A Comprehensive Survey on Passive Techniques for Digital Image Forgery Detection

Mohamed A. Abdelhamed[1], Amira baumy[2], El-Sayed M. El-Rabaie[3]

***Abstract*—One of the most common types of multimedia in daily life is digital photographs. Digital picture editing has been made easier with the availability of sophisticated yet user-friendly editing tools. As a result, it is now crucial to consider the legitimacy of these digital photos. Techniques for detecting digital picture forgeries seek to determine the image's changes and verify its legitimacy. There are two categories of these techniques: active and passive. The paper presents the different types of image forgeries and its detection techniques. Also, we present a survey on passive strategies for image fraud detection. To elucidate the issue of digital image forging and provide clarity on the suggested approaches for detecting forged images, four study points have been presented. Along with discussing numerous issues that require attention, the survey offers suggestions for potential future study avenues.**

***Keywords*— Image Tampering, Forgery Detection, Copy-move Detection, Splicing Detection, deep learning.**

I. INTRODUCTION

Over the past ten years, researchers have become increasingly concerned about the security of image content in contemporary multimedia systems. Several techniques, including watermarking, encryption, steganography, and picture forgery detection, can be used to secure image content. The fundamental principle of steganography and watermarking is to conceal a secret signal, message, or image under a cover image to safeguard the owner's copy rights or to transmit important information. Another perspective for image security is to have the ability of forgery detection. Forgery is known as intended content change of digital images. Changing this content can be made based on the extracted patches from the same or different images with close characteristics. The endeavors toward robust forgery detection algorithms have initiated different approaches for this purpose. It is possible to assess the available articles on image forgery attack detection methods by concentrating on a few key areas. The various kinds of digital image forgeries are first described. Also addressed are the several strategies and modeling techniques that serve as the foundation for forgery detection and localization methods that are available in the literature

II. IMAGE FORGERY TYPES

Splicing, retouching, and copy-move forgeries are the three categories of image forgeries.

Copy-Move Forgery: The process of copying portions of a picture and pasting them in different locations within the same image is known as copy-move forgery. Therefore, the pixel dynamic range of the duplicate portion, which is extracted from the same image, is the same as that of the other portions of the picture. The correlation that exists between these two regions can be explained by this. To conceal an object or add other objects to the image is the goal of copy move forgeries. Fig. 1 provides examples of copy-move forgeries. It demonstrates how copy move can be used to edit images. The original image is used to create the altered photo. There is just one girl in the first picture, which is the original picture. One of the two girls in the second picture is a replica of the other. Following copy-move picture change, post-processing operations such as compression or blurring are carried out. The aim of this post-processing step is to conceal the tampering operation's alteration. Copy-move approaches aim to extract the areas of the image that are replicated. The duplication is indicated by the similarities between features that were taken from two distinct areas of the image.

The advantage of copy-move forgery is no needing external images. The source and the destination location of forged parts is the same image. Localization of duplicated parts in the given image is easy because the duplicated parts have the same lighting condition, the same background, and the same properties.

Splicing Forgery: The process of creating an image out of many images is called splicing forgery. A portion of an image is inserted into the original image to create the forged image. The splicing forgery is more destructive than other types of forgery. The facts can be changed more easily by merging any images with each other's. The purpose of splicing forgery is changing the real information. An example of splicing forgery is given in Fig. 2. The tampered image in Fig. 2 is created by adding a child to the original, which simply had the sky in it.

Manuscript received [19 November 2023]; revised [5 March 2024]; accepted [21 March 2024]. Date of publication [22 May 2024].

[1]Mohamed A. Abdelhameed is with Department of Communications and Computers Engineering, Higher Institute of Engineering, Elshorouk Academy, Elshorouk City, 11837, Cairo, Egypt. (e-mail: m.abdelhamed@sha.edu.eg) ([8]*Corresponding author)*

[2]Amira baumy is with the Department of Communications, High Institute for Engineering and Technology, AL-Obour, Obour City, Egypt (e-mail: osama.elshazly@el-eng.menofia.edu.eg).

[3]Sayed El-Rabaie is with Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, 32952 Menouf, Egypt (e-mail: smr@el-eng.menofia.edu.eg).

(a) Original images

(b) Forgery images

Fig. 1. Examples of copy-move forgery.

Some post-processing methods, blurring, enhancements, color changes, may be used after the combination to hide any details that may help in forgery detection. The methods used to identify image splicing rely on following the traces left behind by the tampering process. The edges of the composed region are different from the remaining image, by tracking the edge discontinuity tampering is detected. Additionally, the tampered area may have uneven lighting compared to other areas of the image due to the differences in image characteristics caused by different types of cameras. So, Discontinuity in edge, inconsistency of lighting condition, geometric situation and camera leaves abnormal artifacts on the forgery image. Generally splicing tampering can be obtained by researching those artifacts.

The disadvantage of splicing forgery is the tampering created by using several external images. Detecting the location of a forgery is easier than detecting copy-move forgery.

(a) Forgery images

(b) Original images

Fig. 2. Examples of splicing forgery.

