iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52401

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

ATM Based Face Recognitions System

Shlok Kailas Khopkar[2], Jayesh Datary Kharat[3], Rutuja Rameshwar Zori[4], Ruchita Jayawant Kakade[5], Prof. Arunadevi Khaple[1]
Department of Computer Engineering, Zeal College of Engineering and Research, Pune

Abstract: Automated Teller Machines are widely used nowadays by people. But it's hard to carry their ATM card everywhere, people may forget to have their ATM card or forget their PIN number. The ATM card may get damaged and users can have a situation where they can't get access to their money. In our proposal, use of biometrics for authentication instead of PIN and ATMcard is encouraged. Here, The Face ID is preferred to high priority, as the combination of these biometrics proved to be the best among the identification and verification techniques. The implementation of ATM machines comes with the issue of being accessed by illegitimate users with valid authentication code. The users are verified by comparing the image taken in front of the ATM machine, to the images which are present in the. If the user is legitimate the new image is used to train the model for further accuracy. This system uses open CV to process the image being obtained and Hear Cascade Classifier to detect the faces in the image. The face recognitions done using Local Binary Pattern.
Keywords: Heer cascade, Automatic Teller Machine, Webxel, Machine learning, Eigen Faces, Fisher Faces

I. INTRODUCTION

An Automatic Teller Machine (ATM) is a computerized machine that is used to withdraw cash from a customer's respective bank account. As financialusers prefer ATM for cash withdrawals, cash deposits and many other transaction, the banks are focusing a lot over the security of ATMs. Hence ATM should be protected properly from the criminal activities or from any unwanted things.

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats. Then another major problem is hacking of PIN. There are other fraudulent attacks like eavesdropping, spoofing , brute force attacks, blackmailing the user. In the worstcase there can also be ATM machine Robbery.

An Automatic Teller Machine (ATM) is a computerized machine that is used to withdraw cash from a customer's respective bank account. As financialusers prefer ATM for cash withdrawals, cash dposits and many other transaction, the banks are focusing a lot over the security of ATMs. Hence ATM should be protected properly from the criminal activities or from any unwanted things.

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats. Then another major problem is hacking of PIN. There are other fraudulent attacks like eavesdropping, spoofing , brute force attacks, blackmailing the user. In the worstcase there can also be ATM machine Robbery.

To overcome these problems, the project 'ATM Security system based on Face recognition, PIN andOTP' consists of conventional features ie is Personal Identification Number (PIN) along with additional features like face recognition and one-time password (OTP) is used. Database holds information about a user's ac- count details, images of his/her face and a mobile number which will improve security to a large extent. First, the user will come to the ATM machine and a live image is captured through the Web Camera interfaced with System defining as the ATM system, which is compared with the images stored in the database. If the face is recognized, then the user is notified to type the PIN. If the PIN matches, an OTP will be sent to the corresponding registered mobile number. If the user correctly enters the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm, PIN and an OTP drastically reduces the chances of fraud. In order to obtain better accuracy deep learning based linear discriminate classification method is utilized. And executed the same in OS.

II. DESIGN PHASE

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

The system contains System board as the main processor. The system is used to contain the dedicated operating system which is compatible with the System board. The Human face is captured by the Web Camera which can be directly interfaced with the System board.The monitor displays the messages for user interface.

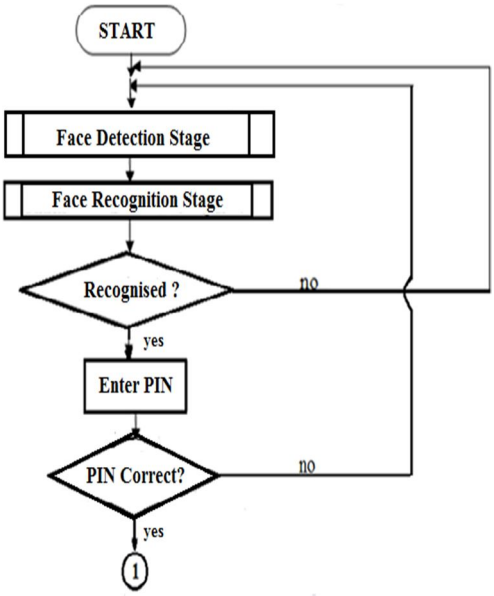


Figure: System flow

III. RECOGNITION FACE DETECTION

The algorithm needs a lot of positive images (images of faces) and negative im- ages (images without faces) to train the classifier. Then it is required to extract features from it. Features are nothing but numerical information extracted from the images that can be used to distinguish one image from another; for example, histogram (distribution of intensity values) is one of the features that can be used to define several characteristics of an image even without looking at the image, such as dark or bright image, the intensity range of the image, contrast, and so on. Using Haar features is a efficient method for face detection. These features are just like the convolution kernel.

