International Journal of Advance Research in Science and Engineering
Volume No. 10, Issue No. 06, June 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

COLOR IMAGE FINDING MASK BY COPY MOVE FORGERY DETECTION

[1]M.Suganthi, [2]Dr. C. Akila

[1]M.Suganthi, Research Scholar, AP / CSE Department,

Thamirabharani Engineering College, Tirunelveli, Tamilnadu, India, sugi.mp@gmail.com

[2]Dr. C. Akila, AP / CSE, Anna University Regional Campus, Tirunelveli, akilavp@gmail.com

Abstract

With the evolution of novel implementation used for picture editing in today's world, the images can copy, resizing, cloning, cropping and slicing. Due to easy availability of alteration tools in nature, images cannot be trusted anymore. A popular manipulation method for improve the detection of the forged image is driven by the need of authenticity. The forensic image is the important evidence to alter the decision. Different technical devices and algorithms were introduced to conduct such forensic investigations method. Here, detection of the forged image by CNN is used to reduce the images into a form which is easier to process.

***Index Terms*—Image Restoration, Feature Extraction, CNN (Convolution Neural Network), Image Forgery, Forgery Detection.**

I. INTRODUCTION

Digital crime along with regularly developing software techniques is exponentially raising the rate which exceeds suspicious actions. In some cases, digital images or videos are unquestionable proof of a crime or the confirmation of a malicious act. Using the information from the digital image, the multimedia forensic agencies intend to develop effective approaches for supporting clue investigation and also offer a basis to make decision regarding a crime. Multimedia forensics [1] defines the upcoming technical devices which operate in the nonexistence of watermark or signature placed in the image. Generally, in contrast to digital watermarking, forensic indicates the passive work due to the fact that it formulates an investigation of a digital document by the presence of digital data itself. These methods fundamentally enable the client to verify whether the specific data has been tampered with or the usage of capturing devices. Particularly, the concentration on the process of the recognition of acquisition devices, two things should be considered: initially, we have to recognize the device model that created the image, for example, scanner, camera, etc., second it to identify the particular kind of the product that captured the particular data. Another important forensic concept is the identification of tampered images, i.e., evaluating the authentication of the digital image.

Data integrity is a basic criterion in various applications, it is also obvious that the invention of digital images and easiness of image processing in the present days makes it authentication. Where the digital image is modified and the crucial meaning of the image is interpreted which influences the court decision. In addition, it is fascinating that the images are given as an important proof to manipulate the information of what actually happened. In the present digital world, “seeing is no more believing”. A massive amount of content is transmitted in the digital way particularly in the outward appearance of images or videos. Hence, it produces the major flow of data carrier and the sources will undergo manipulation in an easier way. This paper focuses on image forgeries which are considered as a crucial task [5]. The image processing software like Adobe Photoshop is readily accessible and it makes the modification of images easier resulting to more consequences, since the tampered images are used as proof in the court judgment to take false decision by providing false information as a portion of evidences.

Introduction to Digital Image Processing:

Digital image processing [1] allows one to enhance image features of interest while attenuating detail irrelevant to a given application, and then extract useful information about the scene from the enhanced image. This introduction is a practical guide to the Challenges, and the hardware and algorithms used to meet them. Digital image processing is a subset of the electronic domain

IJARSE
ISSN 2319 - 8354

wherein the image is converted to an array of small m integers, called pixels, representing a physical quantity such as scene radiance, stored in a digital memory, and processed by computer or other digital hardware. Digital image processing, either as enhancement for human observers or performing autonomous analysis, offers advantages in cost, speed, and flexibility, and with the rapidly falling priceand rising performance of personal computers it has become the dominant method in use.

