ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

A Survey on Copy Move Image Forgery on Forensic using Deep Learning

Shaheena.K.V, Research Scholar, Department of Computer Science, Sri Krishna Arts and Science College

Dhanalakshmi S, Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College.

Abstract

The growing usage of the internet, make it possible that digital multimedia is now more easily transmitted and acquired. As a result, forgery and other forms of tampering are now more easily possible with this media. Copy-move duplication is a specific sort of counterfeit that frequently incorporates image manipulation. In digital image forensics, a technique known as copy-move forgery detection (CMFD) is widely used to verify images by detecting fraudulent copy-move manipulation. To do copy-move forgery, copy a portion of a picture and paste it into another image. More attention was given to CMFD robustness and accuracy than to performance and time complexity in surveys and reviews. It is our goal in this research to identify the most important causes of time complexity. In digital forensics, forgery detection and localization have received increased attention. It is hoped that the information in this article will assist researchers in better understanding the existing copy-move picture recognition algorithms and methodologies.

Keywords: Digital image processing,copy-move forgery,image forensics

1. Introduction

Digital technology is the dominant technology for creating, processing, transferring, and storing information as a form of knowledge and intellectual assets. A variety of multidimensional types of information are available. These include audio, video, text, image, and other forms of visual media. Digital technology has made it feasible to digitise all types of information, including knowledge and intellectual assets, and to store them in digital form. There are various advantages of employing digital technology over analogue technology, including the simplicity with which information may be accessed, searched, and transmitted. Because of the rapid increase in the number of Internet users, digital images are now widely acknowledged as official documents and as a handy mode of communication for many people. With recent improvements in software development leveraging plug-and-play(run) technologies for data capture and processing, as well as data access and transfer, it has never been easier to make changes to digital data than it is now. Copy and move forgery is a common image manipulation technique in which pieces of an image are duplicated and moved around in order to conceal a person or object in the frame of the original photo. Copy and move forgery is also known as copy and paste forgery. The work[11] demonstrates the dissipation of the region detection process as well as the improvement in the accuracy of the region identification process.

The image's colour, dynamic range, and noise variation attributes are to those of textured areas, the human eye will have no means of determining whether or not the two images are incompatible with one another. The copy-move is a technique that is commonly used in the fashion and advertising industries. This method is commonly referred to as "cloning" in the scientific community. To make actors and actresses appear younger, it's as simple as copying and pasting sections of the original image into other portions of the same image. This technique can also be used to restore hair that has been lost or to eliminate undesirable characteristics. In this case, as should be obvious, image tampering could result in serious legal consequences. The employment of this technique by dishonest persons to enhance the severity of injuries or to make a coffee stain on clothing appear to be blood is a possibility. Cryptographic forgery detection (CMFD) is an approach that includes both manual and machine learning techniques. [2].

2. Literature Survey

Copy-Move is an image editing technique that includes copying and pasting a portion of an original image into a portion of another original image, as shown in the example below. A technique known as copy-move forgery is occasionally used to make an object "disappear" from a picture by covering it up with a duplicate of another portion of the same image. Because the duplicated areas will likely blend in with their surroundings and the human eye will be unable to identify any suspicious artefacts, it is recommended to choose textured areas such as grass and leaves, gravel, or fabric with random patterns for this reason. The colour palette, noise components, dynamic range, and other characteristics of the cloned segments will be identical to those of the rest of the image, making it practically impossible for a human eye to distinguish between the two images. An image that has been digitally manipulated with the tools that we have at our disposal may, on occasion, make it more difficult for technology to detect a fabricated image.

In [5], offered another method based on CNN's. The input image is transformed into a feature map using ResNet-50 as a foundation. Rather than using the Feature Pyramid Network (FPN), multiscale feature maps are generated using convolutional layers instead. A Mask-RCNN is then used to identify forgeries based on these maps.

In [6] RRU-Net, a new picture splicing detection technique, was unveiled. For learning image splicing features, RRU-Net uses residual propagation and residual feedback. The residual propagation functions as the human brain recalling process and is employed in the deep network to resolve the problem of

deterioration. The input feature information is consolidated by remains of feedback to augment the image discrepancies in original and fabricated regions.

