DOI: 10.24996/ijs.2024.65.5.33

ISSN: 0067-2904

A Review Study on Forgery and Tamper Detection Techniques in Digital Images

Marwa Emad Mahdi*, Nada Hussein M Ali

Computer Department, College of Sciences, University of Baghdad, Baghdad, Iraq

Received: 16/10/2022 Accepted: 6/5/2023 Published: 30/5/2024

Abstract

Digital tampering identification, which detects picture modification, is a significant area of image analysis studies. This area has grown with time with exceptional precision employing machine learning and deep learning-based strategies during the last five years. Synthesis and reinforcement-based learning techniques must now evolve to keep with the research. However, before doing any experimentation, a scientist must first comprehend the current state of the art in that domain. Diverse paths, associated outcomes, and analysis lay the groundwork for successful experimentation and superior results. Before starting with experiments, universal image forensics approaches must be thoroughly researched. As a result, this review of various methodologies in the field was created. Unlike previous studies that focused on picture splicing or copy-move detection, this study intends to investigate the universal type-independent strategies required to identify image tampering. The work provided analyses and evaluates several universal techniques based on resampling, compression, and inconsistency-based detection. Journals and datasets are two examples of resources beneficial to the academic community. Finally, a future reinforcement learning model is proposed.

Keywords: - Image, Tampering, Passive approach, Forgery Detection.

نظام مصادقة للكشف عن التزوير والنسخ في الصورة الرقمية

مروه عماد مهدي* ،ندى حسين محمد علي

قسم الحاسوب ، كلية العلوم ،جامعة بغداد ،بغداد ،العراق

الخلاصة

يعد التعرف على التلاعب الرقمي، الذي يكتشف تعديل الصورة، مجالًا مهمًا لدراسات تحليل الصور حيث نمت هذه المنطقة بمرور الوقت بدقة استثنائية باستخدام التعلم الآلي للاستراتيجيات القائمة على التعلم العميق خلال السنوات الخمس الماضية. هذه ال تقنيات التعلم القائم على التوليف والتعزيز يجب أيضا ان تتطور. ومع ذلك، قبل إجراء أي تجربة، يجب أولاً فهم الحالة الحالية لهذا المجال. أي يجب ان يتم توضيح المسارات المتنوعة و التي يتم من خلالها الحصول على نتائج مختلفة .وتكون هذه النتائج التي تم الحصول عليها عرضة للتحليل ليتم التعرف على مدى نجاح التجربة و تمييز طريقة عن الاخرى ، و معرفة اي طريقة تعطي نتائج افضل . قبل البدء بالتجارب، يجب إجراء بحث شامل عن طرق التحقق الجنائي للصور. نتيجة لذلك، قرر المؤلفون إنشاء مراجعة للمنهجيات المختلفة. على عكس الدراسات السابقة التي ركزت على ربط الصورة أو اكتشاف حركة النسخ، تهدف هذه الدراسة إلى التحقيق في الاستراتيجيات العالمية المستقلة عن النوع

*Email: marwa.Emad1201a@sc.uobaghdad.edu.iq

المطلوبة لتحديد التلاعب بالصور. يقدم العمل تحليلات وتقييم عدد من التقنيات العالمية القائمة على إعادة
التشكيل والضغط والاكتشاف القائم على عدم الاتساق. يتم الإبلاغ عن نهج المراجعة والأدبيات المقيمة
والملاحظات الختامية في هذه المراجعة. المجلات ومجموعات البيانات هما مثالان على الموارد المفيدة
للمجتمع الأكاديمي. أخيرًا، تم اقتراح نموذج التعلم التعزيزي المستقبلي.

1. Introduction

Digital images have largely replaced traditional photographs over the last decade. They continue to be an important component of knowledge expansion in traditional regular communication, such as social networks, websites, and newspapers [1]. The application of digital photographs in the field of computer-based forensics has become increasingly visible. While major advances in digital image processing have contributed to the invention of many new forensic procedures, they have also simplified image tampering. As a result, image security has become a crucial concern in all fields that employ digital images. Tampered photos, such as images of criminals, crime scenes, biometric images, and so on, have long been employed in forensic studies [2] [3]. A digital image can quantitatively represent any scenario. Manipulating such photos has become an easy operation, even for non-specialists, as a result of simpler tools available on any device, such as smartphones and tablets. Elements are mixed in this context to generate a one-of-a-kind image that can persuade even the most seasoned set of eyes [4].

The procedure for modifying the constituents of a photograph to achieve malevolent purposes is known as digital image manipulation [5]. This form of digital picture adjustment is usually referred to as tampering, manipulation, or forgery. Photo manipulation is not a new notion; it has existed for millennia. There have been several cases of photo tampering that have enraged the general public/administrations throughout history [6]. Photoshop, paint-slinger and the (GNU) Image Manipulation Program seem to be just only a few samples of photo editing software. Only a few of these are free, while others are not, but they are easily available and fairly priced. Furthermore, photographs edited with editing tools are subjected to some rectification processes and are so realistic that the human visual system cannot tell the difference between a genuine and tampered image with the naked eye. This shows high vulnerability and decreases the reliability of digital photographs. Effective and consistent image manipulation detection techniques should be able to distinguish between authentic and tampered photos [7].