Retouching Forgery: Retouching forgery is the process of enhancement of image appearance by changing the color and contrast or hiding visible flaws on skin. The images don't change but increase or decrease some properties in images, such as resolution setting or color changing. The purpose of retouching forgery is enhancement the image quality. Examples of retouching are shown in Fig. 3. In Fig. 3 the tampered image is composed by changing the size or expanding for a certain region, color changes and illumination changes to hide the defects in images.

The advantage of retouching forgery is not destructive. It is used in aesthetic and commercial applications. The disadvantage is the detection of tampering images without actual photo is very difficult.

(a) Forgery images

(b) Original images

Fig. 3. Examples of retouching forgery.

III. Forgery Detection Techniques

Forgery detection techniques have become an indispensable necessity at the present time due to the continuous increase in fake images that surround us in all fields. The intentional manipulation of a digital image is to modify or change the facts contained in the images. The aim of forgery detection techniques is to identify instances of forgery. Techniques for detecting forgeries are divided into two groups: passive methods and active methods. The categorization of methods for detecting forgeries is shown in Fig. 4 [3, 4, and 5].

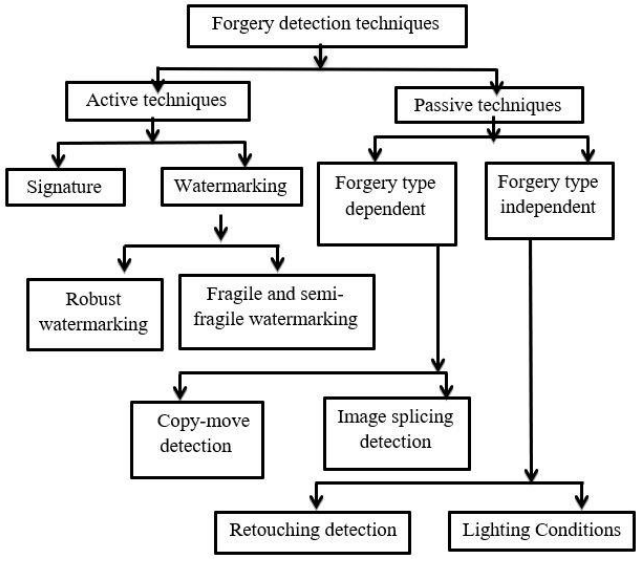

Fig. 4. Classification of forgery detection techniques.

Active Forgery Detection Techniques: The idea behind how forgery detection techniques operate is to include outside data into the image. The embedding process is performed during image acquisition or before the image publishes. The purpose of inserting data is to discover the image acquisition source and to find out if there is a change made in the contents of the image. Examples of active forgery techniques are a digital signature [9, 10, 11] or a watermark [6, 7, 8]. The process of verification involves identifying the watermark or signature. A particular image or message is inserted in an image now of production using watermarking techniques. The watermark is then extracted and matched to the original watermark after the image has arrived at its destination. Forgery is indicated if it is shown to deviate from the original. There are three types of watermarks: semi-fragile, fragile, and robust.

Despite the effectiveness and reliability of the active methods, it is not widely used. It needs special types of acquisition cameras, and these are very expensive.

A robust watermark: A robust watermarking does not affect the different operations applied to the image such as rotation, compression, and scaling. Usually, a robust watermarking is used to identify the image source and protect the copyright and it is embedded in the frequency domain.

A fragile and semi-fragile watermark: A fragile or semi-fragile watermark, in contrast to a robust one, is altered and distorted when processing operations are applied to the image [12, 13, 14]. Spatial alteration affects both fragile and semi-fragile watermarking, however semi-fragile watermarking is more resistant to JPEG compression. To identify modification and demonstrate the integrity of the image, the original watermark and the one that was extracted from the case image are compared.

Passive Forgery Detection Techniques: These methods rely on the signal or image itself to identify the fake. These methods can be used with comparable statistical tools. These methods detect forgeries without the need for more information. The passive methods utilize the features that are extracted from the image to detect forgeries. Several research have been introduced a general survey [15, 16, 17, 18, 19] for different types of forgery techniques. The most common categories are forgery depending on technique and forgery in-depended technique as shown in Fig. (4).

IV. A Comparison Between Copy-Move Algorithms

The cloned portions in the copy-move technique [19–27] have some traits in common with the remaining images, such as backdrop, lighting, and dynamic range. Forgery detection consequently gets more challenging. Various methods for identifying copy-move forgeries are studied. These methods fall into one of two categories: block-based methods or key points-based methods [19]. The general procedures employed in the various copy-move forgery detection techniques are shown in Fig. (5). A lot of methods begin with pre-processing operations like color system conversion, image improvement, or noise reduction. The sole distinction among all methods is the features extraction technique. The feature vectors ought to provide accurate image representation while preserving all

data. Next, by identifying a high degree of similarity between the feature vectors, matching is carried out to obtain the duplication region.

