Journal of Education for Pure Science- University of Thi-Qar
Vol.12, No2 (December, 2022)
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

DOI: http://doi.org/10.32792/utq.jceps.12.02.17

Detection of Image Tempering: Conventional and Deep Learning-based Techniques

Hassin Da. Khallaf [1] **Abbas Hanon Alasadi**[1,2]

[1]College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq.
[2]IEEE and ACIT member

Received 16/07/2019 Accepted 27/12/2020 Published 01/12/2022

Abstract:
In light of the cumulative use of digital images in a wide range of apps, as well as the accessibility of image manipulation software, detecting image alteration has become a difficult task. The copy-move technique is the most commonly used sort of picture counterfeiting. A portion of an image is duplicated and manipulated in various ways. Handcrafted qualities are commonly used in the identification of picture forgery and counterfeiting. It has always been a difficulty with earlier photo reproduction detection systems that they would rather only detect a specific type of tampering if they are aware of specific image features. Deep learning is currently being used to detect image alteration, which is a breakthrough. These strategies were even more efficient than prior methods since they were able to extract complex images from them. The purpose of this work is to teach you about deep learning-based picture forgery detection methods, why they function, and how they can be improved upon. In addition, you will learn about publicly available image forgery datasets.
Keywords: Image Forgery; Copy-move detection; Deep CNN

1. Introduction

Nowadays, all of us have easy access to technologies for processing, distributing, and storing the information. The development of photo editing software contributes to digital image fabrication. Artistic renderings are rapidly eroding multimedia confidence [1].

The image is impressive, and it can be authentic for its consequences to be reasonable. Digital records are employed in everyday life, marketing, and regulatory investigations. As a result, the authenticity of the digital historic image is severely compromised by image editing applications like Editing software and Adobe that do not distinguish between typical journalistic photos. The source and counterfeit photos are visually identical. To sustain the image's value, robust technologies capable of identifying forgeries in digital photographs are required [2]. [3].

The digital image is important in many demonstrations, including corporate forms, scientific works, medical records, media, and court signs. So, there is a potential to build methods to certify digital photos. Digital Image Forensic can help with this issue. One of the main goals of this discipline is to develop the detection system for faked photographs. In recent years, many forgery detection techniques have been proved.

Video and photos seem to be the most commonly targeted digitally falsified items. Photographic honesty is vital in criminal investigation, unlawful analysis, surveillance equipment, security agencies, medical imaging, and journalistic going to report [4].

2. Forgery Image

According to the Dictionary of Oxford [5], the word "tamper" denotes to "interfere with anything to inflict disrupt or make unlawful modifications to it." Fraudulent detecting is the identification of images that have been altered for malicious intentions on a global scale. When the perceptual information and the contextual meaning of an image are altered, this is referred to as manipulating with the photo and is considered illegal. Images were manipulated historically as a political propaganda tool to advance a certain political agenda. Tampering emerged as a result of the greater reliance on visual images as the primary means of communicating core ideas [6].

The majority of the time, forgers delete information from an image without utilizing the content from some other image; on the other hand, forgers who wish to add information must do so by utilizing the material through one single or multiple images, see Figure (1).

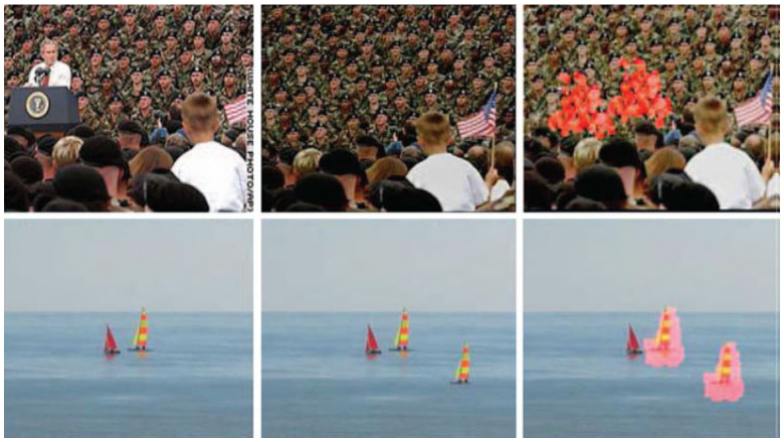

Figure (1): (above) Object removal , (below) its duplication [7].

3. Forgery Image Classification

Generally speaking, image fabrication methods may be split into two primary categories: active methods and passive methods [8], as seen in Figure (2).

