Digital Image Forgery Detection

By Ansari M.Saeem (2019430001)

Faculty Incharge : Prof Kiran Gawande

INTRODUCTION

Maliciously manipulating and tampering of digital images is very successful because of the use of powerful and easily available image editing tools such as Photoshop. Because of this, there is a swift increase of the image forgery in news papers, TV and social media. Advanced Image Forensics is that field which manages the validations of the pictures. Computerized picture forensics checks the uprightness of the pictures by identifying different forgeries. One of the key errands of picture forensics is picture forgery identification. The accessibility of ease equipment and programming devices, makes it simple to make, modify, and controlled advanced pictures with no undeniable clues. Such programming can do an adjustment in computerized picture by changing squares of a picture without demonstrating the impact of the alteration in the produced picture. These changes can not be seen by human eyes. It might never again be conceivable to recognize whether a given advanced pictures is unique or an adjusted variant. Computerized picture forgery is a developing issue in criminal cases and in broad daylight course. Distinguishing forgery in computerized pictures is a rising exploration field for guaranteeing the validity of advanced pictures .In the later past advanced picture control could be found in newspaper magazine, design industry, scientific journals, court rooms, fundamental media outlet and photograph tricks we get in our email.

Types of digital image forgery

Picture altering is characterized as adding, changing, or deleting some important features from an image without leaving any obvious trace. There have been different techniques utilized for forging an image. Taking into account the methods used to make forged images, digital image forgery can be isolated into three primary classifications: Copy-Move forgery, Image splicing, and Image resampling.

1. Copy-Move Forgery :

   In copy-move forgery (or cloning), some part of the picture of any size and shape is copied and pasted to another area in the same picture to shroud some important data as demonstrated in Figure 1. As the copied part originated from the same image, its essential properties such as noise, color and texture don’t change and make the recognition process troublesome.

Figure-1 : Copy-Move Image Forgery

2. Image Forgery using Splicing:

Image splicing uses cut-and-paste systems from one or more images to create another fake image. When splicing is performed precisely, the borders between the spliced regions can visually be imperceptible. Splicing, however, disturbs the high order Fourier statistics. These insights can therefore be utilized as a part of distinguishing phony. Figure 2, demonstrates a decent sample of image splicing in which the pictures of the shark and the helicopter are merged into one picture.

Figure 2: Slicing Image Forgery

3. Image Resampling :

To make an astounding forged image, some selected regions have to undergo geometric transformations like rotation, scaling, stretching, skewing, flipping and so forth. The interpolation step plays a important role in the resampling process and introduces non-negligible statistical changes. Resampling introduces specific periodic correlations into the image. These correlations can be utilized to recognize phony brought about by resampling. In Figure 3, the picture on the left is the original image while the one on the right is the forged image obtained by rotation and scaling it.

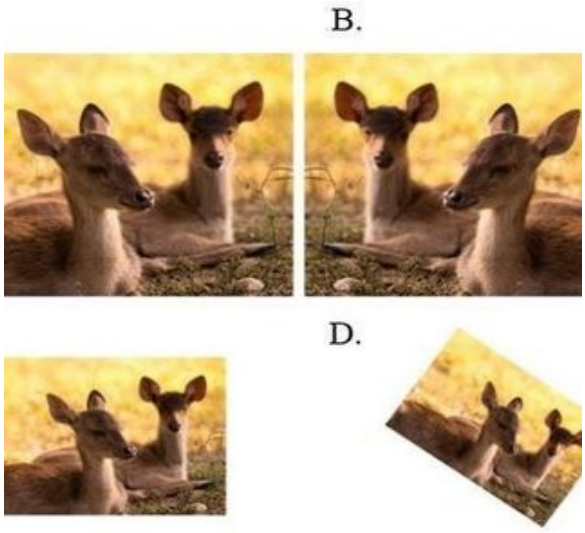

Figure 3: Resampling Image Forgery

LITERATURE SURVEY :

