**Implementation of Secureye- ATM Trajectory Based Anomaly Detection System**

**Prof. Vina Lomte1 Ketaki Kulkarni2,  Pradnya Jeurkar3, Gautami Joshi4 ,**

**Supriya Dharmadhikari5**

1(Professor, Computer Engineering Department, RMD Sinhgad School of Engineering, Pune, Maharashtra, India)

2345(Students, Computer Engineering Department, RMD Sinhgad School of Engineering, Pune, Maharashtra, India)

***Abstract***—**Security is the most important issue arising due to increase in criminal acts such as child-related sexual offenses or commonplace criminal acts, to protect residents in places, and places that require high security like bank lockers, ATM centers, museum and other care facilities. Surveillance technology and its installation are increasingly being used in public areas, as part of common place criminal acts. Video surveillance is a significant application that facilitates in examine region which needs high security.**

**This paper presented an implementation of the system that provides high security to the ATM centres by detecting any anomalous activity. The system helps to judge the situation and notifies the administrator directly or immediately by reducing the human need. Motion History Image (MHI) of the centroid of the moving person and classification based on human moments are used to for abnormal behaviour of user entering in ATM. The proposed system uses algorithms like Motional Region Detection Structure as well as Background Image Update. The system detects whether a person is entering a prohibited area where he/she is not supposed to enter.**

1. **Keyword**

**Secure-eye , ATM Trajectory Anomaly Detection System, Motion History Image (MHI), Human Moment Tracking, Video Recording, Template Matching , Admin Notification , Track/Log Of All Activities.**

1. **INTRODUCTION**

Security mechanisms of automated teller machines (ATMs)

can be undermined by several escalating attacks.

Security mechanisms of automated teller machines (ATMs)

can be undermined by several escalating attacks.

Security mechanisms of automated teller machines (ATMs) [1][6] [7] can be undermined by several increasing attacks as it is one of the typical ways to get cash around the world. Physical attacks on ATMs are measured risky, as it not only leads to economic losses but also contains the risk to property and life. The physical attack involves removal of ATM from the site and later using other techniques to gain access to the cash dispenser, Performing ATM transaction opens the shutter of ATM cash. Figure 1 shows ATM attack where, the attacker amid the breaking of ATM Machine. The ATMs located in remote zones can be equipped with by proper physical security. If the posture and Gesture of the human entering to the ATM machine is detected, we can avoid such threats by alerting admin or any higher authority.

Security mechanisms of automated teller machines (ATMs)

can be undermined by several escalating attac



**Figure: 1** Human posture and Gesture amid the breaking of ATM [2]

ATM systems are equipped with CCTV cameras that keep an eye inside ATM. Unfortunately, due to their inability to detect suspicious activities themselves, CCTV is not adequate to provide protection. . However, most of the ATMs were equipped with a security camera. There was no pace maintained for tracking capabilities. Even due to the absence of security guards outside the jail, the incidence of ATM crime has increased. There is therefore a significant need for an advanced device capable of detecting an ATM anomaly and reporting the ongoing criminal act to the administrator. Detection of the behaviour i.e. abnormal or not abnormal [6] [7], of the person entering the ATM can minimizing the rate of crime and avoiding any serious incidents.

Here an attempt is made to implement a system that can detect any suspicious activity happens in the ATM area. The system also detects if the user is covering his/her face using scarf. System should disable ATM if the user is not presenting clear face. The system also tracks the Trajectory of the entered person using Motion History Image (MHI) [4] of the centroid of the moving person. If the person moves from normal path system play alarm and send notification.

1. **System Objectives**

* To detect intrusion within the real time image frames.
* To provide affordable and quality Surveillance system to user with cost effectiveness.
* To send notification to the administrator so that required action is taken instantly.
* To identify the environmental change or any other suspicious activity and prevent crime with less cost.
* To control mistrustful activity happening around that object.

1. **LITERATURE SURVEY**

Sahar Torkamani et al. (2016) [1] propose an approach to detect anomalies and attacks on ATMs via motif discovery i.e unknown occurring sequences or events in a time series signal. State of the ATM is captured by innovative piezoelectric sensor networks to analyse the occurring vibrations. The captured signals are inspected by the Complex Quad-Tree Wavelet Packet transform which provides broad frequency analysis of a signal in various scales. Next, features are extracted from the selected scale based on the information content, to detect motifs. Detected motifs provide the prototype patterns for anomaly detection or classiﬁcation tasks.

