International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

FACE DETECTION BASED ATM SAFETY SYSTEM FOR SECURED TRANSACTION

S Gayathri[1], Deepika H[2], Keerthana G S[3]

[1]Assistant Professor, Department of Computer Science and Engineering, JEPPIAAR SRR Engineering College, Tamil Nadu, India
[2]Department of Computer Science and Engineering, JEPPIAAR SRR Engineering College, Tamil Nadu, India
[3]Department of Computer Science and Engineering, JEPPIAAR SRR Engineering College, Tamil Nadu, India

---

Abstract - *The broadening within the electronic transactions has resulted in a very nice demand for quick and precise user identification and verification. Users are largely looking on and trusting the Automated Teller Machine (ATM) to handily meet their banking desires. However, the various blessings of the ATM system, the ATM artifice, has recently become widespread. This projected system avoids the ATM thievery and the wrong person misuses the ATM. So we've got to set up things like alarms once in actions of breaking or damaging the machines threatening the ATM user's denial of transactions and also the alternative ATM user by invalid users or masks. The most planned of this technique is to produce improved security to the ATM user through Face Verification System (FRS) and mail authentication.*

Keywords: **Face Recognition System (FRS), Haar-Cascade Algorithm, Mail Authentication**

1. INTRODUCTION

Many bank clients will in general utilize Automatic Teller Machines (ATMs) and Internet entries to lead their financial exchanges with the mechanical advances in budgetary framework. Monetary clients particularly use ATMs for physical exchanges like money withdrawal or money store. Be that as it may, much the same as some other framework, ATMs are likewise experiencing various issues brought about by clients. The principle objective of our work is to propose a PC vision structure which utilizes the installed ATM camera to perform Face Recognition System (FRS) so as to forestall security breaks. After the client embeds the card into the ATM, the proposed framework begins to perform face recognition and assembles a transitory face database for the client utilizing the camera situated inside the ATM. In the event that the framework discovers there is an alternate client moving toward the ATM before the card holder, the ATM will send a caution at that point. This circumstance is on a very basic level not the same as biometric validation circumstances, in which a picture of an individual client is contrasted with an exhibition picture got from various conditions, perhaps some time before coordinating. The comparing picture and display picture right now all things considered isolated by mere minutes.

After some time, shoppers have come to depend on and trust the Automatic Teller Machine (ATM) to provide food for their financial needs helpfully. Dealing with the hazard related with ATM extortion just as decreasing its belongings is a significant issue confronting budgetary foundations as misrepresentation methodologies with expanded events have become more advanced. The ATM is only one of various Electronic Funds Transfer (EFT) gadgets powerless against extortion assaults. The examination distinguishes the basic ATM misrepresentation, how, where and when these fakes are sustained and afterward proffer security suggestions that ought to be clung to by both the banks as money related foundations and the ATM clients so as to take out or decrease it to the barest least. Since the first was propelled during the 1960s, making sure about robotized teller machines (ATMs) has been keeping bank security officials up around evening time. ATMs were constantly dependent upon physical burglary, both of the machine itself or of the money inside. The quickest developing peril to ATMs today, be that as it may, originates from the internet. Not exclusively do ransomware and interruption hurt the attacking explicit PC however they additionally change the entire system. At the point when banks embrace new approaches and techniques to keep ATMs secure, they should likewise protect that they satisfy all the administrative prerequisites that are necessary. At a similar time, monetary foundations will limit the effect of such strides on their ATM system's absolute expense of proprietorship (TCO).
Bank security officers certainly need to monitor and respo nd to those concerns on an ongoing basis. But they also ne ed to protect their systems from the latest threats, which u sually come from the fraud and cyber crime vectors of the 21st century attack.

1.1 FACIAL RECOGNITION SYSTEM

A facial acknowledgment framework is an innovation equipped for distinguishing or confirming an individual from an advanced picture or a video outline from a video source. There are various strategies in which facial acknowledgment frameworks work, however for the most part, they work by looking at chosen facial highlights from a given picture with faces inside a database. It is also

defined as an application based on Biometric Artificial Intelligence which can uniquely identify a person by analyzing patterns based on the facial textures and shape of the individual. Although initially a form of computer application, it has seen wider uses on mobile platforms and other forms of technology, such as robotics, in recent times. It is typically used in security systems as access control, and can be compared with other biometrics such as fingerprinting or eye iris recognition systems.

