Advanced Research in Electrical and Electronic Engineering
p-ISSN: 2349-5804; e-ISSN: 2349-5812, Volume 11, Issue 1; January-March, 2024, pp. 12-20

http://www.krishisanskriti.org/Publication.html

Analysis on Recent Tools and Techniques for Image Forgery Detection

Satyendra Singh[1], Rajesh Kumar[2] and Chandra. Kant Singh[3]

[1]Ph. D Scholar and Department of Electronic and Communication, University of Allahabad, INDIA
[2]Assistant Professor Department of Electronic and Communication, University of Allahabad, INDIA
[3]Uttar Pradesh Rajrshitandon Open University, Prayagraj, INDIA
E-mail: [1]satyendra@allduniv.ac.in, [2]rajeshkumariitbhu@gmail.com, [3]cksingh_apsu@hotmail.com

Abstract—*Image has an importance in people's daily life. In present days, images are everywhere such as social media, healthcare, education, magazines, newspapers, and courtrooms. Image is the popular medium for visual communication. The advancement of internet technology has increased the speed of image transmission. Images are often used as evidence to support claims or statements. If images have been tampered with, the resulting misinformation can have serious consequences. The authenticity of a digital image is more important. This paper presents an investigation into the latest tools and techniques used in the field of photo manipulation detection. Specifically, it explores various active and passive and image manipulation techniques. The active manipulation techniques watermarks and digital signatures. The passive image forgery techniques like copy-move, splicing, deep fake, morphing, etc. The detailed analysis of exiting techniques to detect both types of image manipulations with comparison tables. The machine learning, deep learning techniques based several image manipulation detection techniques has been investigated. Describe about the available dataset in separate table with original and manipulated images. This study also discusses the available method like convolutional neural networks and generative adversarial networks, to detect image manipulations effectively. Additionally, traditional methods such as image forensics and statistical analysis has been discussed. The paper highlights the importance of continued research and development in this area to combat the increasing sophistication of image forgery. By effectively addressing the issue of image forgery, this research aims to safeguard the photo authenticity, maintain the credibility of visual communication, and prevent the propagation of misinformation. The insights and methodologies presented in this paper offer valuable contributions to the ongoing efforts to tackle image forgery and its potential impact on society.*

INTRODUCTION

Image is a popular source of information. Digital images provide a visual representation that is easily understandable and relatable to a broad audience. They offer insights, convey emotions and complex ideas quickly and effectively. Digital image presents everywhere, finding application in diverse fields like healthcare, entertainment, newspapers, magazines, and courtrooms as an evidence. The involvement of the image has been increased day to day in people daily life. Capturing and transmitting digital images has become more convenient, due to availability of cheap camera enabled smartphones. People manipulate images for making them look more attractive and for entertainment. The significance of images raises questions about the reliability and credibility of photos.

Image forgery detection has become increasingly very popular in present days. The widespread use of digital photograph and the easy availability of manipulated software. With the rise of digital media and the internet, images can be easily shared and distributed, making it possible for false or misleading information to be spread quickly and easily [1]. To address this growing concern, researchers and practitioners have been developing new tools and techniques for image forgery detection. These tools and techniques are designed to analyses images and determine their authenticity, making it possible to detect image forgeries and prevent the spread of false or misleading information [2]. The most recent tools and techniques for photo manipulation identification include machine learning algorithms, computer vision techniques, and digital forensics techniques. These tools can be used to analyses various aspects of an image, such as its content, metadata, and statistical properties, to determine its authenticity [3].

Computer vision techniques, such as error-level analysis (ELA), are also being used to detect image forgeries [4]. These techniques can be used to analyze the visual structure and content of an image, making it possible to detect noise or anomalies that suggest that the manipulated photo. Digital forensics techniques, such as passive digital image forensics, can also be used to detect image forgeries. These techniques can be used to analyze the metadata and other digital properties of an image, such as its file format, to determine its authenticity [5]. Image forgery is the manipulation of an image to change its original content or deceive viewers [6].

we have been studied number of research article related to photo forensics. The contribution involves a comprehensive investigation into the realm of manipulated image detection.

Our main aim has been answering different questions related to digital image forgery. Thoroughly studied various existing methods for detecting image forgery, looking closely at how they work. We took a systematic approach to understand these methods better, considering what they can and cannot do. We added valuable information to the understanding of detecting image forgery.

The remaining paper has been organized as follows: in the section 2 study about fake image and types of digital image forgery, in the section 3 learn about the image forgery detection techniques, in the section 4 comprehensive assessment of the different existing research related to digital image forgery, in section 5 study different datasets of different types of image forgery, and finally conclude the overall study in section 6.