This research topic has a considerable number of scholarly publications from all over the world. From 2000 to 2019, a study was undertaken to determine the number of publications per year in digital image forensics from two separate libraries, Elsevier (sciencedirect.com) and IEEE (ieeexplore.org) as shown in Figure 1. This study investigates ways for identifying blind/passive image modification. Digital image alteration detection systems are designed to detect image forgeries. Digital image modification detection techniques are classified into two types: active and passive approaches [8].

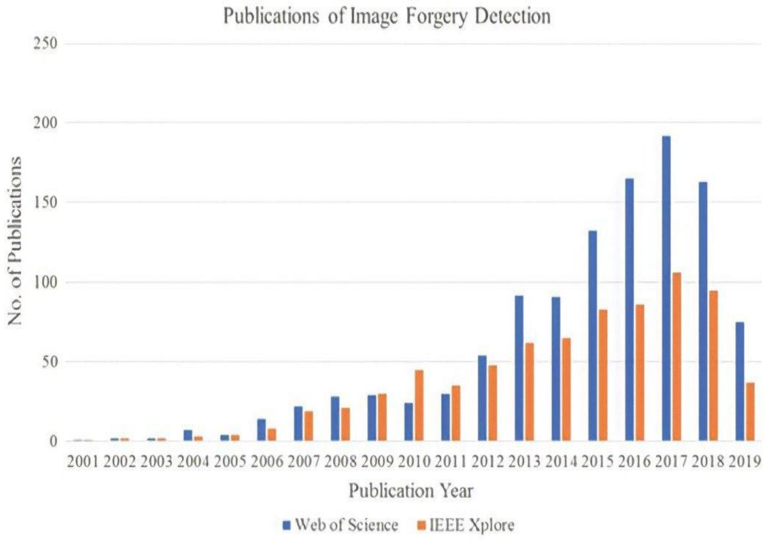


Figure 1: The number of publications per year in digital image forensics [9]

2. Passive Image Forgery Detection Techniques

Passive methods are called blind methods, which can be classified into two groups: dependent forgery and independent forgery, as shown in Figure 2. Passive methods or blind forensic methods use image statistics or the content of the image to verify its genuineness. In practical use, it is impossible to get prior knowledge for most of the cases, which makes digital image forensics remarkably important even compared to digital watermarking or Signatures.

Existing techniques identify various traces of tampering and detect them separately with the localization of tampered regions. On the other hand, one disadvantage is that it requires many prior photos to estimate the internal traces when in some cases, there is only the image in question. These strategies are predicated on the notion that digital forgeries may leave no visible signs of tampering, hence they require alternative picture statistics. As a result, it is complicated [10].

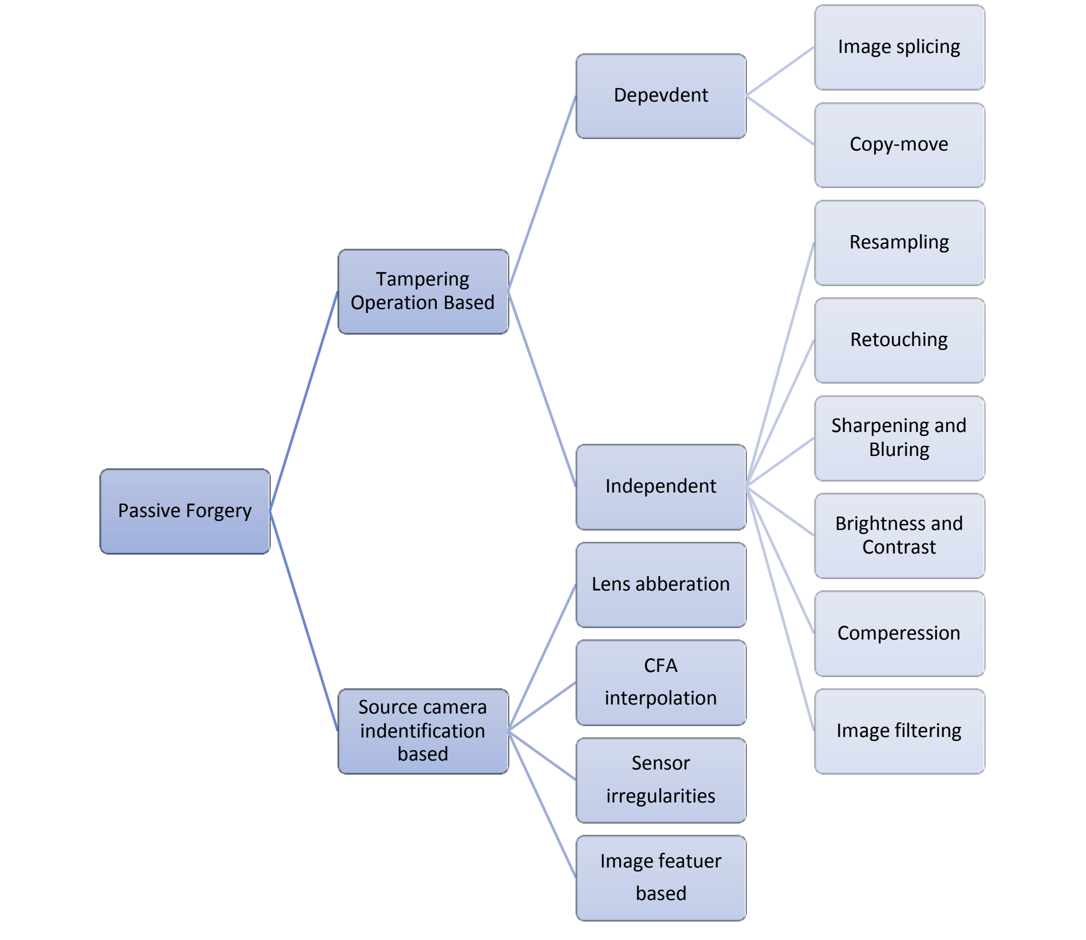
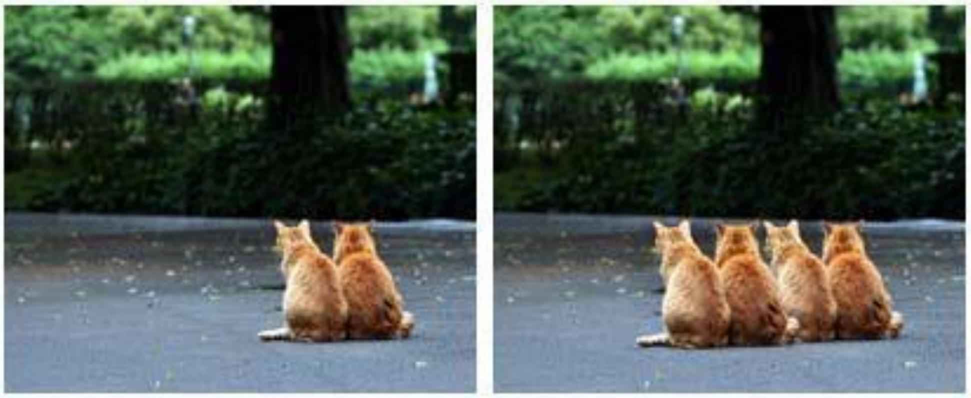