In [7], an approach was presented which is based on a combination of co-occurrence matrices and deep learning. A co-occurrence matrix is a matrix that is defined over an image to be the distribution of co-occurring pixel values at a given offset. First, co-occurrence matrices for the three color channels are obtained in the pixel domain. Then, a deep CNN framework is trained using these matrices to extract features. Detecting GAN generated images requires both real and fake images from the targeted GAN model.

It's a fusion [15] of both splicing and copy-move forgery. To increase the performance and reliability of detection algorithms, fusion rules are formulated by forensics, which uses multiple tools and detection. Outputs obtained by different tools are analysed to decide on fusion-based methods.

In [16] adopted an adaptive method feature point matching and oversegmentation to overcome the problem of low recall rates. Instead of overlapping and regular blocks, they used non-overlapping and irregular segmentation of blocks called image blocks (IB). Due to regularity in the blocks, the recall rate considerably improved when compared to the previous works.

In [17] proposed a novel method for detecting the copy move forged regions of an image. The images are first partitioned into blocks of size 16 X 16 pixels and then the method used RGB values or Zernike moments extracted from the blocks as features. Feature matching is done using a nearest analyses field computation algorithm by name Patch-match algorithm. The authors employed three different versions of the algorithm: the original Patch-match algorithm, the Generalized Patch match algorithm and a modified version of Patch-match algorithm which is capable of dealing with rotation and scaling. The matched patches are further filtered using a predefined threshold and the Same Affine Transformation Selection (SATS) algorithm. Performance of the employed three different algorithms was quantitatively analysed using the F – measure which is a function of true positive, false negative and false positive rates. This method proved to be computationally efficient when compared with many of the other existing methods.

Table 1: Comparison table for Forgery detection and Accuracy Detection using different methods

Year and Ref	**Method Name**	**Forgery detection**	**Classification**	**Maximum Detection Accuracy**
2020 [2]	Detection using morphologically-based mathematical filters	Image splicing forgery detection	Precision and image compression resistance. But mathematical and time complexity.	99.02
2020 [3]	Attention DM for CISDL	Image fabrication due to splicing can be detected.	This algorithm increased the performance. It also reduces the detection rate.	96.2
2020 [4]	Convolution Neural Networks	The detection and localisation of image splices in a video	Intuitive and resistant to picture compression (JPEG). The drawback is great complexity.	97.7
2019 [8]	CNN and support vector machines, K closest neighbour, and Naive Bayes are all used in this analysis.	Detecting image forgery caused by splicing	Has good accuracy and can find the forgery region. However, it is not suitable for copy-move image fraud and requires a fast system.	98.2
2019 [9]	Convolutional neural network (C2RNet) and diluted adaptive clustering are two types of neural networks.	Identify a spliced image that has been tampered with. Detect the fraud of a spliced image	It saves time and effort. This approach has a lower recall than many other comparison algorithms.	97.2
2019 [10]	Deep learning and wavelet transformation are two techniques for improving performance.	Detect forgery	Also, it saves time and money. But it's fragile and time-consuming.	95.3
2018 [11]	Brute Force	The use of artefacts allows for the detection of image frauds.	This method is fast and generalizable. Despite its slow performance and difficulty in most forgery scenarios.	94.6
2018 [12]	Deep learning mechanism	Image detection based on copy-move	With less false positives, it is highly efficient.	93.02
2017 [16]	Pixel based	Detection of splicing image fabrication as well as Copy Move	This procedure is accurate and	93.05

		Image forgery	reliable. However, this method takes longer and is less accurate in detecting counterfeit in noisy images.	
2017 [17]	Format Based	In order to detect image forgery, it is necessary to first analyse the problem of the hypothesis test.	It is simpler and more efficient. But it's not suitable for a noisy image. The estimated inaccuracy grows.	92.08
2017 [18]	Robust method	Copy-move image forgery	It is a less sophisticated way of combining two processes. But it's less precise and didn't perform well with complex backgrounds.	92.05

3. Methods and Process in copy move forgery Detection

a. Robust method

Foremost, it is necessary to have a thorough understanding of how CMFD functions before going into its issues. In order to detect copy move frauds, one can use either a block-based method or an algorithmic approach. An approach based on the most important considerations. Copy-move forgery detection is illustrated in Figure 1 [9, 19-22], which displays the overall approach. The pre-processing phase includes a number of stages such as feature extraction, matching, and verification, to name a few examples. The detection technique begins as soon as a photo suspected of containing copy-move forgeries is entered into the system, according to the manufacturer.

