*Detection of Fraudulent using Public Surveillance Camera*

|  |  |  |  |
| --- | --- | --- | --- |
| Dr.Shanta Kumar B Patil1 | Sriraksha.K2 | Namrata Hejib3 | Vishnu Padi4 |
| *Professor & Head* | *8th semester,UG Student* | *8th semester, UG Student* | *8th semester, UG Student* |
| *Dept of Computer Science & Engg.* | *Dept of Computer Science & Engg.* | *Dept of Computer Science & Engg.* | *Dept of Computer Science & Engg.* |
| *Sai Vidya Institute of Technology* | *Sai Vidya Institute of Technology* | *Sai Vidya Institute of Technology* | *Sai Vidya Institute of Technology* |
| Bengaluru,India | Bengaluru,India | Bengaluru,India | Bengaluru,India |
| [hodcse@saividya.ac.in](mailto:hodcse@saividya.ac.in) | [srirakshak.18cs@saividya.ac.in](mailto:arpithap.18cs@saividya.ac.in) | [namrata.19cs@saividya.ac.in](mailto:keerthisrikari.18cs@saividya.ac.in) | [vishnupadi.17cs@saividya.ac.in](mailto:vishnupadi.17cs@saividya.ac.in) |

# Abstract—The use of autonomous surveillance systems and closed circuit television is increasing as the cost of imaging technology continues to fall (CCTV). Automatic video recording is used in banks, ATM machines, schools, hospitals, and public transportation walkways. The system appears to be relegated to a simple deterrence function because there appears to be little human inspection (in real- time or otherwise) of these surveillance videos (mainly for deterrence of possible felonies). However, understanding the contents of the video is required in many situations for future event detection, storage, and retrieval. Extraction of the desired events necessitates a high level of human semantic understanding as well as a significant quantity of human processing.

**"The exploitation of one's employment for private enrichment through the willful misuse or application of others' goods," according to the ACFE. With the advancement of modern technology and global communication, fraud is on the rise, resulting in significant societal losses. As a result, fraud detection has become a critical topic to consider. Fraud detection refers to detecting fraud as soon as possible after it has occurred. The ability to detect the early indicators of fraud is contingent on the deployment of approved systems and processes..**

**To resolve the problem, A high-quality recording could allow investigators to observe an entire incident develop in full, revealing details such as the order of events, the methods utilised, and the offender's access and leave routes. Even if this isn't possible, CCTV may be valuable in correlating or disputing other types of evidence, such as eyewitness testimony (College of Policing 2014). Investigators may be able to use information from recordings to contextualise other evidence.**

***Keywords— Data Analysis, Tkinter, Image Processing,***

I. INTRODUCTION

Today Due to a lack of evidence and miscommunication within the team, the majority of the cases remain unresolved. The most significant component in getting cases settled is case cracking time. According to a poll, 80 percent of cases are suspended because the time restriction has been exceeded.

Users do not have access to the network mechanism for lodging a complaint and monitoring their status. The police can use public and vehicle surveillance of criminals to assist them crack cases and arrest criminals.

The use of closed-circuit television (CCTV) for police investigation has grown commonplace. Their employment is commonplace in a wide range of contexts to which the general public has access. We have a tendency to be captured on video while walking down Republic Street, visiting a store or bank, or enjoying a cup of tea. One is compelled to recall one of George Orwell's most well-known novels of the twentieth century, "Nineteen Eighty-Four," in which Eric Arthur Blair is situated in a fantastic totalitarian future where everyone is subjected to round- the-clock police investigation. He uses a variety of bold statements, the most renowned of which is "Big Brother is looking at you." Producers have been enticed to create reality television series with a tribe of people together, isolated from the outside world, but continuously filmed on camera for the delight of televiewers.

There has been debate in the academic literature about how CCTV fits into broader surveillance conceptions (Hier 2004; Koskela 2003) and the extent to which it increases or affects the nature of governmental or corporate authority over citizens (Fyfe and Bannister 1996; Norris and Armstrong 1998). CCTV surveillance has sparked concerns that technology may limit the diversity and vitality of life in public locations (Bannister et al. 1998), or contribute to the exclusion of some groups in society (Reeve 1998). There has also been political discussion about how to strike the right balance between preserving the effectiveness of CCTV and protecting citizens' privacy (Sheldon 2011).

