A Systematic Review of Techniques for Detecting Image Forgery

Krishna Kulkarni
dept. of CSE
R.N.S INSTITUTE OF TECHNOLOGY
BANGALORE, INDIA
1rn22cs069.krishnarkulkarni@rnsit.ac.in

Rashmi M
dept. of CSE
R.N.S INSTITUTE OF TECHNOLOGY
BANGALORE, INDIA
Rashmi.m@rnsit.ac.in

***Abstract*—Today, digital images play a crucial role in various domains such as banking, communication, and business. However, the widespread availability of manipulation software makes it easy to alter original images, raising concerns about the integrity of digital content. To address this issue, the field of image forensics has gained prominence. In recent years, the prevalence of image editing tools has led to the creation and dissemination of numerous fake and altered images. Consequently, various methods, particularly those based on Deep Learning (DL) techniques, have been proposed for image forgery detection. This paper conducts a survey of recent DL-based methods, focusing on copy-move and splicing attacks. The analysis includes discussions on key aspects, datasets, and performance comparisons. The growing use of digital photography and editing tools has challenged the trustworthiness of imagery. Composite images, created from different sources and under varying conditions, pose challenges in color matching. The paper also explores composite forgery detection methods in the context of digital image forensics. Overall, the research underscores the importance of developing effective techniques to safeguard the integrity of digital images in today's technologically advanced era.**

***Index Terms*—image forgery detection, copy-move, splicing, DeepFakes, image tampering, forgery detection methods, GAN, CASIA, image forensics, deep learning, forgery survey**

I. *INTRODUCTION*

The ubiquity of desktop computers, the worldwide spread of smart devices integrating high-quality cameras and image processing tools, along with a plethora of "apps," has empowered ordinary individuals to collect, store, and process an unprecedented volume of digital visual data. These devices, almost constantly connected to each other and remote data servers through the Internet, have transformed the scale of data handling from previously unthinkable to commonplace. As a consequence, the almost instantaneous spreading of user-generated images and videos is enabled by a variety of digital technologies, including effective compression methods, fast networks, and user-friendly applications. Everyday facts are extensively documented through smartphones, even by professionals. Web platforms like social networks (e.g., Instagram) and forums (e.g., Reddit) play a crucial role in this massive sharing of visual content. Moreover, the availability of user-friendly, advanced image editing software, both commercial (e.g., Adobe Photoshop) and free and open-source (e.g., GIMP), along with smartphone apps for basic image manipulations, contributes to the widespread creation of visual content. However, these factors have also led to the proliferation of fake or forged images and videos, often for malevolent purposes such as political or commercial manipulation. Major social network platforms are grappling with the challenge of filtering manipulated data to prevent the viral spread of fake content, especially targeting vulnerable users. Legal issues are arising concerning responsibility for the potential damaging consequences of fake content dissemination. Human susceptibility to being fooled by forgeries, compounded by the change blindness cognitive effect, underscores the need for carefully designed digital techniques. While semantic alterations can be applied to various digital media content, this paper focuses on methods and algorithms specifically designed for detecting forgery in still images, the most common case. In this context, the broader problem of determining whether a given image has been altered to modify its semantics is referred to as image authentication or image integrity verification. When the emphasis is on establishing whether a given image has undergone a semantic alteration or forgery, it is often referred to as image forgery detection in the literature. The objective of this paper is to provide a survey of selected forgery detection methods, with a particular focus on deep learning (DL) techniques that have emerged prominently. Before embarking on our examination of forgery detection methods, this Section sets the stage for why we believe this timely and necessary comprehensive, performance-driven survey, describing the most recent DL methods, is essential. We kick off by offering a broad overview of the considered application, primarily to establish some key definitions. Following that, we offer a succinct summary of the most commonly encountered types of forgery. Lastly, we outline the organization of the rest of the paper while also delving into the contributions of our current analysis.

