



IMAGE MORPHING DETECTION USING MACHINE LEARNING

A. Sai Karthik¹, B. Tharun kumar², M. Priyatham³, K. Ravi Teja⁴

¹⁻⁴Jain University, Bangalore

Abstract: The image speaks a thousand words as the advancement in the image processing technology combined with mini cameras and cheap storage made every one photographer as the images are stored locally and in the cloud. The growth of the social media made every one connected by this user post are shared often in the form of an image. With the growth of the image processing technology, the growth of the image manipulation and improvement software has been on the raise as lot of the software is mobile device based. As is the case with other technologies the image manipulation software has its own drawbacks. By using the software the personal identity can be changed to the bad affect this causes the loss of personal identity also results into identity assassination of an individual. Image manipulation software also manipulate the situations in an image which is the primary source of the fake news. The current system also attempts to solve the current problem by detecting the manipulation in an image. The system uses CNN architecture to point out the area of which the image is manipulated and displayed in the window.

INTRODUCTION

Images are the new form of the information exchange due to increase in the social media activity the data is shared between user regularly in the form of text, videos and images. Social Media platforms are flooded with the images on a minute to minute basis. The advancements in the software and graphic cards present on the computing devices led to the improvement in the image manipulation software. The image editing software can be used for enhancement of the images. The editing software often used in the enhancement of the low resolution images and the reconstruction of the images. The editing software such as photo-shop has been in the forefront of the editing software which are used in the context of the digital creation of the graphics, editing of the graphic and conversion of the graphic from one form to another form this made compression from large sized image to a smaller one. This leads to image sharing very effortless and consumes less amount of data on the storage platform. The combination of the editing software and low compression size made an phenomenon of creation of unique images from the existing images. This also led to the creation of the fake images that are circulated on various social media platforms. The images of such kind are often harmless and taken in good humor. But in some cases the their is an individual personality is being targeted for the personality assassination of the individual. This led to the deep rooted problem of the cyber bullying and cyber harassment based on the manipulated images.

There need a new age methodology to avoid such kind of the problems using the machine learning. With the improvement of the image editing software their is also development on the machine learning based image processing front. The machine learning is used for various types of analysis and detection of the patterns in data. With data science the ML(Machine Learning) models are applied on the images also. This made improvements in the field of the facial recognition and various forms of the disease detection which are based on the image processing as its core modeling as its form of the identification methodology.



The current process aims to continue on the current ML trends of the image processing for the identification methodology. The system will be an identification method that will detect the morphology and various other aspects of the image. CNN Convolution Neural Networks are a new age deep learning method to detect patterns from an image. The micro patterns that has to be uncovered from the image data-sets are targeted towards the detection of the given topics. The system in the current paper discusses on the detection of the modifications done in an image by using the deep learning methodology. The system uses a CNN based VGG16 which is a 16 layer network which will detect the micro patterns from the image to detects the manipulations done in an image and points out successfully.

EXISTING SYSTEM

[1] Due to software like Photoshop, GIMP, and Coral Draw, it becomes very hard to differentiate between original image and tampered image. Traditional methods for image forgery detection mostly use handcrafted features. The problem with the traditional approaches of detection of image tampering is that most of the methods can identify a specific type of tampering by identifying a certain features in image. Nowadays, deep learning methods are used for image tampering detection. These methods reported better accuracy than traditional methods because of their capability of extracting complex features from image. In this paper, we present a detailed survey of deep learning based techniques for image forgery detection, outcomes of survey in form of analysis and findings, and details of publically available image forgery datasets.

RELATED WORK

[2] An endeavor is prepared to review the current improvements in the research area of advanced picture fraud detection and comprehensive reference index has been exhibited on passive methods for forgery identification. Passive techniques donot require pre-embedded information in the image. Several image forgery detection techniques are arranged first and after that their summed up organization is produced. Author will review the various image forgery detection techniques along with their results and also compare the various different techniques based on their accuracy.

