Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 1067–1073

IMAGE FORGERY DETECTION USING CONVOLUTIONAL NEURAL NETWORK ALGORITHM

Dr. Gowsic K[1], Vinayaka Moorthi M[2], Siranjeevi S[2], Viswa G[2]

[1] Associate Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Tamil Nadu, India
[2] Department of Computer Science and Engineering, Mahendra Engineering College, Tamil Nadu, India

Corresponding Author
Dr. Gowsic K,
kgowsic@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.2712

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The validity of photos is being called into doubt because to the availability of strong image modification tools. This is particularly problematic where images hold significant influence, such as in legal proceedings, news articles, or insurance claims. The rapid advances in science and technology have made it easier than ever to access a wealth of knowledge through a range of multimedia platforms. However, because it is so easy to alter the contents using a variety of editing programs, the authenticity and integrity of multimedia content are in jeopardy. Forensics technology is being developed to address this issue. We focus on blind image forensics tools for copy-move forgeries in this survey. Copy-move forgeries are among the most used methods for manipulating images. They usually entail adding objects to the same image or covering them with flat regions. Image forensic techniques use a variety of complex procedures that have been documented in the literature to ascertain the integrity of a photograph. To conceal particular objects or provide the appearance of a duplicate, a section of an image is copied, then pasted back onto the original. One study concentrates on a specific type of image faking. Next, build the architecture for a convolutional neural network to determine whether or not the image is fake.

Keywords: Deep learning, Forgery detection, Image features, Multimedia, Forensic analysis

1. INTRODUCTION

Numerous advances in picture technology have made powerful computers and high-resolution digital cameras possible, increasing the accessibility of digital multimedia information in society. Visuals are also a more effective communication tool than words because their information is easier to understand. All of this has led to the widespread usage of digital multimedia content by many organizations in the legal, scientific, governmental, and journalism fields to support critical decision making, information sharing and proof of specific occurrences. But the amazing progress of photo-editing software has also increased the risk associated with relying too much on digital media assets. The ease of access to these software programs has greatly simplified the process of image forging. The Wall Street Journal claims that 10% of all color photos that were published in the US had digital alterations and retouching applied to them. Additionally, there have been forgeries directed toward the scientific community. The adage, "Seeing believes," is not very applicable in today's society. Digital photo evidence is controversial when used in courtrooms and other sensitive settings.

Consequently, it has become imperative to authenticate photographs, leading to a substantial body of study on picture authentication. Picture counterfeiting is the primary factor for the development of the discipline of digital image forensics, which confirms the authenticity and integrity of digital photographs. Copy move is the most often used technique for altering and tampering with digital photographs, although there are definitely a lot more choices available. To hide or enlarge a segment of an image and change the information it sends, you have to copy that portion and paste it somewhere else within the original image.

Copy-move forgery detection is one of the most researched topics in the literature. There are many review papers available in the topic of blind forgery detection. The act of altering certain aspects of a digital image is known as image forging. Active approaches have gained significant importance in security applications since their initial popularity. Digital signatures and watermarking are common methods for confirming an image's originality. However, because the image and digital signature are integrated, the authentication procedure is more costly because more resources are required to separate the image and content during decoding. The validity of the image is verified by the passive technique, which does not require the use of any extra resources. The assumptions made determine whether or not this mechanism is successful. Among the four methods of picture forgery, geometric methods have gained the most traction in the last several decades. In Geometric, you can manipulate individual pixels by using "Copy Move," which merges many image segments into one. The image fabrication techniques are displayed in Fig. 1.

