# Chapter 1 – Introduction

## 1.1 General

This report discusses the result of the work done in development of "Digital Image Processing for Automatic Surveillance and PiCrypt" on Python Platform. The project aims at the development of application framework for providing a common platform that ensures security services and benefits to a user in the field of Home Security and Information Security by implementing innovative techniques and methodologies.

As Security has always been one of the biggest concerns for an individual, there is an immense requirement of some security tools that can provide assurance to a owner in terms of guarding one's belongings in his absence. The primary objective of this project is to implement the Image Processing Technique by using the available resources like Camera (in-built camera of a computer system or an external one) and a mouse or any motion generation device to construct a single platform that provides the user with some Security Tools-

1) An Automatic Surveillance System, based on the techniques of Object Tracking, Body and Face detection along with recognition and Motion Detection where the visuals of the current surroundings are continuously monitored using the camera module and generates an Alert when some intrusion is encountered on the basis of some set parameters. The alert mechanism includes sending E-mail to the owner along with the snapshots of the suspect whose presence has been detected. The owner also receives the message on the registered mobile number reporting the presence of some unregistered party. Finally the owner also receives a graph plot which indicates the overall motion being detected within the given framework. The overall motive of this module is to make the owner aware regarding the unrecognized intrusions being conducted whenever the system is on so that the owner can

take some desirable actions on the basis of the alert reports received in the form of E-mails, SMS and Graphs.

2) Information Security tool that implements image steganography to provide Data Security by hiding sensitive information within an image or a video which can be saved on the user's system and can be shared among the concerned person. This hidden information can also be extracted from the image with the help of a dynamic key generated within this framework using the motion tracking module of the application. In this project, this feature is addressed as PiCrypt.

The idea is that given a system specification, by following the methodology and with the help of the tools developed to support it, the user will be able to synthesize a system that meets his security constraints which includes the information security provided by Steganography and Premisis security as Automatic Surveillance. A tool was required to integrate all the design tools discussed above along with the capability to perform the same functions manually. Analysis and Visualization of the target platform was also required to know its performance.

This project deals with the development of such a tool which will assist in the implementation of the above methodology and is hereby referred as "EagleEye".

## 1.2 The History of Digital Image Processing

Many of the techniques of digital image processing, or digital picture processing as it often was called, were developed in the 1960s at the Jet Propulsion Laboratory, Massachusetts Institute of Technology, Bell Laboratories, University of Maryland, and a few other research facilities, with application to satellite imagery, wire-photo standards conversion, medical imaging, videophone, character recognition, and photograph enhancement. The cost of processing was fairly high, however, with the computing equipment of that era. That

changed in the 1970s, when digital image processing proliferated as cheaper computers and dedicated hardware became available. Images then could be processed in real time, for some dedicated problems such as television standards conversion. As general-purpose computers became faster, they started to take over the role of dedicated hardware for all but the most specialized and computer-intensive operations. With the fast computers and signal processors available in the 2000s, digital image processing has become the most common form of image processing and generally, is used because it is not only the most versatile method, but also the cheapest.

Digital image processing technology has a lot of applications in the field of security. Two such fields are Surveillance system and Steganography.

History of Video Surveillance

Video surveillance, more commonly called CCTV (closed-circuit television), is an industry that is more than 30 years old and one that has had its share of technology changes. As in any other industry, end users' ever-increasing demands on the products and solutions are driving the changes, and evolving technologies are helping to support them. In the video surveillance market, the demands include:

1. Better image quality

2. Simplified installation and maintenance

3. More secure and reliable technology

4. Longer retention of recorded video

5. Reduction in costs

6. Size and scalability

7. Remote monitoring capabilities

8. Integration with other systems

9. More built-in system intelligence

To meet these requirements, video surveillance has experienced a number of technology shifts. The latest is the shift from analog CCTV surveillance to fully digital, network-based video surveillance systems.Video surveillance systems started out as 100-percent analog systems and are gradually becoming digital. Today's systems, using network cameras and PC (personal computer) servers for video recording in a fully digital system, have come a long way from the early analog tube cameras, which were connected to a VCR (videocassette recorder).

History of  Steganography for the evoltion of PiCrypt

In between the fully analog and fully digital systems, there are several solutions that are partly digital, that is, systems that incorporate both digital and analog devices.

Steganographic techniques have been used for ages and they date back to ancient Greece. The aim of steganographic communication back then and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation the existence of hidden communication cannot be detected by third parties. What distinguishes historical steganographic methods from the modern ones is, in fact, only the form of the cover (carrier) for secret data. Historical methods relied on physical steganography – the employed media were: human skin, game, etc. Further advances in hiding communication based on the use of more complex covers, e.g. with the aid of ordinary objects, whose orientation was assigned meaning. This is how semagrams were introduced. The popularization of the written word and the increasing literacy among people had brought about methods which utilized text as carrier. The World Wars had accelerated the development of steganography by introducing a new carrier – the electromagnetic waves. Presently, the most popular carriers include digital images, audio and video files and communication protocols. The latter may apply to network protocols as

well as any other communication protocol (e.g. cryptographic). The way that people communicate evolved over ages and so did steganographic methods. At the same time, the general principles remained unchanged.

## 1.3 Overview of the Project

EagleEye is a desktop application that provides a user with the feature of Digital Image Processing. It provides a Graphical User Interface (GUI) to interact with the user of the application, where the user can select one of the features among - Automatic Surveillance and PiCrypt. The features and facilities provided under these two modules are listed below-

Automatic Video Surveillance:

It is a technique which analysis the video footage of a camera to analyze any kind of human activity in the premises. It detects for a human being in the video followed by face detection and face recognition. A person if gets unrecognized, then a alert is generated in the form of an email and SMS to alert the owner of the premises about the unintended activity at his place. It uses the techniques of Object Detection, Body Detection, Face Detection and Face Recognition. All these parameters are verified before generating an alarm. This uses the existing camera infrastructure of a house, office, godawn, bank, etc. It sends an email Alert with the unrecognized image of the person intruded and an SMS in case of a body is detected. The main objective of this module is to make the owner aware regarding the unrecognized intrusions being conducted whenever the system is on so that the owner can take some desirable actions on the basis of the alert reports received in the form of E-mails, SMS and Graphs.

PiCrypt:

This feature enables the user to hide his or her secret message in a Raw Image File to make the communication secure from the Intruder. It hides the message in the Image in such a way

that a intruder is unable to guess that there is some secret message. Message is embedded into the Image by changing the pixel value of the image and the co-ordinates of the image where we hide the message is generated dynamically by tracking the user's mouse movement. So every time pixel position where the information is hidden is unique. This ensures that the pixels position selected is totally random and even if the intruder knows that the image carries sensitive information, even then he will not be able to decode the message. Only the person holding the key can decode the image to find the secret message hidden in it.

The presence of cameras in personal computers, cell phones is becoming extremely commonplace amongst every individual. As more and more people are equipped with these cameras it becomes feasible to develop a range of applications that utilize the camera for purposes other than simply taking a snapshot. One such application is to use the camera to provide a touch of security to oneself in terms of Data Security System and Automatic Surveillance System. A typical use of techniques like Digital Image Processing and Video Processing in a right direction can contribute a lot towards the security concerns and issues of an individual.

Further to this, the project serves the security tools based on Information Security and Physical Security in following aspects —

    a. To provide a tool to automate the monitoring of the footage coming from the camera source.

    b. To sense the intrusion in the video footage by using techniques like motion detection and object tracking.

    c. To provide a tool that can secretly hide the information inside a image to make it unsusceptible for the intruder.

d. To generate an alert in case of some threat is detected so that quick actions can be taken by the authorities.The alerts can be in the form of e-mails and SMS.

## 1.4 Literature Survey

There are many existing applications in market for automatic surveillance and picrypt. These provide services using the reference frame methodology for surveillance system. In this, the first frame as the reference frame is taken to compare it with all the other upcoming frames in the video to detect any changes in the surrounding over a particular interval of time. Many of these have problems such as such as high cost, low intelligence, poor stability, weak security, slow response and etc.

Automatic Implementation in CCTv cameras are very basic which are using the techniques that is obsolete and has certain drawbacks such as an change in the camera angle can degrade the performance, sometime even failures in detection also it need constant restarting of the system to fix such errors.

For PiCrypt, the Traditional image steganography follows the practice to hide the information in the fixed and predefined positions which the intruder are well aware off. So these encrypted images are easily decoded by the intruder making it an unreliable old technique. These technique are no longer followed by any user as the decoding pattern is already known to the intruder.

Many available applications have worked to raise the degree of accuracy of algorithms under indoor scenes and tried to provide solutions to the aforementioned problems. "Implementation of motion detection system" put forward a motion detection system which provides an efficient method for surveillance purposes and provide a facility to use an audio file as alarm signal. "Tracking And Recognizing The Moving Object In

Real Time Using Frame Difference Method" states motion detection and object tracking method which is simple and direct with which the changing part in video can be quickly detected.

