WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Real Time Face Recognition in ATM for Security System

Prof. Bhagyashree Kadam[1], Mr. Kishor Dukr[2], Mr. Vaibhav Kumbhar[3], Mr. Shivraj Sakunde[4], Mr. Akash Jadhav[5]

[1]*Information Technology*
[2]*Information Technology*
[3]Information Technology
[4]Information Technology
[5]Information Technology

ABSTRACT

Face recognition play a vital role in variety of applications from biometrics, surveillance, security, identification to the authentication. Rather than a PIN or ATM card. Given that the combination of these biometrics has proven to be the finest among identification and verification procedures, The Face ID is given top attention in this situation. The use of ATMs raises the problem of unauthorised persons having access to them with a valid authentication code. By contrasting the photos captured in front of the ATM with those already stored there, users are confirmed. The new photograph is utilised to train the model for even greater accuracy if the user is real. In order to process the image that was obtained and to identify the faces in the image, this system employs OpenCV and the Haar Cascade Classifier. Using a local binary pattern, facial recognition is performed.

Keywords – Face detection, Feature extraction, tracking, Machine Learning.

INTRODUCTION

Human face detection is the most promising field of image processing that has a vast area of research oriented real life applications. A computerised device known as an automatic teller machine (ATM) is used to withdraw money from a customer's specific bank account. As more and more financial users choose ATMs for cash withdrawals, cash deposits, and other transactions, banks are putting a lot of effort into ensuring that ATMs are secure. Therefore, ATMs should be properly secured against criminal activity and other unwanted objects. Future innovations are being constructed with robust security due to the quick advancement of science and technology. On the other hand, there are also threats made to undermine this level of security. Even though increased automation has generally had a positive effect, thefts and frauds continue to occur in a variety of financial institutions like banks and applications like ATMs. The current ATM paradigm employs a card and a PIN, which makes it more vulnerable to assaults including stolen cards, PINs that are statically assigned, duplicate cards, and a variety of other threats. Then PIN hacking becomes a significant issue. Other fraudulent attacks include user blackmailing, spoofing, brute force attacks, and eavesdropping. The worst-case scenario also includes the possibility of ATM robbery.

First, when a user approaches an ATM machine, a live image is taken using a web camera connected to the system designated as the ATM system, and this image is compared to images saved in the database. An OTP will be delivered to the associated registered cell phone number. The transaction can move forward if the user inputs the OTP accurately. Therefore, the likelihood of fraud is significantly decreased by the use of a face recognition algorithm, OTP. Deep learning-based linear discriminate classification is used in order to get greater accuracy. Likewise carried out in OS.

PHASE DESIGN

System board serves as the system's primary processor. The system is where the specific operating system that works with the system is kept board. The Web Camera, which can be connected directly to the System Board, records the Human Face. The user interface messages are displayed on the monitor.

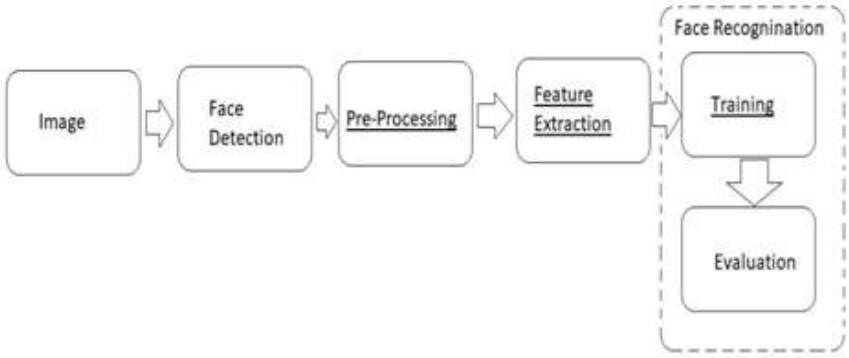


Fig. System Flow

To train the classifier, the method requires a large number of positive images (images of faces) and negative images (images without faces). Then, features must be extracted from it. Features are nothing more than numerical data that is extracted from images and used to differentiate one image from another; for instance, the histogram (distribution of intensity values) is one of the features that can be used to define a number of characteristics of an image even without actually looking at it, such as whether it is dark or bright, the intensity range of the image, contrast, and so forth. Face detection can be done effectively by using Haar characteristics. Similar to the convolution kernel, these properties. Finding a WebEx in the image and cropping a portion of the source image with the chosen Webxel at its centre has the same dimensions as the convolution kernel to represent the convolution. Calculate the element-wise product between the kernel and subimage values. The product's outcome should be added. Put the calculated value in the new image at the same location as you set up the Webxel. The algorithm requires a large number of positive images (images of faces) and negative images (images without faces) to train the classifier. Each feature is a single value derived by subtracting the total of the features. Then, features must be extracted from it. Features are nothing more than numerical data that is extracted from images and used to differentiate one image from another; for instance, the histogram (distribution of intensity values) is one of the features that can be used to define a number of characteristics of an image even without actually looking at it, such as whether it is dark or bright, the intensity range of the image, contrast, and so forth. It is effective to detect faces by using Haar characteristics. These characteristics closely resemble the convolution kernel. A Webxel from the image can be used to summarise the convolution. The Webxel is then cropped from the source image so that it is the same size as the convolution kernel. Calculate a product between the kernel and subimage values on an element-by-element basis. Add the product's outcome. At the same location where you Webcked up the Webxel location, insert the resulting value into the new image. The sum of the Webxels beneath the white rectangle and the sum of the Webxels under the black rectangle are subtracted to provide a single value for each feature. Now, numerous features are calculated using all feasible sizes and locations for each kernel. Find the Webxels' total under the white and black rectangles in order to calculate each feature. To tackle this, the integral image notion is quite helpful. Integral pictures are ones in which the sum of all Webxels that came before the current Webxel is represented by the Webxel value at any (x,y) location.

