Banking Security System by Cross-Domain Deep Face Matching

Akanksha Nalawade[1], Ritesh Bagul[2], Shivani Deshpande[3], Sandeep Chitalkar [4]

[1]Akanksha Nalawde, Department of Computer Engineering & Sinhgad Institute of Technology and Science, Pune
[2] Ritesh Bagul, Department of Computer Engineering & Sinhgad Institute of Technology and Science, Pune
[3] Shivani Deshpande, Department of Computer Engineering & Sinhgad Institute of Technology and Science, Pune
[4] Sandeep Chitalkar, Department of Computer Engineering & Sinhgad Institute of Technology and Science, Pune

---***---

Abstract - Ensuring the security of transactions is currently one of the biggest challenges facing banking systems. The use of biometric authentication of users attracts huge sums of money from banks around the world due to their convenience and acceptance. Especially in offline environments, where face images from ID documents are matched to digital selfies. In fact, comparisons of selfies with IDs have also been used in some broader programs these days, such as automatic immigration control. The great difficulty of such a process lies in limiting the differences between comparative facial images given their different origins. We propose a novel architecture for cross-domain matching problem based on deep features extracted by two well-referenced Convolutional Neural Networks(CNN).

***Key Words*:** Convolutional Neural Networks (CNN), Face Bank, automatic immigration control, Digital selfies, Face-to-face comparison problem

1.INTRODUCTION

Human face detection is the most promising field of image processing that has a vast area of research oriented real life applications. In the real world the concept is widely used for the content annotation, access control, profiling and potential discrimination in the web world. There is always constructive scope of new inventions in the field of technology which is as vast as galaxy on its own. This leads to the better future. There has been a supportive development in the field of technology by the humans since the beginning of mankind. The motive was in rapid development and also in the advancement of technology to ensure the minimization of risk that is prone along with the new inventions which would make life easier, better and much faster. The main intention of face detection is to find out the human face in the given input. The Psychological process of locating the human face in the visual frame is also possible. It is also categorized as a special case of object class detection. The Eigen face approach is considered as a promising technique of face detection. In the field of marketing the facial image detection is playing a role of huge interest for the users. It has always been an issue of personal authentication that needs to be fixed for the purpose of access control of the info-security in the wider context via physical security. Researchers found that the face detection is an issue that needs to be taken into consideration. In terms of appearance, human face has high degree of variability, making it a dynamic object of study. Application of face detection is found in crowd surveillance, video conferencing, biometrics etc. The concept of human face detection makes it difficult for computer vision. Detected face is stored with high level of secrecy and certainty. Assuring that the data is safe, is the most important aspect under discussion. The image data consists of properties associated with, such as high level of redundancy, bulk capabilities and also high correlation between the pixels.

2. Body of Paper

This is a type of Website which can be run on desktop PC or a laptop. We can use an external webcam mounted near a system or built in camera to capture image and recognize a face.

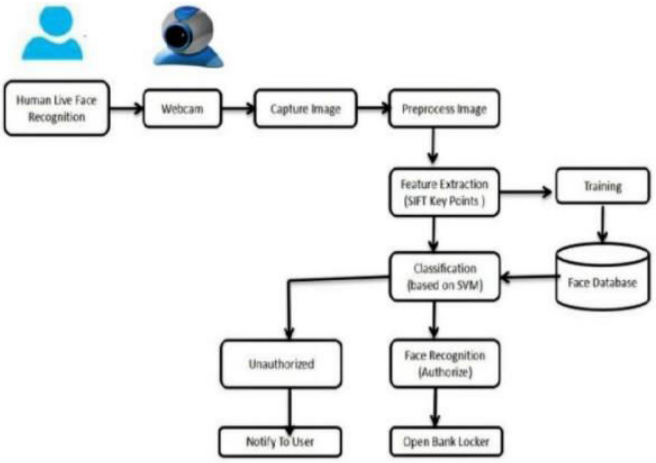

Human Live Face Recognition
Webcam
Capture Image
Preprocess Image
Feature Extraction (SIFT Key Points)
Training
Classification (based on SVM)
Face Database
Unauthorized
Face Recognition (Authorize)
Notify To User
Open Bank Locker

Fig-1. System Architechture

In this Figure we are going to implement eye-blink detection and face recognition Based on LBPH algorithm. The algorithm works in real time through webcam and displays the person name.