FAKE IMAGE

A fake image is a computer-generated image that has been altered or modified to appear as a real picture. It can be created using software such as Adobe Photoshop or by taking an existing image and changing it with digital tools [7]. Fake images can be used for a variety of purposes, such as fraud, entertainment, or propaganda.

There are some important types of forgeries 1. Copy move, 2. Deep fake, 3. Image Splicing, 4. Photo Montages: Photo montages involve taking multiple photos and combining them together to create an entirely new image, 5. Object Removal/Insertion: Objects in images can be removed or inserted using tools such as Photoshop to create false images, 6. Filters: Adding filters or effects to images can drastically change the way the image.

COPY MOVE

Copy move forgery detection is a method of identifying images that have been altered by making a copy of a certain portion and moving it to another part of the picture. This manipulation is usually done to hide something in the image's background [8]. Copy move tampering detection involves analyzing the pixels in an image to detect if any part of the image has been duplicated or moved [9], [10]. In Figure 2 shows the copy move tampering, image (b) is the real image and parts of the image copied and paste on specific place to generate image (a) which is tempered.

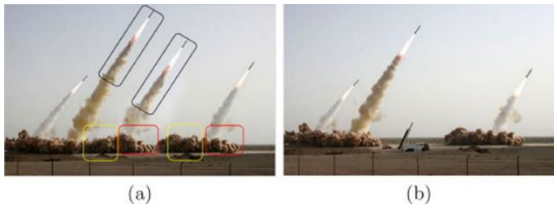

Figure 1: Image (b) is the original image and (A) tempered image

DEEP FAKES

Deep fakes are manipulated videos or audio recordings that are generated using deep learning and AI to change the face of someone with another person's face [11]. Deep fake images are images that have been manipulated using deep learning techniques to create a convincing, but fake, representation of someone or something [12]. Deep learning algorithms are trained to investigate and learn patterns in the large image dataset, and then use that knowledge to create new photo or alter existing ones. In the case of deep fake images, this technology is used to tampered photos in a way that alters the appearance of the person or object depicted in the image. [13]. Deep fake images can be created using a variety of techniques, including face-swapping, where one-person face is replaced with another face, or image synthesis, where an entirely new image is created from scratch using elements from other images [14]. In Figure 3 demonstrate the example of deep fake image.

Figure 2: Example of original and Deep fake image. Which is taken from

IMAGE SPLICING

Image splicing is a technique used to manipulate digital images by adding two or more photos into a single image. This process is often used to create forgeries, or fake images that appear to be real. Image splicing can be done using a variety of methods, including copy-and-paste, image blending, and image warping [15]. In a typical splicing scenario, an attacker might take a source image and paste a section of it onto a target image. The attacker might then use image processing techniques to blend the two images together, complex to detect the manipulation [16]. Figure 4 demonstrate the splicing image.

Figure 3: photo (a) is the real and photo (b) spliced

The splicing has two types of forgery (1) Boundary based splicing and (2) Region based splicing [17]. There are various ways to detect image forgeries created using splicing techniques. Some methods include analyzing the consistency of lighting and shadows in the image, detecting inconsistencies in the texture and pattern of the image, and using digital image forensics tools to examine the underlying data of the image [18, 19].

MORPHING

It is a special effect in computer graphics that allows one object to transform into another. It is commonly used in films and advertisements to show two objects morphing into one. Morphing can be used to create a smooth, seamless transition between two objects or images that are drastically different in appearance [20], [21]. In Figure 5 demonstrate the example of morphed image. In this Figure 5 Kamala Harris vice precedent USA fake paste on original image to create morphed image.

Figure 4: Shows the example of morphed image which taken from alt news official website

Image inpainting

it is used in computer vision and image processing to restore missing or damaged parts of an image [22]. It's like digital image restoration, where aim is to fill in the missing information in a visually plausible and coherent way. This can be particularly useful for restoring old or damaged photographs, removing unwanted objects from images, color black and white pictures, or even in artistic applications to create seamless modifications. Image inpainting technology can be categorized into three types: deep learning-based image inpainting, image editing, and image synthesis inpainting [23].

IMAGE FORGERY DETECTION TECHNIQUES

There are some different ways to identify fake images. These include visual inspection, computer analysis, and forensics. 1.

IMAGE AUTHENTICATION TECHNIQUES

Digital images are important sources of information. To preserve the credibility and integrity of images, various image authentication methods invented. These techniques can be broadly categorized into two types: active authentication and passive authentication techniques. Figure 7 illustrates the active and passive image authentication techniques.