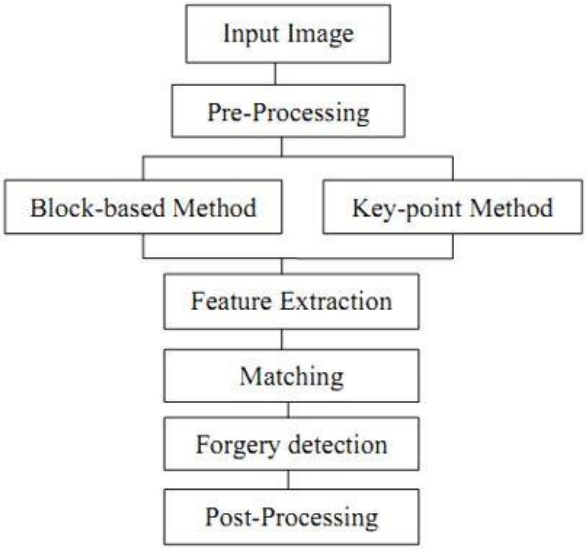

Fig. 5. The general steps used in the different copy-move forgery detection approaches.

Using block-based methods, a tiny overlapping block is used to extract feature vectors. In [20], the images are split up into overlapping blocks, and then Walsh Wavelet (WW) and Discrete Cosine Transform Wavelet (DCTW) are applied to each block. Discriminative characteristics are collected from coefficients for every block. After lexicographic sorting of these feature vectors, a block matching step is used to identify duplicate blocks.

Discrete cosine transform (DCT) is used in [21] on every block.; the dimension of each block will be reduced by representing each DCT coefficients with a circle block and four features are extracted. Finally, the feature vectors are lexicographically sorted, and threshold value is selected to find duplicated image blocks. Dyadic Wavelet Transform (DyWT) [22] is used to extract the features. The image was segmented into low frequency and high frequency sub-bands using the Stationary Wavelet Transform [23]. The low frequency sub-band was then split into overlapping blocks, from which four features were extracted using four triangle segments per block. The 1-level Discrete Wavelet Transform (DWT) results in a low frequency sub-band that is divided into overlapped blocks in [24]. For each block, the coefficients of the fractional Fourier transform are computed, and a feature matrix is created. The authors in [25] preferred to use Gabor response for each overlapping block of the image because Gabor filters provide invariance to illumination, rotation, scale, and translation. After lexicographic sorting of the feature vectors, duplicate image blocks are found.

Duplication Region forgery is found in [26] by dividing the image into overlapping blocks and applying Discrete Cosine Transform for each block. Discrete cosine transform and principal component analysis are used the feature vector of overlapping blocks in [27].

Conversely, to lower the computational cost, key point-based methods like Scale Invariant Feature Transform (SIFT) [35–38] and Speeded Up resilient Features (SURF) [39–41] are employed. These algorithms are resilient to noise and invariant to scaling and rotation transformations. In [35], SIFT key point descriptors are employed as feature vectors, and a comparison is made between them to obtain features that are similar. In [36], detection copy-move is enhanced by first extracting texture information from the image using Local Phase Quantization and then applying SIFT. To extract the feature descriptors, the image in [37] is first broken down using DyWT and then the LL sub-band is subjected to the SIFT transform. DWT and SIFT have been utilized in [38] to extract features.

Because the SIFT key point feature vector has a dimension of (1x128), calculation is sluggish. The descriptor is computed more quickly when integral pictures with a SURF key point descriptor are used instead of SIFT descriptors and feature vector dimensions (1x64). Thus, SURF key point is used in current research, its features are extracted, and their descriptors are matched with one another.

Numerous matching strategies, including nearest neighbor, KD tree, and Euclidean distance [59], are being studied. The spatial positions of the matched points are subjected to an agglomerative hierarchical clustering [60,61]. The nearest feature vector is clustered using K-means [62]. In Tables 1 and 2, the all k data set was used, 30 percent of which was used for testing and 70 percent for training.

V. A COMPARISON BETWEEN SPLICING ALGORITHMS

Splicing forgery detection techniques are intriguing because they identify abrupt changes between segments of an image. It has been suggested to use the algorithm in [50] to determine the shift in the illuminant hues. The illuminant sub bands are estimated using the grey-world technique, and the forged regions are located by comparing the results.

Z. Moghaddasi [51] divided the image to overlapping blocks and applied the singular value decomposition (SVD) and discrete cosine transform (DCT) for each block. The feature vector is composed of 25-DSVD coefficient and 25-D DCT+SVD coefficient. The image [52] is converted from RGB to YCbCr component and chrominance component is divided to overlapping blocks. For each block Local Binary Pattern (LBP) is calculated, then DCT transform is applied on the resulting LBP blocks.

Finally, the standard deviations are determined for every block that symbolizes the vector of features. The authors of [53] suggested combining the DCT frequency domain and spatial domain Markov characteristics.

The image is separated into blocks that don't overlap. After applying the DCT transform to the image blocks, the Markov feature is computed.

The chrominance component [54] is divided into non-overlapping blocks. LBP followed by wavelet transform are applied to each block, then PCA is used to reduce dimension of feature vectors. SVM is used as a classifier.

The features [55] are formed from image quality metrics (IQMs) and moments of characteristic functions of wavelet

sub bands. Image forensic technique [56] depended on the discovery of the inconsistencies in the illumination. This algorithm combines texture and edge points. Texture features are represented by illuminant color and edge points have been estimated using HOG descriptor. Additionally, the idea of lighting discrepancies is incorporated by approach [57]. Illuminant color estimation on image region based on pixels and edges might help detect inconsistencies between distinct images. In Table 3, the all k data set was used, 30 percent of which was used for testing and 70 percent for training.

