Turkish Journal of Physiotherapy and Rehabilitation; 32(2)
ISSN 2651-4451 | e-ISSN 2651-446X

MACHINE LEARNING SYSTEMS IN IMAGE MANIPULATION AND FAKE DETECTION

ABBURI M.N.S.P. PAVAN[1], ARUN SEKAR RAJASEKARAN[2], B.T.GEETHA[3], RADHAMANI.V[4], MUTHUKUMAR SUBRAMANIAN[5], ASHWIN PERTI[6]

[1,2]Department of ECE,GMR Institute of Technology,
GMR Nagar, Rajam - 532 127, Andhra Pradesh, India.
[3]Department of ECE, Saveetha School of Engineering,
SIMATS,Saveetha University,Tamil Nadu, India.
[4]Department of ECE, Rajalakshmi Engineering College,
thandalam, chennai-602105
[5]Department of CSE, Varuvan Vadivelan Institute of Technology
Dharmapuri Tamilnadu
[6]Department of IT, ABES Engineering College,
Ghaziabad – 201009, UP
[1]abburipavan36@gmail.com, [2]arunsekar.r@gmrit.edu.in,[3]dr.geetha.bt@gmail.com,
[4]radhamani.v@rajalakshmi.edu.in,[5]drsm.iiit@gmail.com,[6]ashwinperti@abes.ac.in

ABSTRACT:

Image processing is leading in some of the important areas like science and technology, biological, agriculture, face recognition and other fields. The main aim of machine learning is to improve or compress the image data. It is used to minimise a loss or cost function by optimising differentiable parameters. As a result of combining these two, a greater understanding of image processing has emerged. On other hand improving the image data in machine learning is one of the factors on other hand Image are one of the most common sharing things on the internet. In this emerging era many fake images are also sharing with the real images. Forging the images leads to the cybercrimes, So the area of detecting forging images is difficult task. The tampered images are identified using the neural networks that recognizes a section of an original image that has been manipulated. The false content in a fake image has a different compression ratio than the original image that can be identified by using Error Level Analysis.

Keywords: Image processing, machine learning, fake detection, image manipulation

I. INTRODUCTION:

As vision is apparently human's most important sense, images have always played an essential role in human's life. As a result, the image processing field are updating with copious applications like - it can be used in medical field to sperate the x-rays or combining of images, military field etc. And with the advancement of digital technologies a greater number of images are producing increasing complexity to process these images. For processing of these greater number of images, we need an advanced technology because traditional techniques outdated due to delay, efficiency. And machine learning is emerged as a trending Technology of intelligent computer vision which performs lot of complex works more faster after trained by training data. Here in this work, we implemented some of the machine learning applications in image processing like image segmentation and result are discussed.

About this image processing [1] while doing it we may come across lot of fake images which will deviate the actual result of image processing technique. So, there is also a need to detect these fake images to unveil the image-based cybercrimes. Here in this work, we used convolution neural networks which takes the training data i.e. compressed ratio of image as input and identifies the test input image as whether it is real or fake by deciding a threshold value of compressed ratio.

The remaining part of this work discusses about image manipulation techniques using ML in section II. Techniques used for the fake detection are demonstrated in section III. The section IV concludes the work.

II. IMAGE MANIPULATION:

Image manipulation is the method of altering a digitised image in order to turn it into a desired image. Image processing is used to make the changes possible. Photographs are used to produce magazine covers and albums by image manipulation [2,3]. A single photograph or multiple photographs may be combined to create a collage to satisfy the requirements.

1. Image Processing:

The technique image processing is used for applying operations to an image in order to improve it or extract valuable information from it. It's a type of signal processing in which we pass an image as input and we will get an image or image's properties as outputs.

