Face Detection Open CV Based ATM Security System

Praveena.P[1] | Savithri.V[1] | Saratha.R[1] | Monisha.M[1] | Ashwini.R[2]

[1]UG Students, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India
[2]Assistant Professor, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India

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 ATM card is encouraged.Here, The Face ID is preferred to high priority, as the combination of thesebiometrics proved to be the best among the identification and verificationtechniques. The implementation of ATM machines comes with the issue of beingaccessed by illegitimate users with valid authentication code.The users are verified by comparing theimage 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 forfurther accuracy. This system uses openCV to process the image being obtainedandHaar Cascade Classifier to detect the faces in the image. The face recognitionis done using Local Binary Pattern.

KEYWORDS: Haar cascade, Automatic Teller Machine, Webxel, Machine learning, EigenFaces, Fisher Faces.

DOI of the Article: https://doi.org/10.46501/IJMTST0708016

Available online at: http://www.ijmtst.com/vol7issue08.html

As per UGC guidelines an electronic bar code is provided to seure your paper

To Cite this Article: Praveena.P; Savithri.V; Saratha.R; Monisha.M and Ashwini.R. Face Detection Open CV Based ATM Security System. *International Journal for Modern Trends in Science and Technology* 2021, *7*, 0708009, pp. 84-89. https://doi.org/10.46501/IJMTST0708016

Article Info. Received: 05 July 2021; Accepted: 28 July 2021; Published: 01 August 2021

INTRODUCTION

An Automatic Teller Machine (ATM) is a computerized machine that is used to withdraw cash from a customer's respective bank account. As financial users 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 pro- tected 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 vari- ous other threats.Then another major problem is hacking of PIN. There are other fraudulent attacks like eavesdropping, spoofing , brute force attacks, blackmail- ing the user. In the worst case there can also be ATM machine Robbery.

To overcome these problems,the project 'ATM Security system based on Face recognition, PIN and OTP' consists of conventional features ie is Personal Iden- tification 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 sys- tem, which is compared with the images stored in the database. If the face is recognised, 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. Inorder to obtain better accuracydeep learning based linear discrimintclassifica- tion method is utilized. And excecuted the same in OS.

DESIGN PHASE

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 mes- sages for user interface.

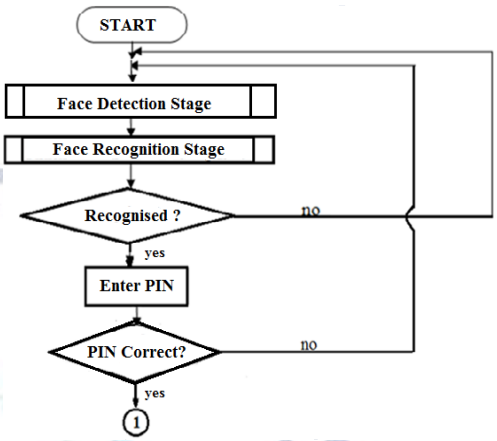

Figure:System flow

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. Cal- culate 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 thealgorithm 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. Cal- culate 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.

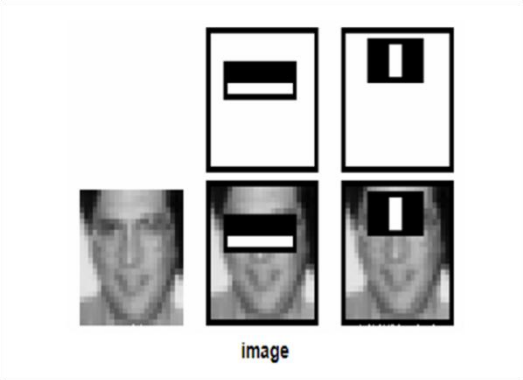

Figure:Haar cascade

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 euclidean distance between feature vectors of a probe and reference image. Some of the latest work on geometric face recognition was, a 22-dimensional fea- ture vector and experiments on large datasets have shown that geometrical fea- tures alone may not carry enough information for face recognition.

METHOD ONE BASED ON MACHINE LEARNING

Machine learning (ML) is the scientific study of algorithms and statistical models that computer systems use 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 fu- ture decisions and model and model functions using data fed to it.

The Eigenfaces and Fisherfaces methods took a holistic approach to face recog- nition. 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 Gabor Wavelets , Discrete Cosinus Transform and Local Binary 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 in this 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.

OpenCV has two built-in face recognizers. The names of those face recognizers are: EigenFaces and FisherFaces.

