Smart Camera: The Design and Implementation of an Anonymous Security System to Intercept Assault

LMU|LA Frank R. Seaver College of Science and Engineering

Keely Jones, Amy Weber, Hossein Asghari

Loyola Marymount University, Department of Electrical Engineering and Computer Science

LMU|LA Frank R. Seaver College of Science and Engineering

Abstract

This project employs a Microsoft® Kinect camera to become a smart security system which can intercept physical assaults. This system stops such crimes with an alert sent to the appropriate response team, based on decisions regarding whether the observed situation is "normal" or "suspicious." As machine learning is a state-of-the-art technology for identifying human behavior, this system will decide whether to alert based on a machine-learning program in MATLAB.[1,2] Also, the security of the system will allay concerns about rights to privacy and anonymity within public spaces by guarding the imaging output of the Kinect. The system has the potential be deployed in train stations and even bathrooms to intercept and diminish the threats of mugging and sexual assault, among other applications.

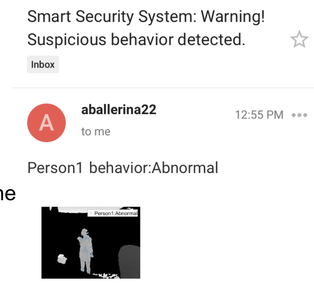

Figure 1: Email alert for system

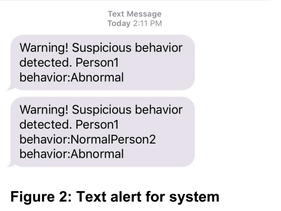

Figure 2: Text alert for system

Objectives

The following objectives define the direction and method of implementation of the Smart Camera system:

- The system will monitor a space in real time while protecting the privacy of those being monitored.
- The system will assess whether the situation it sees is 'normal' or whether the circumstance is an anomaly requiring human intervention.
- Upon detecting an abnormal event, the system will alert the appropriate personnel within 30 seconds of the event.

These objectives provide measures by which to define the accuracy of the Smart Camera:

- System can classify 5 behaviors as normal
- System can make a decision within 30 seconds
- Anomaly detection rate at or above 70%
- False alarm detection rate at or below 20%

Approach

The Microsoft Kinect uses a depth sensor to detect the skeletons of people in a space, thus avoiding images that might invade the individual's right to privacy. The Kinect passes the information about how people are moving to MATLAB, which uses a classifying machine learning program to interpret people's behavior. MATLAB then decides whether the observed behavior is normal or suspicious, then alerts the appropriate personnel. The five behaviors which the system will recognize are walking, standing, waving, walking in groups, and standing in groups. These behaviors will then be classified into 'normal' and 'abnormal' categories by a Hidden Markov Model.

Methodology

The process of predicting behaviors begins with defining normal behaviors to be detected. Each behavior is detected individually, then all behaviors are compiled into an understanding whether the situation is normal or abnormal, as illustrated in Figure 3.

Steps to build detection of a single behavior:

- Choose binary, mutually exclusive predictors (behavior, not behavior)
- Collect data, save data to .csv file
- Train data in Classification Learner and export best-performing algorithm
- Run algorithm in real-time
- Test and modify algorithm, implement feature selection (optional)

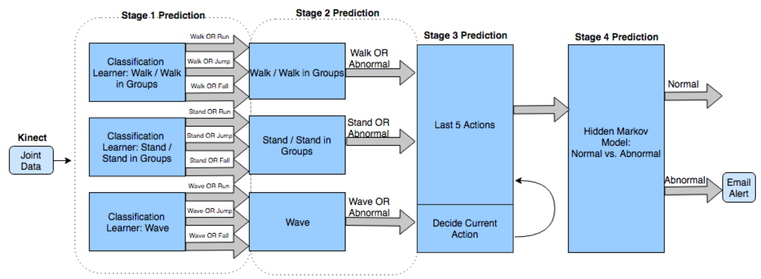

Figure 3: Outline of process used to classify behaviors in real-time

Detected Behaviors

Figure 4: Stand (Normal) vs. Abnormal algorithm detecting 'Stand'

Figure 5: Wave (Normal) vs. Abnormal algorithm detecting 'Wave' and 'Stand'

Figure 6: Walk (Normal) vs. Abnormal algorithm detecting 'Walk'

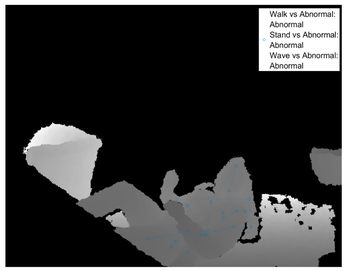

Figure 7: Falling appears as 'Abnormal' for all algorithms

Accuracy Testing

To determine the accuracy for the detection of behaviors, the program was run for fifteen trials of thirty seconds, with a person acting out each movement in front of the camera. After thirty seconds of each behavior, the labels were sorted into 'normal' or 'abnormal' as seen in Figure 8.

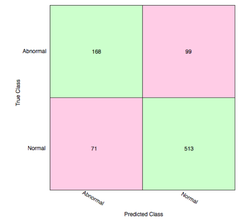

Figure 8: Results of accuracy testing for 'normal' vs. 'abnormal'

Results and Discussion

After collecting the data in Figure 8, the false alarm detection rates and the anomaly detection rates were determined.[3]

$$\frac{\#(normal\ detected\ as\ abnormal)}{\#(predictions)} \quad (1)$$

From Eq. 1, the false alarm rate was 12.2%, and the expected value was at or below 20%, meaning the system does better than expected at predicting 'normal.'

$$\frac{\#(abnormal\ detected\ as\ abnormal)}{\#(predictions)} \quad (2)$$

From Eq. 2, the anomaly detection rate was 62.9% out of an expected 70%. This means that the system does not do as well as expected in detecting 'abnormal.' However, this may be because within abnormal movements such as falling to the ground, there are likely multiple "normal" frames, such as when the person is standing up again.

The system sends an alert at the first identification of 'abnormal,' and then keeps track of the next 30 frames, which is approximately 30 seconds. If 10 of those are predicted as 'abnormal' then the system sends a follow-up alert. The alerts can be sent in both an email and text format, which can be seen in Figures 1 and 2, respectively.

Future Applications

This prototype is designed to be scalable, where more normal movements can be easily added to make the detection more comprehensive.

The system has the potential to work better than traditional security cameras, as it can alert personnel to suspicious activity rather than relying on a human to monitor the images constantly, and protects personal information so that it could be used where standard security cameras would be too intrusive.

References

1. Jie Yang, Yangsheng Xu and C. S. Chen, "Human action learning via hidden Markov model," in *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 27, no. 1, pp. 34-44, Jan 1997.
2. P. Turaga, R. Chellappa, V. S. Subrahmanian and O. Udrea, "Machine Recognition of Human Activities: A Survey," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 11, pp. 1473-1488, Nov. 2008.
3. X. Zhu and Z. Liu, "Behavior Clustering for Anomaly Detection," *Frontiers of Computer Science in China*, pp. 141–27, 2011.

Acknowledgements

We would like to thank Dr. Lei Huang, Dr. Gustavo Vejarano, Dr. Hossein Asghari, and all the EECS faculty at LMU for their support with this project.

Contact: kly_jns@yahoo.com, aballerina22gmail.com