The Recent Digital Image Splicing Detection

Yukun Wan *

School of Computer and Engineering (School of Artificial Intelligence), Chongqing University of Science and Technology, Shapingba, Chongqing, China

* Corresponding Author Email: asakahidechiyo@gmail.com

Abstract. With the great progress of multimedia, digital image tampering has become a critical challenge to modern social credit. Among these abundant tampering methods, image splicing is especially noteworthy. This paper is based on the search and organization of classical and recent papers, aiming to provide a taxonomy analysis on this topic. By classifying the image splicing detection technology into two main classes, four different sub-classes are proposed. Specifically, depending on whether artificial intelligence is applied, traditional methods and deep learning methods are divided from each other. A further classification of the traditional methods can be proposed based on the specific aspect of anomaly focused on by each method. Also, this paper is expected to provide a channel for researchers to quickly get to know the digital image splicing detection area. Besides, this paper finally hopes to provide a way to help researchers understand the status of this area and to conduct their technical assessments.

Keywords: Image Tampering, Image Splicing, Pixel Anomaly, Photo Response Non-Uniformity (PRNU), Lighting Inconsistency.

1. Introduction

Image splicing might be out of mischief, and also can carry targeted malicious intent. Such as guiding the public voice, damaging others' reputations or spreading fake news. During the 2004 U.S. presidential election, a tampered graph that shows John Kerry sitting with Jane Fonda at an anti-war gathering in 1970 was widely spread. This splicing behavior not only misled the public but also tremendously impacted Kerry's election campaign. His political opponents' target had been achieved. Though the graph itself had been proven fake, this attack had not only achieved its goal, but also brought out a terrible credit crisis to the public.

Meanwhile, it's been easier to conduct digital image splicing in recent years. Whether modern image editing software like Photoshop or image generation models like Imagen are making image splicing effortless.

In order to face the challenge brought by image splicing, researchers began to investigate the technology of image splicing detection. The aim of image splicing detection is to recognize whether an image has been tampered with. Then locate the specific tampered area.

In summary, the image splicing detection technology is still playing a vital role in current society. This paper will review the development of modern digital image splicing detection technology and provide a fresh taxonomy view on this technology. Then this paper will look forward based on the analysis of the combination of artificial intelligence and image splicing detection. Through looking back at the classical research and analyzing novel findings, this paper wishes to provide a new channel for researchers' better understanding of this topic. Or assist researchers in better evaluating their detection technology. This paper also wishes to be a brief reference for future research works.

2. Taxonomy Analysis to Image Splicing Detection

Generally, digital image tampering methods mainly include image splicing, copy-move, etc. This paper primarily reviews image splicing detection.

Based on this, through a comprehensive analysis of papers, the following methods based on different anomaly characteristics are proposed.

2.1. Pixel Anomaly

Image splicing always results in parts from different sources in a single image. These parts obtain pixel anomaly characteristics from their original image. To detect the area anomaly, the image splicing can be proved. Further, researchers are able to clarify the borders of spliced areas.

One vital classical method is brought out by Shi et al. [1]. Their work laid the foundation for today's digital image splicing detection. Through analysis of the given image, they obtain a pixel 2-D array. Next, they conduct a block discrete cosine transform (BDCT), obtaining a matrix sized from 2×2 to N×N. The last step of BDCT is to transform the matrix into a 2-D coefficient array corresponding to its own dimension. After transformation, different moment features and Markov features are calculated to help judge if an image is spliced. The following Figure 1 describes the process.

