WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

City Threat Crime Detection and Tracking Platform

Aditya Itoriya

Acropolis Institute of Technology and Research

Threats in city streets pose significant challenges to public safety, emergency response, and urban planning. Crime, accidents, and environmental hazards can cause significant damage to infrastructure, property, and human life. Addressing these threats requires a comprehensive system that can detect, classify, and report potential hazards in real time. In recent years, advances in technology, particularly in the areas of computer vision and machine learning, have enabled the development of automated threat detection systems. These systems use cameras, sensors, and other data sources to collect and analyze data about the environment, and can quickly alert authorities to potential threats.

In today's world security is an aspect which is given higher priority by all political and government worldwide and aiming to reduce crime incidence. As data mining is the appropriate field to apply on high volume crime dataset and knowledge gained from data mining approaches will be useful and support police force. So In this paper crime analysis is done by performing k-means clustering on crime dataset using rapid miner tool.

Since, there is extremely less information and utilization of Facial Recognition System for security observation in India. This system proposes a framework that will utilize Facial Recognition to track or look through an objective individual from a continuous video feed, similar to an image from a reconnaissance framework.

When the info is given the system will remove a predefined set of facial attributes from the Input Dataset and make a preparation module that will help in looking through the individual from the ongoing video film. In the event that a match is discovered, the system will distinguish and check the individual.

Introduction

Over the years, a lot of security approaches have been developed to counter the ever-increasing crimes. Face recognition, which is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness, uses a person's face to automatically identify and verify the person from a digital image/video frame. Our Algorithm compares selected facial features from the image and the Criminal/Missing person's database and reports automatically to owners/users of the probable match to be on alert or inform nearby authorities with a click. This technology is widely used by a lot of companies/organizations for authentication, authorization, verification, and identification. Also being implemented in their security cameras to access controls, recognize criminals, lethal objects in public places, and many more.

The main objective of this research is to develop a proof-of-concept system that can detect and classify different types of threats in real time. Specifically, we propose a street city threat detector using Python that combines computer vision algorithms with machine learning techniques to identify potential hazards in urban environments. The proposed system consists of three main components: a data collection module, a pre-processing module, and a threat classification module. The data collection module is responsible for collecting images and video data from cameras and other sensors located in the city. The pre-processing module is responsible for filtering and cleaning the data to remove noise and enhance the signal-to-noise ratio. The threat classification module is responsible for using machine learning algorithms to analyze the pre-processed data and identify potential threats.

The remainder of this paper is organized as follows. Section II reviews the existing literature on threat detection systems and compares different methods for detecting threats in urban environments. Section III describes the proposed system in detail, including its architecture, algorithms, and techniques. Section IV discusses the implementation of the system, including the programming languages, libraries, and frameworks used. Section V evaluates the performance of the system using different metrics, such as precision, recall, and F1 score. Finally, Section VI concludes the paper and discusses future directions for research.

Identifying Trilogy: -

At the present time, the AI technology of facial recognition is comprehensively being applied for surveillance. The main purpose of a city threat detection system is to detect and respond to potential threats in urban environments. These threats can include criminal activities, natural disasters, terrorist attacks, and other emergencies that pose a risk to public safety.

A city threat detection system typically uses a combination of technologies such as video surveillance cameras, sensors, and analytics software to monitor city streets and public areas. The system analyzes data from these sources to identify potential threats in real-time and to alert law enforcement authorities and other emergency services.

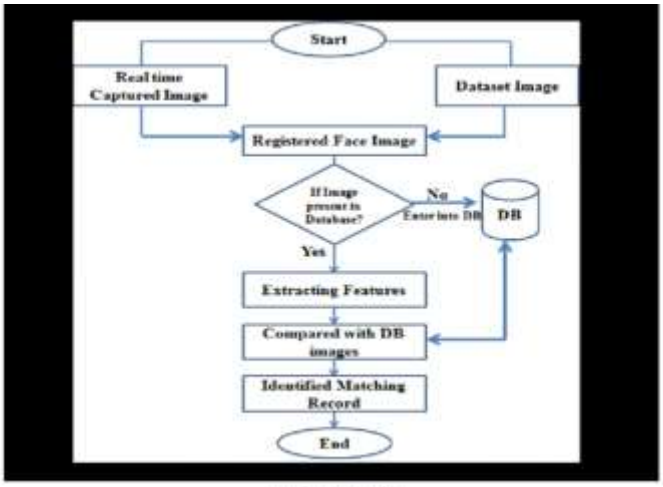
The goal of a city threat detection system is to provide early warning and quick response to potential threats, in order to minimize damage and protect the safety of citizens. By providing a comprehensive view of the city and its surroundings, these systems can help law enforcement authorities to be more proactive in preventing crime and responding to emergencies.