The convolution can be summarized by locating a Webxel from the image, then crop out a sub-image with the selected Webxel as the center from the source image with the same size as the convolution kernel. Calculate an element-wise product between the values of the kernel and sub- image. Add the result of the product. Put the resultant value into the new image at the same place where you Webcked up the Webxel location.

Each feature is a single value obtained by subtracting the sum of the algorithm needs a lot of positive images (images of faces) and negative im- ages (images without faces) to train the classifier. Then it is required to extract features from it. Features are nothing but numerical information extracted from the images that can be used to distinguish one image from another; for example, histogram (distribution of intensity values) is one of the features that can be used to define several characteristics of an image even without looking at the image, such as dark or bright image, the intensity range of the image, contrast, and so on. Using Haar features is a efficient method for face detection. These features are just like the convolution kernel. The convolution can be summarized by locating a Webxel from the image, then crop out a sub-image with the selected Webxel as the center from the source image with the same size as the convolution kernel. Calculate an element-wise product between the values of the kernel and sub- image. Add the result of the product. Put the resultant value into the new image at the same place where you Webcked up the Webxel location.

Each feature is a single value obtained by subtracting the sum of the Webxels under the white rectangle from the sum of the Webxels under the black rectangle.

Now, all possible sizes and locations of each kernel are used to calculate plenty of features. Each feature calculation, requires to find the sum of the Webxels under the white and black rectangles. The concept of integral image is very useful to solve this. Integral images are those images in which the Webxel value at any (x,y) location is the sum of the all Webxel values present before the current Webxel.

©IJRASET: All Rights are Reserved

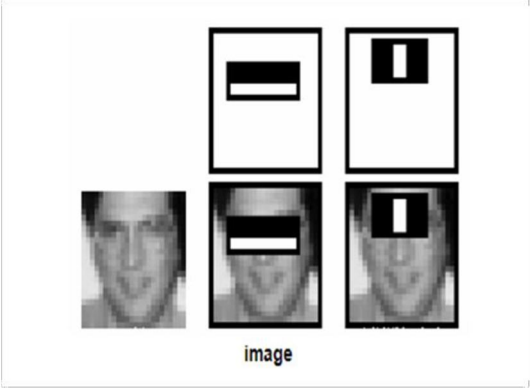


Figure: Haar cascade

A. Face Recognition

Face recognition is an easy task for humans. Face recognition based on the geo- metric features of face is probably the most intuitive approach to face recognition. One of the first automated face recognition systems was marker points (position of eyes, ears, nose etc.) were used to build a feature vector (distance between the points, angle between them etc). The recognition was performed by calculating the Euclideandistance between feature vectors of a probe andreference image. Some of the latest work on geometric face recognition was, a 22-dimensional feature vector and experiments on large datasets have shown that geometrical features alone may not carry enough information for face recognition.

B. Method One Based On Machine Learning

Machine learning (ML) is the scientific study of algorithms and statistical models that computer systemsuse to effectively perform a specific task without using explicit instructions, relying on patterns and inference instead. It is seen as a sub- set of artificial intelligence. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make pre- dictions or decisions without being explicitly programmed to perform the task. Machine learning algorithms are used in a wide variety of applications, such as email filtering, and computer vision, where it is infeasible to develop an algorithm of specific instructions for performing the task Machine learning uses types of automated algorithms which learn to predict future decisions and model and modelfunctions using data fed to it.

The Eigenfaces and Fisher faces methods took aholistic approach to face recognition. Recently various methods for a local feature extraction emerged. To avoid the high-dimensionality of the input data only local regions of an image are de- scribed, the extracted features are hopefully more robust against partial occlusion, illumination and small sample size. Algorithms used for a local feature extraction are GaborWavelets , Discrete Cosines Transform and LocalBinary Patterns.

Mainly there are three easy steps to computer coding facial recognition, which are similar to the steps that human brain use for recognizing faces.

