IDENTIFICATION OF ABNORMALITIES IN LIVE FEEDS IN THE BANKING INDUSTRY - ABNORMAL HUMAN BEHAVIOR DETECTION

Project ID: 18-116

Software Requirement Specification

J.P.K. Savindi

IT15045836

Bachelor of Science Special (Hons) Degree in Information Technology

Specializing in Software Engineering

Department of Software Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

May 2018

DECLARATION

I declare that this is my own work and this Software Requirement Specification titled "Identification of Abnormalities in Live Feeds in the Banking Industry - Abnormal Human Behavior Detection", submitted to Sri Lanka Institute of Information Technology is a record of an original work done by me, under the guidance of my supervisor Ms. Shashika Lokuliyana. This document does not incorporate without acknowledgment any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

Name	Student ID	Signature
J.P.K. Savindi	IT15045836	

The above candidate is carrying out research for the undergraduate Dissertation under my supervision.

…….. ……..

Signature of the supervisor: Date

(Ms. Shashika Lokuliyana)

Table of Contents

Table of Figures

List of Tables

1 Overall Descriptions

The purpose of this chapter is to give the reader an overview of the comparison of knowledge in identification of abnormalities in human behavior by using the image processing component of the overall system. In our research we are focusing on the detection of abnormalities within an ATM environment. ATMs can be susceptible to criminal activity if not properly protected. Cameras installed in ATMs can deter hold ups and violent confrontations, deters ATM skimming and also, assists in criminal investigations of ATM transactions. There are at least two security cameras on ATM machines – one inside the ATM machine, hidden type of security camera; another is usually on top, the visible type of security CCTV camera. Most of the cameras inside the ATM are the Pinhole type of camera, similar to what you see on a doorbell camera. By using the feed recorded in these cameras, you can easily detect the facial features and behavioral patterns of any individual who is present inside the space of an ATM machine – that may look suspicious or abnormal.

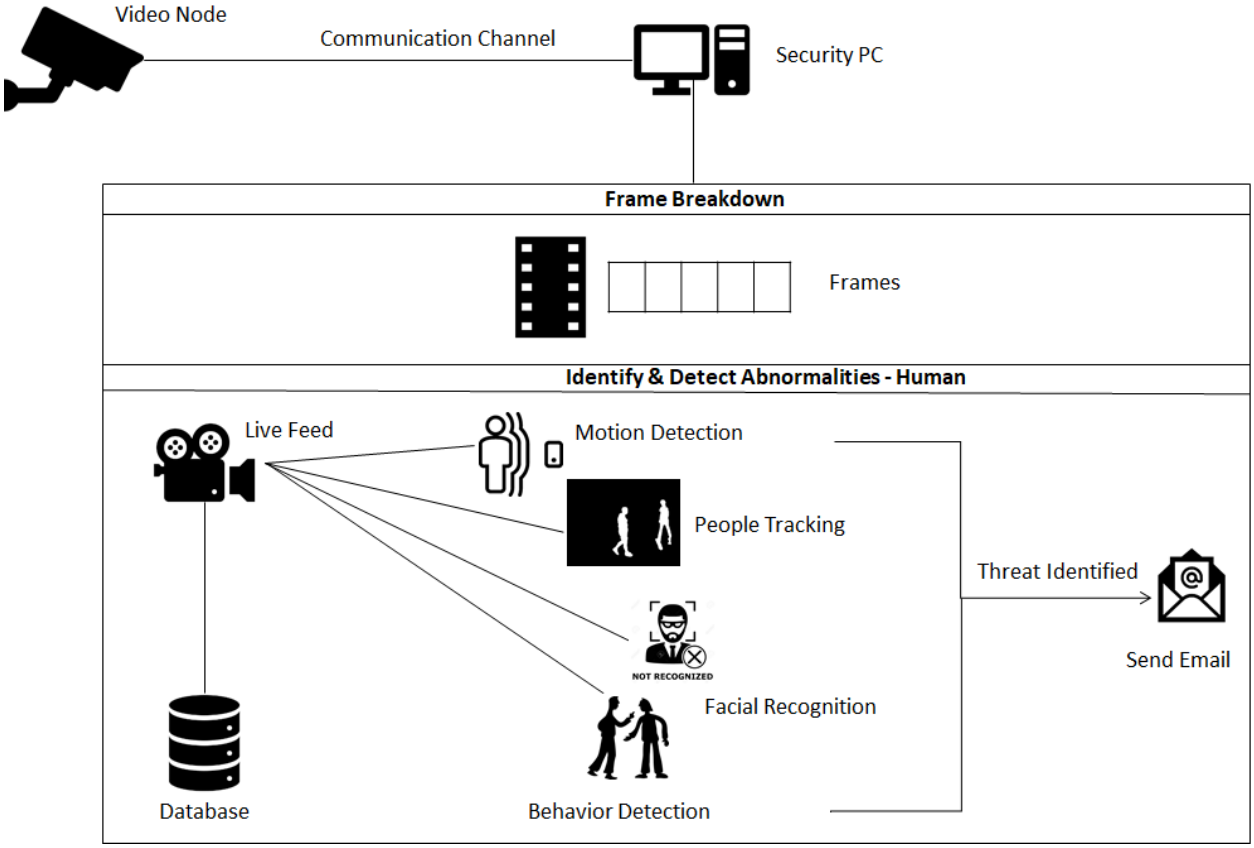

Figure 1 High-Level System Diagram (Abnormal Human Behavior Identification)

