Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

A survey on tamper detection techniques for digital images

Amina taha kasim[1],* ***Sundus Khaleel Ebraheem*** [2]

Department of Computer Science, College of computer science and mathematics, Mosul University, Mosul, Iraq [1] *,*
Department of Computer Science, College of computer science and mathematics, Mosul University, Mosul ,Iraq [2]
**Corresponding author. Email: amina.20csp56@student.uomosul.edu.iq*[1]

Article information

Article history:
Received : 16/3/2022
Accepted :26/6/2022
Available online :

Abstract

Abstract— Recently, fake and fabricated images that have been manipulated for several purposes, including cosmetic and some for illegal purposes, have spread on social media. And because this is not an easy matter, it has become necessary for researchers in this field to search and investigate the types of images, to verify their authenticity and how to manipulate them. Therefore, the aim of this research is to serve as an assistant to the researcher who wants to enter this field. In this research, a survey of the types of forgery was presented with examples. The most important common methods for detecting forgery were also presented, and the previous studies that contributed to the process of detecting fraud, both traditional detection and deep learning-based detection, were highlighted, while giving the most important strengths and weaknesses of both types. We note from this that detecting the forgery process is a difficult process and takes time to detect the changes that have been made to the image that cannot be detected by the naked eye. In this research, researchers have been urged to go towards deep learning for the purpose of detecting the forgery of the features that it enjoys.

Keywords:
copy move forgery, image splicing , passive detection methods, Active detection methods Retouching image Forger.

Correspondence:
Author : Amina taha kasim Alazawe
Email:amina.20csp56@student.uomosul.edu.iq1

1. INTRODUCTION

The development in the field of technology included all aspects of life, especially images, which became the best means of transmitting information. Images express information in a better way than texts, as it is possible to extract more details and facts from them that text messages cannot express because humans by nature believe everything they see. The human visual system equips us with approximately 75% of the information [1], and therefore it is considered as the best way to ensure the credibility of things. With the advancement of science, manipulating digital images has become a very easy process with the presence of many image applications. Images can be manipulated in several ways using programs, such as: adobe Photoshop, coral paint shop and photo plus [2]. Some of those programs connect or merge two images to produce a fake one, others cut part of the image and paste it in different locations of the same image with the possibility of rotating and zooming the copied part. Other manipulating programs, on the other hand, can refine the image, such as filling the image with color and controlling lighting.

Digital images is used in many fields such as promotion, advertising, scientific analysis, crime analysis and forensic medicine. In this study, a survey of the types of forgery was presented with examples due to the various reasons. First, the spread of applications for digital image manipulation and the availability of the Internet, which provides an easy means to share images via social media. Second the availability of photo editing tools that are used to manipulate images in an easy effortless affordable way. Finally, as part of (reliable medical evidence) used in courts, images are important source of information since they can be used as "conclusive evidence" in analyzing suicide cases, intelligence services, and media misinformation for a case affecting contemporary life.

Due to the recent spread of fake and fabricated images on social networking sites that have been manipulated. And because this is not an easy matter, it has become necessary for researchers in this field to search and investigate types of images, to ensure their authenticity and how to manipulate them. Consequently, the process of verifying the credibility of the image became the focus of researchers' attention and a source of inspiration to discover methods of detecting forgery.

Therefore, in this research, the types of forgery will be explained in paragraph 2, the methods of detecting forgery will be mentioned in paragraph 3, and previous studies in this field will be highlighted in paragraph 4, then a comparison will be made that shows the strengths and weaknesses of each type of studies that were addressed in paragraph 5. Finally, the conclusions were presented in paragraph 6.

2. Types of digital image forgery:

Digital image forgery is a term used when any change occurs to the original image (such as copying and pasting, removing, adding and resizing, rotating to a certain degree, enhancing, or combining more than one change to create a new image). Image forgery can be divided into five types [3] see figure (1).

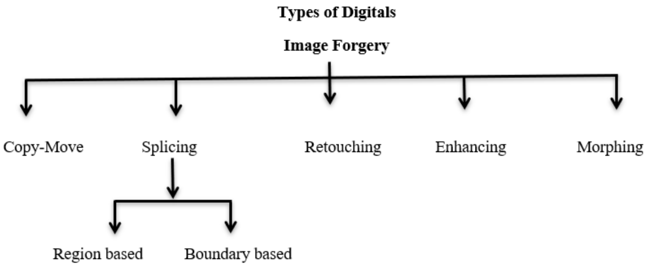
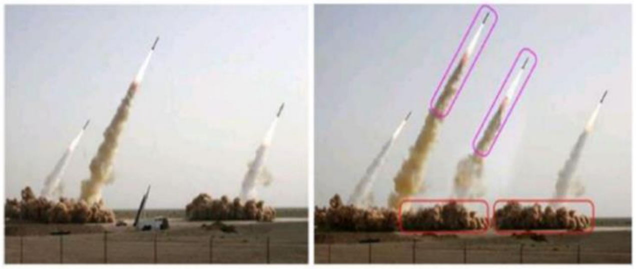


Figure (1) : Types of digital photo forgery.