II. *USE OF IMAGE FORGERY DETECTION*

Forgery detection serves essential roles across diverse fields by safeguarding the integrity of documents and artifacts. In the realm of official documentation, it plays a critical role in verifying the authenticity of passports, driver's licenses, and financial instruments like checks. Moreover, forgery detection is pivotal in the art world, ensuring the legitimacy of valuable artworks and preventing the circulation of counterfeit pieces.

In the digital age, its significance extends to cybersecurity, where it is crucial for validating digital signatures, preserving the integrity of electronic documents, and preventing online fraud.

The legal landscape heavily relies on forgery detection to maintain the credibility of contracts, wills, and other legal documents. This is vital for upholding the accuracy and reliability of legal records. Forensic investigations benefit from forgery detection techniques, particularly in analyzing handwriting, signatures, and physical evidence, contributing to the resolution of criminal cases and the delivery of justice. Educational institutions and employers utilize forgery detection to verify academic credentials, protecting against misrepresentation and ensuring that qualifications are accurately represented.

Furthermore, forgery detection plays a pivotal role in brand protection, particularly in industries where brand reputation is paramount, such as pharmaceuticals, luxury goods, and electronics. It helps in preventing the circulation of counterfeit products that can tarnish a brand's image. Finally, across various sectors, forgery detection is integral to identity verification, preventing identity theft and ensuring that services are provided to legitimate individuals. Historical document authentication is another critical application, with forgery detection techniques being employed to verify the authenticity of historical documents, manuscripts, and artifacts, thereby preserving the accuracy of historical records.

A. *FIELD OF STUDY*

1. Computer Vision: - Utilizes algorithms for feature extraction, image segmentation, and pattern recognition to identify inconsistencies and anomalies in images.

2. Digital Forensics: - Investigates digital artifacts using specialized tools to detect alterations in images and establish the authenticity of digital evidence.

3. Signal Processing: - Applies methods like Fourier analysis and wavelet transforms to analyze digital signals within images, identifying irregularities that may indicate forgery.

4. Cryptography: - Embeds digital signatures and watermarks in images using cryptographic techniques to verify authenticity and detect unauthorized modifications.

5. Machine Learning and Deep Learning: - Employs these approaches to develop models capable of learning and recognizing patterns associated with image manipulation for more accurate and automated detection.

6. Pattern Recognition: - Identifies patterns and structures within data to recognize consistent patterns in authentic images and deviations in manipulated ones.

7. Image Processing: - Utilizes methods for analyzing and manipulating images, helping identify inconsistencies, artifacts, and alterations introduced during manipulation.

8. Biometrics: - Incorporates facial recognition and fingerprint analysis to enhance the verification of the identity and authenticity of individuals depicted in images.

9. Information Security: - Applies principles such as authentication mechanisms, encryption, and secure storage to safeguard digital images from unauthorized access and tampering.

10. Statistics and Probability: - Uses statistical methods to analyze the properties of images, with anomalies in distributions or correlations indicating potential forgery. Probability models inform decision-making in forgery detection systems.

III. *IMAGE FORGERY TYPES*

1) **Copy Move:** The copy-move forgery involves copying one or more regions of an image and pasting them into different locations within the same image. Typically employed to conceal information or duplicate objects/people, this form of forgery significantly distorts the semantic content of the target image. Figure 1a illustrates an example of a copy-move forgery, showcasing the insertion of the right building tower as a copy of the left one.

2) **Splicing:** The splicing forgery shares similarities with the copy-move technique, with the key distinction being that the pasted regions or objects are cut from one or more other images. This method is often employed to either conceal specific content or to depict a fabricated scenario. Illustrated in Fig. 1b is an example of a splicing forgery, where an image portrays two famous individuals together. However, upon closer inspection, it becomes evident that the picture is a composite of two different images.

3) **Inpainting:** This type of attack involves filling a region or a "hole" in an image with plausible content, a process known as inpainting. While inpainting is commonly used to restore damaged patches in images, it can also be exploited by potential attackers as a malicious means to conceal information or eliminate a visible watermark. The filled region may be copied from another part of the same image or synthesized using a specific algorithm, such as a Generative Adversarial Network (GAN). An intriguing example of inpainting is the reconstruction of deleted parts of faces, like the eyes or the mouth. Significant advancements in this area have been achieved by **[1]** (as illustrated in Fig. 1c).