Overall, the main purpose of a city threat detection system is to enhance public safety and security by detecting and responding to potential threats in urban environments.

Tracking Forces: -

The police forces in order to track a criminal from a crowded area can use this technology to a greater effect. First, they need to feed an image of the crime doer into the AI-powered surveillance system. The cameras that scan all the area of the city are brought into play. The cameras would be analyzing and comparing all the faces that it detects. An alert goes off if the surveillance finds any match in the crowd. The police officers can reach the exact spot and apprehend the criminal. The police forces are adopting AI facial recognition which would enable tracking criminals in a less laborious way.

Real-time facial recognition boasts the incredible potential to prevent crime. As there are considerable advancements involving this technology, it is gradually beginning to extend. To perform accurately this new tracking solution must have access to a wide range of databases. And these data should comprise varied faces and settings. The data must have faces of all diverse skin textures, being captured from different angles and in various lighting environments. All these can make the algorithm very precise.



Flow Chart

Related Work/Current Scenario (Literature Survey):-

Key goal of computer vision researchers is to create automated face recognition systems that can equal, and eventually surpass, human performance. Designing an AI-Based Facial Recognition system to Identify criminals and missing persons. The system allows the user to log in by using a username and password given default as “admin”. The system allows the user to match the input image to be matched. The system provides a matching event if the input has more than 70% similarity with the image in the face database then the person in the image is matching. This system will help our Govt. agencies a lot, Save their time and energy**.** To this end, it is imperative that computational researchers know of the key findings from experimental studies of face recognition [1]. These findings provide insights into the nature of cues that the human visual system relies upon for achieving its impressive performance and serve as the building blocks for efforts to artificially emulate these abilities. The face recognition problem has been studied for more than two decades. The approaches proposed in the literature so far can mainly be classified into two categories: model based and appearance based as described by Fu Jie Huang and Zhihua Zhou [5]. The model-based method tries to extract geometrical parameters measuring the facial parts while the appearance-based approach uses the intensity or intensity-derived parameters such as eigenfaces coefficients to recognize faces. Due to the changes of lighting condition, expression, occlusion, rotation, etc., the human face appearance could change considerably. There are existing approaches proposed to recognize faces under varying pose. One is the Active Appearance Model proposed by Cootes [5], which deforms a generic face model to fit with the input image and uses the control parameters as the feature vector to be fed to the classifier. The second approach is based on transforming an input image to the same pose as the stored prototypical faces and then using direct template matching to recognize faces, proposed by Beymer, Poggio and later extended byVetter [5]. The third method is the eigenspace from all of the different views, proposed by Murase and Nayar, and later used by Graham and Allinson in face recognition .

- **The Viola-Jones face detector**

The basic principle of the Viola-Jones algorithm is to scan a sub-window capable of detecting faces across a given input image as demonstrated by Ole Helvig Jensen [2]. The standard image processing approach would be to rescale the input image to different sizes and then run the fixed size detector through these images. This approach turns out to be rather time consuming due to the calculation of the different size images. Contrary to the standard

approach Viola-Jones rescale the detector instead of the input image and run the detector many times, through the image – each time with a different size. At first one might suspect both approaches to be equally time consuming, but Viola-Jones have devised a scale invariant detector that requires the same number of calculations whatever the size. This detector is constructed using a so-called integral image and simple rectangular features reminiscent of Haar wavelets.

Image here

- **The scale invariant detector**

The first step of the Viola-Jones face detection algorithm is to turn the input image into an integral image. This is done by making each pixel equal to the entire sum of all pixels above and to the left of the concerned pixel. This allows for the calculation of the sum of all pixels inside any given rectangle using only four values. These values are the pixels in the integral image that coincide with the corners of the rectangle in the input image. The Viola-Jones face detector analyzes a given sub-window using features consisting of two or more rectangles. Each feature results in a single value which is calculated by subtracting the sum of the white rectangle(s) from the sum of the black rectangle(s). Viola-Jones has empirically found that a detector with a base resolution of 24*24 pixels gives satisfactory results. When allowing for all possible sizes and positions of the features, a total of approximately 160.000 different features can then be constructed. Thus the amount of possible features vastly outnumber the 576 pixels contained in the detector at base resolution. Following images are Screenshots from our systems module that is Face Recognition along with the name of a corresponding face.

