Journal of
Information Hiding
and Privacy Protection

Tech Science Press

DOI: 10.32604/jihpp.2022.039766
Review

An Overview of Image Tamper Detection

Xingyu Chen*

Engineering Research Center of Digital Forensics of Ministry of Education, School of Computer, Nanjing University of Information Science & Technology, Nanjing, 210044, China
*Corresponding Author: Xingyu Chen. Email: 20201220006@nuist.edu.cn

Received: 01 February 2023; Accepted: 06 March 2023

Abstract: With the popularization of high-performance electronic imaging equipment and the wide application of digital image editing software, the threshold of digital image editing becomes lower and lower. This makes it easy to trick the human visual system with professionally altered images. These tampered images have brought serious threats to many fields, including personal privacy, news communication, judicial evidence collection, information security and so on. Therefore, the security and reliability of digital information has been increasingly concerned by the international community. In this paper, digital image tamper detection methods are classified according to the clues that they rely on, detection methods based on image content and detection methods based on double JPEG compression traces. This paper analyzes and discusses the important algorithms in several classification methods, and summarizes the problems existing in various methods. Finally, this paper predicts the future development trend of tamper detection.

Keywords: Image forensics; image tampering traces; image tampering detection

1 Introduction

With the development of the Internet and the popularity of smart phones, the production of digital images is becoming more and more convenient, and the information carrier of digital images is also playing a more and more important role in people's life. Image can record and disseminate information, and the richness of the things it records far exceeds that of other information carriers. The increasingly powerful image processing technology makes the threshold of digital image editing lower and lower. With handy image-processing software, people can easily alter the contents of images, some of which can't be directly discernible to the naked eye. These images are widely used as evidence and to support historical records in forensic investigations, photojournalism, criminal investigations, law enforcement, insurance claims and medical imaging. With the frequent occurrence of all kinds of fake digital images, people have serious doubts about the authenticity of digital images. Such behavior may not only have a huge impact on personal reputation and interests, but also indirectly have a negative impact on social stability and unity, and may even have a huge impact on national security. Therefore, some important digital image application fields, such as national security departments, government departments and commercial departments, should strengthen the detection of image authenticity. Ensure the authenticity and originality of digital images.

Image tampering technology refers to the use of some means to modify or remove the real content in the image scene, or to add some things that do not actually exist in the scene, and finally with the help of image processing/editing technology to cover up the traces of tampering. The purpose of digital image forensics is to solve a series of issues related to image authentication, such as: the image through what kind of imaging equipment, its generation method is credible, whether it has been tampered with some operations, tampered area in the image position and so on. The basic principles of digital image forensics are: In the process of digital image generation, the actual scene content, the characteristics of camera hardware and software processing and other factors will leave some inherent features in the image. When the image is tampered with, the inherent features in the original image will be damaged or changed to varying degrees. By extracting and detecting the inherent features in the image, the related image forensics problems can be solved. After nearly two decades of development, digital image forensics technology for image analysis refinement degree is constantly improving. Earlier forensic techniques could only tell whether a given image had been tampered with, not which areas or pixels of the image had been tampered with. Obviously, compared with image-level prediction, pixel-level prediction can provide more detailed and effective information about tampering and is more in line with the requirements of real application scenarios. Therefore, in recent years, more and more researchers pay attention to the problem of image tampering location, and new image tampering location methods keep emerging. On the other hand, the basic tools that forensic technology relies on have changed. With the remarkable performance of deep learning in computer vision and other applications, various deep learning models have been introduced into image forensics. The combination of deep learning technology and domain knowledge of image forensics improves the performance of forensic methods.

2 Detection Method Based on Image Content

What appears in the real world will be recorded in the digital image taken, and the content recorded in a real image must meet certain natural laws. If the contents of the image violate these rules, the image can be considered doctored.

