Machine Learning Is Used to Forecast Crimes and Identify Individuals.

PROF. M. E. SANAP[1], SARUPTA BHONDAVE[2], NIKITA CHAVAN[3], VAISHNAVI DHAGALE[4], ANISHA GAIKWAD[5]
[1, 2, 3, 4, 5] *Computer Engineering, SAE, Kondhwa*

***Abstract*— Crimes are an irritant to society and have a discernible effect on it. Many law enforcement organizations currently have large amounts of crime-related data that need to be processed in order to become useful information. Crime data are complex since they include a lot of various formats and features. Law enforcement organizations face a number of challenges in their efforts to prevent crimes. To assist law enforcement agencies in conducting descriptive, predictive, and prescriptive analysis on crime data, we propose a desktop application for crime data analysis. Because the application was modular, each component was built separately. Person identification makes use of data analysis and biometric technologies to accurately identify individuals. Databases are able to record and store these characteristics.**

***Index Terms*— Crime, Haar-cascade algorithm, Prediction, Person-Identification, SVM**

I. INTRODUCTION

The problem of criminal activity has grown to be rather serious and is believed to be becoming worse rather quickly. The process of developing predictive models that use past crime data to determine the likelihood that different kinds of crimes will occur in specific places and at specific times is known as crime prediction. Law enforcement agencies can identify high-risk areas, deploy resources there, and proactively halt criminal activity by using these models.

Accurately identifying people requires the application of data analysis and biometric technologies. Physical traits like face patterns are examples of biometrics. Law enforcement can compare these traits to existing records for criminal investigations by capturing and storing them in databases.

Crimes are a social nuisance and it has a direct effect on a society. Governments spend lots of money through law enforcement agencies to try and stop crimes from taking place. Today, many law enforcement bodies have large volumes of data related to crimes, which need to be processed to turn into useful information. The crime rates accelerate continuously and the crime patterns are constantly changing. As a result, the behaviors in crime pattern are difficult to explain. This paper illustrates how social development may lead to crime prevention. The aim is to provide a comprehensive review of theory and research with respect to the prevention of the crime in the society and to implement different data analysis algorithms which address the connections between crime and its pattern. The data for the project are collected from the legitimate government sources. The data was converted to .csv format upon which pre-processing of the data was performed. Technologies used for mining various crime pattern and analysis. The goal of the person re-identification is to retrieve the same pedestrian from the cross-camera, which has been widely applied in a great deal of fields, such as video surveillance, intelligent security, smart city and so on. Owing to the rapid development of deep learning, person re-identification has obtained great success by learning discriminative features from labelled person images with deep Convolutional Neural Network (CNN). Nevertheless, the learned features are very easily weakened by the semantic misalignment of the target and background clutters.

The objective of this project is to analyse dataset which consist of numerous crimes and predicting the type of crime which may happen in future depending upon various conditions.

The ability to predict the crime which can occur in future can help the law enforcement agencies in preventing the crime before it occurs. The capability

to predict any crime on the basis of time, location and so on can help in providing useful information to law enforcement from strategical perspective. Enhancing Security: One of the primary objectives of person identification is to enhance security. This could involve verifying the identity of individuals for access control to secure areas, buildings, or systems.Preventing Identity Theft and Fraud

II. LITERATURE REVIEW

Paper 1: Prediction Analysis of Crime in India Using a Hybrid Clustering Approach

Dr.J.Kiran Assistant Professor Department presents a comprehensive paper on One of the most intricate systems that humans have ever created is the cyberspace; although many people use it frequently, most users only have a cursory understanding of its capabilities. Cyber-attacks used to typically be planned in a haphazard manner with the intention of tricking unsuspecting targets. Further evidence has shown that information about cyber-attacks is disseminated among hackers and hacker forums within the virtual ecosystem. This paper suggests identifying texts related to cyber threats by using open-source intelligence from hacker forums on the deep web and the surface web (Twitter).

Paper 2: Crime Prediction Using K-Nearest Neighboring Algorithm

Akash Kumar presents a comprehensive paper on People frequently hear about crimes occurring in developing nations like India. We need to be aware of our surroundings at all times due to the rapid urbanization of cities. We will attempt to track crime rates using the KNN prediction method in an effort to prevent the unfavorable. The type of crime, its potential location, time, and date will all be tentatively predicted. Criminal investigations may benefit from knowing the crime patterns across a
region provided by this data. Additionally, it will give us information on the highest number of crimes committed in that area. We will employ the machine learning algorithm known as the k-nearest neighbor in this paper.

