**THIRD GENERATION ATM MACHINE USING ADVANCED COMPUTER VISION TECHNIQUES**

**Arun L K1, Aakash S2, Alagupandi J3, Prof. Sathish N4**

*1, 2, 3 UG Student, Dept. of Computer Science, Panimalar Engineering College, Chennai, Tamil Nadu, India*.

*4Assistant Professor, Dept. of Computer Science, Panimalar Engineering College, Chennai, Tamil Nadu, India*.

---------------------------------------------------------------------\*\*\*---------------------------------------------------------------------

**Abstract -**Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. For example, ATMs are typically found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centre's, airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week we are stopping illegal transaction by using face detection and send mail to person email

***Key Words*: ATM, Face detection**

**1. INTRODUCTION**

Banks seek to reduce their infrastructure costs by shifting transactions of their customers to Automatic Teller Machines (ATMs) and Internet websites.. ATM is one such machine which made money transactions easy for customers to bank. The other side of this improvement is the enhancement of the culprit's probability to get his „unauthentic‟ share. Traditionally, security is handled by requiring the combination of a physical access card and a PIN or other password in order to access a customer's account. This model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to no encrypted customer account information and other points of failure. Our paper proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. With the technological advances in financial infrastructure, most bank customers prefer to use Automatic Teller Machines (ATMs) and Internet websites for carrying out their banking transactions. Financial users especially utilize ATMs for physical transactions like cash withdrawal or cash deposit. However, just like any other system, ATMs are also suffering from numerous issues caused by users. Among these problems, card and/or cash forgetting (CCF) is a common issue. The main goal of our work is to propose a computer vision framework which uses the embedded ATM camera to perform face detection and recognition in order to prevent such unnecessary losses generated by CCF. In the studied scenario, we consider the case where a customer withdraws money from an ATM in a conventional setting. After the customer inserts the card into the ATM, the proposed system starts to perform face detection and builds a temporary face database for the customer using the camera located inside the ATM. If the customer leaves the ATM without taking his/her card or cash, the ATM waits for the customer to be back instead of retracting the forgotten item. If the system finds out there is a different customer approaching the ATM before the card/cash holder, the card/cash will be retracted at that moment. This scenario is fundamentally different than biometric authentication scenarios, in which a person’s image is matched to a gallery image acquired, possibly, a long time before the matching, under different conditions. In this scenario, the matching image and the gallery image are separated by mere minutes at most.

.

**2. LITERATURE SURVEY**

[1] This paper describes a novel biometric scenario, where a person is authenticated at an ATM, and has to be re-identified from a camera within a very short time period, under very challenging illumination and pose conditions I using Single Identifying System. We propose a multimodal authentication system that operates under the constraints imposed by this applications scenario, and implement face recognition and RFID Card appearance recognition to create a system that improves ATM behavior in case of forgotten card or cash by re-identifying the user from an embedded ATM camera. We focus on the scenario and the platform, and report tests with the proposed system under challenging conditions, obtained from ATMs placed in the field

[2] This paper describes a novel biometric scenario, where a person is authenticated at an ATM, and has to be re-identified from a camera within a very short time period, under very challenging illumination and pose conditions I using Single Identifying System. We propose a multimodal authentication system that operates under the constraints imposed by this applications scenario, and implement face recognition and RFID Card appearance recognition to create a system that improves ATM behavior in case of forgotten card or cash by re-identifying the user from an embedded ATM camera. We focus on the scenario and the platform, and report tests with the proposed system under challenging conditions, obtained from ATMs placed in the field

[3] User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom, non-universality of the biometric trait and unacceptable error rates. Attempting to improve the performance of individual matchers in such situations may not prove to be effective because of these inherent problems. Multi biometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity. These systems help achieve an increase in performance that may not be possible using a single biometric indicator. Further, multi biometric systems provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. However, an effective fusion scheme is necessary to combine the information presented by multiple domain experts. This paper addresses the problem of information fusion in biometric verification systems by combining information at the matching score level. Experimental results on combining three biometric modalities (face, fingerprint and hand geometry) are presented.