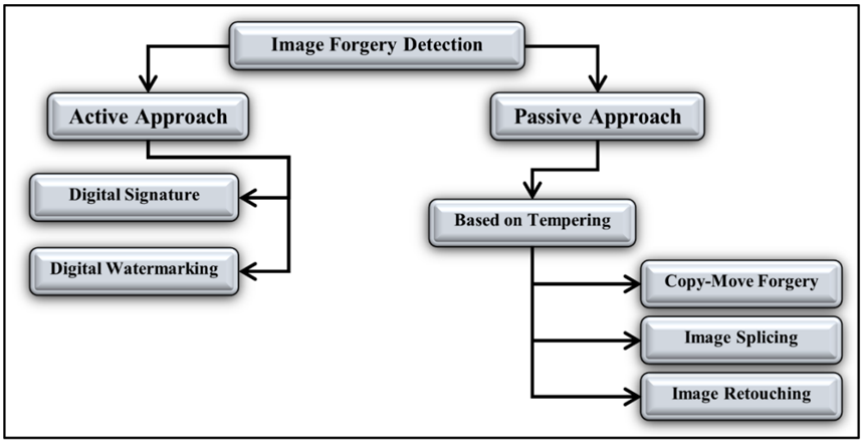

Figure (2): Forgery Image Approaches Classification.

For a person without professional or specialized knowledge, these kinds of modifications can be difficult to find. Forensic studies have focused their labors on the development of knowledges that can prove the validity of an image. Many different ways to determining the validity of an image and determining its quality have been offered [9].

3.1 Active Method:

The active technique includes the detection of digital manipulation by including detailed information such as the user's name, the date, and a signature. These methods necessitate the use of hardware instrumentation in order to get the right completeness of the digital image.

There are numerous advantages to active approaches, including the fact that they reduce the computational cost. In addition, there is simple info on the input images available on the website. However, the active approaches have the disadvantage of being non-automatic due to the requirement for prior knowledge of the original image as well as the requirement for user intercession or the use of a specific camera with specialized equipment. The digital image that is available on the internet does not have a fingerprints, signatures, or steganography [10] attached to it.

In an active approach, the substantiation code is injected or appended to the original image, ensuring that the image is protected. If an identification criterion is in place, the confirmation email is used to validate the authenticity of the image being displayed. Digital forgery can be detected via increasingly internet actual work and digital sign approaches [11].

3.1.1 Digital Signature

A digital signature is formed by encrypting various original picture elements with a public key and utilizing that key to construct a digital signature. In this case, the signature remains permanently connected to the input images. When authentication is required, the signature is decoded with the help of the private key. This is because supplementary material is being communicated with the input images in the case of electronic signature, which increases the size of the image.

3.1.2 Digital Watermarking

When utilizing digital watermarking, the authentication code is hidden within the pristine image, suggesting, which it incorporates the watermark within the input images by means of several image processing techniques accordingly that the human eye is unable to identify it. [12].

3.2 Passive Method:

When it comes to picture forgery detection, passive approaches represent the new frontier of investigation. This is an active field where outstanding work has been done, and this approach makes use of the image summary statistics and the image as a question to determine the authenticity of the image in question [13]. Despite this, it does not make use of the contained data to verify forgeries. Almost no apparent indicators are left behind by the digital forging process, which indicates that the document is not genuine. As a result of this, the picture framework is harmed, and alternative forms are produced, which are incompatible with the original image. Each classification of the passive approach can be divided further. Image copy-move fabrication, retouching fabrication, and picture splicing falsification are the three types of image fraud that are classified according to the hardening process in the image [14].

3.2.1 Copymove Image:

A special case of image splitting is copy-move fabrication, which is the practice of forging digital images by moving them around. Because the manipulation occurs together within single image, with no need to use numerous photos to do this. This means that portion of a picture is replicated and then put in the desired position within a different image [15]. The concept behind such manipulating is to expand or cover a explicit entity in an image, see Figure (3).

input Image **Copymove Image**

Figure (3): Copymove Forgery Examples.

3.2.2 Image Splicing:

Image splicing is the process of combining portions of two or more photos to create a single new image [16]. This operation is essential in single image montaging and, as a result, serves as a method for the generation of image forgeries. Figure (4) is an example of image splicing in action. The image splicing approach, as contrasting to image retouching, takes the possible to modify the meaningful image of digital photos more aggressively.

1st Image **2nd Image** **Fake Image**

Figure (4): Samples of Image_splicing.

3.2.3 Image Retouching:

Image Retouching has a less dramatic effect on the photographs. It merely enhances a few of the image's qualities, nothing more. The image is processed in order to either lessen or improve specific visual characteristics. It is a common sort of image transition, and it is used extensively in commercials to great effect. The cloning of an image component is also quite common in the field of picture editing. Due to the fact that there has been no substantial alteration in the various regions of the picture [17], detection is extremely difficult. Retouching could be used to repair and recreate damaged images [18], as illustrated in Figure (5).

input image

Retouched Image

Figure (5): Example of Retouching image.

