International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

AUTOMATED OBJECT DETECTION AND SUSPICIOUS BEHAVIOR ALERT IN ATM USING EMBEDDED SYSTEM

Ramkumar V

PG Student, Embedded System Technology, Velammal Engineering College, Chennai, India

***Abstract*— We are living in modern world and modern concept, in our daily life extensively utilized financial transaction using one of standard method ATM(automated teller machine).In usage of automated teller machine center the ATM frauds and customer vulnerable attacks increasing day by day .The suspicious activities detection in public area using video surveillance has attracted and increasing level of attention but not sufficient in real time. In general automated offline or semi supervised video analysis have be used for post event detection. To overcome this drawback, this paper proposes a novel method for unsupervised face recognizability with exceptional occlusion handling of user and their activity detection in ATM is advent of technology in field of real time image processing with ARM 11 based embedded system**

***Index Terms*—Facial recognition, ARM 11, Web Server, Embedded system.**

I. INTRODUCTION

Automatic Teller Machine (ATM) use is now one of the standard methods for making financial transactions and is continuously increasing due to its convenience [1].However, as the usage of ATMs increased, related crimes have also been on the rise to become major threats for both the customers and banks worldwide [2]. For the purpose of suppressing the related crimes, there have been considerable efforts by introducing various methods of biometrics. These biometrics-driven efforts can be categorized into two approaches. The first approach is by requesting the biometrics such as face, fingerprints or finger veins as an essential part of on-site user authentication [3]-[5] before being allowed to make any financial transactions. The other approach is to capture the images of a user at the ATM and use those images in the process of criminal face matching for follow-up criminal investigations [6].The second approach is more commonly utilized by the ATM systems because of its advantages in providing non-intrusive environment, and less time consumption in making a transaction. However, it suffers from difficulties in tracking down the suspects when their faces are heavily occluded unable to be recognized. It is reported that the suspects tend to take advantage of its weakness by occluding their faces with typical objects such as sunglasses or masks [7]-[14]. Figure 1 shows the images of the suspects with heavy facial occlusions captured by the actual ATMs mostly difficult to be recognized. To reduce the tendency of similar sorts of fraud, an extensive research has been devised and can be categorized many form approaches: specific attack detection, multi angle-based face recognition . The first approach, specific attack detection, like as fighting. First of all, the method is able to handle users with various partial occlusions since it tries to look for the existence official components instead of detecting specific occluding objects. Moreover, this method can show a relatively superior performance over the second approach in various lighting conditions by employing a gray image sequence-base detection and verification scheme. Although the method can show a degraded performance with the non-frontal faces, this problem can be overcome by applying a scenario that guarantees to provide images of frontal faces. In spite of all the advantages, the above method bears the following problems when applied in the actual ATM environments due to the reason that it uses the local information of facial components such as eyes or mouth. The first type of problem arises when partial, yet acceptable, occlusion over the facial features causes the system to reject the face even if it is recognizable in the global perspective. Another type of problem is falsely accepting a user by wrongly locating a local region closely similar to the regions in the actual facial components. shows a frequently occurred situation where local patterns found on the reflecting surfaces of sunglasses could be mistaken for real eyes To overcome these obstacles, this paper proposes a method that combines an exceptional multi different angle calculation utilize unique training of input image. After the system carries out a face recognisability evaluation based on verifying the facial components within the face area, the trained set reaffirms whether the user is falsely rejected or falsely accepted possibly caused by any misleading occlusions. The proposed process can be carried out by two different approaches: 1) find shape, mouth and eye position , 2) Focus the falsely accepted cases. In this paper, two typical facial occlusions (eyeglasses and mask) which frequently interrupt the facial component-driven recognisability evaluation are chosen to represent the two different approaches of the process. In the experiments, we have acquired a database which consists of trained image sequences including 20 subjects. To build a more realistic database to have used an off-the-shelf ATM while the users were asked to make the actual withdrawals. The evaluation results using the acquired ATM database clearly showed a reasonable performance in the practical ATM environments.

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

Figure 1.Different occlusion face mask and eyeglass

II. FACE RECOGNITION

Facial recognition is one of the boon given to surveillance system advent of technology field of image processing. Face recognition is challenging task of image or video analysis in computer vision. The security of information is very significant and difficult. The security cameras are presently common in Offices, airports, University, ATM, Bank and in any locations with a security system. Recognition is a biometric system used to identify person from a digital image or video. Recognition system is used in security. Face recognition system could be able to automatically detect a face in video. This involves extracts its features and then recognize it, regardless of expression, lighting, illumination, ageing and pose, which is a difficult in real time environment. The real time video for a facial recognition system is to recognize face and extract it for the rest of the scene. then, the system measures edge points on the face, (such as the distance between the shape, and eye of the cheekbones and other distinguishable features.) These edge points are then compared to the nodal points computed from a database of trained model in order to find a match, the facial recognition working flow as shown in the Fig 2 step by step guidance.