- Detect faces in each frame generated by the webcam.
- For each detected face, detect eyes.
- Detect liveness of the face i.e. eyes are blinking or not.
- Recognize face and access the respected locker of the user.

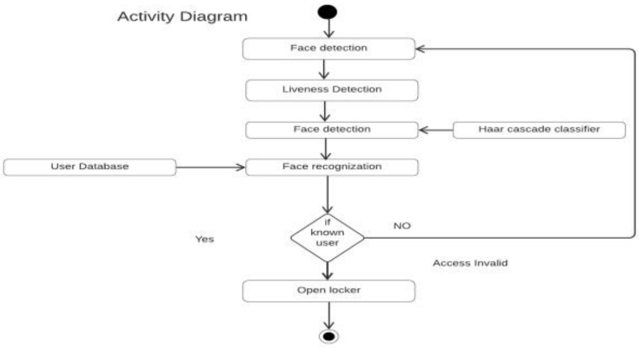


Fig-2. Activity Diagram

In this Figure demonstrates Behavior of the system and also the control flow of from start to end showing the various decision paths that exist while the activity is being executed.

3. RESULT

- Intelligent Video Surveillance Based on Object Detection implemented successfully.
- The Image, Video upload and check functionality is working in proper condition.
- Authorized User is detected by using algorithm.

The following snapshots are the final results that are implemented on the app and all GUI, and functionalities of the app is shown in the snapshots from login to sign up and all main functions of apps are shown in Fig-3, Fig-4.

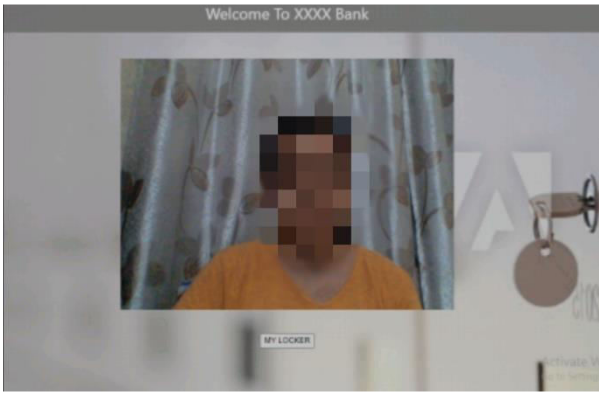


Fig-3. Recognizing Face

In above Fig-3, Recognition of face is done by feature extraction by getting pixels to provide effective information that is useful for distinguishing between faces of different persons. It basically compares the input facial image with all facial images from a dataset with the aim to find the user that matches that face.

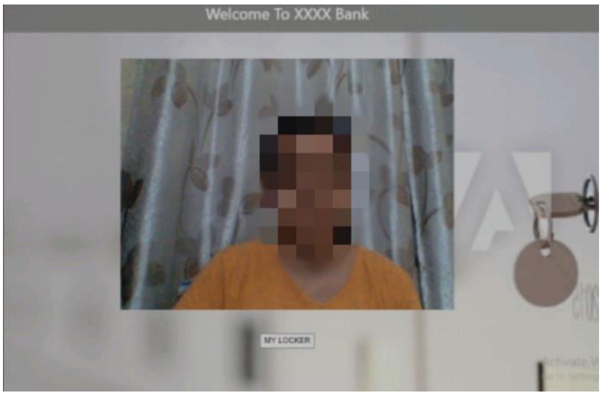
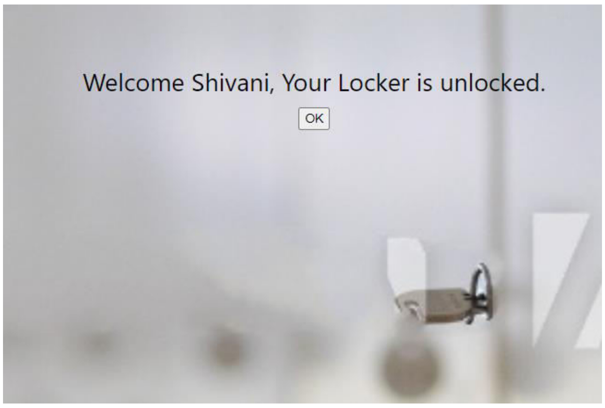