Arpitha K et al.(2018) [2] used the video is considered as a dataset. These videos are converted into image frames. The frames are converted from RGB to grayscale image. SIFT and Gabor highlight descriptors are used for feature extraction. The SVM classifier is used to recognition and classification of human action like abnormal or abnormal.

Nithya Shree R et. all [3] was designed framing and blob recognition. This structure distinguishes chance in the territory under observation. One such perilous condition is executed, similar to a man with a blade. The proposed structure comprises of two fundamental segments: Framing and Blob recognition (FBD) for Input video preparing and (HON) Human tracking, Object recognizable proof and warning organize.

Vikas Tripathi et al[4]. The suggested method makes use of the picture of motion history (MHI) and Hu moments to extract appropriate video features. In order to minimize the dimensionality of features, concept component analysis was used and classification was carried out using the support vector machine. Analysis was performed by varying the window size of the MHI on different video sequences. The proposed system will differentiate between usual and irregular behaviours such as money snatching, fighting damage to the consumer or customer assault with an average accuracy of 95.73 %.

Aditya Parab et al.[7] implemented a system anomalous behaviour is detected using CNN and LSTM on the surveillance videos. The anomaly as well as non-anomaly dataset is fed to a machine and trained to identify abnormal behaviour. It is this system has proposed a method to identify and classify whether it is abnormal behaviour or not.

P B Reddy et al.[8] proposed a system where the foreground extraction is used to obtain a clear outline of people. The fixed window size was used to record motion history images. MHI is a binary image where pixel intensity is a function of recency in motion. Once MHI is obtained features are extracted using Hu moments function. These dimensions are further reduced by applying principal component analysis. The Support Vector Machine is used to predict the behaviour of the human. Data set used was their own and they received accuracy of 72% on single normal, 69.89% for multiple normal and 70% on multiple abnormal. This accuracy is quite low when it comes to the security of an ATM and as the frames increase accuracy decreases.

Machine learning based techniques were used in ATMs to detect anomalous behaviour. V. Tripathi et al. [4] proposed Random forest classification technique and in this approach data was preprocessed by dividing the video into frames and then performing it on every nth frame. It was combined into one frame and then HOG feature descriptor is used to extract useful information from that frame. Three datasets were used CAVIAR, HMDB 51 and also their own created dataset. They received 75.83% accuracy on CAVIAR and 50.84% on HMDB 5.

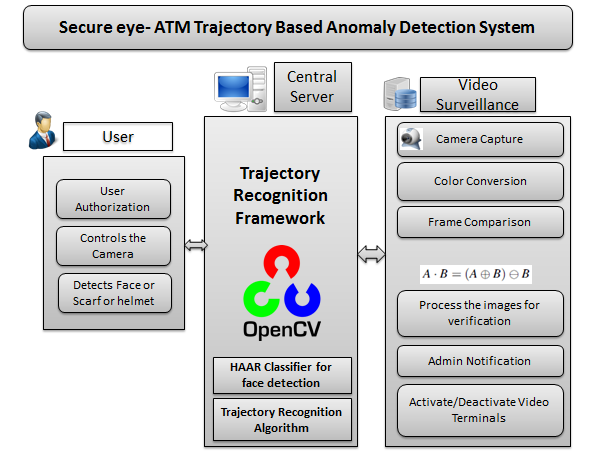
K. Kajendran and A. Pravin et al.[7] gives the system to enhance ATM security and to protect ATM center form untoward incidents. A new mechanism of different window size to capture action-rich frame that helps to identify unusual activity and alert anticrime cell to avert ATM crime. The paper gives the idea of recognizing unusual sounds such as breaking ATM machine with the rod, blaring sound of customer, bursting sound of the pistol within ATM center which generates high decibels than decibels generated by normal human conversation and alert bank personal about an ongoing crime that helps to catch culprit red handed.