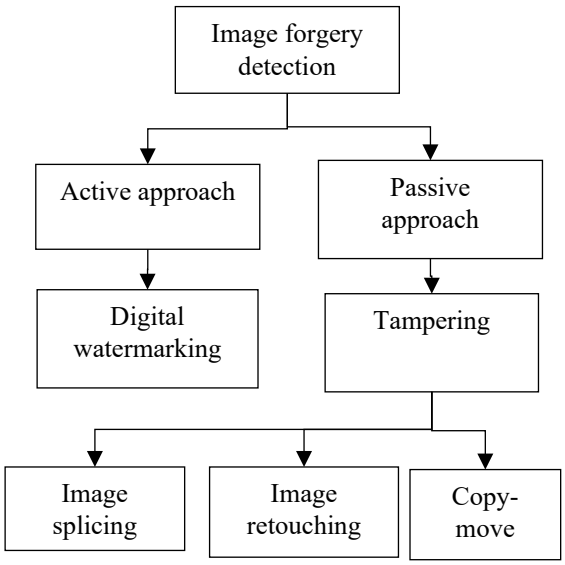

Fig 1: Image forgery Techniques

2. RELATED WORK

A common method of altering images is called "copy-move forgery," or CMF. It is copying and pasting a section of a picture to a different location inside the same image. This technique was proposed by Jun Young Park et al. [1]. The copy-move technique can be used to alter or conceal the meaning of an image. Finding the duplicated and relocated components and verifying the accuracy of the image are therefore essential. Because pirated photographs are sometimes cropped or rotated, it may be challenging to assess an image's validity only by visual inspection. Building reliable copy-move forgery detection (CMFD) systems is therefore imperative. Data pre-processing (optional), feature extraction, matching, false match removal, and localization form the common foundation of CMFD. Pre-processing is the first, optional step in a CMFD process. Converting RGB color channels to grayscale is a common technique used in this phase to minimize the size of the input photographs. An alternative method for using the brightness and chrominance information in RGB colors is to transform them into the YCbCr or HSV color spaces. Numerous block segmentation and division strategies might be considered for preprocessing. An image can be separated into circular chunks, non-overlapping square blocks, and overlapping square blocks. Image segmentation techniques are frequently used in pre-processing to distinguish between the copied source region and the pasted target region.

Belhassen Bayar et al. [2] developed several algorithms that analyze the traces left by different image modifications in order to identify particular editing actions. While this approach has yielded some useful forensic algorithms, there is still a major problem: The process of developing forensic detectors for various picture modification techniques is challenging and time-consuming. Moreover, forensic analysts require "general purpose" forensic algorithms that can recognize a broad variety of image alterations. In this work, we present a unique general-purpose forensic technique based on convolutional neural networks (CNNs) to address all of these issues. Although CNNs can extract classification features directly from the data, in this version of the algorithm, they frequently identify patterns that may hint to a picture's content. It was created in order to solve this problem. Adaptive learning is used by this layer to recognize and hide image manipulation. We demonstrate that restricted CNN can directly learn aspects of manipulation detection from data through a set of trials. Test findings show that our CNN outperforms the state-of-the-art general purpose manipulation detector, identifying a variety of altering processes with up to 99.97% accuracy. Furthermore, even in situations when there is a substantial model mismatch between the testing and training data, our limited CNN can detect picture modifications with accuracy.

Mauro Barni et al. suggested a method for precisely identifying the modified area by identifying the copy-move scam's source and destination locations [3]. Start by organizing the problem into a hypothesis testing framework and attempting to determine which of the two almost identical pieces is the original according to a general copy-move detector. Next, to address the hypothesis testing problem, we construct a multi-branch CNN architecture based on a collection of learnable features by identifying boundary and interpolation artifacts in the copy-moved area. The proposed architecture performs effectively against synthetic and realistic dataset copy-move frauds. A fictitious dataset made especially for this purpose is used to train it. Experimental results show that the proposed disambiguation strategy may successfully disclose the target region even in scenarios where a state-of-the-art copy-move detection method gives an approximation of a copy-move localization mask.

Yue Wu et al. developed the Buster Net, a cutting-edge deep convolutional neural architecture for photo copy-move forgery detection (CMFD) [4]. Buster Net is a fully working, edge trainable deep neural network system, unlike earlier attempts. It has a two-branch architecture with a fusion module in between. The two branches use visual similarities to copy-move regions and visual artifacts to locate likely modification spots. To the best of our knowledge, source and target locations can only be precisely identified using this CMFD method. Give detailed instructions on how to create big CMFD samples from datasets in many disciplines and how to train Buster Nets efficiently. Comprehensive analyses of two publicly accessible datasets, CoMoFoD and CASIA, show that Buster Net performs better than even the most advanced techniques for duplication identification and is resistant to a number of known assaults.

