IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115124

Anti-Spoofing Based Secured Transaction Using Facial Recognition And 2FA

Anukul Muley[1], Akash Bendre[2], Priti Maheshwari[3], Shanmukh Kumbhar[4],

Prof. Bhagyashree Dhakulkar[5]

[1-4]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Maharashtra, India

[5]Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Maharashtra, India

Abstract: People now-a-days utilize Automated Teller Machines (ATMs) in large numbers. People rely on ATMs to meet their daily demands in a convenient manner. As it is a crucial aspect, security is a must. ATMs are automated teller machines that allow clients to deposit or withdraw money from banks. It has been discovered that the frequency of crimes involving ATMs has increased, necessitating the need for improved ATM security. RFID technology, fingerprint, facial recognition, iris scan, OTP, reference number, random keypad, and other technologies are all utilized to ensure the security of ATM machines. In a standard ATM system, card and PIN numbers are required for authentication, which causes security issues like lost cards, stolen pin numbers, card cloning, shoulder surfing, fake keyboard, skimming, etc. This paper mainly focuses on the implementation of Anti spoofing based facial recognition for ATM system using liveness detection.

Keywords: ATM, Liveness Detection, Facial Recognition, Landmark Detection, OTP.

1. INTRODUCTION

Automated Teller Machines (ATMs) have enhanced a basic fact of our existence. It plays a vital act in our regular transactions. An ATM is an e-banking machine that admits clients to complete elementary transactions without going to the bank. Anyone with a credit card or debit card can get cash from an ATM at any time by following a few easy steps.

The first ATMs came in 1967 on the street in Enfield, London at a branch of Barclays Bank, and immediately they have grown in number to over 2 million global. When the investment sector introduced ATMs the habit of credit and debit cards has raised during the whole of the world. Banks had decreased their foundation costs by presenting Automatic Teller Machine (ATM) and Internet websites by which the customer's transactions will carry out easily and in a smooth way. ATM is a digital machine mainly used for gaining approach to different banking services anywhere without the assist of any financial institution staff.

The users prefer ATMs for all physical transaction purposes, like money withdrawal and money deposit without going to the bank. In ATMs, the user experience has become a critical component that banks must deliver. However, this might lead to an increase in robberies and attacks on ATMs and internet banking using a variety of fraudulent tactics. However, technical advancements in the financial sector provide better security against fraudulent activity.

However, there are various technologies like RFID technology, fingerprint, face recognition, iris scan, OTP, reference number, random keypad, and other technologies that are utilised to ensure security for ATM machines. In a standard ATM system, Card and PIN numbers are used for authentication and security is a major problem, with issues such as lost cards, stolen pin numbers, card cloning, shoulder surfing, false keyboards, skimming, and eavesdropping etc.

ATM skimming is a way of action payment card fraud in which the fraudsters try to ransack PINs and additional main facts by rigging machine accompanying secret record device.

Card shimming is an attack that involves inserting a very tiny device containing a microprocessor and flash memory into a card reader or ATM to collect user data. The information obtained this way is subsequently sold on the Internet or used to clone magnetic strip cards.

In an Eavesdropping attack, a small hole is being made in the ATM device or approach gained to the top box of the ATM device by which electronic links are then attached straightforwardly to the card reader that helps them to capture card and PIN details. These problems gave rise to biometric-based ATMs. As biometrics are unique for each consumer, further making the ATMs more impenetrable.

We proposed a biometric system that uses a unique trait or characteristic enables automated authentication for any user to stop these frauds - card cloning, shoulder surfing, fake keyboard, skimming, etc.

DOI: 10.17148/IJARCCE.2022.115124

2. LITERATURE REVIEW

Anukul Muley, Akash Bendre, Priti Maheshwari, Shanmukh Kumbhar, Prof. Bhagyashree Dhakulkar (2022). In this paper, the authors have discussed about all the previous approaches that have been tried and implemented in biometric based ATM system which is more likely to use RFID tags, facial recognition, fingerprint and IRIS.

Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar(2018). The authors have proposed the concept of Fingershield ATM, a biometric identification in the form of the fingerprint is implemented along with ATM which is integrated with smart card and database server. The security was much improved and guaranteed by the system.