A.F. Bobick et al.[9] uses temporal templates to recognize the human action. Two-component versions of the templates are used: The first value is a binary value indicating the presence of motion and the second value is a function of the recency of motion in a sequence. Then a matching temporal template is used to views of known actions. The method automatically performs temporal segmentation, is invariant to linear changes in speed and runs in real-time on standard platforms

Nievas E et al.[12] propose a method to detect violence in video sequences. Here the motion regions are segmented according to the distribution of optical flow fields than by extracting the two kinds of low-level features an appearance and dynamics for violent behaviors is given. The proposed low-level features are the Local Histogram of Oriented Gradient (HOG) descriptor extracted from RGB images and the Local Histogram of Optical Flow (LHOF) descriptor extracted from optical flow images. Finally, the extracted features are coded using Bag of Words (BoW) model to eliminate redundant information and a specific-length vector is obtained for each video clip. By using Support Vector Machine (SVM) video-level vectors are classified.

1. **SYSTEM DESIGN**
2. **System Architecture**

The designed system helps in analysing and tracking the objects and taking the required action accordingly. System helps in providing security which reduces the human need and reduces labour. Figure 1 shows the system framework of the proposed system.



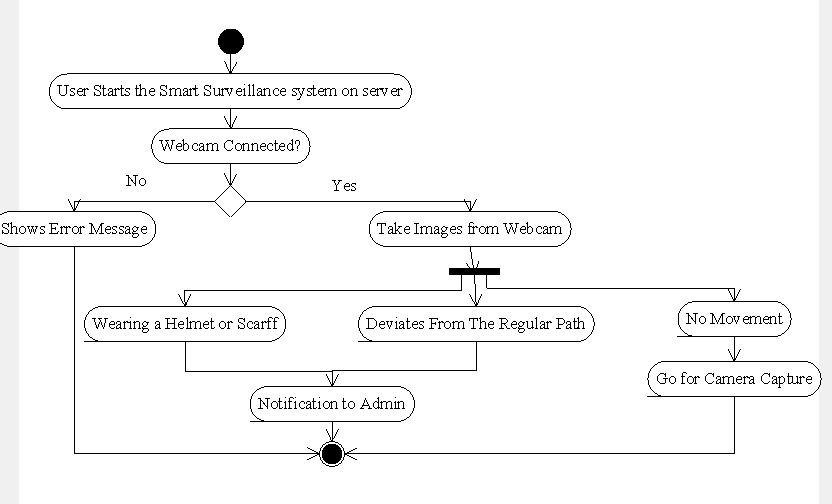
**Figure 1: System Design**

**The admin can control the remote cameras using the features like:**

* System can start and stop camera in ATM using OpenCV functions also video recording takes place using OpenCV.
* System contain 2 modes which DAY MODE and NIGHT MODE in which in day mode only video recording takes place and in night mode image capturing and comparing with template image takes place after detecting intrusion video recording takes place.

**The detailed working of the proposed system is as follows.**

1. **Smart Video Recording:** If any suspicious activity happens in the ATM area or any intrusion occurs in the system then system can record the video of the activity.
2. **Scarf or Helmet Detection:** System needs to capture if the user is covering his/her face using scarf. System should deactivate ATM if the user is not showing clear face.
3. **Image Capture and Template Recording:** When system will start will set or record the targeted area which means we store the particular target area from capture area.
4. **Template Matching against mentioned region:** Selected target area is compare with the current image frame region and analysis on it. If the mismatch found play alarm and send notification.
5. **Trajectory Recognition:** A trajectory is the path that a person moves as a function of time. The trajectory in a scene is recognized using HOG Descriptor is feature extraction algorithm.
6. **Admin Notification:** If any mismatch found at the time of image comparison system will notify the admin by sending SMS that suspectful person is there in ATM area & plays alarm. If the person is suspectful then Admin can stop him from using ATM machine.
7. **Log History:** The system keeps track/log of all the activities. Hence detailed record of messages received is maintained. Also a detailed track of all the activities (intrusion detection, etc.) is also maintained.
8. **System Flowchart**

****

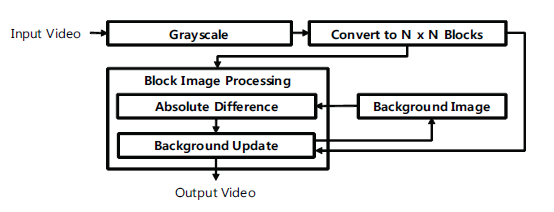
**Figure 2: System Flowchart**

1. **ALGORITHM USED**

### Motional Region Detection Structure:

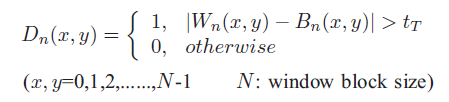
Here we present a new technique such as BSM for motion detection. That is, it uses the subtraction of the recent frame image and the background image. The background image used at this time is not a background image prepared in advance. However, it creates the background screen in real-time when video shooting. The study of this technique followed into three steps:

1. Blocking the input image and pre-processing the image by block zoning
2. Getting the difference image between the background image and block zoning.
3. Updating the background image.