**3. EXISTING SYSTEM**

In existing system magnetic strips card is used as ATM card, IR sensor in order to sense the presence of the card holders and to turn on Fan and Light, if ATM is tampered then SMS is sent to two main stations via GSM. Based on WI fall detection get security, that network access is not that much secured

**4. PROPOSED SYSTEM**

* The study is focused on Design and Implementation of Face Detection based ATM Security System using Embedded Linux Platform.
* The system is implemented on the credit card size Raspberry Pi board with extended capability of open source Computer Vision (Open CV) software which is used for Image processing operation.
* High level security mechanism is provided by the consecutive actions such as initially system captures the human face and check whether the human face is detected properly or not. If the face is not detected properly, it warns the user to adjust him/her properly to detect the face.

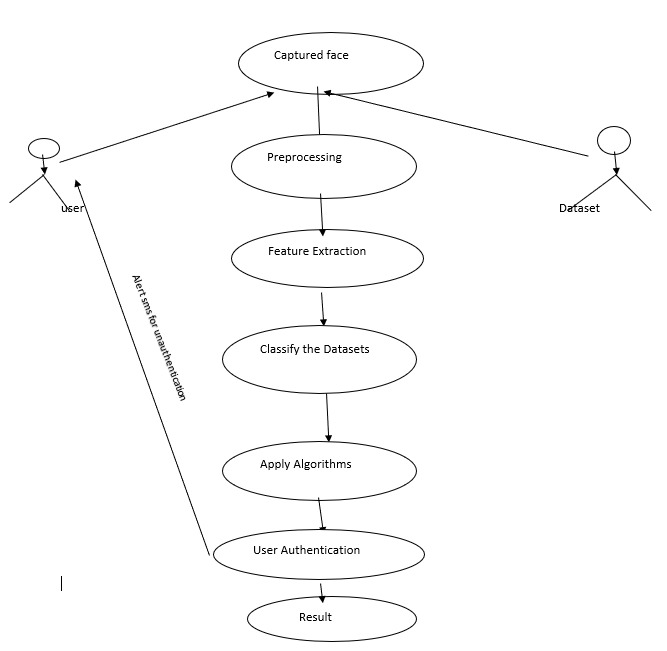
**5. MODULES**

**5.1 Preprocessing**

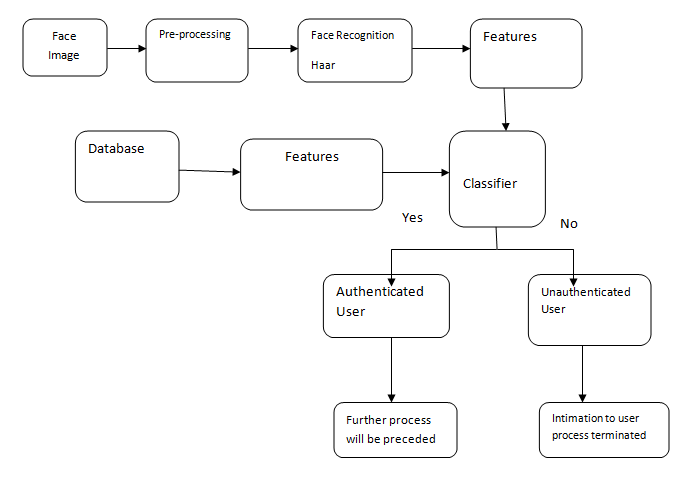
Image pre-processing is the term for operations on images at the lowest level of abstraction These operations do not increase image information content but they decrease it if entropy is an information measure The aim of pre-processing is an improvement of the image data that suppresses undesired distortions or enhances some image features relevant for further processing and analysis task

5.2 Implementation of algorithm

In this section we are implementing a system for face recognition in ATM and don't allow the wanted and illegal transaction using Convolution neural network algorithm. Several python libraries are used such as numpy, pandas, sklearn, and flask are used application.