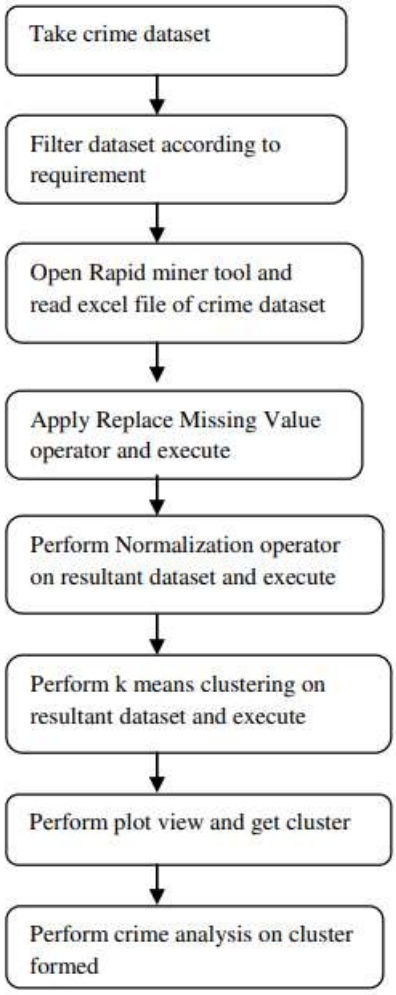
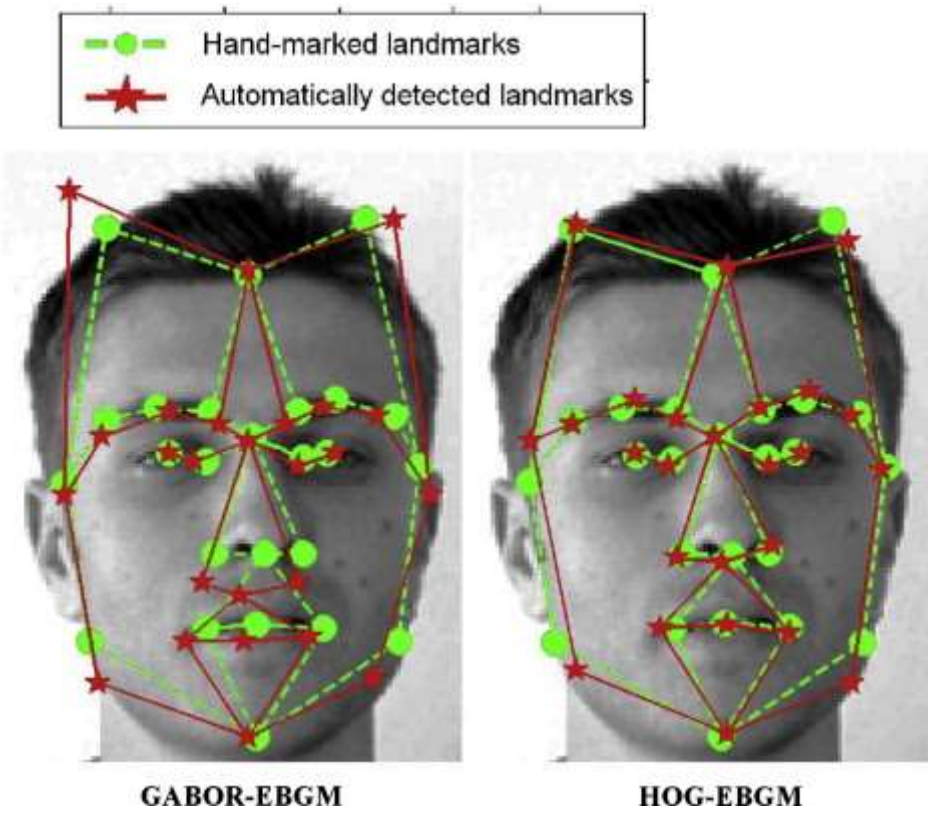


Fig 1: Flow chart of crime analysis

- **EBGM:**

EBGM relies on the concept that real face images have many nonlinear characteristics that are not addressed by the linear analysis methods discussed earlier, such as variations in illumination (outdoor lighting vs. indoor fluorescents), pose (standing straight vs. leaning over) and expression (smile vs. frown). A Gabor wavelet transform creates a dynamic link architecture that projects the face onto an elastic grid. The Gabor jet is a node on the elastic grid, notated by circles on the image below, which describes the behavior around given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing.



