Automated Surveillance System Using Clustered Matching

Rucha Pathari[1], Prof. Sachin Bojewar[2]

[1]PG Scholar, Department of Computer Engineering, Alamuri Ratnamala Institute of Engineering and Technology, Mumbai University, India
[2]Asst. Prof., Department of Computer Engineering, Vidyalankar Institute of Technology, Mumbai University, India

Abstract: The Spy" generally developed to monitor and record suspicious movement in a company during the closing hours of the company. Organizations today face new and more insidious threats than they ever have in the past. To protect personnel and infrastructure alike requires a level of vigilance not previously anticipated. A new technology called Intelligent Video Surveillance employs state of the art computer vision technology to automate the process of watching web cam - making video a proactive defense sensor. One approach is to detect and recognize the actions of individuals within a crowded scene.
We get to know about bank robberies in day to day life and the thieves escape unidentified. When the banks are closed after office hours, it is difficult manning the whole area physically. Therefore we decided to implement motion detection algorithm which will act as security tool. The video can be captured using web cam and once the motion of the object crosses the threshold value, the video is stored. For every motion there is a new video.

1. INTRODUCTION

Features include advanced motion detection, mask out areas which could cause false alarms, stores images in a compressed format, produce reports on captured images, custom motion effects, overlay text onto captured images, write images to an movie file, play sounds when motion is detected.

- **Objectives:**
  - Camera Configuration to start motion detection.
  - Start monitoring [Start video capturing, Capture device- web camera] .
  - Scanning area to detect suspicious movement.
  - Recording suspicious video Module.
  - Playing Alarm after detecting suspicious movement.
  - E-mail the user video recording.

2. PROBLEM DEFINITION

Video Surveillance software as the name itself suggests has to be developed to provide security to the user of the software, so the cost of software adds. The system also requires a webcam and various circuitries so it also adds to the cost.
There is also a case that software gets corrupted or the hardware wares out so there is requirement for the user to check the system at regular intervals.

EXISTING SYSTEM:

In early days, the **CCTV** cameras were used as means of Surveillance system. **CCTV** stands for **Closed-Circuit Television**.

CCTV recording systems are still often used at modern launch sites to record the flight of the rockets, in order to find the possible causes of malfunctions, while larger rockets are often fitted with CCTV allowing pictures of stage separation to be transmitted back to earth by radio link.

Closed-circuit television (**CCTV**) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point wireless links. CCTV is often used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores.

In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room; when, for example, the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing Digital Video Recorders (DVR's), provides recording for possibly many years, with a variety of quality and performance options and extra features (such as motion-detection and email alerts).

Surveillance of the public using CCTV is particularly common in the UK, where there are reportedly more cameras per person than in any other country in the world. There and elsewhere, its increasing use has triggered a debate about security versus privacy.

DISADVANTAGES:

- Wireless CCTV can be hacked into by another receiver.
- Guard must be licensed if the area being monitored is used by the public.
- Must be wary if camera is moveable that you are not looking into private residences.

PROPOSED SYSTEM:

Organizations today face new and more insidious threats than they ever have in the past. To protect personnel and infrastructure alike requires a level of vigilance not previously anticipated. A new technology called Intelligent Video Suspicious employs state of the art computer vision technology to automate the process of watching WEB CAM - making video a proactive defense sensor. One approach is to detect and recognize the actions of individuals within closing hours of the

company. This functionality has applications in public safety and airport security.

- **Increased safety:** If implemented properly, a video surveillance network can greatly improve the security of employers and employees alike. In order to be effective however, the network needs to be properly maintained and monitored on a regular basis so that security threats can be accurately assessed.
- **Theft deterrent:** The proper use of video surveillance has saved companies hundreds of dollars in stolen products. **Prompts good behavior:** Just as the presence of video surveillance cameras deters theft, it also promotes good behavior. Individuals are less likely to behave inappropriately if they know they are being monitored.
- **Provides evidence of a crime:** If a crime has occurred, it is easier to prove what actually took place using recordings of the video surveillance footage. While this method is certainly not fool proof, in most cases, it can prove invaluable.
- **Captures all desktop activities:** This system captures all desktop activities at client side PC and generates video clips.