4) **DeepFakes:** DeepFakes refer to the use of deep learning techniques, particularly deep neural networks, to create or manipulate content, usually involving images or videos. The term "deepfake" is a combination of "deep learning" and "fake." Deep learning models, especially Generative Adversarial Networks (GANs) and other advanced neural network architectures, are employed to generate highly realistic fake content, often indistinguishable from authentic material. **[2]**

The primary application of deepfakes involves manipulating videos or images to make it appear as though individuals are saying or doing things they never did. This technology can be used for various purposes, ranging from harmless entertainment, like creating realistic face swaps in movies, to more malicious activities, such as spreading misinformation or creating forged videos for political or social manipulation.

5) **CGI Generated Images/Videos:** Computer-Generated Imagery (CGI) refers to the use of computer graphics to create images, videos, or animations. CGI-generated content is produced entirely through computer software, without the need for physical objects or scenes. This technology has become a fundamental part of various industries, including film, video

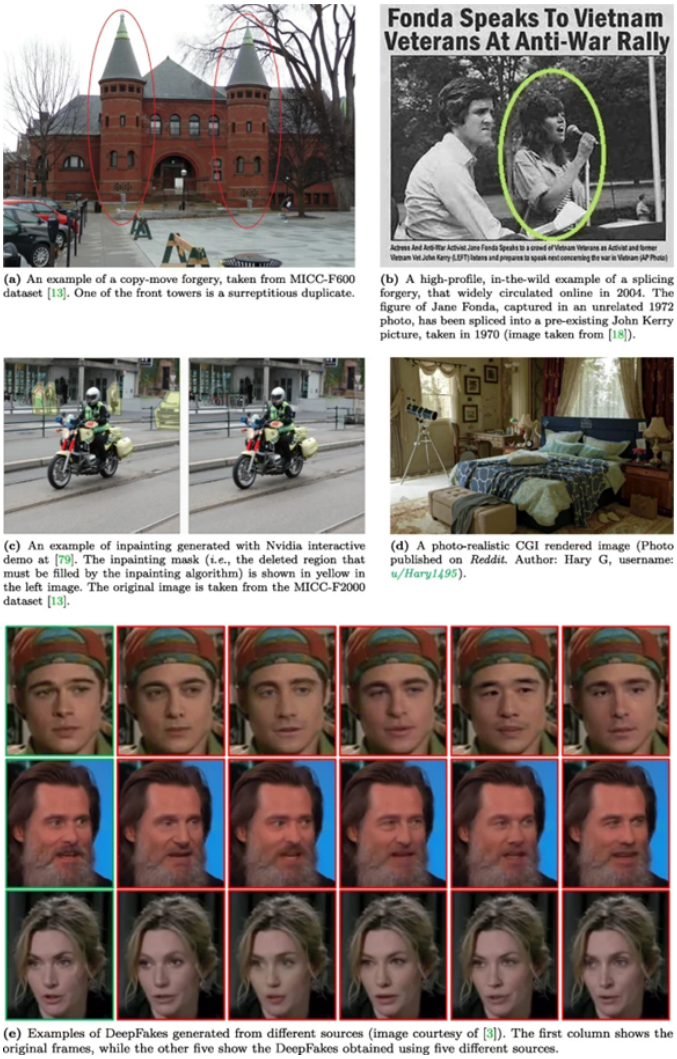
games, advertising, virtual reality, and more. In film and television, CGI is extensively used to create realistic visual effects, such as fantastical creatures, simulated environments, or complex scenes that would be challenging or impractical to film in real life. Video games heavily rely on CGI to render immersive and interactive virtual worlds. Additionally, CGI is employed in architectural visualization, medical simulations, and other fields for creating realistic visualizations. When it comes to CGI-generated images or videos, the distinguishing factor is that the entire content is created by computer algorithms. This is in contrast to DeepFakes, where AI technologies manipulate existing content, often involving real people. CGI allows for the creation of entirely fictional scenes, characters, or environments, and it is typically used for creative and artistic purposes in the entertainment and design industries. However, the realistic nature of CGI also raises ethical considerations, such as the potential for creating lifelike representations that could be misleading or misused. As technology continues to advance, there will likely be ongoing discussions about the responsible use of CGI and its potential impact on various aspects of society.