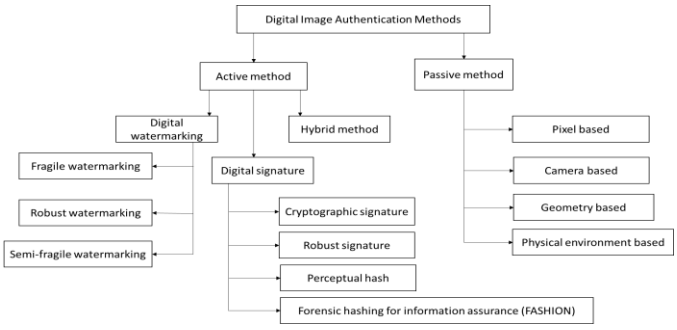

Figure 5: Digital image authentication techniques

1. Active Authentication

Active image authentication is the method to identify authenticity of an image by detecting whether it has been intentionally manipulated or forged. It involves analyzing the image to identify signs of tampering and determining whether the image has been altered from its original form [25]. Digital signature, hybrid methods, and watermarking are an example of active image forgery techniques.

2. Digital Watermarking

Digital watermarking in images refers to the process of embedding a unique and often imperceptible digital mark or signature into an image, for copyright protection, content authentication, or tamper detection [26]. The digital watermark is a form of metadata that is embedded within the image itself, and it can be used to identify the owner of the image, verify the integrity of the image, or track the distribution of the image [27], [28]. Watermarking researchers primarily focus on copyright protection. Numerous researchers have developed security methods for watermarking. The watermarking has fragile watermarking, semi-fragile watermarking, and robust watermarking techniques, all aimed at safeguarding the copyright of images and documents [29].

Sinhal et al. [30] proposed a model to investigate medical image watermarking. The deep neural network-based techniques are used to authenticate fragile watermarking scheme. This is the more effective blind solution to authenticate medical image watermarking. Author [31] introduces a nested block-based self-embedding technique designed for watermarking of fragile image. The method has been achieved good PSNR 40dB, true positive rate 95% and false positive rate less than 1%. Many researchers worked on fragile watermarking authentication techniques [32], [33], [34], [35], [36].

Kolivand et al. [37] introduced a robust watermarking authentication scheme. The experiment was conducted using a DICOM MRI dataset comprising 232 images. While this experiment, an average PSNR of 260.4767 dB and an average bit error rate of 0.2573 were attained. To evaluate the performance of a watermarking model, metrics such as bit error rate and normalized cross correlation (NCC) are employed.

Significant research has been conducted by various researchers in the domain of robust watermarking authentication schemes [38-42].

Semi-fragile watermarking is another form of watermarking authentication method. This approach is more robust in comparison to fragile watermarking. The primary aim of this technique to identify the dangerous manipulations. These manipulations involve adding or removing crucial image features. It also separates such changes from processes that shouldn't alter the image's meaning. Senol et al. [43] proposed a semi fragile watermark authentication method. This method authenticates image with 75% jpeg compression quality. The

watermark we added can survive common image changes like adjusting brightness, making histograms equal, and gamma correction. The method has been achieved PSNR 40.577. This model had better perform in comparison to available studies.

3. Passive Authentication

The method of authentication of digital image without adding any extra information. This technique involves investigation of image's intrinsic properties, such as noise levels, lighting conditions, and camera response, to detect any inconsistencies that may indicate that the image has been manipulated [44]. The passive forgery techniques such as splicing, retouching, copy-move, etc [45].

4. Source Camera Identification

This approach involves analysing the image's metadata to determine the type of camera that was used to capture the image [46]. This information can then be used to verify the authenticity of the image. Computer vision techniques play a critical role in the detection of image forgeries [47].

COMPREHENSIVE ASSESSMENT OF CONCLUDING GROUP OF STUDIES

In this section, we explore various image forgery detection methods, including machine learning, deep learning, and traditional approaches. Our analysis includes crucial parameters: detection domain, chosen models, datasets, performance metrics, and key findings. This assessment sheds light on algorithm effectiveness, dataset importance, model capabilities, and metric evaluation. The insights gained enhance our understanding of contemporary image manipulation detection techniques. In Table 1 presents the different image manipulation detection techniques based on deep learning approaches.

Table 1: Study of existing research to detect image forgery using deep learning techniques