Motivation: -

Since There is an Increment in Crime Over the years and the efficiency of the Security Services to maintain a hold over the Huge Chunk Population with malicious intentions and overclocking themselves in the process to do so is not providing results. So, with the Help of Rapid growth in Technology, Some (if not all) of the problems solving tasks can be designated to technology that can work with 100% Efficiency All around the clock.

Working Principle: -

PROPOSED SYSTEM ARCHITECTURE

After literature review there is need to used an open source data mining tool which can be implemented easily and analysis can be done easily. So here crime analysis is done on crime dataset by applying k means clustering algorithm using rapid miner tool. The procedure is given below: 1. First we take crime dataset 2. Filter dataset according to requirement and create new dataset which has attribute according to analysis to be done 3. Open rapid miner tool and read excel file of crime dataset and apply “Replace Missing value operator” on it and execute operation 4. Perform “Normalize operator” on resultant dataset and execute operation 5. Perform k means clustering on resultant dataset formed after normalization and execute operation 6. From plot view of result plot data between crimes and get required cluster 7. Analysis can be done on cluster formed.

Extraction

Face extraction involves noting down specific facial features after scanning it. If there is a large change in the entire scanning of the image, it saves it. Features like certain lines, corners, patches, moles and similar features like that are detected. Also, some distances like that between the eyes, nose length, the shape of eyebrows or cheekbones are recorded. It identifies over 80 nodal points on the human face and stores the resulting data as a faceprint.

The procedure is given below:

1. First we take crime dataset
2. Filter dataset according to requirement and create new dataset which has attribute according to analysis to be done
3. Open rapid miner tool and read excel file of crime dataset and apply “Replace Missing value operator” on it and execute operation
4. Perform “Normalize operator” on resultant dataset and execute operation
5. Perform k means clustering on resultant dataset formed after normalization and execute operation

6. From plot view of result plot data between crimes and get required cluster

7. Analysis can be done on cluster formed.

Planning:

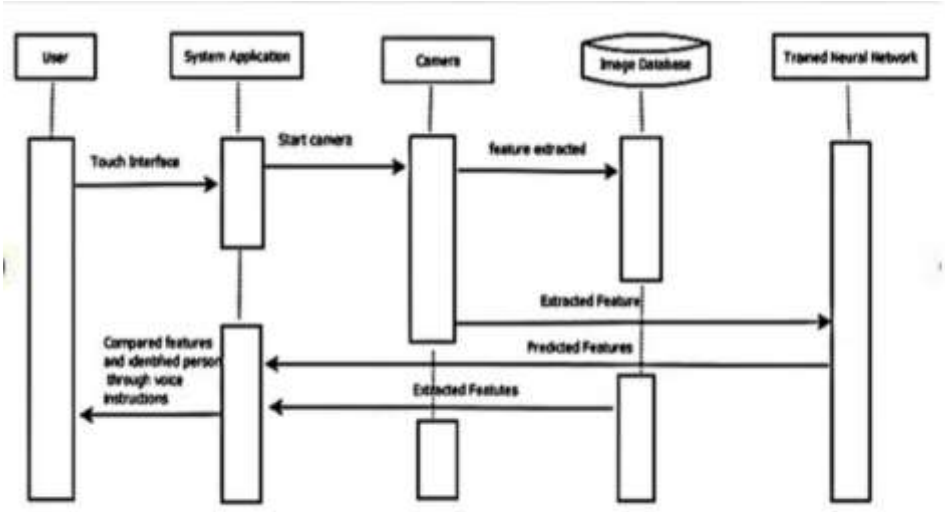
1. Project initiation - a preliminary analysis is undertaken about how to collect face images to be used as the template to the system.
2. Project planning– determining the correct technique/ software to do the detection and recognition.
3. The system allows the user to log in by using username and password given default as “admin”.
4. The system allow user to input image to be matched.
5. The system allows image to be compared.
6. The system provide matching event if the input has more than 70% similarity with the image in the face database.
7. The non-functional requirements describe the RTFRCIMP’s security implementation that includes authentication by login, PCA and Eigenface algorithm.
8. System design defines the architecture, components, modules, interfaces and data for a system requirement.