Paper 3: Empirical Analysis for Crime Prediction and Forecasting Using Machine Learning and Deep Learning Techniques

The threat that crime and violations pose to the rule of law is why they should be monitored. Computing can help to improve metropolitan safety by providing accurate crime predictions and future forecasting patterns. Many computational challenge opportunities arise from the precise estimation of the crime rate, types, and hot locations from historical trends. The present investigation employed various machine learning algorithms, including logistic regression, support vector machine (SVM), Naive Bayes, k-nearest neighbors (KNN), decision tree, multilayer perceptron (MLP), random forest, and eXtreme Gradient Boosting (XGBoost), in conjunction with time series analysis using long-short term memory (LSTM) and autoregressive integrated moving average (ARIMA) model, to enhance the fit of the crime data. In terms of the amount of mean absolute error (MAE) and root mean square error (RMSE), the performance of LSTM for time series analysis was passably good.

Paper 4: Smart Visual Surveillance: Proactive Person Re-identification instead of impulsive Person Search.

Detecting and re-identifying people simultaneously on a live CCTV feed is a more proactive way to address surveillance difficulties than applying person search on CCTV video archives after an incident has occurred. Present person re-identification systems rely on off-the-shelf detectors for their practical application and do not address person detection. While person search techniques do, in theory, detect people, they only do so for a pre-defined selection of people (known as the query set) rather than tracking every individual who is there at any one time. In this study, we provide an independent method for concurrently identifying and re-identifying every individual surfacing inside a network of security cameras. To locate people in specific surveillance photos, a deep backbone network combines the Region proposal network and region of interest pooling.

Paper 5: SCA Net: Person Re-Identification with Semantically Consistent Attention

Person re-identification (re-ID) is a recognition mission at the instance level that relies on particular discriminative traits. However, the semantic misalignment of the goal and background clutters

quickly influences and weakens the learned features from the network. Semantically consistent attention network, or SCANet, is a novel deep re-identification CNN that is proposed in this work to learn the discriminative feature. By creating a foreground mask module on a backbone network made up of residual blocks, we accomplish the goal in this study. Crucially, a novel consistent attention loss is implemented to maintain the similarity of the inferred foreground mask from the shallow-, mid--, and deep-level feature maps dynamically.

III. ALGORITHMS

1) Support Vector Machines (SVM):

The support vector machine (SVM) is a powerful machine learning algorithm utilized in both classification and regression tasks. Its main goal is to discover a hyper plane that effectively separates data points, thereby maximizing the margin between different classes. SVM finds practical applications in various domains including text detection, character recognition, object identification, and human activity recognition. Known for its robust theoretical foundations and efficient problem-solving abilities, SVM is renowned for its versatility in tackling complex tasks.[1]

2) Haar Cascade Algorithm:

The Haar Cascade algorithm is a popular method for object detection, not ably used for tasks like face detection. It works by analyzing features in an image using rectangular patterns, trained to distinguish between the object of interest and the background. Employing a cascade of classifiers and AdaBoost, it efficiently identifies objects by sliding a window across the image and applying a series of filters. While effective and efficient, it may struggle with variations in scale and lighting conditions compared to more advanced techniques like deep learning-based approaches.

Haar Cascade is a machine learning-based approach where a lot of positive and negative images are used to train the classifier.

IV. SYSTEM DESIGN

System Architecture for Machine Learning-Based Crime prediction and Person identification :

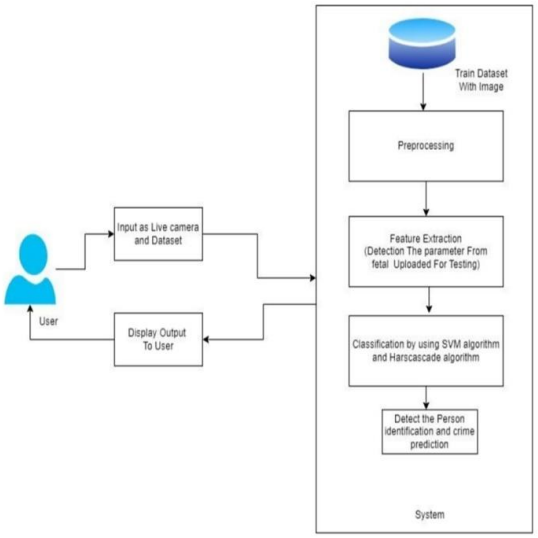

Figure 1: SYSTEM ARCHITECHTURE DIAGRAM

The architecture of a machine learning-based person identification and crime prediction system often includes data collecting from sources such as databases, CCTV, and sensors. After pre-processing, this data is input into crime prediction models, which may use random forests or neural networks as algorithms. Biometric information and facial recognition technology may be used to identify an individual. A feedback loop is necessary for the system's on going learning and development. To preserve data security and privacy, strong encryption and secure database integration are essential.

