Literature Review on Image Forgery Detection Techniques

Sonali Gaikwad[1] and Zainab Mizwan[2]

[1]Assistant Professor, VIVA Institute of Technology, University of Mumbai, MS, India
[2]Assistant Professor, Shree L. R. Tiwari College of Engineering, University of Mumbai, MS, India
E-mail: sonalipgaikwad85@gmail.com, zainab.mizwan@slrtce.in

Manuscript Details

Available online on https://www.irjse.in
ISSN: 2322-0015

Editor: Dr. Arvind Chavhan

Cite this article as:
Sonali Gaikwad and Zainab Mizwan. Literature Review on Image Forgery Detection Techniques, *Int. Res. Journal of Science & Engineering*, 2024, Special Issue A14: 7-13. https://doi.org/10.5281/zenodo.12699229

Article published in Special issue of National Conference on Machine Learning and Data Science (NCMLDS-2024)" organized by College of Computer Science and Information Technology (COCSIT) Ambajogai Road, Latur, Maharashtra, India on date April 16th to 17th 2024

Abstract

Image forgery is the manipulation or alteration of an image. Image forensic is an emerging field since digital images are used in legal proceedings. Image forgery raised the demand to assure the truthfulness of digital image. Popularity of many editing software's lead to manipulation of an images in different ways which cannot be recognized by the naked eye. Therefore, image forgery detection techniques play an important role. Image splicing and copy-move forgery are the most widely used image forgery tools. This paper, will give an analysis of various active and passive methods of an image forgery detection. Passive techniques of forgery detection do not require any pre-embedded information about the image. Previous research studies shown that Convolutional Neural Networks can achieve the art of state performance in some visual problems. Thus, deep learning-based CNN models are preferred for forgery detection in digital images. In this paper a novel method is proposed to classify forged image and original image via Error Level Analysis using deep learning. Compression ratio of the original and forged image compression is different. Error Level Analysis (ELA) is applied on CNN model which analyses this compression ratio of original image and forged image.

Keywords - Image forgery, image forgery detection, Convolutional Neural Networks, Deep learning, Error level analysis

Introduction

The main objective of this paper is to present various methods of image forgery detection. Several active and passive methods are available to detect a forged image. Digital images play a crucial role in field like criminal investigation, forensic, medical imaging etc. Due to the advancement in digital technology images can be easily processed using various advanced tools like Corel, Adobe Photoshop, etc. Images are exploited in a large range of use cases where determining their integrity and origin may have high consequences. Alteration of an image using different tools is considered as image forgery. Some of the most commonly used forgery techniques are copy move, image splicing and image retouching This emphasized the importance of authenticity of an image. As a result, image forgery detection techniques are gaining concern and importance in the society.

Image forensic is a field of digital forensic that deals with image forgery detection and validation. It is an emerging field that seeks to establish the origin and validity of digital media. It works for the detection of the originality of images or videos so that major ramifications on a national and worldwide level due to forgery can be controlled.

Literature review

Digital image forgery detection techniques are classified into two categories such as active approach and passive approach. In the active approach, certain information is embedded inside an image during the creation in form of digital watermark or digital signature. Active approaches were used traditionally by employing data hiding (watermarking) or digital signatures. In the passive approach, there is no pre-embedded information inside an image during the creation. This method works purely by analyzing the binary information of an image. [1]

Active approach

An active forgery detection method needs pre-extracted or pre-embedded data. In active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. [2] Active approaches are used in limited application since pre-processing is required. A Digital signature and Digital watermarking are commonly known methods used in active approach

Digital watermarking

In an active approach, the first phase consists of pre-processing technique that is watermark injecting. Watermarking is also used for image forgery detection. These watermarks are designed to be undetectable, or to blend in with natural camera or scanner noise. Watermarking involves injecting a special pattern into the owner (source) image so that piece of information gets authorized. This special pattern can be further used to notify the user either the image is tampered or not. Active techniques have some disadvantages because they required some human involvement or specially equipped cameras. Also large portion of the imaging application does not contain any watermarking or mark module. To overcome this drawback a passive authentication has been proposed.

