DETECTION OF RECOLORING AND COPY-MOVE FORGERY INDIGITAL IMAGES

[1]Binnar Nikita, [2]Gaikwad Tejaswini, [3]Naik Ravina, [4]Sadgir Sarita

Student,
Shatabdi Institute of Engineering & Research, Nashik, Maharashtra

Abstract - Capturing images has been increasingly popular in recent years, owing to the widespread availability of cameras. Images are essential in our daily lives because they contain a wealth of information, and it is often required to enhance images to obtain additional information. A variety of tools are available to improve image quality;nevertheless, they are also frequently used to falsifyimages, resulting in the spread of misinformation. This increases the severity and frequency of image forgeries, which is now a major source of concern. Numerous traditional techniques have been developed over time to detect image forgeries. In recent years, convolutional neural networks (CNNs) have received much attention, and CNN has also influenced the field of image forgery detection. However, most image forgery techniquesbased on CNN that exist in the literature are limitedto detecting a specific type of forgery (either image splicing or copy-move). As a result, a technique capable of efficiently and accurately detecting the presence of unseen forgeries in an image isrequired., we introduce a robust deep learning based system for identifying image forgeries in the context of double image compression. Thedifference between an image's original and recompressed versions is used to train our model. The proposed model is lightweight, and its performance demonstrates that it is faster than state-of-the-art approaches. The experiment results are encouraging, with an overall validation accuracy of 92.23

***Keywords*: Convolutional neural networks; neural networks; forgery detection; image compression; image processing**

INTRODUCTION

With the advent of digital cameras and other smart devices, it has become easy for anyone to manipulate an image. Some manipulations are not harmful, such as changing the brightness of an image or converting it to black and white. On the other hand, some manipulations can cause harm to others and defame them, especially politicians and celebrities. Image forgery is the process of manipulating a digital image to hide valuable oressential content or to force the viewer to believe an idea [1]. It has been defined as the process of manipulating an original digital image to either conceal its original identity or create an entirely different image than what was originally intended bythe user of the digital platform [2]. Forged images can cause disappointment and emotional distress andaffect public sentiment and behavior [3]. Images cantransmit much more information than text. People tend to believe what they can see, and this affects their judgment, which leads to a series of unwanted responses. Because fabrications have become widespread, the urgency to detect forgeries has significantly increased. It serves to distort information, spread immorality and fake news,obtain money fraudulently from an unsuspecting audience, ruin the reputation of a popular celebrityor any other public figure, and spread adverse political influence among the users of a digital platform. Therefore, clear authentication of images and videos uploaded to digital media platforms, before they are used in any way, makes it moredifficult for digital information users to shareinformation [4]. Image forgery is often used by malicious people to ruin the reputation of publicfigures. Image forgery, especially through Photoshop, can be used to display unethical behavior in public figures. It is also sometimes an attempt to influence consumers of the goods produced or the services offered by these publicfigures to shift to other markets [5]. This forgery could also be used for political reasons against opponent politicians or their agents, spreadingimages that portray their immoral side. This aims to convey a message to the public regarding the lack ofintegrity of the subject. Image forgery often leads to emotional problems for those whose images are released to public websites in disregard for theirprivacy. There have been reports of suicide due to the leaking of private images to public digital platforms, after which the victims undergo significant rebuke. These deaths negatively affect society. Image forgery is also sometimes used to cheat victims of their money in increasingly common fraud schemes. The forged images are uploaded with embedded text, purportedly from the owner of the original image, with instructions that end in innocent people losing money. This is also done with images portraying people who are in dire need of help, with intentions of fraudulently acquiring money from unsuspecting members of the public. Society then ceases helping even those who are in genuine need of help because of the fear of being swindled. For all of these reasons, it is vital to develop methods of detecting whether an image is forged and to locate the region of manipulation.

LITURATURE SURVEY

1. Yerushalmy et al. [1] suggested a new approach for the detection of image forgery. This technique is not adding digital watermarking in the images and does not compare the images for training and testing. The authors proposed that image features extracted during the acquisition phase are themselves proof of authenticity of the image. Thesefeatures are often visible to the naked eye. Specifically, it uses image artifacts caused by various irregularities as markers to determine image validity. [1] 2. Ahmet et al. [3] proposed a techniquefor detecting image tampering using a color filter array. It computes a single feature and a simple threshold-based classifier. The authors tested their approach with authentic, computer-generated, andtampered images. The experimental analysis showedlow error rates.[3] 3. Bi et al. [2] D. Cozzolino et al.

[4] proposed a new technique for the detection of image splicing using a feature-based algorithm. In this technique, the co-occurrence of images is usedto compute local features. Those local features are then used to extract feature parameters. Since spliced and host images can exhibit different properties, the expectation– maximization algorithm, together with the segmentation, is used for learning purposes. In view of the above studies, most of the techniques used for forgery detection arebased on handcrafted methods for feature extraction,which are highly dependent on the individualundertaking the task. The development of deep learning-based methods has led to automatic feature extraction. The use of deep learning thus removes possible human errors and increases the efficiency and reduces the time complexity of the model.[3] 4.
D. Cozzolino et al. [4] proposed a new technique forthe detection of image splicing using a feature-basedalgorithm. In this technique, the co-occurrence of images is used to compute local features. Those local features are then used to extract feature parameters. Since spliced and host images can exhibit different properties, the expectation– maximization algorithm, together with the segmentation, is used for learning purposes. In view of the above studies, most of the techniques used forforgery detection are based on handcrafted methods for feature extraction, which are highly dependenton the individual undertaking the task. The development of deep learning-based methods hasled to automatic feature extraction. The use of deep learning thus removes possible human errors andincreases the efficiency and reduces the time complexity of the model.[4] 5. Salloum et al. [5] suggested the use of a multitasking fully connected network. Since a singletask fully connected network has irregular output, the proposed technique per-formed better compared to the single-task fully connected network. The authors proposed amultitask fully connected network comprising a collection of output streams. One of these streams acquires the surface label, while the interface sectionedge is acquired by the next one.[5]

