Image Recognition Using Neural Networks

Anuj Guha, Pratiksha Moon, Prof. RoshniBhave, KirtiSonkusle, Shubam Gupta

Department of Computer Science and Engineering Guru Nanak Institute of Engineering andTechnology,DahegaonNagpur,Maharashtra,India

Department of Computer Science and Engineering Guru Nanak Institute of Engineering andTechnology,DahegaonNagpur,Maharashtra,India

Abstract- *Neural networks provide state-of-the-art results for most machine learning tasks. Unfortunately, neural networks are vulnerable to adversarial examples: given an input x and any target classification t, it is possible to find a new input x' that is similar to x but classified as t. This makes it difficult to apply neural networks in security-critical areas. Defensive distillation is a recently proposed approach that can take an arbitrary neural network, and increase its robustness, reducing the success rate of current attacks ability to find adversarial examples.In this project, we demonstrate that defensive distillation does not significantly increase the robustness of neural networks by introducing three new attack algorithms that are successful on both distilled and undistilled neural networks with 100% probability. Our attacks are tailored to three distance metrics used previously in the literature, and when compared to previous adversarial example generation algorithms, our attacks are often much more effective (and never worse). Furthermore, we propose using high-confidence adversarial examples in a simple transferability test we show can also be used to break defensive distillation. We hope our attacks will be used as a benchmark in future defense attempts to create neural networks that resist adversarial examples.*

I. Introduction

Image recognition is the task of identifying an already detected object as a known or unknown Image .Often the problem of image recognition is confused with the problem of Image detection, Image Recognition on the other hand is to decide if the "Image" is something known, or unknown, using for this purpose a database of faces in order to validate this input Image.

1.1 Face Recognization:

Different Approaches Of Face Recognition:

There are two predominant approaches to the face recognition problem: Geometric (feature based) and photometric (view based). As researcher interest in face recognition continued, many different algorithms were developed, three of which have been well studied in face recognition literature.

Recognition algorithms can be divided into two main approaches:

1. Geometric: Is based on geometrical relationship between facial landmarks, or in other words the spatial configuration of facial features. That means that the main geometrical features of the face such as the eyes, nose and mouth are first located and then faces are classified on the basis of various geometrical distances and angles between features.

2. Photometric stereo: Used to recover the shape of an object from a number of images taken under different lighting conditions. The shape of the recovered object is defined by a gradient map, which is made up of an array of surface normal (Zhao and Chellappa, 2006)

Popular recognition algorithms include:

1. Principal Component Analysis using Eigenfaces, (PCA)
2. Linear Discriminate Analysis,
3. Elastic Bunch Graph Matching using the Fisherface algorithm

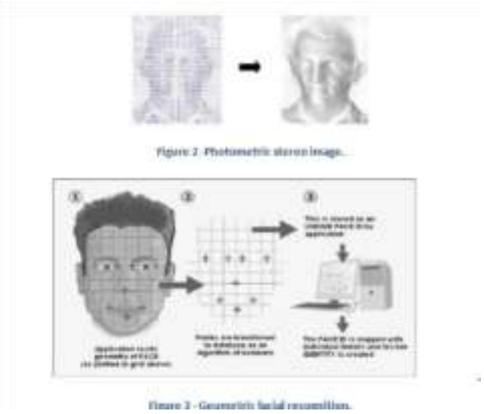


Figure 2 - Photometric stereo image.
Figure 3 - Geometric facial recognition.