VI. DEEP LEARNING MODELS

Deep learning techniques are now applied to the detection of image manipulation [62, 63, 64]. Because these algorithms can extract complicated features from images, they reported higher accuracy than older methods. Typically, CNNs do not extract features through image editing, but rather rely on the content of the images.

Since certain local relationships are altered by manipulation, it extracted the local structural relationship between pixels rather than taking the image's content into consideration.

In Tables 4, the all k data set was used, 30 percent of which was used for testing and 70 percent for training.

VII. CHALLENGES TO BE OVERCOME IN COPY-MOVE FORGERY DETECTION

Previous research has shown that it is challenging to identify which sections are from the same image. Thus, many of the features, including colors, noise, and lighting, remain largely consistent between the copied and pasted regions. Copy-move techniques fall into two categories, as previously mentioned: block-based and key-point-based techniques. Pre-processing is applied in block-based approaches by dividing the image into overlapping and non-overlapping blocks. Block-based matching techniques are used to match feature vectors that are derived from feature extraction algorithms. Thus, the calculations are more involved and need more time. Conversely, the segmentation of the image into blocks using key-point based approaches is eliminated. The identified local features from the image, like corners, edges, and blobs, are displayed with the extracted key-points. Key-point-based techniques, on the other hand, extract fewer key points from smooth surfaces and are quicker and less computationally demanding. Therefore, detection is more challenging. To overcome the drawbacks of using each method separately, the two are blended. To extract key points from the entire image using the hybrid method, segmentation can be done first.

VIII. CHALLENGES TO BE OVERCOME IN SPLICING FORGERY DETECTION

Previous research has shown that there are several issues that need to be resolved. Frequently encountered obstacles include computational intricacy, resilience to post-processing procedures, precise forgery location, and the requirement for resilient statistical attributes.

IX. THE PACKAGES AND PROGRAMS USED IN THE SIMULATION

The experiments were carried out on MATLAB, C++, and Python.

X. CONCLUSION

In this research, the different types of image forgery, which are copy-move, splicing, and retouching, are discussed, explaining the aim, the mechanism of action, and the advantages and disadvantages of each type. Techniques for detecting forgery images were also identified, explaining the aim and classification. Finally, deep learning techniques currently applied to detect image manipulation, in addition to comparisons were made between copy-move algorithms and splicing algorithms and the challenges to be overcome.

XI. FUTURE WORK

It is clear from the literature evaluations that there is still much to be done in forgery detection. Future work can be offered in many different branches because there are many different difficulties that need to be solved. These branches contain the localization of the forgery region and other discrete transform domain, or hybrid transforms may be utilization for forgery detection. Also, deep learning algorithms are used for forgery detection. Different coordinate systems may be tested to identify the more accurate channel. Robust statistical features are needed to enhance accuracy. New techniques are proposed to reduce the computational time

REFERENCES

[1] T. N. Baraskar, M. F. Jwaid, "Study and Analysis of Copy-Move & Splicing Image Forgery Detection Techniques," in International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, Tamilnadu, India, pp. 697-702, 2017.

[2] M. N. Nazli, A.Y. A. Maghari, "Comparison Between Image Forgery Detection Algorithms," in 8th International Conference on Information Technology (ICIT), Amman, Jordan, pp. 442-445, 2017.

[3] N. Kaur Gill, Ruhi Garg, and Er. Ami Doegar, "A Review Paper on Digital Image Forgery Detection Techniques," in 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, pp. 1-7, 2017.

[4] A. H. Mir, S. Mushtaq, "Digital Image Forgeries and Passive Image Authentication Techniques: A Survey," International Journal of Advanced Science and Technology, vol. 73, pp. 15-32, 2014.

[5] S. P. Ghrera,V.Tyag , M. D.Ansari, "Pixel-Based Image Forgery Detection: A Review," IETE Journal of Education, vol. 55, no. 1, pp. 40-46, 2014.

[6] M. DeSantis, G. S. Spagnolo, "Holographic watermarking for authentication of cut images," Optics and Lasers in Engineering, vol. 49, no. 12, pp. 1447-1455, 2011.

[7] D S Tomar, M. Rajawat, "A Secure Watermarking and Tampering detection technique on RGB Image using 2Level DWT," in Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, pp. 638-642, 2015.

[8] M. C. Hernandez, M. N. Miyatake, H. P. Meana, B. Kurkoski, L. R. Roldan, "Watermarking-based image authentication with recovery capability using halftoning

technique," Signal Processing: Image Communication, vol. 22, no. 1, pp.69-83, 2013.

[9] A. Jamil, A. Saldhi, M. Ahmad., S. Alam, "Digital Image Authentication and Encryption using Digital Signature," in International Conference on Advances in Computer Engineering and Applications (ICACEA), Ghaziabad, India, pp. 332-336, 2015.

[10] H. Kaur, A. Kakkar, M. Singh, "Digital Signature Verification Scheme for Image Authentication," International Conference on Recent Advances in Engineering & Computational Sciences (RAECS) -, Chandigarh, India, pp.1-5, 2015.