2.1 Copy Move Forgery

This type is the most common and the easiest to implement and the hardest to detect since there can be more than one forged part in the image, and it can be distributed anywhere in the image. In addition, the source and (target) images share the same destination, color and noise except the forged part. In general, methods for detecting clones depend on comparisons and matching, and they fall into two parts: comprehensive search method and the nested block matching techniques. It is possible to apply many transformations on the image (scaling, rotation, shearing and combining several types) to cause difficulty in the process of visual detection. In addition, if the process of manipulation was carried out by professionals using statistical measurements, the detection process becomes useless with this type. Example. See figure (2) shows an example of this type where the original image on the left, shows images of three missiles, while the image on the right has been manipulated, showing images of four Iranian missiles. The forged image was published in July 2008 by New York Times and Los Angeles thinking it was an original photo, but it turns out later that it is a forged photo [4].

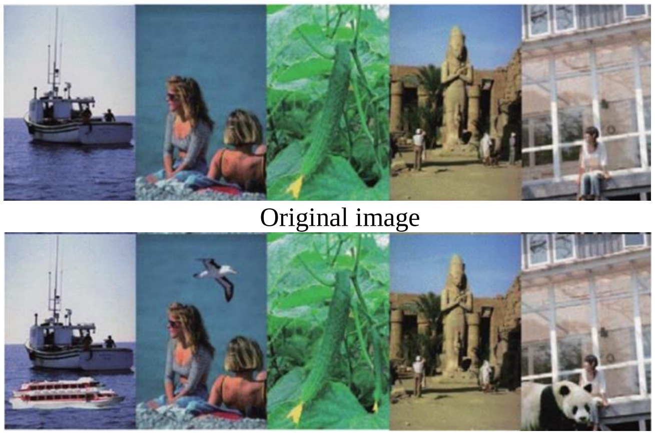


Original image forger image

Figure (2): shows the forgery of the type of cutting and copying [5].

2.2 Forgery of splicing or splicing in digital images

In this type of forgery, two or more images are combined to obtain one image. Many processing operations can be performed on this type of forgery. This kind is classified into two types [6]. The first type depends on the region, and it depends on the characteristics of the camera or statistical characteristics of the features of the region in which it was formed. The second type is based on borders by detecting irregular modification on the binding borders where the consistency of the pixel division surrounding the borders in the color image is checked. This type is more difficult to detect compared to transfer and reproduction due to the fact that the divided image does not contain any repeated regions. In addition, the source of the image does not provide any evidence of forgery [7]. See figure (3)

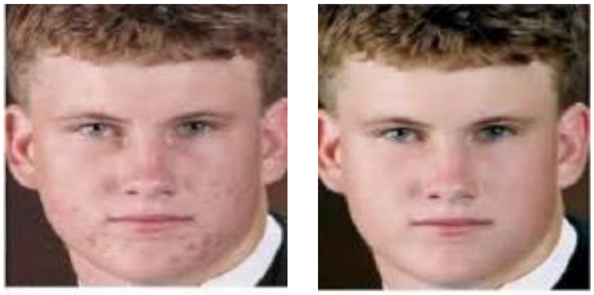


Original image

Figure(3) : shows the image splicing forgery [8]

2.3 Retouching image Forgery

The retouching process in films was previously done with a pointed brush and was accurate with special pigments. Nowadays, due to the availability of digital images, the retouching process became easier and faster. This type of forgery is the least harmful because it does not make important or drastic changes to the image as it works to hide defects such dark spots and shadows under the eyes. Its main purpose is to increase aesthetics and to attract attention. This type is usually used to form magazine covers. See (Fig. 4) [9], the image to the left of the actor Newman where the retouching process was performed by repeating the wrinkle-free skin patches on the wrinkled areas [9]. The revision process can also be used to perform the repairing process, see figure (5)[10].