Apart from this, the previous study and work related to information security usin digital image steganography has been since long. Image cryptography and steganography performed in frequency domain using random phase mask encoding are presented. The use of random phase mask allows to de-correlate initial image and makes it unrecognized. This property is used for proposed image encryption and for steganography to increase the security level of the encoded image and to make it less visible. Finally, two keys are needed to decrypt the image. The efficiency of the proposed approach is demonstrated by the computer modeling that helps for securing the message. Mohammad Ahmad Alia, Abdelfatah A. Yahya, proposes a method which describes two steps for hiding the secret information by using the public steganography based on matching method. This is done by two steps: Find the shared stego-key between the two communication parties over insecure networks by applying Diffie Hellman Key exchange protocol, then sender uses the secret stego-key to select pixels that it will be used to hide. Each selected pixel used to hide 8 bits which depends on the matching method. This steganographic protocol is more efficient than LSBs. It produces matching between the data bit parts and selected or least significant bits of each pixel. But due to the usage of conventional tools and techniques the data hiding process becomes less secure. Because of this reason, there is a need of a methodology which does not follow the traditional mechanism but implements the technique of dynamic key generation in order to make the hidden information more secure and safe from the untrusted parties.

On the basis of this literature survey, following considerations where taken while the development of the application Eagle Eye.

1. Development of such an application that does not restrict the surveillance module with a particular area or region.

2. Development of such application that reports the owner spontaneously along with proper and accurate messages.

3. Development of such application that helps secure data within an image that can not be easily extracted by any attacker.

4. Development of an application that is cost effective or has no installation cost and requires minimal or nil human interventions.

5. The application should be easy to use and minimum skills should be required to run the application.

## 1.5 Problem Statement

To resolve the need of a system that provides the security tools which can-

1) Automate the surveillance task that can detect the intrusion automatically and alert the owner immediately.

2) Hide the information within an image without using the conventional techniques of steganography.

## 1.6 Scope of Study

Based on the survey conducted on the available tools and techniques, following advancement are proposed in this project.

For Automatic surveillance:

Recording everything makes it time-consuming for a human to review the stored video. All these disadvantages limit the effectiveness of traditional video surveillance. To solve these problems, recording only crucial images that contains important information is the only way. This project uses a robust motion detection algorithm for real-time motion detection by considering and information, i.e., image that contains motion in the scene. This can be done with a web camera and a motion detection algorithm that detects motion. The motion detection algorithm robustly distinguishes motion from lighting changes. Web camera can take the snapshot of the moving object and at the same time, it will activate the warning system before storing the frames on the memory. Identifying moving objects from a video sequence is a fundamental and critical task in many computer vision applications.

The conventional approach of using the reference frame model, that is the first frame when the computer vision is called is captured and used as the reference for comparing it with the upcoming frames in order to detect and report intrusion(if any) to the ower. This makes the application restricted to a particular area or region of the vision provided. Any change in position from the initial condition can make the project stop working and show incorrect results. In order to avaoid such scenario, EagleEye does not use reference frame model where as considers each frame as a new frame and looks for only those possibilites where the security concerns are high.

The Alert mechanism of EagleEye provides two facilities such as sending email to the owner which covers the snapshots of intrusion being detected. It also send the SMS to the owner and warning him/her with a risky scenario.

The intrusion detection module covers not only motion detection but also body scanners as face detection, upper, lower and full body detection and biometrics as

face recognition to classify the intruder being a trusted party or a third party who can harm the owner.

For PiCrypt:

Usage of the conventional tools and techniques like DES, Diffie Hellman and many other cryptographic algorithms are very strong in terms of cryptography. But due to the fact of the availability of the loop holes and knowledge of such algoritms, it might become very easy for anyone with the knowledge of such techniques to break the  key and get access to the data hidden within the image. This leads to the requirement of the development of such an application that generates a dynamic key each time user wants based on the motion tracking system within the appliction. This helps to secure the data hidden with in the image as the actual possible coordiantes can not be recognised easily.

# Chapter-2 System Analysis

Systems analysis is the process of observing systems for troubleshooting or development purposes. It is applied to information technology, where computer-based systems require defined analysis according to their makeup and design.

## 2.1 General

In IT, systems analysis can include looking at end-user implementation of a software package or product; looking in-depth at source code to define the methodologies used in building software; or taking feasibility studies and other types of research to support the use and production of a software product, among other things.

Systems analysis professionals are often called upon to look critically at systems, and redesign or recommend changes as necessary. Inside and outside of the business world, systems analysts help to evaluate whether a system is viable or efficient within the context of its overall architecture, and help to uncover the options available to the employing business of the other party.

## 2.2 Preliminary Analysis

The project is divided into two modules-

1) Automatic Surveillance System

This module has been taken considering the need to have a system that can automate the task of CCTV footage surveillance. Automatic surveillance is done in order to remove the manual human support to the system, to make it less prone to the human error that can occur which makes the system vulnerable. The goal is to detect any intrusion in a particular area and to notify the owner through an E-mails and SMS. All this is done using the techniques of Biometrics and Body Scanners as-

      a.   Face and Body Detection

b. Face Recognition

The owner is made aware about the intrusions conducted in his absence using Alert Management mechanism. This includes-

a. Sending Electronic Mail to the owner on his registered e-mail ID which includes the snapshots of the intrusion as the face of the person termed as unknown by the system.

b. Sending SMS to the owner on his registered mobile number which aims at creating awareness about some intrusion being conducted.

c. A Graph plot which depicts to state each and every motion in terms of duration from the start of the application to its termination.

2) PiCrypt

This module is a Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt. The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination. The decrypt module is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that.

The user can also use the Mouse Tracker to generate a random encryption key for performing image steganography. This mouse tracker is available within the application itself. This helps in making the entire process of hiding data within an image a secure process. The key generated is used for hiding the data within the image.

## 2.3 Feasibility Study

Secure-101 provides feasible solution to all of user's requirement in best manner. This project provides each solution keeping in mind technical factors, social factors, and reliability factors so that it provides feasible solution to each requirement.

There are three types of Feasibility Study:

1. Technical Feasibility

2. Economic Feasibility

3. Operational Feasibility

## 2.3.1 Technical Feasibility

This assessment is based on an outline design of system requirements, to determine whether the company has the technical expertise to handle completion of the project. EagleEye has a strong technical background as it is able to handle live footage with the surveillance being done automatically. With requests volumes and varieties constantly increasing this project is a key consideration to solve these. Using Automatic surveillance, we see that it provide great computing power and it is able to process request fast.

Automatic Surveillance is quite stable system. One can easily rely on this system because of its ultimate performance even in tough working conditions. In any unfavorable situation, development team can be consulted when problem arise or improvements are required.

1. Computing Power: Secure - 101 does not need much computing power. It can work in the system with minimal configuration.

2. System Performance: It can be seen using this system that it is able to do the said task in an appropriate manner and under convenient time.

3. Interface: It provides user friendly interface through well developed Tkinter and Python Application named- EagleEye.

4. Manpower Requirement: The interface and functionality of the project is made such that it requires minimal intervention from a human and the services are made automated where results can be generated from a single click.

5. Scalability: The project is scalable enough for any future changes.

## 2.3.2 Economic Feasibility:

The purpose of an economic feasibility study is to demonstrate the net benefit of a proposed project for accepting or disbursing electronic funds/benefits, taking into consideration the benefits and costs to the agency, other state agencies, and the general public as a whole.

EagleEye provides economically feasible solutions as it does not involve huge cost in development and requires minimum investments during operations. Cost involved in development is only for the Systems.

1. Easy Installation: No additional components are required to setup the application. Hence reducing the installation cost.

2. Risk Factor: In a long run, this application does not crash or does no harm to the user system.

3. Low Cost: EagleEye aims at reducing the total cost of the requirements necessary to help protect the belongings from the untrusted parties. Here the requirement for the setup to work correctly is minimal.

4. Labor: The working of application requires least human involvement and skills. Thus reducing the requirements of skillful labor in order to operate it.

### 2.3.3 Operational Feasibility

Operational feasibility is the measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.

EagleEye provide high operational capabilities which is likely to achieve desired objectives of automatic surveillance and image steganography. This objective is attained by providing a user interface which is well designed to guide the user through the app feature. App is well designed and does not crash, so it quite reliable to use the app. Features provided by the app are thoroughly tested by the developer with applying various testing techniques so as to minimize the chances of failures while using the app.

It has a positive effect on the organization since it is able to fit into their existing systems as it does not require any special requirements or additional hardware and other application to install. The basic infrastructure is well supported and does not require any additional component to be installed on the system.

It is so much user-friendly that any non-technical person is able to operate the system without having background knowledge about the system implementation or working and it fits very well into current day-to-day operations.

This application is able to fill user's requirement effectively thus provide a great operational feasibility.

## 2.4 Software and Hardware Requirement

Software Specification

1.  Platform -Python (Version 2 and above)

2.  GUI Designing - Tkinter

3. Computer Vision - OpenCV (Version 2 and above)

4. Alert Generation – 1. SMTP Client Package, MIME (For E-mail)

5. Twilio (For SMS)

6. Graph Plot and Presentation – Bokeh

7. Image Analysis – Pillow (PIL)

8. Operating System- Windows/Linux/ MAC

9. More Packages and Libraries –

    a. Multiprocessing

    b. Numpy

    c. Pandas

Hardware Specification

1. Web Camera

2. Memory: 2GB RAM

3. Secondary Storage: 20 GB Hard disk

4. Processing Power: Intel Dual core processor

5. Mouse or a Touch Panel

Descriptions-

1. Why Python:

Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an ideal language for scripting and rapid application development in many areas on most platforms and Python is Open Source so we

don't need to pay for licensing and python provides rich sets of built in libraries for handling network and web related data in effective and efficient manner.

2. GUI  Designing:

Tkinter is the standard GUI library for Python. Python when combined with Tkinter provides a fast and easy way to create GUI applications. Tkinter provides a powerful object-oriented interface to the Tk GUI toolkit.

