International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 06, 2020
ISSN: 1475-7192

EXPLAINABLE AI IN INTRUSION DETECTION SYSTEMS

Nikita Nerkar[1], Atharva Nile[2], Amit Kulkarni[3], Onkar Kadlag[4], Prashant Gadakh[5]

Abstract: As the use of internet in increasing day by day and the chances of system get compromised due to various types of attacks has increased. Intruders are finding new techniques to compromise the system. The concern about the cyber security is growing and for the user most of the model is perceived as a black box. There is need of finding the attack correctly and then proper reports should be generated to show how the system got compromised. So we are proposing a system where Intrusion Detection System (IDS) can detect the attack and Explainable artificial intelligence tell us about what type of attack is being performed on the system. Intrusion Detection System keeps track of the malicious packets entering in the system. Explainable Artificial Intelligence will show the report on which type of attack took place. In the proposed system we have use the NSL-KDD dataset for classification of attack detected by our proposed Intrusion Detection System.

Keywords: Intrusion detection System, Explainable artificial intelligence, NSL-KDD, classification.

I. INTRODUCTION

Today internet is been used in vast number of areas like organizations, businesses, entertainment industry, personal day to day activities etc. One of the most important issues nowadays is security. When an intrusion takes place the security of the system is compromised. The assumption of the behaviour of the intrusion is different from the legal user in the system. To deal with intrusions in the network is the main aim of the IDS.

Explainable Artificial Intelligence presents the results of the solution that can be understood by the system administrators effectively. Our system consists of four classes of the intrusion like User to Root (U2R), Denial of Service (DoS), and Remote to User (R2U), Probing attacks. An IDS alone is only able to detect that attack has taken place and alarms admins but it is not able to detect type of attack. Using Explainable Artificial Intelligence when can detect which type of attack has took place from the four classes and generate the reports for the same. For Classification purpose we have used NSL-KDD dataset for training a model which classifies the attack. Pre-processing over the model is done by using one hot encoding, label encoding and standard scalar techniques.

II. LITERATURE SURVEY

We have referred "Intrusion Detection System Using Data Mining Technique: Support Vector Machine" [4] In which they have Classified the attack done on the system using support vector machine(SVM) method and using the

[1, 2, 3, 4] *Researcher Department of Computer Engineering, International Institute of Information Technology, Hinjewadi, Pune,India.*
[2] *Professor, Department of Computer Engineering, International Institute of Information Technology, Hinjewadi, Pune,India.*

Received: 22 Dec 2019 | Revised: 13 Jan 2020 | Accepted: 05 Feb 2020

International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 4578 - 4583

"AutoML for Model Compression and Acceleration on Mobile Devices using Reinforcement Learning"

Mr. Prashant Gadakh[1], Ansh Jain[2], Ritika Dave[3]
Department of Computer Engineering, International Institute of Information Technology I[2]IT, Pune, Maharashtra, India[1]
Mukesh Patel School of Technology Management and Engineering[2, 3]
Prashantgadakh31@gmail.com[1]
ansh.jain9090@gmail.com[2]
ritikadave.rd@gmail.com[3]

Abstract

Background: *Model compression has been described as a crucial skill which resourcefully implement neutral network model on mobile devices possessing scarce computation assets and also operating under a tight budget. Most of the ancient model compression depend on methods which are handmade and also they operate under a rule-based procedure which only function under a domain expert so as to investigate one of the greatest design location for trading off for all the model size, speed, and the accuracy i.e. a sub-optimal and time consuming.*

Aim*: The major aim of this paper is to explore AutoML proposal for Model Compression which can leverage corroboration learning in a bid to offer the model compression strategy. Comparing the learning dedicated compression strategy with the ancient rule based one, its performance its far better and advanced in that it has a high compression ratio, accuracy and less human labor is required.*

Results: *Working under the 4 x FLOPs reduction, it was able to attain an accuracy level at 2.7 percent than the conventional compressional model. Also, it attained 1.81x speedup for the calculated inference latency on an android phone and a 1.43x speedup for the Titan XP CPU with a greater accuracy than the ancient techniques.*

Keywords: AutoML, Mobile vision, Model compression

1. Introduction

Evidently, if you observe keenly across most of the machine learning devices i.e. self-driving cars, robots, and advertisement ranking, the deep original network for mobile devices are inhibited by either energy, latency, and model size budget. A lot of the approaches which have been tabled out aims to enhance the hardware effectives and efficiency of the neutral networks by the model compression. The major component of the model compression skills aims to ascertain the compression procedure for every layer as they possess various redundancy requiring the one which are man-made heuristics and area expertise so as to be employed to be investigated for the great space exchange off among the speed,

ISSN: 2005-4238 IJAST

Novel Approach for Measuring Nutrition Values Using Smartphone

Sashikala Mishra, Prashant Gadakh, Chinmay Gosavi, Shivam Bhoskar, Shrinit Padwal and Vishal Kasar