Original image retouching image

Figure (4): Example in retouching image [9]

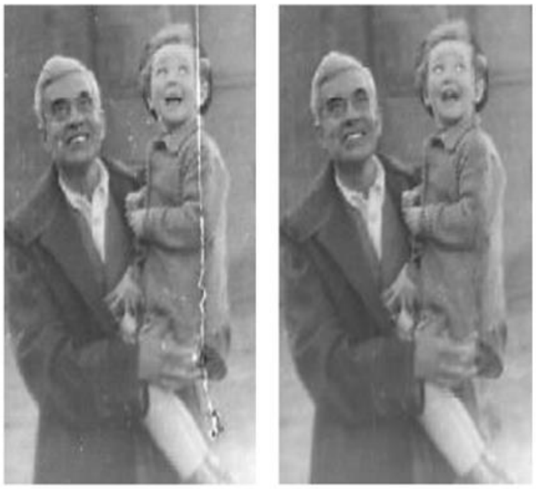


Figure 5 Example in retouching image in the repair process [10].

2.4 Enhancement forgery

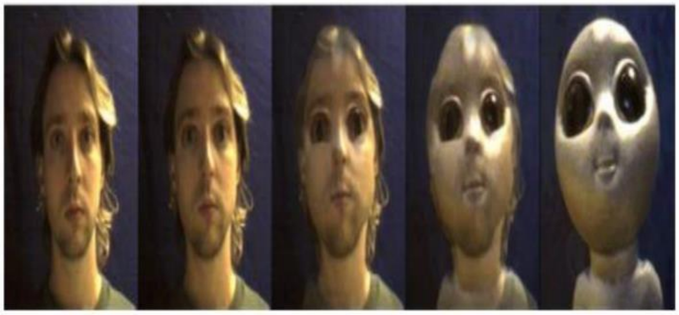
In this type of forgery, the content of the image is not changed, but it includes adjusting the color contrast and distortion. This type has an indirect effect on the interpretation of the image, such as changing the time of the day when the image was taken .see figure(6)[11] shows the process of improving an image where the image to the left represents the original image and the transitions from left to right was done to show the bike and blurring the cars in the background [11].

Figure (6): shows the stage of the improvement process [11].

2.5 Morphing image

In this type of forgery, the image is gradually transformed into another image See figure (7) that shows a picture of a person (the source image) which gradually turns into the target image (the image of the doll's face). The intermediate images include the attributes between the source image and the target image and contain a human part and an alien part [10].

Figure (7): Shows a series of mutated images [10]



3. Methods for detecting forgery of digital images

Forgery detection methods are classified into two categories: passive detection and active detection [12]. See figure (8).

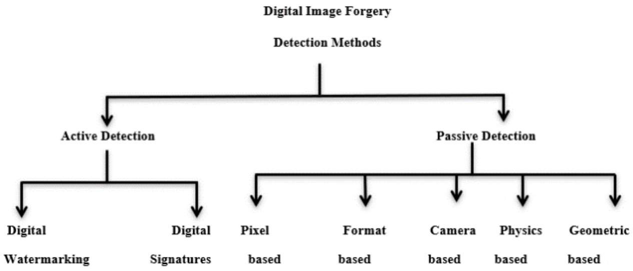


Figure (8): Types of Forgery detection

3.1 passive detection methods

In this type of detection methods, we do not have prior knowledge about the image to be verified. This method is also called (blind-method) and it works by analyzing the content of the image and making statistics for it (13). Detection methods that depend on the content are divided into methods for detecting forgery of the braiding type, and methods for detecting forgery of the transmission and reproduction type. Detection techniques have developed to go through several stages, including weak methods that fail to detect forgery when the image is exposed to treatments such as (compression, camouflage, scaling, and noise attacks), while strong methods succeed in detecting forgery even if the images were exposed to the aforementioned treatments. Negative detection methods are divided into five groups [13] [12]:

3.1.1 Pixel-based detection methods

These methods depend on the basic building block of the image, which is the pixel, and include the processes of transfer, copying, linking, and editing.

3.1.2 Format-based detection methods

In this technique, JPEG format is mostly used. For image forgery detection, these techniques fall into three categories: JPEG quantization, Double JPEG quantization, and JPEG block. When compressing an image, it is almost impossible to distinguish between an original image and a fake image. However, fake images can be detected by compressing images using format-based techniques.

3.1.3 Camera-based detection methods

This method uses changes made by the camera that go into stages in the imaging processes such as segmentation, color correlation, gamma correction, white-tuning, filtering, and JPEG compression. For example, chromatic aberration, color filter set, camera response, sensor noise, and defects can be used.