III. PROPOSED METHOD

In this paper, a facial image sequence that contains a mouth and at least an eye visible is defined as recognizable. In general, a visible mouth and a visible eye mostly guarantees a half of a face visible in longitudinal direction. Moreover, longitudinal half faces are proven to provide adequate information for criminal investigations [15] and automatic face recognition [16]. Nose is excluded from the definition assuming that there are almost no criminals occluding only the nose area when other facial components are completely visible. The proposed method is operated according to the algorithm shown in section 4 . To begin with, the image sequences are acquired during the 25 to 30 second period centred at the moment of the card insertion. Images which have higher probabilities of containing frontal faces are selected to be used in the following procedures. Recognisability evaluation is performed by verifying the facial components (eyes and mouth) found in the face regions using the selected images.

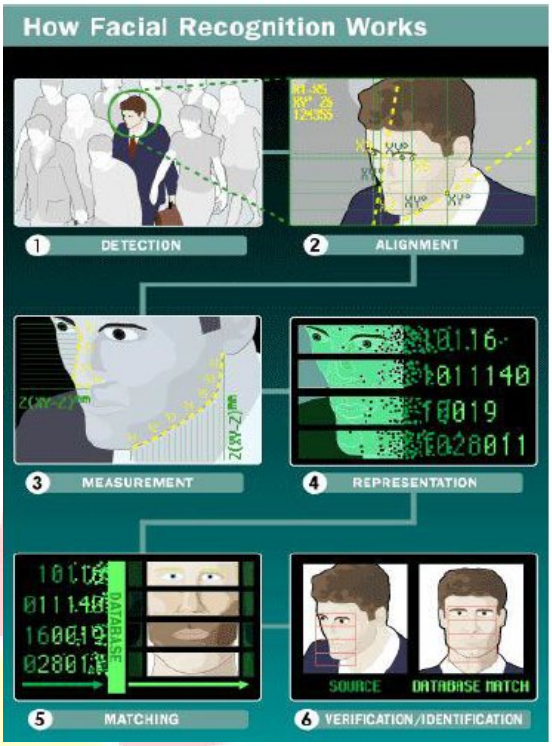


Figure 2 work flow of face recognition

Finally, the exceptional occlusion handling process is carried out to eyeglasses) near the facial components. The latter approach is activated when the face is evaluated as recognizable. It reaffirms the handle problematic, yet typical occlusions which frequently occur in real ATM situations. As shown in the program, the proposed process consists of two different approaches. One is accepting the falsely rejected cases and the other is trained set the multiple accepted cases. The former approach is activated when the recognisability evaluation procedure makes a decision that the face is non-recognizable. The decision is reaffirmed by checking the existence of typical acceptable occlusions (in this case, sunglasses) within the face regions. primary decision by searching for non-acceptable, yet commonly occurring occlusions (in this case, sunglasses) within the face regions. Since the objective of the system is to acquire a recognizable face of the user, it is designed to be terminated as soon as recognizable facial image is acquired

Figure 3 proposed module

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

IV.ALOGRITHM IMPLEMENTATION

In algorithm implementation using Discriminant Analysis(DA) stopover of Principal Components Analysis(PCA) which give eigenvectors correspond to the least-squares (LS) solution. LDA is used to find the subspace representation of a set of face images, the resulting basis vectors defining that space.

Let X be a random vector with samples drawn from c classes:
X = fX1;X2; : : : ;Xcg
Xi = fx1; x2; : : : ; xng
The scatter matrices SB and SW are calculated as:

$$S_B = \sum_{i=1}^{c} N_i(\mu_i - \mu)(\mu_i - \mu)^T$$

$$S_W = \sum_{i-1}^{c} \sum_{x_j \in X_i} (x_j - \mu_i)(x_j - \mu_i)^T$$

where μ is the total mean:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} x_i$$

And μi is the mean of class i $\in$ {1; : : : ; c}:

$$\mu_i = \frac{1}{|X_i|} \sum_{x_j \in X_i} x_j$$

Fisher's classic algorithm now looks for a projection W, that maximizes the class separability criterion:

$$W_{opt} = \arg\max_W \frac{|W^T S_B W|}{|W^T S_W W|}$$

a solution for this optimization problem is given by solving the General Eigen value Problem:

$$S_B v_i = \lambda_i S_w v_i$$
$$S_W^{-1} S_B v_i = \lambda_i v_i$$

SW is at most (N-c), with N samples and c classes. pattern recognition have problems the no of samples N is almost always smaller than the dimension of the input data. so scatter matrix SW becomes singular. DA was then performed on the reduced data, because SW isn't singular. The optimization problem