Although there has been a lengthy and wide-ranging debate regarding CCTV, scientific evidence on the subject has yet to cover all of its features. This essay will seek to provide evidence to educate one aspect of this argument where evidence is currently limited: the value of CCTV in criminal investigations. A review of the available literature follows, followed by an explanation of the mechanisms that may influence the efficiency of surveillance cameras in investigations. The data for this study was gathered from police reports of offences on the British railway network, as described in the next section. The findings section will detail how frequently and in what circumstances CCTV has proved useful in criminal investigations. Finally, the implications of these results for policy makers and practitioners will be discussed.

II LITERATURE SURVEY

In [1] Surveyed fraud detection techniques used in credit card, telecommunication, and computer intrusion. The goal of research was to provide a comprehensive review of different techniques to detect frauds. It involves the characteristics of fraud types, the need of fraud detection systems and several current fraud detection techniques. Due to the security issues, only a few approaches for credit card detection are available in public. Among them, neural networks approach is a very popular tool but difficult to implement because of lack of available data set. For intrusion detection, some techniques have been applied to the real application. However, it is complicated to test existing intrusion detection systems, simulate potential attack scenarios, and duplicate known attacks

Moreover, intrusion detection system has poor portability because the system and its rule set must be specific to the environment being monitored. Most telecommunication fraud detection techniques explore data set of toll tickets and detect fraud from call patterns. These systems were effective against several kinds of frauds, but still had some main problems.

In [2] Studied an advanced detection system which activated emergency alert system to prevent the actual incidence, after computerized evaluation of danger associated behavior captured in CCTV images. The detection of potential danger involved the ability to discern several steps that might ultimately lead to lifethreatening event of an object. The system was designed with preset danger-zone within the zone of interest and analysis of blob composition, based on the assumption that probability of life-threatening event was directly correlated with the proportion of one overlapping with the danger zone. Subsequently, the danger level was evaluated accordingly to the range of encroachment into the danger zone of the targeted objects. To achieve this purpose an advanced detection system was proposed to alert the integrated control center regarding any potentially dangerous behavior of individuals among some pedestrians from CCTV-based images. As mentioned previously, it might not always be the case that the dangerous events involve one person, but many individuals resulted analysis of object composition. Also, this study closely measured danger levels using encroachment rates of the danger zone divided into three categories; safe, warning, and emergent.

III PROPOSED SYSTEM

The proposed system consists of software components. It consists software GUI application.

1. In order to solve the issue It represents the proposes design of prototype for fraud detection using segmentation method and fuzzy logic.
2. A prototype is developed to recognize suspicion activities captured in CCTV footage and depict the same in natural language. This prototype describes objects, object metaphors and object behaviors on the basis of human insight.
3. This project use python and machine learning algorithm, image processing module to detect the criminal from database.A centralised database managed by each police station to file the cases and track it.
4. The users and Police has to register with the correct phone numbers ,which will really helpful while solving the cases.

In addition to all the features of existing system, our proposed system is different from other existing system as it includes the following features:

1. Here the police can check the status of the criminal (i.e whether the criminal found in any of the places or not)using the database and it will scan the database where the videos are present .If the criminal is found ,a notification is sent to the registered number.Even if the criminal moved to any other states the police can easily find him using this proposed idea
2. The existing system does not provide access to any other police of different states, but this project will allow the nearest police station when the criminal moved to different states.

IV METHODOLOGY

Python Application Development: Front- end framework :

1. Using Tkinter toolkit and Spyder(Anaconda)
2. By using Tkinter toolkit and SMTP package we can send the SMS to the login people.
3. Using ImageTk package we can upload imagesThe working principle of the proposed system is quite easy.