Creating a GUI application using Tkinter is an easy task. All you need to do is perform the following steps −

1.  Import the Tkinter module.

2.  Create the GUI application main window.

3.  Add one or more of the above-mentioned widgets to the GUI application.

4.  Enter the main event loop to take action against each event triggered by the user.

3. Smtplib:

The smtplib module defines an SMTP client session object that can be used to send mail to any Internet machine with an SMTP or ESMTP listener daemon. Sending mail is done with Python's smtplib using an SMTP (Simple Mail Transfer Protocol) server.

4. OpenCV:

OpenCV (Open Source Computer Vision) is a library of programming functions mainly aimed at real-time computer vision. It is immensely used in Digital Image Processing. With the help of this library, live streaming of the current scenarios can be easily monitored, recorded and analysed.

5. PIL:

Python Imaging Library (abbreviated as PIL) (in newer versions known as Pillow) is a free library for the Python programming language that adds support for opening, manipulating, and saving many different image file formats. It is available for Windows, Mac OS X and Linux.

6. Twilio:

Twilio with python allows to send SMS, do Video calls, send voice message within the programming control. Here in this project, Twilio is used to send the Alert SMS to the owner, warning against some intrusion conducted in his absence.

## 2.5 Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its *process* aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).DFD for EagleEye can be deoicted in following m

## 2.5.1 Level 0 DFD

A system context diagram (SCD) is a diagram that defines the boundary between the system, or part of a system, and its environment, showing the entities that interact with it. This diagram is a high level view of a system.

The figure below shows a context Data Flow Diagram that is drawn for a EagleEye System. It contains a process that represents the system to model, in this case, the "EagleEye System". It also shows the participants who will interact with the system, called the external entities. In this example, Camera and Raw Image are the two entities who will interact with the system. In between the process and the external

entities, there are data flow that   indicate the existence of information exchange between the entities and the system.
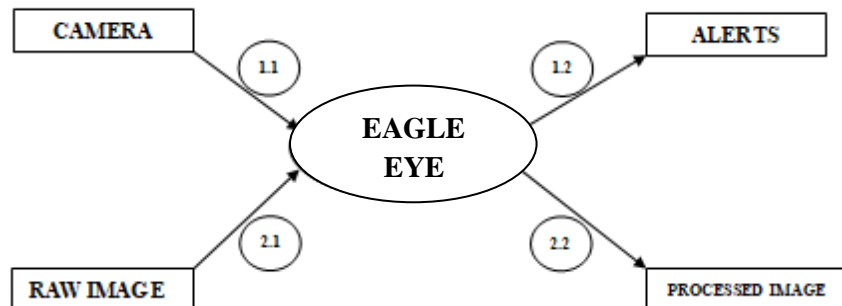


**FIGURE 2.5.1: Level 0 DFD of EagleEye**

The context level diagram for EagleEye describes the system design at level 0. The characteristics of this application can be depicted using the DFD is listed below. Each phase of the level 0 DFD  for EagleEye is:

1.1 Camera Input: This component provide camera input to the EagleEye System. This is the source of live video to the system in the form of continuous frames. It is a device for capturing a photographic image or recording a video.

1.2 Alerts: Alert is the output module of EagleEye system which is trigerd in case the system detect any kind of intrusion in the frame being processed, User is given alert through this module of the system in the form of an email and a SMS.

2.1 Raw image: This is the input to the system in the form of an image which the user wishes to use for hiding the informtion in the image, The image can be of common formats like png, bmp, jpg and etc. It takes the input from the user and pass it to EagleEye System for further encoding and decoding.

2.2 Processed Image: After the EagleEye encode or decodes the image given by the user, a new image is generated which holds the secret message of the user.

EagleEye System: It takes the video frames from the camera input and process it frame by frame. In case of it detect any unauthorized party. It generates an alert to the owner of the system. This system also takes the raw image to apply data hiding techniques on that image. After encoding, a processed image is generated which holds the secret information.

## 2.5.2 Level 1 DFD

Level 1 DFD aim to give an overview of the full system. They look at the system in more detail. Major processes are broken down into sub-processes. Level 1 DFD's also indentifies data stores that are used by the major processes.

The figure below shows the level 1 DFD, which is the decomposition (i.e. break down) of the EagleEye System process shown in the context DFD. Read through the diagram and then we will introduce some of the key concepts based on this diagram.

The EagleEye System Data Flow Diagram contains four processes, two external entities and four processing components. Although there is no design guideline that governs the positioning of shapes in a Data Flow Diagram, we tend to put the haprocesses in the middle and external entities on the sides to make it easier to comprehend.

Based on the diagram, we know that a Automatic Surveillance will receive the frame inputs by the camera source which then analyze it for any unrecognized person in each frame. From here it generates an alert by sending an email and SMS to the user. Analysis is also shown on the user's screen in the form of live video.

EagleEye also used PiCrypt to hide the information inside the image in a secret way, for this it takes raw image as a input and a secret message. PiCrypt generates the secret key by taking dynamic input of the user from the mouse movement of the user. A key is generated which acts as a coordinates to encode the image on that coordinates. After key generation, a processed image is formed which is identical to the raw image but contains the secret message.

Finally, we get the result from EagleEye in the form of alerts and processed images. Alerts are either in the form of email or SMS. Finally, the processed image received from PiCrypt is in the same format as of raw image.

This procedure is expressed pictorially using the Data Flow Diagram and is named as Level 1 DFD. Each step numbered in this DFD is a process involved within the System architecture and design for proper functioning of the application. These steps are explained above.
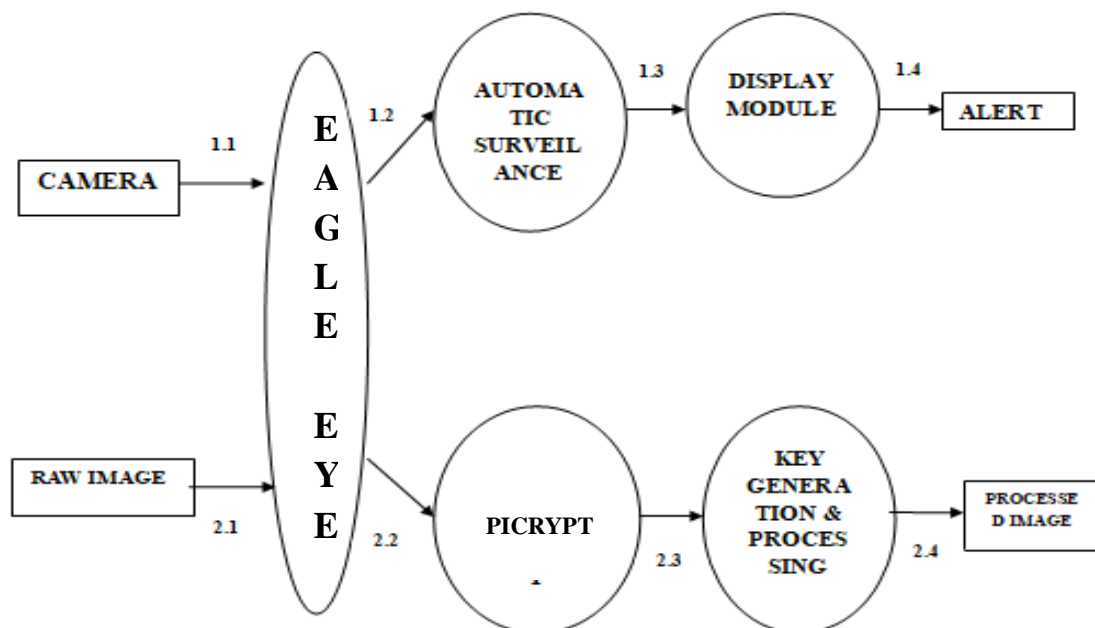


**FIGURE 2.5.2: Level 1 DFD of EagleEye**

### 2.5.3 Level 2 DFD

A level 2 data flow diagram (DFD) offers a more detailed look at the processes that make up an information system than a level 1 DFD does. It can be used to plan or record the specific makeup of a system

For EagleEye, Level-2 DFD is divided into two separate modules namingly, Automatic Surveillance and PiCrypt.

### 2.5.3.1 Level 2 DFD for Automatic Surveillance

The figure below shows the level 2 DFD for Automatic Surveillance, which is the further decomposition of EagleEye system. In this, we will explain the working of Automatic Surveillance System.

Based on the diagram, a real time frame acquisition is done which is taken from the camera. After that, the frame is analysed for the presence of body in the frame through our body detection classifiers. Then the frame is analyzed for the biometrics like Face Detection and Face Recognition. If it is a unrecognized face, then a alert is generated in the form of an email with the snapshots and a SMS with a message alerting the user instantly. A sms is sent in case of a body is detected and an email is sent in case of Face is detected and is unrecognized.