# As shown in above figure, the primary input image is a TV input means given in the form of NTSC model. It is the YIQ technique. It can be transformed into to greyscale with the help of following formula. Herein, F corresponding to the frame image, and r, g, b point towards Red, Green, Blue value, correspondingly, to the pixel subsequent to the position of x and y.

# The images obtained subsequent to converting to greyscale are fragmented into the square block with the complete number of pixels, N. consequently, the complete different image of the block is divided in the front using formula.



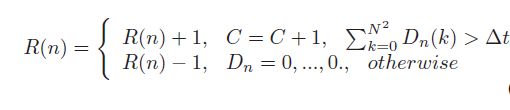
# In above formula, n represents the number of blocks, W the block corresponding to the existing image, B the block keep in touch with the background image, and D the value of the complete difference between W and B complete difference between W and B.

### Background Image Update

**Step 1:** One-dimensional array is stated to accumulate every difference image luminance variance rate by block R(n), and start with to 0. This step is performed only once throughout the first run.

**Step 2:** Integer variable C to compute the degree of the transform for the entire block is confirmed and initialized into 0. Here in, C signifies the number of blocks with a change. For the block difference image (Dn). Steps 3 and 4 are performed repeatedly.

**Step 3:** The number of pixels that have 1 as a value within the block difference image (Dn) is put together. At this time, the sum of pixels represents the change in the luminance within the block. If it is equal to or greater than t, it is considered to have a change in the movement in the block, and the value of R(n) increases by 1. In addition, the value of C increases by 1. Conversely, if the total of the pixels is smaller than t. we consider there is no change, the value of R(n) reduces by 1, and all the values of Dn are initialized to 0. The image having no change in the intensity value in the block is initialized into 0 to remove noise. Herein, t utilizes a random threshold value i.e. block size N.



**Step 4:** In above formula, if the value of R(n) is less than ‘-1', the background image of the block is updated. Otherwise, it is not updated and remains as the previous background image.

1. **MATHMETICAL MODEL**

Problem Statement:

To provide Security in ATM System and detecting, analysing, and tracking any unusual activity detect whether a person is entering a prohibited area where he/she is not supposed to enter.

Problem Description / Definition:

Let us consider S be a Systems such that

**S= {U, MS, SS, K, Dm, DS},** **where**

U= {U1, U2, U3…….Un | ‘U’ is a Set of all USERS }

There may be number of users for making use of system. So this is the Infinite Set.

MS = {MS | ‘MS’is a Set of Motion Detection Service }

This service uses the **Motion detection using block based background subtraction image** algorithm for. So this is a Finite Set as this contains limited attributes.

Cm = {C1,C2,C3| Cm is a Set of Cameras}

System contain 2 modes which DAY MODE and NIGHT MODE in which in day mode only video recording takes place and in night mode image capturing and comparing with template image takes place after detecting intrusion video recording takes place.

DS = {USERINFO, USERDATA | DS is a Set of data for storing data on server }

Dm = {USER activity | Dm is a Set of data for matching on server }

Selected target area is compare with the current image frame region and analysis on it. If the mismatch found play alarm and send notification.

ACTIVITIES / EVENTS:

**EVENT 1**

User will Enter in ATM Machine.

Let *f(U)* be a function of User

Thus, *f*(U) 🡪{ MS U Cm}

**EVENT 2**

User will in front of Camera and Video Recording is Running.

Let *f(U)* be a function of User

Thus, *f*(U) 🡪{ MS U Cm­}

**EVENT 3**

User will be authenticated.

  Let *f(MS)* be a function of Motion Detection Service.

Thus, *f*(MS) 🡪{U1,U2,U3……Un} € U

**EVENT 4**

Camera will send image initially to server side

  Let *f(MS)* be a function of Motion Detection Server.

Thus, *f*(MS) 🡪{F1,F2,F3……Fn} € F

**EVENT 5**

Image will be authenticated with Motion Detection.

