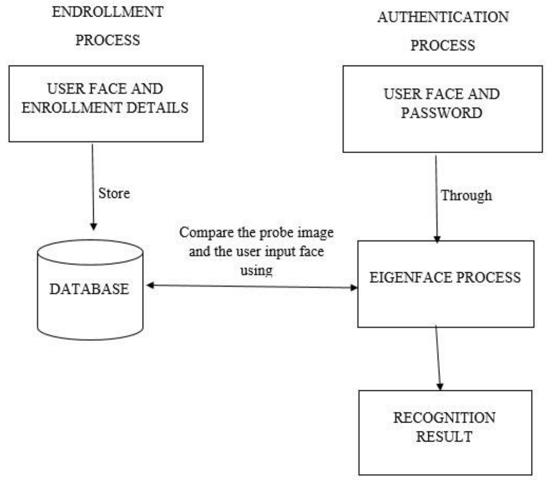

Fig: 2 Flow diagram

ALGORITHM

PCA (Principal Component Analysis)

PCA algorithm is a statistical procedure that convert a set of M face images into a set of K uncorrelated variables called Eigen faces (K< M). Eigenfaces is that the name given to a group of eigenvectors once they are employed in the pc vision drawback of face recognition. The eigenvectors are derived from the covariance matrix of the probability distribution over the high-dimensional vector space of face images. The Eigenfaces themselves form a basis set of all images used to construct the covariance matrix. This produces dimension reduction by permitting the smaller set of basis images to represent the original training images. Classification may be achieved by comparing how faces are pictured by the basis set.

Steps involved in algorithm are as follows,

- Convert image of training set into image of vectors.
- Calculate the average face vector.
- Subtract average face vector from each vector.
- Project the normalized face onto the Eigen space.
- Calculate weight vector of input image.
- Calculate Distance between input weight vector and all the weight vector of training set.
- Is Distance €> threshold-face recognized.

MODULE DESCRIPTION

Enrollment Module

Initially user obtain the webpage through internet. Then the request is forwarded to the bank server. The bank server reply with the authorization web page. The user will upload their facial image and a password. These details are forwarded to bank server and stored in their database.

Bio-Information/ database Module

In this module the user bio-information is stored in the database. Later it is compared with the image in the database for authentication process.

Face-Authentication Module

The user give their authorized details such as new facial image and password. These details are forwarded to bank server. Then face image present in the database (probe image) is matched with the user input image using Eigenface Process. If the match is successful then the user is an authenticated user and can be allowed to access the bank account.

V. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

For secure face authentication scheme, we introduce a two-factor face authentication scheme. It is clear that our scheme works with any linear projection scheme. Its performance is with PCA and we expect that our scheme can be applied to many non-future systems. For face authentication with high security, the effectiveness of external information is sufficient. Therefore our scheme is more suitable for secure face authentication system than for face recognition system.

FUTURE ENHANCEMENT

A possible future application for facial recognition system lies in retailing. A retail store may have cash registers equipped with cameras. Cameras would be aimed at face of the customer so pictures of customer could be obtained. Passport and visa can also be done using facial recognition technology in order to prevent the fraud of ATM in the country. Duplicate voters are being reported at the time of voting, the resolution camera and face recognition equipped of voting site will accept our subject face 100%

and generate the recognition for voting if match is found. To verify terrorists in airport railway station, malls the face recognition may be the future best choice.

ACKNOWLEDGEMENT

One of us would like to thank the Department of Computer Science and Engineering, Christ College of Engineering and Technology, Puducherry

REFERENCES

[1] Payam Hanafizadeh'Byron W. Keating'Hamid Reza Khedmatgozar "A systematic review of Internet banking adoption".

[2] Biggio, B. Dept. of Electr. & Electron. Eng., Univ. of Cagliari, Cagliari, Italy "Security evaluation of biometric authentication systems under real spoofing attacks"

[3] Tassabehji, R. ; Sch. of Manage., Univ. of Bradford, Bradford, UK ; Kamala, M.A "Improving E-Banking Security with Biometrics: Modelling User Attitudes and Acceptance"

[4] Normalini, M.K.a*, T. Ramayah b abSchool of Management, University Sains Malaysia, 11700 Minden, Penang, Malaysia "Biometrics Technologies Implementation in Internet Banking Reduce Security Issues?"

[5] Authentication systems for Secure networks – Rolf Oppliger, Artech House, 1996

[6] Rana Tassabehji, Mumtaz A.Kamala , University of Bradford school of Management,UK "Evaluating biometrics for online banking"

[7] Oka Sudana, A. A. K., 2 Darma Putra, I K. G., 3alan Arismandika Department of Information Technology, Udayana University, Indonesia "Face Recognition on android phones using Eigenfaces".

[8] MuthuKalyani.K, VeeraMuthu.A, M-Tech Information Technology, Sathyabama University, Chennai. Professor, M-Tech IT, Sathyabama University, Chennai "Smart Application For Ams Using Face Recognition".

[9] Abhishek Singh, Saurabh Kumar, Department of Computer Science and Engineering National Institute of Technology Rourkela Rourkela – 769008, India "Face Recognition Using PCA and Eigen Face Approach"

Selvi Grija. P, working as an Assistant professor in Christ College of Engineering and Technology, Puducherry, India

Balakrishnan Nandhini Devi, Perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

Jeevitha.D, perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

Seethalakshmi.R perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India