A REVIEW ON IMAGE FORGERY DETECTION

[1]Pallavi Gaikwad, [2]Sugandha Nandedkar

[1]Mtech Student,[2]Head (CSE)

Department of Computer Science and Engineering,

Deogiri Institute of Engineering & Management Studies, Chh. Sambhajinagar

Maharashtra state, India

ABSTRACT

As society grows more reliant on the internet, it also becomes more susceptible to dangerous dangers. These dangers are intensifying and changing all the time. The legitimacy of data sent via the internet is distorted by these dangers. Since all of us depend entirely or in part on this communicated data, its legitimacy must be maintained. The modification or change of a picture is known as image forgery. Since digital photos are utilized in court cases, picture forensics is a new discipline. The need to ensure the authenticity of digital images was heightened by picture forging. Due to the widespread use of editing software, photographs can be altered in ways that are invisible to the human sight. Techniques for detecting image forgeries are so crucial. This makes image forgeries, which are now a key source of worry, more severe and frequent. Consequently, a method that can effectively and precisely identify hidden forgeries in a picture is needed. In this research, we have provided a quick review of the literature on several methods that include current advances in deep learning and machine learning.

Keywords: image forgery, image forgery detection, deep learning, machine learning.

1. INTRODUCTION

A new area of image processing called "digital image forensics" aims to gather quantifiable proof of a digital picture's authenticity and provenance [1].Detecting picture manipulation is one of the main responsibilities of image forensics. Interfering with something to harm it or make unlawful changes is called tampering. Since images are used as evidence in a variety of contexts, image tampering is the deliberate alteration of photographs for malevolent ends [2]. Political propaganda was the first application of image altering in the early 20th century. Since picture manipulation is a common occurrence, the area of image forensics methods has seen significant advancements over the past ten years.

Because of how simple it is to alter photos using modern editing tools and methods, image forging has become an issue in the modern day. Accurate techniques for identifying picture fraud are essential given the usage of media, online journalism, and digital communication platforms. It might be difficult to tell the difference between photos and ones that have been digitally manipulated in a time when false information is common. This makes it challenging to ensure the validity and dependability of the material.

Image forensics techniques can be classified under two different approaches, Active approaches and Passive/Blind approaches [3]. Active approaches were used traditionally by employing data hiding (watermarking) or digital signatures. Passive approaches or blind forensic approaches use image statistics or content of the image to verify its genuineness [4]. Now days, digital images are widely used all over the world. Exchanging soft copy of various documents is a normal practice in these days. So, there is a possibility of forgery while exchanging such type of documents. Image Forgery is the process of making illegal changes of image information. Forgery may occur in applications which uses digital image because user can change it by using editing tools available in market [5].

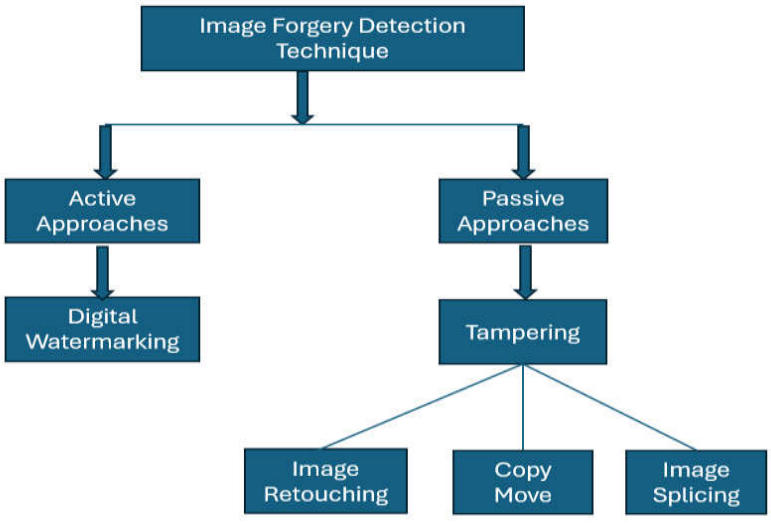

Figure 1. Classification of Image forgery Techniques

Developing effective image forgery detection techniques that can quickly identify and classify manipulated images while distinguishing them from real, unmodified ones is a problem. This

necessitates the development of algorithms that can analyse a wide range of image alterations in a number of contexts and at different levels of complexity, such as copy-move, splicing, retouching, and more. The solution should accommodate many image content sources by supporting a range of picture formats, resolutions, and digital platforms. The primary objective in addressing this problem is to design and deploy state-of-the-art image forensics systems that utilize computer vision, deep learning, and machine learning approaches. In addition to detecting forgeries, these technologies should be able to provide information on the specific manipulation techniques employed.Figure 2 shows an example showing original image and forged image.

