International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2062121

Face Detection Opencv Based ATM Security System

Priyadharshini R[1], Priyadharshini V[1], Vijeletchumi R[1], Dr. Beaulah David[2]
[1]UG Scholar, Department of CSE, Nehru Institute of Technology, Coimbatore, Tamil Nadu, India
[2]Assistant Professor, Department of CSE, Nehru Institute of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

The Aim of this paper is to bolster security of the traditional cash dispenser machine (ATM) model. So a replacement is proposed that enhances the general expertise, usability and convenience of the group action at the ATM. ATM are wide used these days by the people however its exhausting to hold their ATM card all over. The user might forget their ATM PIN number. This paper is developed for identification and authentication of ATM users so creating face as key. Options like face recognition, image steganography and mobile application management are used for sweetening of privacy of users and security of accounts. Face recognition technology helps the machine to spot each and every user unambiguously. Image steganography is the technique used for the image of user by embedding it into an another image and keep. Its one among the ways utilized to guard the image of users from malicious attacks and hackers. The mobile application helps the particular account holders to supply permission to others to do the ATM transactions. The mobile application contains options like secret key and amount withdrawal to offer confirmation. It helps folks to access another person's ATM account in emergency with their authentication. This utterly eliminates all the possibilities of fraud thanks to larceny and duplicity of the ATM cards. Moreover, the experiment is that the method in ATM security framework to enhance security and innovative ATM group action.

Keywords : ATM, Security, Fraud, Face Recognition, Mobile Application Management, Secret PIN

I. INTRODUCTION

In the digital world, The technological advances in money infrastructure, most bank customers like better to use ATM machine and web websites for concluding their banking transactions. Many users particularly utilize ATMs for their physical transactions. Nowadays ATMs are laid low with various problems caused by the theft on many ways. To control this, The main goal of this paper is to propose a pc vision framework that uses the embedded ATM camera to perform face detection and recognition so as to stop such uncalled-for losses. Within the studied situation, we tend to contemplate the case wherever a client withdraws cash from an ATM in a very standard setting. When the client enters into the ATM, the proposed system starts to perform face detection and builds a short lived face information for the client exploitation. The face deducted in camera matches with the already given dataset when it matches it starts process or declined.

Then PIN Transaction, it's for the user cannot go to the ATM but they need to take money in their account for emergency purpose. For this Transaction, mobile access application is proposed.

II. EXISTING SYSTEM

Due to speedy development in science and technology, forthcoming innovations are being settled with sturdy security. However on the opposite hand, threats are being expose to destroy this security level. Although sweetening in automation has created a positive impact overall, however numerous money establishments like banks and applications like ATM are still subjected to thefts and frauds. The present ATM model uses a card and a PIN which supplies rise to extend in attacks within the kind of taken cards, or because of statically allotted PINs, duplicity of cards and numerous different threats. To beat, hybrid model that consists of standard options beside further options like face recognition and one-time countersign (OTP) is employed. Information holds data a couple of user's account details, pictures of his/her face and a mobile variety which can improve security to an outsized extent.

First, the user swipe the ATM card. A live image is captured mechanically through a digital camera put in on the ATM, that is compared with the pictures hold on within the information. If it matches, associate degree OTP are sent to the corresponding registered mobile variety. This indiscriminately generated code has got to be entered by the user within the text box. If the user properly enters the OTP, the dealings will proceed. Therefore, the mix of face recognition algorithmic rule associate degreed an OTP drastically reduces the probabilities of fraud and frees a user from an additional burden of memory advanced passwords.

A. Impacts of existing system

1. Eavesdropping

The ATM card or PIN of a user are often spied upon and might be accessed simply by getting the cardboard by faulty suggests that. This may cause some serious consequences.

2. Spoofing

There's a break that, once a user enters the PIN throughout the group action method, a hacker fakes because the approved web site and prompts the user to enter PIN because of a statement. Once a user complies with the instruction the hacker stores the information and uses it for his future peccadilloes intentions. This man-in-the-middle (hacker) attack is futile as a result of new Arcanum is briefly appointed in each new group action.

3. Brute-force attack

Victimization the brute force, if we tend to attempt to crack the present static four digit PIN it are often tired 9999 tries, therefore weakening the safety. In our model a 6-digit code is distributed to a registered range, therefore increasing the safety and reducing the probabilities of cracking the code victimization brute force.