4. Image Forgery Dataset:

In demonstrate the effectiveness of a proposed system in the detection of image tampering, it is necessary to construct a dataset that contains both real and tampered photos. The images are typically tagged with human familiarity to indicate that they represent the ground truth. Photos in a dataset are categorized with binary variables, 0 for originals and 1 for copy - move forgery, in order to differentiate among the two forms of images. Images necessity to be labeled extreme care with a black-and-white mask which illustrates where its pixel that have been modified are [19] [20] in order to avoid confusion.

It is never easy to develop an optimal wide range of sources of hundreds of images that takes into account all forms of fraud, all varieties of image files, and entirely kinds of imaging circumstances. Numerous early publications only estimated their suggested algorithms on a small number of photos or on standard datasets that were developed in-house by the researchers. Communal image datasets are usually appreciated because they allow academics to initiate their project without being to spend much time get-together private information; and because they agree scientists to compare evolutionary algorithms on another test, which is convenient for beginners. Table (1) lists a number of publicly available image forgeries datasets that are discussed in this section.

Table (1): Datasets of the Common tampered image [22].

Dataset	Release Year	Tampering Types	#Authentic/ #Tampered	Image Size	Format	Mask	Post-processing	Color
Columbia gray	2004	Cut-paste	933/912	128 ×128	BMP	No	No	No
Columbia color	2006	Cut-paste	183/180	757 ×568	TIFF	Yes	No	Yes
CASIA v1.0	2009	Cut-paste	800/921	384 ×256	JPEG	No	No	Yes
CASIA v2.0	2009	Cut-paste\ Copy-move	7491/5123	900 ×600	TIFF	No	Yes	Yes
MICC-F220	2011	Copy-move	110/110	722 ×480	JPEG	No	No	Yes
MICC-F2000	2011	Copy-move	1300/700	2048 ×1536	JPEG	No	No	Yes
IMD	2012	Copy-move	48/48	3000 ×2300	JPEG	Yes	Optional	Yes
MICC-F600	2013	Copy-move	440/160	800 ×533	JPEG	Yes	Yes	Yes
CoMoFoD	2013	Copy-move	5200/5200	512 ×512	JPEG	Yes	Yes	Yes
Wild Web	2015	Cut-paste Copy-move	0/10646	Various	Various	Yes	Yes	Yes
COVERAGE	2016	Copy-move	100/100	Various	TIFF	Yes	No	Yes

5. Forgery Image Methods:

In the field of image forgery detection, there are a number of strategies that have been developed. They may be divided into two categories: those that are considered conventional techniques, and those that are classified as deep neural networks.

5.1 Conventional Techniques:

Image forgery Detection has gotten a lot of attention lately. A number of different approaches have been developed to develop more efficient ways of serving certain apps. The foregoing is a comprehensive record of the most important works of literature.

According to Lee et al. [23], the photos were divided into imbrication blocks, and the histogram-oriented gradient (HOG) was applied to each block. While this method can detect many instances of copy-move forging, it doesn't work well when it's applied to a wide range of rotation and scale.

According to Parihar et al. [24], they proposed a strategy for detecting copy-move forgeries by obtaining selected features utilizing Scale Invariant Feature Transform (SIFT) method and comparing them to one another.

There must be a way to put the feature vectors together before the matching process can start.

A blur-invariant copymove forgery recognition method with enhanced detection accuracy was proposed by Dixit and Mishra [25], who presented an identification technique. They used the stationary wavelet transform and singular value decomposition to achieve greater detection accuracy (SWT SVD).

There are several texture descriptors taken into consideration, including the Local Binary Pattern_LBP, Local Phase Quantization_LPQ, Binary Statistical Image Features_BSIF, and Binary Gabor Pattern [26]. With the Steerable Pyramid Transform_SPT, which is used for picture decomposition, tiny texture variations can be captured at numerous sizes and orientations. Using Random Forest, we can classify this lightweight, multi-texture representation. The Random Forest classifier is used to classify it.

There are two ways to tell if an image is a copy-move forgery [27]: A-KAZE and speed-up robust features_SURF. Both are based on the KAZE algorithm.

A new approach for identifying and localizing copy-move picture counterfeiting was demonstrated by Toqeer Mahmood et al. [28], which was based on the stationary wavelet transform SWT and the discrete cosine transformation. The SWT was chosen because of its translation invariance and ability to be found in both the spectral and spatial domains.