Indranil Banerjee, Sjivangam Mookherjee, Sayantan Saha,Souradeep Ganguli,Subham Kundu,Debduhita Chakravarti (2019). The authors proposed a two-way security check. Firstly, the user inserts the RFID card after that user gives a fingerprint which is verified if there is a mismatch a message is sent to the user. If it's a match, the system further goes on with the level-2 security check i.e., the IRIS scanner, IRIS.

Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu I (2020). The paper presents the security of ATM using facial recognition. In this paper, they have used RFID reader. CCTV is used to recognize the face using haar cascade and local binary pattern and if the face will match to the database transaction will proceed otherwise link will send to user.

Darwin Nesakumar A, T Suresh, Nivedha T, K Nivedha , Priyadharshini G, P Mugilan (2020). In the proposed methodology, system using facial recognition and fingerprint. After inserting an ATM card and entering a pin, the card reader collects the details stored in the card and after capturing the face and fingerprint system will compare with the database and transaction will proceed.

S. Shukla, A.Helonde, S. Raut, S. Salode, J. Zade (2018). In the proposed method, for making any transaction, the user has to go through a two-way security procedure. When a user goes for the transaction, a new page appears in the form of the random keyboard on the screen if the user is already registered if not then a link is provided on that page for the registration.

Prakash Chandra Mondal, Rupam Deb, and Md. Nasim Adnan (2017). The author proposed a system that uses behavioral biometrics for authentication with more security. In this system, authentication is performed using three factors which include online handwriting signature verification, chip-based card, and PIN verification.

Rasib Khan, Ragib Hasan, and Jinfeng Xu (2015). The author proposes the system in which Secure PIN Authentication as a service(SEPIA) is used for authentication of the PIN for ATMs which uses cloud-connected personal mobile and wearable devices.

Sweedle Machado, PrajyotiD'silva, SnehalD'mello,Supriya Solaskar and Priya Chaudhary (2018).The proposed system uses a fuzzy vault system for the security of ATM pins and passwords using a user's fingerprint data. It involves encryption and decryption. In the encryption process, the minutiae points get extracted from the fingerprint which is encoded using a pin password. The main benefit of this system is securing ATM passwords and pin with fingerprint data.

Adrian Fernandes (2020). In the proposed system fingerprint scanner is used for authenticating the users where the user's fingerprint will authenticate it and further proceed for bank transactions.

Dimaunahan, Ericson D, Ballado, Alejandro H, Cruz, Febus Reidj G, Dela Cruz, Jennifer C (2017).The author proposed voice identification along with fingerprint authentication as a solution to existing ATM security for visually impaired users. By using fingerprint authentication and voice recognition to perform ATM transactions, adds two tiers of security, and also provided ease of use of the system for people with visual impairments.

R.D.Salagar, Akshata Patil (2014). In the proposed method, iris recognition is discussed by using MATLAB software. Here, Firstly input of eye images are uploaded from the database, and further region of interest segmentation and localization of iris using canny edge detection is performed successfully. Hence, this proposed system not only ensures security but it also gives easy accessibility to people with visual impairments.

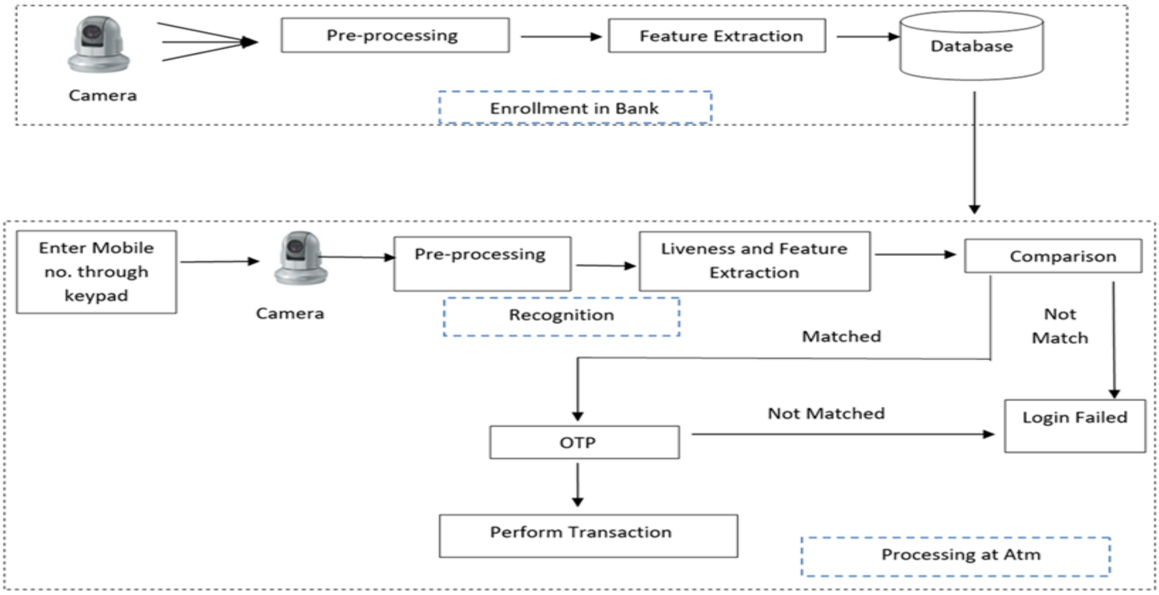
Khushboo Yadav, Suhani Mattas, Lipika Saini (2020). The author proposed a Secure Cardless Transaction System- a method which would eliminate the usage of ATM PIN and physical cards altogether and hence provide a secure environment for cash withdrawal.