Finally, the system is able to generate an alert in case of some intrution in the surveillance area. Based on the intrution, email also contains a video during the time of intrusion and the full video at that point of time. This is sent only after there is unrecongnized person is detected in the premises.
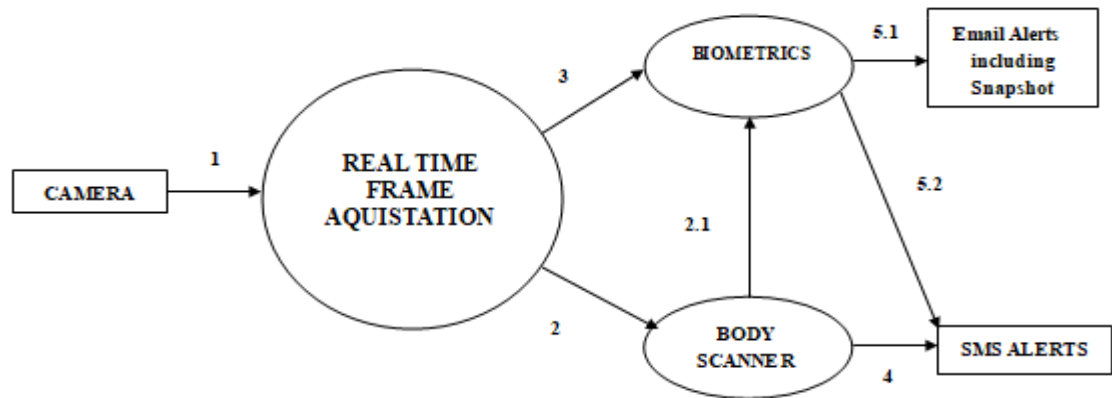
**FIGURE 2.5.3.1: Level 2 DFD for Automatic Surveillance**

## 2.5.3.2 Level 2 DFD For PiCrypt

Level 2 DFD for PiCrypt is shown in the given figure. It has two major processing components: Encoder and Decoder.

Encoder module is responsible for hiding the secret message behind the image pixels by changing the RGB value of the pixels. Pixels where this is done is picked from a secret and user generated dynamic key taken with the user's mouse movements over the screen.

Key Generation is done by tracking the mouse movements of the user over the screen. Those points are recorded and used as the points or pixels position in the image where changes are made. 0

An encoder takes raw image, secret message and Dynamic Key generated through user's mouse movement as an input. It then processes the image using the Key to change the value of the pixel with respect to the ascii value of the each character of the message.

24
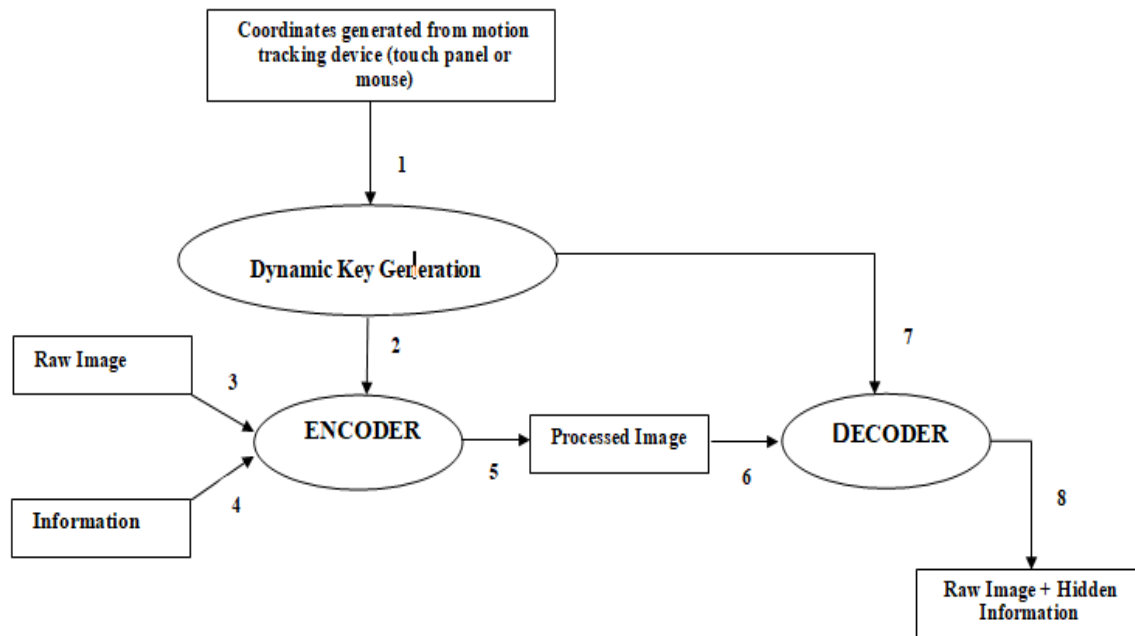
**FIGURE 2.5.3.2: Level 2 DFD for PiCrypt**

Decoder module is responsible for extracting information or secret message from the image using the secret key user has generated and the encoded image.

Decoder takes encoded image and key as an input, it then processes the image by extracting the information from the pixels by going through pixels at the positions as taken from the key. Secret message is extracted successfully from the image after the decoding process.

# Chapter 3- System Design

A design specification is a detailed document providing information about the characteristics' of a project to set criteria the developers will need to meet. Its use is called for where a structure or product has to be specially made to meet a unique need.

For example, a design specification must include all necessary drawings, dimensions, environmental factors, ergonomic factors, aesthetic factors, and cost maintenance that will be needed, quality, safety, documentation and description. It also tells specific examples of how the design of the project should be executed, helping others work properly.

## 3.1 System Overview

Overview of the system with respect to the design, the designing phase has to be carried out properly. It consists of certain diagrams that is important and the coding module is to be implemented here.

The EagleEye developed here is for the use of providing a low cost with high quality secuirty assurance and alert management from intruders and ohter untrusted parties.From the view of the users there can be many more respect, for its usage. We have further generalised the software for various purposes. The software can be used as home surveillance system as well as for bank or hospital, shops, and many more. Further user can add or use any picture or image for hiding data.

Further to make the application easily available to all, an executable file has been created. The .exe file is to be installed in the system and thus can be used for required purpose. The advantage of the software is the independent platform. No Restriction to OS. The use of python makes the developers more comfortable, as the

open community language for it, makes the project worthier. The Graphicaal User Interface here used is tkinter.

The development here though is in python, still for user can easily operate the software without the knowledge of python. GUI helps to provide certain features which we will come through in further document.

### 3.1.1 User Interface

GUI (Tkinter**):**

Tkinter is a python library for creating GUI applications. It is a blending of Python programming language. Tkinter consists of a number of modules. The Tk interface is provided by a binary extension module named _tkinter. This module contains the low-level interface to Tk, and should never be used directly by application programmers. It is usually a shared library (or DLL), but might in some cases be statically linked with the Python interpreter.

The public interface is provided through a number of Python modules. The most important interface module is the Tkinter module itself. To use Tkinter, all you need to do is to import the Tkinter module:

```
import Tkinter
```

Or, more often:

```
from Tkinter import *
```

The Tkinter module only exports widget classes and associated constants, so you can safely use the from-in form in most cases. If you prefer not to, but still want to save some typing, you can use import-as:

```
import Tkinter as Tk
```

It allows to add buttons, grid them together form menus and a complete kit of packages to help provide user with an interactive interface.

## 3.2 Design Considerations

The design considerations phase is where a list of factors is made that need to be considered in broad terms. It does not need to go into the details (i.e. the specifics) at this stage. The type and number of factors we have is unique for each project. That means everyone will have their own set of design considerations specific to their design brief. A good set of design considerations accurately addresses the unique areas of concerns of our proposal as written in our design brief.

The Functionality and the user need to know may come in this phase. The Functionality consists of the Graphical User Interface that the user can work upon. The Developers can also work upon its interface. The important part from developer's point of view is their working in the coding part. They can contribute and work in some of its functionality, like use of certain libraries of the languages and some of its new functions and classes. Further to this, the categories in which the designing of the Application is classified as follows-

    a. Accountability
    b. Budget Management
    c. Communication
    d. Scheduling
    e. Quality Control

## 3.2.1 Design Constraints

Design constraints (or limitations) are the extensions of design considerations.  In every design attempt, there will be limitations or constraints or some form of hindrance. Some projects may be constrained by physical space or budget. Some limited by the choice of materials or colors. And most of them with time constraint.

The Design constraint that 'EagleEye using python' has is related to time constraints, that takes amount of time in the coding part. The GUI development might make the developer somewhat boring and report of the intrusion detection or the alert system might have the issues related to user's internet. Slow internet might have delayed responses or even no results may come up.

For steganography, the user might face certain images not being supported by the application (due to unsupported extensions). There can also be a possiblity where the key generation might take some time.

### 3.2.2 Future Contingencies

This section describes any contingencies that might arise in the design of the system that may change the development direction. Possibilities include lack of interface agreements with outside agencies or unstable architectures at the time this document is produced. Address any possible workarounds or alternative plans.

### 3.3 System Architecture

An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. A system architecture can comprise system components, the expand systems developed, that will work together to implement the overall system.

### 3.3.1 System Hardware Architecture

Hardware architecture refers to the identification of a system's physical components and their interrelationships. This description, often called a hardware design model, allows hardware designers to understand how their components fit into a system architecture and provides to software component designers important information needed for software development and integration.