2.1 Illumination Consistency-Based Methods

In the process of using the camera to take a picture, the lighting information in the scene is also recorded in the picture. The light and dark outline left by the same light source on the object and the shadow cast on the background meet certain rules, so we can use these information to estimate the position and size of the light source. Inconsistencies in the estimated light sources of different objects in an image can be used as evidence that the image has been tampered with. In literature [1], light source inconsistency was used for tamper detection for the first time. This paper estimates the orientation and nature of light source by using the boundary contour formed by light on an object. The reference [2] used Spherical harmonics (SH) to model the multi-light scene. This method can be applied to multi-light source scenarios. Literature [3] estimated the light source by using the shadow cast on the background by the light passing through the object. The method in reference [3] can also be used to find the areas with inconsistent lighting in the image.

At present, the tamper detection method using illumination consistency has been able to model relatively complex light fields and environments, but it is difficult to fully simulate various actual scenes. In future studies, it is also necessary to combine computer vision and computer image processing knowledge to more accurately model the light source and scene. In addition, many detection algorithms based on illumination consistency still need human operation in some aspects, so future research can focus on improving the degree of automation of these algorithms.

2.2 Feature Extraction and Classification-Based Methods

In the process of image tampering, there will be some discontinuous and unnatural distortion. The natural image is satisfied with certain distribution, and the tampering of the image will destroy the original distribution of the natural image. The method based on feature and classifier can use the designed features to detect whether an image conforms to the natural distribution, so as to determine whether the image has been tampered with. Methods based on feature extraction and classification can be roughly divided into three categories: methods based on general features, methods based on Markov features and methods based on SRM features. General features refer to other features besides Markov features and SRM features.

General features-based methods. Moments of wavelet characteristic function has a very good expression on Steganalysis. Literature [4] uses the 24-dimension phase consistency feature and 96 Wavelet characteristic A total of 120 dimensional Moments feature is used for tamper detection. After the image to be detected is transformed by DCT in literature [5], the real image and tampered image are distinguished by Weber local descriptor (WLD) features that can well describe image texture characteristics. Experiments show that the feature dimension and detection accuracy of WLD are better than those used in literature [4].

There is a large amount of semantic information in the brightness channel of the image, so the tampering information is covered by the semantic information in the brightness channel, while the chrominance channel of the image has only a little semantic information. Discontinuous, abrupt tampering boundaries in chroma channels are more obvious than the natural boundaries of objects. In literature [6], features are extracted from chroma channels for tamper detection: First, the image is decomposed by YCbCr, and then the Gray level cooccurrence matrix (GLCM) of the truncated Edge image is extracted in the chrominance channel (Cb channel or Cr channel) as the feature. Finally, Boosting feature selection was used to screen features to reduce computational complexity.

Run-length matrix can reflect the texture information of image well and can be used for tamper detection of image. In literature [7], the image was firstly de-correlated to reduce the influence of the smooth region on the image, and then the run-length run-number (RLRN) vector in four directions was extracted from the run matrix of the image chrominance channel for detection. Literature [8] firstly converted the image to chromaticity channel to enhance the tamper edge, and then Steerable pyramid transform (SPT) was performed on it to generate multi-directional and multi-scale subbands. Then, the Local binary pattern (LBP) histogram is extracted from the generated subbands, and these histograms are connected in series as the final features for classification.

Markov features-based methods. Markov features reflect the relationship between each pixel and its adjacent pixels [9]. The distribution characteristics of adjacent pixels in natural images will be destroyed by splicing and tampering images with unnatural boundaries and post-processing methods such as blurring and interpolation. Multi-size block discrete cosine transform (MBDCT) is a method widely used in the field of wireless communication. MBDCT was used for tamper detection in literature [10]. First, MBDCT is applied to the image to obtain a series of multi-scale representations of the image. Then, two kinds of Statistical characteristics, Markov transition probabilities and Statistical moments of characteristic equation, are extracted from the original image and the obtained MBDCT two-dimensional array characteristic functions) for tamper detection. The traditional Markov model only carries out statistics on the correlation of the model in one direction, while the 2-D noncausual Markov model used in literature [11] can synthesize information in more directions and thus model two-dimensional image signals better. The two-dimensional non-causal model proposed in literature [11] is applied to DCT domain and Discrete Meyer wavelet transform domain to extract multi-domain features for tamper detection.