Fig-4. Eye-Blink Recognition

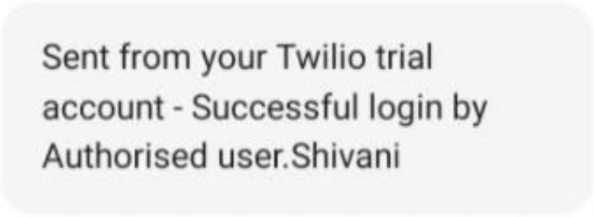
From above Fig-4, Eye-Blink recognition is done for liveness detection to avoid spoofing attack.



Welcome Shivani, Your Locker is unlocked.

Fig-5. Locker Unlocked

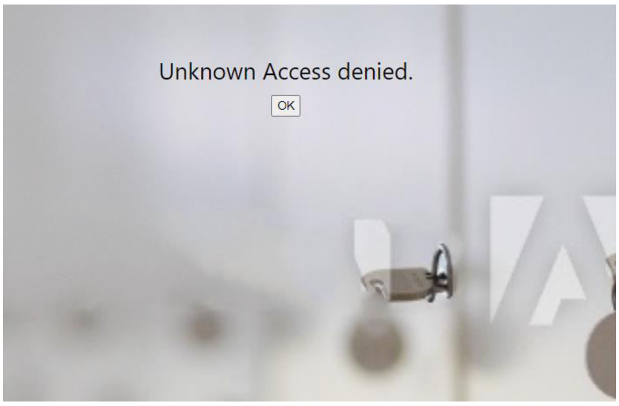
Above figure indicates that face is detected and matched with old dataset then locker is unlocked and granted access to authorized used.



Sent from your Twilio trial account - Successful login by Authorised user.Shivani

Fig-6 SMS for known access

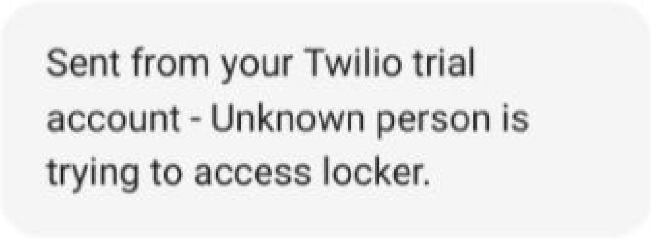
This above sms is sent when user logs in successfully to locker system.



Unknown Access denied.

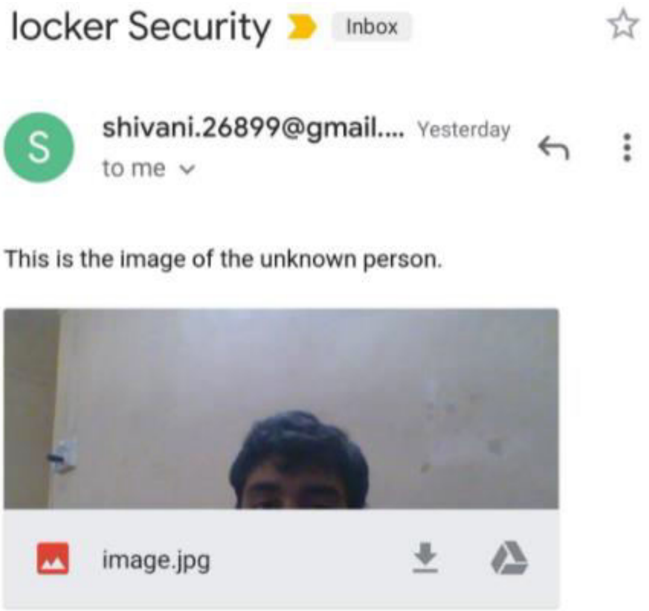
Fig-7. Unauthorized Access

Here above Fig-6, is showing unknown access denied when unknown user is trying to access locker.



