ISSN 2229-5518

Avert E-mail Hacking System with Face Recognition

Infant Vinoth .T[1], Rosario D'souza .B[2], T.Sudalai Muthu[3], M. Roberts Masillamani[4]

Abstract— Now-a-days E-mail system acts as a major role in industry, business, educational institutes etc. Even though many encryption software's and methods trying to prevent the hacking, but still there are possibilities of hacking the user information. This paper tells or explores the new security measures to mail system with the help of Biometric concept called Face Recognition. Face recognition is one of the largely elastic systems. It works effective than others even when the subject or person is unaware of being scanned. It also illustrate assure as a way to search through a lot of people who spent only seconds in front of a scanner. DSCP Algorithm (Depth Surface Closest Point) with e-mail system solves the previous problem and provides effective accuracy. Avert e-mail hacking system shields the user information from hackers, unauthorized users and other hacking techniques so user information will be safe.

Index Terms— Biometric, Face Recognition, DSCP Algorithm, E-mail hacking, Authentication, key logger.

1 Introduction

Login page is the starting point to any web site or e-mail. The most important thing is to authenticate the user. User name and password is important so it must be secured in any format, for that reason developers used lots of encryption, decryption algorithm and some password management techniques. But still there are possibilities to hack the user name, password and other valuable user data.

In the earlier period, face recognition system has relied on a 2D image to evaluate or identify another 2D image from the database. To be successful and precise, the image captured needed to be of a face that was looking almost directly at the camera, with little inconsistency of light or facial expression from the image in the database and this created problems. In most cases the images were not taken in a controlled situation. Even the smallest changes in light or orientation could diminish the effectiveness of the system, so they could not be matched to any face in the database, leading to a high rate of failure.

Here new technique is commenced, integrating the 3D DSCP Algorithm (depth surface closest point) with e-mail communication or system [1]. It averts the hacking e-mail system from the unauthorized user, and it's a new creed of the present user problems.

2 Related Work

Maintain 3D face models database to 2.5D face scans which are captured from different views, using coordinate system invariant properties of the facial surface [9]. 2.5D is converted into 3D model that contains at nearly all one depth value (z direction) for every point in the (x, y) plane. A vigorous similarity metric is defined for matching, based on an (ICP) registration process [1].

The presented matching algorithm is based on ICP (Iterative Closest Point) which aligns one presented probe model to a 3D face model from the gallery data set and provides perfectly its posture [2]. Recognition score is given by a region-based similarity metric which takes into account regions labels. Here, a specific study in facial expression analysis is done for the labeling purpose.

SIFT Method revealed for object or person recognition. It focused on three things namely:
1. Distance between all pairs of key point descriptors in the two images and use as matching score the minimum distance.
2. Use only SIFT features belonging to the areas around the eyes and mouth.
3. The matching is performed considering the SIFT features situated along a regular grid and matching overlapping patches and also SIFT concentrate on key points over the face [3].

Matching of 3D images with 2.5D and other face models [11]. The general model consists in construction a full 3D face gallery using a laser-based scanner (the off-line stage). At the on-line phase, identification or verification, only one captured 2.5D face model is performed with the entire set of 3D faces from the gallery or compared to the 3D face model of the real, respectively [11]. This probe model can be acquired from arbitrary viewpoint, with arbitrary facial expressions, and under arbitrary lighting conditions [4].

New protected e-mail system based on a fingerprint authentication scheme which combines fingerprint authentication technology with IBE scheme [5]. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose [6]. People who engage in computer hacking activities are often called hacker.

3 Previous Problems

Hacking the user information is an important headache for the industry, organization, etc (see figure1). Hacking can be possible in many ways. Few ways of hacking techniques are key capturing (software, hardware), phishing, password guessing, crackers etc [7]. Some of the examples of hacking: phishing is the one type of hacking technique just because it is simple and affordable [10]. It carried out by

- *Infant vinoth is currently pursuing master of engineering in Hindustan University, Country, PH-+91-9994272861. E-mail:infavinoe@gmail.com*
- *Rosario d'souza is currently pursuing master of engineering inHindustan University, India, PH-+91-9600658484. E-mail:rosriodso@gmail.com*

e-mail or instant message, and it often directs users to enter details(user name, password, bank details, credit card details etc.) on a fake website whose look and feel are almost original. Hacker mostly sends an e-mail or message that appears to come from a bank, credit or debit card company, requesting "verification" of information.