6) **GAN-based face synthesization:** It consists of the creation of a realistic face of a completely non-existing person, employing the previously cited GAN networks. This is done by feeding the trained model with a vector of random sampled noise, which is converted by the model to a realistic face (theoretically) different from any existing one. Again, as for the previously discussed CGI generated content, the fake image is synthesized anew instead of being copied from another source. **[3]**

IV. *METHODOLOGY*

We now briefly discuss some of the "conventional" passive image forgery detection approaches that have been proposed since the early 2000s. Conventional passive methods leverage techniques from the fields of signal processing, statistics, physics, and geometry, and are usually also referred to as "classic" or "traditional" approaches. In fact, they come from the pre-DL era that we are currently in and, as such, they require little or no data to perform an eventual training phase. Those that still require data for training are typically based on traditional machine learning techniques, such as clustering, support vector machines (SVM), linear/logistic regression, random forests, and so on. Here, we still consider those as belonging to the classic methods, because they rely on models that have a relatively small number of parameters, and therefore do not require a great amount of data for training.

1) **Pixel-based:** These methods rely on the fact that certain manipulations introduce anomalies that can affect the statistical content of the image at the pixels level. Some of these anomalies can be detected in the spatial domain, while others in the frequency domain or in a combination of both. The authors of **[4]** have proposed a method based on the Discrete Cosine Transform (DCT). In particular, they divided the image into overlapping blocks and applied a DCT on each block. The DCT coefficients were used as feature vectors that describe each block. Duplicated regions then were detected by lexicographically ordering the DCT block coefficients and grouping the most similar ones.



(a) An example of a copy-move forgery, taken from MICC-F600 dataset [13]. One of the front towers is a surreptitious duplicate.

(b) A high-profile, in-the-wild example of a splicing forgery, that widely circulated online in 2004. The figure of Jane Fonda, captured in an unrelated 1972 photo, has been spliced into a pre-existing John Kerry picture, taken in 1970 (image taken from [18]).

(c) An example of inpainting generated with Nvidia interactive demo at [79]. The inpainting mask (*i.e.*, the deleted region that must be filled by the inpainting algorithm) is shown in yellow in the left image. The original image is taken from the MICC-F2000 dataset [13].

(d) A photo-realistic CGI rendered image (Photo published on *Reddit*. Author: Hary G, username: *u/Hary1495*).

(e) Examples of DeepFakes generated from different sources (image courtesy of [3]). The first column shows the original frames, while the other five show the DeepFakes obtained using five different sources.

Fig. 1. Depicting the types of image forgery

2) **Format-based:** Usually, images captured by a digital camera are encoded in JPEG format. This means that the image is divided into 8×8 pixel blocks, which are then DCT transformed and quantized. As a consequence, specific artefacts are generated at the border of neighbouring blocks. The authors of **[5]** observed that image manipulations like copy-move or splicing result in alterations in the JPEG artefact pattern, and proposed a method in which they used a sample region (which is supposed authentic) of the target image to estimate the JPEG quantization table. Then, they divided the image into blocks, and a "blocking artefact" measure is computed for each block. A block is considered tampered if the score given by this measure is sufficiently distant from the average value on the whole image.

3) **Camera-based:** The basic idea exploited by these methods is that every digital camera leaves a particular "footprint"

or "signature" on each image they generate. This fact can also be useful to tie an image to a specific capturing device. In **[6]**, the authors used a set of images taken by a known camera to estimate the parameters of the already mentioned PRNU, which is a camera specific multiplicative term that models the result of in-camera processing operations. These PRNU parameters are also extracted from the target image, which is supposed to be taken with the same camera, and compared with the previously estimated ones. The idea is that, if a splicing operation from a different camera type has been made, this results in a discrepancy between the estimated parameters.