Although the precision of the facial recognition method as a biometric application is lower than the identification of iris and the detection of fingerprints, its contactless and noninvasive operation renders it widely adopted. It's also recently become popular as a method for commercial recognition and marketing. Many uses include advanced human-computer interaction, video surveillance, automatic image indexing and, among others, video storage. Throughout human beings, it is the temporal lobe of the brain that is responsible for facial recognition. The temporal lobe neurons react to certain facial features and store them gradually contributing to facial recognition.

In machine learning systems, the machines are often fed a huge bank of images which the system absorbs and stores. When matching a face it tries to match it with the images stored using face recognition algorithm. According to a new research by a community of MIT researchers, the computers recognize the picture randomly and correctly, and were often able to identify a face even when it was tilted from the middle at an angle of about 45 degrees, to the left or to the right.

1.2 HAAR-CASCADE ALGORITHM

Haar Cascade is an AI object identification calculation used to distinguish protests in a picture or video and dependent on the idea of highlights proposed by Paul Viola and Michael Jones in their paper "Fast Object Detection utilizing a Boosted Cascade of Simple Features" in 2001. A Haar-like element thinks about contiguous rectangular locales at a particular area in a recognition window, summarizes the pixel forces in every district and figures the distinction between these holes.

This qualification is then used to arrange subsections of an image. For instance, let us state we have a picture database with human countenances. It is a typical perception that among all faces the area of the eyes is darker than the district of the cheeks. Thus a typical Haar include for face discovery is a lot of two contiguous square shapes that lie over the eye and the cheek district. The situation of these square shapes is characterized by a discovery window that demonstrates like a jumping box to the objective item (the face right now). It is an AI based methodology where a course work is prepared from a great deal of positive and negative pictures. It is then used to recognize questions in different pictures. The calculation has four phases:

1. Haar Feature Selection
2. Creating Integral Images
3. Adaboost Training
4. Cascading Classifiers

It is notable for having the option to recognize faces and body parts in a picture, however can be prepared to distinguish practically any article. Initial step is to gather the Haar Features. A Haar feature thinks about adjoining rectangular areas at a particular area in a location window, summarizes the pixel forces in every locale and ascertains the contrast between these aggregates.

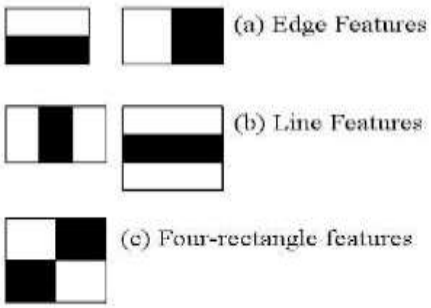

Fig -1: Haar Features

Yet, among every one of these highlights we determined, the greater part of them are unessential. For instance, consider the picture underneath. Top column shows two great highlights. The primary component chosen appears to concentrate on the property that the district of the eyes is frequently darker than the locale of the nose and cheeks. The subsequent component chosen depends on the property that the eyes are darker than the extension of the nose. In any case, similar windows applying on cheeks or some other spot is superfluous.

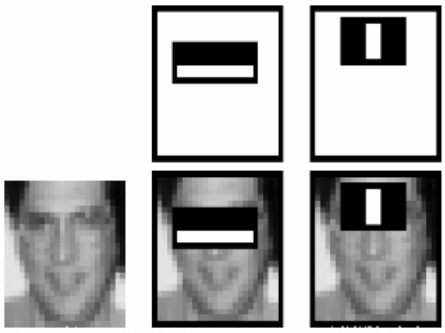

Fig -2: Recognition using Haar Cascade

So how would we select the best highlights out of 160000+ highlights? This is practiced utilizing an idea called Adaboost which both chooses the best highlights and prepares the classifiers that utilization them. This calculation builds a "solid" classifier as a straight blend of

weighted basic "frail" classifiers. The procedure is as per the following.