Fig 1.1 Image Recognition

1.2 Face Detection:

Face detection involves separating image windows into two classes; one containing faces tarning the background (clutter). It is difficult because although commonalities exist between faces, they can vary considerably in terms of age, skin colour and facial expression. The problem is further complicated by differing lighting conditions, image qualities and geometries, as well as the possibility of partial occlusion and disguise. An ideal face detector would therefore be able to detect the presence of any face under any set of lighting conditions, upon any background. The face detection task can be broken down into two steps. The first step is a classification task that takes some arbitrary image as input and outputs a binary value of yes or no, indicating whether there are any faces present in the image. The second step is the face localization task that aims to take an image as input and output the location of any face or faces within that image as some bounding box with (x, y, width, height

1.3 The face detection system can be divided into the following steps:-

1. Pre-Processing: To reduce the variability in the faces, the images are processed before they are fed into the network. All positive examples that is the face images are obtained by cropping images with frontal faces to include only the front view. All the cropped images are then corrected for lighting through standard algorithms.

2. Classification: Neural networks are implemented to classify the images as faces or nonfaces by training on these examples. We use both our implementation of the neural network and the Matlab neural network toolbox for this task. Different network configurations are experimented with to optimize the results.

1.4 Localization: The trained neural network is then used to search for faces in an image and if present localize them in a bounding box. Various Feature of Face on which the work has done on:- Position Scale Orientation Illumination .

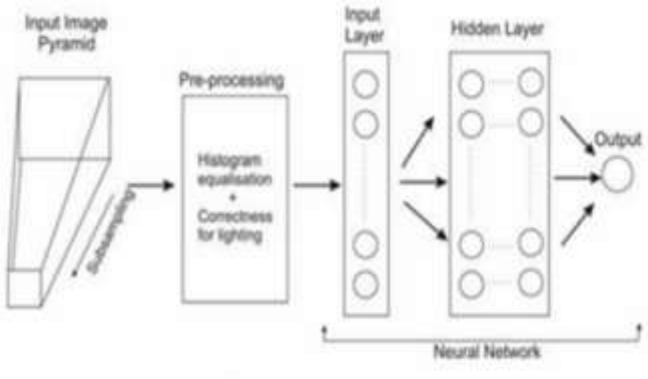


Fig 1.2 Face detection algorithm

1.5 Retinal Fundus Image Datasets

Retinal fundus images are available in public repositories. This encourages the researchers in this field to leverage their computational methods on such images and evaluate the performance of their algorithms. This provides a common platform for comparison of the proposed methods with the existing methods. A large variety of retinal image datasets are available in the publicly available repositories. Retinal datasets related to DR alone are taken up for investigation in this research. A few datasets also contain the benchmark ground truth of a few structural patterns annotated by ophthalmologists, which would help in evaluating the performance of the automated methods. The datasets namely HRF, DRIVE, STARE, DIARETDB0, DIARETDB1, HEI-MED and MESSIDOR datasets are investigated in this study.

II. Literature Survey

2.6.1 Nicholas Carlini& David Wagner

Neural networks provide state-of-the-art results for most machine learning tasks. Unfortunately, neural networks are machine learning tasks. Unfortunately, neural networks are machine learning tasks. Unfortunately, neural networks are vulnerable to adversarial examples: given an input x and any vulnerable to adversarial examples: given an input x and any target classification t, it is possible to find a new input x_ that is similar to x but classified as t. This makes it difficult that is similar to x but classified as t. This makes it difficult to apply neural networks in security-critical areas. Defensive to apply neural networks in security-critical areas. Defensive distillation is a recently proposed approach that can take an arbitrary neural network, and increase its robustness, reducing the success rate of current attacks' ability to find adversarial examples.

2.6.2 Wei Lin and Guanrong Chen

In the literature, it was reported that the chaotic artificial neural network model with sinusoidal activation functions possesses a large memory capacity as well as a remarkable ability of retrieving the stored patterns, better than the conventional chaotic model with only monotonic activation functions such assigmoidal functions. This paper, from the viewpoint of the anti-integrable limit, elucidates the mechanism inducing the superiority of the model with periodic activation functions that includes sinusoidal functions. Particularly, by virtue of the anti-integrable limit technique, this paper shows that any finite-dimensional neural network model with periodic activation functions and properly selected parameters has much more abundant chaotic dynamics that truly determine the model's memory capacity and pattern-retrieval ability. To some extent, this paper mathematically and numerically demonstrates that an appropriate choice of the activation functions and control scheme can lead to a large memory capacity and better pattern-retrieval ability of the artificial neural network models.