Study	Detection domain	Model	Datasets	Performance metrics	Key Findings
Poddar, et al. [48]	Signature forgery	CNN	1320 images	Accuracy is 94%	The proposed system improves signature forgery detection at runtime.
Bibi et al. [49]	Splice and Copy-move	AlexNet	CASIA	93.3% accuracy for TIFF images and 95.9% JPEG images	Improve time complexity for classification.
Bappy et al. [50]	Copy-move, Splicing	CNN, LSTM	NIST Nimble 2016	Classification accuracy is 94.86% and AUC is 0.9138	Efficiently utilizes resampling characteristics for identifying manipulated areas
Wu et al. [51]	Copy-move	Deep neural network	CASIA TIDE v2.0 and	Precision, recall and f-score is 80.12%, 69.49% and 74.43% respectively on CASIA dataset, 67.83% 85.69% 75.72%	The deep neural network-based model better performs in comparison to classical methods
Zhang et al. [52]	Forgery localization	Two stage deep learning techniques	CASIA	Accuracy of the model is 91.09%	Method works on multi format image forgery
Ali et al. [53]	Splicing, copy-move	CNN	CASIA2.0	92.23% validation accuracy	Model has less time to detect forgery and work well in slower device
Kuznetsov et al. [54]	Splice	VGG16	CASIA	Accuracy 97.8%	This method applies on jpeg compress image in narrow range
Agarwal et al. [55]	Copy-move	VGGNet	MICC-F220	Precision 98.026 recall 89.583 and accuracy 95%	It is better working on various attacks
Ouyang et al. [56]	Copy-move	CNN	OXFORD Flower, UCID, CMFD	Find test error rate on Oxford data, UCID, CMFD dataset 2.32, 2.43, 4.2 respectively.	The proposed method is working better if copy-move forgery has geometric attacks.

Mohammed et al. [57]	Copy-move	Sampling algorithm	2017 NIST Nimble C	AUC 0.74	In this work increase 8% to 10% AUC score.
Rao et al. [58]	Splice, Copy-move	CNN, SVM	Casia v2.0, Casia v1.0	Accuracy on cassia v1.0 98.04 and	Compare the performance of the model from existing state of arts study.

In Table 2 present the analysis of image forgery detection using traditional methods of image processing. In this comparative study, we take some important parameter to complete the study. Most of the researcher used Zernike Moments in the study of image forgery detection with and without image processing feature extractors. Zernike Moments are a set of mathematical descriptors used in image processing and pattern recognition to capture and represent the shape and texture information of objects within an image [59], [60]. It is used to describe the spatial distribution of pixel intensities within an image region by quantifying the variations in intensity as well as the object's boundary shape.

Wang et al. [61] proposed a method for detecting copy-move image forgery using a scale-invariant feature detector and PCET point extraction utilized as a descriptor. The enhanced g2NN algorithm is employed to search for identical features. The process includes removing falsely matched features, applying the RANSAC algorithm, and utilizing filtering approaches. Finally, mathematical morphological operations are applied to obtain the output of the proposed model. The authors found that the model excels in localizing copy-move forgery in smooth regions and high-brightness images. In Figure 8 demonstrate the framework of whole process to localize copy move forgery.

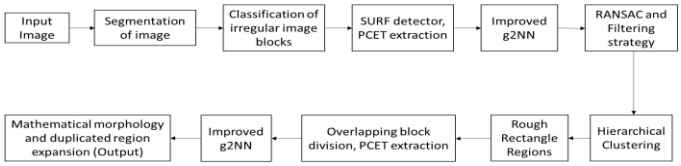

Figure 6: Framework of copy move forgery detection method proposed by Wang, et al. [61].

Hosny et al. [62] proposed a study to focuses on the deceptive practice of copy-move image forgery, where a portion of an image is duplicated and positioned within the same image to create a forgery. Introduce an accurate convolutional neural network (CNN) architecture designed to efficiently detect copy-move image forgery. Author suggest a lightweight architecture in terms of computation, featuring an appropriate configuration of convolutional and max-pooling layers. The research also presents a swift and precise testing process, taking only 0.83 seconds per test. A series of empirical experiments were conducted, demonstrating the model's effectiveness in both accuracy and speed. The experiments utilized benchmark datasets and achieved a perfect accuracy rate of 100%.

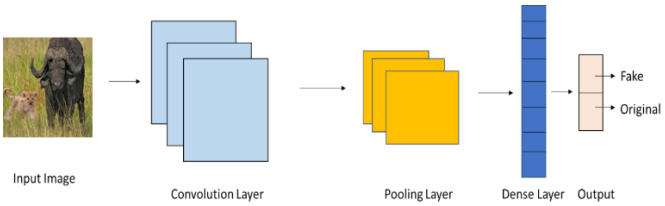

Figure 7: Convolution Neural Network (CNN) Layer

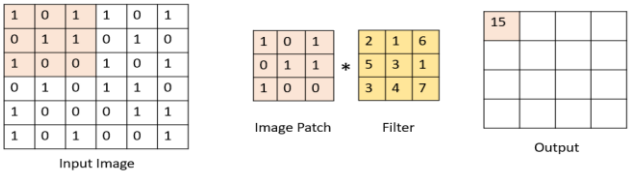

Figure 8: Convolution layer

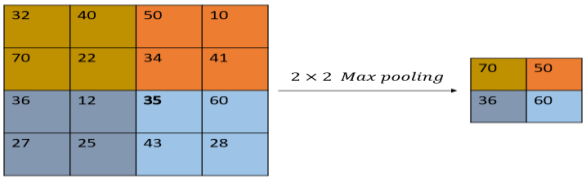

Figure 9: Max pooling layer

In Figure 9 demonstrate the convolutional neural network model, in Figure 10 presents the working of convolution, and in Figure 11 illustrate how max is performed.