Dr. V. Gokula Krishnan. M.Tech. Ph.D, G.N. Kirran, K.P. Deepkarasan, J. Kishore Kumar, (Sep 2020). The proposed paper is a subset of biometric authentication techniques and their deployment possibility in banking applications. It uses a face recognition technique for verification in the ATM system. The author implements a new generation ATM machine that can be operated without the ATM card.

B. Saranraj, N. Sri Priya Dharshini, R. Suvetha, K. Uma Bharthi, (IEEE 2020). The author has proposed a mechanism for the enhancement of ATM security by using Arduino. In the proposed methodology, researchers used two processes, i.e., Arduino Nano along with fingerprint and OTP mechanism. Users can perform transactions either by entering OTP (in the absence of original account holder) or through biometrics (in the presence of original account holder).

DOI: 10.17148/IJARCCE.2022.115124

3. SYSTEM ARCHITECTURE



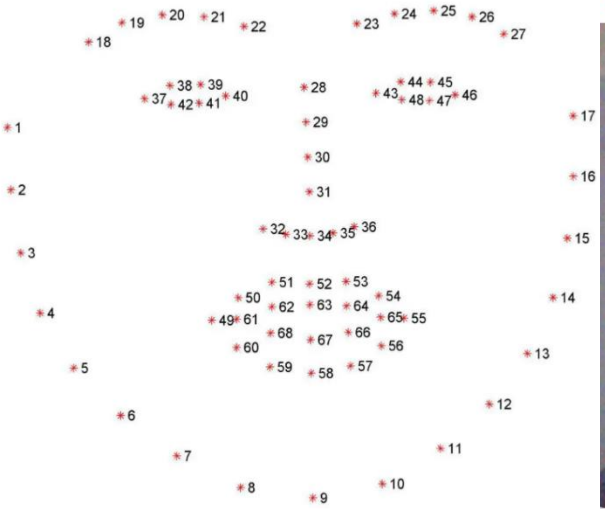
SYSTEM ARCHITECTURE

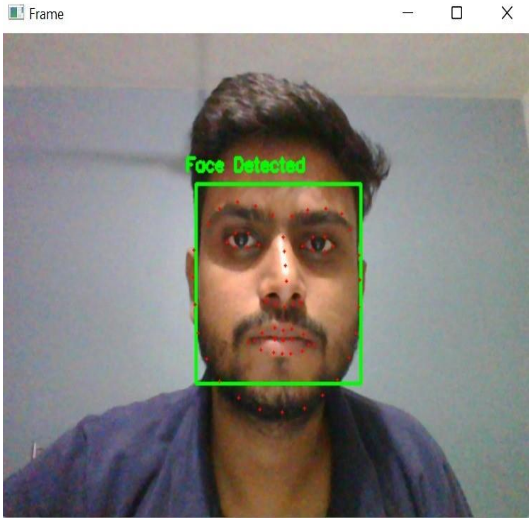
Enrollment at Bank-
User should register themselves in bank database through face, mobile number , account number , valid email id and all other details. Face is captured through landmark and face data will go for preprocessing i.e. the technique of preparing the raw data to make it suitable for a training and after that it will go for feature extraction i.e the process of transforming the raw data into numerical features that can be used to preserve the information in the original data set. After the registration process is completed, user's account is created in the bank database. The registration process is done at Bank side and all the data will be saved in bank database.