Existing features have been able to achieve high detection accuracy on a single data set, but the detection accuracy is not ideal in the case of cross-data sets. In the future, it is necessary to design some more robust features to enable higher detection accuracy for various data sets. In addition, both traditional machine learning methods and deep learning methods require a large number of samples to train the model. Once the number of samples available is too small, the models learned by these methods are prone to overfitting.

2.3 Imprinting of Imaging System-Based Methods

In the process of digital image imaging, image signals will successively pass through lens, CCD, CFA interpolation and other links, which will produce special marks on the digital image. These marks may be the patterns printed on the image by the hardware system or the noise attached to the image. Although the energy of these marks is too weak to be detected by the naked eye, they can be picked up by special methods. For a real digital image, these impressions follow certain patterns. In the process of tampering, it is difficult for the tamper to keep all the imprints in the original distribution.

Imaging chromatic aberration (ICA). ICA refers to the phenomenon of chromatic aberration with different color components in parallel white light chromatic aberration. In literature [12], ICA-based method is used for tamper detection for the first time. This method firstly selects two different color channels (such as red channel and blue channel) from the three-channel, and then calculates the position difference of these two color components on the imaging plane of the same point in the natural scene. The position difference is represented by the arrow symbol. The direction of the arrow represents the symbol of color difference, and the size of the arrow represents the size of color difference. Finally, the color difference distribution of the whole image can be obtained. At present, the detection methods based on color difference still have the following problems: most of the existing algorithms are aimed at horizontal color difference detection, while the algorithm using vertical color difference is very few.

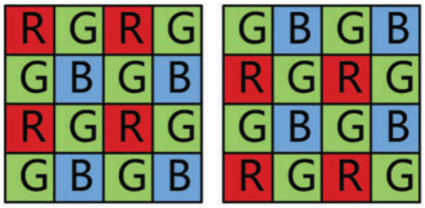
However, it is not reliable to detect tampering with only one chromatic aberration pattern. In addition, if the tampered region in the whole image is too small, the statistics of the tampered region will have too little influence on the overall color difference distribution of the image, resulting in a high detection rate. If the tampering area is too large, it will have a great impact on the global estimation model, and also affect the accuracy of detection. Therefore, only when the proportion of the tampering area in the whole image is within the appropriate range, the existing detection methods based on imaging color difference can have a high accuracy.

Natural blur. Natural blur refers to the blur brought by the imaging system in the imaging process, including Motion blur and Defocus blur/Out-of-focus blur. Motion blur is caused by the camera shaking in the process of taking a picture or the object being photographed is moving too fast, defocus blur is caused by the object being photographed is not in the focus of the camera. In the process of tampering, it is difficult for the tamper to make the tampered object completely consistent with the natural blur of the real object. Literature [13] holds that in the imaging process, two objects at the same depth relative to the camera should have the same defocusing blur. If an image violates this guideline, it is likely to have been tampered with. According to literature [14], the direction of motion blur can be estimated by objects in the image, while the amplitude of motion blur is difficult to be estimated.

Therefore, it is difficult for tamper to keep the motion blur amplitude completely consistent between tampered objects and other untampered objects. At present, the form of fuzzy kernel assumed in many algorithms is too simple, which can not simulate some real fuzzy kernel accurately, and even affect the accuracy of detection. If objects at the same depth are detected to have different defocus blurring, the image can be considered tampered with. However, if two objects are at different depths, the blur and depth information cannot be used to determine whether the image has been tampered with. It is hoped that the corresponding relationship between the depth information and the degree of ambiguity in the real image can be found in the future research, so that the fuzzy degree of objects at different depths can be used for detection.