DATASETS USED TO DETECT DIGITAL IMAGE FORGERY

In Table 3, we have analyzed popular image forgery datasets. These datasets play a crucial role in advancing the field of image manipulation detection by providing diverse and realistic examples of forged images. The availability of such datasets enables researchers and practitioners to train and evaluate sophisticated algorithms and methodologies aimed at effectively identifying various forms of image tampering. Consequently, these datasets contribute significantly to the enhancement and validation of image forensics technologies, fostering progress in the broader domain of digital image authenticity and security

Table 2: Describes several image manipulation datasets

Reference	Dataset	Types of forgery	Tempered images	Original Images
Amerini, et al. [63]	MICC-F220 MICC-F2000	Copy-move Copy-move	110 2000	110 1300

Amerini, et al. [64]	MICC-F600	Copy-move	160	440
Faria Hossain, et al. [65]	FORGERY IMAGE DATASET	Copy-move	3000	1000
Dong, et al. [66]	CASIA v1.0 CASIA v2.0	Splicing Splicing	921 5123	800 7200
Islam, et al. [67]	FBDDF	Splicing, Copy-move	200	200
Ng et al. [68]	Columbia	Splicing	180	183
Wen, et al. [69]	COVERAGE	Copy-move	100	100

We employ two categories of image manipulation techniques: basic manipulations techniques like adjusting contrast, altering colors, enhancing saturation, and complex processes such as splicing, morphing, copy-move, and retouching. Among these, DEFACTO is an image forgery dataset, containing four distinct forms of image forgery—splicing, morphing, copy-move, and inpainting. The DEFACTO dataset includes an extensive collection: 19,000 images involving copy-move forgery, 105,000 images splicing, 80,000 morphing, and an additional 25,000 images featuring inpainting [70]. Zhao et al. [71] describes the GRIP dataset, it contains 80 simple images and 80 tempered images with dimension 768×1024. USCISI is the copy move forgery dataset[1]. It contains 100,000 images with corresponding mask images [72]. The National Institute of Standards and Technology (NIST) and the Défense Advanced Research Projects Agency (DARPA) work in close collaboration to collectively release a series of valuable publicly available datasets. This includes the Nimble Challenge (NC) 2017, MFC18, MFC19, and MFC20 datasets. These datasets, namely NC17, MFC18, MFC19, and MFC20, includes a wide array of images 4K, 17K, 16K, and 20K images respectively [73].

CONCLUSION

In this paper, digital image forensics tools and techniques have been studied as the state of the art. This paper observes that the detection of image forgery is a challenging but important task with significant implications for individuals, organizations, and society. Deep fake images are very complex to identify as fake or real. Transfer learning-based fake image classifiers are working well. The Zernike Moments-based model achieved better accuracy in detecting copy-move forgery with different geometric attacks. The development of effective image forgery detection techniques is crucial to preventing the spread of false or misleading information, preserving the integrity of information, and protecting individuals and society from the negative consequences of forgery. Artificial intelligence-based image forgery detection models demonstrate higher detection accuracy compared to other available models. This paper is very helpful for understanding digital image forensics.

[1] https://github.com/isi-vista/BusterNet/tree/master/Data/USCISI-CMFD-Small

CONFLICT OF INTEREST

Authors have no conflict of interest.

FUNDING

In the preparation of this manuscript, we received no financial support from the institution

REFERENCES

[1] Qureshi, M. A., & Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. Signal Processing: Image Communication, 39, 46-74.

[2] Kaur, G., Singh, N., & Kumar, M. (2023). Image forgery techniques: a review. Artificial Intelligence Review, 56(2), 1577-1625.

[3] Chennamma, H. R., & Madhushree, B. (2023). A comprehensive survey on image authentication for tamper detection with localization. Multimedia Tools and Applications, 82(2), 1873-1904.

[4] Mallick, D., Shaikh, M., Gulhane, A., & Maktum, T. (2022). Copy Move and Splicing Image Forgery Detection using CNN. In ITM Web of Conferences (Vol. 44, p. 03052). EDP Sciences.

[5] Amjed, A., Mahmood, B., & Almukhtar, K. A. (2022, March). Approaches for Forgery Detection of Documents in Digital Forensics: A Review. In Emerging Technology Trends in Internet of Things and Computing: First International Conference, TIOTC 2021, Erbil, Iraq, June 6–8, 2021, Revised Selected Papers (pp. 335-351). Cham: Springer International Publishing.

