Face recognition Based New generation ATM System

Ms.Reshma B Nair[1], Sathiya Priya V[2], Swetha G V[3], Balakrishnan P[4]
[1] Dept of Information Technology
[2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India.
(An Autonomous Institution Affiliated to Anna University, Chennai.),

Abstract- *In today's world there is a wide usage of ATM systems for withdrawal of money but the security measures are not that much efficient.In order to improve the security measures we have proposed the new generation ATM machine which is based on face recognition. In the meantime, high quality image with many details has important role in recognition process. In this paper, face image is used for authentication purpose. Initially, face image of particular person is compared with the database image. Then the comparison output result is send to the control unit through serial communication. If the person is unauthorized means, the message is sent to the concern.*

Keywords- ATM-Automated Teller Machine, Open CV-Open source Computer Vision,IPP-Integrated Performance Primitives, MLL-Machine Learning Library, LBP-Local Binary Pattern, BSIF-Binarized Statistical Image Features

I. INTRODUCTION

Automated teller machines (ATMs) are the devices which are used by everyone to withdraw money for both personal and business purposes. ATMs are now available even in remote places. ATMs becomes more popular and it is familiar to the people and they can access it. ATMs are now found in most of the locations having a regular or consumer traffic at peak volume. For example, ATMs are typically found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centers, airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are available to customers on a continuous basis such that customers have the function to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week. In the proposed system we have used Image Processing concept to detect thieves who are in the most wanted list in the police station database by using a camera to detcet the face of the person and in case if the face matches with the faces in the police database a message will be sent to the near by police station. Image processing is processing of images using mathematical operations by using any form of signal processing for which the input is an image, a series of images, or a video, such a photograph or video frame; the output of image processing may be either an image or a set of imageistics or the arguments related to that image.Most of the image-processing techniques treats their image as a two-dimensional signal and applies standard signal-processing techniques to it. Imagesare also processed as three-dimensional signals where the third-dimensional images are being time or the z-axis.An image is enhanced as shown in Figure 1.

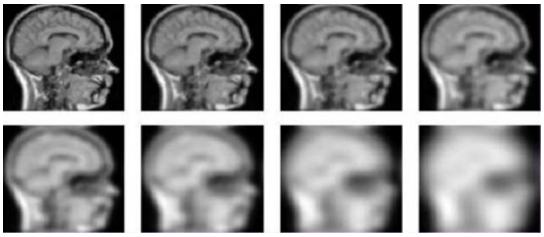

Fig. 1 Enhancement of an image

Ii. Review Of Literature

Introduction

The basic idea for Image Processing is done on various steps and several algorithms have been proposed for it. The below papers are analysed and the captured images are processed and matched based on the idea from these papers. The idea for displaying message when the face is not recognised and sending alert message to the concern has also been referred.Here the major references considered are briefly discussed.

Review

Here the main idea is to focus on how to make the money secure using the biometrics for personal recognition as the no of fraud attacks on ATM's is increasing day by day. Instead of using ID cards or keeping the pin or password in memory, this system proposed a secure method by matching the fingerprint and the recognition of iris. It provides high

accuracy and secure transaction of money.The features of the image and the image quality are taken into account and to recognize the iris Hough Transform is used .False rates to accept and reject were used to provide accurate results .A code is generated from the fingerprint image which is captured .After the fingerprint and iris are recognized the OTP is sent to the registered mobile using GSM technology[1].

An Automated Teller Machine model is well grounded in providing security and the development of such system would serve to protect users and financial institutions alike from burglar and identity thieves. The ATM model of security will combine a physical card access, a PIN,electronic facial recognition, that will go as long as the thief is holding the duplicate card. Faces are protected as like PINs when this technology becomes widely used. However, it is clear that person's biometric features cannot be duplicated, this will take a long time to solve the problem of account safety so that the actual account owner alone can have access to his accounts. The combined biometric features approach serves the purpose of both the identification and authentication of that card and PIN do[2].

The information age is revolutionizing qiuckly the way where the transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. Accurate user identification and authentication is required in a greater demand as electronic transactions has grown to a greater extent. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Using the proper PIN gains access, the successful transactions can occur, but the user of the PIN is not verified[3].

The LBP feature distributions are extracted for face image which divides into several regions and concatenated into an enhanced feature vector to be used as a face descriptor. Different challenges are faced when the proposed method's performance is evaluated. Other applications and several extensions are also discussed along with this paper regarding face image[4].

Secure-PIN-Authentication-as a- Service (SEPIA),which is a secured obfuscated PIN authentication protocol for ATM and other point-of-service terminals that uses cloud- connected personal mobile and wearable devices are being proposed in this system. The shoulder-surfers and partial observation attacks are protected by the user as proposed in this model and is also resistant to relay, intermediate transaction attacks and relay[5].