Imaging system noise. Noise from the imaging system leaves an imprint on the image signal, which is usually consistent in an unaltered image. If the estimated system noise signals in some areas of an image are found to be inconsistent with others, the image is likely to be tampered with. In literature [15], the law of image Band-pass domain Kurtosis and the relationship between kurtosis and noise characteristics are used for tampering detection, and the noise inconsistency in an image is regarded as evidence of tampering. However, this method is not effective for images with a large number of similar textures and images with strong JPEG compression photo response non-uniformity (PRNU) noise introduces a special kind of noise into imaging equipment. This noise results from minor defects in uniformity that occur to the silicon wafers of the camera's sensing device during processing. These faults Defects can leave some special patterns in the generated image. These patterns are called PRNU noise. The noise has nothing to do with the shooting content and scene, but only depends on the camera used for imaging, which can be used as the identity of the camera. In literature [16], PRNU is first estimated using the Maximum likelihood principle, Then, the detection problem of PRNU is transformed into a hypothesis testing problem using Neyman-Pearson criterion, and finally, Optimal detection statistics is used to detect or identify the source of the camera. Because the PRNU noise-based tamper detection method needs to know the imaging device corresponding to the image to be detected or other images taken by the device, the application of this method in reality is very limited. In addition, if the Spatial resolution of the image is not high enough, it is difficult for the tamper detection method based on PRNU imprinting consistency to effectively detect the tamper in small areas in the image. The segmentation method can improve the spatial resolution of the image, and the future research can use more powerful segmentation methods to effectively detect the small area tampering in the image.

Color filter arrays (CFA). A typical photoelectric sensor can only collect information about the intensity of the light, not the wavelength. Therefore, the camera can only record light information of one color per pixel during the imaging process. Therefore, a set of color filters are added to the front of the photoelectric sensor. The filters of three colors are arranged alternately, so that the light information of three colors is interspersed and recorded in the image. The filter system is called CFA. Different cameras have different CFA interpolation modes. The two classical CFA arrays are shown in Fig. 1. In literature [17], the author proposed two algorithms for tamper detection: CFA pattern number estimation method and CFA based noise analysis method. The advantage of these two methods is that the features used do not need to be processed by complex machine learning methods, and only need to set a simple threshold to judge. Literature [18] points out that there is periodicity in the second derivative signal of the interpolated image, and proposes a tamper detection algorithm based on this periodicity, which can effectively detect both integer factor and non-integer factor interpolation methods. A Non-intrusive method of recognition of imaging equipment is proposed in literature [19]. By using only a few output images of the imaging device, the CFA interpolation coefficient of the imaging device can be calculated by linear approximation and local texture analysis, and then the imaging device can be identified. Although the method based on the consistency of CFA imprinting has been able to accurately locate the tamper region, when there are a large number of Uniform region or Sharp region in the image, the detection method may have a relatively high false alarm rate.



R	G	R	G
G	B	G	B
R	G	R	G
G	B	G	B

G	B	G	B
R	G	R	G
G	B	G	B
R	G	R	G

Figure 1: Two common CFA permutations

3 Double JPEG Compression Traces-Based Methods

JPEG compression is the most popular image transmission and storage format because it can make pictures have higher quality without occupying much space. Image tampering process may involve multiple JPEG compression, and double JPEG compression will leave traces in the image, according to which tampering detection can be carried out. The methods for tamper detection using double JPEG compression traces fall into two main categories: Detection method based on Aligned double JPEG compression hypothesis (Aligned double JPEG, A-DJPG) and detection method based on unaligned double JPEG compression hypothesis (Nonaligned double JPEG, NA-DJPG).

3.1 Aligned Double JPEG Compression Trace-Based Methods

A-DJPG means the mesh of two JPEG compressions is perfectly aligned. In the tampering process of JPEG image, the real area and the tampering area show different distribution of DCT coefficients due to the different compression process experienced by the real area and the tampering area, which can be used for tampering detection. Reference [20,21] belongs to the prospective work of A-JPEG. In these two literatures, the author introduces the causes and manifestations of the Double quantization effect of double JPEG compression. An image that has undergone only one JPEG compression will obey the Laplacian (or generalized Cauchy) distribution, which peaks at 0 and declines monotonically to its left and right. And if the image is twice JPEG compression, and the quality factor of the two compression is in a proportional relationship between Q1 and Q2, the DCT coefficient will periodically show the valley value and peak value, this phenomenon is called DQ phenomenon. In reference [22], based on the principle in reference [20,21], combined with a total of 192 DCT distribution histograms of 3 channels and DCT information of each 8∗8 image block, The Block posterior probability map (BPPM) of image blocks was calculated by Bayesian inference. Finally, the features extracted from the tamper probability graph of the whole image are put into SVM to judge whether the image has been tampered with; Benford's law, which describes the probability of a number starting with 0 to 9 in natural data, can be used to test whether statistics are falsified. It is pointed out in reference [23] that if an image has undergone only one JPEG compression, the distribution of its DCT coefficients conforms to Benford's law. If the image is compressed more than once, this rule is broken. The above method is only effective if the two JPEG compression quality factors are not the same. In double JPEG compression, if the quality factor of two compressions is the same, other methods are needed for effective detection. A method of perturbation strategy based on Random jitter strategy was designed in reference [24] to distinguish the perturbation factors of new images with double and single JPEG recompression. This method can also detect images with 3 or even 4 JPEG recompression. In reference