ALGORITHM

Convolution Neural Network

Step1: Select the dataset.

Step2: Perform pre-processing, feature selection.

Step3: Apply Classification algorithm CNN

Step4: Calculate each Feature fx value of input layer

Step5: Calculate bias class of each feature

Step6: The feature map is produced and it goes to forward pass input layer

Step7: Calculate the convolution cores in a feature pattern

Step8: Produce sub sample layer and feature value.

Step9: Input deviation of the kth neuron in output layer is Back propagated.

Step10: Finally give the selected feature and classification results.

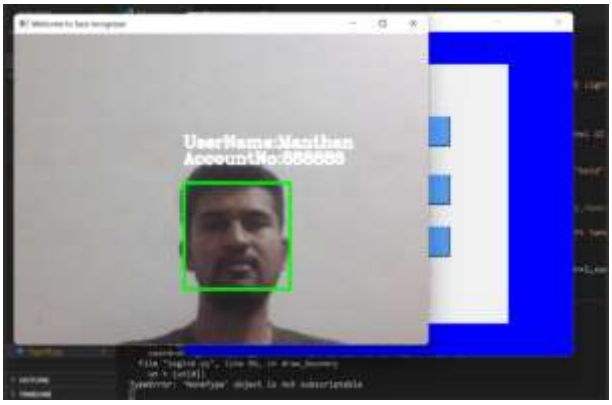
METHODOLOGY

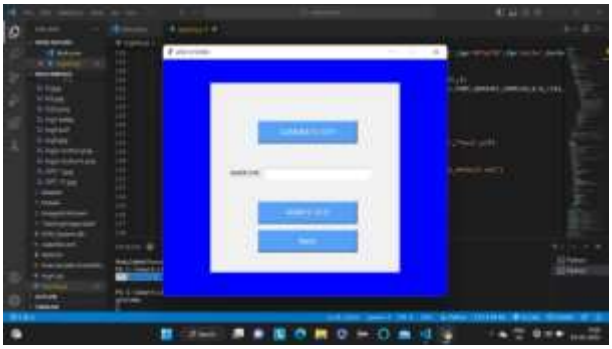
First, when a user approaches an ATM machine, a live image is taken using a web camera connected to the system designated as the ATM system, and this image is compared to images saved in the database. An OTP will be delivered to the associated registered cell phone number. The transaction can move forward if the user inputs the OTP accurately. Therefore, the likelihood of fraud is significantly decreased by the use of a face recognition algorithm, OTP. Deep learning-based linear discriminate classification is used in order to get greater accuracy. Likewise carried out in OS.

1) Data gathering: Collect face information (in this case, face photos) on the individuals you want to identify.
2) Train the Recognizer: Provide the recognizer with the face data as well as the names of each face so that it can learn.
3) Feed fresh images of those persons to the face recognizer you previously trained to see if it can identify them.

Two face recognizers are included with OpenCV.

OUTPUT





CONCLUSION

To a certain extent, facial recognition has shown to be one of the biometric technologies with the highest level of security for preventing ATM robberies and providing protection for ATMs. It takes the place of the conventional ATM system. It provides benefits including reducing card production costs and removing shortcomings of the conventional method such carrying the ATM card, losing the card, receiving fraudulent calls involving the ATM card, etc.The rate of efficacy of the system can be increased using new, enhanced techniques in artificial intelligence that help remove additional disturbances and distortions.

FUTURE SCOPE

Military applications, high security businesses, and real-time security applications like ATM security systems. This is applicable to bank locker access as well. A crucial aspect that must be considered is the lighting that the system provides. Utilising quick computers can increase productivity.

REFERENCES

1. J.J.Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International Conference for Convergence in Technology (I2CT), 2017.
2. M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features",International Conference on Advanced Computing Tech- nologies and Applications (ICACTA), 2015.
3. Sivakumar T. 1 , G. Askok 2 , k. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions, Volume 3, Issue 1, 2013.
4. C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", Interna- tional Journal of Research in Engineering, Technology and Science, Volume VII, Special Issue, Feb 2017.
5. Manoj V , M. Sankar R , Sasipriya S , U. Devi E, Devika T , "Multi Authentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and Technology (IRJET).
6. L. Wang,H. Ji, Y. Shi, " Face recognition using maximum local fisher discriminant analysis",18th IEEE International Conference on Image Processing, 2011.
7. K.Shailaja and Dr.B.Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification ", IEEE International Conference on Computational Intelligence and Computing Research, 2016.
8. H. R. Babaei, O. Molalapata and A.H.Y Akbar Pandor, "Face Recognition Application for Au- tomatic Teller Machines (ATM)", International Conference on Information and Knowledge Manage- ment (ICIKM), 2012.
9. https://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec-tutorial.htmlface-recognition
10. Face recognition using OpenCV and Python: A beginner's guide - Blogs - SuperDataScience | Machine Learning | AI | Data Science Career | Analytics | Success