Figure 2: Categorization of passive-forgery approaches [10]

2.1 Copy Move Forgery

The first category is image tampering, which is one of the most widely used techniques to hide or add new information in an image by copying a portion of the image and pasting one or more copies of it on the same image. This technique is known as copy-move forgery [11], as illustrated in Figure 3.



(a) Original image (b) Copy-move image

Figure 3: An example of the Copy-Move Forgery process in the digital image [12]

2.2 Splicing Image Forgery

The second type is the splicing image forgery, which is the most aggressive type; it is done by cutting part of an image and splicing (pasting) it on another image. When such a process is carefully conducted, the boundaries between the splicing regions are undetectable, making this tampering dangerous [13]. Figure 4 shows an example of splicing forgery.

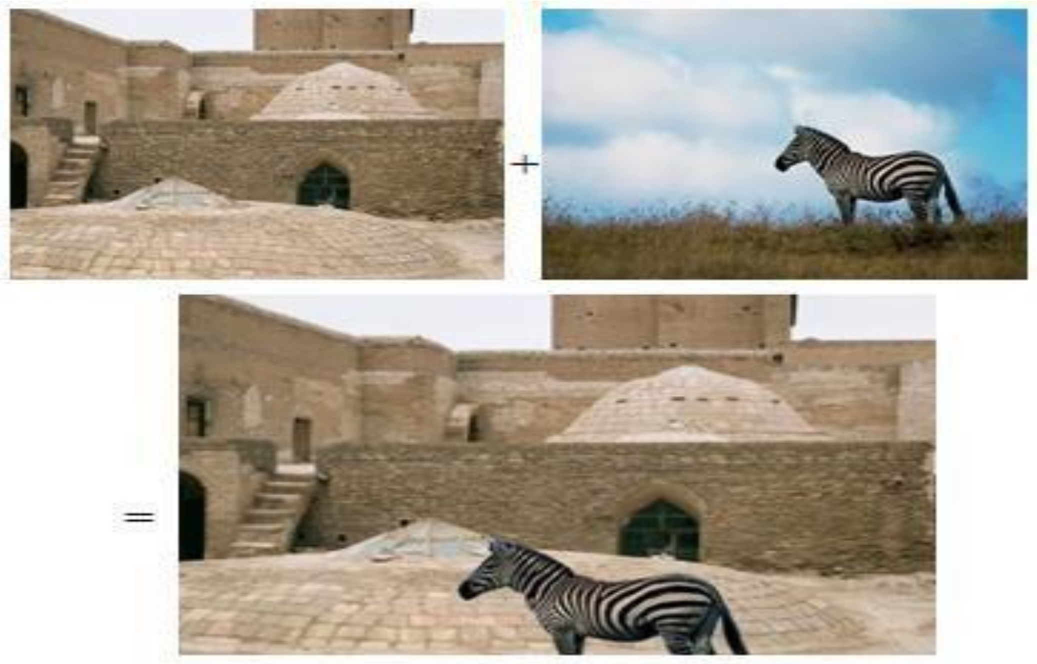


Figure 4: An example of the Splicing Forgery process in the digital image [14]

3. Related Work

Several strategies have been proposed to detect various types of image manipulation and copy transmission of fake images [15]. The primary goal of transcriptome transfer forgery detection is to classify the same regions, but the main challenge is to identify the ones comparable. Grayscale images extracted from color images through black-and-white conversion can be pre-processed in the initial stage of copy-move forgery detection algorithms or even merged more than one image into one. Where the image is processed and then, the extracted features are represented [16]. As a result, these extracted features can be used in template matching as well. Classified lexical sorting, adjacent pixels, other clustering approaches, etc [17]. Between vectors of adjacent features, a type of location estimation known as Euclidean distance is used. Finally, a specific morphological procedure is used to identify the artificial location. Figure 5 depicts the main stages used to detect any tampering occurring in the digital images.