### 3.3.2 System Software Architecture

Software application architecture is the process of defining a structured solution that meets all of the technical and operational requirements, while optimizing common quality attributes such as performance, security, and manageability. It involves a series of decisions based on a wide range of factors, and each of these decisions can have considerable impact on the quality, performance, maintainability, and overall success of the application.
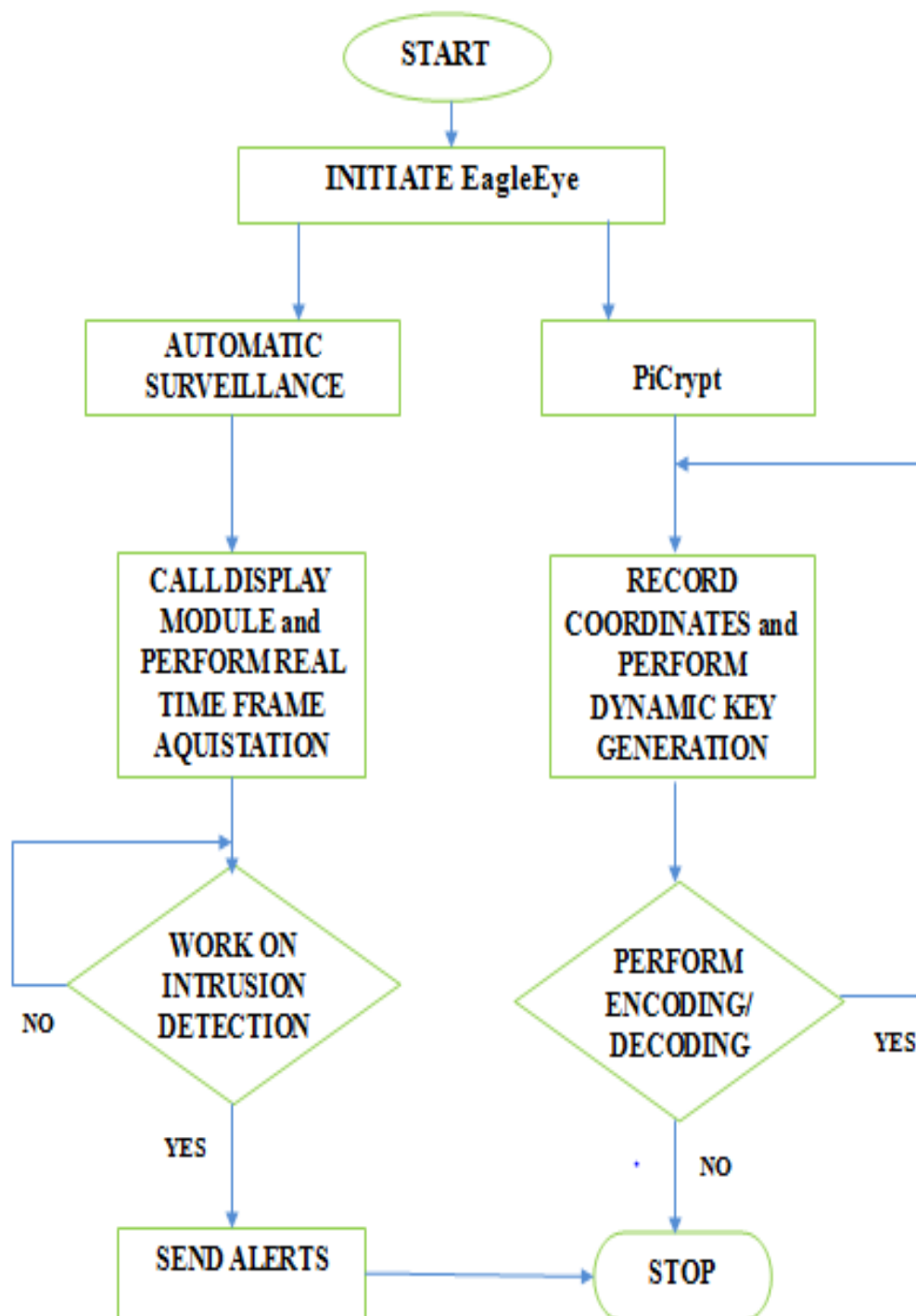
### 3.3.3 Flowchart



FIGURE 3.1 Flowchart for EagleEye

## 3.4 Interface Design and Description

The Unified Modeling Language (UML) is a general-purpose, developmental, modeling language in the field of software engineering that is intended to provide a standard way to visualize the design of a system. UML offers a way to visualize a system's architectural blueprints in a diagram (see image), including elements such as-

1. any activities (jobs)

2. individual components of the system and how they can interact with other software components

3. how the system will run

4. how entities interact with others (components and interfaces)

5. external user interface.

## 3.4.1 Use Case Diagram

Use case diagrams are usually referred to as behavior diagrams used to describe a set of actions (use cases) that some system or systems (subject) should or can perform in collaboration with one or more external users of the system (actors). Each use case should provide some observable and valuable result to the actors other stakeholders of the system.

For Eagle Eye, the actors are-

1. Admin of the system

2. User of the System

3. Outsider
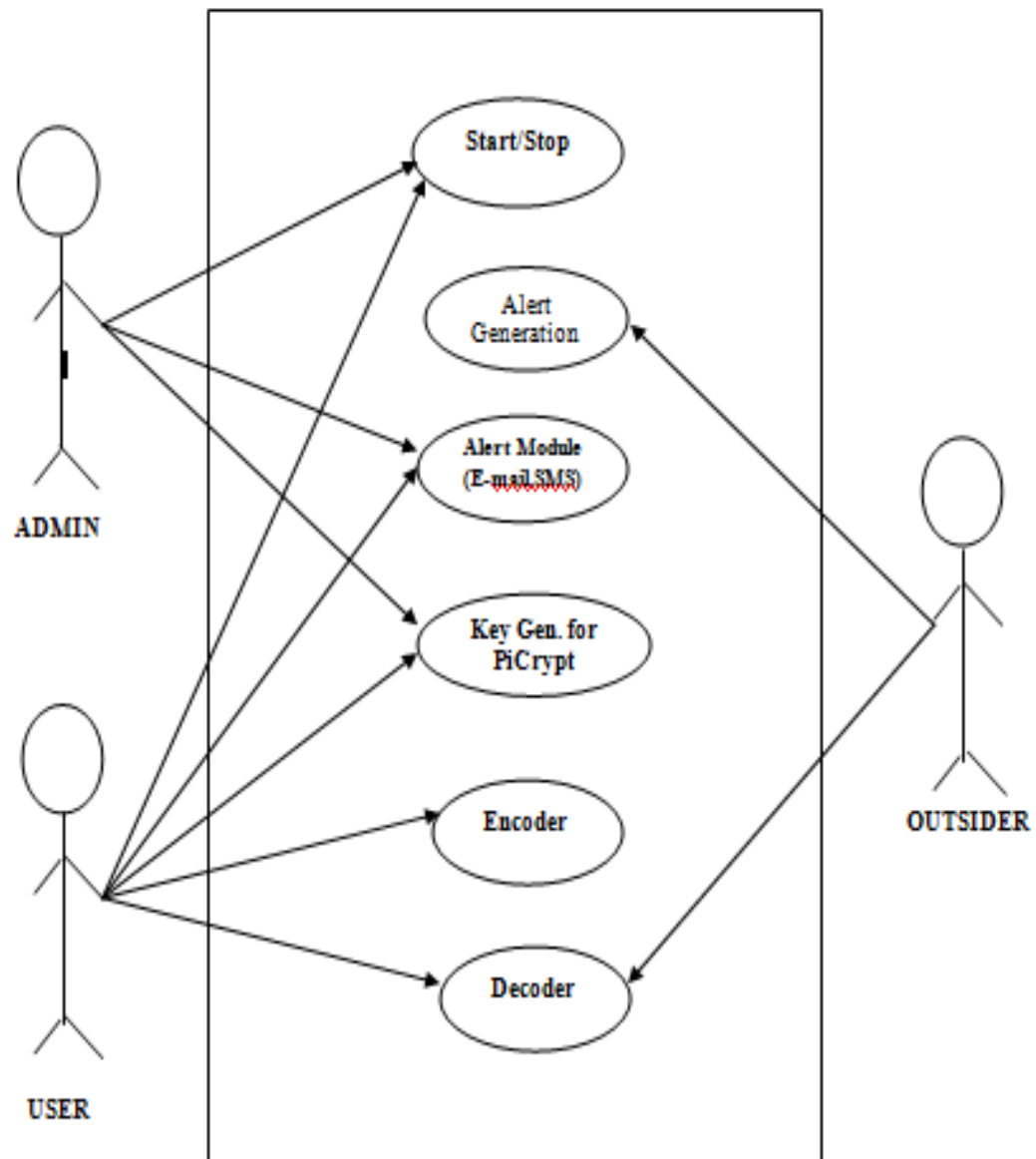
**Figure 3.4.1: Use Case Diagram**

# Chapter-4 Testing

A testing strategy is a general approach to the testing process rather than a method of devising particular system or component tests. Different testing strategies may be adopted depending on the type of system to be tested and the development process used. There are two different strategies available: Top-Down Testing and Bottom-Up Testing.

In Top-Down Testing, high levels of a system are tested before testing the detailed components. The application is represented as a single abstract component with sub-components represented by stubs. Stubs have the same interface as the component but very limited functionality.

After the top-level component has been tested, its sub-components are implemented and tested in the same way. This process continues recursively until the bottom - level components are implemented. The whole system may then be completely tested. Top-down testing should be used with top-down program development so that a system component is tested as soon as it is coded. Coding and testing are a single activity with no separate component or module testing phase.

If top-down testing is used, unnoticed design errors may be detected at an early stage in the testing process. As these errors are usually structural errors, early detection means that extensive re-design re-implementation may be avoided. Top-down testing has the further advantage that we could have a prototype system available at a very early stage, which itself is a psychological boost. Validation can begin early in the testing process as a demonstrable system can be made available to the users.

Bottom-Up Testing is the opposite of Top-Down. It involves testing the modules at the lower levels in the hierarchy, and then working up the hierarchy of modules

until the final module is tested. This type of testing is appropriate for object-oriented systems in that individual objects may be tested using their own test drivers. They are then integrated and the object collection is tested.

## 4.1 Testing Techniques and Testing Strategies

Black Box Testing

This treats the system as one that cannot be seen in detail. The structure of the program is not taken into account. The tests are performed based on what the program does. This is sometimes called Functional Testing.