Fundamentals Steps In Image Processing Image Enhancement:

The classification [4] given is useful but neither complete nor unique. The algorithms are broadly divided into two classes, point transforms and neighbourhood operations. Point transforms produce output images where each pixel is some function of a corresponding input pixel. The function is the same for every pixel, and is often derived from global statistics of the image. With neighbourhood operations, each output pixel is a function of a set of corresponding input pixels. This set is called a neighbourhood because it is usually some region surrounding a corresponding centre pixel, for example a 3x3 neighbourhood.

Pixel mapping:

Point transforms include a large set of enhancements that are useful with scalar-valued pixels (e.g., monochrome images). Often these are implemented by a single software routine (or hardware module) that uses a lookup table. Lookup tables are fast and can be programmed for any function, offering the ultimate in generality at reasonable speed. MMX and similar processors, however, can perform a variety of functions much faster by direct computation than by table lookup, at a cost of increased software complexity.

Thresholding:

Is a commonly used enhancement whose goal is to segment an image into object and background. A threshold value is computed above (or below) which pixels are considered “object” and below (or above) which “background”. Sometimes two thresholds are used to specify a band of values that correspond to object pixels. Thresholds can be f fixed but are best computed from image statistics. Thresholding can also be done using neighborhood operations. In all cases the result is a binary image-only black and white are represented, with no shades of gray.

Color space conversion:

Color is used to convert between, for example, the RGB space provided by a camera to the HIS space needed by an image analysis algorithm. Accurate color Space conversion is computationally expensive, and often crude approximations are used in time critical applications. These can be quite effective, but it is a good idea.

Geometric pattern matching (GPM):

Is replacing NC template matching as the method of choice for industrial pattern recognition. Template methods suffer from fundamental limitations imposed by the pixel grid nature of the template itself. Translating, rotating, and sizing grids by non-integer amounts requires re - sampling, which is time consuming and of limited accuracy. This limits the pose accuracy that can be achieved with template- based pattern recognition. Pixel grids, furthermore,represent patterns using gray- scale shading, which as we've observed is often not reliable.

Feature Extraction:

Feature extraction[3] is the part of CNN architecture from where this network derives its name. Convolution is the mathematical operation which is central to the efficacy of this algorithm. Let's understand on a high level what happens inside the red enclosed region. The input to the red region is the image which wewant to classify and the output is a set of features. Think of features as attributesof the image, for instance, an image of a cat might have features like whiskers, two ears, four legs etc. A handwritten digit image might have features as horizontal and vertical lines or loops and curves. Later we'll see how do we extract such features from the image.

In this part, the network will perform a series of convolutions and pooling operations during which the features are detected. If you had a picture of a zebra, this is the part where the network would recognize its stripes, two ears, and four legs.

After a convolution layer once you get the feature maps, it is common to add a pooling or a sub-sampling layer in CNN layers. Similar to the Convolutional Layer, the Pooling layer is responsible for reducing the spatial size of the Convolved Feature. This is to decrease the computational power required to process the data through dimensionality reduction. Furthermore, it is useful for extracting dominant features which are rotational and positional invariant, thus maintaining the process of effectively training of the model. Pooling shortens the training time and controls over-fitting.

Forgery Detection:

It will aim at decision making process [2] in this section over an input image, either it is illustrated or not. We imply color image chrominance element, in spite of assuming image luminance part for extracting splicing artifacts. In detail, feature extraction and chrominance space in chroma space is demonstrated. We employed YCbCrcolor model image format that is a color space family like RGB.

In this, Cr and Cb demonstrates Chroma channel or chrominance component, whereas luminance component is demonstrated through Y in this color model. Cr and Cb are the chrominance components that are known as red-difference and blue-difference correspondingly. In contrast to Cr or Cb, Y element stores high image contents. For extracting features, the luminance element of color image splicing detection method has high concern when compared to chrominance component. But, by using many splicing artifacts, we examined that chroma store channel stores. Therefore, image chrominance element might be employed, to splicing artifacts. To the authentic image, the bird region is spliced. It is noted that details of image mask in splicing is initiated in Y element through bird contour observation in Y. When comparing with other object in image, the bird's contour looks sharper. Therefore, the edges that get affected through splicing can be detected simply.