[11] J. Xue, Z. Zheng, Z. Liu and N. Li, X. Wang, "Image forensic signature for content authenticity analysis," Journal of Visual Communication and Image representation, vol. 23, no. 5, 2012.

[12] C. Wang, X. Zhou, X. Yu, "Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images," Future Internet, vol. 9, no. 4, pp. 56, 2017.

[13] Y. CHEN, WANG, Y. XIE, "Tamper Detection of Electronic Bills based on Semi-Fragile Watermarking," in First International Conference on Multimedia and Image Processing (ICMIP), Bandar Seri Begawan, Brunei, pp. 41-4., 2016.

[14] P. K. Dhar, T. Shimamura, I. Sikder, "A Semi-Fragile Watermarking Method Using Slant Transform and LU Decomposition for Image Authentication," in International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, pp. 881-885, 2017.

[15] V. H. Mankar, G.K. Birajdar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no. 3, pp 226–245, 2013.

[16] K. Hayat, S.U. Khan, S. A. Madani,T. Qazi, "Survey on blind image forgery detectionx," IET Image Process, vol. 7, no. 7, pp. 660–670, 2013.

[17] Anthony T.S., Ho and Shujun Li, "Handbook of Digital Forensics of Multimedia Data and Devices," Forensic Camera Model Identification", Wiley-IEEE Press, 2015.

[18] J. Malik, A. Singh, "A Comprehensive Study of Passive Digital Image Forensics Techniques based on Intrinsic Fingerprints," International Journal of Computer Applications, vol. 116, no. 19, pp. 16-21, 2015.

[19] Tu K. Huynh, Khoa V. Huynh, Thuong Le-Tien, and Sy C. Nguyen, "A Survey on Image Forgery Detection Techniques," International Conference on Computing & Communication Technologies, Can Tho, Vietnam, pp. 71-76, 2015.

[20] N. Vaswani, T. K. Sarode, "Copy – Move Forgery Detection using Orthogonal Wavelet Transforms," International Journal of Computer Applications, vol. 88, no. 8, pp. 41-45, 2014.

[21] A. Khade, D. K. Chitre, R. A. Maind, "Image Copy Move Forgery Detection using Block Representing Method," International Journal of Soft Computing and Engineering (IJSCE), vol. 4, no. 2, pp. 49-53, 2014.

[22] R. Naskar, R. Dixit, " DyWT based Copy-Move Forgery Detection with Improved Detection Accuracy," in International Conference on Signal Processing and Integrated Networks, vol., pp.133-138, Noida, India, IEEE 2016.

[23] T. Nawaz, Z. Mehmood, Z. Khan, M. Shah, R. Ashraf, T. Mahmood, "Forensic Analysis of Copy-Move Forgery in Digital Images Using the Stationary Wavelets," in Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, pp.578-583, 2016.

[24] Z. Bai, L. Yin, H. Gao, R. Yang, "Detecting of Copy-Move Forgery in Digital Images Using Fractional Fourier Transform," in Seventh International Conference on Digital Image Processing (ICDIP15), Los Angeles, United States, vol. 9631-96310B, 2015.

[25] M. Manuel, R. P. Yohannan, "Detection of copy-move forgery based on Gabor filter," in 2nd IEEE International Conference on Engineering and Technology (ICETECH), India, Coimbatore, pp. 629-634, 2016.

[26] N. Saxena, S.K Vasistha, A. Gupta, "Detecting Copy move Forgery using DCT," International Journal of Scientific and Research Publications, vol. 3, no. 5, pp. 1-4, 2013.

[27] D. Jagan, M. Shaktidev, K. Sunil, "DCT-PCA Based Method for Copy-Move Forgery Detection," ICT and Critical Infrastructure, Springer International Publishing Switzerland, vol.2, pp. 577-583, 2014.

[28] Y. Gan, J. Young, L. Huang, and P. Lin, J. Zhong," A new block-based method for copy move forgery detection under image geometric transforms," Multimedia Tools Appl., vol. 76, no. 13, pp. 14887-14903, 2016.

[29] S. M. Fadl and N. A.," Robust Copy-Move forgery revealingin digital images using polar coordinate system," Neurocomputing, vol. 265, pp. 57-65, 2017.

[30] A. Kunbazand, S.Saghir, "Fake Image Detection Using DCT and Local Binary Pattern," in Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), Istanbul, Turkey, pp. 1-6, 2019.

[31] F. H. Pugarand, S.Muzahidin, "Copy-Move Forgery Detection Using SWT-DCT and Four Square Mean Features," in International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, pp. 63-68, 2019.

[32] A. K. Jaiswal, D. Gupta," Detection of Copy-Move Forgery Using Hybrid approach of DCT and BRISK," in International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 471-476, 2020.

[33] R. Ashraf, M. S. Mehmood," An Efficient Forensic Approach for Copy-move Forgery Detection via Discrete Wavelet Transform," in International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, pp. 1-6 2020.

[34] Norziana Jamil, Ismail Taha Ahmed, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," in IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, pp. 92-96, 2021.

[35] Kh. M. Singh, R. Rajkumar, "Digital Image forgery detection using SIFT feature," in International Symposiwn

on Advanced Computing and Communication, , Silchar, India, pp.186-191, 2015.