Abstract Food is the source of energy, and it plays a vital role in human existence. The quality of food is suffering day by day such as adulteration and heavy use of various pesticides. The traditional approach to analyze food nutritional values involves the use of various sensors and laboratory procedures to detect the quality, but such sensors and methods really take lots of time. There is a need of a system which we can use to quickly evaluate the quality of food by methods which are ubiquitous. The number of handheld devices and their processing capabilities has increased manifolds over the last few years. In this paper, the novel methodology has been proposed which uses the smartphones to take the image, and instantly, it provides the nutrition value. The proposed model helps detect the nutritional quality of the food by utilizing the various sensors which are present in smartphones such as cameras and microphone. The model uses the classifiers to detect the type of food and process all the algorithms in cloud. Four datasets are used with multi-class level. Machine is trained with various algorithms such as CNN and RNN, and we have used transfer learning. The whole system is implemented successfully, and the accuracy of 82% has been achieved.

Keywords Statistics · Data mining · NLP · Object detection · Machine learning · DietCam

1 Introduction

As per the economist in 2016, more than 1.9 billion adults aged 18 years and older were overweight. Of these, over 650 million adults were obese [1]. Similarly, about 13% of the world's adult population (11% of men and 15% of women) were obese in 2016 [2]. Obesity increases the risk of various diseases and health conditions such

S. Mishra · P. Gadakh (✉)
International Institute of Information Technology, Hinjawadi, Pune, India
e-mail: prashantgadakh31@gmail.com

C. Gosavi · S. Bhoskar · S. Padwal · V. Kasar
International Institute of Information Technology, Pune, India

D. Swain et al. (eds.), *Machine Learning and Information Processing*,
Advances in Intelligent Systems and Computing 1101,
https://doi.org/10.1007/978-981-15-1884-3_24

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

A Review Paper on Face Recognition Methodologies

Raghuveer Bohara
Information Technology Department
Interntional Institute of Information Technology, Pune
(SPPU, Pune)

Gourav Joshi
Information Technology Department
Interntional Institute of Information Technology, Pune
(SPPU, Pune)

Ojas Ingale
Information Technology Department
Interntional Institute of Information Technology, Pune
(SPPU, Pune)

Prof. Anand Bhosale
Information Technology Department
Interntional Institute of Information Technology, Pune
(SPPU, Pune)

Hitesh Joshi
Information Technology Department
Interntional Institute of Information Technology, Pune
(SPPU, Pune)

***Abstract*— In the previous few years, the procedures of face recognition have been researched thoroughly. Well-versed reviews, for various human face recognition methodologies, are provided in this paper. Initially, we proffer a summary of face recognition with its application. Followed by a literature review of various face recognition techniques. Several face recognition algorithms are analyzed and elaborated with their limitations as well. It also includes brief overviews regarding various modern approaches like neural networks, line edge mapping, and many others, which are widely used nowadays to make the process of face recognition more efficient. Conclusively, the research results are reviewed and are summarized.**

I. INTRODUCTION

In various fields and disciplines, face recognition is traversing as a modern research problem. Generally, face recognition includes 2 steps, face detection, and face recognition. Face detection means catching or discovering a face in an image. Then it is followed by recognition which includes identifying or recognizing the detected face. To date, various effective approaches have been introduced. In [1], a conventional method for distinguishing faces is used i.e. Eigen faces. To collect different profiles int the form of curves, calculating their norm and differentiating other profiles based on the deviation from the norm, is what proposed by the author. This results in a vector with independent standards, and further, it can be compared with the other vectors. While in [2] the author proposes a more complex but effective approach. This approach is the combination of KFDA and nearest neighbor where one performs feature extraction and the other performs recognition. [4] Proposes the approach called Hidden Markov Model. In this approach, the hardware is also upgraded to achieve better results. The next methodology [6] is one of the most commonly used approaches in machine learning applications. The support vector machine is a simplistic, yet efficient machine learning model which can be used to classify profiles into multiple classes. In the
next approach [9] author proposes the use of neural networks for face recognition. This approach uses various algorithms concurrently to obtain the best possible result.

II. LITERATURE REVIEW

In this section, we elaborate on different face recognition techniques by reviewing some of the works. The methodologies include Eigen faces, KFDA with Nearest Neighbor, Hidden Markov Model, SVM, and Neural Networks. The OCR architecture is broken down in following stages:

1. Eigen Faces

The Eigen face algorithm is the most commonly used approach when it comes to face recognition. In the Eigen face algorithm, the Eigen faces are the eigenvectors. These eigenvectors are derived from the covariance matrix of the dataset. Eigen faces are also sometimes referred to as ghostly images. The main reason for using the Eigen face approach is that it represents the input data efficiently. This is done by representing each face in terms of the linear combination of Eigen faces. To achieve this, a dimension reduction technique is required. Conventionally, the dimension reduction technique, which is used here, is Principal Component Analysis.

The author in this paper [1] is using face recognition to mark the attendance of the students in the class. So the author here [1] starts by elaborating what is Principal Component Analysis. The author states it used to examine face recognition issues by using it as a dimension reduction technique. It is also mentioned that is comprehended as Eigen face projection. The principal component analysis is used to reduce the dimension of the data and accurately decompose the face structure into orthogonal principal components which we know as 'Eigen faces'. In simple words, PCA is used to remove information that is not useful to generate Eigen faces. Moreover, PCA gives a suitable representation for the face space which otherwise forms a cluster.