II. EXISTING SYSTEM

To avoid resizing by means of patch-wise processing, at the cost of renouncing whole-image analysis.The CNN-based image forgery detection framework which makes decisions based on full resolution information gathered from the whole image. Gradient check pointing, the framework is trainable end-to-end with limited memory resources and weak supervision, allowing for the joint optimization of all parameters.

III. PROBLEM DEFINITION

In existing system, CNN was trained to detect the forgery by forward pass and backward pass method. During the forward pass, a memory-efficient implementation allows us to process the entire full-resolution image as a whole. During the backward pass, all framework blocks are optimized jointly and the network learns how to extract and aggregate the most discriminant information towards the correct classification of the whole image.

IV. PROPOSED SYSTEM

The pre-trained CNN is used as patch descriptor to extract dense features from the test images, and a feature fusion technique is then explored to obtain the final discriminative features for Support Vector Machine (SVM) classification. The experimental results on several public datasets show that theproposed CNN based model outperforms some state-of-the-art methods. We proposed a new CNN-based framework for image forgery detection. Thanks to suitable architectural solutions, the framework can be trained end-to-end, based only on weak supervision, exploiting information gathered at full-resolution from the whole image.

V. SYSTEM ARCHITECTURE

A system architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

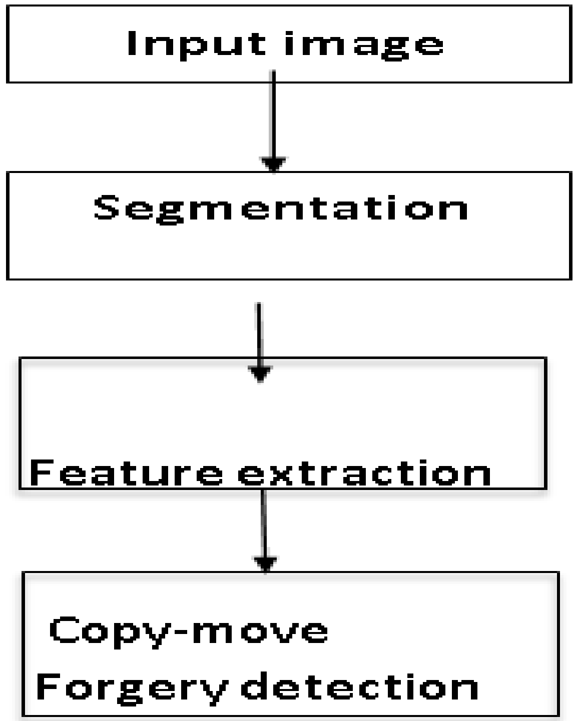

Fig. 1 System Architecture

The proposed system having four modules. The modules are:

- Image Dataset
- Segmentation
- Feature Extraction
- Copy-move forgery detection

Image Dataset:

A dataset in computer vis/ion is a curated set of digital photographs that developers use to test, train and evaluate the performance of their algorithms. A dataset in computer vision therefore assembles a collection of images that are labeled and used as reference for objects in the world.

A dataset in computer vision therefore assembles a collection of images that are labeled and used as reference for objects in the world, to 'point things out' and name them.

Segmentation:

Image segmentation is the process of portioning a digital image into multiple segments. Image segmentation is typically used to locate objects andboundaries in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such certain characteristics.

The result of image segmentation is a set of segments that collectively cover the entire image, or set contours extracted from the image.

Feature Extraction:

Feature extraction is a process that identifies important features of attributes of data and need to reduce the number of resources without losing any important relevant information. The selected features are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data.

Copy-Move Forgery Detection:

This method is successful to detect the forged path even when the copied area is enhanced or retouched to merge it with the back ground. Images are usually manipulated in two ways such as image splicing and region duplication through copy-move forgery. In image splicing, regions from multiple from multiple image are used to create a forged image.