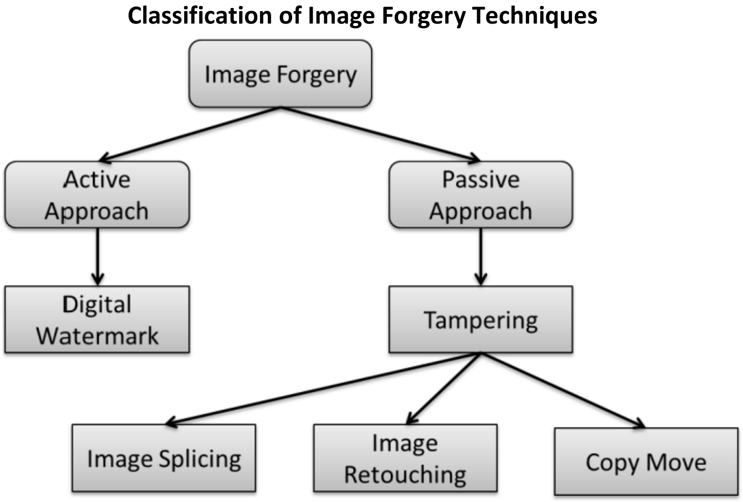

Fig.1. Classification of Image Forgery Techniques [21]

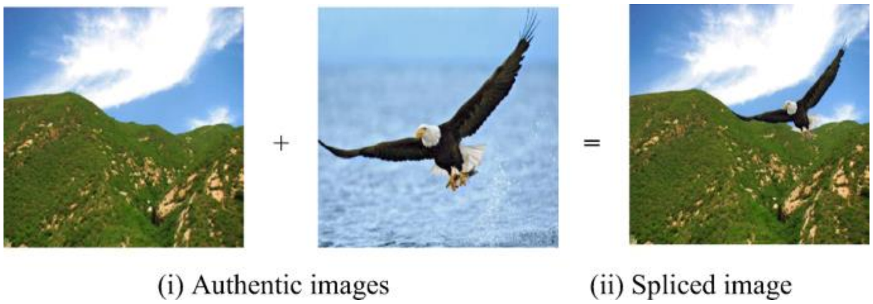

Fig.2.Example of Image splicing type image forgery [22]

Discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete sine transform (DST), and singular value decomposition (SVD) [3] are common transforms applied in frequency domain watermarking. In recent years, these transforms are still applied widely in the watermarking field. Luo et al. [4] presented an adaptive robust watermarking scheme based on discrete Fourier transform (DFT) and SIFT to deal with the synchronization errors.

2.1.2. Digital signature

Digital signature is one of the active methods used for detecting image forgery or tampering. This one is mathematical approach applied to confirm the integrity and authenticity. Representing the authenticity of digital document using a kind of mathematical format is named as digital signature. In digital signature a robust bit is extracted from the original image. An image is partitioned of into blocks of 16*16 pixels. A secret key k is employed to get N random matrices with entries uniformly distributed in interval [0, 1]. A low pass filter is applied on every random matrix frequently to obtained N random smooth pattern [5]. System produce digital signature by applying signing process on digital image.

2.2. Passive Approach

Passive image forensics is usually a great challenge in image processing techniques. There is not a particular method that can treat all these cases, but many methods each can detect a special forgery in its own way. The localization of tampering is solely based on image feature statistics. Hence, algorithms and methods of detection and localization of image based on passive tampering vary depending upon the type of security construct used. Nevertheless, passive tampering detection typically aims for localization of tampering on raw image.

2.2.1. Image splicing:

This is a manipulation technique that copies one or many regions of an image and pastes them onto another image. It can be used for the purpose of adding an additional element to a scene. Image Splicing is a process of making a composite picture by cutting some object from image and adding it to some other image. Image splicing is fundamentally simple process and can be done as crops and pastes regions from the same or separate sources. In Image Splicing technique there is composition of two or more images, which are combined to create a fake image.

2.2.2. Copy-move forgery:

Copy Move forgery is a process of making a composite picture by cutting some object from image and adding it to the same image. It can be used for the purpose of adding false information or hiding information. It is one of the most common image tampering techniques, and it’s also one of the most difficult to spot because the cloned image is taken from the same image. A section of an image is copied and pasted to another part of the same picture in Copy-Move image forgery. In the Copy-Move image, manipulation technique a part of the same image is copied and pasted into another part of that image itself. In a copy-move attack, the intention is to hide something in the original image with some other part of the same image [6]. The example of Copy-Move type is as shown below.