Another type is key logger (device). When fix this key logger with pc then we can be able to sketch or capture all the strokes or personal information such as email id, password, bank id, credit card etc. It has two types 1.hardware key logger, 2.software key logger. We must fix or insert the device between the keyboard and pc. Through this we can physically access victim's Personal computer. Key strokes or Personal information can be collected in a temporary file and are stored in to the flash memory of the key logger. Software key loggers are essentially acted as a spyware; they are used to hack the remote personal computer. Hacker usually sends key logger application (small software or exe files) via email [10]. When customer trying to click that mail then they will capture all details of the customer [7][8].

Fig. 1. Hackers using hacking method Like phishing, key logger,

Fig.2. Image taken from different light variation.

Previously some of the 2D and other face recognition system fail to recognize the face see (Figure 2). It struggle or fail to distinguish when it taken images from different light variation, fail to recognize the twins face, it detects the human face when we sit direct or straight in front of the camera [11]. It struggled to recognize the face when smiling, frowning and yawning. And accuracy of recognizing face also very less so it made big trouble for the security.

4 PROPOSED SYSTEM

Here implementing the three dimensional with depth surface closest point algorithm. It gives the solution for previous problems with the help of DSCP (depth surface closest point) Algorithm. This system works by systematically analyzing exact features that are common to everyone's face - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin and so forth. These numerical quantities are then united in a single code that uniquely identifies each person.

Fig. 3. Coarse alignment.

Fig. 4.Fine alignment.

4.1 3D Face model

3D face model has two important processes: coarse alignment and fine alignment

i. Coarse alignment

First it has been traced (eye, mouth, and nose) then it is used to perform rigid form. Mesh or surface texture used to cover on the human face [1]. See (Figure 3) the process, called Surface Texture Analysis, mechanism much the similar way facial recognition does. An image is taken of a piece or patch of skin, called a skin print. That patch is then broken up into smaller blocks [4].

ii. Fine Alignment

See (Figure 4) Human face covered with the mesh or web then automatic point focuses particular portion of the image like mouth, eyes, nose and forehead. Then it zoomed those portions of the image. It used to calculate the mean square error based on two points. Two sets of points DB = $\{d_i\}$, as a reference data, and TB= $\{b_i\}$, as a test data, the goal is to find the rigid transformation (*R, t*) which minimizes the distance between these two sets of points.

$$e(R,t) = 1/N \sum_{i=0}^{N} || (R_{di} + t) - b_i||^2 \qquad (1)$$

$$e(R,t) = 1/N \sum_{i=0}^{N} || (R_k(R_{di} + t) + t_k - b_i||^2 \qquad (2)$$

This procedure is alternated and iterated until convergence (i.e. stability of the minimal error). Indeed, total Transformation (*R, t*) is updated in an incremental way as follows: for each iteration *k* of the algorithm: *R* = *Rk.R* and t = *t* + *tk*. The criterion to be minimized in the iteration *k* becomes (2)

Algorithm 1 Depth Surface Closest Point Algorithm

Require: DB = $\{d_i\}$ (from gallery), TB= $\{b_i\}$ (probe)
Ensure: (*R, T*) which minimize error (MSE), matched points, spatial deviation between matched points
1: Get the image, zoom the precise area and construct depth closest point pairs
2: Compute best transform which minimizes the error (MSE)
3: Apply transform to the probe model TB= $\{b_i\}$
4: Iterate (1) and (2) until mathematical convergence, compute at each iteration (*Rk*, *tk*)
5: Calculate error part and matched points then conclude whether exact person or not
Return: (*R, t*); (*pi, yi*): matched points: (*di*): spatial deviation.

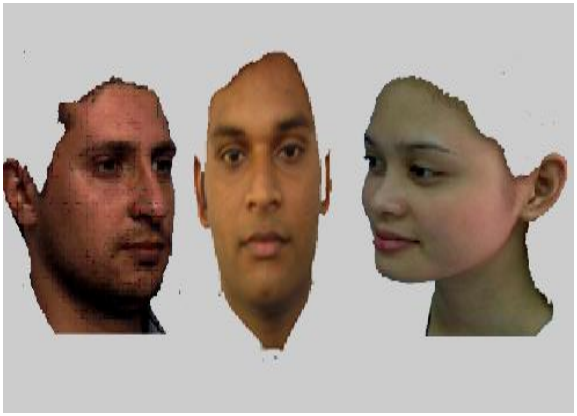

Fig. 5. Frontal, left, and right view of the 3D model.