VI. IMPLEMENTION:

Implementation is the stage where the theoretical design is turned into a working system. The most crucial stage in achieving a new successful system. The system can be implemented only after the testing is done and if it is found to work according to the specification. The implementation phase comprises of several activities. The hardware and software acquisition are carried out. The system may require some software to be developed.

International Journal of Advance Research in Science and Engineering
Volume No. 10, Issue No. 06, June 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

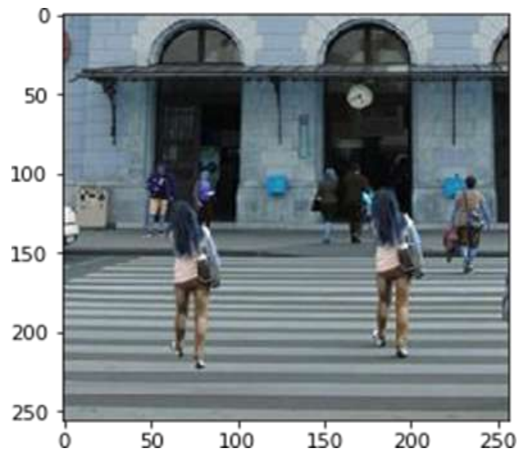

Fig. 2 Forged Input image

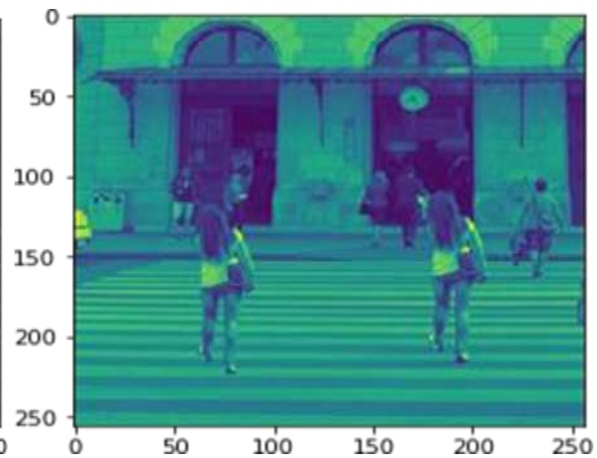

Fig. 3 Gray image of the forged input image

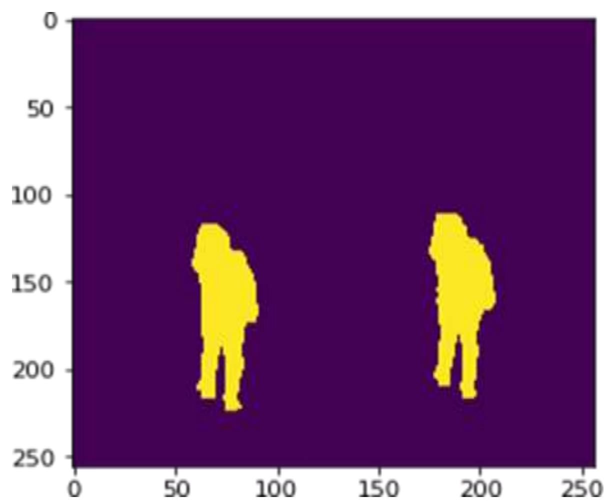

Fig. 4 Finding the Mask of the forged input image

Fig. 5 Original input image

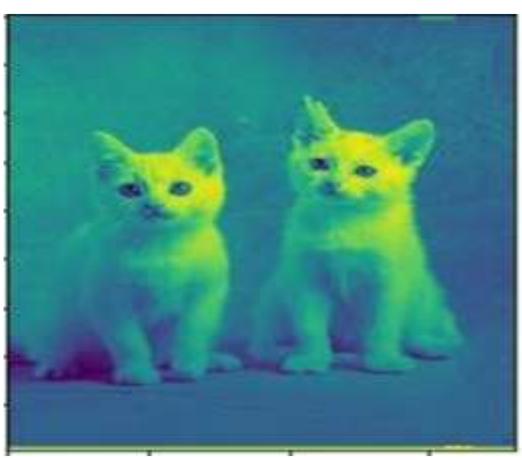

Fig. 6 Gray image of the Original input image

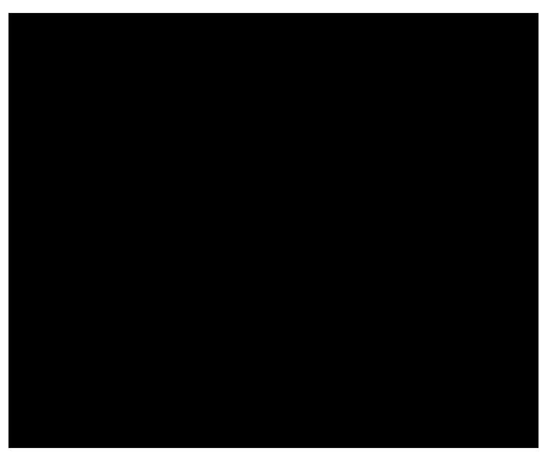

Fig. 7 Finding the mask of the Original input image

VII. CONCLUSION

Digital image processing is the processing of images and is a framework which is used to enhance raw images which are gotten from cameras, sensors set on satellites and air make. Various techniques are discussed to protect the digital images from image forgery attacks. Surveyed studies provide different types of techniques to detect copy-move image forgery. The analyzation of the studies still suffers from some drawbacks. There is need to investigate region transformation so that copy-move attacks can be easily detected. The proposed study focuses on the detection of copy-move attack on digital images. The image region transformation includes rotation, rescale and reflection in copy- move forgery. The rotation invariant with block- based copy-move forgery detection method is used which shows better results as compared to blur invariant copy – move forgery detection and provides accuracy rates between 96% to 100%.

VIII. FUTURE ENHANCEMENT