3.1.4 Physics-based detection methods

Under various lighting conditions, natural photographs or a photorealistic image is generally taken. The brightness level and contradiction of the original image can be used to identify or detect any distortion used to create an altered image. Since the brightness of a tampered image is different from that of the original image, checking for lighting fluctuations can be one of the most effective ways to detect image spoofing.

3.1.5 Geometry-based detection methods

A technique that depends on analyzing the relationship between the camera and the object in the image. It determines the reflection of the objects in the image, and through reflection, we can know if there is any manipulation of the image or not

3.2 Active detection methods

This type requires the presence of previously available information, noting that there is a difference between the two images to indicate the presence of forgery. In this type, some data is added to the original image to produce a new image that includes both the watermark and digital signature [14].

3.2.1 Watermark

It is a series of bits in the digital image. It might be special information, such as the serial number of the tuner or a company logo, and it is added to the digital image to determine the copyright. See figure (9) which shows the presence of the watermark in the digital image (15).

Figure (9): shows the presence of a watermark [15]

3.2.2 Digital signature

It is a mathematical method that seeks to solve the problem of tampering. It uses a digital signature to verify the authenticity of digital messages. Depending on the digital signature, the recipient can verify the credibility of the message. It is widely used in many areas such as financial transactions. The digital signature contains some secondary information obtained from the digital message or image, and only the sender has the right to sign the image, so the recipient must verify the authenticity of the signature. Also, the digital signature cannot be forged by unauthenticated persons [15].

4.Previous studies

Previous studies can be divided into two parts according to the type of methods used in detecting forgery. The first part relies on traditional manual methods to find the important features in the image. It performs image processing and then inserts it into algorithms that extract properties based on image texture analysis. After obtaining these properties, a classifier is used for the purpose of classification, while the second part relies on deep learning methods to explore the important features of the image, in recent years, deep learning models including deep neural networks and pre-trained network models have been able to extract complex features from images and effectively learn these features. It is also possible to rely on learning models in the detection process for their ability to learn automatically. Incorporating the extraction and classification stage into these models also makes an effective contribution to deep learning models in broad areas such as computer vision and speech recognition. Here are some of the studies presented by researchers.

4.1 Studies that depend on traditional methods

These methods rely on hand-made features, and they have many weaknesses that include a high degree of computational complexity, low detection accuracy, and they work on a certain form of forgery[16]. Studies in this field are:

- In 2013, [17] Zaho and Guo proposed a method for detecting transcription-type forgery based on discrete cosine transform (DCT) and single value analysis (SVD). The results showed that this method can detect forgery even if the image is distorted by Gaussian and that this method is strong against noise and its disadvantage is that it has not been tested on more complex image transformations such as rotation and scaling.
- In 2015, Lee et al. [18] presented a method for detecting copy and transfer type forgery by converting the image to gray scale and then dividing the image into overlapping blocks of size (16 * 16), applying the Gabor filter and calculating the histogram of oriented Gabor magnitude descriptor. After calculating the vector characteristic, it is stored lexicographically, then the matching blocks are found using the Euclidean distance. To reduce the false matching, a threshold is used. By using this method, the researcher was able to detect forgery even when the image was subjected to distortion, color reduction, brightness changes and weak detection when applying rotation and scaling on large areas of the image.
- In 2016, Sreelakshmy et al. [19] presented a method for detecting copy and transfer type forgery by integrating block-based detection methods, and key point-based detection methods where the Adaptive overlapped segmentation algorithm segments that divide the image into a set of blocks are applied. Then a speeded up robust features (SURF) algorithm is applied to extract the main features of the image and then these features are matched with each other to detect forgery.
- In 2018, Fernández et al. [20] presented a technique for detecting digital image tampering of the image splicing type based on spectroscopic analysis of artifacts using a color filter array that works on spectroscopic analysis arising from pixel differences. Then they applied a DCT to each block. The parameter value in each block is used to analyze the forged area. The method was able to detect tampering of images that were subjected to manipulations such as rotation, coloring and scaling. One of the disadvantages of the method is partial detection, as some original areas were identified as forged ones .
- In 2019, Parveen et al. [21] presented a method for detecting forgery in the digital image transmission and copying type on the basis of pixels to ensure the authenticity of the image. The (DCT) was used to extract the features and using the (k-mean) algorithm to made blocks , and finally blocks are matched. The method failed to detect the forged parts in the rest of the image.
- In 2019, Ghanekar & Sharma [22] also proposed an algorithm to detect forgery of the braided image, where the rgb color image is converted to ycbcr, that is, the cr& cb is extracted from the image channels and then the image is divided into overlapping blocks of size 3 * 3 and then the features were extracted from the image using the local direction pattern (LBP) for each block and then making a HISTOGRAM for each LDP. For classification SUPPORT VECTORE MACHINE) (It is known whether the image is real, or fake is used. The algorithm was able to detect forgery even when the image was subjected to post-forgery manipulations such as Jpeg and Gaussian compression.
- In 2020, Abrahim, et al. [23] proposed a new method for detecting splicing in digital form, where a new descriptor called Adaptive threshold or ternary pattern was developed, which integrates local binary pattern (LBP) that is strong against noise, and the local triple pattern (LDP) that is strong against noise and other optical attacks. I this method, the image is converted to grayscale, divided into overlapping blocks of size (12 * 12"), and each block is divided into non-overlapping blocks of size 3 * 3 and then is ATMTP was applied to each block to extract the image features and for classification (Artificial Neural Network). The method was applied to CASIA V 0.2 database.
- In 2021, Asif Hassan & VK sharma [24] investigated the forgery of splicing in the digital image by defining the technique of linking images based on image texture analysis that distinguishes image regions with texture content by converting the image to grayscale and converting it to the image texture and creating a rough mask, and then make a division of the tissue. This