[25], JPEG image Error blocks are constructed first, and then Truncating and Rounding error blocks are used. 13-dimensional Error based statistical features (EBSF) were extracted for detection.

3.2 Unaligned Double JPEG Compression Trace-Based Methods

NA-DJPG means the mesh of two JPEG compressions is skewed, as shown in Fig. 2. Without considering the background image cropping, some areas are cut from a JPEG image and pasted to another BMP image and re-saved as JPEG format. In this way, the tamper area is recompressed and the non-tamper area is single compressed. The classic scenario of NA-JPEG dual compression is image Mosaic. In this forgery, it is assumed that an area in the JPEG image is cropped and pasted onto the host image in BMP format, and the resulting composite image is saved in JPEG format. As shown in Fig. 3, (a) is the splicing image, (b) is the DCT grid diagram of some areas in the splicing image, where the dotted line represents the DCT grid of the splicing material in the original image, the solid line represents the DCT grid when the image is saved after splicing, (c) is the mask of the splicing image, and the green area (non-tampering area) is the single compression. The red area (tamper area) is unaligned recompression. In this scenario, the NA-DJPEG detection tool can be used to assist in distinguishing between the original and tamper regions. Assuming that the forgery region is placed randomly, the probability of NA-DJPEG compression artifacts appearing in the forgery region is up to 63/64.