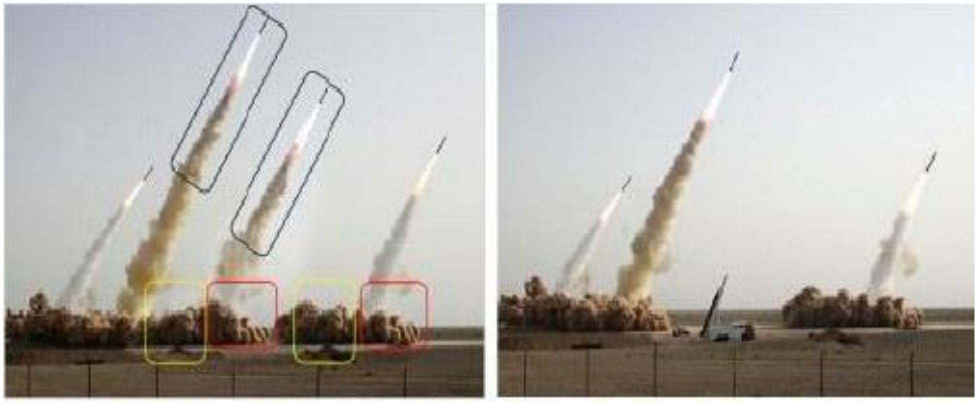

Fig.3.Example of copy-move type image forgery [23]

Table1: Comparative study on existing copy-move image forgery detection methods

Sr. No.	Title of the paper	Method used	Type of forgery detection	Pros/cons	Publishing year
1	Detection of copy-move forgery in digital image [9]	DCT	Copy-move region is detected	Will not work in noisy image	2003
2	Robust detection of region duplication in digital image [10]	Similarity matching	Copy-move region detected in noisy conditions	Time complexity is reduced	2006
3	A new approach for detecting copy-move forgery detection in digital image [11]	DWT	Exact copy-move region is detected	Works well in noisy and compressed image	2008
4	Fast, automatic and fine-grained tempered JPEG image detection via DCT coefficient analysis [12]	Double Quantization DCT	Tampered region is detected accurately	Works only in JPEG Format	2009
5	Detecting copy-paste forgeries using transform-invariant features [13]	Transform-invariant features	Copy-paste forgery detection	Difficult detection in case of blurred image	2011
6	A fast image copy-move forgery detection method using phase correlation [14]	Phase correlation C	Copy move region detected	Valid in detecting the image region duplication and quite robust to additive noise and blurring	2012
7	Copy-move forgery detection in imagesvia2D-fourier transform [15]	2D- Fourier transform	Copy-move region detected accurately	This work detects multiple copy move forgery and it also robust to jpeg Compression attacks hence highly accurate	2013
8	A scheme for copy-move forgery detection in digital images based on2D-DWT [16]	2D-DWT	Copy- move region is detected	Works well in noisy and compressed image	2014

Lu S. [7] proposed a new scheme that makes use of the circular domain coverage (ECDC) algorithm. The proposed scheme combines forgery detection methods based on blocks and key points. First, from an entire image, speed-up robust features(SURF) in log-polar space and scale-invariant feature transform (SIFT) are extracted. Second, generalized two nearest neighbors (g2NN) are used to generate a large number of matched pairs.

Rani et al. [8]. This research proposes a pixel-based forgery detection framework for copy-move and splicing-based forgeries. Initially, image data is pre-processed to improve the textural information. For the identification of bogus picture regions, the suggested method estimates multiple attributes using augmented SURF and template matching.

2.2.3. Image Retouching:

Image Retouching is considered as less harmful kind of digital image forgery than other types present. In case of image retouching original image does not significantly change, but there is enhancement or reduces certain feature of original image. This technique is popular among magazine photo editors they employ this technique to enhance certain features of an image so that it is more attractive. Actually, the fact is that such enhancement is ethically wrong. Image retouching is adding or removing something from the image for enhancing features of an image. Compared to all available forgery techniques Image Retouching is considered as less harmful. Removing blemishes on a picture of a model would be a great example of image Retouching.