4.2 Process

- 3D Database: when user try to enter the e-mail, it gives two option already registered user or new user, if already registered user means web camera capture the human face and check with the database images finally it will allow if he/she is already an user otherwise it will not allow.
- If she/he is not having any account then the new user registry form will be open. She/he must fill the form and through the web camera it will store the image into the database. Instead of user name and password it creates face as a password.
- Then the user can access his account or perform operation like composing mail, reading, deleting, etc.
- It prevents the Unauthorized user access in the very beginning itself so it's a better security methods.
- After performing operation Users exit from the e-mail system

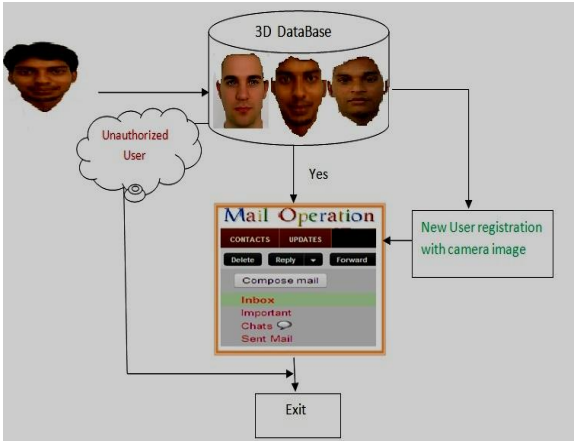

Fig. 6. E-mail operation with face recognition Flow chart

5 CONCLUSION

3D Face Recognition with the help of DSCP Algorithm solves the various techniques of hacking. It provides the efficient service to the users and also it provides effective security compare to other techniques. This new system (Avert E-mail Hacking System with Face Recognition) averts the unauthorized user access and it recognizes the face when smiling, frowning and yawning. Compare to other algorithm this system will provide more accuracy also it works during poor light. So user's information will be secluded and it's a new system which will attract more number of users in future. Multiple Biometric Logic will be included in prospect with e-mail so as to improve the security and efficiency of e-mail.

6 REFERENCES

[1] Xiaoguang Lu, Dirk Colbry and Anil K. Jain, "*Three-Dimensional Model Based Face Recognition*", Pattern Recognition, ICPR 2004 Proceedings of the 17th International Conference 2004

[2] Boulbaba Ben Amor, Mohsen Ardabilian, and Liming Chen, *" Enhancing 3D Face Recognition By Mimics Segmentation "* Intelligent Systems Design and Applications

[3] Bicego M, Lagorio A, Grosso, E.; Tistarelli, M, "*On_the_Use_of_SIFT_Features_for_Face_Authentication*", Computer Vision and Pattern Recognition Workshop 2006.

[4] Amor B.B, Ardabilian, M, Liming Chen, **"***New Experiments on ICP-Based 3D Face Recognition and Authentication***"** Computer Vision and Pattern Recognition Workshop 2006.

[5] Zhe Wu, Jie Tian, Liang Li and Cai-ping Jiang, Xin Yang, "*A Secure Email System Based on Fingerprint Authentication Scheme*" , Intelligence and Security Informatics 2007

[6] Mamatha G, Ashoka, B.M, "*Unofficial hacking algorithms*", Control, Automation, Communication and Energy Conservation 2009.

[7] Petr Hanaeek, Kamil Malinka and Jiri Schafer "*e-Banking Security -A Comparative Study"* in Aerospace and Electronic Systems Magazine 2010.

[8] Juan Chen and Chuanxiong Guo, *"Online Detection and Prevention of Phishing Attacks*" Communications and Networking in China, ChinaCom '06.

[9] Abate A.F, Nappi M, Ricciardi S, Sabatino. G, *"Fast 3D face recognition based on normal map*", Image Processing 2005.

[10] Qiong Ren, Yi Mu, Susilo W, "*SEFAP: An Email System for Anti-Phishing",* Computer and Information Science 2007.

[11] B. BenAmor, K. Ouji, M. Ardabilian, and L. Chen, "*3d face recognition by icp-based shape matching"*. In *Proceeding of* IEEE *International Conference on Machine Intelligence*, Tozeur, Tunisie, November 2005.