These steps are:

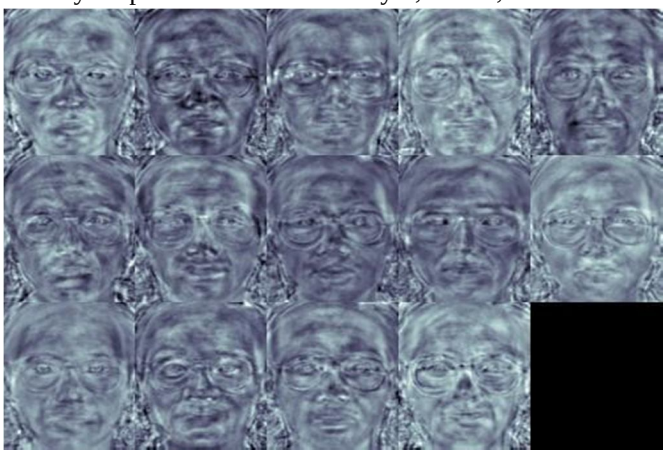
1) *Data Gathering:* Gather face data (face images inthis case) of the people you want to identify.
2) *Train the Recognizer:* Feed that face data and respective names of each face to the recognizer so that it can learn.
3) *Recognition:* Feed new faces of that people and see if the face recognizer, just trained before, recognizes them.

IV. HAAR CASCADE FACE RECOGNIZER ALGORITHM

In this algorithm, a facial image is a point from a high-dimensional image space and a lower-dimensionalrepresentation is found, where classification becomes easy. The lower-dimensional subspace is found with Principal Component Analysis(PCA), which identifies the axes with maximum variance. While this kind of transformation is optimal from a reconstruction standpoint, it doesn't take any class labels into account. Imagine a situation where the variance is generatedfrom external sources, let it be light. The axes with maximum variance do not necessarily contain anydiscriminative information at all, hence a classification becomes impossible. So a class-specific projection with aLinear Discriminant Analysis was applied to face recognition. The basic idea is to minimize the variance within a class, while maximizing the variance between the classes at the same time.

This algorithm considers the fact that not all parts of aface are equally important or useful for face recognition. Indeed, when you look at someone, you recognize that person by his distinct features, like the eyes, nose, cheeks or fore- head; and how they vary respect to each other. Focus is on the areas of maximumchange. For example, from the eyes to the nose there is asignificant change, and same applies from the nose to the mouth. When multiple faces are given, comparisonis done by looking at these areas, because by catching the maximum variation among faces, they help to differentiate one face from the other. This is how Eigenfaces recognizer works. It looks at all the training images of all the people as a whole and tries to extract the components which are relevant and useful and discards the rest. These important features are called principal components.

So, Eigenfaces recognizer trains itself by extracting principal components, but it also keeps a record of which ones belong to which person. Thus, whenever a new image is introduced to the algorithm, it repeats thesame process as follows: Extract the principal components from the new Webcture. Compare those features with the list of elements stored during training.Find the ones with the best match. Return the 'person' label associated with that best match component. In simple words, it's a game of matching. However, one thing to note in above image is that Eigenfaces algorithm also considers illumination as an important feature. In consequence, lights and shadows are Webcked up by Eigenfaces, which classifies them as representing a 'face'. Face recognition Webcks up on human things, dominated by shapes and shadows: two eyes, a nose, a mouth.



V. CONCLUSION

Facial recognition has proven to be one of the most secure methods of all biometric systems to a point for high level security and to avoid ATM robberies and provide security for ATM. It replaces the traditional ATM system. It has advantages such as saves manufacturing cost of cards and overcomes drawbacks of the traditional system like carrying the ATM card, losing of card, fraud calls related to ATM card, etc. With new improved techniques in the field of artificial Intelligence that help eliminate more disturbances and distortions, the rate of effectiveness of the system can be improved.

VI. FUTURE SCOPE

The real time security applications like in ATM security systems, military applications, high security companies.This can also be used in bank locker access. Lighting provided to the system is a key factor to be taken care of. Usage of high-speed computers can improve theefficiency.

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.