1.1 Product Perspective

With the pace at which crime and fraud rates are going up, it is important for banks to be more proactive in their security measures. After conducting numerous interviews and discussions with a selected group of bank personnel, what our team discovered was that, over the years, there was no proper technology to identifying unusual human behavior in the bank environment — much less a real time system to alert the security personnel whenever an unusual activity which threatens the security of the bank is detected. With lessons learnt, the banking industry, however, has been developing and conducting experiments with their current security systems, and as a result, has implemented high end surveillance systems to monitor and detect anomalies that pose as a threat to the bank. In the recent years, there has been an increase in the number of banks worldwide who are making use of the technologies such as, facial recognition, biometrics and motion detection to ensure their security but, as of now, there is no proper system to identifying abnormal behavior of individuals that will breach the security of the bank.

Though there is a lack of abnormal human behavior detection tools used in the banking industry, there is an abundance of applications that are made for this particular purpose available online. Smart Surveillance Annotation Tool (SSAT), as its name indicates, “is an annotation tool, free and interactive, for the computer vision community” [1]. This tool uses the computer vision technique called image annotation, where the system can be used to assign metadata in the form of captioning or keywords to an image. This can be used to organize and locate images of interest from a database. Using this tool, you can upload videos straight from the file system and then apply annotations by establishing attributes in which the user desires to base his annotation on.

1.1.1 System Interfaces

1.1.2 User interfaces

1.1.3 Hardware interfaces

Following are the basic hardware that are needed for the product,

- PC with a Windows OS installed
- Inbuilt web camera of a PC to simulate the pinhole camera in the ATM
- A Bluetooth camera / or an outside camera connected to the PC to simulate the CCTV camera set up on the ceiling of the ATM kiosk

The user needs to have a PC with Windows OS is installed in order to install and work with the abnormal human behavior identification process. In order to use this application, it requires minimum 1 GHz RAM.

1.1.4 Software Interfaces

Our research centers on building a system that obtains data from the live feed and performing the human behavior anomaly detection algorithms on the said data. And once a threat is detected, it will send an automatic email that contains a warning message to the security personnel. This system is designed and implemented using,

- Microsoft Windows environment
- C# language with OpenCV library
- The Smart Surveillance Interest Group Library (SSIGLib) as a support library [2]
- Microsoft Visual Studio 2015
- The system is using the windows filesystem as its database component
- Draw.io is a completely free online diagram editor built around Google Drive (TM), which allows you to create the flow diagrams, class diagrams and activity diagrams and process flow diagrams, etc.
- Microsoft PowerPoint is used to design presentation slides and diagrams (i.e. High-level diagram). Also to be used in order to create presentation slides that aide the team when presenting the status of the project, progress, etc., to those interested (i.e. Project Supervisor and Lecturer-In-Charge).

1.1.5 Communication Interfaces

1.1.6 Memory Constraints

In order for the abnormal human behavior detection process to run smoothly the system requires having a minimum of 4 GB RAM and also a minimum storage memory (non-volatile) of 10 GB.

One great advantage of this system is, that it can be run on a machine composed of standard PC requirements.

1.1.7 Operations

1.1.8 Site adaptation requirements

1.2 Product Functions

In order to detect abnormalities in the behavior of the users' of the ATM, fundamental principles of image processing have been followed. The approach to identifying and tracking abnormal features/behavior in a specific individual will be done as a 4 step process that is run parallel to each other, namely motion detection, people tracking, facial recognition and behavioral detection.

Motion Detection - In this system, in terms of abnormal human behavior identification, motion detection function will be used to identify any kind of suspicious movement inside the ATM. As an example, if an individual is attacking another individual inside the ATM, motion detection function will identify their movements as a threat and will notify the security personnel via a notification email.

People Tracking - Usually, in a secure ATM environment more than one individual should not be present, hence providing the people tracking function with an important requirement that is to check if there is more than one individual using the ATM at once. As an example, if there are more than two well-built individuals (adults) present inside the ATM, which could pose as a threat to the security of the premises, and so it will be detected by the people tracking function of the system.