Yaqi Liu et al. suggested a copy-move forgery detection method based on Convolutional Kernel Networks [5]. A kind of information local descriptors with deep convolutional structure is deep neural kernel networks, in contrast to techniques that rely on features that are typically generated. Data-driven algorithms are competitive in a range of scenarios due to their enhanced discriminative strength, which is made feasible by the development of deep learning ideas and the availability of large datasets. Furthermore, we have redesigned our Convolutional Kernel Network to achieve exceptional efficiency by combining a series of matrix and convolutional operations that are easily replicable and GPU-accelerated. After that, Convolutional Kernel Network is used with the proper pre-treatment and post processing to identify copy-move fraud. In particular, a distribution strategy based on segmentation for critical sites is combined with a GPU-based adaptive cross segmentation algorithm. The effectiveness and resilience of a GPU version of the Convolutional Kernel Network are also demonstrated, along with the state-of-the-art performance of the copy-move detection system based on the Convolutional Kernel Network, through extensive testing.

3. IMAGE FORGERY DETECTION METHODS

There are two types of digital picture forgery detection techniques: active and passive (blind). The active techniques require prior knowledge of the source image. The techniques search for the purportedly manipulated portions of the bogus image. Most of the active technique restricts its use by needing some pre-processing, including watermark implantation or signature formation during image collecting. As a result, a blind forgery detection technique that doesn't require prior knowledge of the source image is required. There are several kinds of blind picture fraud detection methods, including those that rely on cameras, formats, pixels, physical environments, geometry, and physical environments. Pixel-by-pixel pixel-level picture fraud detection identifies irregularities in a digital image. These methods fall into four categories: statistical, slicing, cloning, and resampling.

- Detection of photo forgeries using pattern-based methods depends on the image formats, particularly JPEG formats. JPEG quantization, blocking, and double JPEG make up its three categories. Even compressed photographs can be used to detect fakes.
- Camera response, color filter arrays, chromatic aberration, and sensor noise are some examples of picture fraud detection systems that use cameras to detect image manipulation at various stages of the image processing process.
- The identification of picture frauds is based on the physical setting of the lightning environment in which an object or photograph is shot. There are three categories for these techniques: Light environment, Light direction 2D, and Light direction 3D.
- Principal points and metric measures are the two types of geometry-based image fraud detection techniques. Principal points calculate the distances between surrounding objects and the camera to detect frauds.

4. COPY MOVE FORGERY DETECTION

Copy-move is the most often used technique for image counterfeiting. This image editing technique involves copying and pasting a section of the image to a new location in order to hide particular characteristics or objects. Due to region-duplication, a modified region has at least two comparable regions. Copy-move forgeries aim to either replicate existing objects in the image by copying them to the desired location, or make an object appear "hidden" from the image by covering it with a thin background block. Since the replicated segments are components of the same image, their color scheme, noise levels, dynamic range, and other features will all be the same, making it very difficult for the untrained eye to distinguish between the actual thing and a fake. Copy-move forgeries can be recognized by block-based or key-point-based methods. Block-based techniques are utilized to compute a feature vector for every block subsequent to the division of the picture into overlapping and non-overlapping segments. Identical feature vectors are matched and positioned in a comparable fashion to identify fabricated regions. Finding key points in an image and creating a feature vector for each one is the process of key-point based approaches. Rather of segmenting the image to find duplicate parts, feature vectors are compared.

As a result, there is a high link between the copied region and the remainder of the image, which can be used to identify any fabricated portions. The main problem with copy-move detection is that large-scale search methods are computationally complex. Copy-Move forgery detection techniques come in two flavours: block-based and key point-based.

4.1. Block Based Method

The analysis of image blocks to identify forgeries forms the foundation of these systems. These methods' fundamental concept is to split the image into overlapping or non-overlapping sections rather than looking at the entire thing at once. The blocks are subsequently exposed to many feature extraction approaches. The matching matrix for every block contains these restored features. A sorting approach is used to put similar qualities close to one other. In order to identify the blocks that shift similarly, the idea of a shift vector is presented. A counter value is used to count the number of blocks that have the same shifting value, and a threshold value is used to identify similar regions.