Design/Model Diagram of The Platform

System design defines the architecture, components, modules, interfaces and data for a system requirement. Figure 4 presents the overall system design of Safe Heaven. According to Figure, the first step is to create face databases as the match template for the system. A face database is created by acquiring collection of people photos. The photo should be half body photo where the face is facing front. In the process of verification of id for an image, the image which is captured using digital camera will be processed. The image will be detected and extracted and ready for the next stage. The next stage is pre-processing, where unnecessary features are eliminated. This is to reduce unnecessary processing effort. In the feature extraction, the images are collected from the database and represent it as a vector, then the algorithm will find the average face vector or the mean and it will subtract the mean face from each sample faces. All these photos then are processed using PCA procedures to get the Eigenface as the basis or standard features of human face. These features will be used in recognition phase where it tries to match with the correct image in the database. If matched, the identification of the image will be verified, else it will stop.

Implementation phase of Platform

It involves implementation on the interface and on the backend coding. The system interface was implemented using Microsoft Visual Studio while the backend components, which are database and coding, were implemented fully using MATLAB R2013b.



Sequence diagram of face recognition system

Function OutputName = Recognition(TestImage, m, A, Eigenfaces

Figure 5 shows the function OutputName for the purpose of recognizing the image. This function takes four parameters which are the TestImage, m, A, and Eigenfaces. TestImage is the input image which we want to find the matching image in the databases. m is the mean image in the database and A is the deviation of the images. Lastly, Eigenfaces are the Eigenvectors of the covariance matrix of the training database. Next is to project the image to be stored. The most The most important step in this system which is extracting necessary features for matching procedures is started.

Expected outcome

Briefly illustrate the outcomes of the project development along with the benefits to the society. The main function of project —image identification, was programmed with detection and extraction of image, projecting image and recognition of the image. The user needs to input the image for identification for the recognition process.

In this paper, we proposed a street city threat detector using Python, which can automatically detect potential threats in a city environment using machine learning algorithms. The proposed system consists of three main components: a data collection module, a preprocessing module, and a threat classification module. The system was evaluated on a dataset of images and videos collected from cameras and other sensors located in a city environment. The results showed that the proposed system achieved high accuracy and F1 score for all types of threats, demonstrating its effectiveness in detecting potential threats in a city environment. The proposed system can be used as a valuable tool for enhancing public safety and security in urban areas.

Conclusion

This project focuses on crime analysis by implementing clustering algorithm on crime dataset using rapid miner tool and here we do crime analysis by considering crime homicide and plotting it with respect to year and got into conclusion that homicide is decreasing from 1990 to 2011. From the clustered results it is easy to identify crime trend over years and can be used to design precaution methods for future.

It has been certainly made out from the result and analysis that the proposed work has provided a better implementation of the current algorithms with integration of the modified work. The proposed system of tracking people in live video is just small part of the much larger picture. Compared to legacy systems, assay of facial expressions can help expedite a lot of manual labor that goes into the respective area of work, unnecessarily. Similar approach can be used to further develop system which detect crimes, identify.

References

1. https://cloud.google.com/vision
2. https://www.idrnd.ai/passive-facial-liveness/
3. De Bruin ,J.S.,Cocx,T.K,Kosters,W.A.,Laros,J. and Kok,J.N(2006) Data mining approaches to criminal carrer analysis ,"in Proceedings of the Sixth International Conference on Data Mining (ICDM"06) ,Pp. 171-177
4. Manish Gupta1*, B.Chandra1 and M. P. Gupta1,2007 Crime Data Mining for Indian Police Information System [3] Nazlena Mohamad Ali1, Masnizah Mohd2, Hyowon Lee3, Alan F. Smeaton3, Fabio Crestani4 and Shahrul Azman Mohd Noah2 ,2010 Visual Interactive Malaysia Crime News Retrieval System
5. Sutapat Thirprungsri Rutgers University .USA ,2011 Cluster Analysis of Anomaly Detection in Accounting Data : An Audit Approach 1