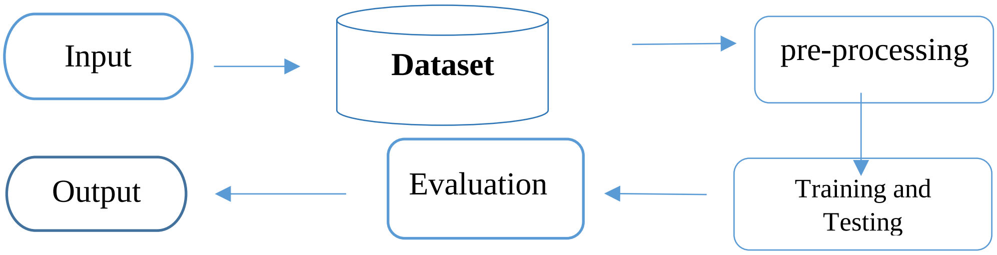


Figure 5: The main stages of image tamper detection

These steps will be illustrated by an illustrative example, which is when a group of images is taken from a specific database. The processing procedure is done by scaling the image or converting the image to another domain. After that, the image is divided into interfering or non-interfering blocks, according to the model being built. The features are extracted after that. In Feature Selection, the unnecessary features can cause some problems to appear in the model, for example slow model training time due to high dimensionality, poor performance due to useless features, and a complex model overfitting problem. To avoid such issues, selecting the best feature algorithm to be used is important. Furthermore, any feature selection methods necessitate training several candidate models to find out such a model. Feature selection strategies can be divided into three categories 1-Wrapper Strategies, 2- Filtering Strategies, 3-Embedded Strategies, and features are matched to reach the required resolution of the system. These steps are illustrated in Figure 6.

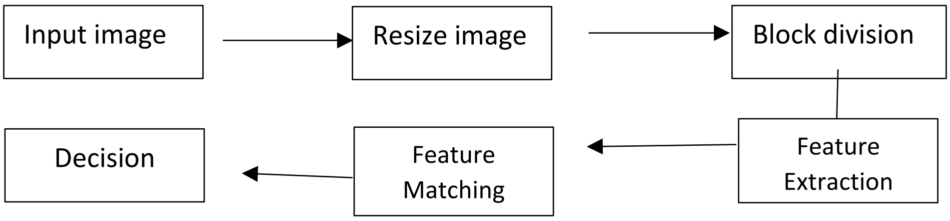


Figure 6: The steps of methods

The image tampering-related works are subdivided into subsections and will be introduced in the following.

3.1 Splicing Image Forgery-Related Work

Zhang et al. [18] proposed a method to boost the detection efficiency of the DWT-based technique. Initially, the block Discrete Wavelet Transform (DWT) was implemented on the input images; the Markov features were built to describe the dependence between wavelet coefficients across positions. Finally, Support Vector Machin (SVM) was employed to distinguish the authentic and spliced images. Experiments indicated the detection efficiency of the features obtained in DWT with 89% accuracy in the best combination of block size and the number of features.

Tianyu et al. [19] introduced a new way of investigating the convergence of features to create a model for integrating hand-crafted features with a Convolution Neural Network (CNN). To help boost the efficiency of (CNN) origin, several hand-crafted characteristics have been tested. Experiments revealed that this approach exceeded the CaffeNet origin on the Cifar10 Dataset with an accuracy of 79.16%.

Jaiswal A. et al. [20] employed a mix of four handmade features Histogram Oriented Gradient (HoG), Discrete Wavelet Transform (DWT), and Local Binary Pattern(LBP)) for creating a feature vector of the Gray image. The logistic regression classification model was then used to train these function vectors. To determine the best results, a 10-fold cross-validation test estimation method was used. Logistic regression of a machine learning classification technique was used to divide images into two classes, spliced and non-spliced images. An accuracy of 99.5% was gained with the CASIA II.0 dataset. This method was implemented and resulted in wrong results with 59% accuracy.

Habibi M and Hassanpour [21] proposed a procedure based on the color distribution of edge pixels in the neighborhood. A method of segmentation was used to boost localization efficiency and minimize total measurement time. The obtained experimental results using the Columbia Picture Splicing dataset showed an accuracy of 97%.

Salloum, et al [22] developed a technique for localizing image-splicing attacks that is entirely based on Fully Convolutional Networks (FCN). They started by testing a single-task FCN (SFCN) that had only been trained on the surface label. Despite outperforming existing methods, the SFCN produces coarse localization results in some cases. Thus, for multi-task learning, they suggested using a multi-task FCN (MFCN) with two output branches. The surface label is understood by one branch, while the edge or border of the spliced region is understood by the other. The network was trained on the ASIA v2.0 dataset and tested on the CASIA v1.0 Columbia Uncompressed dataset, DARPA/NIST Nimble Challenge 2016, and Carvalho SCI datasets in trials. The SFCN and MFCN outperform existing splicing localization techniques, with the MFCN obtaining finer localization.