Following that, images are divided into several overlapping blocks for segmentation using the block-based technique, which is described below. With the keypoint-based method, an image is scanned through from beginning to end in order to discover high-entropy image regions (also known as "keypoints") [23]. A specific number of keypoints is extracted based on the feature descriptor that is being used in the analysis. Because of this, we may proceed to the following phase, which is feature extraction.

Features are calculated for each block or keypoint in the feature extraction technique, utilising a feature descriptor for each block or keypoint. Forgeries should be detected using the best or most robust features that can be extracted by a competent feature extractor or feature descriptor. For storing the computed features, a feature vector is employed. This allows the features to be matched later on [24]. When two feature sets are compared, they will be able to discover traits that are comparable. Due to the great degree of resemblance between two feature sets, it is obvious that a region has been replicated. Even after the block matching was completed, there were still numerous comparable blocks in the image, which meant that the process was not completed at that point [25]. This was the spot where the verification procedure took place.

In order to limit the likelihood of false matches in the detection image, a filtering procedure known as verification has been developed. The detection map, a visual representation of the image's duplicated regions, is the process's ultimate result. When it appears to be a simple operation, the CMFD pipeline might be challenging to identify the exact area of an image that has been replicated. When geometric transformations and post-processing manipulations are present, CMFD is still unable to reliably detect repeated regions. For images that have been post-processed, the detection rate may be reduced, but it will not be completely lost [26]. It's possible to discover a total failure if a region is re-created using geometric transformations like scaling, translation, or rotation.

b. Process in Keypoint based Copy Move forgery detection using Deep learning

Keypoint-based photo forensics is based on the Helmert transformation and the SLIC algorithm, among other things [27]. Three of the most critical elements in this procedure are the extraction of keypoints and the comparison of those keypoints with previously discovered forgery regions[5]. With the help of the SIFT technique [28], we are able to detect all of the possibly relevant locations in a photograph as well as their corresponding descriptions. We'll hunt for the finest feasible pairings for additional groupings based on this list of potential possibilities. To begin, using the related descriptors, compute the Euclidean distance between each candidate's keypoints. Then, for each keypoint, apply the matching process as described in the preceding section. This method makes use of the nearest neighbour distance ratio (NNDR) [29], which determines how far apart two points are from one another in terms of distance.

c. Process in Block based Copy Move forgery detection using Deep learning

If it is dealing with a blind picture forgery detection system that doesn't include any watermarks or signatures, it can be a difficult process to identify fake images. Blind picture forgery detection techniques such as copy move forgery are extensively employed by forgers because they are easy to use and efficient. An even more difficult forgery to detect is a copy-move fraud that is followed by rotation and scale of the faked component. The goal of this research to demonstrate that a copy move forgery detection algorithm may be developed that is more accurate and less time-consuming than other current techniques [30]. In this method, feature vectors around Harris Corner points are identified using the HOG descriptor. Sum of squared differences (SSD) and nearest neighbour distance ratio (NNDR) are two methods for comparing feature vectors in a feature space to find a good match (NDR).

Using RANSAC, outlier matches from the previous stage can be eliminated. The results are evaluated using a variety of performance indicators, including the True Positive Rate (TPR), the False Positive Rate (FPR), Precision, and Recall. Data from Adrizzone et al. and CoMoFoD are used in the evaluation (small) [31]. Results show that our method has a good True Positive Rate against mild rotation and scaling.