[6] Hamid, Y., Elyassami, S., Gulzar, Y., Balasaraswathi, V. R., Habuza, T., & Wani, S. (2023). An improvised CNN model for fake image detection. International Journal of Information Technology, 15(1), 5-15.

[7] Hamid, Y., Elyassami, S., Gulzar, Y., Balasaraswathi, V. R., Habuza, T., & Wani, S. (2023). An improvised CNN model for fake image detection. International Journal of Information Technology, 15(1), 5-15.

[8] Meena, K. B., & Tyagi, V. (2019). Image forgery detection: survey and future directions. Data, Engineering and Applications: Volume 2, 163-194.

[9] Meena, K. B., & Tyagi, V. (2020). A copy-move image forgery detection technique based on tetrolet transform. Journal of Information Security and Applications, 52, 102481.

[10] Islam, M. M., Karmakar, G., Kamruzzaman, J., & Murshed, M. (2020). A robust forgery detection method for copy–move and splicing attacks in images. Electronics, 9(9), 1500.

[11] Yu, C. M., Chang, C. T., & Ti, Y. W. (2019). Detecting deepfake-forged contents with separable convolutional neural network and image segmentation. arXiv preprint arXiv:1912.12184.

[12] Hsu, C. C., Zhuang, Y. X., & Lee, C. Y. (2020). Deep fake image detection based on pairwise learning. Applied Sciences, 10(1), 370.

[13] Yang, J., Xiao, S., Li, A., Lan, G., & Wang, H. (2021). Detecting fake images by identifying potential texture difference. Future Generation Computer Systems, 125, 127-135.

[14] Abdulreda, A. S., & Obaid, A. J. (2022). A landscape view of deepfake techniques and detection methods. International Journal of Nonlinear Analysis and Applications, 13(1), 745-755.

[15] Pandey, A., & Mitra, A. (2022). Detecting and Localizing Copy-Move and Image-Splicing Forgery. arXiv preprint arXiv:2202.04069.

[16] Xiao, B., Wei, Y., Bi, X., Li, W., & Ma, J. (2020). Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. Information Sciences, 511, 172-191.

[17] Sharma, P., Kumar, M., & Sharma, H. (2023). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. Multimedia Tools and Applications, 82(12), 18117-18150.

[18] Nataraj, L., Mohammed, T. M., Chandrasekaran, S., Flenner, A., Bappy, J. H., Roy-Chowdhury, A. K., & Manjunath, B. S. (2019). Detecting GAN generated fake images using co-occurrence matrices. arXiv preprint arXiv:1903.06836.

[19] Tariq, S., Lee, S., Kim, H., Shin, Y., & Woo, S. S. (2019, April). Gan is a friend or foe? a framework to detect various fake face images. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (pp. 1296-1303).

[20] Wolberg, G. (1998). Image morphing: a survey. The visual computer, 14(8-9), 360-372.

[21] Farbman, Z., Hoffer, G., Lipman, Y., Cohen-Or, D., & Lischinski, D. (2009). Coordinates for instant image cloning. ACM Transactions on Graphics (TOG), 28(3), 1-9.

[22] Mehrjardi, F. Z., Latif, A. M., Zarchi, M. S., & Sheikhpour, R. (2023). A survey on deep learning-based image forgery detection. Pattern Recognition, 109778.

[23] Liu, K., Li, J., & Hussain Bukhari, S. S. (2022). Overview of image inpainting and forensic technology. Security and Communication Networks, 2022.

[24] Mani, R. G., Parthasarathy, R., Eswaran, S., & Honnavalli, P. (2022). A Survey on Digital Image Forensics: Metadata and Image forgeries. In Workshop on Applied Computing, January 27-28, 22 (Vol. 55, pp. 22-55).

[25] Kaur, G., Singh, N., & Kumar, M. (2023). Image forgery techniques: a review. Artificial Intelligence Review, 56(2), 1577-1625.

[26] Kumar, S., Verma, S., Singh, B. K., Kumar, V., Chandra, S., & Barde, C. (2023). Entropy based adaptive color image watermarking technique in YC b C r color space. Multimedia Tools and Applications, 1-27.

[27] Gutub, A. (2023). Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing. CAAI Transactions on Intelligence Technology, 8(2), 440-452.

[28] Hosny, K. M., Mortda, A. M., Lashin, N. A., & Fouda, M. M. (2023). A New Method to Detect Splicing Image Forgery Using Convolutional Neural Network. Applied Sciences, 13(3), 1272.

[29] Garg, P., & Jain, A. (2023). A robust technique for biometric image authentication using invisible watermarking. Multimedia Tools and Applications, 82(2), 2237-2253.