III. PROPOSED SYSTEM

The study is targeted on style and implementation of face detection based mostly ATM security system victimization embedded unix operating system platform. The system is enforced on the master card size with extended capability of open supply pc vision (OpenCV) software package that is employed for image process operation.

High level security mechanism is provided by the consecutive actions like at first system captures the external body part(face) and check whether or not the external body part is detected properly or not.

If the face is detected properly, ATM transaction will be processed.

If the face isn’t detected properly, then there'll be an alternative method using mobile application. The person who is in the ATM can choose secret key transaction and enter the key(PIN) which is created by user and ATM account holder can give the amount in the mobile application.

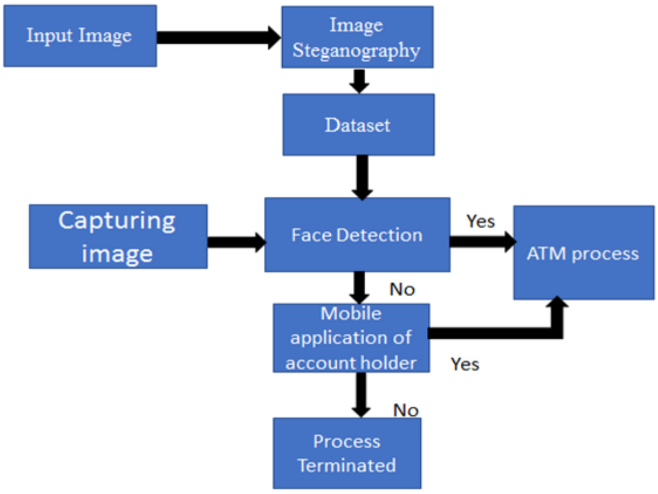


Fig 3.1. Proposed System

A. Purpose and benefits of using face recognition and mobile access in the ATM

Face recognition finds its application in a variety of fields such as homeland security, criminal identification, human-computer interaction, privacy security, etc. The face recognition feature inhibits access of account through stolen or fake cards. The card itself is not enough to access account as it requires the person as well for the transaction to proceed. Eigen face based method is used for the face recognition.

However, the drawback of using Eigen face based method is that it can sometimes be spoofed by the means of fake masks or photos of an account holder. To overcome this problem 3d face recognition methods can be used. However, its computation cost is high and requires large storage space which makes it very difficult to store information about a large number of users and 3d masks can also be used to spoof the 3d facial recognition based model. 3d printing is mostly used for such attacks.

These drawbacks can be easily overcome by using one-time passwords (OTP). OTP ensures that the user is authentic by sending the randomly generated 6-digit code to the registered mobile number of the corresponding account holder. In addition, the user will not have to remember PIN. It prevents the fraudulent attacks like:

- Card trapping
- Card skimming
- Transaction Reversal fraud
- Cash trapping

IV. METHODS AND DESIGNS OF SYSTEM

A. Image steganography for hiding images

During this module, the image of the account holder is encrypted victimisation steganography into a another image so as to extend the safety of the information. In this method, the photographs within the info of the bank server square measure stenographed victimisation cipher rule. The photographs square measure then encrypted into a another image known as secondary image. Once the image is encrypted the can't be viewed and thus the information is secured. Then whenever face recognition rule is started, then the image within the info is decrypted and compared with the first image so the method is sustained.

1) B. Secure ATM by Facial Recognition Technology

Identity verification victimisation OpenCV and capturing the image, comparison with the datasets and displaying the result as matched if the faces square measure same. If the faces square measure mismatched then there'll be a alert in mobile application of account holder.

A identity verification system could be a laptop application for mechanically characteristic or substantiative someone from a digital image or a video frame from a video supply. Proposed paper uses face recognition technique for verification in ATM system. Locate a person in the camera view. Identify the object is a face. Compare face with the database. Face recognition can work with hign or low resolution cameras.

C. Mobile access management for PIN Transaction

Mobile application is installed in the users mobile for easy transaction and to take money by the folks with the knowledge Of the user. User needs to enter amount and the secret one time PIN then should activate, then the user give access to the folk in the ATM. The folk should choose secret key in the screen and enter the secret PIN and withdraw the money from ATM.

