A Snapshot Model for Web Based Surveillance System

Yuvraj Saini, N. C. Bajia, Abhinandan Jain

Department of Electronics & Communication,
Pratap University, Jaipur

Abstract: **Today's world is computerized world. The cybercrime is also on an increase the web of www is increased day by day. So protection of software is the important part. In existing system, email account can be accessed by providing username and password. Disadvantage of existing system is username is known to everyone and password can be guessed. It is a tedious job to remember password of each account as user has many accounts like on Gmail, yahoo, social networking sites etc. Proposed system will overcome all these disadvantages. Aim of proposed system is to implement a 2D face recognition technique using image processing and design a SMTP/POP3. Email client application that will use the face recognition module for validation and authentication of user. A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. This kind of email application ensures that a person is who they claim to be, eliminating any worry of someone using illicitly obtained keys or access cards.**

***Keywords – Detection, Image processing, Spontaneous facial expression, Principal Component Analysis (PCA), facial recognition system, 2D face recognition, POP3*.**

I. INTRODUCTION

Electronic mail (e-mail) is one of the most popular network services nowadays. Most e- mail systems that send mail over the Internet use simple mail transfer protocol (SMTP) to send messages from one server to another. The messages can then be retrieved with an e-mail client using either post office protocol (POP) or Internet message access protocol (IMAP). SMTP is used as the common mechanism for transporting electronic mail among different hosts within the transmission control protocol/Internet protocol (TCP/IP) suite. It is an application layer protocol. Under SMTP, a client SMTP process opens a TCP connection to a server SMTP process on a remote host and attempts to send mail across the connection. A face recognition system is a computer application for automatically identifying and verifying a person from a digital image/picture or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. Face recognition is an active field of research and has increased significantly since the early 1990s. Our aim is to study different face recognition techniques and implement a 2D face recognition technique using image processing and design a SMTP/POP3. E Mail client application will use the face recognition module for validation and authentication of user. The application will allow the user to send/receive emails like ordinary email client but instead of asking the user to specify the user name and password the face recognition module must do the authentication.

There are many systems based on face recognition but there is no previous system which is using face recognition for email access. When an e-mail is sent from the sender to receiver, in most cases this involves, the sender machine sends the email to local SMTP sever, which in then sends mail to recipients local SMTP sever, and finally to recipients local machine.

II. RELATED WORK DONE

2.1 Face-based PC login:

Face verification and matching a face against a single stored face, is possible within the capabilities of current Personal Computer hardware. Since personal computer cameras are used widespread, their use for face-based PC logon has become feasible.

2.2 Airport security:

Airport and other transportation terminal security is not a new thing. People have long had to pass through metal detectors before they boarded a plane, been subject to questioning by security personnel, and restricted from entering "secure" areas. The use of biometric identification, can enhance security efforts already under-way at most airports and other major transportation hubs.

2.3 Access control on mobile:

Face verification matching is now well within in a mobile phone. Face of user is used as password to unlock the mobile phone. Facial recognition systems are also beginning to be incorporated into unlocking mobile devices. The android market is working with facial recognition and integrating it into their cell phones. They have created an application called Vision Applock. This application allows you to put a facial recognition lock on any of your applications.

2.4 Passport validation:

The Australian Customs Service has an automated border processing system called Smart Gate that uses facial recognition. The system compares the face of the individual with the image in thee-passport microchip, certifying that the holder of the passport is the rightful owner.

III. PROPOSED SYSTEM

We are supposed to develop an email application that will allow the user to access his/her account by face recognition instead of providing username and password. The system provides face recognition technique to access an account. After login, account will be opened if and only if face of the user matched with the photograph of user stored in the database.
In our project we are developing a System such that we capture the image of the authorized as well as unauthorized person by using the webcam. Then image matching of that image is done with admin stored image from the database. Image matches admin image, admin can access the system and if image does not match then the person will be unauthorized, so for security we send a message on the admin mobile phone with help of any gateway and a mail on admin email-id with hackers' image and some notification.