method achieved accuracy success rate of 79%, but failed to reveal the divided regions in the image.

4.2 Studies that depend on deep learning

recent studies have addressed this type due to its ability to learn automatically, its accuracy compared to traditional methods for identifying modified regions, and time and effort saving nature required to determine the needed characteristics [16]. These methods have been met with unparalleled success in various fields, such as image processing in forensic digital images and fraudulent images. The following are some studies based on deep learning.

- In 2016, Raio et al.[25] proposed a method for forgery detection of the digital image splicing type that relies on deep learning to detect spurs in a digital image. This method uses a convolutional neural network (CNN) to automatically teach features from an image input. This method was applied using high-pass filters to obtain residual noise and (SVM) was used for classification. The pre-trained CNN extracts the dense features and then combines the features to get the final discriminative features of the input image. The method was applied to the casiav0.1 database and the method provided superior performance.
- In 2019, Taha et al. [26] presented an algorithm based on deep learning to detect forgery of the digital image braiding type, where a convolutional neural network (CNN) was used to extract features automatically from the image and then the (Harr wavelet transform) was used to reduce the dimensions of features in the image. Where it was noted that it reduces the dimensions from 4096 to 1024, SVM was used, which is used for linear classification, to find out whether the image is fake or real. HWT was replaced by DCT, after that, Principal Components Analysis is applied (where image normalization is done) and (Convenience matrix) is calculated and then (Egin value) is calculated, and in the last step the data is transformed into a vector of new features. CASIA V 0.1 & CASIA V 0.2 data and high fraud detection was obtained.
- In 2019, Rajee & Ankil [27] presented a deep learning model that is used to detect forgery of the image-link type to identify images or classify them into specific categories. Resnet-50 is used, which is a pre-trained convolutional neural network that is applied to the input images to extract the features. The model was applied to a total of CASIA V 0.2 database, and three classifiers were used, respectively (SVM, KNN, and Naïve Bayes), and the accuracy for the three classifiers was 59.91%, 69.81, and 70.26%.
- In 2020, YUAN RAO et al. [28] made a proposal to detect forgery of splice-type images in a digital image by converting an RGB image to grayscale and using a feature descriptor learned by a two-branch CNN neural network where the convolutional layer with 30 high-pass filters prepares the basic features of the image and is set Strictly by constraining the learning strategy to retain filter properties. For classification, a support vector machine was used, which is used for binary classification to determine whether the image is original or forged. This method proved its efficiency in detecting even in the case of a compressed jpeg image.
- In 2020, Almawas et al. [29] proposed a strategy for detecting image forgery of the digital image splicing type using three models of CNN which are: (vgg16, Google net and dense net 201), which are pre-trained models that are used to extract features with images. Three classifiers were used in succession (SVM, Navies Bays, and KNN). Each model contains a different number of layers. The purpose of using more than one model is to identify different representations of features. Image The proposed method has been applied to a set of Cassia v 0.1 and Cassia v 0.2 database types. The proposed method suffers from increasing the feature dimensions, which made the classification task difficult. The researchers expect that in the future, they will be able to find a way to reduce the feature dimensions. The method lacks accuracy, as it reached the highest limit in Naive Bayes classifier to 49.83.
- In the year 2020, Meena et al. [30] presented a method for detecting forgery of the type of braiding by using deep learning to obtain the residual noise, and the Resnet-50 was used, which is a neural network consisting of 50 layers that is the backbone for detecting image forgery and for classifying images. Then, SVM was used, which is from Algorithms that perform linear and non-linear classification based on the kernel is a supervised learning model with data analysis algorithm for future classification.
- In 2020, Ahmed and others [16] presented a method for detecting forgery of the digital image splicing type. The method includes converting the image to gray scale and then using Pretrained Alex Net Model, which is a type of pre-trained CNN that is used to extract the important features of the image and these features enter the canonical classifier Correlation Analysis (CCA), which in turn categorizes whether the digital image is fake or