 Let *f(Un)* be a function of n Users.

Thus, *f*(Un) 🡪{MS} € U

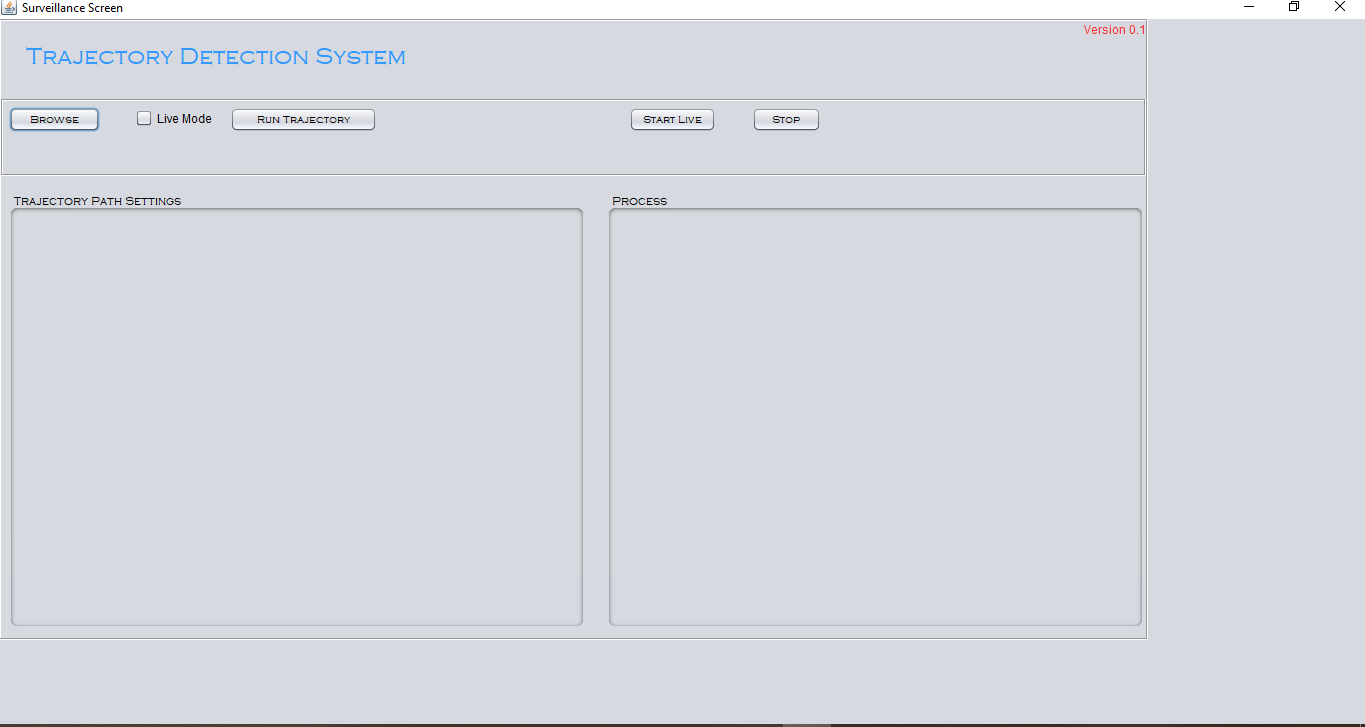
**EVENT 6**

Server reports malicious activity.