[36] G. Muzaffer, G. Uluts, B. Usutbioglu, "A Novel Keypoint Based Forgery Detection Method Based on Local Phase Quantization and SIFT," in International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, pp.185-189, 2015.

[37] V. Anandb, A. G. Keskar, M.F. Hashmi, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-Decimated Wavelet Transform and Scale Invariant Feature Transform," AASRIProcedia, science direct, vol. 9, pp.84 – 91, 2014.

[38] S. Budhiraja, A. Dhindsa, L. K. Bhullar, "DWT and SIFT based Passive Copy-Move Forgery Detection," International Journal of Computer Application, vol. 95, no. 23, pp. 14-18, 2014.

[39] S. Sodhi, M. kaur, "Surf Technique for Copy Move Forgery Detection," International Conference on Advances in Emerging Technology, ICAET, India, pp. 10-12, 2016.

[40] N. Josephb ,R. Raj, "Key point Extraction Using SURF Algorithm for CMFD," Procedia Computer Science, vol. 93, pp. 375-381, 2016.

[41] A. Paulose, S. Krishna, 41. V.S. Babu, ""Digital Image Forgery Detection Using SURF," IOSR Journal of Computer Engineering, vol. 18, no. 6, pp. 144-164, 2016.

[42] Fan Yang, Jingwei Li, Wei Lu, Jian Weng,"Copy-move forgery detection based on hybrid features," Engineering Applications of Artificial Intelligence, vol. 59, p. 73-83, 2017.

[43] Abdul Wahab AW, IdnaIdris MY, Fazidah O.RS, Abdul Warif NB, "SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack," Journal of Visual Communication and Image Representation, vol. 46, p. 219–232, 2017.

[44] Pun CM, Yuan XC., Bi X, "Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection," Information Sciences, vol. 345, p. 226–242, 2016.

[45] S. K. Shah, 45. P. S. Raskar, "A Fast Copy-Move Forgery Detection Using Global and Local Features," in 5th International Conference on Computing Communication Control and Automation, Pune, India, pp. 1-4, 2019.

[46] N. A. Kurien, S. Danya, D. Ninan, C. Heera Raju and J. David, "Accurate And Efficient Copy-Move Forgery Detection," in 9th International Conference on Advances in Computing and Communication (ICACC), Kochi, India, pp. 130-135, 2019.

[47] X. YANG, H. CHEN, "Copy-Move Forgery Detection Based on Key point Clustering and Similar Neighborhood Search Algorithm," IEEE ACCESS, vol. 8, pp. 36863 - 36875, 2020.

[48] A. Youssif, A. Badr, "A Robust Copy-Move Forgery Detection In Digital Image Forensics Using SURF," in 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, pp. 1-6, 2020.

[49] Krishna A N, Sunitha K., "Efficient Key point based Copy Move Forgery Detection Method using Hybrid Feature Extraction," in International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, pp. 670-675, 2020.

[50] P. e Carré, C. F. Maloigne, Y. Fan, "Image Splicing Detection With Local Illumination Estimation," in International Conference on Image Processing (ICIP), Quebec City, QC, Canada, pp.2940-2944, 2015.

[51] H. A. Jalab, R. M. Noor, Z. Moghaddasi, "SVD-based Image Splicing Detection," in 6th International Conference on Information Technology and Multimedia (ICIMU), Putrajaya, Malaysia, pp.27-30, 2014.

[52] M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, A. A. Alahmadi, "Splicing Image Forgery Detection Based on DCT and Local Binary Pattern," in Global Conference on Signal and Information Processing (Global SIP), Austin, TX, USA, pp. 253-256, 2013.

[53] M. A. Qureshi, E. M. El-Alfy, "Combining spatial and DCT based Markov features for enhanced blind detection of image splicing," Pattern analysis and application, vol. 18, no. 3, pp. 713-723, 2015.

[54] M. Hariri, F. Gharehbaghi, F.Hakimi, "Image Splicing Forgery Detection Using Local Binary Pattern and Discrete Wavelet Transform," in International Conference on knowledge based engineering and innovation, Iran, pp. 1074-1077, 2015.

[55] Z. Zhang, Z. Kaizhen, "A Novel Algorithm of Image Splicing Detection," in International Conference on Industrial Control and Electronics Engineering, Xi'an, China, pp. 1972-1930, 2012.

[56] J. Esther, P. Sabeena, "Detection of digital image splicing using luminance," International Journal of Engineering Research and Applications, pp. 29-33, 2014.

[57] R. R.Cherian, S. N. Youseph, "Pixel and Edge Based Illuminant Color Estimation for Image Forgery Detection," ,Procedia Computer Science, vol. 46, pp. 1635 – 1642, 2015.

[58] Gupta S., Kaur M, "A passive blind approach for image splicing detection based on DWT and LBP histograms," International Symposium on Security in Computing and Communication, vol. 625, Springer, pp. 318–327, 2016.

[59] U. Kumar, S. P. Tripathi, E. Tripathi, "Automated Image Splicing Detection using Texture based Feature Criterion and Fuzzy Support Vector Machine based Classifier," in International Conference on Cutting-edge Technologies in Engineering, Uttar Pradesh, India, pp. 81-86, 2019.