[3] There are two types of image forgery detection copy move and image splicing, and various attacks like blurring, noise, scaling, etc may occur. The overview of forgery detection techniques, the basic flow of how the forged image can be detected is presented. And finally it is concluded with the comparative study with some parameters, merits and demerits.

[4] Preprocessing is done at the initial stage to convert RGB to LAB space conversion, Proceeded with feature selection by employing image integration. The next step is to extract the features like kurtosis, Maximum Probability, Block artificial Grid. In Continuation with feature extraction, feature selection is performed using an improved crow search algorithm followed by enhanced convolution neural network classification. Finally, the performance of the proposed improved crow search algorithm is discussed.

[5] Recently, works on forgery detection based on neural networks have proved to be very efficient in detecting image forgery. Neural networks are capable of extracting complex hidden features of an image, thus giving better accuracy. Contrary to the traditional methods of forgery detection, a deep learning model automatically builds the required features, hence it has become the new area of research in image forgery. The paper initially discusses various types of image forgery techniques and later on compares different approaches involving neural networks to identify forged images.

[6] To detect such scams, we proposed techniques. In our paper, we proposed two important aspects of employing deep convolutional neural networks to image forgery detection. We first explore and examine different pre-processing



method along with convolutional neural networks (CNN) architecture. Later we evaluated the different transfer learning for pre-trained ImageNet(via-fine-tuning) and implement it over our dataset CASIA V2.0. So, it covers the pre-processing techniques with basic CNN model and later see the powerful effect of the transfer learning models.

[7]With the appearance of means of image processing and editing tools, creating or transform images has become simple and available. There are many types of image forgery, one of the most important and prominent type is called copy-move forgery in which a part of the image is copied and pasted into the same image with the aim of hiding something important or showing a false scene. This paper surveys different types of digital image forgeries and forgery detection methods. The survey has been done on existing techniques for forged image

PROPOSED SYSTEM

The proposed method uses a VGG 16 network VGG (Visual Geometric Graphic) is the deep convolution network methodology that is used in the image processing consisting of the multiple layer approach this is generally having 16 or 19 layers as the processing network. This architecture is brought into light by the object recognition methodology. The VGG will take the input from the data-sets that are converted into the vectors these vectors are the probability for the classification which will be linked to the targeted classes. The classes are the images class that which it belongs the image which are manipulated belong to the class A and the image which are not manipulated belong to the class B. The class A and class B are differentiated based on the basis of the contents of the dataset. The current dataset is the CG1050 dataset which consists of the 150 original images and 1050 tampered images.

From the CG1050 dataset all the images which are original images are stored in an large subset which in our case is a tensor subset1. Then this subset is further divided into small subset2 of the images and these are categorized as the vectors which has the image morphology of an un-tampered image sample. The morphology of the subset 2 has 75 image vectors which has 2 samples stored in each vector. The samples in the vectors will be further divided into layer wise sub-division of the image resolution. Based on resolution the images will be divided into the micro-resolutions. The micro-resolution of the individual image vector will give raise to the Kernels. The kernels will be attached to an individual filter. Each kernel filter will have an individual resolutions that have to processed as pixel based entity. The pixel based analysis is conducted each layer of the algorithm. In this layers namely input, Convolution, Max pooling, Fully connected and Soft-max layer the image will process and the image morphology will be calculated. The morphology is the density of the pixels that are distributed among the entire resolution of the image. The original images has not extra or excess pixel density regions but it has uniformly distribute pixel regions all across the image. This morphological information is detected as follows