The functional requirements have been agreed with the customer. Thus they can see that the program performs as it was requested at the specification stage. It is difficult to know just how much of the program coding has been tested in this case.

The acceptance testing stage takes place nearer the end of the software development and it follows an agreed test plan. It applies a black box approach to see how software conforms to the customer's functional requirements.

White Box Testing

This treats the system as one in which the workings can be seen. The structure of the program is taken into account when tests are designed for the program. This is sometimes called Structural Testing. It should do the following:

Guarantee that all statements in the program have been tested at least once, ie: identify all pathways through code (eg: sequence, selection and iteration).

Test all the decision statements on their true and false side and check to see which of these paths have not been tested in the Black Box approach. Test all loops at their boundaries and their operational limits. Exercise internal data structures to check their validity. Create new test data for paths not already tested.

EagleEye is tested using both the testing models: Black Box Testing and White Box Testing. The two types of testing, i.e, Unit testing and System testing are-

A. Unit Testing: It is the testing which is done on individual components of the tool EagleEye to test the functionality of it independently. We have built the project doing the unit testing of each component and at the same time integrating them after successful tests.

B. System Testing: After complete integration of the modules of EagleEye, a complete system test is conducted where each functionaliy is tested for accurate result as a whole. It involved performing repeated tests on the top level of the hierarchy, which uses the components in the bottom hierarchy as a whole.

Advantages of unit testing:

Issues are found at early stage. Since unit testing is carried out by developers where they test their individual code before the integration. Hence the issues can be found very early and can be resolved then and there without impacting the other piece of codes.

2. Unit testing helps in maintaining and changing the code. This is possible by making the codes less interdependent so that unit testing can be executed. Hence, chance of impact of changes to any other code gets reduced.

3. Since the bugs are found early in unit testing hence it also helps in reducing the cost of bug fixes.

4. Unit testing helps in simplifying the debugging process. If suppose a test fails, then only latest changes made in code needs to be debugged.

## 4.2 Debugging and Code Improvement

Verification and Validation

Before getting into the various forms and strategies of testing we must understand the process of verifying and validating the software code. Verification and validation is the generic name given to checking processes which ensure that the software conforms to its specification and meets the needs of the customer.

The system should be verified and validated at each stage of the software development process using documents produced in earlier stages. Verification and validation thus starts with requirements reviews and continues through design and code reviews to product testing.

Verification and validation are sometimes confused, but they are different activities.

The difference between the two can be summarized as follows:

Validation: Are we building the right product?

Verification: Are we building the product right?

Verification involves checking that the program conforms to its specification.

Validation involves checking that the program as implemented meets the expectations of the customer. Requirements validation techniques, such as prototyping, help in this respect. However, flaws and deficiencies in the requirements can sometimes be discovered only when the system implementation is complete.

To satisfy the objectives of the verification and validation process, both static and dynamic techniques of system checking and analysis should be used. Static techniques are concerned with the analysis and checking of system representations such as the requirements document, design diagrams and the program source code. Dynamic techniques or tests involve exercising an implementation.

Static techniques include program inspections, analysis and formal verification. Some theorists have suggested these techniques should completely replace dynamic techniques in the verification and validation process and that testing is not necessary, this is not a useful point of view and could be 'considered harmful'. Static techniques can only check the correspondence between a program and its specification (verification). They cannot demonstrate that the software is operationally useful.

Although static verification techniques are becoming more widely used, program testing is still the predominant verification and validation technique. Testing involves exercising the program using data like the real data processed by the program. The existence of program defects or inadequacies is inferred from unexpected system outputs. Testing may be carried out during the implementation phase to verify that the software behaves as intended by its designer. This later testing phase checks conformance with the requirements and assesses the reliability of the system.

Python unit test

Python's unit testing module, unit test, comes packaged with all standard Python Installations. Unit test will do the following:

i.  ⬜Provide setup and teardown functions that run before and after each unit test.
ii. ⬜Provide several types of "assert" statements to allow tests to pass or fail.
iii. ⬜Run all functions that begin with test_ as unit tests, and ignore functions that are not pretended as tests

The following provides a very simple unit test for ensuring that 2+2 = 4, according to Example Python:

```
import unittest
```

```python
class TestAddition(unittest.TestCase):

    def setUp(self):

        print("Setting up the test")

    def tearDown(self):

        print("Tearing down the test")

    def test_twoPlusTwo(self):

        total = 2+2

    self.assertEqual(4, total);

if __name__ == '__main__':

unittest.main()
```

Problems and Errors encounterd while building the project while UNIT TESTING are-

1. OpenCV Installation:

2. Accuracy in Face Recognition:

    i) Light intensity

    ii) All angles needs to be recorded

    iii) Ambiguous Results

3. Alert Generation

4. Recording Coordinates and Key Generation:

Problems and Errors encounterd while building the project while SYSTEM TESTING are-

1. Multiprocessing Issues

2. System Accuracy

All these encountered errors and issues where timely reported and rectified in order to attain the maximum accuracy level.

# Chapter 5- Implementation

EagleEye is a application which provide features of Automatic Surveillance and Image Steganography which covers the domain of Image Processing. The System is designed in a simple way to make it easier for a non-technical person to use the system effectively.

There are 6 phases of EagleEye:

1. Installation: EagleEye can be installed by using an executable file. The .exe file is to be installed in the system and thus can be used for required purpose. Also it can be used in other operating systems by just using the main.py script of the project and by installing necessary packages as mentioned in the requirements.

2. Start/Stop: EagleEye provides an interface where a user can start the surveillance task and the image steganography task with the click of the buttons. Once the surveillance task starts, it can be stopped only by the owner's authentication.

3. Automatic Surveillance/ Steganography: This phase of EagleEye is associated with the continuous monitoring of the video for the intrusion in the camera's view. Video input is monitored for Body Detection, Face Detection, Face Recognition. And on unrecognized face, an alert is generated.

4. Alert and Sharing(Encoded Image): Whenever an intrusion is occurred, then an alert is generated in the form of an email or a SMS. User get notified about the intruder with the intruder's image and a small video during the time of intrusion.

5 Saving Records: A complete timestamp is recorded for each activity during the intrusion and even during the there is no intrusion. Owner is notified with complete graph showing all the time when there was some activity in the area.

6 Uninstallation: EagleEye can only be uninstalled with the owner's permission. A normal uninstallation is not possible without the permissions.

## 5.1 System Implementation

EagleEye can be installed by using an executable file. The .exe file is to be installed in the system and thus can be used for required purpose. Also it can be used in other operating systems by just using the main.py script of the project and by installing necessary packages as mentioned in the requirements.

EagleEye is platform independent, which means it will work on the Linux as well on the Windows OS. It has following components:

1. Interface - EagleEye is a desktop application. It has a menu from where the user can select one of the feature out of the two, which are Automatic Surveillance and Image Steganography. Tkinter is a Python binding to the Tk GUI toolkit. It is the standard Python interface to the Tk GUI toolkit,[1] and is Python's *de facto* standard GUI.[2] Tkinter is included with the standard Microsoft Windows and Mac OS X install of Python.

Window

This term has different meanings in different contexts, but in general it refers to a rectangular area somewhere on the user's display screen.

Top Level Window

The window that exists independently on the screen. It will be decorated with the standard frame and controls for the desktop manager. It can be moved around the desktop, and can usually be resized.

Widget

The generic term for any of the building blocks that make up an application in a graphical user interface. Examples of widgets: buttons, radio buttons, text fields, frames, and text labels.

Frame

In Tkinter, the Frame widget is the basic unit of organization for complex layouts.

A frame is a rectangular area that can contain other widgets.

Child and parent

When any widget is created, a parent-child relationship is created. For example, if you place a text label inside a frame, the frame is the parent of the label.

2. Surveillance - It takes an input from the user and analyze it frame by frame. First a body is detected in the frame, if found a SMS is sent to the owner stating that some intrusion is occurred in the premises. After that, the frame is recognized for the presence of the human face followed by the face recognition. In case, an unrecognized face is there, an email is sent to the owner with the picture of the intruder and a short clipping of that time. Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network, and may be watched by a security guard or law enforcement officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage, but analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database, and by video analysis software (such as VIRAT and Human ID). The amount of footage is also drastically reduced by motion sensors which only record when motion is detected. With cheaper production techniques, surveillance cameras are simple and inexpensive enough to be used in home security systems, and for everyday surveillance.

3. Image Steganography - Steganography is the practice of concealing a file, message, image, or video within another file, message, image. The advantage of steganography over cryptography alone is that the intended secret message does not

attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

## 5.2 Software Implementation

A product software implementation method is a systematically structured approach to effectively integrate a software based service or component into the workflow of an organizational structure or an individual end-user.

The aim of the project was to implement the software in such manner, so that user can easily access it. The language was considered to be tough for general users. To provide them Graphical User Interface was the approach. Tkinter helps to get user interface, it has also been designed using Python. The software is compatible with all the Operating Systems i.e. Linux, Windows, Mac OS etc. The cost for the software can be minimize as per the requirement. This Software has the instance of searching the jobs using the software.

## 5.3 Software Installation:

Software Implementation is an important part to analyse the environment in which the software is to be installed. After the analysis, comes the phase of proper installation in the particular system. The software here has an executable file. For different platform, this file extension may change, but the installation is easy with agreement to all terms and conditions. The process is simple in the system and after the complete installation of the software in the system, the user can use the application can be easily used in accordance to the requirements.