IV. IMPLIMENTATION DETAILS

4.1 Method

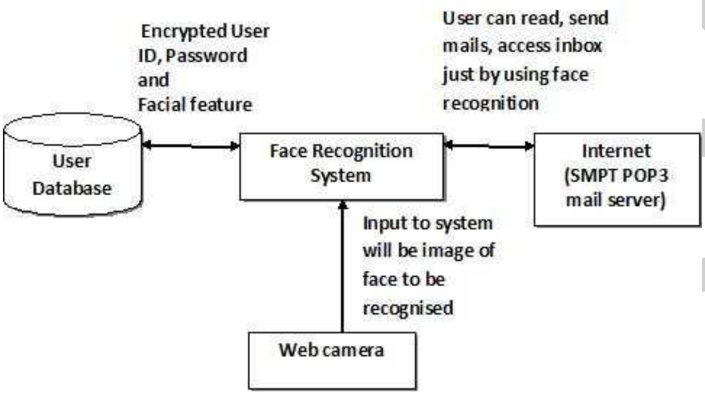

Fig.1 Facial Scan Process Flow.

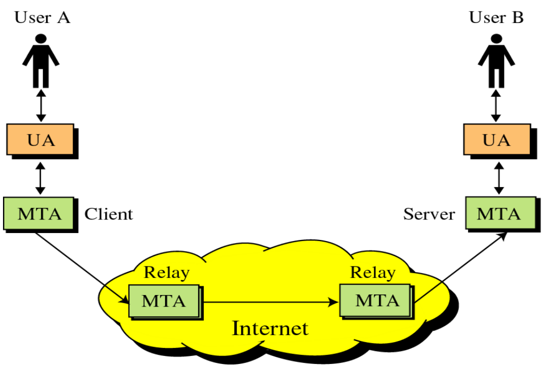

Fig.2 Process Flow Chart

4.2 Using MATN to Model and Control Snapshot Browsing in Surveillance Monitor

4.2.1 Functionalities of Surveillance Monitor

The design principals and functionality of the Surveillance Monitor are discussed as follows.

• *Delegation-based Visual User Interfaces:*

In the design of the Surveillance Monitor, a delegation-based event model that has been proposed since JDK 1.1 for larger-scale GUI development is adopted. The reason for adopting the delegation-based event model is that the earlier event-loop and inheritance-based AWT model requires to write a loop, wait for some events to occur, and then take the associated actions. In the new model, one simply needs to register event handlers (called event listeners) with an AWT (Abstract Window Toolkit) component. Whenever some events come up on the component, its associated event listener will be invoked.

• *Image Viewer:*

Image Viewer is a sub-component within the Surveillance Monitor (as shown in Figure 1). It periodically receives snapshot signals in the integer array format provided by Snapshot Feeder through RMI, constructs a JPEG image, and then displays the image on the Surveillance Monitor frame. There are two routines that can be called by Image Viewer. The Local Backup Routine is used to store images on the local (or networking) repository; whereas the Local Hardcopy routine is used to obtain a hardcopy of an image.

• *Archives Viewer:*

Archives Viewer is a sub-component within the Surveillance Monitor (as shown in Figure 1). Time-stamped image archives carried by Archiving Server over RMI slide-by-slide can be examined by the Archives Viewer. Though network bandwidth or computer processing power makes the delivery of live videos expensive, some interesting images can still be marked up by using a mouse so a simulated video could be obtained for browsing. Similar to the Image Viewer, Archives Views can save and print suspicious images locally.

• *Alert Caller:*

Alert Caller is a sub-component within the Surveillance Monitor (as shown in Figure 1). Alert Caller provides users a convenient way to send an urgent signal to the manager on-duty via pager or e-mail when an emergency occurs. The Pager Server powered in Java Communications API in Surveillance Server routes the pager number sent by Alert Caller through RMI to the RS232 serial port on the server machine. The signal recipient then may remotely sign onto DSS and inspect the spot being monitored.

4.3 Login module

In this module login into proposed system will be done by capturing face of a user with web cam and comparing this captured face with user's face stored in database during registration. If both faces match, access will be given to the user.