During the identification stage, a window of the objective size is moved over the information picture, and for every subsection of the picture and Haar highlights are determined. You can see this in real life in the video underneath. This distinction is then contrasted with a scholarly limit that isolates non-objects from objects. Since each Haar highlight is just a "feeble classifier" (its recognition quality is somewhat superior to irregular speculating) countless Haar highlights are important to portray an item with adequate precision and are hence composed into course classifiers to frame a solid classifier.

2. EXISTING SYSTEM

An Automated teller machine (ATM) is an electronic broadcast communications gadget that empowers clients of budgetary establishments to perform money related exchanges, for example, money withdrawals, stores, reserves moves, or record data requests, whenever and without the requirement for direct connection with bank staff. An ATM is commonly comprised of the accompanying gadgets:

- CPU (to control the UI and exchange gadgets)
- Magnetic or chip card per user (to recognize the client)
- A PIN cushion for tolerating and scrambling individual ID number EPP4 (comparable in format to a touch tone or mini-computer keypad), made as a feature of a safe walled in area
- Secure crypto processor, by and large inside a safe nook
- Display (utilized by the client for playing out the exchange)
- Record printer (to furnish the client with a record of the exchange)
- Function key catches (typically near the showcase) or a touchscreen (used to choose the different parts of the exchange)
- Vault (to store the pieces of the hardware requiring confined access)
- Housing (for style and to join signage to)
- Sensors and markers

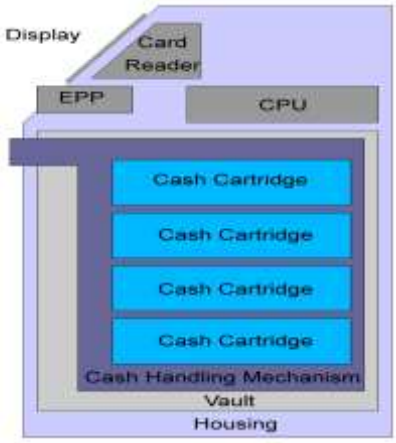

Fig -3: ATM Block Diagram

2.1 INTEGRITY OF THE SYSTEM

The security of ATM exchanges depends for the most part on the respectability of the protected crypto processor: the ATM regularly utilizes general ware segments that occasionally are not viewed as "confided in frameworks". Encryption of individual data, legally necessary in numerous purviews, is utilized to forestall misrepresentation. Delicate information in ATM exchanges are typically encoded with DES, yet exchange processors currently as a rule require the utilization of Triple DES. Remote Key Loading procedures might be utilized to guarantee the mystery of the initialization of the encryption enters in the ATM. Message Authentication Code (MAC) or Partial MAC may likewise be utilized to guarantee messages have not been altered while in travel between the ATM and the money related system.

There have additionally been various occurrences of extortion by Man-in-the-center assaults, where crooks have connected phony keypads or cards per user to existing machines. These have then been utilized to record clients' PINs and bank card data so as to increase unapproved access to their records. Different ATM producers have set up countermeasures to shield the gear they make from these threats.

Elective strategies to confirm cardholder characters have been tried and sent in certain nations, for example, finger and palm vein patterns, iris, and facial acknowledgment advancements. Less expensive mass-created gear has been created and is being introduced in machines all inclusive that distinguish the nearness of outside items on the facade of ATMs, current tests have demonstrated 99% discovery accomplishment for a wide range of skimming devices.

2.2 RELATED WORKS

Arun Kumar, Vasanth Kumar, and Aravindan “ATM Security Using Face Recognition” International Journal of Current Engineering and Scientific Research, Vol. 5, 2018**:**