4) **Light-based:** Typically, when an attacker performs a copy-move or splicing attack, it is hard to ensure that the lighting conditions of the forged region are consistent with that of the surrounding image. Compensating for this effect can be hard even using professional software like Adobe Photoshop. Therefore, the basic idea of lighting (or physics) based techniques is to build a global lighting model from the target image, and then to find local inconsistencies with the model as evidence of forgery.

5) **Geometry-based:** Geometry-based methods rely on the fact that a copy-move or a splicing attack usually results in some anomalies in the geometric properties of the 3D scene from which the image is obtained. The authors of **[7]** proposed a method to estimate the so-called principal point through the analysis of known planar objects, and observed that this is usually near the center of the image. They also showed that a translation of an object in the image plane results in a shift of the principal point, and thus this fact can be used as evidence of forgery.

V. *DATASET DESCRIPTION*

NAME OF DATASET	COLOR IMAGES	FORGED+COLOURED	YEAR OF FOUNDATION	IMAGE TYPE	RESOLUTION
CASIA v1.0 (CASIA1) [8]:	1725	975+750	2004	JPG	386X256
CASIA v2.0 (CASIA2) [8]	12614	5123+7491	2013	JPG TIFF BMP	Between 240X160 AND 900X600
DVMM [9]	1845	912+933(B/W)	1994	BMP	128X128
MICC-F220[10]	220	110+110	2012	JPEG	Between 722X480 AND 800X600
MICC-F600[10]	620	160+440	2012	JPEG PNG	Between 800X532 AND 3888X2592
MICC-F2000 [10]	2000	700+1300	2012	JPEG	2048X1536
SATs-130 [11]	130	120+10	NA	JPEG	Between 1028X683 TO 3264X2448
CMFD [12]	48	NA	2010	JPEG PNG	NA
CoMoFoD [13]	9600	4800+4800	NA	JPEG	512x512, and 3000x2000
Korus [14,15]	440	220+220	NA	TIFF	1920X1080

Fig. 2. DATASET for Image forgery detection

It is apparent from the above data, CASIA v2.0 (CASIA2) is the latest Dataset available for detection of image forgery, but Korus provides the best image resolution.

VI. *LITERATURE SURVEY*

In this section, we proceed to compare the previously described detection of the two forgery methods (copy-move and splicing) from a performance perspective.

1) **Copy-Move Forgery Detection:** We start the present analysis by first comparing methods **[16,17]**, and **[18]**, as they have been all tested on the MICC-F220 dataset. The first method achieved a slightly better accuracy and a considerably better FPR than the other two, along with a considerably better accuracy. In addition, **[17]** has been shown to achieve perfect results on MICC-F600 and almost perfect ones on MICC-F2000, which are more significant evaluation datasets. However, it should be considered that **[17]** only gives as output a global decision on the authenticity of the image, while **[16]** also provides the location of the forgery. Regarding the forgery localization property, it is worth noting that the techniques presented in **[19]** and **[20]** allow not only to detect the copy-moved regions, but also to distinguish them from the source patches used to perform the attack. This property is useful in real forensic scenarios, in which it is important to understand the semantic aspects of an image manipulation. A further interesting feature of **[19]** is the adoption of a GAN network to generate increasingly hard-to-detect forgeries that are used to train the discriminator network. This is an original approach to address the problem of data-scarcity that plagues many different existing standard datasets. However, from a performance point of view, it is hard to compare this method to the other ones, as it was evaluated on a custom dataset and not on one of the benchmark datasets. This is not the case for **[20]**, which was evaluated on CASIA2.