Sent from your Twilio trial account - Unknown person is trying to access locker.

Fig-8. SMS for unknown access



locker Security Inbox

shivani.26899@gmail.... Yesterday
to me

This is the image of the unknown person.

image.jpg

Fig-9. Mail of Unauthorised access

From the above Fig-8, Fig-9 SMS and Mail having image is sent to Authorized user when unknown person tries to access the locker which is of other person.

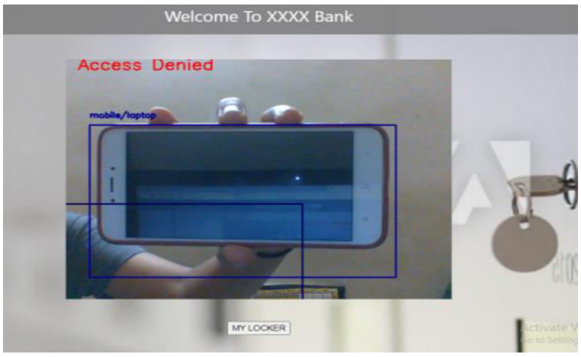


Fig-6. Mobile/Laptop Detected

Above Fig-5, describes the locker is unlocked when authorized live user is detected by the system.

3. CONCLUSIONS

In this project, we have proposed a machine learning based face detectionrecognition and liveness detection for bank locker. Using this System user will use bank locker by using face detection and liveness technique. This face detected locker is much better than traditional locker because it does not require any traditional key to unlock the locker. It is highly reliable system to ensure the security of our valuables.

ACKNOWLEDGEMENT

We express our gratitude to my guide Prof. S. M. Chitalkar for his competent guidance and timely inspiration. It is our good fortune to complete our

Project under his able competent guidance. This valuable guidance suggestions, helpful constructive criticism, keep interest in the problem during the course of presenting this Banking Security Systems by Cross-Domain Deep Face Matching project successfully. We would like to thank our Project Coordinator Prof. T. D. Khadtare and all the Teaching, Non-Teaching staff of our department. We are very much thankful to Prof. Mrs. G. S. Navale, Head of the Department of Computer Engineering and also Dr. S. D. Markande, Principal, Prof. S. A. Kulkarni, Vice principal, Sinhgad Institute of Technology and Science, Narhe for their unflinching help, support and co- operation during this project work. We would also like to thank the Sinhgad Technical Educational Society for providing access to the institutional facilities for our project work.

REFERENCES

1. G. Kim, S.Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim " Face liveness detection based on texture and frequency analyses" 5th IAPR International Conference on Biometrics (ICB), New Delhi, India. pp. 67-72, March 2012.
2. J. Maatta, A. Hadid, M. Pietikainen, "Face Spoofing Detection From Single images Using Micro Texture Analysis" Proc. International Joint Conference on Biometrics (UCB 2011), Washington, D.C., USA.
3. sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, Sangyoun Lee, " Face liveness detection using variable focusing" Biometrics (ICB), 2013 International Conference on, On page(s): 1 – 6, 2013.
4. K. Jee, S. U. Jung, and J. H. Yoo, "Liveness detection for embedded face recognition system, International Journal of Biological and Medical Sciences" vol. 1(4), pp. 235-238, 2006.
5. Wei Bao, Hong Li, Nan Li, and Wei Jiang "A liveness detection method for face recognition based on optical flow field, In Image Analysis and Signal Processing"2009, IASP 2009, International Conference on, pages 233 –236, April 2009.
6. W. Yin, Y. Ming, and L. Tian "A face anti-spoofing method based on optical flow field," in International Conference on Signal Processing Proceedings, ICSP, 2017, pp. 1333–1337.
7. Z. Lu, X. Wu, and R. He "Person identification from lip texture analysis" in International Conference on Digital Signal Processing, DSP, 2017, pp. 472–476.
8. an, J.Y.; Li, S.L.; Zhai, Y.K.; Liu, C.Y. "3D convolutional neural network based on face anti-spoofing." In Proceedings of the International Conference on Multimedia and Image Processing, Wuhan, China, 17–19 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.