Facial Recognition - As a security measure, many banks worldwide do not allow their customers to wear and form of headgear or any accessory (i.e. sunglasses) covering their face, inside an ATM. The reason behind this, is to ensure that no one is misusing the ATM or performing any fraudulent activity inside the ATM – all the while hiding their faces from the security cameras. This particular rule acts as the requirement for our system's facial recognition function. The

video captured from the pinhole camera inside the ATM will be processed using the facial recognition algorithm. Once the algorithm is running, if the system does not detect any facial features of the individual using the ATM, it will be classified as a threat and the security personnel will be notified.

Behavior Detection - If any individual/s using the ATM showcases any kind of suspicious behavior, the behavior detection algorithm will identify the said suspicious behavior as a threat to the security of the ATM. The behavior detection model of the system will be able to detect if a person is trying to vandalize the ATM using physical force, which of course will be classified as abnormal behavior.

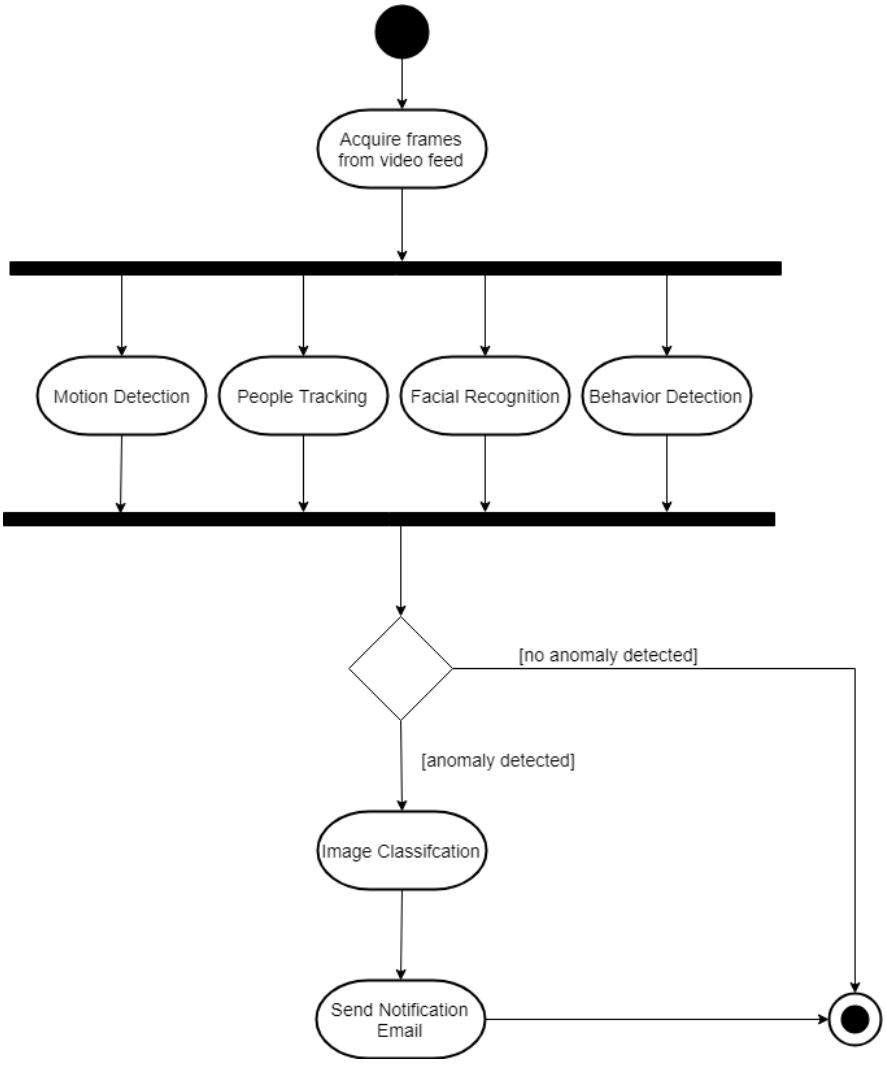

Figure 2 Activity Diagram (Abnormal Human Behavior Identification)

1.3 User Characteristics

The service, abnormal human behavior identification is mainly applied to surveillance systems operating in a banking environment. Since this is an automated process, the users associated with this system are limited. However, once an anomaly in the ATM environment is detected, the security personnel of the bank will be getting a notification email prompting him to take action to prevent/control the threat.

User Type	Description
Security Personnel	The person who directly involved and responsible for the bank security. They should have the ability to operate a Windows PC and should have sound knowledge and practice of handling emails.
Researchers	An interested party who is experimenting or conducting research related to enhancing the security in a video surveillance system in an ATM.

Table 1 Descriptions of User Types

1.4 Constraints

Since the system is based on a surveillance network in a banking environment, it is limiting the developers' work, in terms of obtaining actual footage from an ATM camera for testing purposes, because the said video footage is considered confidential and would be against the bank's regulatory policies involving the identity of its customers.