ConvNet Configuration					
A	A-LRN	B	C	D	E
11 weight layers	11 weight layers	13 weight layers	16 weight layers	16 weight layers	19 weight layers
input (224 × 224 RGB image)					
conv3-64	conv3-64 LRN	conv3-64 conv3-64	conv3-64 conv3-64	conv3-64 conv3-64	conv3-64 conv3-64
maxpool					
conv3-128	conv3-128	conv3-128 conv3-128	conv3-128 conv3-128	conv3-128 conv3-128	conv3-128 conv3-128
maxpool					
conv3-256 conv3-256	conv3-256 conv3-256	conv3-256 conv3-256	conv3-256 conv3-256 conv1-256	conv3-256 conv3-256 conv3-256	conv3-256 conv3-256 conv3-256 conv3-256
maxpool					
conv3-512 conv3-512	conv3-512 conv3-512	conv3-512 conv3-512	conv3-512 conv3-512 conv1-512	conv3-512 conv3-512 conv3-512	conv3-512 conv3-512 conv3-512 conv3-512
maxpool					
conv3-512 conv3-512	conv3-512 conv3-512	conv3-512 conv3-512	conv3-512 conv3-512 conv1-512	conv3-512 conv3-512 conv3-512	conv3-512 conv3-512 conv3-512 conv3-512
maxpool					
FC-4096					
FC-4096					
FC-1000					
soft-max					

Figure: VGG16 Layer Arrangement

- Input image vector is given to the convolution layer.
- In the second stage the image will process through the convolution layer for the sub divisions of the image.
- The sub divided image will process through the max pooling layer for the image morphology detection, the morphology is analyzed for each regions of the image.
- After the analysis the original image which has the uniform morphology will be stored in the fully connected layer.
- After this stage the data of the original images are then fed into soft-max layer
- Finally the image is stored in the output layers of the VGG16 and concludes the training.

After the training of the original images. This set of images will be stored in the class A. Then the manipulated images are processed through the same methodology and the morphology of the manipulated images are processed by the VGG16 network. The manipulated image will have the non-linear, irregular and non-uniform distribution of pixels since the manipulation results in the concentration of the pixel density at a single location. The morphology of the image is also non-uniform in manner since that manipulations will results in the concentration of all the color and pixels at certain locations in image. This data will also be trained in the algorithm and the manipulated images trained data will belong to Class B. The class A trained data and class B trained data will combine to become a model which is used in testing an image that will be given by the input from the user. If the image is given as input from the user side then the algorithm loads the model and compares the image input with class A and class b the trained model will detects the subsequent class and plots the region on the window which is gray-scaled for the detection.

METHODOLOGY

The methodology used in the current system is divided into following Modules.

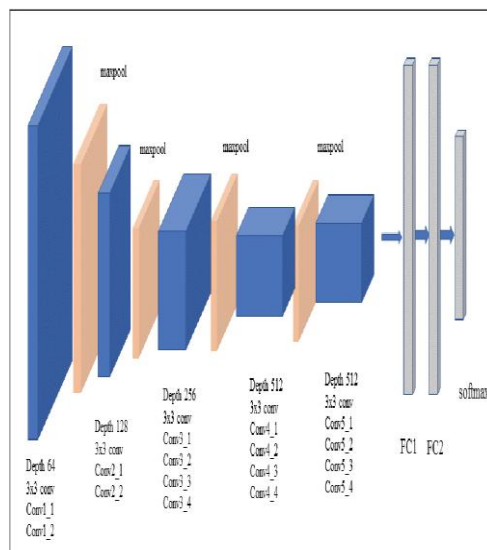


Figure: The System Architecture Of The VGG16

Input Factorization.

In the input factorization the VGG takes input image of the 224x224 pixel RGB vector. The image size is kept constant in this layer both original image and the manipulated image passes through this layer. All the images are converted into the 224x224 RGB vector that will be processed through the input layer. The individual images in data set which is either a original image or a manipulated image will be tested for the originality will be processed to next layer for morphological analysis this is defined by following equation

$$V^{u}_{j,q} = g(h^{u}_{j,q}).$$

Here v is the input layer h is the sample g is the multiplier of the input layer.

