IJITCE

ISSN 2347- 3657

# International Journal of Information Technology & Computer Engineering


Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

# Anomaly Detection Using Open Source Computer Vision and Deep Learning Algorithms

**Mohammed Akram, Dr. N. Sudhakar Yadav**

***Article Info***

*Received: 17-01-2023 Revised: 25-02-2023 Accepted: 26-03-2023*

**Abstract:**

Due to the monumental growth of Internet applications in the last decade, the need for security of information network has increased manifolds. As a primary defence of network infrastructure, an intrusion detection system is expected to adapt to dynamically changing threat landscape. Many supervised and unsupervised techniques have been devised by researchers from the discipline of machine learning and data mining to achieve reliable detection of anomalies. Deep learning is an area of machine learning which applies neuron-like structure for learning tasks. Deep learning has profoundly changed the way we approach learning tasks by delivering monumental progress in different disciplines like speech processing, computer vision, and natural language processing to name a few. It is only relevant that this new technology must be investigated for information security applications. The aim of this paper is to investigate the suitability of deep learning approaches for anomaly-based intrusion detection system. For this research, we developed anomaly detection models based on different deep neural network structures, including convolutional neural networks, autoencoders, and recurrent neural networks

***Keywords: neural networks, Haar cascade, defence, anomaly***.

## Introduction:

**Anomaly Detection** is the technique of identifying rare events or observations which can raise suspicions by being statistically different from the rest of the observations. Such “anomalous” behaviour typically translates to some kind of a problem like a credit card fraud, failing machine in a server, a cyber attack, etc. The major problem that occurs in examination system is malpractices. This is identified due to the absence of credible identity verification system for offline and also for online examinations. In order to overcome the above problem researchers have focused on the use of artificial

**Ph.D (CSE), Assistant professor, Department of Information Technology.**
**Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology (VNR VJIET), pragati nagar, Nizampet (S.O.), Hyderabad 500090**

ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

techniques and use of biometrics. In the past history work has been carried out on examination malpractices. Examination malpractice is any form of an illegal act committed during the examination. There are different forms of examination malpractice including copying from another student's test, getting notes to examination, plagiarism and impersonating another student during a test. All these scenarios and many others give students an unfair advantage. There may be many factors that cause examination malpractice like physiological factors, societal value system, over emphasis on paper qualification and poor learning facilities.

**Types of anomaly:**

An anomaly can be broadly categorized into three categories –

1. **Point Anomaly:** A tuple in a dataset is said to be a Point Anomaly if it is far off from the rest of the data.
2. **Contextual Anomaly:** An observation is a Contextual Anomaly if it is an anomaly because of the context of the observation.
3. **Collective Anomaly:** A set of data instances help in finding an anomaly.

**Proposed System:**

Anomaly detection with Keras, TensorFlow, and Deep Learning

Neural Network

Tensor flow

Deep learning is a subfield of machine learning that is a set of algorithms that is inspired by the structure and function of the brain.

TensorFlow is the second machine learning framework that Google created and used to design, build, and train deep learning models. You can use the TensorFlow library do to numerical computations, which in itself doesn't seem all too special, but these computations are done with data flow graphs. In these graphs, nodes represent mathematical operations, while the edges represent the data, which usually are multidimensional data arrays or tensors, that are communicated between these edges.

TensorFlow can hardware, and software requirements can be classified into

Development Phase: This is when you train the mode. Training is usually done on your Desktop or laptop.

Run Phase or Inference Phase: Once training is done Tensorflow can be run on many different platforms. You can run it on

ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

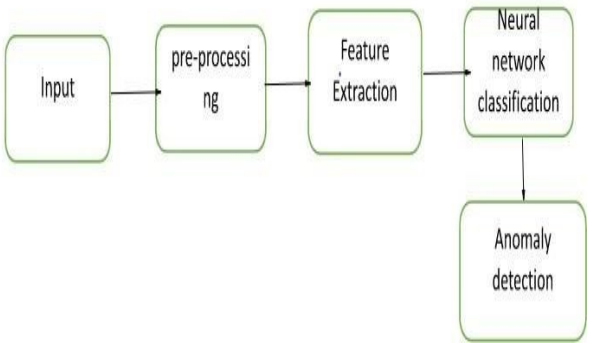
- Desktop running Windows, macOS or Linux
- Cloud as a web service
- Mobile devices like iOS and Android

You can train it on multiple machines then you can run it on a different machine, once you have the trained model.