Fig.3 Window for the login

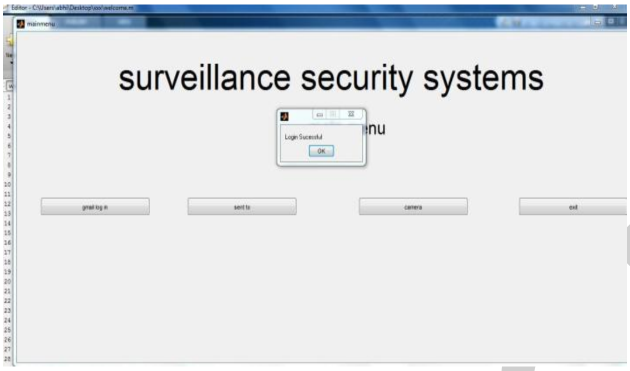

Fig.4 Window for the confirmation

Fig.5 Window for opening the system

Fig.6 Window for the camera

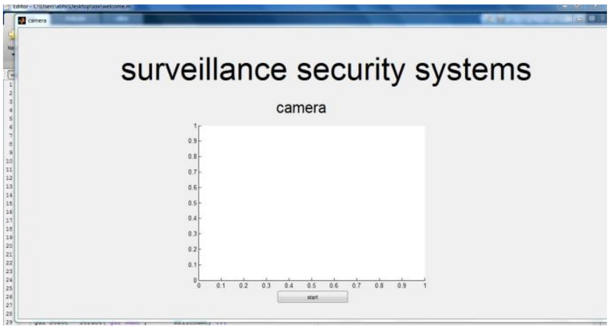

Fig.7 Window for the output of the camera

Sample capture - When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale algorithm is used to search for faces in low resolution. The system switches to a high resolution search only after a head-like shape is detected.
Alignment - Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it.
Normalization -The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process.
Representation - The system translates the facial data into a unique code also called as template. This coding process allows for easier comparison of the newly acquired facial data to stored facial data the template is much smaller than the image from which it is drawn whereas quality facial images generally require 150- 300 kb, the templates are approx. 1300 bytes or less than 1/100th of original.
Matching - The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation. The degree of similarity required for verification also known as threshold can be adjusted for different personnel's, pcs, time of the day and other factors. If face of the user matched with the photograph stored in the database. His account will get opened.

4.4 Registration module

In this module proposed system will gather all personal details of user and just like registration done at other social websites or email website for e.g. Gmail, yahoo etc. In addition to common personal details such as Name, Address, Date of Birth, Age, Gender, nationality proposed system is supposed to capture face of a user; this captured face will be stored in the database.

4.5 Sending and receiving of mails

In this module after getting access to email account user will be able to send or compose mails, attach files to mails, download files form mails, delete mails, read mails, move mails, and receive mails normally.

Face recognition algorithms and identification: As with any biometric data, two images of the same person are never identical. On the other hand, authentication based on passwords or cryptographic keys always expects the user to enter the same password or use the same key.

Representations used in recognition must be designed to produce the same results for similar, but not necessarily identical, inputs. In cryptographic algorithms only identical inputs enable successful authentication, and therefore they cannot be applied to biometric recognition.

V. PROPOSED ALGORITHM

5.1 Eigen face

Eigen face is 2d global gray scale images representing distinctive characteristics of a facial image. In this distinctive characteristics of the entire face are highlighted for use in future authentication. The vast majority of faces can be reconstructed by combining features of approximately 100-125 Eigen faces. During enrolment, the subjects Eigen face is mapped to a series of numbers i.e. coefficients. For one to one authentication, in which the image is being used to verify a claimed identity, ones live captured face is compared against the stored face image to determine coefficient variation. The degree of variance from template will determine acceptance or rejection.

5.1.1 Steps

(1) The original images of the training set are converted into a set of Eigen faces E.

(2) The weights are calculated for each image of the training set and stored in the set W.

(3) Upon observing an unknown image X, the weights are calculated for that particular image and stored in the vector WX.

(4) Then, WX is compared with the weights of images, of which one knows that they are faces (the weights of the training set W). One way to do it would be to regard each weight vector as a point in space and calculate an average distance D between the weight vectors from WX and the weight vector of the unknown image WX (the Euclidean distance described in appendix A would be a measure for that) If this average distance exceeds some threshold value, then the weight vector of the unknown image WX lies too far apart from the weights of the faces. In this algorithm the unknown X is considered to not a face. Otherwise (if X is actually a face), its weight vector WX is stored for later classification. The optimal threshold value has to be determined empirically.

VI. EXPERIMENTAL RESULTS

It is showing that screen for composing message activity.