The image is divided into overlapping chunks in the majority of the other ways, on the other hand. The goal here is to identify blocks that have been copied and relocated. Many overlapping blocks would be found in the duplicated area. Since each block is moved with the same amount of shift, the distance between each pair of identical blocks would be the same. Once these blocks were extracted, the next step would be to calculate comparable or identical values for each of the blocks that had been replicated. Several authors proposed a variety of ways to represent the image block using various attributes [32]. An algorithm is used to vectorize these blocks and insert them into a matrix where the vectors are lexicographically sorted for further detection [8].

4. Conclusion

Using the SIFT algorithm, the approach is able to extract the pixels that are the most interesting in the image (Scale invariant feature transform). In the following step, the SIFT keypoints are matched by utilising the best bin first closest neighbour algorithm. There are a number of keypoint-based approaches proposed after this work. These approaches have the disadvantage that keypoint-based algorithms are unable to detect forgeries in low contrast regions since there are not enough keypoints in such areas. It has been discovered that there is another another approach to detect this type of counterfeit. All of the research cited in this section incorporates hand-crafted features. Deep learning-based algorithms outperform hand-crafted methods in image tasks such as image classification and image retrieval, according to recent findings in the literature. When the copy region is neither scaled nor rotated, the copy-move forgery can also be detected. Furthermore, the vast majority of them failed to study the impact of varying image illumination conditions. Even the most sophisticated algorithms struggle to detect forgeries because they are so difficult to detect.

References

[1] Huynh KT., Ly TN., Le-Tien T. (2020) ORB For Detecting Copy-Move Regions With Scale And Rotation In Image Forensics. In: Dang T.K., Küng J., Takizawa M., Chung T.M. (Eds) Future Data And Security Engineering. Big Data, Security And Privacy, Smart City And Industry 4.0 Applications. FDSE 2020. Communications In Computer And Information Science, Vol 1306. Springer, Singapore.

[2] Giulia Boato, Duc-Tien Dang-Nguyen, and Francesco G. B. Denatale, " Morphological Filter Detector for Image Forensics Applications" IEEE Access 2020.

[3] Yaqi Liu, and Xianfeng Zhao, "Constrained Image Splicing Detection and Localization With Attention-Aware Encoder-Decoder and Atrous Convolution" IEEE Access2020.

[4] Yuan Rao, Jiangqun Ni, and Huimin Zhao, "Deep Learning Local Descriptor for Image Splicing Detection and Localization" IEEE Access2020.

[5] Bi, X., Wei, Y., Xiao, B., Li, W.: RRU-Net: The ringed residual U-Net for image splicing forgery detection. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. Long Beach, CA, USA, Jun. 16–17 (2019)

[6] Abdosalehi, S.-E. & Mahmoodi-Aznaveh, A. (2019), Splicing localization in tampered blurred images, in '2019 4th International Conference on Pattern Recognition and Image Analysis (IPRIA)', IEEE, pp. 46–51.

[7] Mehrish, A., Subramanyam, A. V. & Emmanuel, S. (2019), 'Joint spatial and discrete cosine transform domain-based counter forensics for adaptive contrast enhancement', IEEE Access 7, 27183–27195.

[8] Ankit Kumar Jaiswal and Rajeev Srivastava, "Image Splicing Detection using Deep Residual Network," 2nd International Conference on Advanced Computing and Software Engineering (ICACSE-2019).

[9] Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, andJianfeng Ma, "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering " Elsevier Information Sciences, 2019.

[10] Thuong Le-Tien, Hanh Phan-Xuan, Thuy Nguyen-Chinh, and Thien Do-Tieu, " Image Forgery Detection: A Low Computational-Cost and Effective Data-Driven Model " International Journal of Machine Learning and Computing, Vol. 9, No. 2, April 2019.

[11] N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on, 2017, pp. 1-7.

[12] T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, B. Manjunath, et al., "Boosting Image Forgery Detection using Resampling Detection and Copy-move analysis," arXiv preprint arXiv:1802.03154, 2018.

[13] D. Mistry and A. Banerjee, "Comparison of Feature Detection and Matching Approach: SIFT and SURF," GRD Journals- Global Research and Development Journal for Engineering, vol. 2, no. 4, pp. 7-13, 2017.