Image processing is related to the examination of discontinuous targets in an image. Using ML and Artificial Intelligence can result in significant changes in the image processing industry. Google Lens is one example of such pillars, as it uses deep ML and Artificial Intelligence [4] techniques to process complex images. Assume one person is walking through a park in a other country and he wants to know the names and description of few flowers. But he don't know the language which is used on the message board in that foreign country. What would one do in this scenario? Of course we will use a tool like Google Lens, a Google app that uses image processing techniques as well as Artificial Intelligence technologies and deep machine learning, will come into picture. Google Lens recognises and tells what it sees in order to provide actions depending on it. And in this scenario we need to place our phone's cam on that flower and then we need to ask to Google that what it is seeing.

Machine Learning has succeeded in the creation of software that can recognise and describe the contents of a drawing. In the field of image processing, AI and machine learning will work together and make wonders. The following are some of the improvements that can be seen in various industries:

a. Health Care Industry:

In the healthcare sector, image processing can be extremely beneficial. At present deep learning algorithms are making things easier in the health care and computer vision software fields. This type of software enables mechanized analysis to produce more reliable results at a faster pace. The majority of hospitals have yet to implement such innovations. When used correctly, such technologies will help us reduce our dependence on manual research.

b. Defence:

Since they do not know what lies ahead, it was difficult for the security staff to gain access to certain specific locations. The advancement of image processing has essentially revolutionised warfare. Drones can now be used to capture viewpoint of such locations, which can then be analysed exploiting algorithms of deep learning.

Monitoring cameras that warn you when someone is approaching the door may also learn who that person is. Image processing will make it possible, and it will fully transform the universe.

These are the examples which have some more importance in the emerging new era.

2. Image Manipulation Techniques:

We have discussed few of the algorithms and techniques for image manipulations [5] which are used to process the digital images in machine learning below.

a. Interpolation:

Some image processing techniques have been evolved that can change how an image is perceived without altering the image's information material. Interpolation is one of these techniques. This technique is most commonly used on images with small picture matrices. Because of the compact nature of the picture elements,

small matrices are often aesthetically unappealing. The image presentation can be enhanced by using a larger viewing matrix without changing the original image data.

b. Filtering:

Filtering is one of the main methods of image processing, as well as one of the most used. Filtering is a term that most of us are familiar with because it is used in our daily lives with audio systems. The bass and treble controls, as well as the similar but more advanced balance control, are used to improve or stops frequencies in these systems. The frequencies in an audio signal can be used to understand the spatial frequencies in a picture, as well as the corresponding filters that are used to improves or stops the spatial frequencies and preferentially pass high frequencies, as in a high pass filter.We can create a low pass filter by lowering the treble control. Frequencies are boosted when the audio balance control is increased at a certain frequency range. Some frequencies are attenuated as a result of a decrease.

c. Gray Level Manipulation:

In a digital image, each pixel is indicated by a number stored in computer memory. We may choose how the brightness or colour of the image is related to stored number in which each pixel is shown when presenting the digital image. In most cases, a linear grey scale map is the best option. In a linear map, we try to show every pixel at a brightness that is proportional to the numerical value stored, i.e. pixels with two times the stored value are shown at twice the brightness. Image features are improved by often using Non-linear maps or look-up tables.

d. Geometric Processing:

The majority of image manipulation algorithms work by changing the pixel intensities to achieve a desired shift in concept. Geometric manipulations are another form of image manipulation that deals not only with pixel intensity but also with pixel position. The subtraction angiography which is imaging a test that exploits X-rays to view our body's blood vessels and performed to align contrast- containing images with the mask image is done by using simple pixel shifts and image translations.

e. Image Subtraction:

Image subtraction is one of the most basic but efficient algorithms for extracting image features. Although image subtraction cannot create some properties that are not already present in the image, it can enhance the visibility of features by removing undesired structures or which are appear to confuse the scene. Subtraction is clearly restricted to certain areas at which we can obtain mask image.

f. Segmentation:

The emergence of modern and efficient 3-D image display systems and techniques has resulted in a renewed focus on image segmentation. The term "segmentation" is most widely used to describe the identification and extraction of features in digital images.