Feedback Loop:

Feedback Gathering: Information about the results of crime forecasts. This can contain data on actual crime incidences, law enforcement reactions, and prediction accuracy

V. IMPLEMENTATION DETAILS

1) Forecasting The Crime Type-

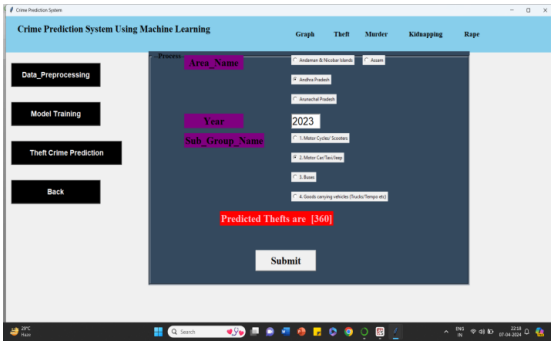

Figure 1: CRIME PREDICTION

Overview:

Crime forecasting using deep learning and machine learning involves leveraging advanced algorithms to predict the types of crimes that are likely to occur in specific locations and time periods. By analyzing historical crime data and relevant contextual information, such as demographics, weather conditions, and socio-economic factors, these techniques aim to provide law enforcement agencies with insights to allocate resources effectively and prevent criminal activities. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can capture complex patterns in large datasets, while traditional machine learning algorithms like decision trees and random forests offer interpretability and scalability. This innovative approach holds the potential to enhance

2)Person-Identification-

Overview:

Person identification using machine learning and deep learning involves developing algorithms that can

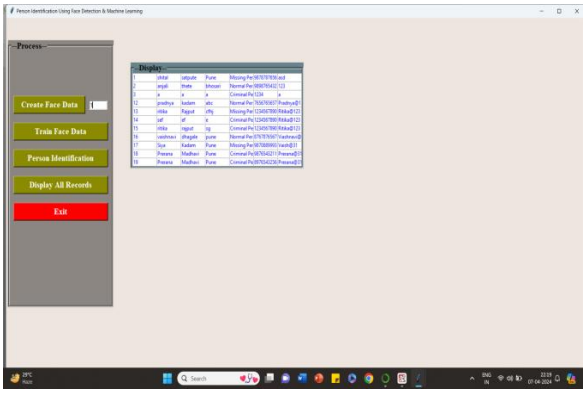

Figure 2: PERSON IDENTIFICATION

accurately recognize and identify individuals from images or videos. By leveraging features extracted from facial or behavioral data, these techniques enable automated identification of people for various applications, including security, surveillance, and access control. Machine learning algorithms like support vector machines (SVMs) and k-nearest neighbors (KNN) can be used for traditional feature-based recognition, while deep learning models such as convolutional neural networks (CNNs) and siamese networks excel at learning representations directly from raw image or video data, allowing for more accurate and robust identification. This technology has wide-ranging implications for law enforcement, retail, healthcare, and other industries where reliable person identification is crucial.

VI. RESULT

Enhanced Public Safety: By predicting crime hotspots and identifying individuals involved in criminal activities, law enforcement agencies can deploy resources more effectively, leading to reduced crime rates and improved public safety. Efficient Resource Allocation: Machine learning algorithms enable law enforcement agencies to allocate resources such as personnel, patrol routes, and surveillance efforts efficiently, focusing on areas and individuals with the highest risk of criminal activity. Timely Response: Real-time crime prediction and person identification systems allow for rapid response to incidents, enabling law enforcement to intervene quickly and prevent crimes from occurring or escalating.