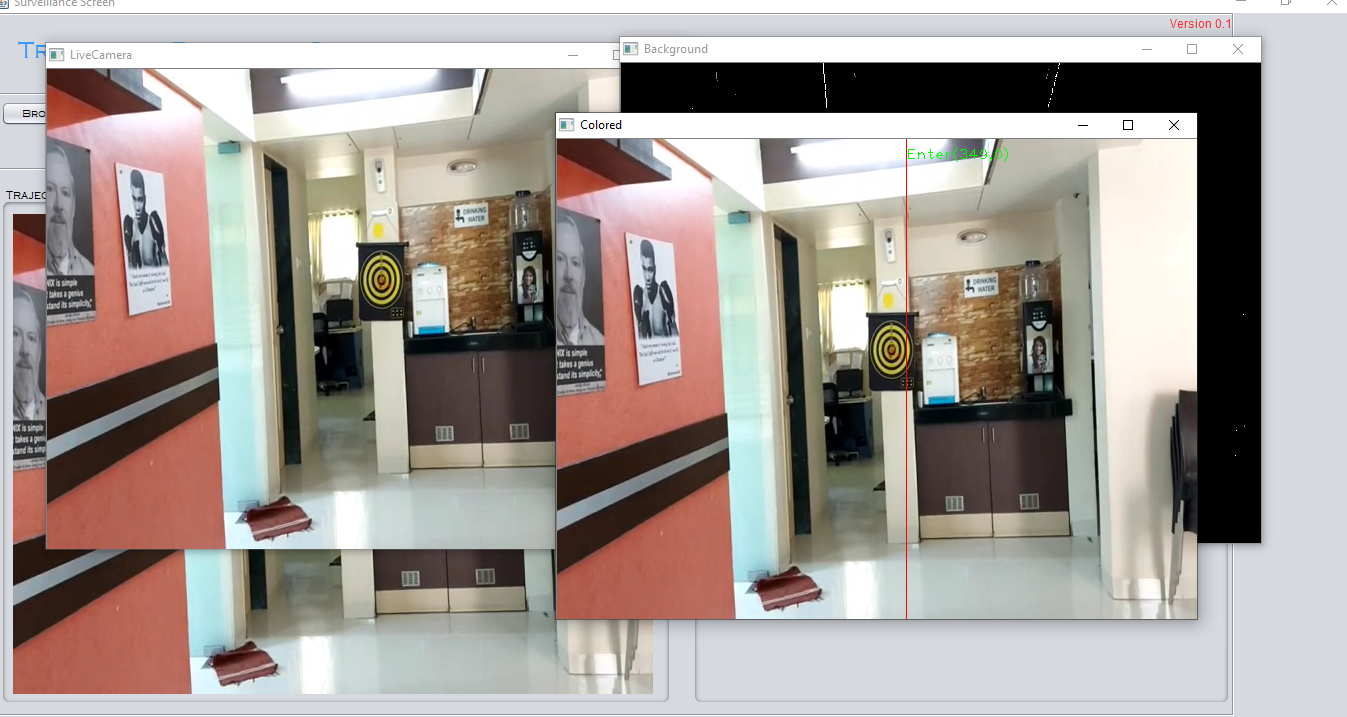
Let *f(Un)* be a set of N Users.