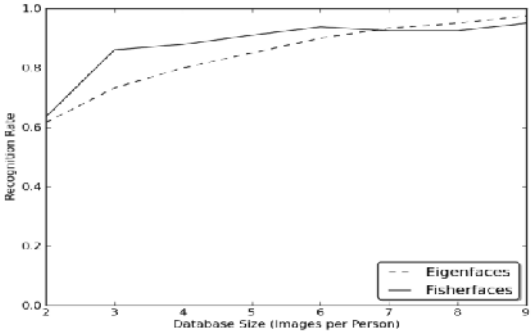
$$W_{pca} = \arg\max_W |W^T S_T W|$$
$$W_{fld} = \arg\max_W \frac{|W^T W_{pca}^T S_B W_{pca} W|}{|W^T W_{pca}^T S_W W_{pca} W|}$$

The transformation matrix W, that projects a sample into the (c-1)-dimensional space is as denote

$$W = W_{fld}^T W_{pca}^T$$

Although SW and SB are symmetric matrices, the product of two symmetric matrices is not necessarily symmetric. so have to use an eigen value solver for general matrices. OpenCV's cv::Eigen only works for symmetric matrices in its current version; since eigen values and singular values aren't equivalent for non-symmetric matrices then can't use a Singular Value Decomposition (SVD)

The optimization problem evaluate as the curve denote accuracy of recognition rate at fig3.



In Face database has the same length as an original image, thus it can be displayed as an image. Well again load the data, learn the faces and make a subplot of the first 16 faces. The PCA faces method learns a class-specific transformation matrix, so the they do not capture illumination as obviously as the Eigen faces method. The Discriminant Analysis instead finds the facial features to discriminate between the persons. It's important to mention, that the performance of the Fisher faces heavily depends on the input data as well. if learn the Fisher faces for well-suited pictures only and you try to recognize faces in bad-illuminated scenes, then method is likely to find the wrong components (just because those features may not be predominant on bad illuminated images). This is some what logical, since the method had no chance to learn the illumination.

```
import sys
 sys . path . append ("..")
import numpy as np
from tinyfacerec . subspace import fisherfaces
from tinyfacerec . util import normalize , asRowMatrix , read_images
from tinyfacerec . visual import subplot
# read images
[X,y] = read_images ("/ home  / data / faces_recognition ")
 [D, W, mu] = fisherfaces ( asRowMatrix (X), y)
import matplotlib .cm as cm
E = [1]
for i in xrange ( min(W. shape [1] , 16) ):
e = W[:,i]. reshape (X [0]. shape )
E. append ( normalize (e ,0 ,255) )
e = W[:,i]. reshape ( -1 ,1)
P = project (e, X [0]. reshape (1 , -1) , mu)
R = reconstruct (e, P, mu)
```

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

The above steps import the face recognition model training search path that include as format, follow in extension of image. the multi-angle with various direction. In real time running video read the image sequence with 0-7frame separation and then compute with trained model to predict the observed face identified or not, the each trained model assigned with unique Identification (ID)

V.WEB SERVER

As ARM processor based web servers do not use computer directly, it helps a lot in cost reduction. The aim of the proposed work is to implement an Embedded Web Server (EWS) based on ARM11 processor and Linux operating system , It gives a strong networking answer with wide range of application areas over internet. The web server runs on an embedded system having limited resources to serve embedded web page to a web browser. Different software can be used to implement the embedded web server, and these are mentioned below:

- Linux–operating system
- Apache–web server (http)software
- Mysql – database server
- PHP or Perl – programming languages

VI.EXPERIMENTAL SETUP

Hardware setup for experimental using ARM 11 based embedded system processor booting from linux then connect Ethernet cable to assign static IP address for access SSH control on user monitor detail in Fig 4.
It have quad-core ARM Cortex-A7 CPU and a Video Core IV dual-core GPU; 1 GB of RAM with 700 MHz . The algorithm run for facial recognition which train set of input maintain database. In real time activate camera to recognize user face in video sequence. the centriod of image Region of interest calculate displacement and overall fast changes in recognized sequence. It indicate that the most reliable mean for defining fights in environment .A minimal speed in different direction condition was also added to ensure the presence of a highly dynamic level activity. Thus defined semantics for fighting and make alarm for real time incident avoidance, all are recorded and cloud based storage for feature suspects identification and reference.

VI.RESULT AND OUTPUT

Security and passive assets in ATM rooms are managed manually and it ends up in larger physical interaction, that increase the time period and therefore shrinks the gross margin of ATM management. These MSPs are duty-bound to create certain that every ATM site is up as costs of downtime are too high. With rising overheads ATM and customer safety to pass on the cost and so are looking for a reliable unsupervised monitoring with real time solution to revitalize ATM customer usage. The proposed work implements a secure way of accessing an ATM by customers in terms of without panic, In using hardware and the above said module is accomplished by using ARM 11 based embedded system. The Fig4 capture video real time and analyze the face from trained input, and said known and unknown using unique identification ,the false analysis compare with Lucas kande algorithm in the displacement of moving object region calculate shown Fig.5 a and b.