Processing at ATM-
After the registration process, the user will enter their registered mobile number through keypad in ATM and after that a window will open for capturing the user's face and face data will go to system for pre- processing then it will go for liveness detection i.e., the ability of a system to detect if a face is real (if a live person is present at the point of capture) or fake (from a spoof artifact or lifeless body part). If the face gets matched then the verification of user is done and one time password (6-digit OTP) will be sent to the user's mobile number. After entering the valid OTP, a window will open for the transaction in ATM otherwise if face is not matched or wrong OTP is entered either in any of the case the login will be failed.

4. FACE RECOGNITION-

Face landmark detection is a computer vision task where we want to detect and track key points from a human face. For example, we can use the key points for detecting a human's head pose position and rotation. Facial landmarks are used for the purpose of localizing and representing salient regions of the face, such as: Eyes, Eyebrows, Nose, Mouth, Jawline etc.
Facial landmarks are successfully applied to face alignment, head pose estimation, face swapping, blink detection, etc.
Facial recognition is task of identifying of a face during a photo or video image against a pre-existing database of faces. It begins with detection - distinguishing human faces from other objects within the image - then works on identification of the detected faces.





Firstly, at the time of registration we are using 68 Landmarks of the face to recognize the face properly and store it in database for further process.

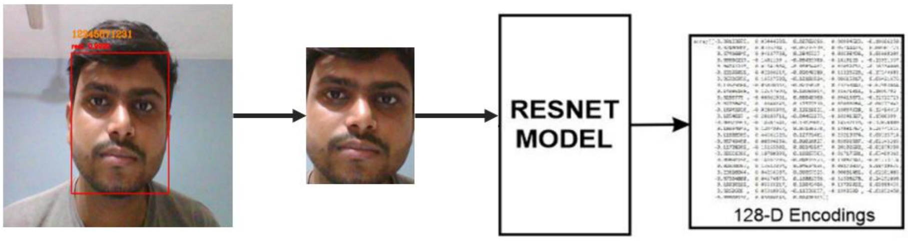
The approach we are using for face recognition is easily understood and straight forward. The motive here is to get a deep neural network to produce a bunch of numbers that describe a face (known as face encodings). When you pass in two different images of a similar person, the network should return similar outputs (i.e., closer numbers) for both images, whereas once you pass images of two different people, the network should return different outputs for both images.

This means that the neural network must be trained to automatically identify different features of faces and calculate numbers based on that. The output of the neural network is often thought of as an identifier for a specific person's face — if you pass in several images of an equivalent person, the output of the neural network is going to be very similar/close, whereas if you pass in images of an any other person, the output will come very different.

We don't have to go through the hassle of training or to build our own neural network. Here we have access to a trained model through dlib . Dlib library is helpful for facial landmark detection. The pre-trained facial landmark detector inside the dlib library is used to deliver location of 68 (x, y)-coordinates that maps to facial structures on the face. Cv2 ilibrary is used perform operations on the image. Imutils Face Aligner is used to align the different orientations of faces so that all the faces are forward looking faces. We will be storing the 128 dimensions of face encodings which we get from the face encoder from all the training images into the faces list and the corresponding labels in the name list.

We have set a confidence threshold of 0.5 here. Any detection which has a confidence value above 0.5 will be taken as the face image and will be taken forward to the Face Aligner for aligning the face. Then we'll drop out the landmarks from the aligned face and pass the aligned face a well as landmarks to the face encoder which is called as pre trained Resnet model. The pre trained model will give us the (128,1) dimension encoding for all the pictures and we will keep appending the output with the label to the faces, name list respectively.

In simple terms, it takes the number of outputs (face encodings) when we pass in the image of someone's face; by comparing the face encodings of known faces with those from test images which tells who is in the picture.



5. LIVENESS DETECTION:

In real time, if we implement the facial recognition-based ATM system then the major problem the user will encounter is of getting spoofed.

As we know the face recognition system can be spoofed in the different ways like for example by showing user's image or video.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 7.39 ⁙ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115124

Attackers can use these techniques to bypass the recognition system, in order to overcome here we can use the liveness detection.