V. Srivastava and S. K. Yadav [23] suggested a method that converts an RGB image to a YCbCr image and extracts the Cb and Cr image components, which are more sensitive to tampering artifacts. A standard deviation (STD) filter and higher-order texture descriptors were also applied to the Cb and Cr components. The STD filter was used to highlight important elements in an image. A support vector machine classifier was used to classify counterfeit and manipulated pictures.

E. Tripathi et al [24] study examined the methodological issues related to the concept of multifractal analysis, with a focus on the Differential Box-Counting method for calculating the Intensity-Level Multi-Fractal Dimension. Furthermore, the research paper compared various cutting-edge image splicing techniques, and discovered that using Twin Support Vector Machine as a classifier with Intensity-Level Multi-Fractal Dimension as a Feature extraction method achieves significantly higher efficiency than other methods.

A. Parnak et al [25], the paper presents a novel forgery detection technique. Using traditional Benford's rule. The suggested method extracts the Mean Absolute Deviation (MAD) characteristic. Furthermore, the broadened mantissa distribution feature vector is subjected to Benford's law. Other statistical features, in addition to Benford's law-based features, were employed to generate the final feature vector. Finally, to distinguish between original and faked images, a support vector machine (SVM) with three independent kernel functions was used.
Table 1 shows the types of splicing algorithms, advantages, and disadvantages of each algorithm. Additionally, Figure 7 demonstrates the accuracy of percentage comparisons obtained from the aforementioned related works.

Table 1: The types of splicing detection algorithms

Ref	Target of Tampering	Methodology	Warrants /Drawback	Accuracy
[18]	Spliced Images	SVM-RFE	Warrants:- Method to boost the detection efficiency of the DWT-based technique. Drawback:- Low achieved accuracy compared to the methods that are published at the same time.	89% accuracy
[19]	Spliced Images	CNN	Warrants:- Some strong edge, texture, and local	79.16% accuracy

			characteristics. Secondly, CNN's collaborative teaching methodology makes features fuse easier. Drawback:- This method was private and with deep learning and achieved low accuracy.	
[20]	Spliced Images	(HoG LTE, DWT, and LBP)	Warrants:- Logistic regression of a machine learning classification technique was used to divide images into two classes, spliced and non-spliced images. An accuracy Drawback:- It does not give highly accurate results with all the data sets that are used.	Accuracy of 99.5% is gained with CASIA II.0 dataset. This method was implemented and gave wrong results with 59% accuracy
[21]	Spliced Images	Interquartile Range (IQR)	Warrants:- Reliably distinguishing original from tampering edges increase localization efficiency and reduce scores on measures of time. Drawback:- The used dataset was a small one with no underlying data and also a very apparent spliced area. This high accuracy with such a small dataset may be due to fitting problems. In addition, the design may not ever work on highly qualified forgery.	Accuracy of 97% with the Columbia dataset
[22]	Image splicing	MFCN, edge probability map, and surface probability	Warrants:- The proposed methodology performs better than current. splicing. Drawback:- Uses the training set for image assessment on new images.	0.52 Matthews Correlation Coefficient MCC score
[23]	Splicing Image	SVM	Warrants:- Access to a high accuracy rate with different databases Drawback:- The system has not been tested with the other type of forgery, copy-move.	98.8%
[24]	Splicing Image	SVM	Warrants:- Focus on the Differential Box-Counting method for calculating the Intensity-Level Multi-Fractal Dimension Drawback:- The system has been tested with agray level, not with other domains.	97.8%
[25]	Splicing Image	SVM	Warrants:- Presents a novel forgery detection algorithm using combined features. Drawback:- Numerous databases were not used. Other types of forgery were not detected.	98.45

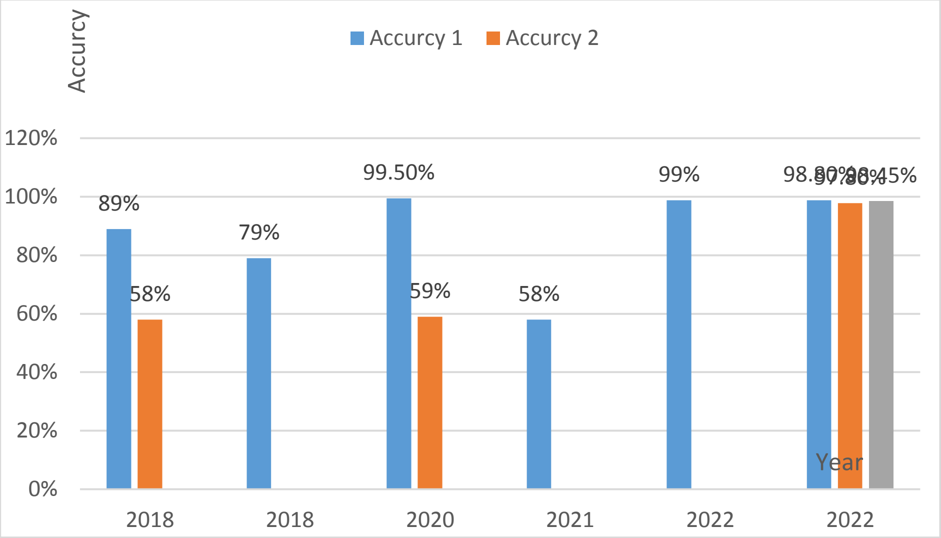


Figure 7: Accuracy measurement

3.2 Copy-Move Forgery-Related Work

Lee et al. [26] proposed a method that divided the overlapping blocks and included the a (HOG) for each block. The overlapping block of the input image. Used segmenting each block and was given a histogram of oriented gradients. To make similarity measurement easier, statistical features were obtained and lowered. Finally, after post-processing, CoMoFoD was used as a test dataset in this study. With F-score of 90%, the proposed algorithm outperforms other methods whenever the dimensions of the hand calculation is reduced.