The model can be trained and used on GPUs as well as CPUs. GPUs were initially designed for video games. In late 2010, Stanford researchers found that GPU was also very good at matrix operations and algebra so that it makes them very fast for doing these kinds of calculations. Deep learning relies on a lot of matrix multiplication. TensorFlow is very fast at computing the matrix multiplication because it is written in C++. Although it is implemented in C++, TensorFlow can be accessed and controlled by other languages mainly, Python.

Finally, a significant feature of TensorFlow is the TensorBoard. The TensorBoard enables to monitor graphically and visually what TensorFlow is doing.

Block Diagram:




**NEURAL NETWORKS**

In machine learning and related fields, artificial neural networks (ANNs) are computational models inspired by biological neural networks (the central nervous systems of animals, in particular the brain) and are used to estimate or approximate functions that can depend on a large number of inputs and are generally unknown. Artificial neural networks are generally presented as systems of interconnected "neurons" which can compute values from inputs, and are capable of machine learning as well as pattern recognition thanks to their adaptive nature.

For example, a neural network for handwriting recognition is defined by a set of input neurons which may be activated by the pixels of an input image. After being weighted and transformed by a function (determined by the network's designer), the activations of these neurons are then passed on to other neurons. This process is repeated until finally, an output neuron is activated. This determines which character was read. Like other machine learning methods - systems that learn from data - neural networks have been used to solve a wide

ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

variety of tasks that are hard to solve using ordinary rule-based programming, including computer vision and speech recognition.

Advantages and disadvantages of ANN networks:

- It is usually much faster to train a ANN/GRNN network than a multilayer Perception network.
- ANN/GRNN networks often are more accurate than multilayer perception networks.
- ANN/GRNN networks are relatively insensitive to outliers (wild points).
- ANN networks generate accurate predicted target probability scores.
- ANN networks approach Bays optimal classification.
- ANN/GRNN networks are slower than multilayer perception networks at
- Classifying new cases.
- ANN/GRNN networks require more memory space to store the model.

Artificial neural networks are statistical models of real world systems which are built by tuning a set of parameters. These parameters, known as weights, describe a model which forms a mapping from a set of given values known as inputs to an associated set of values, the outputs. The process of tuning the weights to the correct values –training- is vehicleried out by passing a set of examples of input-output pairs through the model and adjusting the weights in order to minimize the error between the answer the network gives and the desired output. Once the weights have been set, the model is able to produce answers for input values which were not included in the training data. The models do not refer to the training data after they have been trained; in this sense they are a functional summary of the training data.

The use of artificial neural network (ANN) in OCR applications can dramatically simplify the code and improve quality of recognition while achieving good performance. Another benefit of using neural network in OCR is extensibility of the system i.e. ability to recognize more character sets than initially defined. In the character recognition algorithm using neural networks, the weights of the neural network were adjusted by training it using back propagation algorithm. The size of each character is 28-by-18 pixels which are arranged column wise to give 504 _ 1 arrays as input. In order to train the neural network, we have created different sets each containing digits from 0 to 9. This is called Block training. The complete net work was implemented as a library, which was statically tied to the project. This helped to isolate the neural network code from the rest of the preprocessing and segmentation code . It also helped to reduce the memory required for the program. Character recognition of the number-plate is a fairly well developed field in computer vision in which template matching and neural networks are often used and can produce satisfactory results However, template matching has its drawbacks in some aspects comparing with neural networks. For

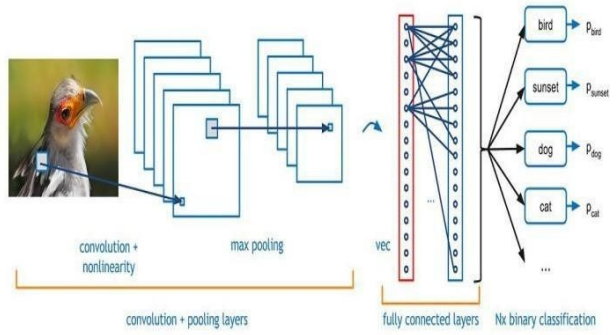
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

example, when characters of number-plate are segmented, neural network approach is preferred to template match one due to more computation cost of the later method.