1.5 Assumptions and Dependencies

We have found few assumptions and dependencies, that the security office should consider after we implemented the application ATM.

- Notifications need to be identified by the security personnel in order to ensure the safety of the ATM.
- The security personal must react immediately in order to avoid further damage.

1.6 Apportioning of requirements

All the requirements, namely motion detection, people tracking, facial detection and behavior detection falls under the functional requirements category of the system, and they are to be implemented in the system in its first release.

2 Specific requirements

2.1 External interfaces

2.2 Classes/Objects

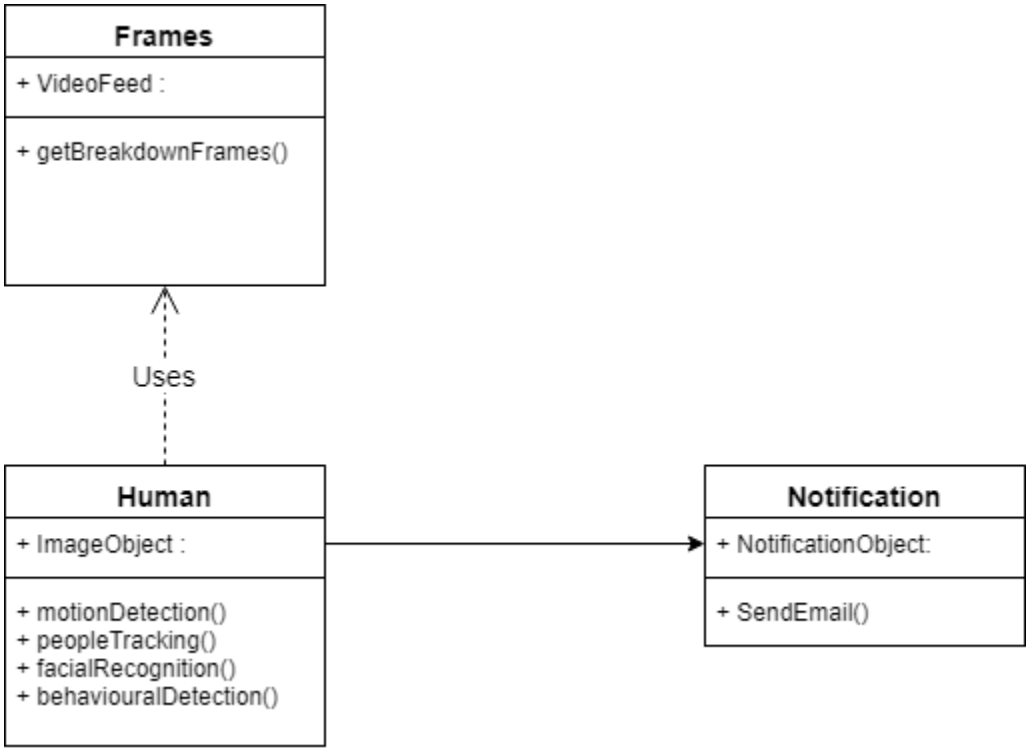

Figure 3 Class Diagram (Abnormal Human Behavior Identification)

2.3 Performance requirements

This product will be built to function itself without any interaction with other external systems. For efficient performance of the system, the system should use machines running Windows with a minimum speed of 1.80 GHz and 4GB RAM. The overall performance of the application is determined by the CPU and the RAM working together, as well as GPU Processing power.

2.4 Design constraints

2.5 Software system attributes

2.5.1 Reliability

In a system such as this, that deals with ensuring the security of a banking environment, the reliability is a crucial attribute to be looked at, which is why the proposed application is being developed to in a way it will perform the functions for which it was designed or intended for a specified time. All the latest technology is used to provide the precise service and, in less time.

2.5.2 Availability

Since all ATM transactions takes place 24 hours a day, every day, the system needs to be available during that time period as well.

2.5.3 Security

It is essential that the ATM network be totally secure against any conceivable type of attack. Security is a very important characteristic for this type of application because all the details that are provided to the system must be valid and accurate.

2.5.4 Maintainability

The maintenance ability is an important aspect since it is intended to be improved further in the future. Standard coding practices will be followed during the implementation of the system. The system will be implemented to minimize bugs and errors as much as possible.

References

1] “SSAT - Smart Surveillance Annotation Tool - SSIG - Smart Surveillance Interest Group.” [Online]. Available: http://www.ssig.dcc.ufmg.br/ssat-annotation-tool/. [Accessed: 03-May-2018].

2] “Smart Surveillance Interest Group Library (SSIGLib)” [Online]. Available: https://github.com/ssig/ssiglib.wiki.git [Accessed: 08-May-2018].