EIGENFACES FACE RECOGNIZER ALGORITHM

In this algorithm, a facial image is a point from a high-dimensional image space and a lower-dimensional representation is found, where classification becomes easy. The lower-dimensional subspace is found with Principal Component Anal- ysis(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 generated from external sources, let it be light. The axes with maximum variance do not necessar- ily contain any discriminative information at all, hence a classification becomes impossible. So a class-specific projection with a Linear 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 a face are equally im- portant 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 maximum change. For example, from the eyes to the nose there is a significant change, and same applies from the nose to the mouth. When multiple faces are given, compar- ison is 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 the same 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.

FISHERFACES FACE RECOGNIZER ALGORITHM

This algorithm is an improved version of the Eigenfaces. Eigenfaces looks at all the training faces of all the people at once and finds principal components from all of them combined. By doing that, it doesn't focus on the features that dis- criminate one individual from another. Instead, it concentrates on the ones that represent all the faces of all the people in the training data, as a whole. Since EigenFaces also finds illumination as a useful component, it will find this varia- tion very relevant for face recognition and may discard the features of the other people's faces, considering them less useful. In the end, the variance that Eigen- Faces has extracted represents just one individual's facial features. This can be done by tunningEigenFaces so that it extracts useful features from the faces of each person separately instead of extracting them from all the faces combined. In this way, even if one person has high illumination changes, it will not affect the other people's features extraction process.

The Principal Component Analysis (PCA), which is the core of the Eigenfaces method, finds a linear combination of features that maximizes the total variance in data. While this is clearly a powerful way to represent data, it doesn't consider any classes and so a lot of discriminative information may be lost when throwing components away.

The Linear Discriminant Analysis performs a class-specific dimensionality re- duction. In order to find the combination of features that separates best between classes the Linear Discriminant Analysis maximizes the ratio of between-classes to within-classes

scatter, instead of maximizing the overall scatter. The idea is simple: same classes should cluster tightly together, while different classes are as far away as possible from each other in the lower-dimensional representation.

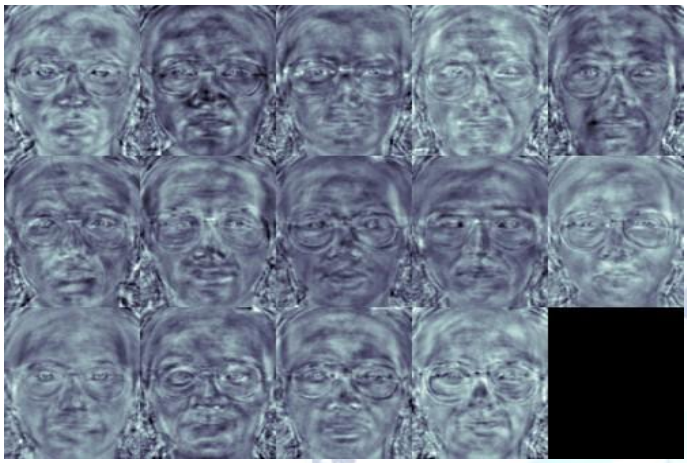

Figure:Face recognition

Precisely, FisherFaces face recognizer algorithm extracts principal components that differentiate one person from the others. In that sense, an individual's com- ponents do not dominate (become more useful) over the others.Below is an image of principal components using FisherFaces algorithm.

One thing to note here is that FisherFaces only prevents features of one person from becoming dominant, but it still considers illumination changes as a useful feature. But light variation is not a useful feature to extract as it is not part of the actual face, another face recognizer Algorithm must be used.

Machine Learning yielded about 75% accuracy for face recognition. Moreover the model was very sensitive to lighting conditions.Hence a new method was designed for face recognition and that is deep learning. This model gives an accuracy upto 95% .

Deep learning (also known as deep structured learning or hierarchical learning) is part of a broader family of machine learning methods based on artificial neural networks.In the case of machine learning, the algorithm needs to be told how to make an accurate prediction by providing it with more information, whereas, in the case of deep learning, the algorithm is able to learn that through its own data processing. It is similar to how a human being would identify something, think about it, and then draw any kind of conclusion.Deep learning interprets data features and its relationships using neural networks which pass the relevant information through several stages of data processing.The key here is to get a deep Convolutional Neural Network(CNN) to produce a bunch of numbers that describe a face (known as face encodings). When two dif- ferent images of the same person are passed to the network, the network should return similar outputs (i.e. closer numbers) for both images, whereas when images of two different people are passed, the network should return very differ- ent outputs for the two images. This means that the neural network needs to be trained to automatically identify different features of faces and calculate numbers based on that.

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 systemcan be improved.

FUTURE SCOPE

The real time security applications like inATM 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 the efficiency.

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. https://www.superdatascience.com/opencv-face-recognition/
11. https://www.rankred.com/face-recognition-algorithms-techniques/