Review of Copy-Move Image Forgery Detection

Amit Kumar [a], Namita Tiwari [a] and Meenu Chawla [a]

[a] *Maulana Azad National Institute of Technology Bhopal, M.P, Bhopal, India*

Abstract

In today's technology world, digital photographs serve a critical function in a variety of fields. Using advanced photo editing tools, altering and rearranging the contents of a digital image is a simple operation. Now it is possible to add, edit, or eliminate essential aspects from such an image without behind any perceptible alterations. Copy-move forgery is now the most frequent type of image manipulating in digital pictures, in which an item or region is duplicated in the digital image. Forgery detecting and localization are two major areas of study in digital forensics that have gotten a lot of attention. This paper reviews various techniques for copy- move image forgery detection using the deep learning method.

Keywords

Image, Copy Move Forgery, deep learning, Convolutional neural network.

1. Introduction

Images are now utilized as one of the most valuable assets of information in different disciplines, including medicine, education, digital forensics, health research, and sources of information. It's simple to make a cast image with tools like Adobe, GIMP, Coral Draw, and Mobile applications like Image Hacker. When a photograph has been used as evidence in courts of law, the authenticity of the image becomes extremely important [1]. These created pictures have the possibility to have a great impact on society and affect people's opinions. Social media campaigning has now become a new trend in elections all over the world in recent years. On the plus side, digital images are often used to increase election awareness. Simultaneously, faked photographs containing false information have been noticed being shared on social media in an attempt to influence the public. Furthermore, some faked images with misleading information concerning the COVID-19 epidemic have lately gone popular on social media networks. [2]

[1] Digital image counterfeiting is one of the most widespread and developing criminal issues. There are currently no adequate approaches for automatically verifying the trustworthiness of digital photographs. Detecting fraud in digital photos is an emerging study area for verifying the legitimacy of digital photographs. [3]. There are two types of digital image forgery detection approaches first is an active method and the second one is a passive method. The active method retrieves features of the image that is otherwise obscured. Watermarking and digital signatures are used to hide confidential messages. In a picture, passive techniques identify the duplicate region, such as image splicing and copy-move forgeries. There are two methods for detecting manipulation in the copy- move forgery detection first one is the traditional technique and the second one is the deep learning technique. However, the old approach does not function consistently over different manipulating methods. [4]

WINS-2022: Workshop on Intelligent Systems, April 22 – 24, 2022, Chennai, India.
EMAIL: amitbcebhagalpur@gmail.com (Amit Kumar)
ORCID: 0000-0002-2010-3707 (Amit Kumar)