Furthermore, it is also stated that PCA has major applications in various fields, such as image analysis, identifying anonymous faces, and dimensional data reduction. A comparison of test images, with training images, is done by

ADHYAYAN—An Innovative Interest Finder and Career Guidance Application

Akshay Talke, Virendra Patil, Sanyam Raj, Rohit Kr. Singh, Ameya Jawalgekar and Anand Bhosale

Abstract ADHYAYAN is an innovative mobile application which determines a user's interest in a particular domain and nurtures them effectively so that they can pursue career in the field which they are interested in. The system takes into account social media posts, results of a test and application activity to find out the interest of users in different fields and then assists, guides and evaluates them continuously to improve their skills in these fields. ADHYAYAN is a three-tier system which consists of a front-end, middle layer, and back-end. Front-end is an Android application which provides personalized GUI for each user. Middle layer is Firebase, while back-end is a server hosted on 'Google Cloud Platform'. An algorithm has been developed for ADHYAYAN which calculates the ratio of user's interest in different domains and eventually feeds are generated in the same ratio on user's profile. To cater the increasing need of skilled employees in different fields and promote interest-based learning, ADHYAYAN has been proposed to overcome various limitations and drawbacks of existing solutions.

Keywords Unemployability · Social media · Continuous evaluation · Test · Feeds · Profile · Skills · Career · Short term profile · Long term profile · Personalized · Real-time

A. Talke (✉) · V. Patil · S. Raj · R. K. Singh · A. Jawalgekar · A. Bhosale
International Institute of Information Technology (IIIT), Pune, India
e-mail: akshaytalke@gmail.com

V. Patil
e-mail: viren21096@gmail.com

S. Raj
e-mail: sanyamraj22@gmail.com

R. K. Singh
e-mail: rohit.12.ks@gmail.com

A. Jawalgekar
e-mail: jawalgekar007@gmail.com

N. R. Shetty et al. (eds.), *Emerging Research in Computing, Information, Communication and Applications*, Advances in Intelligent Systems and Computing 906,
https://doi.org/10.1007/978-981-13-6001-5_45

Pramana Research Journal

ISSN NO: 2249-2976

RADIATIVE PROPERTIES OF AEROSOL MIXTURES OBSERVED OVER ARID AND ISLAND AERONET STATION

Dr. Sandeep R. Varpe

International Institute of Information Technology, Pune 411 057

Abstract

We have examined multiyear observational data at the AERosol RObotic NETwork (AERONET) sites at Jaipur (26.90° N, 75.80° E), and Hanimaadhoo (6.74° N, 73.17° E), were utilized to study the climatological characteristics of aerosol radiative properties. Both sides shows linear fall in SSA against FMF suggests aprobable combination of a linear mixture of fine and coarse aerosol components. Under clear sky conditions, change in the sign of radiative forcing from negative (cooling) to positive (warming) occurs at SSA about 0.85, while in the presence of clouds it can occur even at higher SSA due to the semi-direct effect. A change of 0.07 in SSA is shown to produce a 21% change in radiative flux at the top of the tropopause over the ocean at constant aerosol optical depth. The refractive index (RI) is one of the important optical parameters providing information relating to the nature of aerosols and is highly dependent on the chemical composition of the aerosols. Values of RI give an indication of highly scattering (real RI) or highly absorbing (imaginary RI) aerosol types.

Keywords: AEROSOL RADIATIVE FORCING, SINGLE SCATTERING ALBEDO, REFRACTIVE INDEX, HEATING RATES.

INTRODUCTION

Aerosols participate in the Earth's energy budget "directly" by scattering and absorbing radiation and "indirectly" by acting as cloud condensationnuclei and, thereby, affecting cloud properties [1]. Moreover, the direct absorption of radiant energy by aerosols can influence the atmospheric temperature structure and, thereby, cloud formation - a phenomenon that has been labelled the "semi-direct effect" [2]. The indirect effect of aerosols on weather and climate system takes place through the modification of cloud optical and microphysical properties [3]. A large number of studies have found that the anthropogenic aerosols change clouds and their optical properties [4, 5, 6]. Atmospheric aerosols change the concentration and size of the cloud droplets which in turn lead to a change in cloud albedo, its lifetime and thereby affect the precipitation [3, 7]. The picture of aerosols is more complex due to their large spatio – temporal ambiguity, diversity in the atmosphere associated life span [8, 9, 10, 11]. The addition of anthropogenic aerosols to the atmosphere may change the radiative fluxes at the top-of-atmosphere (TOA), at the surface, and within the atmospheric column. A positive radiative effect at the TOA indicates the addition of the energy to the earth-atmosphere system (i.e., a warming effect) whereas a negative effect indicates a net loss of energy (i.e., a cooling effect).The aerosol single scattering albedo (SSA), the ratio of scattering to extinction