real. The method was applied to a database from CASIA V 0.1. In the future it is expected that it will be developed to detect falsification of the digital image retouching type.

5. Strengths and weaknesses of previous algorithms

In this paragraph, a summary will be given of the strengths and weaknesses of the algorithms that are being studied, and according to the type of forgery in the images applied to the algorithm within the database used see Tables (1) and (2).

Table (1): shows the most important strengths and weaknesses of the database set used in traditional methods.

Type of image	Research	Method	Strength's point	Weakness point	Data set
Copy move	Zaho &Guo[17]	DCT &SVC	strong against noise	Not checked on rotation and scaling	USC-SIPI Image Database
	Lee et al.[18]	Segmentaion image & Gabour filter & Hog descriptor	Strong when the image is subjected to distortion, color reduction and brightness changes	Weak detection when applying rotation and scaling to large areas of the image	CoMoFoD database
	Sreelakshmy [19]	Adaptive overlapped segmentation algorithm & SURF	Strong and fast against rotation and zoom	Produces a false positive* in flat regions	CoMoFoD database
	Parveen& Ahmad[21]	DCT & K MEAN	Detect one fake part of the picture	It fails to detect the rest of the parts if there is more than one forged part	MICC-F600
Image splicing	González et al. [20]	Color Filter Array& DCT	The method was able to detect if the image was subjected to manipulations such as rotation, coloring, and scaling	Some areas that are not fake have been detected as fake	CASIA V 0.1
	Sharma & Ghanekar [22]	Image Conversion To YCBCR &Segmentation LBP &HOG &SVM	Strong in detecting fraud after image compression process such as jpeg or gaussian process	The method failed to detect fraud in some photos	Canon G3, Nikon D70, Canon EOS 350D Rebel XT, and Kodak DCS330.
	Abrahim[23]	ATMTP descriptor & ANN classifier	Strong against noise and change in lighting	Couldn't detect other types of forging	CASIA V 0.2
	Hassan& Sharma[24]	Analyzing the image texture and creating a rough mask, then making a division of the image texture	Achieved accuracy up to 79%	method failed to detect some areas of forgery	Colombia image

Table (2): shows the most important strengths and weaknesses of the database set used on splicing forged images in the methods based on deep learning.

Research	**Method**	**Strength's point**	**Weakness point**	**Data set**
Raio & Ni [25]	CNN &SVM	Accuracy reached 87%.	You need complex calculations	CASIA V 0.1
Taha et al.[26]	CNN &HWT &SVM	Detected as fake photos	The location of the forgery was not specified	CASIA V 0.1 CASIA V 0.2
Jaiswal & Srivastava [27]	(Res net -50) (SVM ,KNN, and naïve bayes)	The accuracy achieved, respectively, 59.91%, 69.81, and 70.26%. achieved straight accuracy 59.91%, 69.81, 70.26%	It requires building a high-performance system to get the work done	CASIA V 0.2
Rao & Zhao [28]	CNN &SVM	Efficient in detecting fraud even in the case of compressed images	You need complex calculations	CASIA V 0.1 CASIA V 0.2
Almawas et al. [29]	(vgg16,googlenet and dense net 201) SVM ,navies Bayes ,and KNN	It achieved high detection accuracy in the KNN. classifier	The proposed method suffers from an overload of features	CASIA V 0.1 CASIA V 0.2
Meena et al.[30]	Resnet-50 SVM	Effectively detect forgin	The forgery area has not been specified	Cuisde
Ahmed et al. [16]	Pretrained Alex Net Model CCA -classifier	It achieved a high detection accuracy of 98.8%.	It is not applied to other types	CASIA V 0.1

Through the study that I presented, I advise researchers to use deep learning models in the event of detecting forgery in digital images, because of their effective role in increasing the accuracy of detection, due to the features that characterize them, including the feature extraction and classification stage, which have been integrated into deep learning models for its ability to learn Features automatically and its ability to distinguish patterns. Even in the case of a small database, we can use pre-trained network models and it is possible to achieve distinct results as in the research [16], which achieved an accuracy of 98% using the Alex-Net model, where it is possible to build a neural network from scratch or it is possible to use trained models In advance, it is superior to traditional methods that depend on extracting features manually, which must pass through three stages: the pre-processing stage, the feature extraction stage and the classification stage.