Sr no	Title	Author	Methodology/ Algorithm	Result/Performance Matrix
1	Deep Fake Image Detection based on Pairwise Learning	Chih-Chung Hsu , Yi-Xiu Zhuang , and Chia-Yen Lee	CNN, GAN, deep learning	BIGGAN - 90.9 SA-GAN – 93.0 SN-GAN – 93.4
2	A copy-move image forgery detection technique based on Gaussian-Hermite moments	Kunj Bihari Meena & Vipin Tyagi	Gaussian-Hermite Moments (GHM)	CoMoFoD Dataset Scaling And rotation - 94.54 color reduction - 95.00
3	A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection	Francesco Marra, Diego Gragnaniello, Luisa Verdoliva and Giovanni Poggi	CNN	E2E-RGB – 73.9 E2E-NP – 79.1 E2E-RGB+NP - 76.9 E2E-Fusion – 82.4
4	Image Forgery Detection Based on Motion Blur Estimated Using Convolutional Neural Network	Chunhe Song, Peng Zeng, Zhongfeng Wang, Tong Li, Lin Qiao, Li Shen	CNN, gradient checkpointing	96.33%

1. Authors propose a deep learning-based approach to detect the fake image by combining the contrastive loss. First, several state-of-the-art GANs will be collected to generate the fake-real image pairs. Then, the contrastive will be used on the proposed common fake feature network (CFFN)to learn the discriminative feature between the fake image and real image (i.e., paired information). Finally, a smaller network will be concatenated to the CFFN to determine whether the feature of the input image is fake or real.

In fake general image detection, They have collected three GANs to generate high-quality general images as the follows:

• BIGGAN (Large Scale GAN Training for High Fidelity Natural Image Synthesis)

• SA-GAN (Self-Attention GAN)

• SN-GAN (Spectral Normalization GAN)

2. In this paper, a new robust copy-move image forgery detection technique is proposed using Gaussian-Hermite Moments (GHM). The proposed technique divides the input image into overlapping blocks of fixed size and then the Gaussian-Hermite moments are extracted for each block. The matching of similar blocks is done by sorting all the features lexicographically. The experimental results show that the proposed technique can locate the copy-move forged regions in a forged image very accurately. The proposed technique shows promising results in the presence of various post-processing operations scaling, blurring, color reduction, adjustment of brightness, rotation, and JPEG compression.

3. In the proposed system, Authors propose a CNN-based image forgery detection framework which makes decisions based on full-resolution information gathered from the whole image. Using gradient check pointing(fit large network into memory), the framework is trainable end-to-end with limited memory resources and weak (image-level) supervision, allowing for the joint optimization of all parameters. Experiments on widespread image forensics datasets prove the good performance of the proposed approach, which largely outperforms all baselines and all reference methods.

4. This paper proposes a novel motion blur based image forgery detection method, which includes three steps. First, a convolutional neural network (CNN) based motion blur kernel reliability estimation method is proposed, which is used to determine whether an image patch should be involved in the image forgery detection process. Second, a shared motion blur kernels based image tamper detection method is proposed to detect whether a group of motion blur kernels are projected from the same 3D camera trajectory effectively. Third, a consistency propagation method is proposed to localize tampered regions efficiently. Experiments on synthetic images and natural images show the availability of the proposed method.

MOTIVATION

In today's world, as we interact more with social media we see cases where people are polarized to follow one critical topic, rumors are spread without any base information. Fake images are great way of sharing information and we should be careful while sharing information online. Since there is no system to detect the forgery in digital images. So I am inspired to make a system to detect forgery in digital images.

OBJECTIVES

1. To study basics of image forgery detection methodology/techniques and give various insight about it.
2. To provide solution, that effectively detect forgeries, tempering in digital images.

FUTURE PLAN

1. To carry more study on methodologies/approaches.
2. To design work flow diagram for proposed system.
3. To provide solution that helps in improving efficiency in forgery detection in digital images.

CONCLUSION

We have studied image forensic, image forgery and its type. In some papers, datasets were readily available to work with whereas on the other hand some papers have mentioned the need of multimodal database system where they have used CNN algorithm to do the detection. Various methodologies helped us to decide which one were feasible and which were costly. We plan to study further into these methodologies.

REFERENCES

1. Deep Fake Image Detection based on Pairwise Learning by Chih-Chung Hsu , Yi-Xiu Zhuang , and Chia-Yen Lee
2. A copy-move image forgery detection technique based on Gaussian-Hermite moments by Kunj Bihari Meena & Vipin Tyagi
3. A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection by Francesco Marra, Diego Gragnaniello, Luisa Verdoliva and Giovanni Poggi
4. Image Forgery Detection Based on Motion Blur Estimated Using Convolutional Neural Network Chunhe Song, Peng Zeng, Zhongfeng Wang, Tong Li, Lin Qiao, Li Shen