3. ALGORITHM USED:

Cluster Matching Algorithm:
A new method for estimating displacements in computer imagery through cluster matching is presented. Without reliance on any object model, the algorithm clusters two successive frames of an image sequence based on position and intensity. After clustering, displacement estimates are obtained by matching the cluster centers between the two frames using cluster features such as position, intensity, shape and average gray-scale difference.

The performance of the algorithm was compared to that of a gradient method and a block matching method. The cluster matching approach showed the best performance over a broad range of motion, illumination change and object deformation.

In this study, clustering is used as a means to group pixels with similar feature‘s in each image frame; the displacements are estimated by matching clusters between two frames in the image sequence. The method should also be applicable to motion estimation for images containing deformable objects with varying brightness.

First, pixels in each image frame are clustered the two successive frames are treated independently. Each of the resulting clusters tends to be spatially connected because of the position constraint and contains pixels of similar gray-scale values because of the intensity constraint. Second, clusters are matched between the two consecutive frames. In addition to the position and the intensity, the shape of each cluster and the average gray-scale difference between two clusters are used as matching criteria.

The Displacement between the two matching cluster centers is assigned to every pixel in the cluster. This results in a dense set of displacement estimates.

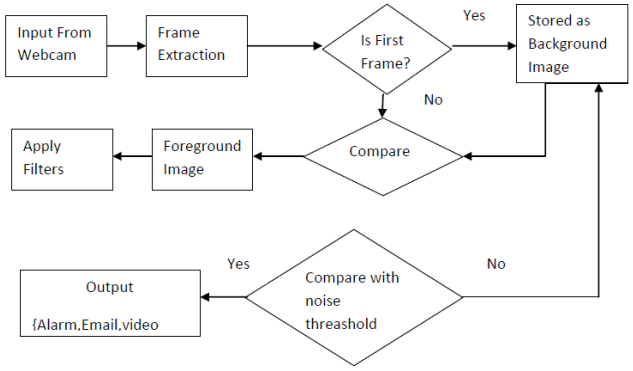

Fig.1 System Flow Diagram

Algorithm:
1. START.
2. One of the most common approaches is to compare the current frame with the previous
Assume that we have an original 24 bpp RGB image called current frame (image), a grayscale copy of it (current Frame) and previous video frame also gray scaled (background Frame).
I. For the purpose we can declare new difference and threshold filters.
II. We initialized value to background Frame and apply the filters.
III. Store the filter value differences filter and threshold filter temporarily.
3. On this step we'll get an image with white pixels on the place where the current frame is different from the previous frame on the specified threshold value.
4. It’s already possible to count the pixels, and if the amount of it will be greater than a predefined alarm level we can signal about a motion event.
5. At the beginning, we get the first frame of the video sequence as the background frame. And then we'll always compare the current frame with the background one. But it will give us the result with some drawback.
6. Our approach is to "move" the background frame to the current frame on the specified amount.
8. We move the background frame slightly in the direction of the current frame - we are changing colors of pixels in the background frame by one level per frame.
9. We create new filter as move towards and assign its current value to the background frame value. And this value assign to temporarily.
10. Assign processing filter value to the filter sequence and difference and threshold value with background value.
11. STOP.

4. CONCLUSION

In this paper, we presented methods for detecting motion in a video surveillance system using webcam. We implemented the system which automatically detected suspicious activity. The proposed object tracking method successfully tracks the motion in consecutive frames. The system calculates Histogram for each frame and compare with threshold value, gives alarm, E-mail to user and do video recording from the time motion gets detected.

5. REFERENCES

[1] IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 16, and NO. 11; on title **"Motion Estimation via Cluster Matching",** author is **'**Dane P. Kottke and Ying Sun**'.**
[2] http://www.cs.cmu.edu/~VSAM
[3] http://www.research.ibm.com/journal/rd/312/ibmrd3102P.pdf
[4]http://ieeexplore.ieee.org/Xplore/login.jsp?url=/stamp/stamp.jsp?arnumber=219740&isnumber=5754
[5] http://www.movsd.com/bm.htm
[6] http://www.darnok.org/programming/motion-detection/