6.Conclusion

There is a need to build accurate algorithms and find ways that combine algorithms to obtain high detection accuracy due to the importance of digital images and for our reliance on them in fact-finding. Therefore, it was required to conduct a survey on methods for detecting forgery in digital images. Several fraud detection methods were presented that can detect any form of fraud. Almost all the algorithms discussed above suffered from low detection accuracy. Some of them lack the ability to detect all types of fraud, while others require additional cost for the calculation process or time consuming. Most of the methods were able to detect forgery of transmission, reproduction and forgery of linkage to digital images. We note from this that the detection of the forgery process is a difficult and takes time to detect the changes made to the image that cannot be detected with the naked eye as summarized in Tables (1) and (2).

6. References

[1]. Aggarwal S. Satellite remote sensing and GIS applications in agricultural meteorology. World Meteorological Organisation, Switzerland. 2004.

[2]. Mishra M, Adhikary F. Digital image tamper detection techniques-a comprehensive study. arXiv preprint arXiv:1306.6737. 2013 Jun 28.

[3]. Sreelakshmy IJ, Anver J. An improved method for copy-move forgery detection in digital forensic. In2016 Online International Conference on Green Engineering and Technologies (IC-GET) 2016 Nov 19 (pp. 1-4). IEEE.

[4]. Qazi T, Ali M, Hayat K. Seamless Copy Move Manipulation in Digital Images. arXiv preprint arXiv:2110.05747. 2021 Oct 12.

[5]. Shivakumar BL, Baboo SS. Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors. International Journal of Computer Applications. 2011 Aug;27(3):9-17.

[6]. Chauhan D, Kasat D, Jain S, Thakare V. Survey on keypoint based copy-move forgery detection methods on image. Procedia Computer Science. 2016 Jan 1;85:206-12.

[7]. Mishra M, Adhikary F. Digital image tamper detection techniques-a comprehensive study. arXiv preprint arXiv:1306.6737. 2013 Jun 28.

[8]. Wang W, Dong J, Tan T. Effective image splicing detection based on image chroma. In2009 16th IEEE international conference on image processing (ICIP) 2009 Nov 7 (pp. 1257-1260). IEEE.

[9]. Elaskily, M. A., Elnemr, H. A., Sedik, A., Dessouky, M. M., El Banby, G. M., Elshakankiry, O. A.,& Fathi, E. (2020). A novel deep learning framework for copy-moveforgery detection in images. Multimedia Tools and Applications, 79(27), 19167-19192.

[10]. Khayeat, A. (2017). Copy-move forgery detection in digital images (Doctoral dissertation, Cardiff University).

[11]. Mahdi MS, Alsaad SN. Detection of Copy-Move Forgery in Digital Image Based on SIFT Features and Automatic Matching Thresholds. InInternational Conference on Applied Computing to Support Industry: Innovation and Technology 2019 Sep 15 (pp. 17-31). Springer, Cham..

[12]. Ahmad M, Khursheed F. Digital Image Forgery Detection Approaches: A Review. InApplications of Artificial Intelligence in Engineering 2021 (pp. 863-882). Springer, Singapore.

[13]. Abraham, D. (2020). Digital Image Forgery Detection Approaches: A Review and Analysis.

[14]. Gupta A, Saxena N, Vasistha SK. Detecting copy move forgery using DCT. International Journal of Scientific and Research Publications. 2013 May;3(5):1.

[15]. Khudhair ZN, Mohamed F, Kadhim KA. A Review on Copy-Move Image Forgery Detection Techniques. InJournal of Physics: Conference Series 2021 Apr 1 (Vol. 1892, No. 1, p. 012010). IOP Publishing.

[16]. Ahmed IT, Hammad BT, Jamil N. Effective Deep Features for Image Splicing Detection. In2021 IEEE 11th International Conference on System Engineering and Technology (ICSET) 2021 Nov 6 (pp. 189-193). IEEE.

[17]. Zhao J, Guo J. Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic science international. 2013 Dec 10;233(1-3):158-66.