Convolution Factorization

In the convolution factorization in VGG the image is further divided into 3x3 micro resolutions, the current process used this size for the morphological analysis. There are also 1x1 convolution filters which are used in the current procedure which has acted as the transformation vector unit for the input. The convolution vector size padding is fixed to 1 pixel so that the resolution is conserved. In this layer the VGG will be analyzing the color distribution of an original image and a manipulated image. The color exposure of the original image will be in a uniform and linear manner and that of manipulated image is of a non linear manner. The following equation will define the above phenomenon

$$h^{u}_{i,p} = \sum_j \sum_s w^s_{i,j} V^{u}_{j,p+s} + b_i$$

Now the w is the multiplier of the convolution layer and v is the vector for the micro-resolution

Max-pooling Morphology Factorization

In this layer the images from the dataset will be assigned a 2x2 micro resolutions for the detection of morphology distribution in the image. The image which is tested for the color uniformity will be transferred into the current layer. In this layer the micro-resolution of the image will be a individual matrix of unique value. Here the matrix is a 2x2 matrix and the window size is 2x2x22. The each element in the matrix is a pixel each pixel with its corresponding hexa code is assigned a value. The value of original images matrix element values are incremented with a constant increment value. The manipulated image will have the random incremented value means each pixel morphology is a non-linear one this causes the dissimilarity in pixel distribution which is the case with manipulated images. This values of original images



and manipulated images are to be stored and trained in the further layers. This is represented as follows

$$\frac{\partial E}{\partial w_{i,j}^s} = -\sum_{\mu,p} [C^{\mu}_{i,p} - g(h^{\mu}_{i,p})] g'(h^{\mu}_{i,p}) V^{\mu}_{j,p+s}$$

The system differentiation will be defined by the following equation is the color differentiation of the input channels.

Fully-Connected Vector.

The system has 3 fully connected layers the first two will have the 4096 channels and third will have 1000 channels. These channels are assigned 1 for each class. The morphological data will be stored in the first two layer. The color values of the original images and manipulated images are stored in the third layer. First 4096 channel only store original and manipulated image array values calculated by the hex-code of the individual pixel and that which are detected for the uniformity will be stored in the channels. The RGB color values are stored in the third layer. This process can be denoted as follows.

$$\Delta w^s_{i,j} = \eta \sum_{\mu,p} \delta^{\mu}_{i,p} V^{\mu}_{j,p+s}$$

The Δw is the resultant of the morphological analysis of the image

Soft-Max Vector

The information which is stored in channel of three layers of the fully connected layer will be processed to the soft-max layer. The channels will contain all the hex values of the individual pixel that are calculated in the max pooling layer. These values are now be processed for the storage in the soft-max layer. The soft-max layer will have storage channels which the tuple or a map equivalent to store the morphology information and RGB information of the original and a manipulated image. All the information of the area wise data to detect on the image will be stored in the data structure for forwarding to the output layer.

$$(f * g)(t) \stackrel{\text{def}}{=} \int_{-\infty}^{\infty} f(T)g(t - T)dT$$

The integration factor is the channel storage of the various tuple values.

RELU Layer

In the RELU layer the data which is stored in the data structure will be directed into the model. This models contains all the information of the manipulated and original images. This model file forms the basis of the fake image detection which compares the input data from an image with the model file. If irregularities are found then the image manipulated area will be pointed out in the window and image will be gray-scaled and the manipulation will be clearly displayed to the user. After this step the model file is dumped into the models folder of the system.

Output Layer:

In the output layer the model file is compared with the input from user, and shows user which region is manipulated. The output layer is used in the testing process which compares the image model and tests if the image is matching with manipulated morphology and RGB. The model will inform the system that the image is a forged one. The models has all the information about manipulated and original image. By this model the image manipulation can be accurately pointed out.