6.1 Receiving and reading of mails

This window opens up when user does successful login that is when face are matched. This is the first window that opens up after login. In this window user has to enter server address of map protocol, user name, and password, check SLS connection option and then click on Start button. As soon as start button is clicked all the mails of a user will appear in right hand side section of window. By clicking on any mail user can read, delete, undelete, make it unread, pure i.e. refresh and can move that mail and can upload files.

VII. CONCLUSION

SMTP and MIME protocol is used for sending notification to user. For electronic mail (e-mail) transmission across Internet Protocol (IP) networks Simple Mail Transfer Protocol (SMTP) is used. Email is submitted by a mail client (MUA) to a mail server (MSA, mail submission agent) using SMTP. The MSA delivers the mail to its mail transfer agent (MTA, mail transfer agent). SMTP protocol is connection-oriented, text-based protocols in which a mail sender can communicates with a mail receiver by sending command and provide necessary data over a reliable ordered data stream channel. These include text in other languages like English using character encodings and files containing images, sounds, movies. Mapping messages into and out of MIME format is typically done automatically by an email client or by mail servers when sending or receiving Internet (SMTP/MIME) email. Face recognition is also resulting in other dares, like expression recognition or body motion recognition. Overall, face recognition techniques and the emerging methods can see use in other areas. Therefore, it isn’t just an unresolved problem but also the source of new applications and challenges. Administrator can get complete idea of who is trying to access the system with help of image capturing of unauthorized person and then sending image via SMS and E-Mail alert. Enhance security should be provide with the help of face recognition technique.

REFERENCES

[1] Jafri, R.; Arabnia, H. (2009): “A Survey of Face Recognition Techniques”, Journal of Information Processing Systems, Vol.5, No.2.

[2] Kawaguchi, Y.; Shoji, T.; Lin, W.; Kakusho, K.; Minoh, M. (2005): “Face Recognition-based Lecture Attendance System”.

[3] Senior, A. W.; Bolle, R. M. (2002): “Face Recognition And Its Applications”, Chapter 4.

[4] Verdi,J.(2014):“Facial Recognition Technology” Electronic Privacy Information Center.

[5] Zhang, Z.; Zhou, Z.; Sun, H.; Dong, F. (2012): “Comparison of Three Face Recognition Algorithms”, International Conference on Systems and Informatics”.

[6] M. Osadchy, Y. LeCun, and M. Miller, “Synergistic face detection and pose estimation with energy-based models,” Journal of Machine Learning Research, vol. 8, pp. 1197–1215, May 2007.

[7] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” in Proc. IEEE Conf. on Computer Vision and Pattern Recognition, 2001, pp. 511–518.

[8] C. Chen, R. Veldhuis, T. Kevenaar, and A. Akkermans, “Biometric binary string generation with detection rate optimized bit allocation,” in CVPR Workshop on Biometrics, 2008, pp. 1–7.

[9] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, “The FERET evaluation methodology for face-

recognitionalgorithms," PAMI, vol. 22, no. 10, pp. 1090–1104, 2000.
[10] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression database," PAMI, vol. 25, pp. 1615–1618, 2003.
[11] A. Juels and M. Sudan, "A fuzzy vault scheme," in Symposium on Information Theory, 2002.
[12] P. Tuyls and J. Goseling, "Capacity and examples of template protecting biometric authentication systems," in ECCV Workshop BioAW, 2004.
[13] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.
[14] Y. Adini, Y. Moses, and S. Ullman, "Face recognition: the problem of compensating for changes in illumination direction," PAMI, vol. 19, no. 7, pp. 721–732, 1997.
[15] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.
[16] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," PAMI, vol. 29, no. 4, pp. 561–572, 2007.
[17] T. Boult, "Robust distance measures for face-recognition supporting revocable biometric tokens," in IEEE, 7th Intl. Conf. on Automatic Face and Gesture Recognition, 2006, pp. 560–566.
[18] S. Avidan and M. Butman, "Blind vision," in ECCV (3). Springer, 2006, pp. 1–13.
[19] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, A. Ekin, J. Connell, C. F. Shu, and M. Lu, "Enabling video privacy through computer vision," IEEE Security and Privacy, vol. 3, no. 3, pp. 50–57, 2005.
[20] F. Dufaux and T. Ebrahimi, "Scrambling for Video Surveillance with Privacy," in IEEE Workshop on Privacy Research in Vision. IEEE, 2006.