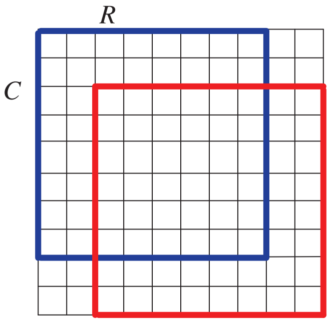


Figure 2: Misalignment of DCT grids between two compressions

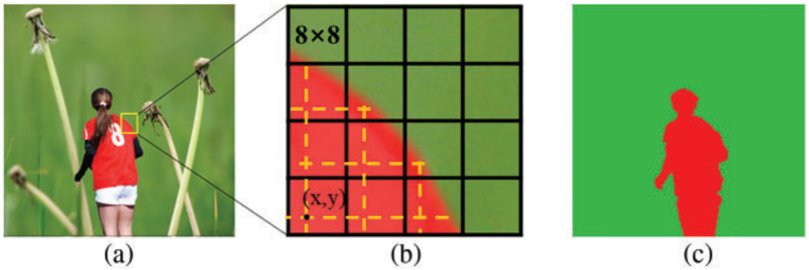


Figure 3: Schematic diagram of unaligned double JPEG compression

In this paper [26], Blocking artifact characteristics matrix (BACM) is used to detect the double compressed image. The paper states that BACM is symmetric in images that have undergone a single JPEG compression, while NA-DJPG breaks this symmetry. Reference [27] pointed out that BACM was prone to interference from image semantic information, so it could not be used as reliable measurement to distinguish NA-DJPGs. In this paper, it was proposed to use block blocking artifacts to detect NA-DJPGs. The periodic feature of block effect is extracted from the difference of quantization error of adjacent DCT blocks, which is less disturbed by semantic information than BACM. Literature [28] analyzes in detail the periodicity characteristics of JPEG image in spatial domain and transform domain, and uses the joint characteristics of spatial domain and transform domain to detect JPEG recompression. It is worth noting that this method can detect both A-DJPG and NA-DJPG. Compared with the periodic feature of block effect [27], the feature proposed in literature [28] is less susceptible to the influence of image semantic information, and can also dig deeply into the block effect characteristics of JPEG images. In literature [29], based on literature [26], a Noisy convolutive mixing mode is used to model NA-DJPG. Literature [29] pointed out that NA-DJPG would destroy the independence of block DCT, so an Independent component analysis (ICA) method was designed for detection. Experiments show that the detection accuracy of the method used in literature [29] is significantly higher than that of BACM [26]. It was pointed out in reference [30] that if the block DCT coefficient of an NA-DJPG image is calculated according to the grid of the first JPEG compression, the DCT coefficient will present an Integer periodicity. Based on the above observations, this paper designs a detection method: after extracting features from DCT coefficients, a simple threshold detector is needed to detect NA-DJPG in images, instead of using a classifier to classify complex features as in literature [26–29]. Literature [31] proposes A new statistical model, which can be used to model A-DJpg and NA-DJPG in the image, and calculate the probability of each 8∗8 DCT block being recompressed, so as to realize the location of the tamper region. Literature [32] has analyzed the influence of NA-DJPG on DCT coefficient in detail, and proposed a model that can simulate NA-DJPG in tampered images. This model can be used to effectively estimate the quantization noise brought by NA-DJPG, so as to realize the detection and localization of NA-DJPG. Experiments show that the detection accuracy of the method used in literature [32] is higher than that in literature [30] and literature [31].

Detection methods based on double JPEG compression traces also have some drawbacks: although most images available on the Internet are in JPEG format, some are stored in other formats, which makes them impossible to detect. In addition, most methods carry out tampering detection by counting the coefficients of each DCT block of an image. If the tampering area is too small, tampering will have limited influence on the overall DCT distribution of an image, and tampering traces will be difficult to detect. Many detection algorithms are effective only when the first compression coefficient is known, which is difficult to know in the real world. Many current algorithms can only be effectively detected when the quality factor Q1 of the first JPEG compression and Q2 of the second JPEG compression satisfy a specific relationship. It is hoped that this condition can be gradually relaxed in future research.

4 Evaluation Index of Tamper Detection Performance

The evaluation criteria of detection methods need to use the classification quantity of samples, including true class, false negative class, true negative class and false positive class. For a binary classification problem, the samples are divided into positive and negative categories according to the real label. If a positive sample is classified as positive, it is called True positive (TP). If a positive sample is classified as a negative class, it is called a False negative class (FN); If a negative sample is classified as a negative class, it is called True negative (TN); If a negative sample is classified as positive, it is said to be False negative (FN). Image level tamper detection is a simple binary problem, while pixel level tamper detection is a binary problem of each pixel. Therefore, the performance of tamper location model can be measured by the commonly used classification evaluation index. Commonly used evaluation indicators mainly include: Accuracy (ACC), F1-score (F1-score), Area Under the Curve (AUC), Matthews Correlation Coefficient (Matthews Correlation Coefficient, MCC) and Intersection over Union (IoU). The definition and applicability of these performance indicators are briefly described below.

Where, TPR represents the proportion of all positive samples that are correctly classified; FPR represents the percentage of all negative samples that are misclassified. The higher the TPR, the stronger the classifier performance, and the lower the FPR, the stronger the classifier performance. The values of TPR and FPR are between 0 and 1. ACC represents the accuracy rate of classification of all samples. The higher ACC is, the stronger the classifier performance is. ACC is between 0 and 1. This measure is less applicable to cases where two types of samples are not balanced.

ACC. Accuracy gives the same weight to both positive and negative samples, and in actual tampering scenes, there is usually a serious imbalance between tampered pixels and original pixels. For data sets with seriously unbalanced ratio of positive and negative samples, taking precision as an evaluation index of tamper location performance can not effectively measure the quality of a model. The prediction accuracy of the model is given by the following formula:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

F1-score. In the case of unbalanced sample categories, the accuracy can not objectively reflect the performance of the model, and another more appropriate performance index is F1-score. F1-score is the harmonic average of Precision and Recall. The formula is as follows:

$$F1 = 2 \times \frac{precision \times Recall}{precision + Recall} \tag{2}$$

The Precision and recall ratios are defined as $Precision = TP/(TP + FP)$, $Recall = TP/(TP + FN)$. Since F1-score comprehensively considers the accuracy and recall ratio, it can better measure the performance of the tamper positioning model than the accuracy.