[60] K. Kumar, S. Walia," Characterization of splicing in digital images using gray scale co-occurrence matrices," in Twelfth International Conference on Contemporary Computing (IC3), Noida, India, pp. 1-6, 2019.

[61] A. Girdhar, L. Kaur, N. Kanwal, "Detection of Digital Image Forgery using Fast Fourier Transform and Local Features," in International Conference on Automation, Computational and Technology Management, London, United Kingdom, pp. 262-267, 2019.

[62] M. M. Goswami, Z. J. Barad, "Image Forgery Detection using Deep Learning: A Survey," in International Conference on Advanced Computing & Communication Systems, Coimbatore, India, pp. 571-576, 2020.

[63] K. Kumar, S. Walia, "Digital image forgery detection: a systematic scrutiny," Australian Journal of Forensic Sciences, pp. 1-39, 2018.

[64] M. A. Khan, A. H. Saber, "A Survey on Image Forgery Detection Using Different Forensic Approaches," Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 361-370, 2020.

[65] H, et al., Choi, "Detecting composite image manipulation based on deep neural networks," in International Conference on Systems, Signals, and Image Processing (IWSSIP), Poznań, Poland, pp. 1-5, 2017.

[66] Ni J., Rao Y, "A deep learning approach to detection of splicing and copy-move forgeries in images," in IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, pp. 1-6, 2016.

[67] A. K. Jaiswal, R. Srivastava, "Image Splicing Detection using Deep Residual Network," SSRN Electronic Journal, 2019.

[68] J. Ni, H. Zhao, Y. Rao, "Deep Learning Local Descriptor for Image Splicing Detection and Localization," IEEE Access, vol. 8, pp. 25611-25625, 2020.

Table 1. techniques of block-based CMFD

Paper [Publication Year]	Features used	Block size	classifier/ matching	threshold	Dataset	Performance metric	Advantage	Disadvantage
23 [2016]	Stationary Wavelet Transform	8*8	Euclidean distance matching.	0.01	Google image search,	tPr = 97.8% fPr = 2.6%	demonstrating the detection capability for multiple CMF.	Don't evaluate the proposed technique on large scale image databases
24 [2016]	Gabor Transform	8*8	Euclidean distance matching.	3	CoMoFoD dataset	tPr = 90.9% fPr = 5.6%	Robustness against Gaussian blurring,Rotation,Additive white Gaussian noise	Weak to identify multiple copy-move
28 [2016]	Discrete Radial Harmonic Fourier Moments	circular block	2 Nearest Neighbors	0.6	MICC-F220, MICC-F600, MICC-F2000	Precision (pr)=94.7% Recall (re)=91%	Low false matching, robust to geometrical transformations	The JPEG compression and detection performance under Gaussian noise need to be improved
29 [2017]	Polar Coordinate System (PCS)+ Fourier transform	8*8	Correlation between each pair	Correlation threshold 0.99	DVMM Colombia university	Precision (pr)=99.5%	Robust to compression, blurring, rotating, scaling, and brightness.	Geometric and intensity modification need to improve
30 [2019]	LocalBinaryPatternand 2D Discrete Cosine Transform	16*16	Support Vector Machine (SVM)		CASIA TIDE v1.0	Accuracy=96.8%	increase the performanceby capturing the micro-texture patterns using LBP	Untested to different variations
31 [2019]	Stationary Wavelet Transform (SWT), Discrete Cosine Transform (DCT)	8*8	distance similarity threshold	0.00005	CoMoFoD dataset	F1-scores = 94.060% recall = 89.074%	Quick processing speed and resilience to changes in brightness, contrast, blurring of images, and color	Don't evaluate the proposed technique on large scale image databases

							reduction.	
32 [2020]	DCT (Discrete cosine Transform) and BRISK (Binary Robust Invariant Scalable Keypoints) features	8*8	FLANN matcher and Euclidean distance-based clustering		CoMoFoD dataset	Precision=86.14% Recall=87% f1-score=86.45 %	resilient not only to scaling and rotation but also to blurring and the ability to identify numerous fabricated regions.	Need to enhance the performance
33 [2021]	discrete wavelet transform (DWT)	8*8	phase correlation	1.5	CoMoFoD dataset	Precision=98.6 % Recall=96.3 % f1-score=97.5%	minimizes the execution time effective and efficient CMIF detecting technique	Untested to different variations
34 [2021]	statistical features,like mean and standard deviation	32x32	Support Vector Machine (SV	----------	MICC-F220	Accuracy=96.3%	High detection accuracy, robust to rotation and scaling	Untested to different variations

Table 2. CMFD techniques based on keypoints

paper [Publication Year]	Features used	Feature dimension	classifier/ matching	Dataset	Performance metric	Advantage	Disadvantage
42 [2017]	SIFT, KAZE	128, 64	2NN	CMFD	Precision = 95.45% recall = 87.25% f-score = 91.11%	robust against noise addition, scaling, rotation, and JPEG compression	Extract more key-point
43 [2017]	SIFT-Symmetry	128	g2nn/ symmetry matching	cAsiA v2.0	f-score = 89.4%	strong resistance to CMF with reflection	less successful at identifying high rotational degrees when combined with reflection