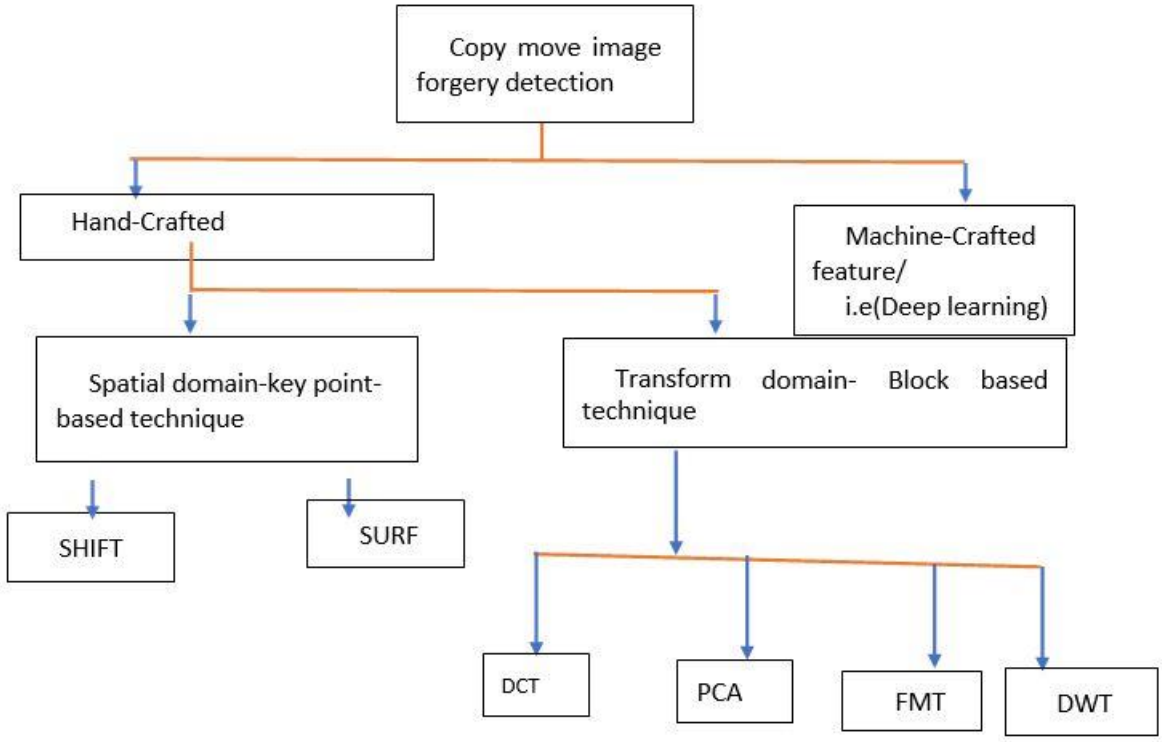

Figure 1: Copy-move Image forgery detection approach

2. Traditional Techniques

Paragraph In copy-move manipulating, an area of the picture (of any size) is picked for copy-move action and placed in another section with the same picture. As a result, there will be a strong association between such two areas. The copy-move tampering detection method's goal is to find replicated portions in a given picture. The repetition is shown by the similarity (correlation) or distance between characteristics derived from two separate sections of the picture. To retrieve region-wise characteristics from the picture, researchers used the following methods: (i) the image is split into tiny sections known as blocks, and characteristics for every block are retrieved, as proposed in (ii) all of the image's keypoints are recognized, and characteristics for each keypoint are retrieved. To generate similar blocks or similar keypoints pairs, the extracted characteristics are compared block-by-block or keypoint-by- keypoint. If matching pairings are detected between two locations, the duplication is confirmed, and the picture is categorized as tampered with. These methods are based on the assumption that the modified region is large enough to hold numerous blocks or key points.[5] suggested utilising the Fourier-Mellin Transform (FMT) to features extracted from picture frames. Furthermore, the author makes an effort to minimize response time, which has increased detection performance by employing counting bloom filters (CBF). the usage of the pixel matching concept, [6] suggested a Discrete Wavelet Transform (DWT) for efficient detection of copy-move forgeries. The approach is based on recursively analysing segmented sub-images in order to detect spatial-temporal regions of copy-move image forgeries.

[7] used the Fourier Transform (FT) correlation coefficient as a measure of similarity between picture blocks in log-polar form. [8] developed the PatchMatch method, which finds approximate closest- neighbour matches among picture chunks efficiently.

[9] used a SIFT-based algorithm to build a method for detecting copy-move forgeries and restoration. This technique was then improved by introducing an upgraded resilient clustering phase based on the J-Linkage algorithm. These three innovative forensic detectors presented by [10] are capable of eliminating global and regional key points, as well as abnormalities or inconsistencies in key-point distribution following tampering. [17] presented speeding up robust features (SURF) as a

technique for detecting copy-move image forgeries, with SURF keypoints collected and matching with the KD-Tree algorithm.