Figure 2: (a) the forged image with four missiles (b) the original image with three missiles

2. LITERATURE REVIEW

There are two types of methods for detecting digital picture forgeries: active methods and passive methods. The active technique involves embedding specific information, such as a digital watermark or digital signature, into a picture as it is being created. In the past, active techniques were employed by using digital signatures or data concealing (watermarking). When using the passive technique, a picture is created without any pre-existing information. This technique just analyses an image's binary content. [6]

Technologies such as digital watermarking and digital signatures serve as the foundation for active techniques for general visual content protection. Digital signatures are simple cryptographic techniques used to verify the bitstream. It is more suited for other uses, such copyright protection, because the authentication in this instance is weak, meaning that any modification to the bitstream renders the signature invalid. As modifications do not alter the semantics, this is not desired for confirming the semantic meaning of images. Stated differently,

the authentication process must be reliable. Another significant disadvantage is that the signature must be included with the picture as metadata, which means a malevolent user might remove it or perhaps even replace it [7].

The removal of copyright watermarks, the creation of false news, and the use of modified or falsified photos as evidence in court are just a few of the ways that these images are becoming more and more harmful, harming not only individuals but also society as a whole. As the Internet continues to grow rapidly, online social networks (OSNs) have taken over as the primary information transmission platforms, with a significant amount of photos. Naturally, a lot of fake photos are shared on different OSNs, greatly affecting people's perceptions of things like political concerns, commercial goods, vital papers (certificates), etc.

In order to guarantee the validity of the information, many techniques [8] have been put forth to identify and pinpoint picture forgeries. While some of these forensic approaches are intended to identify more complicated or compound forgeries, others are made to detect particular types of tampering, such splicing [9], copy-move [10], and inpainting[11].Few studies, nonetheless, have specifically addressed how to provide reliable forgery detection against lossy operations in the widely used OSN systems. Because these lossy procedures have the potential to significantly impair detection performance, this issue is crucial.

Due to its simplicity, picture forgery is frequently carried out at the pixel level, which encourages the widespread usage of pixel-based techniques for image forgery detection [12].Different portions of an image are duplicated and relocated to various positions inside the same picture in copy-move forgery. There is a substantial correlation between the properties of different portions of a picture. Either splitting an image into overlapping or disjoint chunks, or calculating local key points for the whole picture, are methods used to compute abrupt features. The process of extracting the most informative and manipulation-sensitive characteristics from an image's collection of features is known as feature extraction and feature selection. To detect any similarities, Feature Matching compares each block's chosen characteristics to each other [13].

Convolutional neural networks (CNNs) and machine learning have demonstrated in recent years that they can effectively learn their representations and extract complex statistical features, which enables them to generalize well across a wide range of computer vision tasks, such as

image recognition and classification. Training a convolutional neural network (CNN) on a dataset containing both authentic and forged photos is one method of deep learning-based image forgery detection. Based on the characteristics it has trained to identify, the CNN can then be used to categorize fresh photos as either authentic or manipulated [14].

As a sort of deep learning algorithm that can be trained to extract features from images and classify them into different categories, Convolutional Neural Networks (CNNs) have actually gained popularity as a tool for detecting fake images. CNNs are modelled after the human visual system and comprise multiple layers of interconnected neurons that perform convolution operations on the input image to extract features. Active methods require the capturing camera to have specific hardware and/or in-board post processing software in order to compute the watermark or signature on the unaltered version of the image, ideally at the acquisition level. Additionally, any entity interested in verifying the semantic content of a given image must be able to decode the authentication information, which requires having access to the watermark detector and/or the creator's (private or public) key. Nevertheless, leaving both the security information embedding and the decoding devices vulnerable to potentially malicious users is typically a threat to the entire system [15] .

3. DATASETS

Benchmarked picture forgery datasets are necessary in order to assess the effectiveness and validate the outcomes of various forgery detection techniques. A few publicly available datasets for picture splicing, image retouching, and copy-move forgeries are available. A brief overview of available datasets is provided below.

Copy-move forgery datasets:

The MICC-F2000, MICC-F220, MICC-F600, and CoMoFoD copy-move forgery datasets are available to assess the effectiveness of the copy-move forgery detection method. These datasets' modified images are created by copying tiny portions of the original image and relocating them to a different spot inside the same image. These tiny patches have undergone a variety of post-processing operations (such as rotation, scaling, translation, or their mix) in an effort to fully integrate them into the image. The MICC-F600 dataset contains the underlying facts pertaining to the copy-move forgeries, which are not included in MICC-F2000.

The 260 picture sets in the CoMoFoD [16] dataset are separated into two categories: small and large. There are five groupings of images. Each picture collection includes binary masks, colored masks, forged images, and genuine photos.

Image Splicing Datasets :

The first picture splicing dataset, known as the Columbia picture Splicing Detection Evaluation (CISDE) dataset, was produced by Columbia University's Digital Video and Multimedia Lab (DVMM) [17]. Grayscale photos make up the CISDE dataset. DVMM created the Columbia Uncompressed Image Splicing Detection, Evaluation (CUISDE) dataset for color pictures [18]. The Chinese Academy of Sciences, Institute of Automation (CASIA) provides another picture grafting dataset. The CASIA v2.0 dataset is an expanded version of the v1.0 dataset [19,20]. These datasets contain altered photos created by splicing at least two photographs together. Various post-processing techniques and geometric adjustments, including rotation, scaling, and concealing, are performed to the manipulated photos with the sole aim of leaving no visually apparent trace.