V. MATERIAL USED

A. Web camera

An internet camera may be a device that helps to require footage and video usually used for video chatting and video and image capturing for authentication and verification method. In our example, the Logitech camera is employed for this method. It's one in every of the most cost effective nonetheless a decent internet camera obtainable within the market. Alternative cameras can even be used for face capturing. The Logitech camera supports 720p recording and 5mp image capturing. 5mp image is over enough for a decent face identification.

The camera supports USB 2.0 serial communication, that is wide used. Thus there's no hardship whereas connecting this camera to the system. The motive force computer code for the camera doesn't got to be singly downloaded. The universal driver obtainable in each software can support the Logitech internet camera. No further driver installation is needed for victimisation Logitech camera. There's no further power provide is needed for the camera, because it consumes power from the USB slot it self.

Fig 5.1 Web Camera

VI. ALGORITHMS

A. AES Algorithm

In cryptography the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption as well as for decryption. The AES algorithm, a symmetric block cipher can encrypt as well as decrypt the data. The length of data blocks is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. Encryption translates data to a secret form called cipher-text. Encryption of the cipher-text then converts the data back into its original form, which is known as plain-text. AES is also reversible for many encryption algorithms. This helps us to understand that almost the same steps with some simple changes are performed to complete both encryption and decryption in reverse order.

For encryption, each round consists of the following four steps:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

For decryption, each round consists of the following four steps:

- Inverse Shift Rows
- Inverse Sub Bytes
- Add Round Key
- Inverse Mix Columns.

B. SVM Algorithm

Support Vector Machine (SVM) is a supervised machine learning algorithm which is used for classification or regression challenges. within the SVM algorithm, we have a tendency to plot every information item as a degree in n-dimensional space with the worth of every feature being the worth of a selected coordinate. Support vectors square measure the information points nearest to the hyper plane, the points of an information set that, if removed, would alter the position of the dividing hyper plane.

The learning algorithm can also compare its output with the correct dataset. It is formulated to solve a classical two class pattern Recognition problem.

VII. TECHNOLOGIES

A. Python 3.7

Python is an interpreted, high-level, general-purpose programming language. Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an ideal language for scripting and rapid application development in many areas on most platforms and may be freely distributed. These include:

- Easier access to debuggers through a new breakpoint() built-in
- Simple class creation using data classes
- Customized access to module attributes
- Improved support for type hinting
- Higher precision timing functions

The breakpoint() Built-In it makes using debuggers more flexible and intuitive.

B. Image processing

Digital image processing is the utilization of a digital computer to process digital images through an algorithm as a subcategory or field of digital signal process, digital image process has several blessings over analogue image process. It permits a far wider vary of algorithms to be applied to the input file and may avoid issues like the build-up of noise and distortion during process. Since pictures square measure outlined over 2 dimensions (perhaps more) digital image process is also sculptural within the type of multidimensional systems stages.

C. Machine learning

Machine learning is associate application of computer science (AI) that gives systems the flexibility to mechanically learn and improve from expertise while not being expressly programmed. Machine learning focuses on the event of laptop programs that will access knowledge and use it learn for themselves.

The process of learning begins with observations or knowledge, like examples, direct expertise, or instruction, so as to appear for patterns in knowledge and create higher choices within the future supported the examples that we offer. The first aim is to permit the computers learn automatically without human intervention or help and regulate actions consequently.

D. Open CV

OpenCV is that the most well liked library for laptop vision. Originally written in C/C++, it currently provides bindings for python. OpenCV uses machine learning algorithms to look for faces at intervals an image. As a result of faces square measure therefore sophisticated, there isn't one straightforward take a look at which will tell you if it found a face or not. The algorithms is uses for distinguishing the face into thousands of smaller, bite-sized tasks, every of that is straightforward to resolve. These tasks are called classifiers.

For one thing sort of a face, you would possibly have half-dozen,000 or a lot of classifiers, all of that should match for a face to be detected (within error limits, of course). However in that lies the problem: for face detection, the rule starts at the highest left of an image and moves down across tiny blocks of knowledge, observing every block, Since there square measure half-dozen,000 or a lot of tests per block, you would possibly have numerous calculations to try and do, which can grind the laptop to a halt. Rather than taking hours, face detection will currently be tired real time

E. Steganography

The steganography is the art or practice to hide a message, image or file within another image, file or message. Steganography means to hide something through writing. Steganography takes cryptography a level more by hiding an encoded message using least significant bit (LBS) technique.