In this context, feature extraction refers to the separation of an object from its surroundings. Obviously, the segmentation algorithm must be programmed to identify any aspect of the object that is distinct from its context. As a result, segmentation algorithms are as diverse as the objects of interest. Geometric, textural, and intensity variations have traditionally been used in segmentation.

In segmentation by thresholding, the most basic segmentation algorithm is used. A grayscale image is converted to a binary image using the thresholding algorithm. White is defined as pixel values above a given threshold, and black is defined as pixel values below the threshold. After segmentation, the display or measurement algorithm may choose whether to show or measure either white or black features.

All these image manipulation techniques are used in the machine learning methods.

There are three main machine learning methods used in image manipulation techniques.

- DECISION TREES
- ARTIFICIAL NEURAL NETWORKS
- INSTANT-BASED LEARNING

1. Decision Trees:

Decision Tree is a type of supervised learning method that can be exploited to solve both classification and regression problems, but it is most often used to solve classification issues. Internal nodes represent dataset attributes, branches represent decision laws, and each leaf node represents the outcome in this tree-structured classifier.

The Decision Node and the Leaf Node are the two nodes in a Decision tree. Leaf nodes are the product of such decisions and do not have any additional branches, while Decision nodes are used to make any decision and have several branches. The decisions or tests are made based on the properties of the specified dataset. It is a graphical representation for acquiring all possible outcomes to a problem based on certain parameters. It is called a decision tree because, like a tree, it starts with the root node and enhance into a tree-like structure with extra branches. We use the Classification and Regression Tree algorithm (CART algorithm), to construct a tree. A decision tree simply asks a question and divides the tree into subtrees depending on the answer (Yes/No).

2. Artificial Neural Networks (ANN):

Each input neuron corresponds to image colour information, and each output neuron corresponds to an image. To make learning simple and fast, all images will be scaled to the same size (width and height). The image sizes will be defined by the scale of the input vector as well as the number of neurons. For this type of problem, the transfer function is known as the sigmoid function. The learning rate should be between [0.1] and [0.1], and the error should be less than 0.1. Image processing with ANN entails a number of steps, including:

i. Image preprocessing is an operation that displays a picture of the same dimensions (contrast improvement, noise reduction)in the same proportions as the original. The aim of using Artificial Neural Networks to improve, restore, or reconstruct images is the goal of image preprocessing. The issues that have been resolved are cartographic forms, optimising a function, and an approximation function for image reconstruction.

ii. Data reduction, also known as feature extraction, is the process of removing a collection of features that are lower than the number of pixels in the input window. The procedure entails reducing the image before removing geometric properties (edges, corners, joints), facial features, and so on.

iii. The division of an image into regions is known as segmentation.

iv. Object recognition is the process of identifying objects in an image and classification.

1. Instance-Based Learning:

Machine Learning systems that are classified as instance-based learning learn the training examples by heart and then generalise to new instances using some similarity measure. It's called instance-based because the hypotheses are built from the training data. It's also known as lazy learning or memory-based learning. The size of the training data defines the time complexity of this algorithm. This algorithm's toughest case time complexity is O (n), where n is the number of training instances.

One of the important algorithms for instance-based learning is K Nearest Neighbor (KNN)

- A learn-by-memorizing method: **K-Nearest Neighbor**
- Given a data set $\{X_i, Y_i\}$ it estimates values of Y for X's other than those in the sample.
- The process is to choose the **k** values of X_i nearest the X and average their Y values.

- Here k is a parameter to the estimator. The average could be weighted, e.g. with the closest neighbor having the most impact on the estimate.

III. FAKE DETECTION

In today's world, fake images are widely disseminated through social media. The recognition of such fake images is unavoidable if image-based cybercrime is to be exposed. In this digital age, forging photographs and finding forgeries are promising research fields. The tampered images are identified using a neural network, which also identifies the distorted regions of the image and shows the actual image segments [6,7].