MOTIVATION

This project provides two level analysis for the image. At first level, it checks the image metadata. Image metadata is not that much reliable since itcan be altered using simple programs. But most of the images we come across will have non-altered metadata which helps to identify the alterations

SYSTEM ARCHITECTURE

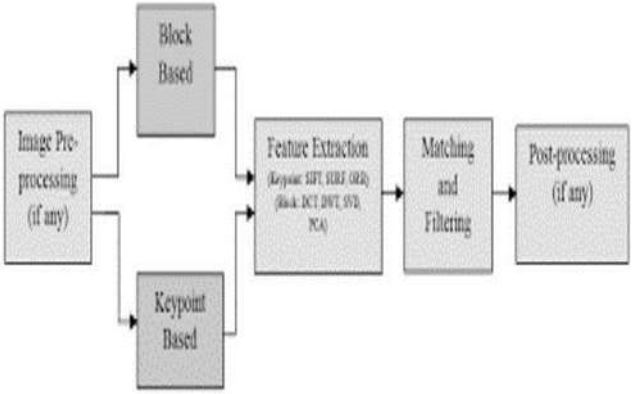

Fig -1: System Architecture Diagram

APPLICATION:

1. Legal Evidence.
2. Forensics Investigations.

FUNCTIONAL & NON-FUNCTIONALREQUIREMENTS

Functional requirements: may involve calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describe all the cases where the system uses the functional requirements; these are captured in use cases.
Nonfunctional Requirements: (NFRs) define system attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system across the different backlogs.

Functional requirements

- Registration
- User Login
- Creation of database: Users MandatoryInformation

Design Constraints:

1. Database
2. Operating System

3. Web-Based Non-functional RequirementsSecurity:
1. User Identification
2. Login ID
3. Modification Performance Requirement:
1. Response Time
2. Capacity
3. User Interface
4. Maintainability
5. Availability

SYSTEM REQUIREMENTS

Software Used:

1. OperatingSystem: Windows xp/7/8/10
2. Programming Language: Python
3. Software Version: Python 4.4
4. Tools: Anaconda/pycharm
5. Front End: Python

Hardware Used:

1. Processor - Pentium IV/Intel I3core
2. Speed - 1.1 GHZ
3. RAM - 512 MB(min)
4. Hard disk - 20 GB
5. Keyboard - Standard Keyboard
6. Mouse - Two Or Three ButtonMouse
7. Monitor - LED Monitor

CONCLUSION

The present work demonstrates that, by employing different CNN architectures, deep learning can be successfully applied in tasks such as image classification, image identification and objectrecognition. Cost-effective image classification is achieved on manipulated and/or larger datasets, and improved image feature mapping are obtained from similar images in text metadata using CNNs. However, although using feature map representations is shown to be cheaper and faster, it does not improve the quality of the image classifications, indicating that this approach is not optimal for evaluating quality, given the weak correlation between feature labels and similar (and/or non-) images. Nevertheless, the results ofthe present work could lead to future investigations that include looking at other forms of forgery detection by applying the newly transfer learned weights. Overall, the present work indicates that metadata sampling and classification requires highlydisciplined scaling model which can be scored by employing pre-trained model with and that can be a future extension steps to this work

REFERENCES

[1] M. Sridevi, C. Mala, and S. Sanyam, “Comparative study of image forgery and copy-move techniques,” in Advances in Computer Science, Engineering Applications, D. C. Wyld, J. Zizka, and D. Nagamalai, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 715–723.

[2] S. Walia and K. Saluja, “Digital image forgery detection: a systematic scrutiny,” Australian Journal of Forensic Sciences, pp. 1–39, 03 2018.

[3] C. Shen, M. Kasra, W. Pan, G. A. Bassett, Y.Malloch, and J. F. OBrien, “Fake images: Theeffects of source, intermediary, and digital medialiteracy on contextual assessment of imagecredibility online,” New Media Society, vol. 21, no.2. pp. 438–463, 2019. [Online].Available:https://doi.org/10.1177/1461444818799526.C. N. Bharti and P. Tandel, “A survey of image forgery detection techniques,” 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp.877–881, 2016.

[4] C. Salge, “Is that social bot behaving unethically?” Communications of the ACM, vol. 60,pp. 29–31, 08 2017.

[5] J. Bunk, J. H. Bappy, T. M. Mohammed, L.Nataraj, A. Flenner, B.S. Manjunath, S.Chandrasekaran, A. K. Roy-Chowdhury, and L.Peterson, “Detection and localization of imageforgeries using resampling features and deeplearning.” in CVPR Workshops. IEEE ComputerSociety, 2017, pp. 1881–1889. [Online].
Available:http://dblp.unitrier.de/db/conf/cvpr/cvprw2017.html BunkBMNFMCRP17

[6] Y. Abdalla, M. Iqbal, and M. Shehata, “Imageforgery detection based on deep transfer learning,”European Journal of Electrical Engineering and 36Computer Science, vol. 3, no. 5, Sep. 2019.[Online].
Available:https://ejece.org/index.php/ejece/article/view/125

[7] J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath, and A. K. Roy-Chowdhury, “Hybrid lstm and encoderdecoder architecture for detectionof image forgeries,” IEEE Transactions on Image Processing, vol. 28, no. 7, pp. 3286–3300, July 2019.