## 5.3.1 Installing Packages

The required packages and libraries necessary of setting up the software in a system are:

Software Specification

1. Platform -Python (Version 2 and above)

2. GUI Designing - Tkinter

3. Computer Vision - OpenCV (Version 2 and above)

4. Alert Generation – 1. SMTP Client Package, MIME (For E-mail)

5. Twilio (For SMS)

6. Graph Plot and Presentation – Bokeh

7. Image Analysis – Pillow (PIL)

8. Operating System- Windows/Linux/ MAC

9. More Packages and Libraries –

    a. Multiprocessing

    b. Numpy

      c.  Pandas

## 5.3.2 How to run Eagle Eye

1. Go to folder Eagle Eye.

2. Open the command line window there.

3. Run script main.py as

   --Python main.py

4. From the available choices select :

   Automatic Surveillance

   Or

   PiCrypt

5. Based on the selection of the services, the application functions accordingly. When Automatic Surveillance selected, a cv window will open which will continuously monitor  and based on the intrusions, alerts will be generated. When PiCrypt selected, user gets option to either generate a new dynamic key for encoding data within an image or use built-in encryption. After encoding the image, the user can also share it. Decoding the hidden information within an image can also be done using this application.

# CONCLUSION

The final conclusion of the above discussed project 'EagleEye' based on Digital Image Processing for Automatic Surveillance and PiCrypt using Python aims at providing the user(owner of the application ) with the utmost security assurance in with the help of Automatic Surveillance and PiCrypt.

As Security has always been one of the major concerns for an individual or any organization. The major idea behind the development of this application is to provide the user some security tools which help protect two of the most important and valuable assets. The Data, which can be protected with the help of the module named as PiCrypt which is evolved from Information Security using Steganography. The usage of traditional techniques and algorithms make the data hiding process less secure. In order to avoid this, we have used the approach of Dynamic Key Generation by recording the coordinates of the mouse or any touch panel and further used for hiding data within the image.

The second service, that is, Automatic Surveillance helps the user to protect the belongings even in his absence. With the help of this, the installation of CCTV cameras within a home, office or anywhere can be deprecated. In this way, the need of continuous monitoring of the environment or rewinding of the recorded video when some mishappening has been conducted is replaced by the Alert Management module of the application. The user receives emails, SMS and graph whenever some unwanted disruptions are encountered which helps the owner to take specific actions right in the nick of time.

Thus the provided features in the above discussed software gives it long scope in the future.

# FUTURE SCOPE

The application "Eagle Eye" has a long scope in the future. Following are few features that the development team aims at releasing in the coming time:

1. Implementation of the application on Raspberry Pie to make it portable and flexible for usage.

2. Live Coverage of the environment under surveillance on the mobile phone of the owner. This requires the development of the mobile app.

3. The application can be used for monitoring ill people and track their movements.

4. The Surveillance module can be implemented for traffic management.

5. The PiCrypt can further be extended to image analysis system where the details of a particular image in terms of the visual features made available in text form.

Further to these there are many more aspects where the development of the application can be extended.

# APPENDIX

## I. SCREENSHOTS

The software Eagle Eye starts as-
1. Run command python main.py
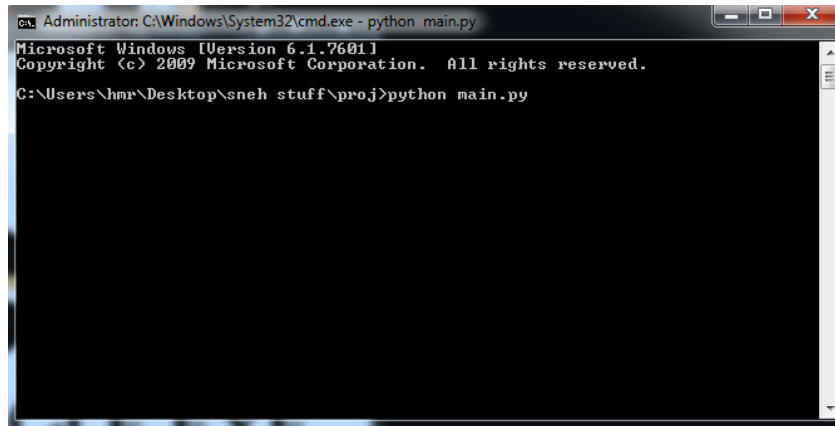


**Figure AI.1: Run the main Script**

2. The Application opens as-



**Figure AI.2: Initialization of EagleEve**

3. About the Application:
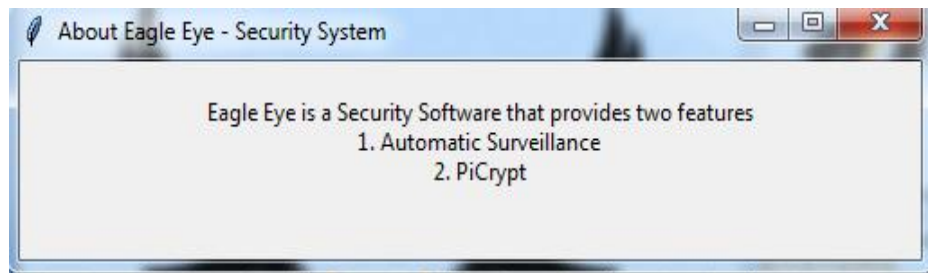


**Figure AI.3: About EagleEye**

4. On selecting service PiCrypt
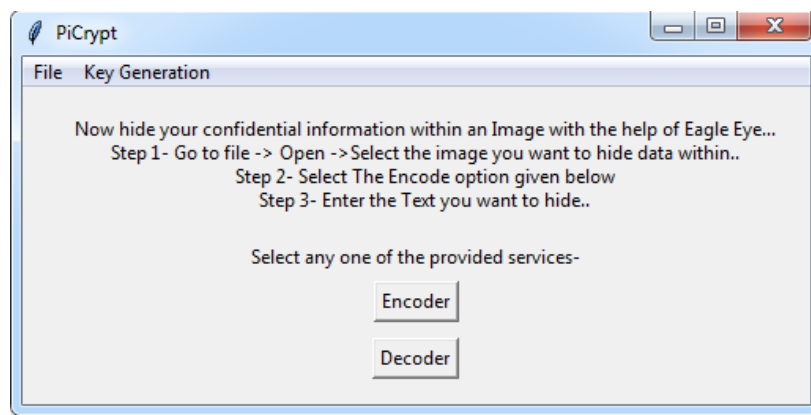


**Figure AI.4: Calling PiCrypt**

5. Generation of dynamic key:
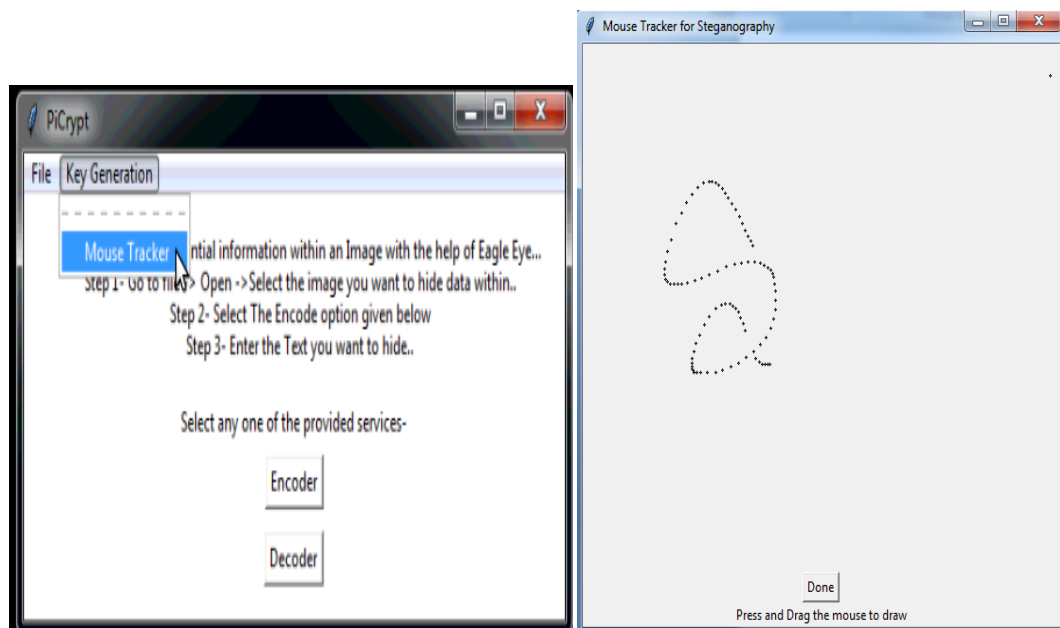


**Figure AI.5: Generating Dynamic Key**
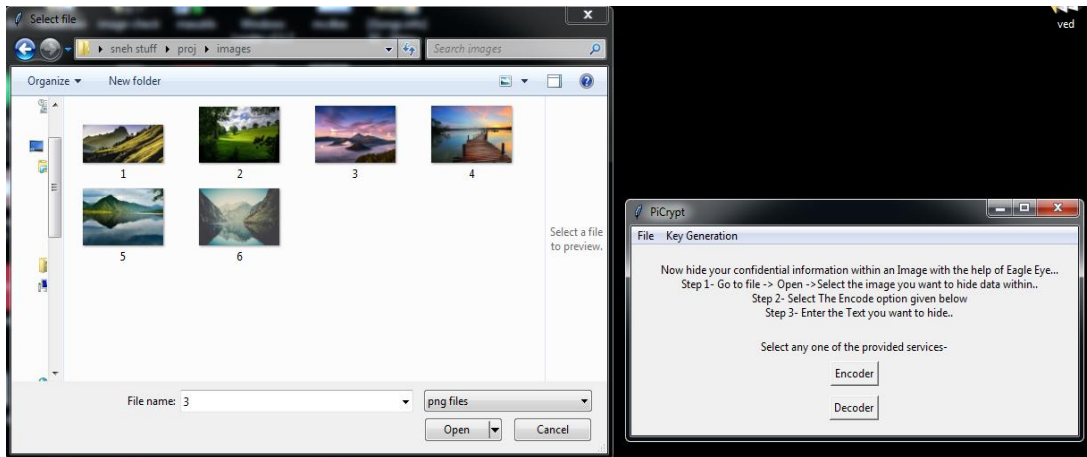
6. Encoding of images
Select image for encryption.