[30] Sinhal, R., & Ansari, I. A. (2023). Machine learning based multipurpose medical image watermarking. Neural Computing and Applications, 1-22.

[31] Rijati, N. (2023). Nested Block based Double Self-embedding Fragile Image Watermarking with Super-resolution Recovery. IEEE Access.

[32] Lin, C. C., Lee, T. L., Chang, Y. F., Shiu, P. F., & Zhang, B. (2023). Fragile Watermarking for Tamper Localization and Self-Recovery Based on AMBTC and VQ. Electronics, 12(2), 415.

[33] Benrhouma, O. (2023). Cryptanalysis and improvement of a semi-fragile watermarking technique for tamper detection and recovery. Multimedia Tools and Applications, 82(14), 22149-22174.

[34] Ouyang, J., Huang, J., Wen, X., & Shao, Z. (2023). A semi-fragile watermarking tamper localization method based on QDFT and multi-view fusion. Multimedia Tools and Applications, 82(10), 15113-15141.

[35] Sanivarapu, P. V., Kandala, R., & PVSSR, C. M. (2023). A Fragile Watermarking Scheme for Image Tamper Detection and Recovery Using Hybrid Transform. Available at SSRN 4476008.

[36] Renklier, A., & Öztürk, S. (2023). Image authentication and recovery: Sudoku puzzle and MD5 hash algorithm based self-embedding fragile image watermarking method. Multimedia Tools and Applications, 1-23.

[37] Kolivand, H., Wee, T. C., Asadianfam, S., Rahim, M. S., & Sulong, G. (2023). High imperceptibility and robustness watermarking scheme for brain MRI using Slantlet transform coupled with enhanced knight tour algorithm. Multimedia Tools and Applications, 1-40.

[38] Mehraj, S., Mushtaq, S., Parah, S. A., Giri, K. J., & Sheikh, J. A. (2023). A robust watermarking scheme for hybrid attacks on heritage images. Journal of Ambient Intelligence and Humanized Computing, 14(6), 7367-7380.

[39] Awasthi, D., & Srivastava, V. K. (2023). Robust, imperceptible and optimized watermarking of DICOM image using Schur decomposition, LWT-DCT-SVD and its authentication using SURF. Multimedia Tools and Applications, 82(11), 16555-16589.

[40] Rajput, S. S., Mondal, B., & Warsi, F. Q. (2023). A robust watermarking scheme via optimization-based image reconstruction technique. Multimedia Tools and Applications, 1-22.

[41] AlShaikh, M., Alzaqebah, M., & Jawarneh, S. (2023). Robust watermarking based on modified Pigeon algorithm in DCT domain. Multimedia Tools and Applications, 82(2), 3033-3053.

[42] Rakhmawati, L., Tjahyaningtijas, H. P. A., Yustanti, W., & Wiryanto, W. (2023). A Block-Based Image Characteristics

Robust Watermarking with Optimal Embeddable AC Coefficient. International Journal of Intelligent Engineering & Systems, 16(4).

[43] Senol, A., Elbasi, E., Topcu, A. E., & Mostafa, N. (2023). A Semi-Fragile, Inner-Outer Block-Based Watermarking Method Using Scrambling and Frequency Domain Algorithms. Electronics, 12(4), 1065.

[44] Mushtaq, S., & Mir, A. H. (2014). Digital image forgeries and passive image authentication techniques: a survey. International Journal of Advanced Science and Technology, 73, 15-32.

[45] Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital investigation, 10(3), 226-245.

[46] Freire-Obregon, D., Narducci, F., Barra, S., & Castrillon-Santana, M. (2019). Deep learning for source camera identification on mobile devices. Pattern Recognition Letters, 126, 86-91.

[47] Ahmed, F., Khelifi, F., Lawgaly, A., & Bouridane, A. (2019, January). Comparative analysis of a deep convolutional neural network for source camera identification. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 1-6). IEEE.

[48] Poddar, J., Parikh, V., & Bharti, S. K. (2020). Offline signature recognition and forgery detection using deep learning. Procedia Computer Science, 170, 610-617.

[49] Bibi, S., Abbasi, A., Haq, I. U., Baik, S. W., & Ullah, A. (2021). Digital image forgery detection using deep autoencoder and CNN features. Hum. Cent. Comput. Inf. Sci, 11, 1-17.

[50] Bappy, J., Mohammed, T. M., Nataraj, L., Flenner, A., Chandrasekaran, S., Roy-Chowdhury, A., & Lawrence Peterson, J. H. (2017). Detection and localization of image forgeries using resampling features and deep learning. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 69-77).

[51] Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018, March). Image copy-move forgery detection via an end-to-end deep neural network. In 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (pp. 1907-1915). IEEE.