With the mechanical advances in money related foundation, most bank clients like to utilize Automatic Teller Machines (ATMs) and Internet sites for doing their financial exchanges. Money related clients particularly use ATMs for physical exchanges like money withdrawal or money store. Be that as it may, much the same as some other framework, ATMs are additionally experiencing various issues brought about by clients. The primary objective is to propose a PC vision system which utilizes the installed ATM camera to perform face location and acknowledgment. A facial acknowledgment framework is a PC application for consequently distinguishing or checking an individual from an advanced picture or a video outline from a video source. Proposed paper utilizes face acknowledgment strategy for check in ATM framework. The facial acknowledgment and confirmation right now dependent on Local Binary Patterns (LBP) surface highlights. It is demonstrated to be profoundly discriminative and its key favorable circumstances, in particular, its invariance to monotonic dark level changes and computational effectiveness, make it reasonable for requesting picture investigation assignments. For facial characterization a technique dependent on Kullback separation of test and model appropriations is utilized. The arrangement results for single highlights with one-dimensional component esteem conveyances and for sets of corresponding highlights with two-dimensional disseminations are introduced. In yield structure it is resolved how the data is to be dislodged for sure fire need and furthermore the printed version yield. It is the most critical and direct source information to the customer. Effective and savvy yield configuration improves the framework's relationship to help client dynamic. To maintain a strategic distance from ATM burglaries and give security to ATM this technique can't be a lot of proficient on the grounds that the use of Local Binary Patterns may create longer histograms and diminishes the facial acknowledgment speed in bigger and complex databases.

Tomas Larrain, John Bernhard, Domingo Mery and Kevin Bowyer "Face Recognition Using Sparse Fingerprint Classification Algorithm" IEEE Access, Vol.12, pp. 1646-1647, July 2017:

Face acknowledgment has been an extremely dynamic territory of research in PC vision, making numerous significant commitments since the 1990s. Lately the accentuation of face acknowledgment investigation has moved to managing unconstrained conditions, remembering inconstancy for surrounding lighting, present, demeanor, face size, impediment and good ways from the camera. Unconstrained face acknowledgment is as yet an open issue as best in class calculations have not yet arrived at high acknowledgment execution in certifiable conditions. This paper tends to this issue by proposing another methodology called Sparse Fingerprint Classification Algorithm (SFCA). Calculations dependent on Sparse Representation Classification (SRC) have been generally investigated as of late. In the scanty portrayal approach, a word reference is worked from the display pictures, and coordinating is finished by recreating the question picture utilizing an inadequate straight blend of the lexicon.

Two main contributions of the approach are:

- A new representation for the gallery face images of a subject; this is based on representative dictionaries learned for each subject of the gallery which correspond to a rich collection of representations of selected relevant parts that are particular to the subject's face.
- A new representation for the query face image: this is based on
  - i) A discriminative criterion that selects the best test patches extracted from a grid of the query image.
  - ii) A 'sparse fingerprint' made with a binary sparse representation of the best patches.

This baseline approach, however, shows three important disadvantages:

- The location information of the patch is not considered, i.e., a patch of one part of the face could be erroneously represented by a patch of a different part of the face.
- The method requires a huge dictionary for reliable performance, i.e., each sparse representation process would be very time consuming.
- Not all query patches are relevant, i.e., some patches of the face do not provide any discriminative information of the class (e.g., patches over sunglasses or other kinds of occlusion).

Chang-TsunLi1 and Xufeng Lin "A fast source-oriented image clustering method for digital forensics" EURASIP Journal on Image and Video Processing, 2017:

These days, advanced imaging gadgets, particularly cell phones with worked in cameras, have become a basic piece of current life. They empower us to store, record everything about our life wherever and anywhere. In the interim, the ascent of web based life, for example, Facebook, Twitter, and Instagram, has encouraged and invigorated our enthusiasm for sharing photographs and recordings over informal communities utilizing versatile

imaging gadgets. From one perspective, internet based life manages us another approach to communicate kinship, closeness and network. In any case, then again, the trouble of confirming the profiles or personalities of clients on interpersonal organizations additionally offers ascend to the cybercrime.

This paper introduces a calculation that is fit for bunching pictures taken by an obscure number of obscure computerized cameras into gatherings, to such an extent that each contains just pictures taken by a similar source camera. It first concentrates a sensor design commotion (SPN) from each picture, which fills in as the unique mark of the camera that has taken the picture. The picture grouping is performed dependent on the pairwise relationships between camera fingerprints separated from pictures. During this procedure, each SPN is treated as an irregular variable and a Markov arbitrary field (MRF) approach is utilized to iteratively allot a class name to each SPN (i.e., arbitrary variable). By turning to gadget fingerprints separated from pictures, source-arranged picture grouping can be isolated into two fundamental successive tasks: the extraction of gadget unique finger impression from pictures followed by a picture bunching activity dependent on the gadget fingerprints. The primary goal in bunching applications is to aggregate examples into groups of comparative highlights (e.g., the SPNs). The proposed calculation makes the accompanying enhancements:

i) Redefining the similarity in terms of the shared nearest neighbors.

ii) Speeding up the calculation of the reference similarity.

iii) Refining the determination of the membership committee.

iv) Reducing the complexity of calculations in each iteration.

v) Accelerating the speed of convergence.