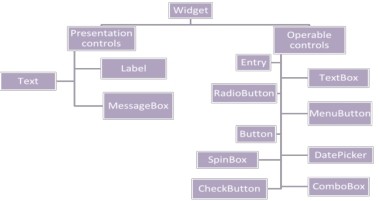


Figure 1 : Framework of Tkinter

Backend Technologies :

Using Firebase:

A . U s e r n a m e a n d P a s s w o r d Authentication

* 1. Person Sign up
  2. Store data into real-time database
  3. Access the data from real-time database
  4. Store image into real-time database

Machine Learning

A.Linear regression model for crime prediction B.Decision tree classifier for crime prediction

1. Brute force matching algorithm for face detection and

comparison

1. Matplotlib used for plotting the multiple graph such as linear , bargraph
2. Application uses local server to store authenticated data, image captured data.
3. Application refer kaggle data set and Indian crime

portal data set to extract the real time large database

The following steps are followed for the proposed system :

**Step 1**: The user must signup ,there will be different signup for normal people and police person.

**Step 2**: If people login , we can file the complaint and see the status of their complaint

**Step 3**: User must upload the picture of the criminal.

**Step 4**: Once people submit their complaint, their respective police station person can see the complaint.

**Step 5**: The police person checks through the real database obtained from the public cctv.

**Step 6**: If the criminal capture in any of the public cctv , then immediately the police receives the SMS of the location of the criminal.

**Step 7:** And we have other module like analyses of crime, where we can analyse based on the respective states,different crimes.

**Step 8**: We will get a graph summary of respective crimes of particular state and next 3 years prediction through bargraph.