Liveness detection is a feature that helps us to identify/ distinguish between real and fake face or we can say it helps us to find difference between live human and its fake representation.

It is trained using Convolutional Neural Network Binary Image Classifier.

Binary Image Classifier is the type of classification where the output is either 0 or 1.

Here, we have used it to detect where the user is real or fake.

Let's understand how the dataset is built for the liveness detection.

We have recorded 20 seconds video from the mobile where facial features are captured properly.

Then we replayed the same video and recorded it using desktop/laptop.

So, these two videos just make simple basic dataset. Similarly, we have recorded other attacks.

We have labelled video captured by mobile as real and of desktop/laptop as fake (Note: This naming convention were used for better understanding).

Once the dataset was built, it was feeded to the neural network where the actual training is done.

And based on that model gives prediction/output whether user is real user or fake user.

Once the dataset is built then on both the set of videos (real & fake) face detection is applied to extract the face ROI.

Let's now understand how ROI is extracted. or the procedure of extracting ROI is as follows:

First the input video is provided to the face detector. Then the rectangular box is created around the face to capture the features. Once this is done, then we crop the face from the frame and save it at the destination folder which ultimately creates the ROI.

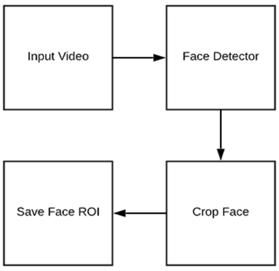


Fig. Extraction of ROI

Liveness detector:

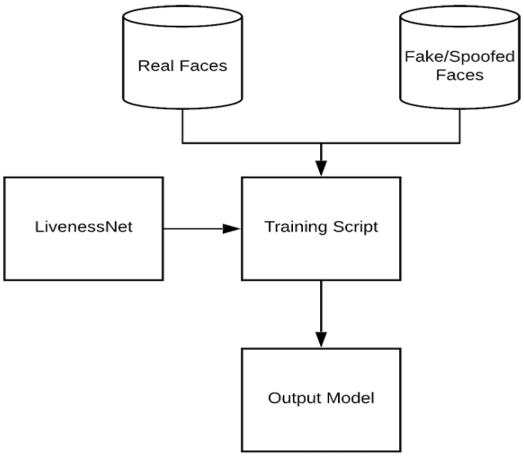


Fig. Liveness Detector

Now, we will create the liveness detector. To do so, we will require dataset of real faces and fake faces.

Next step is to feed the dataset to training script along with LivenessNet. LivenessNet is actually just a simple Convolutional Neural Network (CNN) model which is used to detect face liveness in images and videos. Here, the actual training part takes place.

Model is trained using OpenCV, Keras, and deep learning.

Based on input received, the training is done and the final output model is produced. The output model predicts whether the image is real or fake.

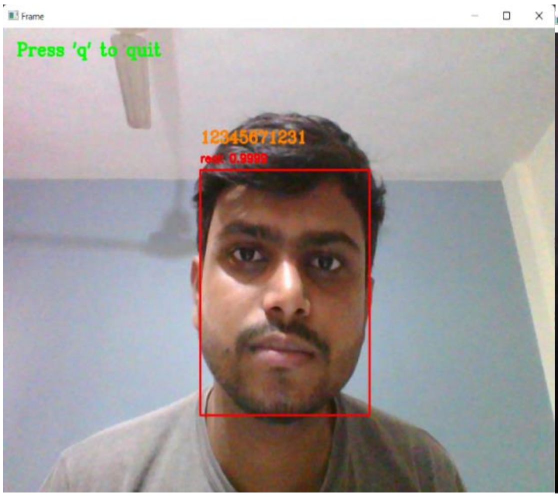
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⚟ Impact Factor 7.39 ⚟ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115124

In this way, we have achieved the liveness detection.