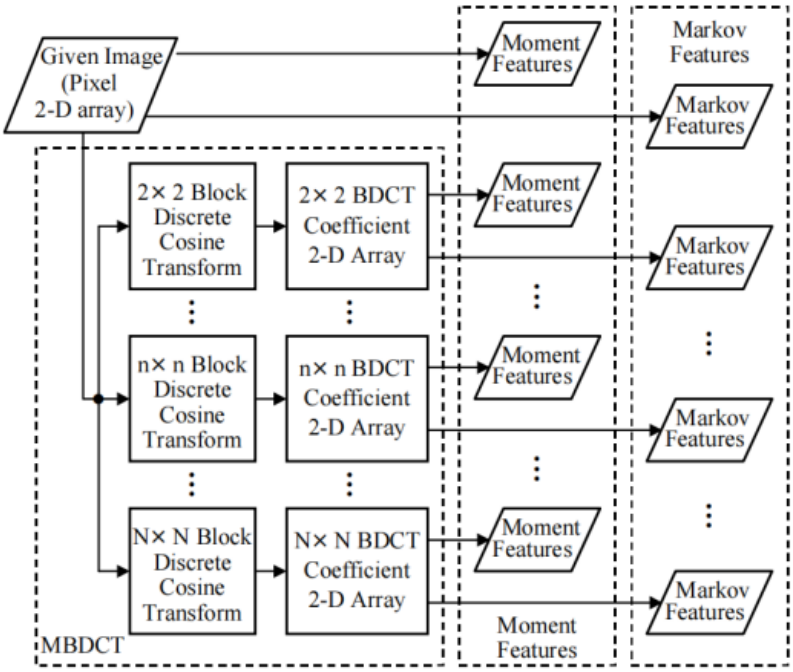

Figure 1. A natural image model frame [1]

2.2. Camera Anomaly

To realistic cameras, it has been proven that images shot by cameras definitely carry several features. This can be an easy anomaly for image splicing detection. By verifying the consistency of camera features in one image, the authenticity and credibility can be proved [2, 3].

Photo response non-uniformity (PRNU) was first stably applied to actual detection in 2012. Chen et al. proposed that a natural image should contain consistent PRNU [4]. Based on this proposal, they extracted the PRNU noise model from multiple images, and finally discovered that through execution like this, researchers can prove that if an image is spliced.

Zhang et al. proposed a solution to PRNU-based image tampering localization, as shown in Figure 2 [5]. Through a specific algorithm called SLIC, they sliced the test image into multiple-scale non-overlapping irregular blocks. Then perform PRNU correlation, calculate directly on these blocks. Finally, a tampering probability map is obtained. Additionally, if people apply CRF modeling to the probability map, the final decision map can accurately pinpoint the tampered area. The solution actually fixed probably border issues in classical methods, and improved the specific splicing area locating accuracy. According to their work, this solution performs well under the datasets shot by Sony α57, Canon 60D, Nikon D90 and Nikon D7000.