4.2. Key point-Based Method

By copying portions of the original image and post-processing the copied segments to mask the forged regions and paste them over other areas of the same image, these techniques for detecting copy-move forgeries create a correlation between the original and pasted image segments. It used the Scale Invariant Feature Transform, or SIFTS, to identify cloned portions. This method can identify forgeries when post processing is used on a cloned segment, but it cannot identify minutely altered sections. For the most part, copy-move forgeries are difficult to spot because the copied area is processed through several stages before being placed over the original image. It is particularly challenging to identify forgeries when using image editing techniques including scaling, rotation, compression, bending, and noise addition. Computational complexity is another important concern. Key point-based techniques such as SIFT can help detect forgeries if the faked region is scaled and rotated. Although robust against changes in lighting and noise, a limitation of key point-based techniques is their inability to detect recurrent flat areas. Zernike moments are able to detect scaled copy-moved regions, but not flat faked portions. Block-based algorithm-based techniques are unable to distinguish between duplicate sections that have been scaled and rotated. Algorithms that use circular blocks rather than square or rectangular blocks can detect rotational forgeries because they are rotation invariant.

5. MODULES IN FORGERY DETECTION

Evidence of a copy-move fake could be demonstrated by a strong correlation between the copied and pasted sections of a document.

A. Pre-processing enhancing some visual properties that are crucial for additional detection or suppressing undesired distortions is the goal of pre-processing. With the exception of algorithms that require color channels, the supplied image is converted to grayscale (color conversion) when suitable. Dimension reduction, image scaling, and low-pass filtering are other pre-processing techniques. The necessary pre-processing can be completed with block-based or key-point-based techniques.

B. Feature vectors are retrieved for each block via algorithms that rely on feature deletion blocks. However, key-point-based techniques only compute feature vectors for significant picture places, such as entropy-rich regions.

C. Following feature extraction, complementary blocks with comparable features are looked for in order to identify possible copy-move pairings. When feature descriptors exhibit a significant degree of similarity, duplicate regions could be taken into consideration. While key-point-based techniques assist with feature matching by predicting the nearest neighbor by utilizing the Best-Bin-First search strategy, block-based approaches sort related features lexicographically.

D. Sorting To determine whether duplicate areas exist, more than one similarity criterion is needed. Therefore, the possibility of erroneous matches is reduced when filtering techniques are used. Finally, matches exhibiting comparable behavior can be preserved through post-processing. The DenseNet framework shown in fig 2.

Dense Block: A DenseNet is made up of dense blocks. All dense blocks have convolution layers. A transition layer is positioned after a dense block to go on to the following dense block. Every layer in a thick block is connected to every other layer directly. As a result, feature-maps from all previous levels are transmitted to every layer.

Convolutional layers: Each convolution layer consists of three sequential processes: 3 × 3 convolution (Conv), rectified linear unit (ReLU), and batch normalization (BN). Incorporating dropout is also possible, depending on your architectural requirements. Downsampling layers are a crucial component of convolutional networks since they minimize the size of feature maps. In the DenseNet architecture, the network is divided into several densely connected blocks to enable downsampling.

Transition Block: DenseNets have no optimization problems and are inherently scalable to hundreds of layers. For a variety of computer vision tasks that depend on convolutional features, DenseNets may be helpful feature extractors due to their compact internal representations and decreased feature redundancy. Fig 2 shows the Dense framework structure.

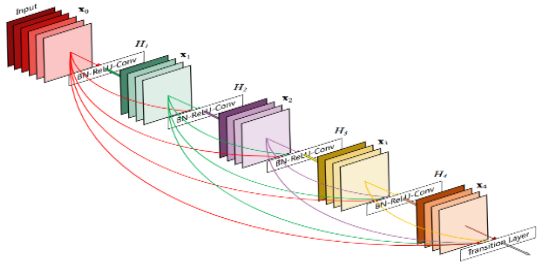

FIG 2 DENSE FRAMEWORK

6. RESULTS AND DISCUSSION

A convolutional neural networks (CNN) performance during training is assessed in part by its training accuracy. On the training dataset—the collection of data used to train the model—it assesses how accurate the model is in making predictions. The CNN gains accuracy through training as it learns to identify patterns in the input data and modifies the layer weights accordingly. The model's performance on the training dataset should get better as the training goes on, leading to a higher training accuracy. High training accuracy, however, does not guarantee high accuracy on fresh, untested data. This is due to the possibility that the model overfits to the training dataset, becoming overly specialized to the unique patterns and noise present in the training data and underperforming when applied to fresh data. It is crucial to keep an eye on the CNN's performance using a different validation dataset in order to prevent overfitting. The validation dataset is used to evaluate the model's performance on new, untested data during the training phase. If the

model starts to perform poorly on the validation dataset but still retains a higher training accuracy, it might be overfitting to the training dataset. In this situation, applying regularization or early halting strategies might assist reduce overfitting and enhance the generalization capabilities of the model. To sum up, training accuracy is a crucial measure for assessing how well a CNN performs during training, but it must be combined with validation accuracy to make sure the model isn't overfitting to the training set. The CNN can be trained to achieve high accuracy in real-world applications and to generalize well to new, unseen data by tracking both training and validation accuracy. Fig 3 shows the training accuracy.