[18]. Lee JC, Chang CP, Chen WK. Detection of copy–move image forgery using histogram of orientated gradients. Information Sciences. 2015 Nov 10;321:250-62.

[19]. Sreelakshmy IJ, Anver J. An improved method for copy-move forgery detection in digital forensic. In2016 Online International Conference on Green Engineering and Technologies (IC-GET) 2016 Nov 19 (pp. 1-4). IEEE.

[20]. González Fernández E, Sandoval Orozco AL, García Villalba LJ, Hernandez-Castro J. Digital image tamper detection technique based on spectrum analysis of CFA artifacts. Sensors. 2018 Sep;18(9):2804.

[21]. Parveen A, Khan ZH, Ahmad SN. Block-based copy–move image forgery detection using DCT. Iran Journal of Computer Science. 2019 Jun;2(2):89-99.

[22]. Sharma S, Ghanekar U. Spliced Image Classification and Tampered Region Localization Using Local Directional Pattern. International Journal of Image, Graphics & Signal Processing. 2019 Mar 1;11(3).

[23]. Abrahim AR, Rahim MS, Sami AS. Image Splicing Forgery Detection Scheme Using New Local Binary Pattern Varient. Academic Journal of Nawroz University. 2020 Jul 19;9(3):208-15.

[24]. Hassan A, Sharma VK. Texture based Image Splicing Forgery Recognition using a Passive Approach. International Journal of Integrated Engineering. 2021 Apr 8;13(4):112-21.

[25]. Rao Y, Ni J. A deep learning approach to detection of splicing and copy-move forgeries in images. In2016 IEEE International Workshop on Information Forensics and Security (WIFS) 2016 Dec 4 (pp. 1-6). IEEE.

[26]. El-Latif A, Eman I, Taha A, Zayed HH. A Passive Approach for Detecting Image Splicing using Deep Learning and Haar Wavelet Transform. International Journal of Computer Network & Information Security. 2019 May 1;11(5).

[27]. Jaiswal AK, Srivastava R. Image splicing detection using deep residual network. InProceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019 Mar 12.

[28]. Rao Y, Ni J, Zhao H. Deep learning local descriptor for image splicing detection and localization. IEEE Access. 2020 Jan 31;8:25611-25.

[29]. Almawas L, Alotaibi A, Kurdi H. Comparative performance study of classification models for image-splicing detection. Procedia Computer Science. 2020 Jan 1;175:278-85.

[30]. Meena KB, Tyagi V. A deep learning based method for image splicing detection. In Journal of Physics: Conference Series 2021 (Vol. 1714, No. 1, p. 012038). IOP Publishing.

دراسة استقصائية عن تقنيات الكشف عن التلاعب بالصور الرقمية

سندس خليل ابراهيم

قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، الموصل، العراق
sunduskhaleel_2019@uomosul.edu.iq

امنة طه قاسم العزاوي

قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، الموصل، العراق
amina.20csp56@student.uomosul.edu.iq

تاريخ الاستلام 16/3/2022 **تاريخ القبول 26/6/2022**

الملخص

انتشرت في الآونة الأخيرة على مواقع التواصل الاجتماعي الصور المزيفة والمفبركة التي تم التلاعب بها لأغراض عدة منها التجميلية ومنها لأغراض غير شرعية. ولأن هذا الأمر ليس بالهين لذا بات من الضروري دخول الباحثين في هذا المجال للبحث والتقصي عن انواع الصور والتأكد من صحتها وكيفية التلاعب بها. لذا فان الهدف من هذا البحث هو ان يكون بمثابة مساعد للباحث الذي يرغب الدخول في هذا المجال، فقد تم في هذا البحث عرض دراسة استقصائية عن انواع التزوير مع الامثلة.

تم عرض اهم الطرائق الشائعة للكشف عن التزوير، وتم تسليط الضوء عن الدراسات السابقة التي ساهمت بعملية الكشف عن التزوير بنوعيها الكشف التقليدي والكشف المعتمد على التعلم العميق مع إعطاء اهم نقاط القوة والضعف لكلا النوعين. ونلاحظ من ذلك ان الكشف عن عملية التزوير عملية صعبة وتستغرق وقتا لكشف التغيرات التي تم اجراها على الصورة التي لا يمكن كشفها بالعين المجردة وقد تم في هذا البحث حث الباحثين على التوجه نحو التعلم العميق لغرض الكشف عن التزوير للميزات التي يتمتع بها.

الكلمات المفتاحية تزوير النقل والنسخ ،ربط الصورة , طرائق الكشف السلبي ،طرائق الكشف النشط، كشف التزوير .