EFFICIENT AUTHENTICATION SYSTEM FOR DATA TRANSACTION THROUGH EYE BLINKING APPROACH

A. Menaka[1], M. Arun Kumar[2], G. Kavi Ganesh[3] & A. Nithish[4]

[1]Assistant Professor, Department of Information Technology, A.C.E, Hosur
[2]Student, Department of Information Technology, A.C.E, Hosur
[3]Student, Department of Information Technology, A.C.E, Hosur
[4]Student, Department of Information Technology, A.C.E, Hosur

---

Abstract: *In this paper we focuses on efficient vision based human computer interface for authentication using eye blinking approach. The interface detects eye-blinks and interprets them as control commands. The employed image processing methods includes Dlib and OpenCV-like features for automatic face detection, and template matching based eye tracking and eye-blink recognition. Dlib can staggeringly discover 68 diverse facial landmarks focuses including jaw and stunning, eyebrows, nose, eyes and lips. We can remove accurate facial territory dependent on those landmarks focuses past harsh face location. This will increase the accuracy of face identification model dramatically due to the fact we can discard any noise on this way. OpenCV is a cross-platform library using which we can develop real-time computer vision applications. It specifically focus on image processing, video seize and evaluation consisting of functions like face detection and object detection.*

Keywords*:* **Eye blinking, Dlib, OpenCV, eye-blink recognition, Landmark focuses.**

1. INTRODUCTION

The ascent of innovation bring into power heaps of kinds of devices that yearn at more client delight. ATM is a machine which brought in cash exchanges easy for clients. Be that as it may, it has the two benefits and burdens. Current ATMs utilize nothing in excess than access card and PIN for uniqueness confirmation. This has ATM Using Face Recognition System exhibit the path to a lot of fake attempt and abuse through card theft, PIN theft, stealing and hacking of client's account details and other part of security. To utilize an ATM with facial recognition framework, all you need is walk to the atm. its computerized camera is on 24hours every day, and its computer will consequently start a face recognition procedure, whenever the computer detects a human face in camera gets an image of your face, the computer compares the picture of your face to the pictures of enrolled clients in its database. On the off chance that your face (as seen by the ATMs camera) coordinates with the image in the database you are automatically perceived by the machine. When your face is perceived a message will be shown as your face has been perceived.

ATM is one such machine which brought in cash exchanges simple for clients to bank. The opposite side of this improvement is the upgrade of the offender's likelihood to get his „unauthentic‟ share. Customarily, security is dealt with by requiring the mix of an actual access card and a PIN or other secret word to get to a client's record. This model welcomes deceitful endeavors through taken cards, severely picked or naturally allocated PINs, cards with next to zero encryption plans, representatives with admittance to non-encoded client account data and different marks of disappointment. In an automated teller machine security model that would join an actual access card, a PIN, and electronic facial acknowledgment is proposed. By compelling the ATM to coordinate with a live picture of a customer‟s face with a picture put away in a bank data set that is related with the record number, the harm to be brought about by taken cards and PINs is viably killed. Just when the PIN coordinates with the record and the live picture and put away picture match would a client be considered completely checked.

The principle issues looked in growing a particularly model are keeping the time slipped by in the check interaction to an insignificant sum, taking into consideration a fitting degree of variety in a client's face when contrasted with the data set picture, and that Visas which can be utilized at ATMs to pull out reserves are by and large gave by establishments that don't have in - individual contact with the client, and henceforth no chance to secure a photograph.

2. RELATED WORK

Johnson Olabode Adeoti. [1], Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out The problem of Automated Teller Machine (ATM) frauds is global in nature and its consequences on bank patronage should be of concern to the stakeholders in banks. This paper investigates the dimensions of ATM frauds in Nigeria and

proffer solutions that will mitigate the ATM frauds in the Nigerian banking system. The paper employs both primary and secondary data to investigate the ATM frauds in Nigerian banks. The chi-square statistical technique was used to analyze the data and test the hypothesis raised.

Penio S Penevy, et al.[2], Local Feature Analysis: A General Statistical Theory for object Representation In this paper a new mathematical construction, local feature analysis (LFA), for deriving local topographic representations for any class of objects. The LFA representations are sparse-distributed and hence, are effectively low-dimensional and retain all the advantages of the compact representations of the PCA. We illustrate the theory by using it to extract local features for three ensembles: 2D images of faces without background, 3D surfaces of human heads, and finally 2D faces on a background. The resulting local representations have powerful applications in head segmentation and face recognition.