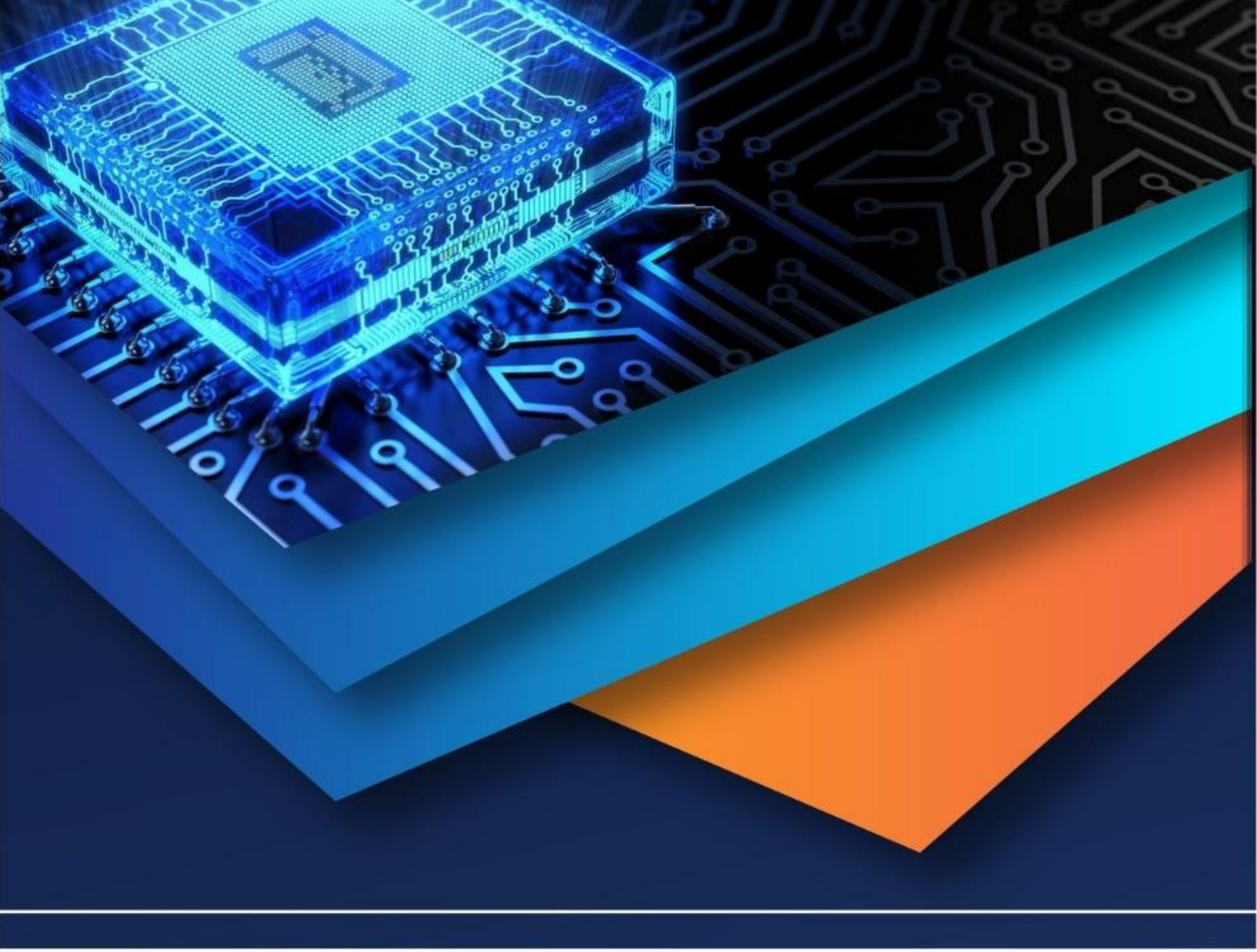
[2] M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Tech- neologies and Applications (ICACTA), 2015.

[3] Sivakumar T. 1 , G. Askok 2 , k. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of EngineeringInventions, Volume 3, Issue 1, 2013. C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", International Journal of

[4] Manoj V , M. Sankar , Sasipriya S , U. Devi E, Devika T Multi Authentication ATM Theft Prevention Using"Multi Authentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and 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 UsingiBeacon", 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 FaceRecognition using Deep Learning based Linear Discriminant Classification ", IEEE International Conferenceon 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 Management (ICIKM), 2012.
[9] https://docs.opencv.org/2.4/modules/contrib/doc/facerec/ face rectutorial.htmlface- recognition
[10] https://www.superdatascience.com/opencv-face-recogniti on/
[11] https://www.rankred.com/face-recognition-algorithms-tech



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)