44 [2016]	colour texture, Pcet		Hierarchical feature Matching	cMfD, cMfDPM	Precision = 91.37% recall = 84.64% fscore = 87.88%	robustness against various attacks.	Achieve low accuracy
45 [2019]	Zernike moments and local features are extracted by using SIFT descriptors		Hash Generation	CoMoFoD	success rate=95%	robust against various tampering fast and more accurate results	Untested for post-processing various tampering
46 [2019]	SIFT		Euclidean distance	CoMoFoD	Precision =93.75% Recall=62.5 % Accuracy=61. 5%	effective and reliable	Low accuracy
47 [2020]	SIFT		classified according to color and scale	GRIP, FAU	Precision = 99.7% recall = 99.6% f-score = 99.7%	superior robustness and the ability to precisely identify tampered sections, particularly on easy forgeries	This approach has low effect and is unstable when used in large-scale forgeries.
48 [2020]	SURF		ANN	CoMoFoD, MICC-F2000, MICC-F220, and MICC-F600	TPR=95% FPR=5.42%	Fast computing	To detect more intricate and hard copy-move forgeries, the detection accuracy must be increased.
49 [2020]	SURF+SIFT		Agglomerative hierarchical clustering	MICC-F220	TPR=92.5% FPR=8.9% F1-Score=91.7%	significant performance	Need to improve accuracy and increase false positive

Table 3. Splicing methods

paper [publication year]	Features used	Feature dimension	classifier/ matching	Dataset	Performance metric	Advantage	Disadvantage
50 [2015]	generalized grey-world		Euclidian distance	CASIA V2.0.	TPR=52.3% FPR=19.5% Accuracy=76.	works well with minimal human	The accuracy very weak. Need to enhancement

	algorithms .				6%	interaction.	
51 [2014]	singular value decomposition with discrete cosine transform	50	Support vector machine	Columbia Image Splicing Detection	TPR=80.1% FPR=77.6% Accuracy=78.7%	In terms of detection rate, SVD+SVD-DCT is superior to SVD and SVD-DCT alone.	need more improvement Not applicable to color images.
52 [2013]	Local BinaryPatternand Discrete Cosine Transform		support vector machine	CASIA v 1.0, CASIA v2.0 Colwnbia datasets	Accuracy=97.5%	Give the best accuracy so far.	----------
53 [2014]	Markov features in spatial and Discrete Cosine Transform domain	150	support vector machine	Columbia Image Splicing Detection	TPR=98.6%FPR=98.01% Accuracy=98.3%	This method works better than the most recent splicing detection techniques.	Principal, decrease precision in order to lessen the computational complexity brought on by excessive dimensionality
54 [2015]	Local binary pattern +wavelet transform +PCA		support vector machine	Columbia, CASIA v 1.0	Accuracy=97.2%	Effective detection technique	Untested to post processing operation
57 [2015]	inconsistencies in illuminant color of images by Weighted gray edge estimation		support vector machine	----------	Accuracy=74 %	demonstrated how to use illuminant color estimate under different limitations to detect forgeries.	Low accuracy computational complexity
58 2016]	DWT and LBP	1024	SVM classifer	cAsiA V1, V2, columbia compressed and uncompressed	accuracy = 94.09%	minimal processing complexity and is unaffected by continuous variations in illumination	When the image size is too small, the method's performance suffers.
59 [2019]	texture based featuresof		fuzzy support vector	CASIA TIDE v1.0	Precision = 89% recall = 88% f-score	More effective	Untested to post processing operation

	Grey Level Run Length Matrix		machine		= 90%		
60 [2019]	gray scale co-occurrence matrices		SVM classifier	CASIA TIDE v1.0	TPR=74% FPR=87% Accuracy=82 %	Compare between unsupervised andsupervised method for classification	Need to increase the accuracy
61 [2019]	fast fourier transform		SVM classifier	CASIA v1.0.	Accuracy=88. 6%	suggests a relatively better texture descriptor	increases the complexity

Table 4. Deep learning methods

paper [Publication Year]	Forgery type	Feature used	Dataset	Advantage	Disadvantage	Performance metric
65 [2017]	detection of composite forgeries Gaussian blurring Median filtering adjustment for gamma	based on deep learning	Dresden image Database	Reliability and high performance	need to test another types of forgery	accuracy= 87.31%
66 [2016]	applications for copy-move detection and splicing	Deep learning based	CASIA v1.0, CASIA v2.0, Columbia gray DVMM	high accuracy	High computation time	Acc.cAsiAv1.0 = 98.04% Acc. cAsiA v2.0 = 97.83% Acc.DVMM = 96.38%
67 [2019]	Image splicing	Deep learning based	CASIA 2.0 datase	Improve the precision Effective localization of a spliced forged image	Unsuitable for detecting copy-move forgeries High-performance system needed to put the algorithms into practice	Accuracy=70% Specificity=63% Sensitivity=74%
68 [2020]	Splicing Detection and Localization	Deep learning based	CASIA v2.0, Columbia gray DVMM.	Sturdiness against JPEG encoding Exceptionally accurate detection	Significant complication when using a 30-line high-pass filter for future fusion	Accuracy=97.5%