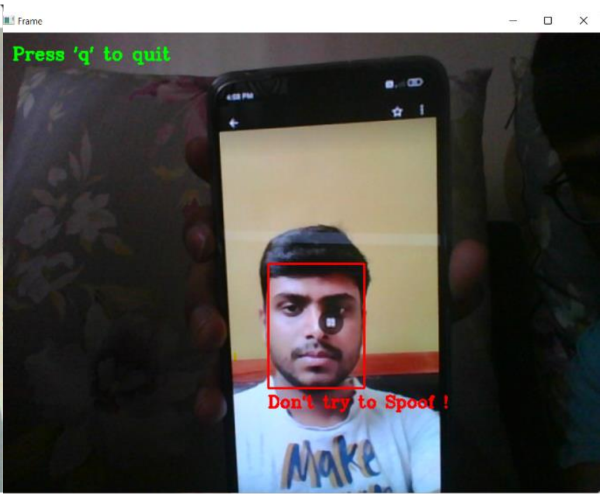


Press 'q' to quit

12345671231

real: 0.9999

Image: When Real User present



Press 'q' to quit

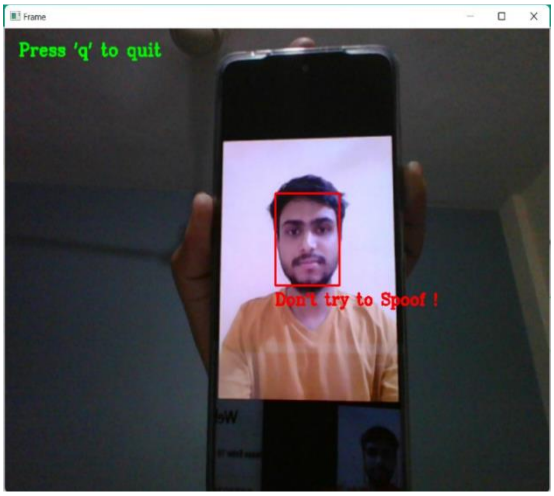
Don't try to Spoof !

Image: Spoofing of User

Attacks which are covered by the system:

1.Photo Spoofing- It is categorised into two sub attacks:

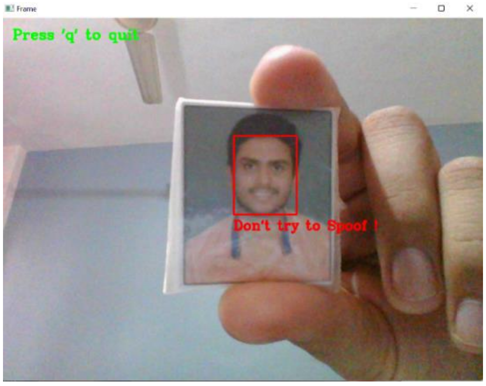
i)Digital photograph attack: Here, User's digital version of photo/pic is used to spoof the system.



Press 'q' to quit

Don't try to Spoof !

ii) Printed Photograph attack: Here, the hard copy of photo is used to spoof the system.

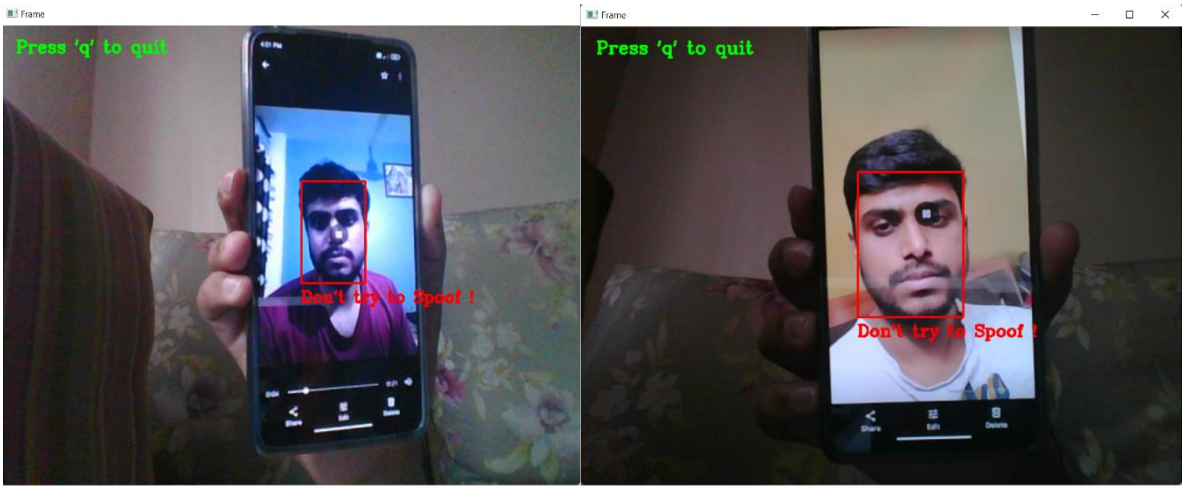


Press 'q' to quit

Don't try to Spoof !