Gross. et al. [3], Quo Vadis Face Recognition In this paper, We quantified the influence of these factors, individually and in combination, on face recognition algorithms that included Eigenfaces, Fisherfaces, and FaceIt. Image data consisted of over 37,000 images from 3 publicly available databases that systematically vary in multiple factors individually and in combination.We also found small but significant differences related to gender, which suggests that greater attention be paid to individual differences in future research. Algorithm performance across a range of conditions was higher for women than for men.

Mike, et al. [4], Evaluating Facial Recognition Technology for Drug Control Applications: In this paper, an overview of the FRVT 2000 evaluation and examine case studies of potential drug control applications. We provide a requirements analysis for each application and show how the FRVT 2000 evaluation report could be used to determine if the current level of facial recognition technology is appropriate to meet those requirements.

S. Sruthy. [5], Literature Survey Automated Person Identification Techniques A wide variety of organizations are using automated person identification systems to improve customer satisfaction, operating efficiency as well as to secure critical resources. This paper gives a literature survey on the recent developments in person identification techniques and the survey highlight on two major approaches for automatic human identification, namely biometric identification and gait identification. Gait identification provides a way to automatic person identification at distance in visual surveillance and monitoring applications.

Zigelman, et al. [6], Texture mapping using surface flattening via multi-dimensional scaling : Presents a novel technique for texture mapping on arbitrary surfaces with minimal distortion by preserving the local and global structure of the texture. The recent introduction of the fast marching method on triangulated surfaces has made it possible to compute a geodesic distance map from a given surface point in O(n lg n) operations, where n is the number of triangles that represent the surface. We use this method to design a surface flattening approach based on multi-dimensional scaling (MDS). MDS is a family of methods that map a set of points into a finite-dimensional flat (Euclidean) domain, where the only data given is the corresponding distance between every pair of points. The MDS mapping yields minimal changes of the distances between the corresponding points. We then solve an "inverse" problem and map a flat texture patch onto a curved surface while preserving the structure of the texture.

3. PROPOSED WORK

In this section, we describe our technique for efficient and reliable eye-blinking detection for authentication. The working process of the system is shown in the figure in this the user will stand in front of the system camera then the face image will be taken and pre processed and sent to feature extractor to get the facial points then will be sent to classifier to match with the database then will sent to training set to train the image and fed to classifier to perform next process.

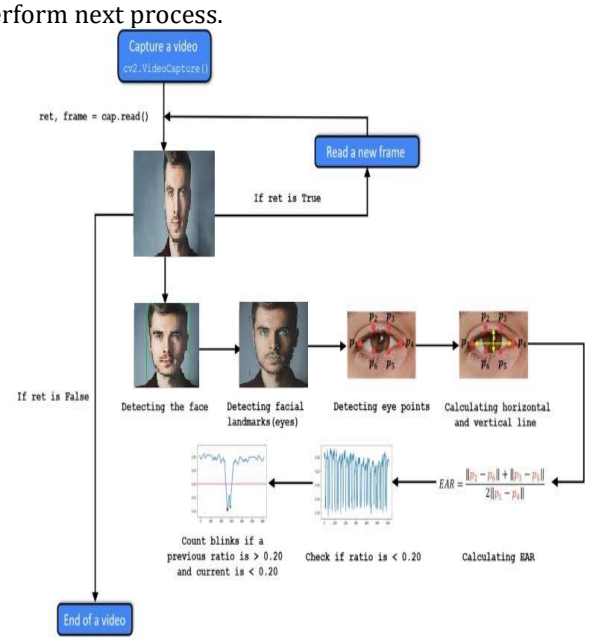
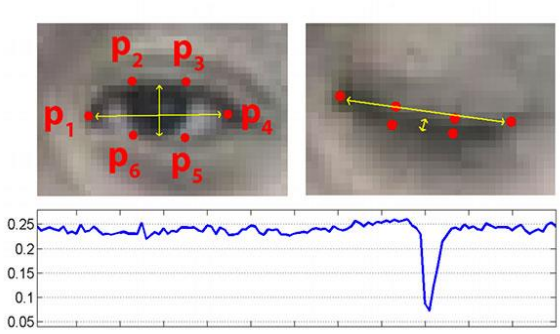