It can be introduced on the Android platform, making it accessible to the general public. The foreign content in a false image has a different compression ratio than the original image, which can be identified using Error Level Analysis. Image metadata is another function that is used in conjunction with compression ratio. Although metadata content can be changed, making it irregular on its own, it is being used as a supporting parameter in the error level analysis decision.

A large number of people have been victims of picture forgery in this technological era. Many people use technology to alter photographs and present them as proofs in court to deceive the judge. To put a stop to this, all persons who take photos posted on digital media should be properly classified as either true or fake. Social networking is a fantastic tool for socialising, sharing, and spreading information, but if used without care, it has the potential to deceive people and even create chaos due to unintended false propaganda.

Let’s see how this machine learning can be useful by using the metadata analysis and error level analysis techniques.

1. MetaData:

The majority of image files contain more than just a frame. They often provide information about the image (metadata). Metadata describes a photograph's provenance, such as the camera type used, colour space detail, and application notes. Different forms of metadata are used in various picture formats. Beyond the image dimensions and colour space, some formats, such as BMP, PPM, and PBM, contain very little details. A JPEG from a camera, on the other hand, generally consists a lot of information, such as the camera's parameters like model and make, focal and aperture information, and timestamps.

Unless the image was converted from a JPEG or edited with Photoshop, PNG files usually contain very little detail. Metadata from the source file format can be included in converted PNG files.

Metadata contains information about how the file was created and treated. This data may be used to determine if the metadata was captured with a digital camera, processed by a graphical programme, or manipulated to communicate false information. The following are some common items to look for:

- The identification of the application or device that creates the picture, and the software may contain the camera’s firmware version or the information of the application.

- The dimensions of the image are often recorded in the metadata. Is it true that the size of the rendered image (listed at the bottom of the metadata) fit the metadata's other sizes? Many programmes resize themselves or cropping photos without changing other metadata.

- Look for fields that contain timestamp information. These are used to determine when a photograph was taken or changed. Do the timestamps correspond to the planned timeline?

- There are several forms of metadata. Some are created solely by cameras, while others are created solely by applications.

2. Error Level Analysis:

Since JPEG is a lossy format, each resave introduces a different amount of error. Any change to the image would cause the image to become unstable in areas that were previously stable (no additional error). Figure 1 depicts a Photoshop-edited image. The updated image was created using the first 75% resave. A toy dinosaur was attached

to the shelf and books on the shelf were duplicated. The adjustments are identified by the 95 percent ELA because they are places where the minimum error level has been exceeded. Since Photoshop combined information from different layers, it effectively modified several of the pixels, additional areas of the image display slightly more volatility.

The amount of error is limited to the JPEG algorithm's 8x8 cells; after roughly 64 resaves, there is practically no difference. When an image is changed, however, the 8x8 cells that contain the changes are no longer at the same error level as the rest of the image. Error level analysis (ELA) works by saving again an image with a already known error rate, such as 95%, and after that calculating the difference between the two photos. The cell has reached its local minima for error at that quality level if there is virtually no improvement. If there is a significant load of transition, the pixels are no longer at their local minima and are productively "original." JPEG is a lossy format, but the error caused by each resave is not linear, so changing the image will cause stable areas (with no additional error) to become unstable.

A toy dinosaur was attached to the shelf and books on the shelf were duplicated (Fig 1). The adjustments are identified by the 95 percent ELA because they are places where the minimum error level has been exceeded.

Since Photoshop combined information from different layers, it effectively modified several of the pixels, additional areas of the image display slightly more volatility. In the original image, nearly all pixels are not at their local minima. Wide areas where the pixels have hit their local minima are visible in the first resave (75 percent). More areas that have hit their local minima for error are introduced in the second resave.

Figure 1. Error Level analysis of an image is left, and the fake image is right.

We may determine which part of the image is likely faked by examining the pattern in the Error Level Analysis applied image (Fig 1 left side). Since small scale changes in images are difficult to detect with the naked eye, we chose to use machine learning to detect irregularities in the error level analysed images. How it can be analysed is described below.