2)Video Spoofing – In Video spoofing, User's different videos are used to spoof the system.

DOI: 10.17148/IJARCCE.2022.115124



Press 'q' to quit

Don't try to Spoof !

Press 'q' to quit

Don't try to Spoof !

CONCLUSION

In these times, every individual uses an ATM for withdrawal and transferring cash. In the past few decades, the fraudulent activities related to ATMs have also increased gradually. The existing ATM systems racked up so many hackers and fraud towards fraudulent activities such as shoulder surfing, card skimming, etc.

Hence, we have successfully worked on making ATMs more secure by implementing facial recognition as authentication for ATMs, along with this face liveness has also been used to safeguard against spoof attacks.

An additional layer of security has been provided with help of two-factor authentication using OTP.

In the future, the Liveness model can be trained on a variety of different attacks & people's faces to make the model more accurate and efficient. This system can also be implemented in many other areas for secure authentication using face.

REFERENCES:

1. Anukul Muley, Akash Bendre, Priti Maheshwari, Shanmukh Kumbhar, Prof. Bhagyashree Dhakulkar "Survey on Biometric Based ATMs", International Journal of Scientific Research in Science and Technology (IJSRST) 2021.
2. Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar (2018) "Fingershield ATM – ATM Security System using Fingerprint Authentication", International Symposium on Electronics and Smart Devices (ISESD) 2018.
3. Indranil Banerjee, Sjivangam Mookherjee, Sayantan Saha,Souradeep Ganguli,Subham Kundu, Debduhita Chakravarti "Advanced ATM System Using Iris Scanner", International Conference on Opto-Electronics and Applied Optics (Optronix) 2019.
4. Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu I "Securing ATM Transactions using Face Recognition", International Journal of Advanced Trends in Computer Science and Engineering, March April 2020.
5. Darwin Nesakumar A, T Suresh, Nivedha T, K Nivedha, Priyadharshini G, P Mugilan "Smart ATM Security Using Face Recognition", European Journal of Molecular & Clinical Medicine, April 2020.
6. Shivani Shukla, Anjali Helonde, Sonam Raut, Shubhkirti Salode, Jitesh Zade "Random Keypad and Face Recognition Authentication Mechanism", International Research Journal of Engineering and Technology (IRJET), March 2018.
7. Prakash Chandra Mondal, Rupam Deb, and Md. Nasim Adnan "On Reinforcing Automatic Teller Machine (ATM) Transaction Authentication Security Process by Imposing Behavioral Biometrics", 4th International Conference on Advances in Electrical Engineering (ICAEE), 2017.
8. Rasib Khan, Ragib Hasan, and Jinfeng Xu "SEPIA- Secure PIN Authentication as a service for ATM using Mobile and wearable devices",3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering ,2015.
9. Sweedle Machado, Prajyoti D'silva, Snehal D'mello, Supriya Solaskar and Priya Chaudhary "Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System", IEEE 2018.
10. Adrian Fernandes "Biometric ATM", International Journal for Research in Applied Science & Engineering Technology (IJRASET) 2020.
11. Dimaunahan, Ericson D, Ballado, Alejandro H, Cruz, Febus Reidj G, Dela Cruz, Jennifer C. "MFCC and VQ Voice Recognition Based ATM Security for the Visually Disabled", IEEE 9th International Conference on Humanoid,

DOI: 10.17148/IJARCCE.2022.115124

Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM),2017.

12. R.D.Salagar, Akshata Patil (2014). “Voice Enabled ATM Machine With Iris Recognition For Authentication”, 3rd IRF International Conference 10th May-2014.
13. Khushboo Yadav, Suhani Mattas, Lipika Saini, “Secure Card-less ATM Transactions”, First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA), 2020.
14. Dr. V. Gokula Krishnan. M.Tech. Ph.D, G.N. Kirran, K.P. Deepkarasan, J. Kishore Kumar, “face detection-based ATM safety system in IOT using secure transaction”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 09 | Sep 2020.
15. B. Saranraj, N. Sri Priya Dharshini, R. Suvetha, K. Uma Bharthi, “ATM Security System Using Arduino”, International Conference on Advanced Computing & Communication System (ICACCS), pp 940-944, IEEE 2020.