It hides the messages in such a way that no one except the receiver knows how to expose the secret message Image steganography data is encoded and then put, using a special algorithm, data that is part of a particular file format such as a bitmap image. LSB (Least Significant Bit) technique will replace the least significant bits with the message to be encrypted. We have used the bmp images as it does lossless compression so LBS can be resourcefully while using bmp. It will embed secret message into image.

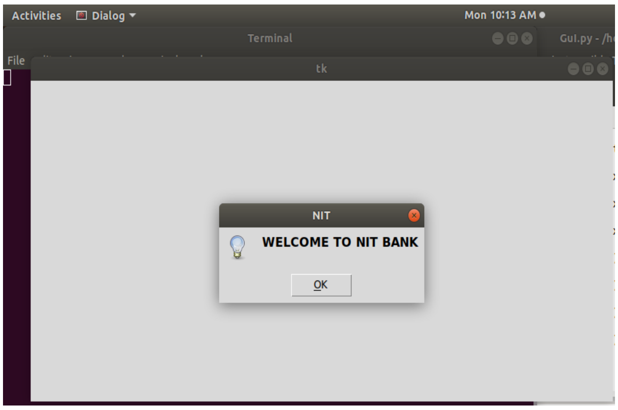
We will use least significant bit because of following reason.

A. After hiding the message, the intensity of image is change by 1 or 0.

B. Change of intensity is either 0 or 1 because it changes the last bit .e.g.

00101111 ----> 00101110

VIII.RESULT



WELCOME TO NIT BANK

Fig 8.1. Welcome page

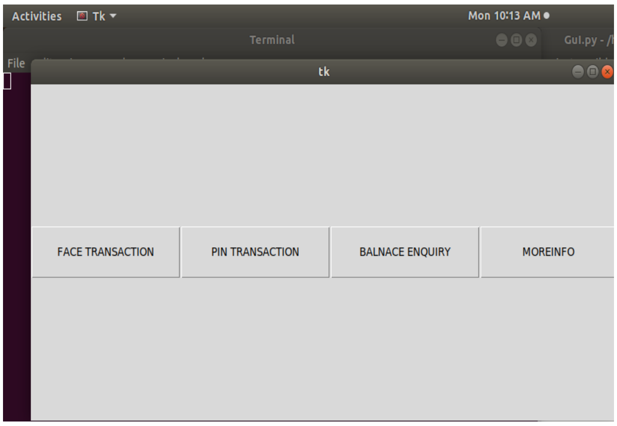


Fig 8.2. Main screen

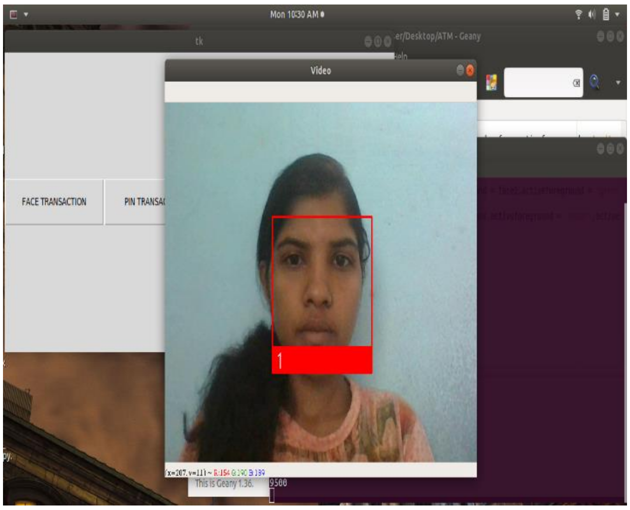
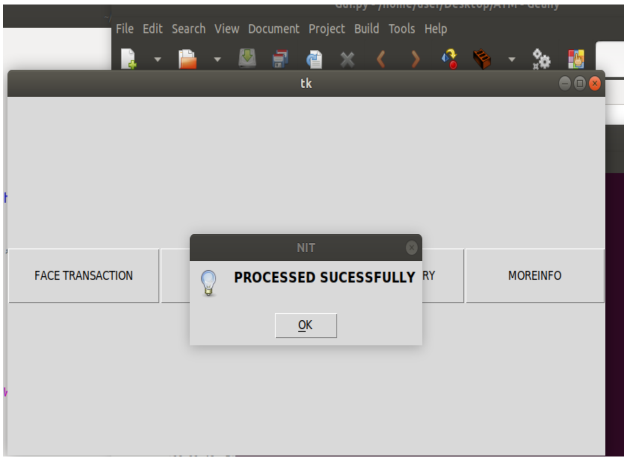
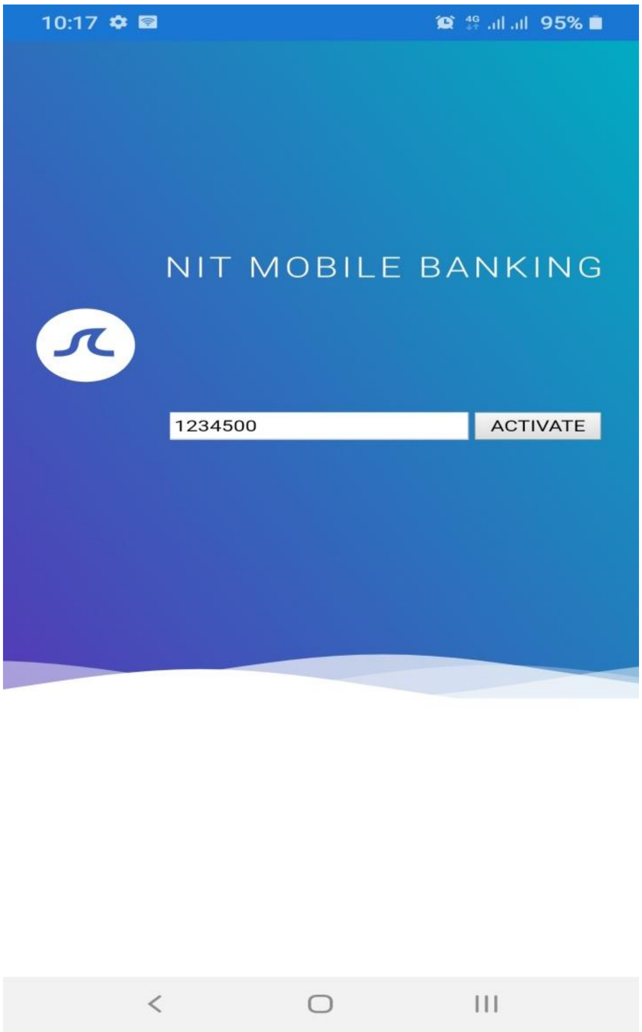