Parihar and Mehtre [27] introduced an algorithm that is used to detect copy-move forgery (CMFD). The SIFT algorithm was used to extract feature vectors. Following that, they chose three different datasets to test the results. The first dataset consisted of four different directories containing various types of geometrically based attacks on images. Firstly with 50 image accuracy of 65% was achieved. For the second dataset with more than 1000 images the accuracy was 70 %, and the third dataset with 100 images was 90%.

I Bondi, et al [28] the dataset, which included 50 tampered images, contained only translation attacks, and the accuracy with the dataset used reached about 65 percent. Second dataset: this dataset contained over 10000 images with geometric and post-operation-based attacks. The accuracy with the dataset used was approximately 70%. The third dataset contained various types of atmospheric images. Only 100 translation images were chosen for testing purposes. With the third data set, the Image Manipulation Data set, the method's accuracy reached around 90%.

T. Uricchio et al [29] presented an algorithm for detecting and localizing tampering to expose forgeries performed on images from various camera models. The proposed method extracts features from image patches using a CNN to capture camera model traces using an iterative algorithm. When using different camera models, images with different features are taken for each model. In the training step when using CNN, the algorithm detected forged images with an accuracy of 0.91. Detection accuracy could reach 0.81 if forgery camera models are never used for training. Tampering localization results showed that forged regions could be detected with an accuracy ranging from 0.90 to 0.82, based on the information or based on the knowledge (or lack thereof) of the models of the camera used during the training stage.

Cozzolino et al [30] developed a new algorithm for detecting blind image splicing. They treated spliced area features as anomalies and distinguish them using an auto-encoder-based model and discriminative labelling. The exploratory results published were promising not only under optimal circumstances but also under less ideal conditions, when post-processing is present. However, a comprehensive evaluation of the capacity to extract features directly from data using a proper neural network, as well as the many degrees of freedom (DOF) in the autoencoder structure, is necessary. The detection of forgeries is the final significant topic. They ignored this problem because they assumed it would be working after detection.

J. A. Kumar and . R. Srivastava [31] study builds a deep-learning CNN model with multi-scale input and multiple stages of convolutional layers. These layers are divided into two categories: encoder and decoder. The encoder block integrates and down samples feature maps acquired from different levels of convolutional layers. Similarly, feature maps are concatenated and up-sampled in the resulting decoder block. Using the final feature map, a sigmoid activation function is used to determine if pixels are fabricated or not.

Solaiyappan, S., & Wen, Y [32] paper used a structured case study to address the identification of such attacks. They assess the ability of different machine learning algorithms to distinguish between tampered and untampered pictures, including three standard machine learning approaches (Support Vector Machine, Random Forest, and Decision Tree). Each pre-trained model is fine-tuned before being used to extract features. The results of this investigation show near-perfect accuracy in detecting tumor injections and removals.

T. Nazir et al [33] proposed a deep learning (DL)-based technique for detecting CMF accurately. A custom Mask-RCNN model with DenseNet-41 as the basic network was presented, capable of nominating a superior selection of image features and effectively presenting the complex picture modification. More specifically, the DenseNet-41 model is employed as the base network for deep key point extraction, after which the Mask-RCNN model localizes, segments, and categorizes the manipulated area. These will be the key research directions in the future. Table 2 shows the type of Copy-move algorithms, advantages, and disadvantages of each algorithm. The percentage of accuracy which is illustrated in Figure 8

Table 2: The types of algorithms to copy-move forgery detection

Ref	Target of Tampering	Methodology	Warrants /Drawback	Accuracy
[26]	Cut/paste	(HOG)	Warrants:- It facilitates the measuring of similarity by extracting and reducing statistical information. Drawback:- It was used as a tested dataset in this study. There were 200 PNG images with a resolution of 512* 512 in total (small image category)	The F-score increased to 90% when the size of the averaging filter was lowered.
[27]	Cut/paste	SIFT	Warrants:- The method is faster than the referenced methods. Drawback:- The accuracy of the algorithm varies with the difference in the data set, that is, it does not give	The use of three datasets firstly with 50 images with an accuracy of 65%, a second dataset with more than 1000 images with