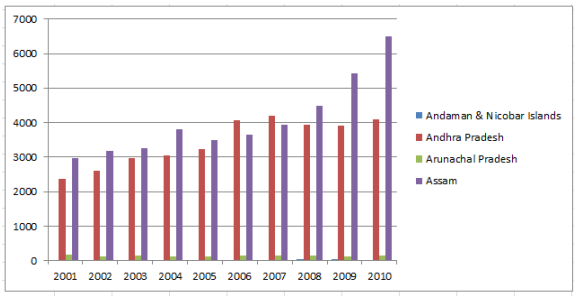

Figure 1: KIDNAPPING

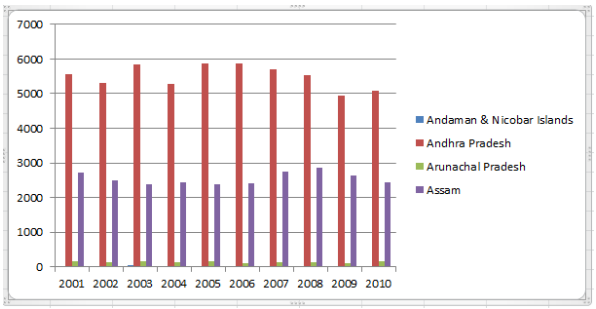

Figure 2: MURDER

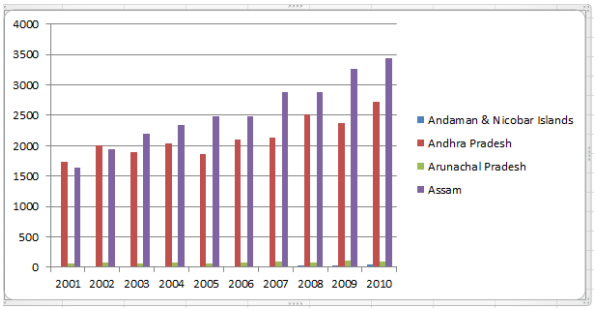

Figure 3: RAPE

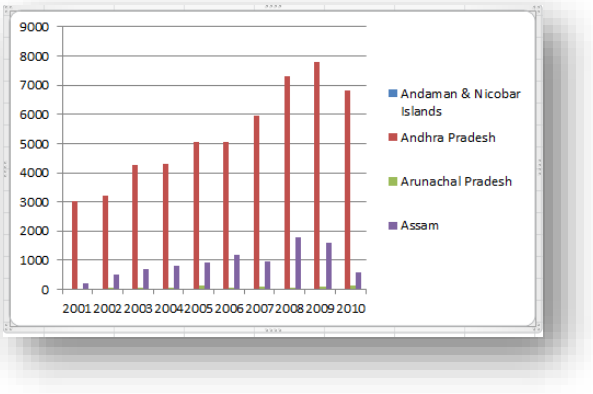

Figure 4: THEFT

DISCUSSION

Generally, the adoption of machine learning algorithms for the prediction and detection of crime has demonstrated substantial promise in addressing the increasingly complex issue. Through the use of advanced algorithms and vast datasets, these technologies can enhance the effectiveness and accuracy of crime prediction models. On the basis of the results, there are a number of valuable insights that have been acquired. First, Random Forests have been considered and used the most by researchers and have been identified to offer quite accurate results. Second, all the studies, except for one study, showed the effectiveness and accuracy of ML algorithms and methods in predicting and forecasting crimes. Third, it is essential to actually perform thorough experiments and tests using the models and approaches discussed by the authors. Many authors have mentioned the need to test their models in the real world before using them. In addition, it might be challenging to use these models in a real situation due to the large amount of data that would be required to be considered and analyzed. Fourth, different models proposed by the authors tend to offer and produce varying results and findings in different situations using different types of datasets.

CONCLUSION

This paper is useful to Crime analysis and prediction is a methodical way of detecting criminal activity. By forecasting places with a high probability of crime occurrence, this system can identify and visualize areas that are prone to crime. Data mining is a notion that allows us to extract previously unknown, meaningful information from unstructured data.

REFERENCES

[1] Prediction Analysis of Crime in India Using a Hybrid Clustering Approach.

[2] Crime Prediction Using K-Nearest Neighboring Algorithm.

[3] 3. Empirical Analysis for Crime Prediction and Forecasting Using Machine Learning and Deep Learning Techniques.

[4] Smart Visual Surveillance: Proactive Person Re-identification instead of Impulsive Person Search.

[5] SCA Net: Person Re-Identification with Semantically Consistent Attention.

[6] Kim, Suhong, Param Joshi, Parminder Singh Kalsi, and Pooya Taheri. ”Crime Analysis Through Machine Learning.” In 2018 IEEE 9th Annual Information Tech nology, Electronics and Mobile Communication Conference (IEMCON), pp. 415 420. IEEE, 2018.

[7] Shah, Riya Rahul. ”Crime Prediction Using Machine Learning.” (2003).

[8] Lin, Ying-Lung, Tenge-Yang Chen, and Liang-Chih Yu. "Using machine learning to assist crime prevention." In 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 1029-1030. IEEE, 2017.

[9] M.V. Barnadas, Machine learning applied to crime prediction, Thesis, Universitat Polit`ecnica de Catalunya, Barcelona, Spain, Sep. 2016.

[10] Crime Prediction Using Machine Learning Sacramento Stateathena.ecs.csus.edu shahr progressreportbyRRShah−2003