3. Deep Learning technique in CMFD

The investigation of the community of deep learners is now considered as a wide and evolving networkof researchers who have influenced each other through various ways or methodologies. Various forensic researchers are seeking to apply a deep convolutional neural network as an image forgery detecting method [18], and this technique is influencing digital image forensics as well. The technique of learningan artificial neural network (ann) by layering deeper layers on top of each other is known as deep learning (DL). Multi-layered information representations, which generally take the shape of a neural network with far more than two layers, are the most essential element of deep learning. Such strategies allow for the automated generation of data descriptors or characteristics at a higher level based on the lower ones.[19] developed a median filtering detection technique based on a deep learning approach depending on CNN, which allows the system to detect and retrieve features from images dynamically. The suggested CNN varies from other standard CNN models in that the CNN's initial layer architectureis a filtering layer. This filtration layer accepts a picture as inputs and outputs of its residual filtering of the media (MFR). Using layers that alternate between convolution and pooling, the approach gets various features for subsequent classification, allowing hierarchical representations to be learned. Fivecommonly used picture datasets are put to use to assess the efficacy among the suggested model. In comparison to current technology, approaches, the suggested method exhibited considerable performance improvements, especially in order to identify copy-move image forgery. In JPEG compression, the approach may also identify median filtering and tiny picture chunks.

CNN used a deep learning technique for picture fraud detection, using RGB color images as input to construct hierarchical representations automatically. The CNN approach was created by the author to detect images that have been manipulated with using splicing and copy-move procedures. The suggested technique has a unique feature in that it uses a simple high-pass filter set to initialize the weight of the network's first layer, which is then used to calculate a spatially rich model's residual maps. The suggested technique makes a few major contributions. A supervised CNN is first taught to learn the information hierarchy aspects of the training image's modifying operations. The CNN's initial convolutional layer acts as a pre-processing module, suppressing the influence of picture contents as effectively as possible. The characteristics retrieved from an image are then used to scan the whole picture using a patch-sizes sliding window. Finally, in the framework's final layer, the SVM classifier is trained for binary classification using the generated feature representation, which might be real or modified. The suggested technique outperforms certain current picture fraud detection methods in terms of accuracy. [20] presented a CNN-based technique for copy-move image forgery detection. According to the results of the experiments, the suggested approach produces a suitable fake picture automatically generated via the use of the computer using a basic image under the copy-move manipulation technique. The strategy, however, is not resistant to copy-move picture fraud in a real-world scenario. Even if the suggested approach is not flawless, it is the first time CNN has been used to identify copy-move forgeries, and it has become a pioneer for further research in this sector. [21] employ a deep learning methodology for digital picture forgeries based on CNN, where the CNN methodology was refined and it has been built expressly to enable the identification of the traces left by the change. This approach is based on a modified traditional CNN architecture that includes a layer of filtering to guarantee that the major content of the input picture is suppressed.

It is capable of reducing textures and edges that cause visual interference. After removing the effect of unneeded data, It's feasible. to study the evidence left behind by the recommended smooth filtration in this manner. On a range of public datasets, the suggested CNN-based model outperforms several cutting-edge techniques, and it also performs well under a number of operational situations such as Filtering techniques including bilateral, average, and Gaussian. To detect copy-move image counterfeiting, a Convolutional Kernel Network (CKN) was developed. Based on data [22], It's a

patch- level CKN analysis. Among the most essential objectives in copy-move image forgery detection is for the feature extraction to be resilient against specific feature alterations. The proposed CKN method for copy-move image fraud detection and CKN based on GPU rebuilding, as well as the proposed key point distribution based on segmentation method for trying to generate uniform dispersion major facts and GPU-based adaptive over-segmentation, are all significant components of (COB). According to the results of thorough testing, the recommended CKN outperformed hand-crafted aspects and can also deliver great results when employing GPU-based CKN. [23] employed a convolution neural network- based coherent framework called dual-domain-based convolution neural networks (D-CNN). The suggested technique employs two sub-networks: Sub-SCNN and Sub-FCNN. Both sub-networks are connected to locate the areas where a transfer technique is in operation. The Sub-SCNN uses the statistical characteristics depending on three DWT levels as inputs to identify and locate picture counterfeiting, whereas the Sub-FCNN uses statistical parameters based on these three DWT frequencies as input. Using the characteristics of pre-trained Sub-SCNN and Sub-FCNN networks, the recommended approach generated greater accuracy and avoided a significant computational cost for such training stage whenever used to the D-CNN of the training stage.