The main challenges in this scenario are:

i) The investigator does not have the cameras that have taken the photos to generate quality reference device fingerprint.

ii) No prior knowledge about the number and types of the cameras are available.

iii) Given the sheer number of photos, analyses each image in its full size is computationally prohibitive.

These algorithms are evaluated and compared on real-world databases to provide insight into the pros and cons of each algorithm and offer a valuable reference for practical applications.

Marc Oliu Simón, Ciprian Corneanu, Kamal Nasrollahi, Olegs Nikisins, Sergio Escalera, Yunlian Sun, Haiqing Li4, Zhenan Sun, Thomas B. Moeslund, Modris Greitans "Improved RGB-D-T based face recognition" The Institution of Engineering and Technology, March 2016:

Solid facial acknowledgment frameworks are vital in different applications from diversion to security. On account of the profound learning ideas presented in the field, a noteworthy improvement in the exhibition of the unimodal facial acknowledgment frameworks has been seen in the ongoing years. Simultaneously a multimodal facial acknowledgment is a promising methodology. This investigation consolidates the most recent accomplishments in the two bearings by applying profound learning convolutional neural systems (CNN) to the multimodal RGB, profundity, and warm (RGB-D-T) based facial acknowledgment issue beating recently distributed outcomes. Moreover, a late combination of the CNN-based acknowledgment hinder with different hand-made highlights (neighborhood double examples, histograms of arranged angles, Haar-like rectangular highlights, histograms of Gabor ordinal measures) is presented, exhibiting surprisingly better acknowledgment execution on a benchmark RGB-D-T database. The acquired outcomes right now that the traditional designed highlights and CNN-based highlights can supplement each other for acknowledgment purposes. The related work area has been written in three sections: first, they survey a portion of the multimodal face acknowledgment frameworks. At that point, the related best in class profound learning-based frameworks are talked about. Next, the subtleties of the HOGOM highlights which appear to contribute decidedly to the combination with profound learning-based facial highlights are returned to. The proposed CNN approach is executed as a parallel arrangement issue anticipating whether two information outlines compare to a similar individual or not. The methodology takes as info the rescaled facial areas of the two methodology explicit edges to be looked at as isolated channels, preparing a different CNN for every methodology. CNN doesn't encode the position and direction of the article into their forecasts. CNN are not really invariant to huge changes of the info information. This shows both the intensity of surface descriptors which is a decent alternative while segregating between a little arrangement of people. This system, however, can't sum up to inconspicuous people, which drives us to additionally break down the other thought about methodologies.

3. PROPOSED WORK

3.1 OVERVIEW

One of the major issues in the banking sector is the ATM security breach and misuse of the user's account. This can be solved by using the Facial Recognition System in the ATM stations to identify and verify the user's transaction account. Extra protection is given by submitting an email to the customer to confirm the transaction, so it often provides the individual using the device a live picture such that no violation or failure will occur throughout the ATM station. If there is a breakage or some unexplained user entry, the device sounds an alarm.

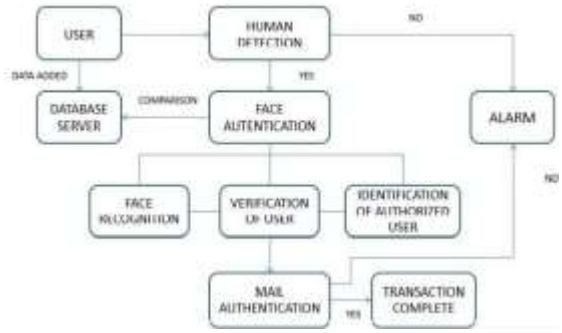

Fig -4: Data Flow Diagram

3.2 MODULAR DESIGN

3.2.1 Human Detection*:*

Sense movement and presence of individuals inside the ATM utilizing Passive Infrared Sensor (PIR).A standoffish infrared sensor (PIR sensor) is an electronic sensor that gauges infrared (IR) light exuding from objects in its field of view. They are regularly utilized in PIR-based movement locators. PIR sensors are ordinarily utilized in security cautions and programmed lighting applications. PIR sensors perceive general improvement, anyway don't give information on who or what moved. For that reason, a functioning IR sensor is required. PIR sensors are regularly called just PIR, or some of the time PID, for inactive infrared finders. The term detached alludes to the way that PIR gadgets don't transmit vitality for location purposes. They work completely by identifying infrared radiation (brilliant warmth) produced by or reflected from objects.