Fig: Architecture Structure

3.1 Understanding the “eye aspect ratio” (EAR)

We can apply facial landmark detector to restrict significant areas of the face, including eyes, eyebrows, nose, ears, and mouth. This likewise infers that we can extract specific facial structures by finding the index of the specific face parts. Each eye is addressed by 6 (x, y)-coordinates, starts from the left-corner of the and then working clockwise around the rest of the part. Real Time Eye Blink Detection using Facial Landmarks, we would then be able to infer a condition that reflects the relation called the eye aspect ratio (EAR). Where p1, p2, p3 ..., p6 are 2D facial landmark. The numerator is the distance between the vertical eye landmarks and the denominator is the distance between horizontal eye landmarks, weighting the denominator properly since there is just one set of horizontal points yet two sets of vertical points. The eye aspect ratio is approximately constant while the eye is open; however will quickly falls to zero when a blink occur

$$\mathrm{EAR} = \frac{\|p_2 - p_6\| + \|p_3 - p_5\|}{2\|p_1 - p_4\|}$$



3.2 Eye blinks detection using OpenCV and Python

In this project, we will build up a vision based application that can detect and counting blink in video streams using facial landmarks and OpenCV. To build our blink detector, we'll be using the eye aspect ratio (EAR). To find face and eyes in our video we need to call a frontal face detector dlib.get_frontal_face_detector () and facial landmark detector dlib.shape_predictor from dlib library. With the assistance of following order, you can download and unfasten dlib.shape_predictordirectly to your python. We use dlib.shape.predictor code to download and unzip directly to python script. Next, we will load the video, characterize the four code and create a VideoWriterobject. Furthermore, we will define a text style that we will use later when we will show number in the video. Now, the time has come to recognize the face and facial landmarks

3.3 Face detection using MTCNN:

The MTCNN is famous because it achieved the state-of-the-art results on a scope of benchmark datasets, and it can be able to identify other facial features like eyes and mouth, called landmark detection. The network uses a cascade structure with three organizations; first the picture is rescaled to a range of various sizes (called an image pyramid), then the primary model P-Net proposes candidate facial regions, the subsequent model R-Net filters the bounding boxes, and the third model O-Net proposes facial landmarks. The model is known as a multiple tasks network because of the fact that each one of the three models in the cascade (P-Net, R-Net and O-Net) are prepared on three tasks. The three models are not associated directly. Instead, output of the past stage are taken as input for following stage. This allows extra processing to be performed between stages.

3.4 Training Data

We perform both face recognition and alignment, here we use four various types of data annotation in our training process: (i) Negatives: Regions that the Intersection-over-Union (IoU) proportion under 0.4 to any ground-truth faces; (ii) Positives: IoU above 0.65 to a ground truth face; (iii) Part faces: IoU which range between 0.4 and 0.65 to a ground truth face; and (iv) Landmark faces: faces named 5 landmarks positions. Negatives and positives are used for face arrangement task, positives and part faces are used for bounding box relapse, and face landmarks are used for facial landmark localization. The training data for each organization is portrayed as follows: 1) P-Net: We arbitrarily crop a few patches from WIDER FACE to gather positives, negatives and part face. At that point, we crop faces from CelebA as milestone faces 2) R-Net: We use first phase of our system to distinguish faces from WIDER FACE to gather positives, negatives and part face while landmark faces are recognized from CelebA. 3) O-Net: Similar to R-Net to gather information however we utilize initial two phases of our structure to identify faces

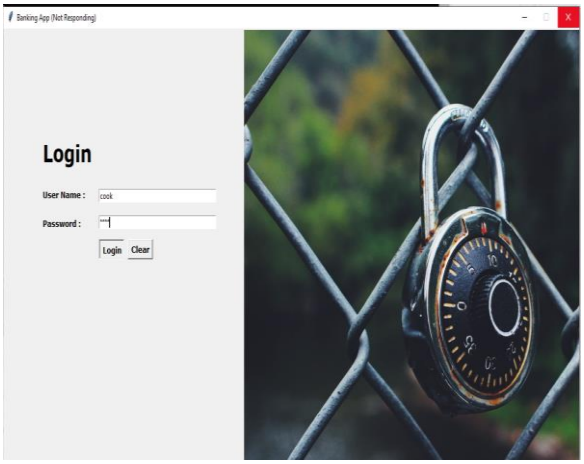
4. RESULT

We compute the overall detection accuracy and the detection accuracy of the eye blink detection. This method avoids Shoulder-Surfing, Thermal Hacking and many other which can be a threat to the user. This is the safe method to authenticate. Therefore, our overall detection accuracy is 89.6%, and our detection accuracy is 92.6%. From the experiments, inaccuracy of our eye blink detection is occasionally occurred in two situations. The first situation is when a subject moves his/her head swiftly.