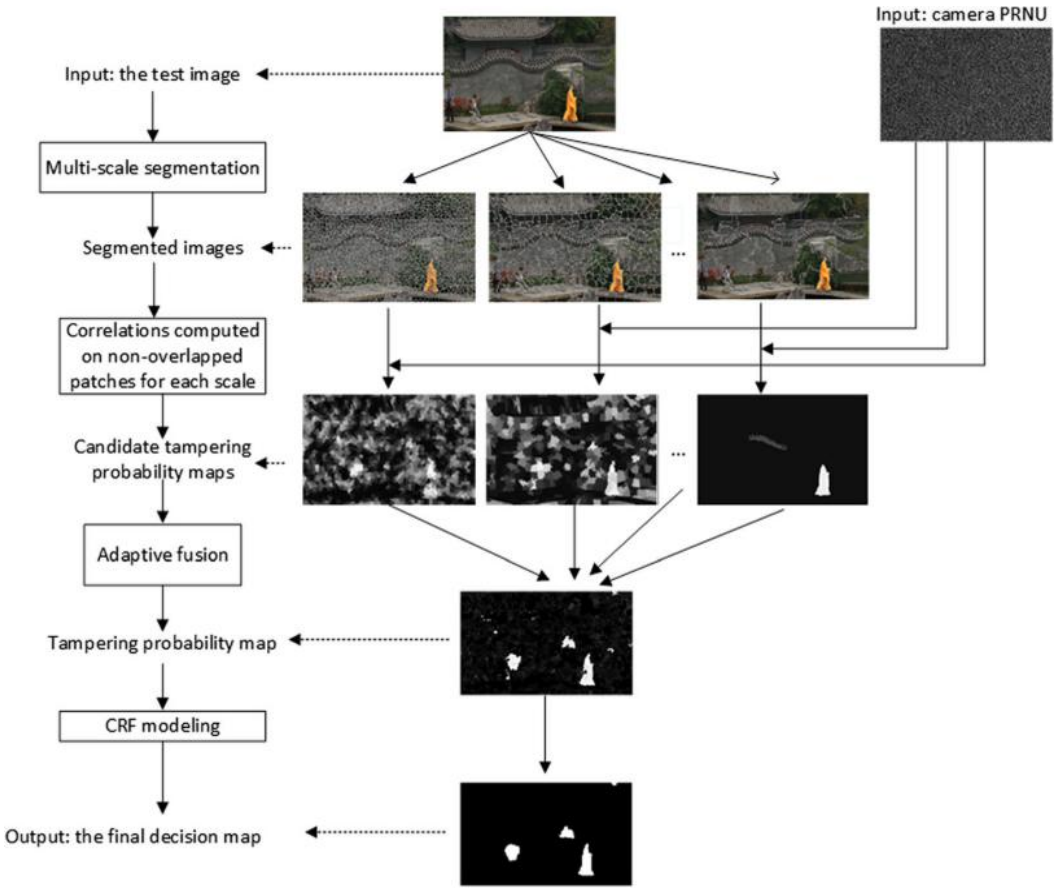

Figure 2. A multi-scale image tampering localization frame [5]

2.3. Physical Anomaly

It is easy to be aware of the fact that image splicing tampering is hard to maintain consistency in physical properties, especially lightning consistency. By capturing the inconsistency of lightning, researchers are able to verify the authenticity of the given image.

Peng et al. improved the algorithm of 3-D lighting environment estimation [6]. This algorithm analyzes the lighting property on every single pixel and constructs a 3-D lighting model based on this. Thus, the inconsistency in illumination caused by splicing is exposed. This method does not rely on deep learning or data training. Focused on detecting physical anomalies of images, it possesses great robustness to small samples. However, as the number of samples increases, due to the necessity to check every pixel's property, the efficiency will significantly reduce.

At the same time, image splicing technology is progressing in solving illumination inconsistency. It raised new challenges, or chances, to detection methods based on physical anomaly. Wei et al. proposed an image splicing algorithm based on enhanced optimal seam and brightness optimization, as shown in Figure 3 [7]. This algorithm performs excellently in anti-detection. In future works, this algorithm should be evaluated.

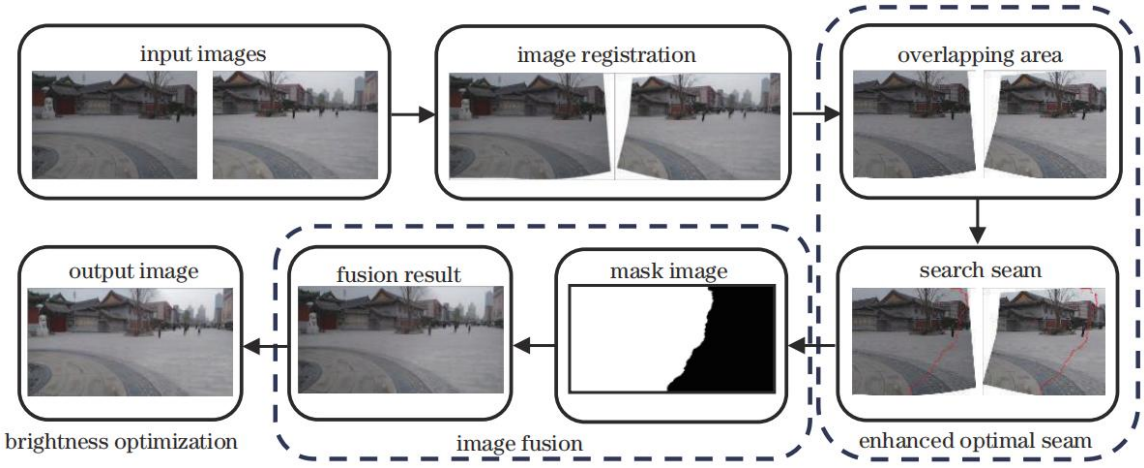

Figure 3. An anti-detection image splicing algorithm [7]