****

**Fig 1: UML Diagram for the system**

****

**Fig 2: Flow Diagram**

**7.SOFTWARE SPECIFICATION**

**7.1 Python**

Python is an [interpreter](https://en.wikipedia.org/wiki/Interpreted_language), [high-level](https://en.wikipedia.org/wiki/High-level_programming_language) and [general-purpose programming language](https://en.wikipedia.org/wiki/General-purpose_programming_language). Python's design philosophy emphasizes [code readability](https://en.wikipedia.org/wiki/Code_readability) with its notable use of [significant indentation](https://en.wikipedia.org/wiki/Off-side_rule). Its [language constructs](https://en.wikipedia.org/wiki/Language_construct) and [object-oriented](https://en.wikipedia.org/wiki/Object-oriented_programming) approach aim to help [programmers](https://en.wikipedia.org/wiki/Programmers) write clear, logical code for small and large-scale projects. Python is dynamically-typed and garbage-collected. It supports

multiple programming paradigms, including structured (particularly, procedural), object-oriented and functional programming.[5]

**7.2 open cv**

OpenCV-Python is a library of Python bindings designed to solve computer vision problems.Python is a general purpose programming language started by **Guido van Rossum** that became very popular very quickly, mainly because of its simplicity and code readability. It enables the programmer to express ideas in fewer lines of code without reducing readability.Compared to languages like C/C++, Python is slower. That said, Python can be easily extended with C/C++, which allows us to write computationally intensive code in C/C++ and create Python wrappers that can be used as Python modules. This gives us two advantages: first, the code is as fast as the original C/C++ code (since it is the actual C++ code working in background) and second, it easier to code in Python than C/C++. OpenCV-Python is a Python wrapper for the original OpenCV C++ implementation.OpenCV-Python makes use of **Numpy**, which is a highly optimized library for numerical operations with a MATLAB-style syntax. All the OpenCV array structures are converted to and from Numpy arrays. This also makes it easier to integrate with other libraries that use Numpy such as SciPy and Matplotlib

**8. EXPLANATION**

The base idea is to create more secure ATM which should know the illegal transitions before it is done. when some misusing your ATM card in any ATM it will transfer the picture of that person to the mail id of the person .so it can b used to the user who is activating his card before the transactions done. that's the main methodology of this project. we are creating a datasets in a database after database is created we area extracting data in data set that is our image of the user after the person enter the ATM it detects him after putting card if so your pin also wrong it will send he picture to the email.

**9. CONCLUSION**

To avoid ATM robberies and provide security for ATM , To secure such a complex system will be even more difficult than design it. And now people just begin to discuss some issues of ATM security. It will provide some experience for us to implement security services in ATM network

**10. FUTURE ENHANCEMENTS**

In future we are planning to implement voice detecting process for blind people and the physically challenged persons .

**11. REFERENCES**

H. R. Babaei, O. Molalapata and A. A. Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rd ed. vol.45, pp.211-216, 2012.

Aru, O. Eze and I. Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online] 2013, pp. 188-193, Available:http://www.ajer.org/papers/v2 (5)/Y02501880193.pdf ¬ K.

J. Peter, G. Nagarajan, G. G. S. Glory, V. V. S. Devi, S. Arguman and K. S. Kannan, Improving ATM Securityvia Face Recognition, in ICECT, Kanyakumari, 2011,vol.6, pp.373-376.

E. Derman, Y. K. Gec¸ici and A. A. Salah, Short Term Face Recognition for Automatic Teller Machine (ATM) Users, in ICECCO 2013, Istanbul, Turkey, pp.111-114

A. Ross and A. Jain, Information Fusion in Biometrics,in Pattern Recognition Letters, vol.24, pp.2115-2125,2003.