2) **Splicing Detection:** These techniques fit the best in a general application context, in which the type of attack is not known a priori, so it is better to cover as many attacks as possible. In particular, we consider the methods tested on CASIA2, which is likely the most significant dataset for copy-move and splicing detection evaluation, both for its sheer size and for the various applied post-processing operations. Among the methods that we discussed, the one presented in **[21]** obtained the best overall accuracy. It also gives as output the localization of the forged areas, which as we mentioned is of course relevant in many application contexts. Looking at its forgery detection pipeline, it features both a pre-processing stage, in this case based on YCbCr space conversion and DCT compression, as well as a post-processing phase that through further features extraction allows to perform localization. Therefore, the good performance that it achieved indicates that an exclusively end-to-end deep learning model, without any pre-processing or post-processing, could be indeed a sub-optimal choice for the task of forgery detection. On the same note, another comment can be made about the method in [22]. Even if its performance is worse than the others in terms of accuracy, the proposed approach is quite interesting because it involves a "shallow" deep learning model. This allows reducing not only the number of network parameters (and consequently the training time), but also the risk of over-fitting. This idea is in contrast to the common trend in computer vision to use ever deeper networks to achieve high accuracy on specific datasets, that usually cannot be achieved on slightly different ones, which is a clear indicator of over-fitting issues. A remark should be made on the approach

proposed in **[23]**. This method has a wide applicability even outside the field of forgery detection. In fact, the possibility to extract the noise camera pattern and suppress the high-level scene content of a target image is of great utility in other forensic scenarios as well as for sophisticated camera-specific denoising applications. It is important to also note that the authors evaluated the performance of their algorithm on different datasets, which contain a wide set of forgery attacks such as copy-move, splicing, inpainting, GAN-synthesized content, face-swap, etc., thus proving its wide applicability and robustness. Still, it would have been interesting to have the detection results on other more classic benchmark data, such as the CASIA2, thus allowing a better comparison with other existing methods.

VII. *CONCLUSION*

In this study, our focus is on surveying recent AI-powered methods, specifically those developed from 2016 onward, for copy-move and splicing detection. While various reviews have been published on forgery detection, most have emphasized traditional approaches, such as key-points/blocks, segmentation, or physical properties. In contrast, we concentrate on deep learning-based methods due to their demonstrated effectiveness in terms of performance and generalization capabilities. We categorize our performance analysis into three sections: copy-move only detection, both copy-move and splicing detection, and DeepFake detection. Notably, deep learning methods, like the one presented in **[17]**, showcase almost perfect accuracy in copy-move detection on standard benchmark datasets. For both copy-move and splicing detection, method **[21]** on the CASIA2 dataset demonstrates the best accuracy, offering localization of the forged regions. DeepFake detection, however, lacks a consistently superior approach, with EXception Net-based models in **[24]** showing better performance on selected benchmark datasets. The survey highlights a lack of a clear trend in deep learning-based forgery detection methods along with DeepFakes, suggesting that the field is still exploring various possibilities without a definitive winning strategy. Notably, techniques combining deep learning with pre-processing and post-processing exhibit the best accuracy in splicing and copy-move detection. This prompts the suggestion that future research should explore algorithms integrating deep learning approaches with traditional techniques from the broader field of signal processing. The study raises concerns about the evaluation of deep learning methods, noting that custom datasets or the merging of different datasets may hinder comparisons with other methods. The authors advocate for the creation of a standardized testing approach, using a custom dataset for training and established benchmark datasets for testing, to facilitate fair comparisons between different forgery detection methods. Addressing the issue of dataset realism, the paper proposes automating the creation of custom datasets with realistic forgeries using techniques such as GAN networks or encoder-decoder models. Additionally, it emphasizes the need for datasets containing more realistic, "in-the-wild" forgeries, reflecting the complex and potentially malicious attacks prevalent on social media. The study concludes with a philosophical observation, acknowledging the dynamic nature of forgery attacks. It emphasizes the importance of continuous research to develop forgery detection methods that can adapt to evolving attacker strategies. The authors propose a proactive strategy, incorporating new forgery techniques during algorithm development to better understand their flaws and create potential countermeasures.