2.4. Deep Learning-Based Splicing Detection Methods

Research on image splicing forgery detection centers on overcoming the limitations of existing methods, such as multi-scale missed detection, low localization accuracy, poor computational efficiency, and sensitivity to sample imbalance. This has led to the formation of a universal technical logic: "enhancing differences → precise capture → efficient integration → optimizing bias." In the preprocessing stage, CLAHE is used to enhance hidden features or introduce image residual features to highlight pixel differences. In the feature processing stage, multi-scale mechanisms (such as multi-level convolution and dilated convolution) are employed to cover forgery regions of different sizes. Global/local attention mechanisms (such as GAB and MBAM) are combined to focus on tampering traces, and modules or progressive strategies like MFFB and SCAM are used to achieve multi-source/multi-layer feature fusion. Network structures mostly adopt a dual-branch/dual-channel design (such as the semantic + noise branches of MSNP-Net and the original + residual feature channels of DAAD-Net) to complement information. Some studies also balance precision and efficiency through a "modified CNN + SVM" combination of traditional and deep learning methods, while addressing sample imbalance through weighted binary cross-entropy loss combined with dice loss. Among them, Shivnarayan Ahirwar's RAMFF-Net demonstrates a research trend that centers on deep learning and integrates attention mechanisms, multi-scale, and multi-branch techniques while also considering the efficiency of traditional algorithms. All of these ultimately point to the goal of enhancing the performance of "high-precision detection + efficient localization" for image splicing forgery on the CASIA dataset.

Kaur's article presents a novel hybrid method that integrates an improved Convolutional Neural Network (CNN), a Support Vector Machine (SVM) classifier, and Contrast Limited Adaptive Histogram Equalization (CLAHE) [7]. CLAHE is used to enhance hidden features obscured by forgery operations. The improved CNN achieves high classification accuracy through complex feature extraction techniques without the need for customized algorithms. The SVM is included due to its excellent processing speed and efficiency. The three components work together to address the limitations of existing deep learning models in terms of computational efficiency and accuracy, thereby enhancing the performance of image splicing forgery detection.

Ahirwar's article proposes a method for detecting and localizing multi-scale splicing forgeries in images using a Residual Attention and Multi-level Feature Fusion Network (RAMFF-Net) [8]. The method first integrates multi-level convolutional feature maps through an encoder to optimize feature representation and enhance the model's ability to locate forgery regions of different scales. It then refines the features further using a Multi-level Feature Fusion Block (MFFB) to increase the relevance of task-related regions and reduce irrelevant information. A Global Attention Block (GAB) is also designed to capture the extended relationships between different parts of the image to handle complex

forgery situations. The method achieved significant results on the CASIA dataset, with an F1 score of 89.7%, outperforming existing advanced methods.

Liang's study proposes a Multi-scale Feature Attention Fusion Network (MFAF-Net) [9]. The Multi-scale Atrous Feature Attention (MAFA) module is used to capture rich contextual features and achieve multi-scale high-level feature fusion. The Multi-branch Attention Mechanism (MBAM) module fuses contextual information from each branch to process low-level features, enhancing the ability to generate finer pixel-level attention from low-level features. At the same time, MFAF-Net uses weighted binary cross-entropy loss and dice loss to overcome the problem of positive and negative sample imbalance.

Zhang's article proposes a Dual-branch Multi-scale Noise-guided Progressive Network (MSNP-Net) for image splicing forgery detection and localization [10]. The multi-resolution branch uses HR-Net as the backbone to extract deep semantic features of the image and suppress redundant noise. The multi-scale noise-guided branch extracts a noise map through an improved Bayar convolution and captures subtle tampering traces through a noise-guided module, guiding the network to strengthen spatial structure feature learning. The two branches complement and constrain each other. The network uses a progressive mechanism to fuse features of different scales and aggregates feature expressions through a Spatial Channel Attention Module (SCAM). It also optimizes performance through relevant loss functions.

Xings' article proposes a Dual-channel Enhanced Attention Dense Convolutional Network (DAAD-Net) model [11]. The model consists of three parts: backbone network feature extraction, enhanced attention feature extraction, and tampering region detection. The backbone network feature extraction module fuses the features of the original tampered image with the image residual features and inputs them into the backbone network to extract feature maps. The enhanced attention feature extraction module extracts tampering region features from high and low layers through hierarchical encoding and decoding operations. Finally, the feature maps from each layer are sent to the tampering region detection module, and the network parameters are optimized in combination with the losses of each feature map.