Table 1: Comparison of image tampering detection methods based on deep learning

Author	Tampering Methods	Model	Datasets	Accuracy
Bayar et al. [11]	Median filtering, Gaussian blurring	CNN	Collected from 12 differentcamera models	99.10%
Amerini et al. [12]	Double JPEG compression, Cut paste	Multi-domain CNN	UCID (1338 Images)	95%
Chen et al. [13]	Median filtering, Cut-paste	CNN	15352 photos (NRCS Photo Gallery, BOSSbase 1.01, UCID, Dresden, BOSS RAW)	85.14%
Bondi et al. [14]	Cut-paste	CNN	Image Database of Dresden (16k images from 26 different cameras)	81% Detection Accuracy of localization is 82%.
Rao and Ni [15]	Cut-paste, Copy- move	CNN	Columbia grey DVMM, CASIA v1.0, CASIA v2.0	98.04%
Wang et al. [16]	Copy-move, Cut- paste	Mask Regional Convolution Neural Network (Mask R-CNN)	Cover, Columbia	93 percent precision on average (for cover) 97 percent precision on average (for Columbia)

4. Analysis and Findings

These are some key aspects discovered after a thorough examination of many study publications. The detection of tampering job concentrates on coarse-grained image analysis, whereas the task of localization concentrates on perfectly correct image processing. Tampering detection is more difficult than locating the image's modified region. Researchers have developed a number of ways for detecting tampering, but only a handful of them can pinpoint the modified region. Techniques for detecting

tampering that has been used in the past (both block-based and keypoint-based methods) rely on scustom-made products characteristics. The DL approach can automatically analyze conceptual and sophisticated features that are essential for identifying tampered regions. The DL models may be utilized for (i) The input is classified as binary picture into genuine (original) and manipulated classifications, as well as (ii) tampered region localization. CNN models were shown to have great accuracy in the both classifying tampered photos and producing fine-grained masks for locating tampered regions, according to the researchers. Deep training in networks, Alternatively, is challenging and needs much computing power and influence a huge dataset. Because the individual analyzing the manipulated image is unaware of the sort of forgeries used on the actual picture, detection that is particular approach may not be effective. There is a need for a forgery detection technology that can identify any sort of forgery. Researchers employ a variety of metrics to assess the efficacy of tamper detection techniques (Receiver Operator, F-measure, accuracy, precision, recall Factors MCC, IoU, ROC Curve, and so on). When evaluating the performance of various Algorithms for detecting tampering, consistent criteria (measures) must be employed. On a collection of original (genuine) and tampered photos, tampering detection's effectiveness methods are tested. The dataset must contain as many distinct types of original photos as feasible, as well as a range of various tampering techniques, in order to properly evaluate the algorithms. Several public datasets on image manipulation are accessible. However, the size of these datasets is insufficient, limiting DL-based tampering detection methods.

5. Conclusion

We presented a complete analysis of existing approaches for Copy-move detection image forgeries in this study, including both traditional and deep learning methods. The relevance of the approaches was reviewed, as well as the overall workflow or procedure of the method used. The essential processes fortraditional approaches are divided into two categories: block-based and keypoint-based. Deep learningtechniques are based on the principle of ensuring feature extraction in order to learn and instantaneouslyfulfil classification. According to the results of this survey, several of the deep learning fraud detection approaches outperformed other forgery detection systems. Furthermore, they are said to be more efficient, particularly when GPU-based technology is used. However, there are still significant drawbacks and limits to using deep learning to identify counterfeit. One of the drawbacks is data since there are few databases for images relevant to CMFD, but deep learning techniques demand a large amount of data, particularly for training and validation. Furthermore, the use of a deep learning technique to CMFD has yet to be extended. However, deep learning is rapidly being used in other domains such as object detection, diagnostic imaging, and remote sensing. Furthermore, picture forgery detection has limits when used to real-world images, multioperation of manipulating images, and homogeneous images. As a result, improved approaches are still needed to attain higher performance, efficiency, and the ability to cope in conjunction with obstacles that remain in the detection of image forgery using copy-move.