2.6.3 Lu Chi, and Yadong Mu

In recent years, autonomous driving algorithms low-cost vehicle-mounted cameras have attracted increasing endeavors from both academia and industry. There are multiple fronts to these endeavors, including object detection on roads,3-D reconstruction etc., but in this work we focus on a vision based model that directly maps raw input images to steering angles using deep networks. This represents a nascent research topic in computer vision. The technical contributions of this work are three-fold. First, the model is learned and evaluated on real human driving videos that are time-synchronized with other vehicle sensors. This differs from many prior models trained from synthetic data in racing games. Second, state-of-the-art models, such as PilotNet, mostly predict the wheel angles independently on each video frame, which contradicts common understanding of driving as a stateful process. Instead, our proposed model strikes a combination of spatial and temporal cues, jointly investigating instantaneous monocular camera observations and vehicle's historical states. This is in practice accomplished by inserting carefully-designed recurrent units (e.g., LSTM and Conv-LSTM) at proper network layers.

2.6.4 VarunChandola, Arindam Banerjee, and Vipin Kumar

Anomaly detection is an important problem that has been researched within diverse research areas and application domains. Many anomaly detection techniques have been specifically developed for certain application domains, while others are more generic. This survey tries to provide a structured and comprehensive overview of the research on anomaly detection. We have grouped existing techniques into different categories based on the underlying approach adopted by each technique. For each category we have identified key assumptions, which are used by the techniques to differentiate between normal and anomalous behaviour. When applying a given technique to a particular domain, these assumptions can be used as guidelines to assess the effectiveness of the technique in that domain.

2.6.5 Sunil Kumar Khatri,Shivali Dutta &prashantJohri

Recognizing the digits has become an integral part in terms of real world applications. since, digits are written in different styles therefore to identify the digits it is necessary to recognize and classify it with the help of machine learning techniques. This research is based on supervised learning vector quantization neural networks categorized under artificial neural network. the images of digits are recognized, trained and tested. After the network is created digits are trained using training dataset vectors and testing is applied to the images of digits which are isolated to each other by segmenting the image and resizing the digit image accordingly for better accuracy.

2.6.6 Daniel Andor, Chris Alberti, David Weiss, AliakseiSeveryn, Alessandro Presta, KuzmanGanchev, Slav Petrov and Michael Collins

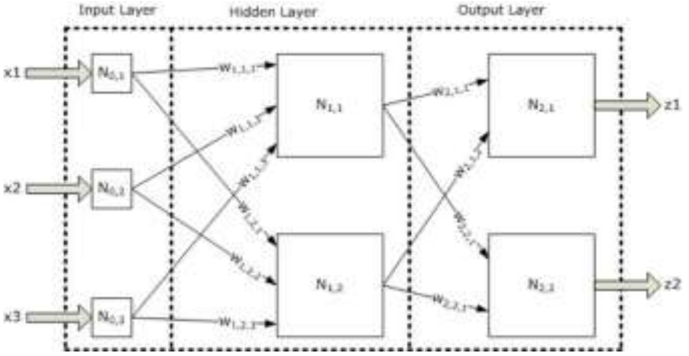
We introduce a globally normalized transition-based neural network model that achieves state-of-the-art part-of speech tagging, dependency parsing and sentence compression results. Our model is a simple feed-forward neural network that operates on a task-specific transition system, yet achieves comparable or better accuracies than recurrent models. We discuss the importance of global as opposed to local normalization: a key insight is that the label bias problem implies that globally normalized models can be strictly more expressive than locally normalized models