The complete process here includes vein capturing, extracting, and pattern matching. If we shine near-infrared (NIR) light through fingers, human tissues pass through most of them whereas hemoglobin in our blood blocks it. Thus veins become visible darker in the image. The vein image of each fmger has different properties such as brightness and contrast. Accordingly some image enhancement techniques should be needed for improving the quality of the image. Then the veins are extracting out by detecting centre line of the vein by means of maximum curvature points. The width of the vein may differ when blood pressure or temperature changes but the center line of the vein always stable. Then the extracted lines will be stored in a database for future purpose. To implement the proposed system on image analysis platform, LABVIEW (Laboratory Virtual Instrument Engineering Workbench) is preferred. It is the effective programming language to implement data acquisition, image analysis and image processing functions in a graphical manner[6].

The FDS system consists of The four components of FDS system are rule-based filter, Dumpster–Shafer adder, Bayesian learner and transaction history database. In the rule-based component, the suspection level of each and every incoming transaction based on the extent of its deviation from good pattern is determined. An initial belief is computed based on multiple evidences using Dempster-Shafer's theory. Then the initial belief values are combined to obtain an overall belief by applying Dumpster–Shafer theory. Either the transaction is classified as suspicious or the depending on this initial belief. When the transaction is suspicious, based on its similarity with fraud transaction or genuine transaction history, belief is then strengthened or weakened. For this process Bayesian learning is used. It has high accuracy and high processing Speed. It improves detection rate and reduces false alarms and also it is applicable in E-Commerce. But its processing Speed is low and it is highly expensive[7].

The fake terminal problem occurs in many setting, such as ATMs and point of sale terminals, and public internet kiosks. The internet kiosks is the short-term access to the Internet from public terminals and is increasingly common feature in malls, airports, browsing centers and other public places. There is little risk for users who merely want to search in the web from these terminals. The central system knows about legal terminals and can authenticate them. To authenticate the central server information is necessary and the information needed for the central server to authenticate users has already been set up during user initialization steps e.g., agreeing on a shared key. Once an entity authenticates another, A confidential, authenticated channel is established only when an entity authenticates another. Ie., an attacker cannot hijack a channel resulting from the authentication

procedure. First we consider the scenario where a user has a full-fledged trusted personal device with its own output channel, such as a display screen. The terminal cannot access the device output channel. Consequently, the user can be sure that any information is communicated to him via this channel does in fact originate from his trusted personal device. In other words, there is a trusted path from the trusted personal device to the user. When a user U walks up to an untrusted terminal, he attaches his device D to the terminal T by some means (e.g., infrared link, physical connection) and the following message flows take place[8].

Local features were used for object category recognition and classification. The comparison of descriptors in this context requires a different evaluation setup. It is not clear how to prepare the ground truth and how to select preventatives set of images for object category because there is no linear transformation relating images in a category.

Here, the comparison is carried out for different descriptors, interest regions, and for different matching approaches It introduces a new descriptor by performing more exhaustive evaluation. Several types of descriptors and detectors have been added to the comparison. A larger variety of scenes types and transformations are present in the data set. The evaluation criterion have been modified and recall-precision for image pairs is used. The ranking of the top descriptors and the ROC-based evaluation is the same. The gradient location and orientation histogram (GLOH), outperforms SIFT and the other descriptors[9].

A computation and theoritical simple approach which is robust in terms of gray scale variations and is shown to discriminate a large range of rotated textures efficiently. Extending our earlier work. It presents a gray-scale and rotation invariant texture operator based on local binary patterns. From the starting, the joint distribution of gray scale values of a symmetric circular neighbor set of pixels in a neighborhood of local, we derive an operator that is, by definition, invariant against any monotonic transformation of the grey scale. The gray-scale invariant operator has a fixed set of rotation invariant patterns and hence rotation invariance is achieved. The major contribution of this work lies in recognizing that local binary texture patterns which terms “uniform” are fundamental properties of local image texture and in developing a generalized gray-scale and rotation invariant operator for detecting these “uniform” patterns[10].

Conclusions

Considering the pros and cons of the existing systems, a combination of everything can be done so that a new system can be introduced with a completely wide usage. By keeping the time elapsed, in the verification process to a negligible amount we even try to maintain the efficiency of this ATM system to a greater degree. The problem of illegal transactions can be solved by using biometrics for identifying account owners and authenticating them at Automated Teller Machine’s. In this paper, we have tried to prefer a solution to the much dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics that can be made possible only when the account holder is physically present. In the Face recognition technology of ATM, pose variance, false positives are still a problem. LBP clearly show that facial images can be seen as a composition of micropatterns such as flat areas, spots, lines, and edges. A proof-of-concept prototype implementation was used to perform experimental analysis and a usability study.