[52] Zhang, Y., Goh, J., Win, L. L., & Thing, V. L. (2016). Image region forgery detection: A deep learning approach. SG-CRC, 2016, 1-11.

[53] Ali, S. S., Ganapathi, I. I., Vu, N. S., Ali, S. D., Saxena, N., & Werghi, N. (2022). Image forgery detection using deep learning by recompressing images. Electronics, 11(3), 403.

[54] Kuznetsov, A. (2019, November). Digital image forgery detection using deep learning approach. In Journal of Physics: Conference Series (Vol. 1368, No. 3, p. 032028). IOP Publishing.

[55] Agarwal, R., & Verma, O. P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimedia Tools and Applications, 79(11-12), 7355-7376.

[56] Ouyang, J., Liu, Y., & Liao, M. (2017, October). Copy-move forgery detection based on deep learning. In 2017 10th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI) (pp. 1-5). IEEE.

[57] Mohammed, T. M., Bunk, J., Nataraj, L., Bappy, J. H., Flenner, A., Manjunath, B. S., ... & Peterson, L. (2018). Boosting image forgery detection using resampling features and copy-move analysis. arXiv preprint arXiv:1802.03154.

[58] Rao, Y., & Ni, J. (2016, December). A deep learning approach to detection of splicing and copy-move forgeries in images. In 2016 IEEE international workshop on information forensics and security (WIFS) (pp. 1-6). IEEE.

[59] Liao, S. X., & Pawlak, M. (1998). On the accuracy of Zernike moments for image analysis. IEEE transactions on pattern analysis and machine intelligence, 20(12), 1358-1364.

[60] Khotanzad, A., & Hong, Y. H. (1990). Invariant image recognition by Zernike moments. IEEE Transactions on pattern analysis and machine intelligence, 12(5), 489-497.

[61] Wang, C., Zhang, Z., Li, Q., & Zhou, X. (2019). An image copy-move forgery detection method based on SURF and PCET. IEEE Access, 7, 170032-170047.

[62] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra. "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol. 6, iss. 3, pp. 1099-1110, 2011.

[63] Hosny, K. M., Mortda, A. M., Fouda, M. M., & Lashin, N. A. (2022). An efficient CNN model to detect copy-move image forgery. IEEE Access, 10, 48622-48632.

[64] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, G. Serra. "Copy-Move Forgery Detection and Localization by Means of Robust Clustering with J-Linkage", Signal Processing: Image Communication, vol. 28, iss. 6, pp. 659-669, 2013.

[65] Faria Hossain, Asim Gul, Rameez Raja, Tasos Dagiuklas, Chathura Galkandage. (2022). Forgery Image Dataset. IEEE Dataport. https://dx.doi.org/10.21227/9dmj-yn86

[66] Dong, J., Wang, W., & Tan, T. (2013). CASIA Image Tampering Detection Evaluation Database. 2013 IEEE China Summit and International Conference on Signal and Information Processing, 422-426.

[67] Islam, M. M., Karmakar, G., Kamruzzaman, J., & Murshed, M. (2020). A robust forgery detection method for copy–move and splicing attacks in images. Electronics, 9(9), 1500.

[68] Ng, T. T., Hsu, J., & Chang, S. F. (2009). Columbia image splicing detection evaluation dataset. DVMM lab. Columbia Univ CalPhotos Digit Libr.

[69] Wen, B., Zhu, Y., Subramanian, R., Ng, T. T., Shen, X., & Winkler, S. (2016, September). COVERAGE—A novel database for copy-move forgery detection. In 2016 IEEE international conference on image processing (ICIP) (pp. 161-165). IEEE.

[70] Mahfoudi, G., Tajini, B., Retraint, F., Morain-Nicolier, F., Dugelay, J. L., & Marc, P. I. C. (2019, September). DEFACTO:

Image and face manipulation dataset. In 2019 27Th european signal processing conference (EUSIPCO) (pp. 1-5). IEEE.

[71] Zhao, K., Yuan, X., Xie, Z., Xiang, Y., Huang, G., & Feng, L. (2023). SPA-Net: A Deep Learning Approach Enhanced Using a Span-Partial Structure and Attention Mechanism for Image Copy-Move Forgery Detection. Sensors, 23(14), 6430. https://doi.org/10.3390/s23146430

[72] Zhang, Y., Zhu, G., Wang, X., Luo, X., Zhou, Y., Zhang, H., & Wu, L. (2022). CNN-Transformer Based Generative Adversarial Network for Copy-Move Source/Target Distinguishment. IEEE Transactions on Circuits and Systems for Video Technology.

[73] Guan, H., Delgado, A., Lee, Y., Yates, A. N., Zhou, D., Kheyrkhah, T., & Fiscus, J. (2021). User guide for nist media forensic challenge (mfc) datasets.