Figure 4 predititction output image from video sequence

Figure 5(a) displacement detection

In fast moving detection using hand position to analyze displacement of recognized object and their speed of

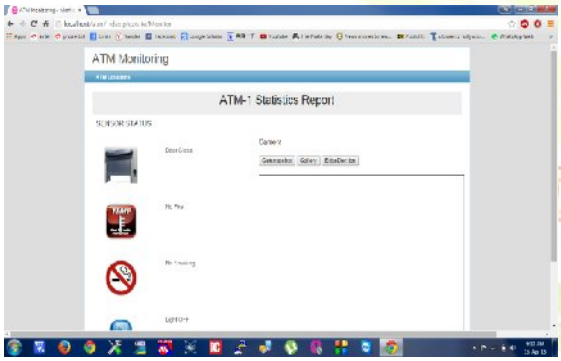
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

variation.

FIGURE 5(B) DISPLACEMENT DETECTION

VII .CONCLUSION AND FEATURE

The proper face recognition with reduce false prediction output and calculate speed of detected object using displacement calculation is done successfully using the ARM 11 based embedded system, the feature work fully implemented securely using and maintenance the ATM centre in real time environment, that attention it provides real-time monitoring and control without the need for human intervention like as unsupervised. The control is meant by smoke and fire detection Door and light ON or OFF all are Machine-to-machine(M2M)communication.



VIII. REFERENCES

[1] A. Hutchinson, "The top 50 inventions of the past 50 years,"Popular Mechanics, Dec. 2005.

[2] "ATM Crime: Overview of the European situation and golden rules on how to avoid it," European Network and Information Security Agency (ENISA), Aug. 2009.

[3] H. Sako and T. Miyatake, "Image-recognition technologies towards advanced automated teller machines," In Proceedings of the International Conference on Pattern Recognition, Aug. 2004, vol. 3, pp. 282-285.

[4] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," IEEE Security& Privacy, vol. 1, no. 2, pp. 33-42, Mar. 2003.

[5] G. Graevenitz, "Biometric authentication in relation topayment systems and ATMs," vol. 31, no. 9, 2007

[6] L. Duan, X. Yu, Q. Tian, and Q. Sun, "Face pose analysis from mpeg compressed video for surveillance applications,"In Proceedings of the International Conference on Information Technology: Research and Education, Aug. 2003, pp.549-553

.

[7] C. Wen, S. Chiu, J. Liaw, and C. Lu, "The safety helmet detection for ATM'ssurveillance system via the modifiedHough transform," In Proceedings of the Annual IEEEInternational Carnahan Conference on Security Technology,Oct. 2003, pp. 364-369.

[8] C. Wen, S. Chiu, Y. Tseng, and C. Lu, "The mask detection technology for occluded face analysis in the surveillancesystem," Journal of Forensic Science, vol. 50, no. 3, pp. 1-9,May 2005.

[9] R. Min, A. D'Angelo, and J.-L. Dugelay, "Efficient scarf detection prior to face recognition," In Proceedings of the 18th European Signal Processing Conference, Aug. 2010, pp.259-263.

[10] D. Lin and M. Liu, "Face occlusion detection for automated teller machine surveillance," Lecture Notes in Computer
Science, vol. 4319, pp. 641-651, Dec. 2006.

[11] G. Kim, J. K. Suhr, H. G. Jung, and J. Kim, "Face occlusion detection by using b-spline active contour and skin color information," In Proceedings of the International Conference on Control, Automation, Robotics and Vision,Dec. 2010, pp. 627-632.

[12] P. Kakumanu, S. Makrogiannis, and N. Bourbakis, "A survey of skin-color modeling and detection methods," Pattern Recognition, vol. 40, no. 3, pp.1106-1122, 2007.

[13] J. Kim, Y. Sung, S. M. Yoon, and B. G. Park, "A new video surveillance system employing occluded face detection",Lecture Notes in Computer Science, vol. 3533, pp. 65-68,Jun. 2005.

[14] I. Choi and D. Kim, "Facial fraud discrimination using detection and classification," Lecture Notes in ComputerScience, vol. 6455, pp. 199-208, Dec. 2010.

[15] A. Paterson, "Computerised facial construction andreconstruction," In Proceedings of the Asia Pacific Police Technology Conference, Jan. 1991, pp. 135-144.

[16] N. Ramanathan and R. Chellappa, "Face verification across age progression," IEEE Transactions on Image Processing,
vol. 15, no. 11, pp. 3349-3361, Nov. 2006.

[17] www.google.com