TRAINING NEURAL NETWORK:

In off-line training of BP neural network, input and output vector sets are prepared for 36 character sets as mentioned in image segmentation section. The deformed character images are also used to prepare learning set to obtain sensitivity through the undesired effects. The designed ANN includes 209 nodes in the input layer, and 36 nodes in the output layer. The number of nodes in hidden layer is 36, and choosen experimentaly. Learning rate and the momentum rate are experimentally choosen as 0.2 and 0.8, respectively. Error at the end of the learning is 0.000763. The error is computed using the equation (19) known as average squared error [1]. Here, N denotes the total number of samples in training set, and the set C includes all the neurons in the output layer of the network.

Convolutional neural networks. Sounds like a weird combination of biology and math with a little CS sprinkled in, but these networks have been some of the most influential innovations in the field of computer vision. 2012 was the first year that neural nets grew to prominence as Alex Krizhevsky used them to win that year's ImageNet competition (basically, the annual Olympics of computer vision), dropping the classification error record from 26% to 15%, an astounding improvement at the time.Ever since then, a host of companies have been using deep learning at the core of their services. Facebook uses neural nets for their automatic tagging algorithms, Google for their photo search, Amazon for their product recommendations, Pinterest for their home feed personalization, and Instagram for their search infrastructure.




The Problem Space

Image classification is the task of taking an input image and outputting a class (a cat, dog, etc) or a probability of classes that best describes the image. For humans, this task of recognition is one of the first skills we learn from the moment we are born and is one that comes naturally and effortlessly as adults. Without even thinking twice, we're able to quickly and seamlessly identify the environment we are in as well as the objects that surround us. When we see an image or just when we look at the world around us, most of the time we are

ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

able to immediately characterize the scene and give each object a label, all without even consciously noticing. These skills of being able to quickly recognize patterns, generalize from prior knowledge, and adapt to different image environments are ones that we do not share with our fellow machines.

**Preprocessing**

Image Pre-processing is a common name for operations with images at the lowest level of abstraction. The preprocessing is the initial step for the process of video frames; it includes conversion of image frames into grayscale image. The preprocessing of input video is done to remove the noise and outliers, which are performed by Gaussian Filter. Its input and output are intensity images. The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing.Image restoration is the operation of taking a corrupted/noisy image and estimating the clean original image. Corruption may come in many forms such as motion blur, noise, and camera misfocus.Image Pre-processing is a common name for operations with images at the lowest level of abstraction. Its input and output are intensity images. The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing.

**Advantages:**

if time is infinite, then we must make better

All of these small human errors are sent to marketers as alerts to address now or later

**Disadvantages:**

It can be intimidating or seem complex.

**Hardware Requirements**

- system
- 4 GB of RAM
- 500 GB of Hard disk

**SOFTWARE REQUIREMENTS:**

- Python
- Open-CV

Results:

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 2, Apr 2023



Conclusion:

Visual anomaly detection is an important and challenging problem in the field of machine learning and computer vision. This problem has attracted a considerable amount of attention in relevant research communities. Especially in recent years, the development of deep learning has sparked an increasing interest in the visual anomaly detection problem and brought a great variety of novel methods. In this paper, we provide a comprehensive survey of the classical and deep learning-based approaches for visual anomaly detection in the literature. We group the relevant approaches in view of their underlying principles and discuss their assumptions, advantages, and disadvantages carefully. We aim to help the researchers to understand the common principles of visual anomaly detection approaches and identify promising research directions in this field.

**REFERENCES**

ISSN 2347–3657
Volume 11, Issue 2, Apr 2023

[1] D. Weinland, R. Ronfard, and E. Boyer, “Free viewpoint action recognition using motion history”, volumes. Computer Vision and Image Understanding, 104(2), 2006

[2] M. Blank, L. Gorelick, E. Shechtman, M. Irani, and R. Basri, “Actions as space-timeshapes”. In Proc. ICCV, 2005

[3] Dehghani, Alireza, and Alistair Sutherland. "A novel interest-point-based background subtraction algorithm." ELCVIA Electronic Letters on Computer Vision and Image Analysis 13.1 (2014).

[4] Ben-Musa, Ahmad Salihu, Sanjay Kumar Singh, and Prateek Agrawal. "Suspicious Human Activity Recognition for Video Surveillance System." (2014).

[5] Yong, Lu, and He Dongjian. "Video-based detection of abnormal behavior in the examination room." Information Technology and Applications (IFITA), 2010 International Forum on. Vol. 3. IEEE, 2010.