Fig 8.3. Face recognition for Face transaction



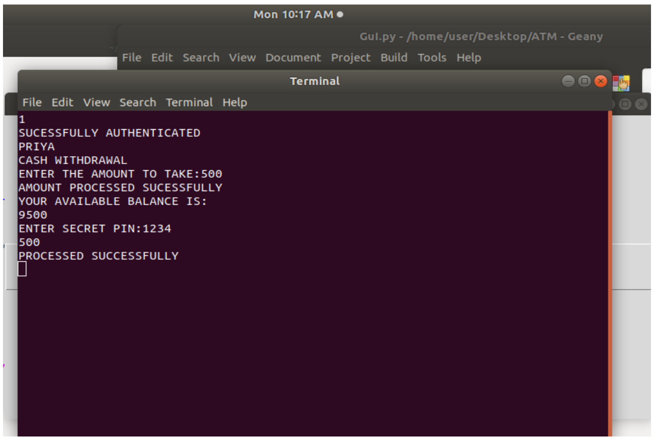
PROCESSED SUCESSFULLY

Fig 8.4. Face Recognition and deduction



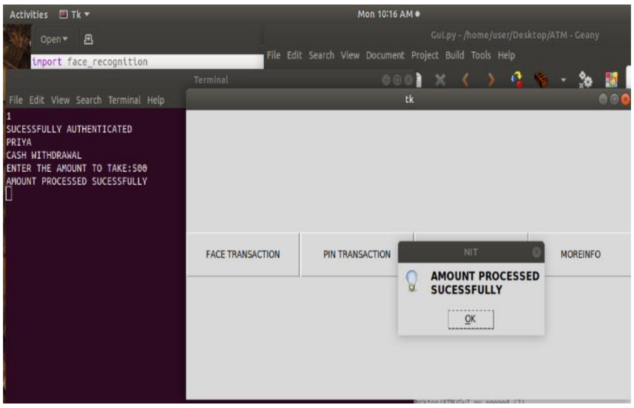
1234500

Fig 8.5. Mobile Access Management


Mon 10:17 AM
Gui.py - /home/user/Desktop/ATM - Geany
File Edit Search View Document Project Build Tools Help
Terminal
File Edit View Search Terminal Help

```
1
SUCESSFULLY AUTHENTICATED
PRIYA
CASH WITHDRAWAL
ENTER THE AMOUNT TO TAKE:500
AMOUNT PROCESSED SUCESSFULLY
YOUR AVAILABLE BALANCE IS:
9500
ENTER SECRET PIN:1234
500
PROCESSED SUCCESSFULLY
```

Fig 8.6. PIN Transaction


Activities
Tk
Mon 10:16 AM
Open
Gui.py - /home/user/Desktop/ATM - Geany
File Edit Search View Document Project Build Tools Help
Terminal
File Edit View Search Terminal Help
tk
FACE TRANSACTION
PIN TRANSACTION
NIT
MOREINFO
OK

```
import face_recognition
```

```
1
SUCESSFULLY AUTHENTICATED
PRIYA
CASH WITHDRAWAL
ENTER THE AMOUNT TO TAKE:500
AMOUNT PROCESSED SUCESSFULLY
```

AMOUNT PROCESSED SUCESSFULLY

Fig 8.7. PIN Transaction successful

IX. CONCLUSION

In this work we propose a ATM security that is more reliable by using open CV Face Recognition and Deduction. It reduces the fraud actions in ATM. It ensures higher Withdrawal and Transaction limits and it gives customer satisfaction. This added security will improve the rate of transaction and also the bank can profit through this system.the experiment results in card loosing and PIN forgetting issues.

The combination of biometrics will always result in high security. The face id, message alert, mobile access and PIN as combined, this gives Higher level of security applied to the account they result in a hard-secure authentication.

X. REFERENCES

[1]. Faune hughes, daniel lichter,richard oswald, and Michael whitfield ,face biometrics:a longitudinal study, seidenberg school of csis,pace university, white plains,ny 10606,usa.

[2]. Garyg.yen, nethrie nithianandan, facial feature extraction using genetic algorithm, intelligent systems and control laboratory school of electrical and computer engineering. Okla homa state university, stillwater, ok 74074-5032, usa.

[3]. Jiang, y.x. Hu, s.c. Yan, h.j. Zhang, "efficient 3d reconstruction for face recognition", 0031_3203/2004pattern recognitionsociety:doi:10.1016/j.patcog.2004.11.00

[4]. Animetrics offers facer credentialme service on sprint 3g and 4g networksaugust 12th, 2010

[5]. Zigelman, g., kimmel, r., kiryati, n. Texture mapPINg using surface flatten-ing via multi-dimensional scaling, ieee trans. Visualization and comp. Graphics, 8, pp. 198-207 (2002).

[6]. F. Cootes, c. J. Taylor, d. Cooper, and j. Graham. Ac-tive shape models - their training and application. Cviu, 61(1):38 59, jan. 1995

[7]. Vogler, z. Li, a. Kanaujia, s. Goldenstein, and d. Metaxas. The best of both worlds: combining 3d de-formable models with active shape models. Iccv 2007.

[8]. Mordohai and g. Medioni. Tensor voting: a perceptual organization approach to computer vision and machine learning. Morgan and claypool publishers, 2007.

[9]. Pennec. Intrinsic statistics on riemannian manifolds: ba-sic tools for geometric measurements. Journal of mathemat-ical imaging and vision, 25(1):127-154, july 2006.

[10]. Gu and t. Kanade. 3d alignment of face in a single image. Cvpr 2006, pp. 1305-1312.

Cite this article as :

Priyadharshini R, Priyadharshini V, Vijeletchumi R, Dr. Beaulah David, "Face Detection Opencv Based ATM Security System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 425-432, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT2062121
Journal URL : http://ijsrcseit.com/CSEIT2062121