Frame rate	TP	FN	FP	TP
30	611	23	21	96.4
100	738	29	13	96.2
150	612	22	6	96.5
200	758	15	3	98.1

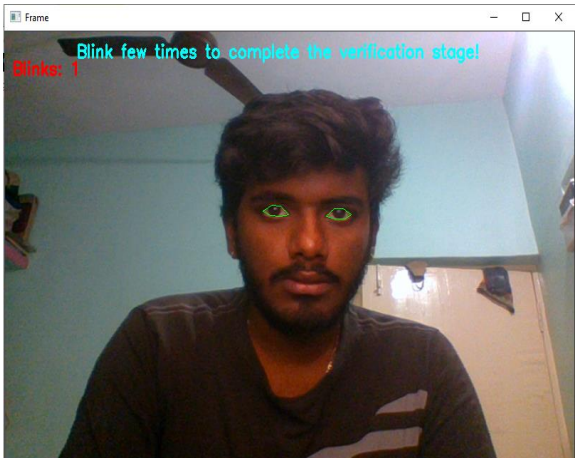
4.1 User Login

The User Login page this will be the first stage of the authentication process. In this the user has to enter the user id and the password to access the next authentication process. Each user will be provided with specific user id and password. Then the user will be directed to next stage of authentication.



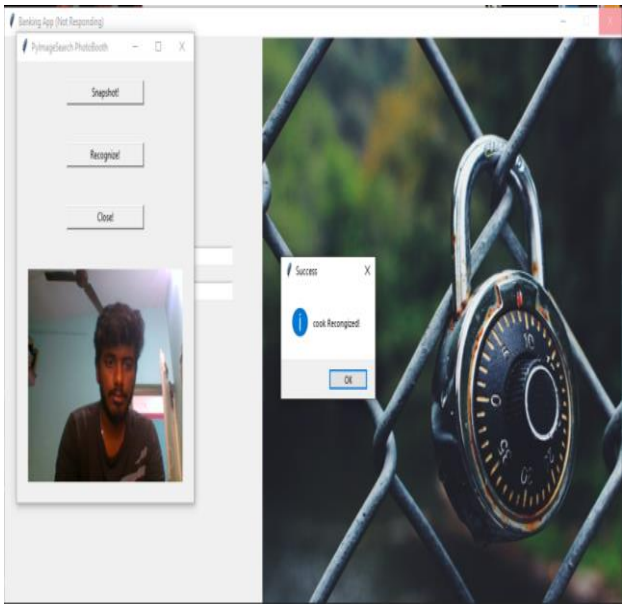
4.2 Blink Authentication

This will be the next stage of authentication in this the user will be authenticated through the blink detection. The user will blink his/her eyes to verify and the system will detect the blink and then authorize the user to proceed to the next stage of authentication.



4.3 Face Detection

This will be the third and final stage of authentication in this the user will be authenticated by verifying the face which is previously stored in the database. The user face will be recognized and processed to the banking interface.



5. CONCLUSION

There is a disadvantage of failing to remember your passwords, shoulder surfer attack this can be overcome by this technology. Use of this technology will be useful for every single area of this corporate world. Uses of this technology can be used further for high security frameworks by making some more upgrades and research. In the entirety of the experiment in which the subjects were seated in the range of 1 and 2 feet from the camera, it never took in excess of three involuntary blinks by the client before the eyes were found effectively. Another improvement is this frameworks similarity with low cost USB cameras, instead of high quality video CCD camera. These Logitech USB cameras are more reasonable and compact, and maybe above all, support a high real time frame rate of 30 frames each second. The reliability of the framework has been shown with the high accuracy. The experiments show that the framework performs truly well in extreme lighting conditions. The accuracy rates in these cases were around equivalent to those that were retrieved in ordinary lighting conditions.

REFERENCES

[1]Johnson Olabode Adeoti, "Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out" Business Administration Department, University of Ilorin, Ilorin, Nigeria Kamla-Raj 2011 J Soc Sci, 27(1): 53-58 (2011).

[2]Penio S Penevy, Joseph J Atickz X, "Local Feature Analysis: A general statistical theory for object representation" research gate November 1996 with 111 Reads DOI: 10.1088/0954-898X/7/3/002.

[3]Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. "Quo vadis Face Recognition." Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001

[4]Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. "Evaluating Facial Recognition Technology for Drug Control Applications." ONDCP International Counterdrug Technology Symposium: Facial Recognition Vendor Test., June 2001.

[5]S. Sruthy. "Literature Survey Automated Person Identification Techniques." (2013).

[6] Zhiwei Zhu, and Qiang Ji, "Robust Real-Time Face Pose and Facial Expression Recovery" Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06) 0-7695-2597-0/06 © 2006 IEEE.