ALGORITHM:

Start

The result is based on two assumptions

Step1: The sampling consists of all 2^{25} examples of the 8-of-25 function, or is the uniform distribution



Step2:The threshold for classification is 0.5. That is, an example E belongs to class + if and only if $p(+\backslash E) > 0.5$. the corresponding probabilities can then be obtained explicitly

$$\text{Step3: } p(+) = \frac{\sum_{i=m}^n \binom{n}{i}}{2^n}$$

$$p(-) = \frac{\sum_{i=0}^{m-1} \binom{n}{i}}{2^n}$$

$$\text{Step4: } p(A_i = 1 \backslash +) = \frac{\sum_{i=m-1}^{n-1} \binom{n}{i}}{\sum_{i=m}^n \binom{n}{i}}$$

$$\text{Step 5: } p(A_i = 1 \backslash -) = \frac{\sum_{i=0}^{m-2} \binom{n-1}{i}}{\sum_{i=0}^{m-1} \binom{n-1}{i}}$$

Step6: Let q denoted $p(A_i = 1 \backslash +)$. obviously, $q > 0.5$. The class probability estimate produced by output, denoted by $p_{nb}(+\backslash E)$, is

$$\text{Step 7: } p_{nb}(+\backslash E) = p(+)q^i(1 - q)^{(n-i)}$$

End

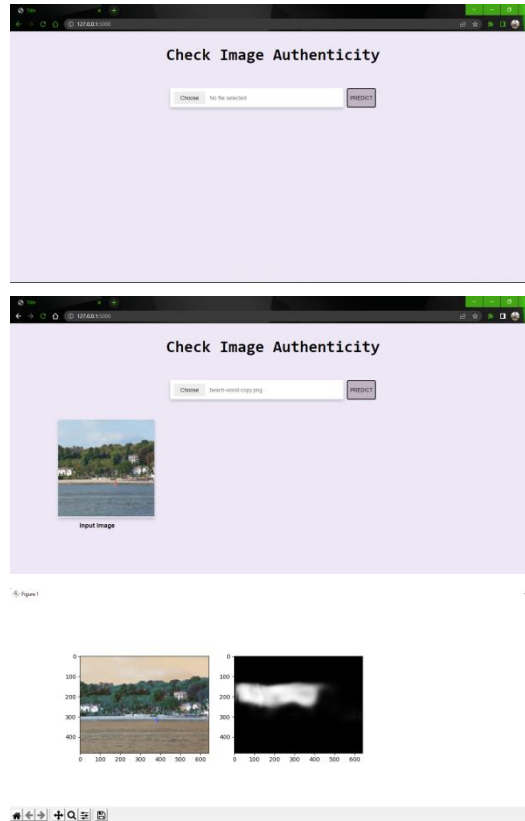
RESULTS

The system is designed based on the model that has been based on the procedure described above. The system loaded all the images in the training phase all the images processed through the input layer but the images were resized to the 224x224 micro-resolution this is kept constant and was passed into the convolution layer which is resized into 3x3 micro resolution and the filter was used in this layer will of 1x1 the filter is specifically designed to detect the color distribution on the image. Since the manipulated images have heavy concentration of color pixels at the specific areas the filter detected was trained to do so. The filter specifically have detected the unusual color areas on the image and the had processed it to the max pooling layer. The max pooling layer detected the image morphology by dividing the image into several 2x2 micro resolutions. The each 2x2 micro resolution is a matrix that will have a standard amount of the 4 pixel density in them, the matrix calculations are processed in this layer and has standard growth rate of the individual pixel value. The multiplier of the individual cell has a constant for the original images but for the manipulated images the growth rate of the individual pixel had a random multiplier constant. The fully connected layer had the channel for the storage of the color values for a original images and other channels for the morphological data. The data after the soft-max layer has the actual data of morphology and color storage into the tuple form. Each tuple had an actual color and a morphological pixel value. The output layer trained the original and manipulated images into a model file which is of a custom extension. The model file had been stored in the model folder.