2.6.7 OsbertBastani, YaniIoannou, Leonidas Lampropoulos, DimitriosVytiniotis, Aditya V. Nori& Antonio Criminisi

Despite having high accuracy, neural nets have been shown to be susceptible to adversial examples, where a small perturbation to an input can cause it to become mislabeled. We propose metrics for measuring the robustness of a neural net and devise a novel algorithm for approximating these metrics based on an encoding of robustness as a linear program. We show how our metrics can be used to evaluate the robustness of deep neural nets with experiments on the MNIST and CIFAR-10 datasets. Our algorithm generates more informative estimates of robustness metrics compared to estimates based on existing algorithms. Furthermore, we show how existing approaches to improving robustness "overfit" to adversarial examples generated using a specific algorithm. Finally, we show that our techniques can be used to additionally improve neural net robustness both according to the metrics that we propose, but also according to previously proposed metrics.

III. System Architecture

In this chapter, we are going to discuss the design of our system including the implementation approach that we are using in building the system. Also, we are going to state the language used in the implementation.



IV. Result

This chapter presents the conclusions of the research work undertaken highlighting some of the key points and research contributions on exploitation of image processing and data mining techniques towards discovery of retinal image patterns detection.

V. Conclusion

The need for better image understanding software is increasing since it can be used in different fields such as medical, military, etc. According to the application of this system, we are intending to apply complicated images for the detection process, taking into account building the knowledge database that includes groups of images for each class of objects. So, we are going to detect objects embedded in given images regardless of the scale, translation, or rotation of the specified object. As a result, we are going to implement this system for indoor 2-D processes; this may have benefits regarding several applications such as robotics and security.

VI. Future Scope

The proposed methodologies for extraction of image patterns could be utilised for automated image analysis system to be used by the practitioners in the field of Science for image analysis. However, there still exist challenges that need to be addressed:

- The need for improved image filtering techniques to better expose the regions of interest
- The need for new evaluation metric for assessing the distinguishability of split attributes.

VII. Application

This software contains all the data related to the different objects. It detect the images like the human eye.

Reference

[1]. 2017 IEEE Symposium on Security and Privacy, Towards Evaluating the RobustnessofNeural Networks, Nicholas Carlini David Wagner, University of California, Berkeley.

[2]. ANDOR, D., ALBERTI, C., WEISS, D., SEVERYN, A., PRESTA, A., GANCHEV, K., PETROV, S., AND COLLINS, M. Globally normalized transition-based neural networks.arXiv preprint arXiv:1603.06042 (2016).

[3]. BASTANI, O., IOANNOU, Y., LAMPROPOULOS, L., VYTINIOTIS, D., NORI, A., AND CRIMINISI, A. Measuring neural net robustness with constraints. arXiv preprint arXiv:1605.07262 (2016).

[4]. BOJARSKI, M., DEL TESTA, D., DWORAKOWSKI, D., FIRNER, B., FLEPP, B., GOYAL, P., JACKEL, L. D., MONFORT, M., MULLER, U., ZHANG, J., ET AL. End to end learning for self-driving cars. ArXiv preprint arXiv:1604.07316 (2016).

[5]. CARLINI, N., MISHRA, P., VAIDYA, T., ZHANG, Y., SHERR, M., SHIELDS, C., WAGNER, D., AND ZHOU, W. Hidden voice commands. In 25th USENIX Security Symposium (USENIX Security 16), Austin, TX (2016).

[6]. CHANDOLA, V., BANERJEE, A., AND KUMAR, V. Anomaly detection: A survey. ACM computing surveys (CSUR) 41, 3 (2009), 15.

[7]. CLEVERT, D.-A., UNTERTHINER, T., AND HOCHREITER, S. Fast and accurate deep network learning by exponentiallinearunits(ELUs).arXiv preprint arXiv:1511.07289 (2015).

[8]. MISHKIN, D., AND MATAS, J. All you need is a good init. arXiv preprintarXiv:1511.06422 (2015).