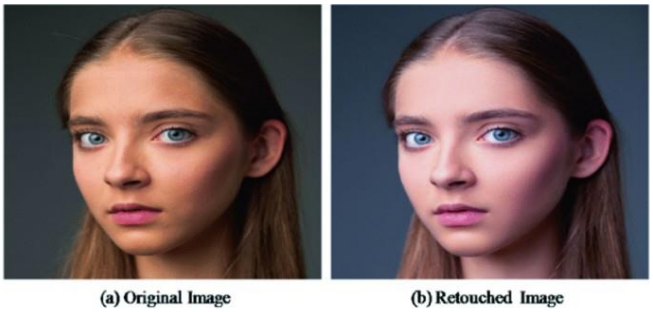
(a) Original Image (b) Retouched Image

Fig.4.Example image retouching type of image forgery [24]

Xing et al. [17] describe a new algorithm based on an 8-neighborhood quick sweeping technique. The experimental result shows that there is a significant increase in the rate of the image in painting while maintaining quality effect.

2.3. Deep learning models:

In recent years, machine learning and neural networks, such as convolutional neural networks(CNNs), have shown to be capable of extracting complex statistical features and to efficiently learn their representations, allowing to generalize well across a wide variety of computer vision tasks, including image recognition and classification and so on.

One approach to image forgery detection using deep learning is to train a convolutional neural network (CNN) on a dataset of both genuine and forged images. The CNN can then be used to classify new images as either genuine or forged based on the features it has learned to recognize [18]. This paper presents a deep learning-based approach to image forgery detection, specifically using Error Level Analysis (ELA) with Convolutional Neural Networks (CNNs) and a pre-trained VGG-16 model. The study compares the performance of the two models and provides an in-depth analysis of the results. The experiments show that the ELA CNN model achieves a remarkable accuracy rate of 99.87% and correctly identifies 99% of invisible images, while the VGG16 model achieves a lower accuracy rate of 97.93% and a 75.87% validation rate. The research highlights the significance of using deep learning techniques in image forgery detection and explores the implications of the findings. A primary method in image forgery detection is the Error Level Analysis (ELA), a technique that quantifies the compression levels across an image Error Level Analysis (ELA), a passive method for finding fake images, assesses how consistently different levels of compression are used throughout an image. The compression levels of the edited area in an image are frequently different from the surrounding portions. ELA draws attention to these discrepancies, which makes it simpler to spot forgeries [19].

Sudiatmika, I.B.K. and Rahman et al [20] using DL to solve the statement of discriminate between original images and forged images. Proposed a system of the combination of Error Level Analysis (ELA) and used the transfer learning model called Visual Geometry Group (VGG). With 100 epochs, results showed the 92.2% and 88.46% of training and validation accuracy respectively.

advantage of these CNN based approaches is that they are capable of learning classification features directly from image data.

Conclusion

The main objective of this paper is to present various aspect of image forgery detection. Various active and passive image forgery detection methods are highlighted in this paper. From the literature survey, we observed that the Active method needs an information to be incorporated inside an image. Digital watermark and digital signature are widely used active methods. In the passive approach, there is no need to incorporate information inside an image during the creation. In this paper we presented a step forward into adopting convolutional neural networks for the task of detecting splicing forgery. We began to explore CNN capabilities to classify and localize uncompressed, single and double compressed patches of images. First, the choice of the CNN architecture can lead to very different performance as it was seen on the object classification task where deep architectures are used. The ELA-CNN model successfully incorporated the benefits of Convolutional Neural Networks and Error Level Analysis preprocessing, obtaining a remarkable validation accuracy.