Image processing technology extracts information from images and integrates it for a wide range of applications. Here, we’ve outlined the most prominent fields where image processing could bring significant benefits. Image processingapplications can make it possible for machines to act as more self-sufficient and ensure the quality of products. Assuming processing systems work faster than humans, inline quality controls like 100% controls can be very quickly implemented. Damaged parts can be replaced or corrected, which would lead to more efficacies of production facilities. With the help of advanced image processing technologies, even an entire production facility can be manage. Irrigation monitoring and providing information can be made possible by tracking satellite imaging of the fields. Processing of infrared images can act as an additional means to monitor and analyze irrigation. This analysis can then be utilized in pre-harvesting operations for deciding whether to harvest or not. Growth of weeds can be detected by using a combination of machine learning and image processing algorithms and techniques. Quality of yields can be ensured by the reliable and accurate method of image processing.

REFERENCES

[1] Gang Cao, Yao Zhao, Rongrong Ni and Xuelong Li (2014), "Contrast Enhancement-Based Forensics in Digital Images", IEEE Access, Vol. 9, No. 3,
pp. 515-525.

[2] DavideCozzolino, Giovanni Poggi and Luisa Verdoliva (2015), "Efficient dense-field copy-move forgery detection", IEEE Transactions on Information Forensics and Security, Vol. 10, pp. 1-14.

[3] Xufeng Lin and Chang-Tsun Li (2016), "PRNU-Based Content Forgery Localization Augmented with Image Segmentation", IEEE Access, Vol. 4, pp. 1-16.

[4] Francesco Marra, Diego Gragnaniello, Luisa Verdoliva and Giovanni Poggi (2020), "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection", IEEE Access, Vol. 8, pp. 133488-133502.

[5] Haipeng Chen, Xiwen Yang and YingdaLyu (2020), "Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search", IEEE Access, Vol. 8, pp. 36863-36875.