3.2.2 Face Authentication*:*

Biometric facial authentication makes use of biological characteristics to identify people. Facial Recognition System uses Haar-Cascade algorithm to identify the user.

User Recognition*:*

User Recognition used in the description of biometric systems such as facial recognition. PIR sensor detects the entry of a human, and the user's first five live images are obtained from the webcam installed in the ATM system.

Verification of user:

User Verification is the process in which the biometric program seeks to validate the reported identification of a person by matching a sample provided to previously enrolled photographs.

Identification of user:

User Identification is the function where the biometric device searches for a reference database and identifies a match for the biometric sample submitted.

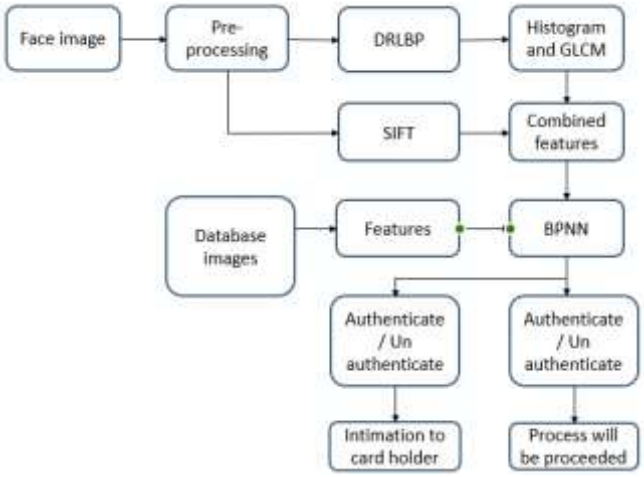

Fig -5: Face Recognition System

3.2.3 Email Authentication:

Email protection is a technical solution that proves a user is not being forged. In other words, it provides a means to check that an email originates from who it seems to be. The most growing use of email security is to restrict users. Here email protection is used in the proposed system to transfer ATM-recognized photos and to submit a One Time Password (OTP) only by the authorized user.

3.2.4 Alarm Module:

Detects the wrong person, notifies the administrator and activates the alarm. Helps discourage acts that smash or destroy devices, intimidating ATM operators with incorrect software masks to do transfers and any other ATM customers.

4. CONCLUSION

Time and protection are the key benefits of biometric authentication at the ATM. Not only will hackers have a harder time getting into a consumer's account when it is secured by facial recognition. Facial recognition can improve account security and customer privacy.

REFERENCES

[1] Rahimeh Rouhi, Flavio Bertini, Danilo Montesi, Xufeng Lin, Yijun Quan, And Chang-Tsun Li "Hybrid Clustering of Shared Images on Social Networks for Digital Forensics", IEEE Access, Vol 7, pp 87288, July 2019.

[2] Giuseppe Amato, Fabrizio Falchi, Claudio Gennaro, Fabio Valerio Massoli, Nikolaos Passalis, Anastasios Tefas, Alessandro Trivilini and Claudio Vairo "Face Verification and Recognition for Digital Forensics and Information Security", IEEE Access, May 2019.

[3] Arun Kumar, Vasanth Kumar, and Aravindan "ATM Security Using Face Recognition" International Journal of Current Engineering and Scientific Research, Vol. 5, 2018.

[4] Tomas Larrain, John Bernhard, Domingo Mery and Kevin Bowyer "Face Recognition Using Sparse Fingerprint Classification Algorithm" IEEE Access, Vol.12, pp. 1646-1647, July 2017.

[5] Chang-TsunLi and Xufeng Lin "A fast source-oriented image clustering method for digital forensics" EURASIP Journal on Image and Video Processing, June 2017.