[14] Zhang W, Yang Z, Niu S, Wang J. Detection of copy-move forgery in flat region based on feature enhancement. In: Shi Y, Kim H, Perez-Gonzalez F, Liu F, editors. Digital Forensics and Watermarking, IWDW 2016. Lecture Notes in Computer Science, vol 10082. Springer, Cham; 2017. 2017:159–171.

[15] Abdul Warif NB, Abdul Wahab AW, Idna Idris MY, Fazidah Othman RS. SIFT-Symmetry: A robust detection method for copy-move forgery with a reflection attack. J Vis Commun Image Represent, 2017;46:219–232.

[16] Wo Y., Yang K., Han G., Chen H., Wu W., "Copy move forgery detection based on multi-radius PCET," IET Image Processing, vol. 11, no. 2, pp. 99-108, 2 2017.

[17] Wenchang S., Fei Z., Bo Q., Bin L., "Improving image copy-move forgery detection with particle swarm optimization techniques," China Communications, vol. 13, no. 1, pp. 139-149, Jan. 2016.

[18] Rao, Y., Ni, J.: A deep learning approach to detection of splicing and copy-move forgeries in images. In: Proceedings of the IEEE International Workshop on Information Forensics and Security. Abu Dhabi, UAE, Dec. 4–7, pp. 1–6 (2016)
[19] Sreelakshmy, I. & Anver, J. (2016), An improved method for copy-move forgery detection in digital forensic, in '2016 Online International Conference on Green Engineering and Technologies (IC-GET)', IEEE, pp. 1–4.
[20] Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y. & Yang, H. (2016), 'Fusion of block and key points based approaches for effective copy-move image forgery detection', Multidimensional Systems and Signal Processing 27(4), 989–1005.
[21] Pun, C.-M., Yuan, X.-C. & Bi, X.-L. (2015), 'Image forgery detection using adaptive over segmentation and feature point matching', IEEE Transactions on Information Forensics and Security 10(8), 1705–1716.
[22] Liu, F & Feng, H 2014, 'A Novel Algorithm for Image Copy-move Forgery Detection and Localization based on SVD and Projection Data', International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 9, pp. 189-200.
[23] Zhong, L. and Xu, W., 2013, May. A robust image copy-move forgery detection based on mixed moments. In 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2013. (pp. 381-384).
[24] Bin, Y, Xingming, S, Xianyi, C, Zhang, J & Xu, L 2013, 'An Efficient Forensic Method for Copy--move Forgery Detection Based on DWTFWHT', Radioengineering, vol. 22, no. 4.
[25] Li, L, Zhang, W, Li, S & Pan, J-S 2013, 'Detection of Region Duplication Forgery in Images under Affine Transforms', in Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on, pp. 543-546.
[26] Sekeh, MA, Maarof, MA, Rohani, MF & Mahdian, B 2013, 'Efficient image duplicated region detection model using sequential block clustering', Digital Investigation, vol. 10, no. 1, pp. 73-84.
[27] Ulutas, G & Ulutas, M 2013, 'Image forgery detection using color coherence vector', in Electronics, Computer and Computation (ICECCO), 2013 International Conference on, pp. 107-110.
[28] Wang, T, Tang, J & Luo, B 2013, 'Blind detection of region duplication forgery by merging blur and affine moment invariants', in Image and Graphics (ICIG), 2013 Seventh International Conference on, pp. 258-264.
[29] Zhong, L & Xu, W 2013, 'A robust image copy-move forgery detection based on mixed moments', in Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on, pp. 381-384.
[30] Zhong, L. and Xu, W., 2013, May. A robust image copy-move forgery detection based on mixed moments. In 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2013. (pp. 381-384).
[31] Ghorbani, M., Firouzmand, M. and Faraahi, A., 2011, June. DWT-DCT (QCD) based copy-move image forgery detection. In 18th International Conference on Systems, Signals and Image Processing (IWSSIP), 2011 (pp. 1-4).
[32] Kang, L., & Cheng, X. P. "Copy-move Forgery Detection in Digital Image," International Congress on Image and Signal Processing (CISP2010) IEEE Computer Society, pp. 2419-2421. 2010.