References

1. H. Farid, “A survey of image forgery detection,” IEEE Signal Process.Mag., Vol. 26, no. 2, pp. 16-25, (2009).
2. 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.
3. Qi, X.J.; Xin, X. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J. Vis. Commun. Image Represent. (2015), 30, 312–327.
4. Luo, H.J.; Sun, X.M.; Yang, H.F.; Xia, Z.H. A robust image watermarking based on image restoration using SIFT. Radio engineering (2011), 20, 525–532.
5. Fridrich J, “Robust bit extraction from images.” IEEE international conference on in multimedia computing and systems, (1999), pp. 536-540.
6. B. Mahdian and S. Saic, “Detection of copy-move forgery using a method based on blur moment invariants,” Forensic science international, vol. 171, no. 2, (2007) , pp. 180–189.
7. 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.
8. Rani A, Jain A, Kumar M. Identification of copy-move and splicing based forgeries using advanced SURF and revised template matching. Multimed Tools Appl. (2021);80(16):23877–23898. doi: 10.1007/s11042-021-10810-6.
9. I. Amerinietal., “A SIFT-based forensic method for copy-move attack detection and transformation recovery,” IEEE Trans. Inf. Foren. Sec., Vol. 6, no3, pp.1099-1111, (2011).
10. W.Q. Luo, J.W. Huang, and G.P. Qiu, “Robust detection of region duplication forgery in digital image,”18th International Conference on Pattern Recognition(ICPR), (2006), Vol.4, pp.746-749.
11. J. Zhang, Z. Feng, and Y. Su, “A new approach for detecting copy-move forgery in digital images,” IEEE International Conference on Communication Systems, China, (2008), pp.362-366.
12. Z. Linet al., “Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis”, Vol.42, pp.24922250, (2009).
13. P. Kakar and N. Sudha, “Detecting copy-paste forgeries using transform invariant features,” IEEE 15th International Symposium on Consumer Electronics(ISCE), Singapore, (2011), pp.58-61.
14. B. Xu, G. Liu and Y. Dai, “A Fast Image Copy-Move Forgery Detection Method Using Phase Correlation, “Fourth International Conference on Multimedia Information Networking and Security, Nanjing, (2012), pp.319322.
15. S. Ketenci and G. Ulutas, “Copy-move forgery detection in images via 2D-Fourier Transform,”36th International Conference on Telecommunications and Signal Processing(TSP), (2013) ,Rome,2013, pp.813-816.
16. S.A. Fattah, M.M. I. Ullah, “A scheme for copy-move forgery detection in digital images based on 2D-DWT,” IEEE57th International Mid-West Symposium on Circuits and Systems (MWSCAS), College Station, TX, (2014), pp.801-804.
17. Xu J, Feng D, Wu J, Cui Z “An image in painting technique based on 8-neighborhood fast sweeping method.” In:2009 WRI International Conference on Communications and Mobile Computing, (2009 , pp 626–630.
18. R. Agarwal, D. Khudaniya, "Image Forgery Detection and Deep Learning Techniques: A Review," 4th International Conference on Intelligent Computing and

Control Systems (ICICCS), Madurai, India, (2020), pp. 1096-1100, doi: 10.1109/ICICCS48265.2020.9121083.

19. Sharma, S., & Yadav, S. Image forgery detection using error level analysis and deep learning. Research gate (2019).
20. I. B. K. Sudiatmika et al, "Image forgery detection using error level analysis and deep learning," Telkomnika, vol. 17, (2), pp. 653-659, (2019).
21. N.Parashar, N.Tiwari "A survey of digital image tampering techniques", International journal of signal processing, image processing and pattern recognition, October (2015).
22. Navneet Kaur, Neeru Jindal "A passive approach for the detection of splicing forgery in digital images", Research Gate, (2020).
23. Hashmi, Mohammad Farukh "Passive Detection of Copy-Move Forgery using Wavelet Transforms and SIFT Features" Journal of Information Assurance and Security(JIAS) ISSN 1554-1010, (2018).
24. Kaur, H., Agrawal, S., Dhindsa, A. "An Improvement in Dense Field Copy-Move Image Forgery Detection" International Conference on Paradigms of Computing, Communication and Data Sciences. Algorithms for Intelligent Systems, doi.org/10.1007/978-981-15-7533-4_25, February (2021).

Conflicts of interest: The authors stated that no conflicts of interest.

Publisher's Note
IJLSCI remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Correspondence and requests for materials should be addressed to Sonali Gaikwad.

Peer review information
IRJSE thanks the anonymous reviewers for their contribution to the peer review of this work. A peer review file is available.

Reprints and permissions information is available at https://www.irjse.in/reprints