To train the network from the ground up, we should calculate the number of filters and layers, as well as the other requirements. A large amount of data, accumulated based on millions of samples, is required to train a particular model from the beginning, which can take a long time. The exploitation of a pre-training model to automatically withdraw the features from a newly formed dataset is an appropriate replacement to Convolution Neural Network training from scratch. Transfer learning is a simple way to implement deep learning without a big data set or a lengthy calculation and training time.

Alexnet, Classic CNN, and Alexnet with Transfer Learning are the three networks. There is a teaching dataset and a test dataset for each network. In certain instances, the evaluation data is derived from the training data, and vice versa. we used 2 datasets for example. The 1st dataset includes 1400 training images and 400 testing images. Another dataset includes 400 training images and 40 testing images. The fake images in the training data are bring out from the original images in the second data collection, and three fake images are created for each original image. The researcher altered the original photographs by adding, removing, and altering the colours. The steps for training a dataset using a CNN network are as follows.

- Load the sample's data into the image's data store. Image Datastore automatically marks images depending on the folder name and stores information as an image datastore object. When training a convolutional neural network, an image datastore allows you to store large amounts of image data and efficiently analyse image batches.

- Build network layers based on the CNN architecture.

- After the network architecture has been defined, the training options are defined. Learning rate, epochs, momentum, and batch size are all factors to consider.

- Use layer-defined architecture, training data, and training options to train the network.

- Anticipating new data labels and evaluate classification precision.

Using the qualified network, predict the labels of the data and assess the final accuracy.

Note that the Alexnet network and the Transfer Learning network both go through the likely training stages, with the exception that the load pretrained network is an extra step in Alexnet and the replace final layers is an extra step in Transfer Learning.

IV. RESULTS AND CONCLUSION:

This paper discusses about the various image manipulation techniques has been handled with machine learning algorithms. Machine learning was discovered to present a new paradigm that aided in the better processing of images. It was used in image processing to solve many of the issues that had previously existed. The error network analysis was used to successfully train a neural network. The trained neural network was identified the fake images with 83% of success rate. It reduces the spreading of fake images through digital media and also rejects the false proofs in digital authentication and the assessment of court proofs.

REFERENCES

1. H. Cao and A. C. Kot, "Manipulation Detection on Image Patches Using FusionBoost," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 992-1002, June 2012, doi: 10.1109/TIFS.2012.2185696.
2. S. Baluja, "Hiding Images within Images," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 7, pp. 1685-1697, 1 July 2020, doi: 10.1109/TPAMI.2019.2901877.
3. H. Choi et al., "Detecting composite image manipulation based on deep neural networks," 2017 International Conference on Systems, Signals and Image Processing (IWSSIP), 2017, pp. 1-5, doi: 10.1109/IWSSIP.2017.7965621.
4. S. D. Thepade, D. M. Bakshani, T. Bhingurde, S. Burghate and S. Deshmankar, "Performance Appraise of Machine Learning Classifiers in Image Splicing Detection using Thepade's Sorted Block Truncation Coding," 2020 IEEE Bombay Section Signature Conference (IBSSC), 2020, pp. 16-20, doi: 10.1109/IBSSC51096.2020.9332167.
5. S.Usha Kiruthika, S.Kanaga Suba Raja , Jaichandran R, Priyadharshini C, 2019 'Detection and Classification of Paddy Crop Disease using Deep Learning Techniques', International Journal of Recent Technology and Engineering, ISSN: 2277-3878, Volume 8, Issue - 3, pp. 4353-4359.
6. H. -T. Wang and P. -C. Su, "Deep-Learning-Based Block Similarity Evaluation for Image Forensics," 2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), 2020, pp. 1-2, doi: 10.1109/ICCE-Taiwan49838.2020.9258247.
7. S. Ranjan, P. Garhwal, A. Bhan, M. Arora and A. Mehra, "Framework for Image Forgery Detection and Classification Using Machine Learning," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 1-9, doi: 10.1109/ICOEI.2018.8553924.