AUC. The Receiver Operating Characteristic curve (ROC curve) is usually used to demonstrate the performance of the classification model. The ROC curve takes false positive rate and true positive rate as the horizontal and vertical axes respectively to comprehensively reflect the relationship between them. The area under ROC curve, or AUC, is an important index to evaluate the performance of classification models. The value of AUC ranges from 0 to 1, and the larger the value, the better the classification performance of the model.

MCC. MCC is also an index often used to evaluate the performance of unbalanced classification problems. Its calculation formula is as follows:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{3}$$

The value of MCC is between −1 and 1. −1 indicates that the classifier completely separates positive and negative samples; 0 indicates that the classifier's performance is comparable to random guesses; 1 indicates that the classifier can achieve perfect classification.

IoU. In tamper localization, the IoU commonly used in the field of image semantic segmentation is sometimes used to evaluate the performance. At this point, IoU is denoted as the ratio between the intersection area of the model predicted tampering area and the actual tampering area and the area of their union, which can be calculated according to the following formula:

$$IoU = \frac{TP}{TP + FP + FN} \tag{4}$$

The value of IoU ranges from 0 to 1, with a larger value indicating better model performance.

5 Conclusion

With the rapid development of science and technology in recent years and the significant improvement of computing performance of hardware equipment, digital image forensics technology has also made great progress, and there are many new factions and branches. Although new technology and new methods are put forward constantly, there are still many problems that have not been effectively solved. In this paper, the existing algorithms in each class of methods are analyzed in detail. In addition, this paper also lists the performance indicators used in several tamper detection methods. In view of the complexity and diversity of digital image forensics technology, we still need to rely on relevant knowledge of various disciplines, and constantly combine with practical problems to develop new methods. On the other hand, the combination of tamper detection knowledge and deep neural network is also an important development direction of new tamper detection technology in the future.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in *Proc. of the 7th Workshop on Multimedia and Security (MM&Sec '05)*, New York, NY, USA, pp. 1–10, 2005.

[2] E. Kee, J. F. O'Brien and H. Farid, "Exposing photo manipulation with inconsistent shadows," *ACM Transactions on Graphics*, vol. 32, no. 3, pp. 1–12, 2013. https://doi.org/10.1145/2487228.2487236

[3] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 450–461, 2007. https://doi.org/10.1109/TIFS.2007.903848

[4] W. Chen, Y. Q. Shi and W. Su, "Image splicing detection using 2D phase congruency and statistical moments of characteristic function," in *Proc. of SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, United States, pp. 281–288, 2007.

[5] X. X. Liu, F. Li and B. Xiong, "Image splicing detection using weber local descriptors," *Computer Engineering and Applications*, vol. 49, no. 12, pp. 140–143, 2013.

[6] W. Wei, J. Dong and T. N. Tan, "Effective image splicing detection based on image chroma," in *Proc. of the 16th IEEE Int. Conf. on Image Processing*, Cairo, Egypt, pp. 1257–1260, 2009.

[7] X. Zhao, J. Li, S. Li and S. Wang, "Detecting digital image splicing in chroma spaces," in *Int. Workshop on Digital Watermarking*, Berlin, Heidelberg, pp. 12–22, 2010.

[8] G. Muhammad, M. H. Al-Hammadi, M. Hussain and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, vol. 25, no. 4, pp. 985–995, 2014.

[9] Y. Q. Shi, C. H. Chen and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," in *Information Hiding*, Berlin, Heidelberg, Springer, pp. 249–264, 2006.

[10] Y. Q. Shi, C. H. Chen and W. Chen, "A natural image model approach to splicing detection," in *The 9th Workshop on Multimedia & Security-MM&Sec '07*, New York, NY, USA, pp. 51–62, 2007.