V. RESULTS AND ANALYSIS

# Signup Page

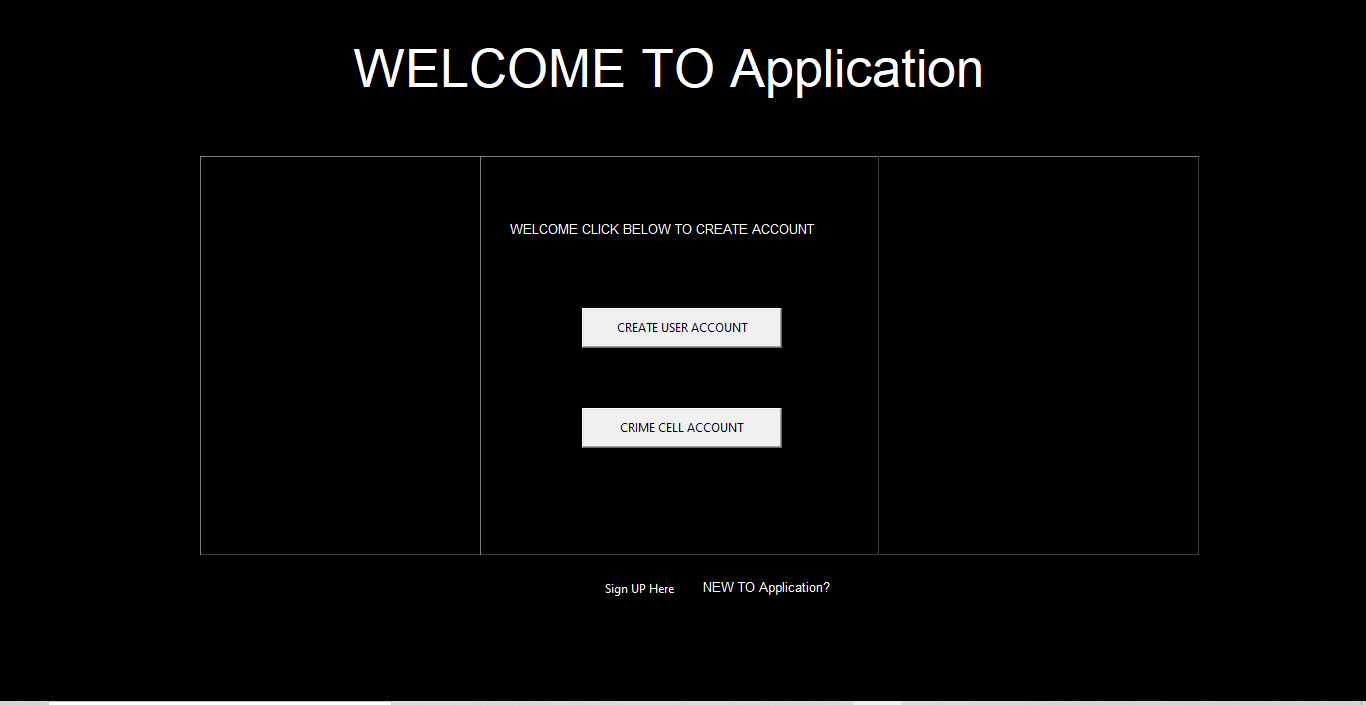


Fig 1

User ans Policeman can signup , if they are new user by giving some basic information.

# Registration Page

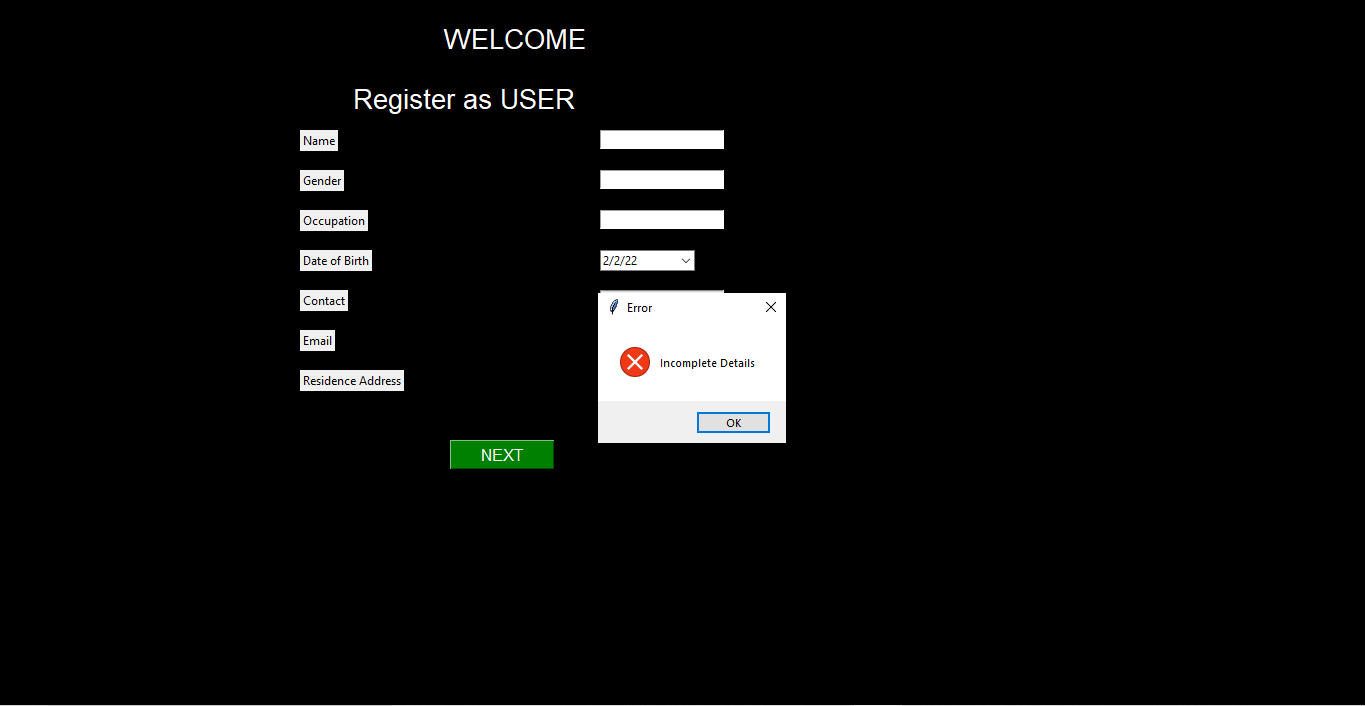


FIG 2

User must give basic information to registration.