III. EXISTING SYSTEM

Most of the users are finding ATM’s as a convinient and easy way for withdrawing money whenever needed. In our existing system, ATMs typically provide instructions on an ATM display screen that are read by a user and this provides interactive operation of the user and the ATM. Having read the display screen instructions, a user is able to use and operate the ATM via data and information entered on a keypad. And a camera is fixed on every ATM to detect any problem. However the drawback in the existing system is that the camera which is fixed there is not continuously monitored. Camera will record the video and in case if there is any problem, it will be checked later. The main drawback is that the camera is checked only after the robbery has taken place and the thieves are not immediately caught and because of this it takes a lot of time to recover the money.

IV. PROPOSED SYSTEM

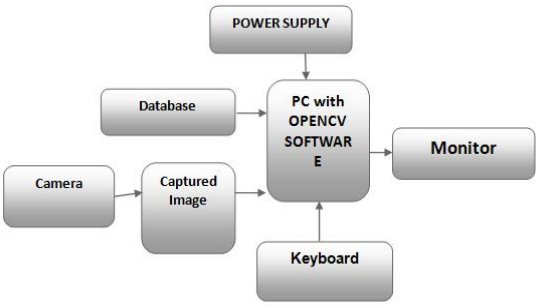

Fig. 2 Block Diagram for the proposed system

Figure 2 shows the block diagram of the proposed system. A camera will be fixed at the ATM system and the video will be recorded continuously. So when a person enters

into ATM to withdraw money the his image will be recorded by the camera and his face will be detected. When the person has covered his face with the mask ie., when the face of the person is not detected by the camera a message will be displayed on the display screen stating that he should remove his mask for entering the pin number. In case if the person's face matches with the face in the police database a message will be sent to the nearby police station.

The following are the modules in the proposed system,

1. Face Detection using Haarcascade Method
2. Face reorganization using LBP Algorithm
3. Alert message Through the Way2SMS.

After the face is detected from the image it should be recognized. A typical image recognition system consists of pre-processing, segmentation, feature extraction, classification and recognition, and post processing stages.

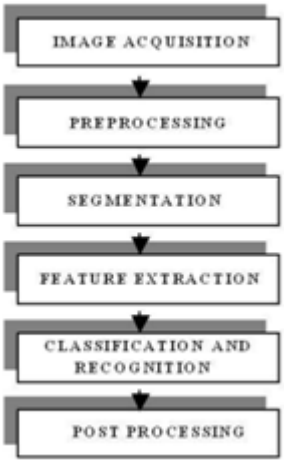

Fig. 3 Block Diagram for Image Recognisation.

After the image has been processed as shown in Fig 3 and recognized based on the results the SMS is sent to the nearby police station to catch the thief.

V. CONCLUSIONS

The proposed system can be used to detect the most wanted thieves in the police database who are entering into the ATM systems. This system is more reliable and accurate as compared to the previous existing systems. Therefore police can easily find the thieves continuously involved in ATM robbery. The Police arrests the thieves a bit earlier and thus ATM is also secure and safe from thieves.

REFERENCES

[1] Joyce Soares,A.N.Gaikwad,"A Self Banking Biometric Machine with Fake Detection Applied to Fingerprint and Iris along with GSM technology for OTP"-IEEE International Conference on Communication and Signal Processing, April 2016

[2] Aru, Okereke Eze, Ihekweaba Gozie," Facial Verification Technology for Use In Atm Transaction"-American Journal of Engineering Research(AJER) Volume 2, Issue 5,2013.

[3] KJohnPeter, G. Nagarajan,G. GiminiSahaya Glory, Sanjana Devi. V.V ,Dr S.Argman, Dr. K Sentamarai Kannan, "Improving ATM Security via Face Recognisition"-IEEE Volume 3,Issue 11,2011

[4] TimoAhonen, AbdenourHadid, and MattiPietika¨inen, "Face Description with Local Binary Patterns:Application to Face"- IEEE transaction on pattern analysis and machine intelligence Volume 28,Issue 12,2006

[5] Rasib Khan, RagibHasan, and Jinfang Xu, "SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices"IEEE conference on mobile cloud computing and engineering Volume 5,Issue 15,2015

[6] N.Sugandhi, M.Mathankumar, V.Priya," Real Time Authentication System using Advanced Finger Vein Recognition Technique"-IEEE international conference on Communication and signal processing April 2014

[7] S. Benson Edwin Raj, A. Annie Portia,"Analysis on Credit Card Fraud Detection Methods"-IEEE International conference on computer communication and electrical technology(ICCCET) March 2011

[8] Chang Yu Cheng, KamaruzamanSeman, JasmyYunus," Authentication Public Terminals with Smart Cards"-IEEE 2000

[9] KrystianMikolajczyk and CordeliaSchmid," A Performance Evaluation of Local Descriptors"-IEEE Transactions on pattern analysis and machine intelligence Volume 27,Issue 10,Oct 2005.

[10] TimoOjala, MattiPietika¨inen," Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns"-IEEE transactions on pattern analysis and machine intelligence Volume 24,Issue 7,July 2002.