Thus, *f*(Un) 🡪{F1,F2,F3…..Fn} € F

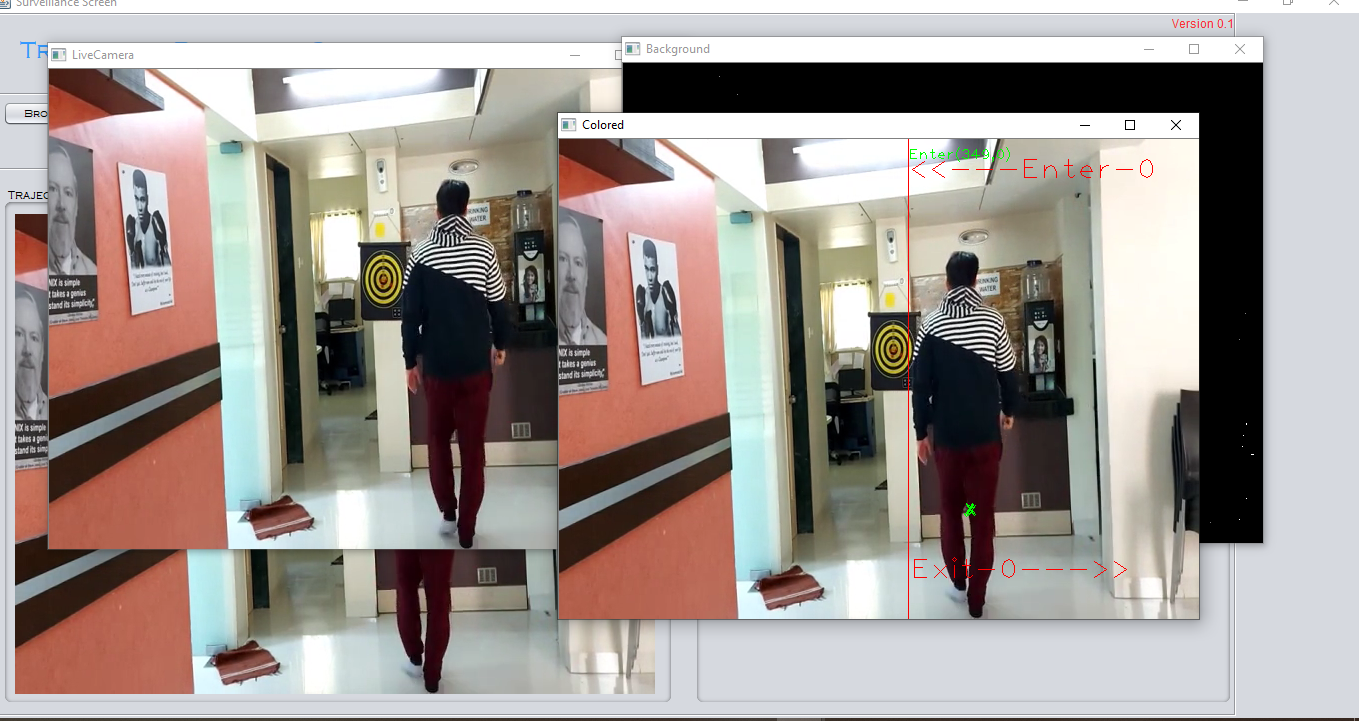
1. **RESULT SCREENSHOTS**



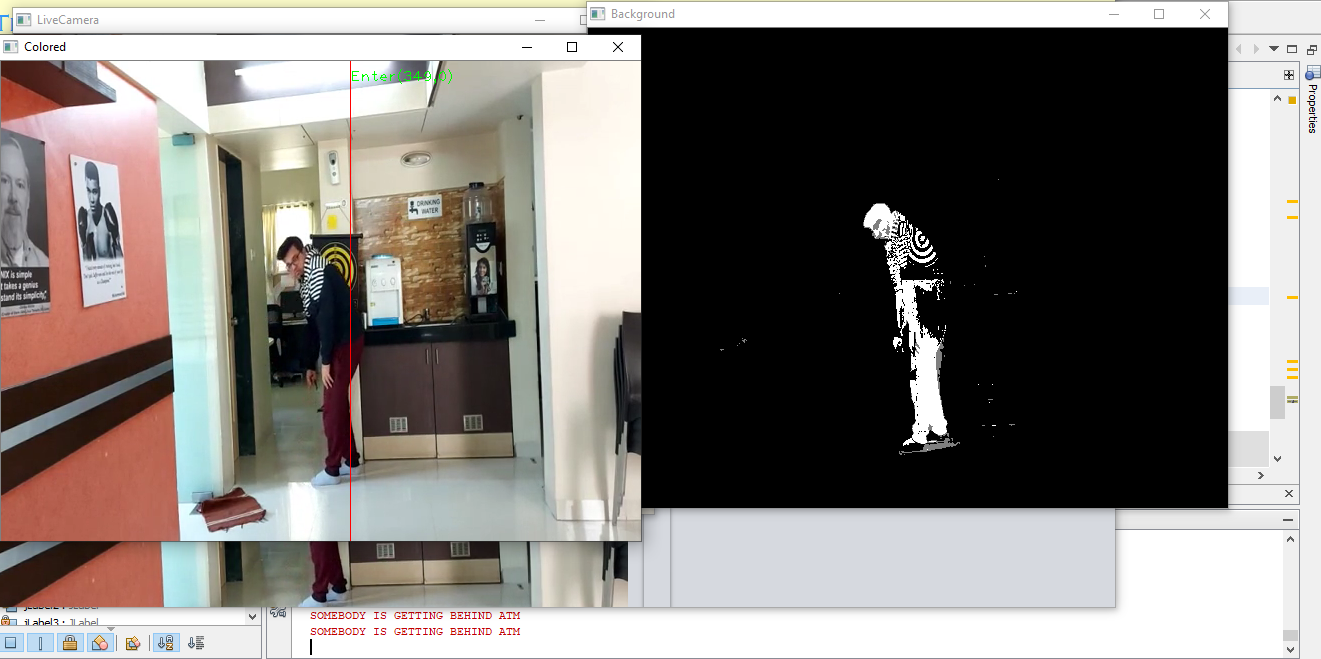
**Figure 3:** GUI



**Figure 4: CCTV Surveillance**



**Figure 4: CCTV Surveillance**



**Figure 5: Anomaly Detection**

1. CONCLUSION

The given solution can prevent the malicious activity with high precision happening in the ATM system and send alert to the administrator in real time. Here we have used the Motional Region Detection Structure for trajectory path recognition and Background Image Update. The system It offers a high security over the criminal acts as security is a most important feature. No doubt the above techniques are enormously useful. We can conclude that our models give accurate prediction on the malicious activity in the ATM.