[11] X. D. Zhao, S. L. Wang, S. H. Li and J. H. Li, "Passive image-splicing detection by a 2-D noncausal Markov model," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 2, pp. 185–199, 2015.

[12] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in *The 8th Workshop on Multimedia and Security*, New York, NY, USA, pp. 48–55, 2006.

[13] X. Wang, B. Xuan and S. L. Peng, "Digital image forgery detection based on the consistency of defocus blur," in *Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, Harbin, China, pp. 192–195, 2008.

[14] P. Kakar, S. Natarajan and W. Ser, "Detecting digital image forgeries through inconsistent motion blur," in *IEEE Int. Conf. on Multimedia and Expo*, Singapore, pp. 486–491, 2010.

[15] S. W. Lyu, X. Y. Pan and X. Zhang, "Exposing region splicing forgeries with blind local noise estimation," *International Journal of Computer Vision*, vol. 110, no. 2, pp. 202–221, 2014. https://doi.org/10.1007/s11263-013-0688-y

[16] M. Chen, J. Fridrich, M. Goljan and J. Lukas, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[17] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in *Proc. of the 16th IEEE Int. Conf. on Image Processing*, Cairo, Egypt, pp. 1497–1500, 2009.

[18] A. C. Gallagher, "Detection of linear and cubic interpolation in JPEG compressed images," in *Proc. of the 2nd Canadian Conf. on Computer and Robot Vision*, Victoria, BC, Canada, pp. 65–72, 2005.

[19] A. Swaminathan, M. Wu and K. J. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91–106, 2007.

[20] J. Lukáš and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. of Digital Forensic Research Workshop*, Cleveland, OH, USA, pp. 5–8, 2003.

[21] A. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proc. of Int. Workshop on Information Hiding*, Berlin, Heidelberg, pp. 128–147, 2004.

[22] Z. C. Lin, J. F. He, X. O. Tang and C. -K. Tang, "Automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognition*, vol. 42, no. 11, pp. 2492–2501, 2009.

[23] D. D. Fu, Y. Q. Shi and W. Su, "A generalized Benford's Law for JPEG coefficients and its applications in image forensics," in *Proc. of SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, United States, vol. 6505, pp. 574–584, 2007.

[24] F. J. Huang, J. W. Huang and Y. Q. Shi, "Detecting double JPEG compression with the same quantization matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 848–856, 2010. https://doi.org/10.1109/TIFS.2010.2072921

[25] J. Q. Yang, J. Xie, G. P. Zhu, S. Kwong and Y. Q. Shi, "An effective method for detecting double JPEG compression with the same quantization matrix," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1933–1942, 2014.

[26] W. Q. Luo, Z. H. Qu, J. W. Huang and G. Qiu, "A novel method for detecting cropped and recompressed image block," in *2007 IEEE Int. Conf. on Acoustics, Speech and Signal Processing-ICASSP '07*, Honolulu, HI, USA, pp. II–217, 2007.

[27] Y. L. Chen and C. T. Hsu, "Image tampering detection by blocking periodicity analysis in JPEG compressed images," in *2008 IEEE 10th Workshop on Multimedia Signal Processing*, Las Vegas, NV, USA, pp. 803–808, 2008.

[28] Y. L. Chen and C. T. Hsu, "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 396–406, 2011. https://doi.org/10.1109/TIFS.2011.2106121

[29] Z. H. Qu, W. Q. Luo and J. W. Huang, "A convolutive mixing model for shifted double JPEG compression with application to passive image authentication," in *2008 IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Las Vegas, NV, USA, pp. 1661–1664, 2008.

[30] T. Bianchi and A. Piva, "Detection of nonaligned double JPEG compression based on integer periodicity maps," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 842–848, 2012. https://doi.org/10.1109/TIFS.2011.2170836

[31] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1003–1017, 2012. https://doi.org/10.1109/TIFS.2012.2187516

[32] S. L. Wang, A. W. C. Liew, S. H. Li, Y. J. Zhang and J. H. Li, "Detection of shifted double JPEG compression by an adaptive DCT coefficient model," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, pp. 101, 2014.