6. References

[1] Zhong, Jun-Liu, and Chi-Man Pun. "An end-to-end dense-inception net for image copy-move forgery detection." IEEE Transactions on Information Forensics and Security 15 (2019): 2134-2146.

[2] Rao, Yuan, Jiangqun Ni, and Huimin Zhao. "Deep Learning local descriptor for image splicing detection and localization." IEEE Access 8 (2020): 25611-25625.

[3] Rhee, Kang Hyeon. "Generation of novelty ground truth image using image classification and semantic segmentation for copy-move forgery detection." IEEE Access 10 (2021): 2783-2796.

[4] Bappy, Jawadul H., et al. "Hybrid LSTM and encoder–decoder architecture for detection of image forgeries." IEEE Transactions on Image Processing 28.7 (2019): 3286-3300.

[5] Yan, Yanyang, Wenqi Ren, And Xiaochun Cao. "Recolored image detection via a deep discriminative model." IEEE Transactions on Information Forensics and Security 14.1 (2018): 5-17.

[6] Shabanian, Hanieh, And Farshad Mashhadi. "A New Approach for detecting copy-move forgery in digital images." 2017 IEEE Western New York Image and Signal Processing Workshop (WNYISPW). IEEE, 2017.
[7] Bravo-Solorio, Sergio, And Asoke K. Nandi. "Automated Detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics." Signal Processing 91.8 (2011): 1759-1770.
[8] Barnes, Connelly, et al. "Patchmatch: A randomized correspondence algorithm for structural image editing." Acm Trans. Graph. 28.3 (2009): 24.
[9] Amerini, Irene, et al. "A sift-based forensic method for copy-move attack detection and transformation recovery." IEEE Transactions on Information Forensics and Security 6.3 (2011): 1099- 1110.
[10] Costanzo, Andrea, et al. "Forensic Analysis of sift keypoint removal and injection." IEEE Transactions on Information Forensics and Security 9.9 (2014): 1450-1464.
[11] Bayar, Belhassen, and Matthew C. Stamm. "A Deep Learning Approach to universal image manipulation detection using a new convolutional layer." Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. 2016.
[12] Amerini, Irene, et al. "Localization of JPEG double compression through multi-domain convolutional neural networks." 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE, 2017.
[13] Chen, Jiansheng, et al. "Median Filtering Forensics based on Convolutional Neural Networks." IEEE Signal Processing Letters 22.11 (2015): 1849-1853.
[14] Bondi, Luca, et al. "Tampering Detection and localization through clustering of camera-based Cnn features." CVPR Workshops. Vol. 2. 2017.
[15] Rao, Yuan, And Jiangqun Ni. "A Deep Learning approach to detection of splicing and copy-move forgeries in images." 2016 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2016.
[16] Wang, Xinyi, et al. "Detection and localization of image forgeries using improved mask regional Convolutional Neural Network." Mathematical Biosciences and Engineering 16.5 (2019): 4581-4593.
[17] Bo, Xu, et al. "Image Copy-Move Forgery detection based on Surf." 2010 International Conference on Multimedia Information Networking and Security. IEEE, 2010.
[18] Kim, Dong-Hyun, and Hae-Yeoun Lee. "Image manipulation detection using Convolutional Neural Network." International Journal of Applied Engineering Research 12.21 (2017): 11640-11646.
[19] Chen, Jiansheng, et al. "Median Filtering Forensics based on Convolutional Neural Networks." IEEE Signal Processing Letters 22.11 (2015): 1849-1853.
[20] Liu, Ying, and Xiaomei an. "A Classification Model for prostate cancer based on Deep Learning." 2017 10th International Congress on Image and Signal Processing, Biomedical Engineering and Informatics (CISP-BMEI). IEEE, 2017.
[21] Shan, Wuyang, et al. "Robust Median Filtering Forensics using image deblocking and filtered residual fusion." IEEE Access 7 (2019): 17174-17183.
[22] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using sift algorithm." 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application. Vol. 2. IEEE, 2008.
[23] Shi, Zenan, et al. "Image Manipulation Detection and localization based on the dual-domain Convolutional Neural Networks." IEEE Access 6 (2018): 76437-76453