			high accuracy with all types of data sets	accuracy of 70%. For the third dataset with 100 images it was 90%
[28]	Cut/paste	CNN	Warrants:- The proposed method uses camera point hints using a CNN. Drawback: - Unable to locate localization as well as camera model traces	The accuracy of localization was 81%, and the accuracy of detection was 82%.
[29]	Cut/paste,	JPEG double compression Multi-domain CNN and RGB features of DCT	Warrants:- For localization, the proposed methodology employs a CNN. image patch classification that have been compressed. Drawback:- It does not employ CNNs. to recognize various types of compressions.	95%
[30]	Cut/paste	Autoencoder and landscapes with noise	Warrants:- The proposed methodology yields reasonable results. Drawback:- It does not investigate the use of several degrees of freedom	0.41 F-Measure
[31]	Cute/paste	CNN	Warrants:- The performance of the proposed model is better when compared with another approach. Drawback:- The system has not been tested with spliced images	96.7% with CMFD 99.4% with CoMoFoD
[32]	Cute / paste	Support Vector Machine, Random Forest, and Decision Tree	Warrants: - Reaching a high accuracy rate Drawback:- The system has not been tested for various situations such as noise	99.0%
[33]	Cute / paste	RCNN	Warrants:- The presence of translation, scale variations, rotation, color changes, noise, compression, and blurring in images. Drawback:- When using the algorithm with spliced images, the system does not reach high accuracy.	98.12%, 99.02%,

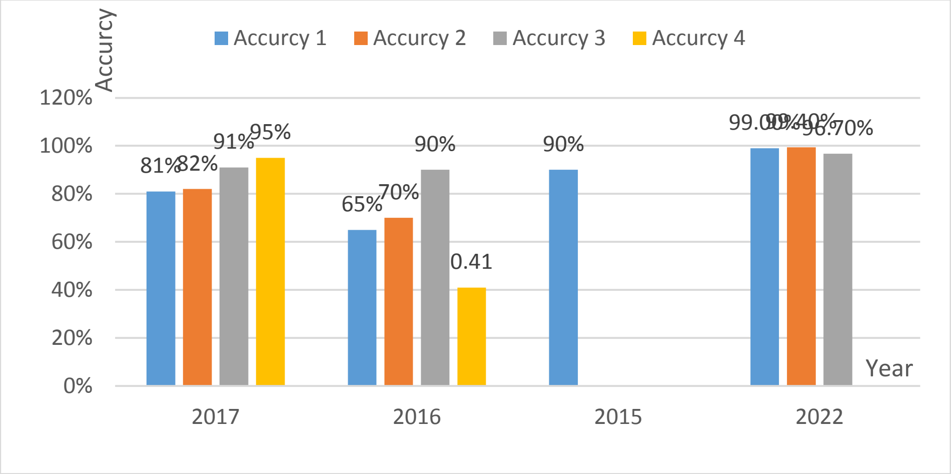


Figure 8: Accuracy measurement

To solve the problem of tampering with images of all kinds passive or active, several algorithms were used in the feature extraction process, as well as during the training and testing process, and then the classification process. Where more than one algorithm can be combined in one system to get the best results and thisis one of the important techniques that have been used. They are artificial intelligence techniques where deep learning can be used, such as CNN, RNN, and YOLO، with other algorithms. Or machine learning is used, for example, SVN, DT, and RF، with other technologies.

Conclusion

Various tamper detection methods have been proposed and implemented in recent years. Passive or blind approaches do not require any prior knowledge about the image being scanned, providing them a substantial advantage over their competitors. In addition, no extra equipment is needed to introduce the cipher into the image during image acquisition. Several approaches developed recently are good at detecting tampering but insufficient at pinpointing the forged area. They identify various faults in the currently existing techniques. To begin with, most systems involve human analysis and so cannot be automated. The forged region's localization is the second difficulty.

The topic of robustness to image processing operations such as JPEG compression, blurring, and scaling follows. Because a part of the restructuring predictor may be unable to determine which tampering method was used to alter the image, it is prudent to utilize an exact identification technique. As a result, a forgery detection method that is capable of detecting any type of image tampering is required. It was clarified in this review what are passive techniques and how they can be distinguished from others, as well as the algorithms used and the accuracy rates achieved. It has been established that various methods of detection are not without flaws. Some of the primary issues that must be addressed are decreasing processing time, enhancing accuracy, decreasing inaccuracy, and being adaptable to diverse technical modifications. As a result, future research must investigate the fundamental issues, and detect approaches that provide a dependable flexible solution.

References

[1] A. F. H. Sewan and M. S. M. Altaei, "Copy Move Forgery Detection Using Forensic Image," *Iraqi Journal of Science*, vol. 62, no. 9, pp. 3167-3181, 2021.

[2] L. D. Griffin, M. Caldwell, J. T. A. Andrews, and H. Bohler, "Unexpected item in the bagging area”: Anomaly detection in X-ray security images," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1539-1553, June 2019, doi: 10.1109/TIFS.2018.2881700.

[3] M. Vafadar and H. Ghassemian, "Hyperspectral anomaly detection using combined similarity criteria," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 11, no. 11, pp. 4076-4085, 2018.

[4] M. Ning, P. Yu, W. Shaojun and G. Wei, "A weight SAE based hyperspectral image anomaly targets detection," in *2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI)*, 2017, pp. 511-515.

[5] M. G. Alex, C. Rajalakshmi, and R. Balasubramanian, "Study of image tampering and review of tampering detection techniques," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, pp. 963-967, 2017.

[6] H. Farid, "Image forgery detection," *IEEE Signal processing magazine*, vol. 26, no. 2, pp. 16-25, 2009.

[7] P. Korus, "Digital image integrity–a survey of protection and verification techniques," *Digital Signal Processing*, vol. 71, no. 2017, pp. 1-26, 2017.