After this process the test images are taken randomly from the internet and put to the test for how the trained model is performing on the random images. The images was first gray scaled by the convolution layer to test the color distribution on the given test image. The max-pooling layer had highlighted the regions where the manipulations are done in the image. The model also specifically highlighted all the regions around where the actual manipulations have been done with precision. The system had developed a user interface for the user to give input of the image for the testing of the image manipulation. The image input will be evaluated with the model and the manipulation of the image is displayed on a separate window for the user to view. The images which are manipulated will be displayed with the



modified areas.



Comparative Analysis

Table shows the diverse exhibition estimated by utilizing various boundaries. Condition is utilized to ascertain the precision, arrangement mistake and standard deviation of accessible dataset individually. Precision of strategic relapse is more noteworthy and arrangement

Sno	Algorithm	Datasets	Length of Data	Accuracy
1	KNN	American photo society	2000 records	69%
2	CNN	kaggle	12000 records	72%
3	Naive bayes	European photographer collection	8590 records	80%
4	SVM	European photographer collection	769580 records	74%
5	Current Classifier	Pinterest photographer collection	100000 records	93%

Camera based methods recognize imbalances in the picture by under-using the relics presented by the camera focal point, imaging sensor, sensor commotion and so forth Irregularities in these antiquities can be utilized as proof of



altering the handling steps associated with the camera based methods are, principally, the camera is utilized to catch the picture. A few antiquities are available related with the apprehended picture due to the variation in the camera focal point, imaging sensor, and so on. These antiquities show the presence of picture manipulation as a result of changing attribute of the camera image, the dynamic reach and shading stays same. In this strategy, we add or eliminate data to cover a piece of the picture. Some picture or text is concealed in unique image. A VGG Classifier recognizes falsehood in pictures by computing the hash value for removed highlights. In the preparation stage, the CNN is utilized in testing stage to guarantee the actuality of individual. Picture order, morphology detection, bio-succession investigation, hand-composing acknowledgment, and a lot more perplexing true issues can be achieved through VGG16. VGG16 works in two stages – the preparation stage and testing stage. At first, an information base is made with a bigger number of jpg or jpeg pictures and prepared in the preparation stage. These pictures can be of any measure and can be caught through a camera or downloaded from the web. The above table proves the current classifier is the efficient among all of the above algorithm.

CONCLUSION

The current system successfully developed a Machine learning model based on the VGG16 which had trained images samples above 2000. The system was based on the deep learning model which trained all the manipulated and original images. The manipulated images for testing are randomly taken from the internet and a user interface had been developed to take input from the user. The system precisely pointed out the manipulation done in the image. The current model can be further developed into the detection of the manipulated video detection which is near tougher task. The future model will be developed to determine if the video is genuine or a doctored video.

REFERENCES

1. Z. J. Barad and M. M. Goswami, "Image Forgery Detection using Deep Learning: A Survey," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 571-576, doi: 10.1109/ICACCS48705.2020.9074408
2. N. K. Gill, R. Garg and E. A. Doegar, "A review paper on digital image forgery detection techniques," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1-7, doi: 10.1109/ICCCNT.2017.8203904.
3. C. N. Bharti and P. Tandel, "A survey of image forgery detection techniques," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 877-881, doi: 10.109/iSPNET.2016.7566257.
4. T. Daniya, J. T. Thirukrishna, B. S. Kumar and M. V. Kumar, "ICSA-ECNN based Image Forgery Detection in Face Images," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402302.
5. R. Agarwal, D. Khudaniya, A. Gupta and K. Grover, "Image Forgery Detection and Deep Learning Techniques: A Review," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 1096-1100, doi: 10.1109/ICICCS48265.2020.9121083.
6. Singh and J. Singh, "Image forgery detection using Deep Neural Network," 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), 2021, pp. 504-509, doi: 10.1109/SPIN52536.2021.9565953.
7. N. Kanagavalli and L. Latha, "A survey of copy-move image forgery detection techniques," 2017 International Conference on Inventive Systems and Control (ICISC), 2017, pp. 1-6, doi: 10.1109/ICISC.2017.8068703.