3. Datasets

To evaluate a method or algorithm in image splicing detection, datasets play a vital role in this final phase. As far as the author's knowledge goes, there is an extremely rich selection of datasets. The time span ranges from 2004, Columbia Gray, the foundation of modern datasets, to the present, diverse and segmented choices. Table 1 presents a few common datasets at the current time.

Table 1. Common datasets

Datasets	First Release	Version	Resolution	Image Count	Feature
Columbia	2004	Gray	128×128	1845	Foundation of modern datasets
Columbia	2006	Color	757×568/1152×768	363	Introduce a color image and a tampered area mask
CASIA	2009	v1.0	384×256	1721	A large number of images, using the JPEG format
CASIA	2009	v2.0	240×160/900×600	12614	
IMD	2011	Origin	3000×2300	96	Introduce high-resolution images and a refined tampering area mask
IMD	2020	Synthetic	ALL	70000	
IMD	2020	Manual	ALL	4000	
Wild Web	2015	Origin	ALL	13577	Get the image directly from the Internet

4. Conclusion

This paper provides a brief review of classical methods for image splicing detection from three categories which are pixel anomaly, camera anomaly, and physical anomaly. As for new methods,

specifically methods based on deep learning, the principles and advantages of several approaches are analyzed. At the same time, it is also recognized that there is a lack of more versatile methods among existing methods, as well as various issues with modern datasets.

The future belongs to artificial intelligence. Deep learning methods are going to gain further substantial development. According to the analysis of new deep learning methods, it becomes evident that cross-fusion deep learning networks may reveal an innovative, clear research path. By combining the advantages of neural networks, the reliability of detection can be enhanced.

Regarding the development of artificial intelligence, datasets should also emphasize image splicing data involving the participation of artificial intelligence. Hereby, this paper provides researchers with a means to test their algorithms against AI-generated splicing images. Meanwhile, it is necessary to integrate the advantages of previous datasets, striving for a large amount, a full range of resolution, and introducing the tampering area mask.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Shi Y Q, Chen C, Chen W. A natural image model approach to splicing detection. In Proc. 9th Workshop on Multimedia & Security, Dallas, TX, USA, 2007: 51 - 62.

[2] Zheng L, Zhang Y, Thing V L. A survey on image tampering and its detection in real-world photos. Journal of Visual Communication and Image Representation, 2019, 58: 380 - 399.

[3] Chen C, McCloskey S, Yu J. Image splicing detection via camera response function analysis. In Proc. 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 2017: 1876 - 1885.

[4] Chen Y, Thing V L. A study on the photo response non-uniformity noise pattern-based image forensics in real-world applications. In Proc. 2012 IEEE International Conference on Image Processing, 2012.

[5] Zhang W, Tang X, Yang Z, et al. multi-scale segmentation strategies in PRNU-based image tampering localization. Multimedia Tools and Applications, 2019, 78: 20113 - 20132.

[6] Peng B, Wang W, Dong J, Tan T. Optimized 3D lighting environment estimation for image forgery detection. IEEE Transactions on Information Forensics and Security, 2017, 12 (2): 479 - 494.

[7] Kaur N. Hybrid image splicing detection: integrating CLAHE, improved CNN, and SVM for digital image forensics. Expert Systems with Applications, 2025, 273: 126986.

[8] Ahirwar S, Pandey A. Enhancing multiscale splicing forgery detection in images through RAMFF-net. Signal, Image and Video Processing, 2025, 19: 770.

[9] Liang E, Zhang K, Hua Z, Jia X. Multi-scale feature attention fusion for image splicing forgery detection. ACM Transactions on Multimedia Computing, Communications, and Applications, 2025, 21 (1): 18.

[10] Zhang D, Jiang N, Li F, Chen J, Liao X, Yang G, Ding X. Multi-scale noise-guided progressive network for image splicing detection and localization. Expert Systems with Applications, 2024, 257: 124742.

[11] Xing J, Tian X, Han Y. A dual-channel augmented attentive dense-convolutional network for power image splicing tamper detection. Neural Computing and Applications, 2024, 36: 8301 - 8316.