VIII. *REFERENCES*

1) Liu G, Reda F, Shih K, Wang TC, Tao A, Catanzaro B (2018) Image inpainting for irregular holes using partial convolutions

2) Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial networks. Adv Neural Inf Process Syst 3

3) Karras T, Laine S, Aila T (2019) A style-based generator architecture for generative adversarial networks, pp 4396–4405. https://doi.org/10.1109/CVPR.2019.00453

4) Fridrich J, Soukal D, Lukás J (2003) Detection of copy move forgery in digital images. Proc. Digital Forensic Research Workshop

5) Lukás J, Fridrich J (2003) Estimation of primary quantization matrix in double compressed jpeg images. Proc Digital Forensic Research Workshop. https://doi.org/10.1117/12.759155

6) Fridrich J, Chen M, Goljan M (2007) Imaging sensor noise as digital x-ray for revealing forgeries. In: Proceedings of the 9th international workshop on information hiding, Sant Malo, France, pp 342–358. https://doi.org/10.1007/978-3-540-77370-2-23

7) Johnson MK, Farid H (2007) Detecting photographic composites of people. In: Proceedings of the 6th international workshop on digital watermarking, Guangzhou. https://doi.org/10.1007/978-3-540-92238-4-3

8) Dong J, Wang W, Tan T (2013) Casia image tampering detection evaluation database. In: 2013 IEEE China summit and international conference on signal and information processing, pp 422–426. https://doi.org/10.1109/ChinaSIP.2013.6625374

9) Various. Columbia image splicing detection evaluation dataset - list of photographers, 2004. https://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm.

10) Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2011) A SIFT-based forensic method

for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur:1099–1110. https://doi.org/10.1109/TIFS.2011.2129512

11) Birajdar GK, Mankar VH (2013) Digital image forgery detection using passive techniques: a survey. Digit Investig 10(3):226–245. https://doi.org/10.1016/j.diin.2013.04.007

12) Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensics Secur 7(6):1841–1854. https://doi.org/10.1109/TIFS.2012.2218597

13) Tralic D, Zupancic I, Grgic S, Grgic M (2013) Comofod — new database for copy-move forgery detection. In: Proceedings ELMAR-2013, pp 49–54

14) Korus P, Huang J (2016) Evaluation of random field models in multi-modal unsupervised tampering localization. In: 2016 IEEE international workshop on information forensics and security (WIFS), pp 1–6. https://doi.org/10.1109/WIFS.2016.7823898

15) Korus P, Huang J (2017) Multi-scale analysis strategies in prnu-based tampering localization. IEEE Trans Inf Forensic Secur

16) Agarwal R, Verma O (2020) An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimed Tools Appl 79. https://doi.org/10.1007/s11042-019-08495-z

17) Elaskily M, Elnemr H, Sedik A, Dessouky M, El Banby G, Elaskily O, Khalaf AAM, Aslan H, Faragallah O, El-Samie FA (2020) A novel deep learning framework for copy-move forgery detection in images. Multimed Tools Appl 79. https://doi.org/10.1007/s11042-020-08751-7

18) Doegar A, Dutta M, Gaurav K (2019) Cnn based image forgery detection using pre-trained alexnet model. Electronic

19) Abdalla Y, Iqbal T, Shehata M (2019) Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network. Information 10(09):286. https://doi.org/10.3390/info10090286

20) Wu Y, Abd-Almageed W, Natarajan P (2018) Busternet: detecting copy-move image forgery with source/target localization. In: Proceedings of the European conference on computer vision (ECCV), pp 168–184. https://doi.org/10.1007/978-3-030-01231-1-11

21) Rajini NH (2019) Image forgery identification using convolution neural network. Int J Recent Technol Eng 8

22) Majumder MTH, Alim Al Islam ABM (2018) A tale of a deep learning approach to image forgery detection. In: 2018 5th international conference on networking, systems and security (NSysS), pp 1–9. https://doi.org/10.1109/NSysS.2018.8631389

23) Cozzolino D, Verdoliva L (2020) Noiseprint: a cnn-based camera model fingerprint. IEEE Trans Inf Forensics Secur 15:144–159. https://doi.org/10.1109/TIFS.2019.2916364

24) Rössler A, Cozzolino D, Verdoliva L, Riess C, Thies J, Nießner M (2019) Faceforensics++: learning to detect manipulated facial images