**Figure AI.6.1: Select the Image for encoding**
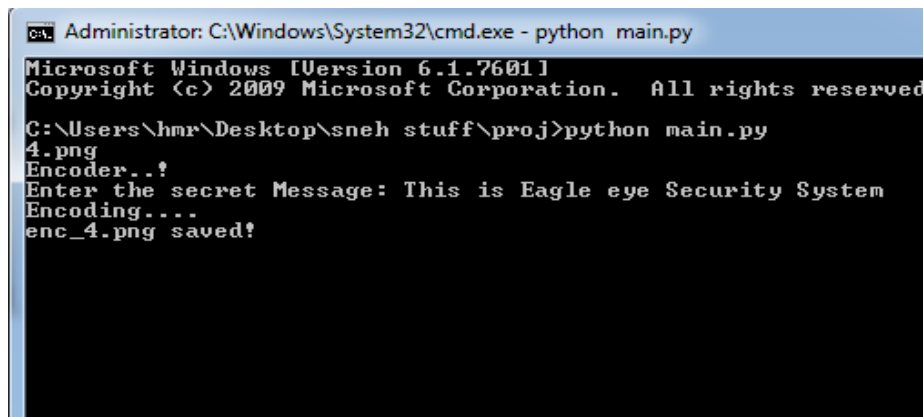


**Figure AI.6.2: Enter Secret Information**

7. Decoding of the Image
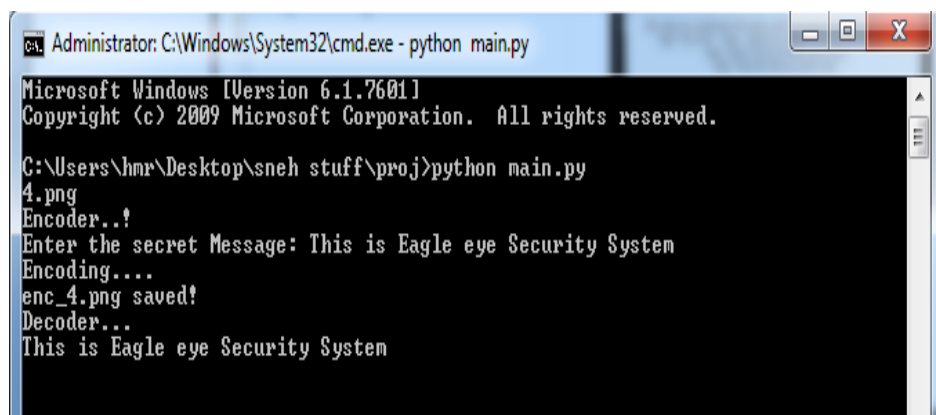


**Figure AI.7: Decoding the Information**

8. For Surveillance

For a Recognized faces-
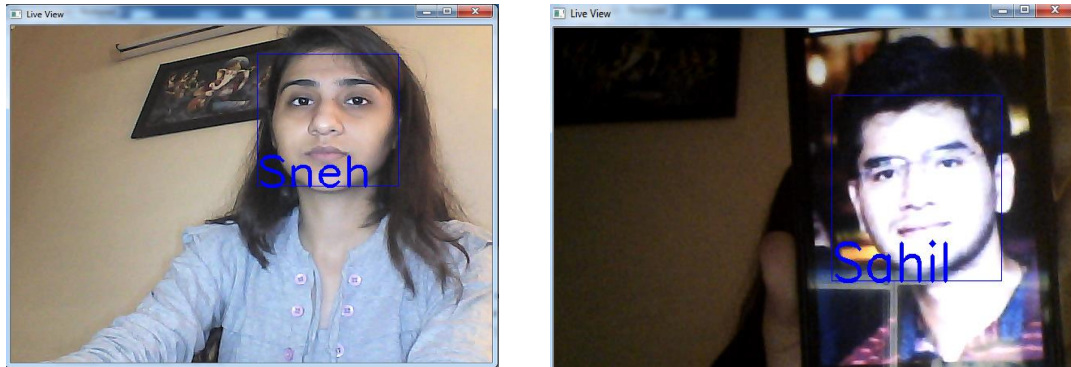


**Figure AI.8.1: Encounter with Trusted Party**

For Unrecognized faces-



**Figure AI.8.2: Encounter with Untrusted Party**

When the Unrecognized human is encountered, the alert module is activated and SMS, Emails are sent to the owner.
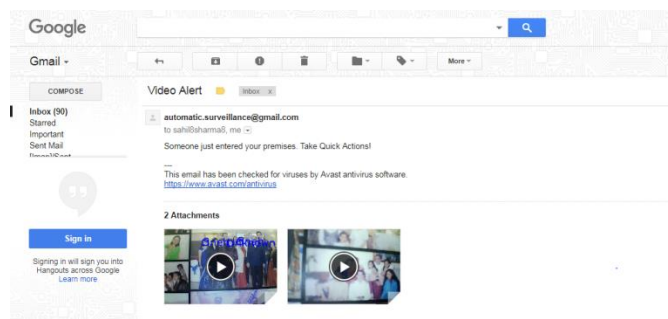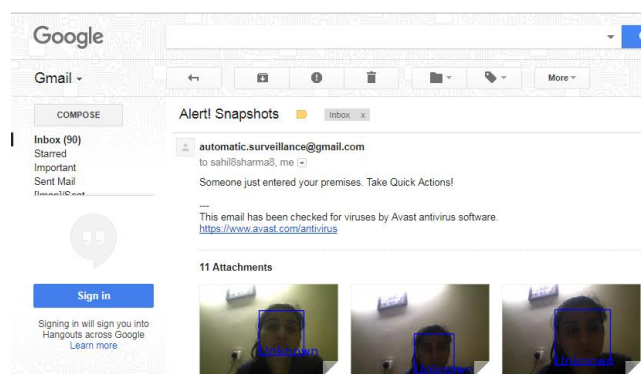
9. Received Alerts-

I.    I. SMS
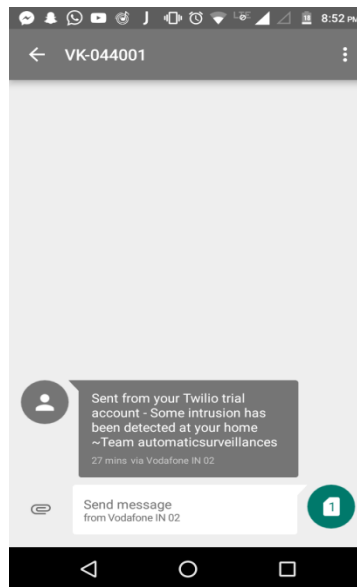
**Figure AI.9.1: Screenshot of SMS received**
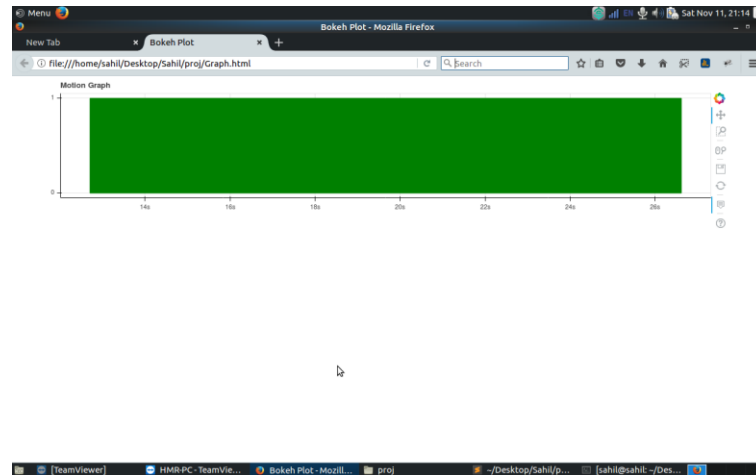
II. E-mail

From Video Alert Mail



From Snapshot Alert Mail



**Figure AI.9.2: Screenshot of E-mails received**

III. Graph



**Figure AI.9.3: Screenshot of Graph generated**

# REFERENCES

[1] Al Sweigart, "Automate the boring Stuff" (2015)

https://automatetheboringstuff.com

[2] OpenCV in Python for Image Processing

http://opencv-python- tutroals.readthedocs.io

[3] Image Steganography techniques and Implementation

https://link.springer.com

[4] GUI development in python using Tkinter

http://python-textbok.readthedocs.io

[5] Python for image processing

https://docs.python.org/2/tutorial/

[6] Libraries and Packages of Python

https://en.wikipedia.org/wiki/Python

[7] OpenCV Face Detection and Recognition

http://opencv-python-tutroals.readthedocs.io/

[8] Information Security using digital image steganography

https://semanticscholar.org/

[9] Digital Image processing tutorial

https://www.tutorialspoint.com/

[10] Building Haar Cascades for coding

https://docs.opencv.org