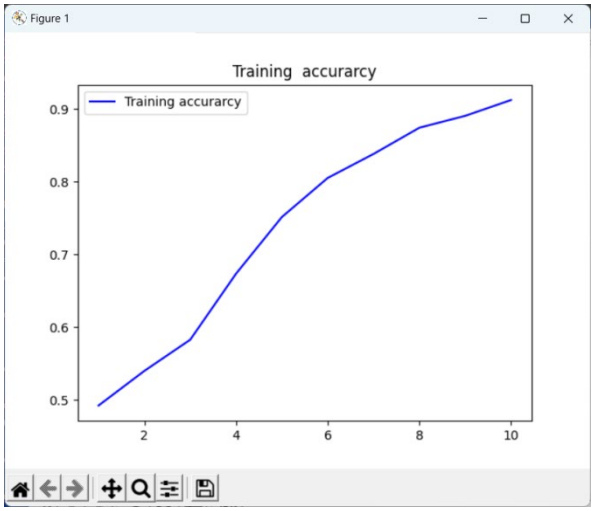

FIG 3: TRAINING ACCURACY

7. CONCLUSION

Forgeries of photographs are now quite simple to carry out. It is an extremely fascinating area of study to detect this kind of forgery. One popular area of research is copy-move forgery. To detect such forgeries in photos, academics have proposed a variety of methods. Many approaches have been covered in this work. When post-processing activities are carried out over cloned segments, these approaches hold up well. Scholars have developed a number of features-extraction-based algorithms, but there is still much opportunity in this field to find methods that can handle various post-processing steps at once. various assumptions are made by various algorithms in order to produce useful results. Analysis of several copy-move forgery detection methods showed that a hybrid approach produces more accurate results at a lower computing cost. This area of research is growing. Moreover, a substantial dataset is needed to assess how well methods for detecting forgeries work.

CONFLICT OF INTERESTS

None

ACKNOWLEDGEMENTS

None

REFERENCES

Park, Jun Young, et al. "Copy-move forgery detection using scale invariant feature and reduced local binary pattern histogram." Symmetry 12.4 (2020): 492.

Bayar, Belhassen, and Matthew C. Stamm. "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection." IEEE Transactions on Information Forensics and Security 13.11 (2018): 2691-2706.

Barni, Mauro, Quoc-Tin Phan, and Benedetta Tondi. "Copy move source-target disambiguation through multi-branch CNNs." IEEE Transactions on Information Forensics and Security 16 (2020): 1825-1840.

Wu, Yue, Wael Abd-Almageed, and Prem Natarajan. "Busternet: Detecting copy-move image forgery with source/target localization." Proceedings of the European conference on computer vision (ECCV). 2018.

Wu, Yue, Wael Abd-Almageed, and Prem Natarajan. "Busternet: Detecting copy-move image forgery with source/target localization." Proceedings of the European conference on computer vision (ECCV). 2018.

Hegazi, A. Taha, and M. M. Selim, "Copy-Move Forgery Detection Based on Automatic Threshold Estimation," International Journal of Socio-technology and Knowledge Development, vol. 12, no. 1, pp. 1–23, 2020.

Y. Wang, X. Kang, and Y. Chen, "Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures," Journal of Information Security and Applications, vol. 54, pp. 1–11, 2020.

P. Niyishaka and C. Bhagvati, "Copy-move forgery detection using image blobs and BRISK feature," Multimedia Tools and Applications, 2020.

C. Lin, W. Lu, W. Sun, J. Zeng, T. X. J. Lai, and W. Lu, "Region duplication detection based on image segmentation and key point contexts," Multimedia Tools and Applications, vol. 77, pp. 14241–14258, 2018.

C. Lin, W. Lu, X. Huang, K. Liu, W. Sun, and H. Lin, "Region duplication detection based on hybrid feature and evaluative clustering," Multimedia Tools and Applications, vol. 78, pp. 20739–20763, 2019.