[8] S. Ozturk and E. Gul, "A novel hash function based fragile watermarking method for image integrity," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 17701-17718, 2019.

[9] Z. Zhang, Y. Ren, X. Ping, Z. He and S. Zhang, "A survey on passive-blind image forgery by doctor method detection," *in 2008 international conference on machine learning and cybernetics*, 2008, pp. 3463-3467.

[10] T. Aditya,, "Survey on passive methods of image tampering detection," in *2010 International Conference on Communication and Computational Intelligence (INCOCCI)*, 2010.

[11] T. Qazi *et al.*, "Survey on blind image forgery detection," *IET Image Processing*, vol. 7, no. 7, pp. 660-670, 2013.

[12] A. K. Chakraverti and V. Dhir, "A Review on Image Forgery & its Detection Procedure," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 4, pp. 440-443, 2017.

[13] M. Kumar and S. Srivastava, "Image forgery detection based on physics and pixels: a study," *Australian Journal of Forensic Sciences*, vol. 51, no. 2, pp. 119-134, 2019.

[14] V. Sharma, S. Jha, and R. K. Bharti, "Image forgery and its detection technique: a review," *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 3, pp. 756-762, 2016.

[15] A. M. Ali and M. J. Mohammed, "Gap-filling restoration methods for ETM+ sensor images," *Iraqi Journal of Science*, vol. 54, no. 1, pp. 206-214, 2013.

[16] R. I. Yousif and N. H. Salman, "Image compression based on arithmetic coding algorithm," *Iraqi Journal of Science*, vol. 62, no. 1, pp. 329-334, 2021.

[17] S. M. Ali and S. S. Salman, "New Tasseled Cap Classification Technique using Landsat-8 OLI Image Bands," *Iraqi Journal of Science*, vol. 57, no. 2C, pp. 1612-1619, 2016.

[18] Zhang, Q. et al. "Digital image splicing detection based on Markov features in block DWT domain", *Multimedia Tools and Applications*, vol. 77, no 23, DODOI10.1007/s11042-018, 2018.

[19] Z. Tianyu, M. Zhenjiang and-. Z. Jianhu, "Combining CNN with hand-crafted features for image classification," *in 2018 14th IEEE international conference on signal processing (ICSP)*, 2018, pp. 554-557.

[20] A. K. Jaiswal, and R. Srivastava, "A technique for image splicing detection using hybrid feature set," *Multimedia Tools and Applications*, vol. 79, no. 17, pp. 11837-11860, 2020.

[21] M. Habibi and H. Hassanpour, "Splicing image forgery detection and localization based on color," *International Journal of Engineering*, vol. 34, no. 2, pp. 443-451, 2021.

[22] R. Salloum, Y. Ren, and C. C. J. Kuo, "Image splicing localization using a multi-task fully convolutional network (MFCN)," *Journal of Visual Communication and Image Representation*, vol. 51, pp. 201-209, 2018.

[23] V. Srivastava and S. K. Yadav, "Digital Image Tampering Detection Using Multilevel Local Binary Pattern Texture Descriptor," *Journal of Applied Security Research*, vol. 17, no. 1, pp. 1936-1610, 2022.

[24] E. Tripathi, U. Kumar and . S. P. Tripathi, "Image splicing detection system using intensity-level multi-fractal dimension feature engineering and twin support vector machine based classifier", *Multimedia Tools and Applications*, pp. 1-19, 2022.

[25] A. Parnak, Y. D. Baleghi and . S. Kazemitabar, "A Novel Image Splicing Detection Algorithm Based on Generalized and Traditional Benford's Law," *International Journal of Engineering*, vol. 35, no. 4, pp. 626-634, 2022.

[26] Lee, J. C., Chang, C. P., & Chen, W. K. "Detection of copy-move image forgery using histogram of orientated gradients". *Information Sciences*, vol. 321, pp 250-262, 2015.

[27] V. Parihar and B. M. Mehtre, "Copy move forgery detection using key-points structure," Sardar Patel University of Police, Security and Criminal, vol. 6, no. 5, pp. 240-251, 2016.

[28] L. Bondi, S. Lameri, D. Guera, P. Bestagini, E. J. Delp and S. Tubaro, "Tampering Detection and Localization Through Clustering of Camera-Based CNN Features.," *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1855-1864, doi: 10.1109/CVPRW.2017.232.

[29] T. Uricchio, L. Ballan and R. Caldelli, "Localization of JPEG double compression through multi-domain convolutional neural networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2017.

[30] D. Cozzolino and L. Verdoliva, "Single-image splicing localization through autoencoder-based anomaly detection," in *2016 IEEE international workshop on information forensics and security (WIFS)*, 2016, pp. 1-6.

[31] J. A. Kumar and . R. Srivastava, "Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model," *Neural Processing Letters*, vol. 54, no. 1, pp. 75-100, 2022.

[32] S. Solaiyappan and . Y. Wen, "Machine learning based medical image deep fake detection: A comparative study, *Machine Learning with Applications*, vol. 8, no. 2, pp. 2666-8270, 2022.

[33] T. Nazir, M. Nawaz, M. Masood, and A. Javed, "Copy move forgery detection and segmentation using improved mask region-based convolution network (RCNN)," *Applied Soft Computing*, vol. 131, pp. 1568-4946, 2022.