References

1. Sahar Torkamani, Alexander Dicks and Volker Lohweg, Senior Member, IEEE,"Anomaly Detection on ATMs viaTime Series Motif Discover",Conference: 21th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2016)At: Berlin.
2. Arpitha K, Honnaraju B ,"Vision Based Anomaly Detection System for ATM",International Research Journal of Engineering and Technology (IRJET),2018.
3. Nithya Shree R, Rajeshwari Sah and Shreyank N Gowda, “Surveillance video based robust detection and notification of real time suspicious activities in indoor scenarios,” The sixth international conference on computer science, engineering and information technology, 2016.
4. .Prarthana Sanas1 , Pradnya Kasbe2, Ankita Shelke3, and Srushti Salunkhe4,"Anomaly Detection at ATM Center using Machine Learning Algorithm",International Journal of Advanced Research in Science, Communication and Technology (IJARSCT),2021.
5. Vikas Tripathi, Durgaprasad Gangodkar, Vivek Latta, Ankush Mittal, "Robust Abnormal Event Recognition via Motion and Shape Analysis at ATM Installations", Journal of Electrical and Computer Engineering, vol. 2015, Article ID 502737, 10 pages, 2015. https://doi.org/10.1155/2015/502737
6. Roongtawan Laimek; Natsuda Kaothanthong,"ATM Fraud Detection using Behavior Model", 2018 5th Asian Conference on Defense Technology (ACDT).
7. Aditya Parab; Abhishek Nikam; Prajwal Mogaveera; Ashwini Save,"A New Approach to Detect Anomalous Behaviour in ATMs", 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).
8. Kande A, P B Reddy "To detect abnormal event at ATM system by using image processing based on IOT technologies" International Journal of Engineering & Technology, 7 (3) (2018), pp. 1000-1004.
9. V. Tripathi, A. Mittal, D. Gangodkar, V. Kanth, “Real time security framework for detecting abnormal events at ATM installations”, Springer-Verlag Berlin Heidelberg, 2016, pp 1-11, pp. 1-8.
10. K. Kajendran and A. Pravin "ENHANCEMENT OF SECURITY RELATED TO ATM INSTALLATIONS TO DETECT MISBEHAVIOR ACTIVITY OF UNKNOWN PERSON USING VIDEO ANALYTICS ",ARPN Journal of Engineering and Applied Sciences,VOL. 12, NO. 21 , NOVEMBER 2017.
11. Abdul Monem S. Rahma, Ph.D,Abeer Salim Jamil, M .Sc,"Build Architecture Design for an Intelligent Security System b ased on Behavior Tracking",International Journal of Computer Applications (0975 – 8887) Volume 99 – No.1 1 , August 2014.
12. A.F. Bobick ; J.W. Davis ,"The recognition of human movement using temporal templates", IEEE Transactions on Pattern Analysis and Machine Intelligence ( Volume: 23 , Issue: 3 , Mar 2001 10.
13. Mirela Kundid ; Irena Galić ; Daniel Vasić ,"Human action identification and search in video files", 2015 57th International Symposium ELMAR (ELMAR).
14. Navneet Dalal and Bill Trigg"Histograms of Oriented Gradients for Human Detection".
15. Nievas E.B., Suarez O.D., Garcı ́a G.B., Sukthankar R. 2011. Violence detection in video using computer vision techniques, pp. 332 – 339. Computer Analysis of Images and Patterns. Springer, Berlin Heidelberg. Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.Spector, A. Z. 1989.
16. Versavel J. Road, “Safety through video detection”, Journal, Proceedings of 1999 IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems, 1999, pp.753-757.
17. Yaser Sheikh, Mubarak Shah,“Bayesian Modeling of Dynamic Scenes for Object Detection”, Journal, Proceedings of the IEEE,2005,pp.1778-1792.