4. CONCLUSION

In recent years, photography has gained popularity due to the increased availability of cameras. Due to their rapid comprehension by the public, images have become an indispensable tool for communicating information and play a vital part in our daily lives. There are many tools available for picture editing; these tools are mostly designed to improve photographs; however these technologies are often used to create fake images in order to disseminate false information. Image forgery has thus grown to be a serious issue and cause for worry.

An overview of many passive picture forgery detection methods was presented in this research. Additionally, a comparison of several forgery detection methods is provided. Additionally, this document offers a variety of data sets that are used in the various forgery detection techniques. Additionally, this document offers a variety of data sets that are used in the various forgery detection techniques. Despite their potential, deep learning-based methods lack the strength to deliver satisfactory results in a variety of digital picture forensics applications. All of these characteristics require a significant amount of effort to be done.

REFERENCES

[1]E. Lin, C. Podilchuk, E. Delp, "Detection of image alterations using semi-fragile watermarks," Proc. SPIE, Security and Watermarking of Multimedia Content II, vol. 3971, 2000, pp. 152–163.

[2] Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no.3, 2013, pp. 226-245.

[3] S. Kumar, P. Das, and S. Mukherjee, "Copy-Move Forgery Detection in Digital Images: Progress and Challenges," International Journal on computer Science and Engineering, vol. 3, no. 2, 2011, pp. 652-663.

[4] O. M., Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," *Forensic Science International*, vol. 231, no. 1, 2013, pp. 284–295.

[5] J. Fridrich, D. Soukalm, J. Luka ´s ˇ, "Detection of copy-move forgery in digital images," Digital Forensic Research Workshop, Cleveland, OH, 2003, pp. 19–23.

[6] Lu S, Hu X, Wang C, Chen L, Han S, Han Y "Copy-move image forgery detection based on evolving circular domains coverage" Multimed Tools Appl: 1–26. (2022) 10.1007/s11042-022-12755-w.

[7] Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no.3, 2013, pp. 226-245.

[8] P. Zhuang, H. Li, S. Tan, B. Li, and J. Huang, "Image tampering localization using a dense fully convolutional network," *IEEE Trans.Inf. Forensics Security*, vol. 16, pp. 2986–2999, 2021.

[9] M. Huh, A. Liu, A. Owens, and A. A. Efros, "Fighting fake news: Image splice detection via learned self-consistency," in *Proc. Eur. Conf.Comput. Vis.*, 2018, pp. 101–117.

[10] J.-L. Zhong and C.-M. Pun, "An end-to-end dense-InceptionNet for image copy-move forgery detection," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2134–2146, 2020.

[11]A. Li *et al.*, "Noise doesn't lie: Towards universal detection of deep inpainting," in *Proc. 13th Int. Joint Conf. Artif. Intell.*, Aug. 2021, pp. 1–7.

[12] W. Sun, J. Zhou, L. Dong, J. Tian, and J. Liu, "Optimal pre-filtering for improving Facebook shared images," *IEEE Trans. Image Process.*, vol. 30, pp. 6292–6306, 2021.

[13] SecurityAi Competition: Forgery Detection on CertificateImage. Accessed: Jan. 23, 2022. [Online]. Available: https://tianchi.aliyun.com/competition/entrance/531812/information

[14] R. Agarwal, D. Khudaniya, "Image Forgery Detection and Deep Learning Techniques: A Review," 4th International Conference on Intelligent Computing.

[15] Elaskily M, Elnemr H, Sedik A, Dessouky M, El Banby G, Elaskily O, Khalaf AAM, Aslan H, FaragallahO, El-Samie FA (2020) A novel deep learning framework for copy-move forgery detection inimages. Multimed Tools Appl

[16] D. Tralic, I. Zupancic, S. Grgic, M. Grgic, *CoMoFoD - New Database for Copy-Move Forgery Detection*, in Proc. 55th InternationalSymposium ELMAR-2013, pp. 49-54, 2013.

[17] T.-T. Ng and S. Chang, *A Data Set of Authentic and Spliced Image Blocks*, Columbia University Technical Report, 2004.

[18] J. Hsu and S.-F. Chang, *Columbia Uncompressed Image Splicing Detection Evaluation Dataset*,Available:http://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/.

[19] W. Wang and J. Dong, *CASIA v1.0, Tampered Image Evaluation Database*, Available: http://forensics.idealtest.org/casiav1/.

[20] W. Wang and J. Dong, *CASIA v2.0, Tampered Image Evaluation Database*, Available: http://forensics.idealtest.org/casiav2/.