# Front Page

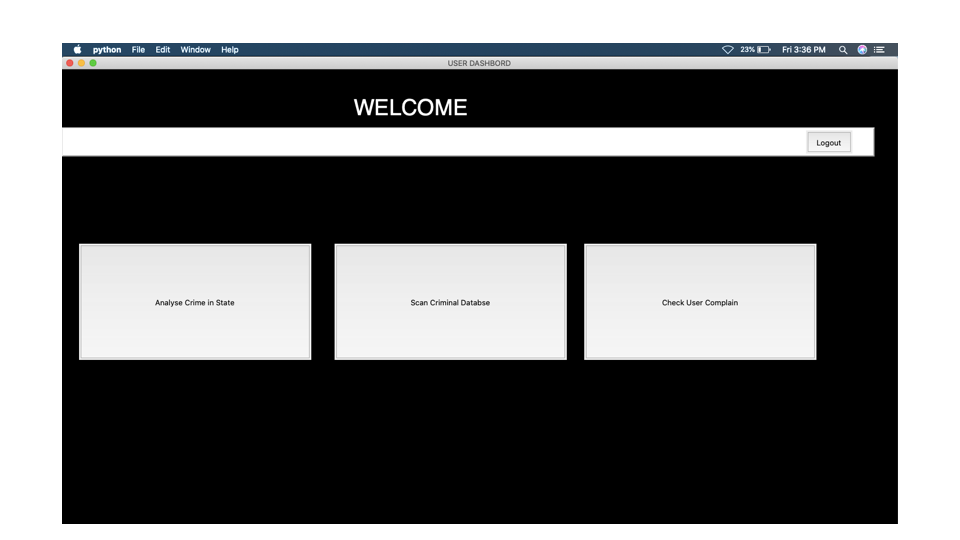
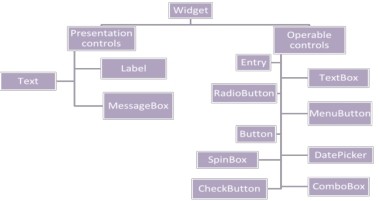


Fig 3

**VI CONCLUSION**

The proposed solution provides an easy, transparent, trustworthy and comfortable way for police to analyse the cases and investigate it. With the technology we have today, it is easy to reach out to communicate with the police station or the cyber cell to transfer and access the evidence as per requirement.

We mainly focus on increases in the cases cracks with proper evidence and easy investigation.

VII REFERENCES

1. Yufeng Kou, Chang-Tien Lu, Sirirat Sinvongwattana,
2. Yo-Ping Huang “Survey of Fraud Detection Techniques”, International Conference on Networking, Sensing & Control, March 21-23, 2004. [2]
3. Syed Ahsan Shabbir, Kannadasan R, “An Effective Fraud Detection System Using Mining Technique”, International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250- 3153. [3]
4. Young-Bin Shim, Hwa-Jin Park and Yong-Ik Yoon, “A Study on Surveillance System of Object‟s Abnormal Behavior by Blob Composition Analysis”, International Journal of Security and Its Applications, Vol.8,No.2 (2014), pp.333-340. [4]
5. Y. Ramadevi, T.Sridevi, B.Poornima, B.Kalyani, “Segmentation And Object Recognition Using Edge Detection Techniques”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010. [5]
6. Dong ping Tian, “A Review on Image Feature Extraction and

Representation Techniques”, International Journal of Multimedia and Ubiquitous Engineering Vol. 8, No. 4, July, 2013. [6] [http://](http://en.wikipedia.org/wiki/CCTV-A-Basic-Overview-of-Video-Surveillance-System) [en.wikipedia.org/wiki/CCTV-A-Basic-Overview-of-Video-](http://en.wikipedia.org/wiki/CCTV-A-Basic-Overview-of-Video-Surveillance-System) Surveillance-System.

1. [7] <http://www.fraudadvisorypanel.org/pdf_show>.