A strategy for detecting picture counterfeiting proposed by Hashmi and colleagues [29] combined DWT and SIFT in order to take advantage of both approaches. The dimension reduction property of the DWT is used to reduce processing time, while the SIFT algorithm is applied to improve precision. Nevertheless, by replacing the DWT with the Dyadic Wavelet Transform_DyWT, which makes use of the shift-invariant, the standing method can be made more effective.

Anand et al. [30] advised a new technique for copymove template matching that uses DyWT and SIFT techniques. Due to the fact that the True Positive Rate can be enhanced by using this approach, it is more affordable than other available ways, and because the resilience of this approach can be observed in the case of geometric changes, it is superior to the other existing methods.

5.2 Deep Neural Networks:

The following are the most important deep neural network types in literature, each with a detailed description:

According to a paper by Wu et al. [31], the paper proposes a scheme named BusterNet, which is a final based on convolutional neural networks solution for identifying falsified copymove images through two terms locating the source and target , with two sections discovering the origin and goal.

Rao et al. [32] introduced a novel deep learning system known as a Generalized Approximate Reasoning Based Intelligence Control_GARIC, which is based on approximate reasoning. When it comes to data images, GARLIC is employed to detect counterfeit.

A Sobel filter was used in conjunction with an upgraded regional deep convolutional network filter developed by Wang et al. [33]. In order for the expected filters to categorize gradients that are equivalent to those of the real filter, the Sobel filter is utilized as an extra function. This includes copymove, which is one of two types of image manipulation that can be seen by the network as a whole.

Leekha and colleagues [34] developed an image forgery identification approach that may be used to detect both splitting and copy-move manipulations at the same time. At the beginning of the process, the original image was converted into the YCbCr color space. Following that, the block discrete cosine transformation and decorrelation of images are performed as part of the preprocessing stage, and the model is trained using both created and original images. Instead of this, the image is classified as a split form or copy-move by means of a deep convolutional neural network.

The authors [35] proposed a unique neural layer that trains image modification features by conquering visual content, which they called the Bayar neural layer. For this reason, rather than evaluating the image features, this layer looks at the local spatial correlations among pixels. Using this technology, it is possible to see many changes in a single image.

Chinese researchers, Zhang et al. [36], presented a two-step technique for distinguishing genuine from counterfeit photographs. Using a multilayer auto-encoder model, they first divided the image into patches, after which they learned the features associated with each patch. In order to acquire accurate results, the relevant information must be available to another fix in the next stage of development.

Salloum et al. [37] advocated the use of multi-task deep convolution networks to pinpoint image splicing. There was a skipped connection between the base network (FCN VGG-16) and the internet. Multi-task FCN (MFCN) has been shown to be better than single-task FCN (SFCN) in most cases. This is in order to SFCN gives inaccurate connectivity yield in a few conditions. MFCN is better than SFCN in most cases.

Amerini et al. [38] found a method for containing double JPEG compression using multi-domain deep neural networks, which they applied to images. A multi-domain CNN is composed of several layers, including a spatial CNN, a fourier transform CNN, and other layers. To train a spatial domain-based CNN, input regions of RGB color bands of n*n sizes are fed into the network. It is made up of two convolutional blocks and two fully linked layers that are linked together.

6. Performance Measurements :

The following four performance measures can be applied to estimate results that define forgery images to be positive and non-forgery images to be negative [39].

$$Accuracy = 100 \times \frac{TP+TN}{TP+FP+TN+FN} \quad \dots (1)$$

$$Precision = \frac{TP}{TP+FP} \quad \dots (2)$$

$$Recall = \frac{TP}{TP+FN} \quad \dots (3)$$

$$F1 = 2 \times \frac{TPPrecision \times Recall}{Recall+Precision} \quad \dots (4)$$

Where

- True Positive (TP) calculates the number of fabricated photos and organizes them as such.
- False Positive (FP) calculates the number of forgeries images and organizes them as genuine.
- True Negative (TN) counts the collection of images that are not fabricated and organizes them as such.
- False Negative (FN) calculates the number of images that are not forgeries and classifies them as falsified.
- The accuracy rate counts the number of discovered photos that are genuine forgeries.
- The recall rate is the likelihood that actual counterfeit photos will be discovered.
- The F1 score is a metric that combines precision and recall into a single value.
- Accuracy is expressed as a percentage of properly categorized photos and scopes ranging from 0 to 100.

7. Conclusion:

In spite of the fact that digital image fraud is a relatively new area of research, there is still space for improvement in detection methods. There are two major challenges that must be solved in order for the platform to perform well in research: performance and flexibility in contradiction of horrible actions. The major concern is the scheme should outperform current approaches in terms of the true-positive rate and the number of false alarms.

A final solution is found in the form of two techniques to tampering detection: (1) the traditional methodology and (2) Deep Learning. In order to identify tampering, previous approaches rely on handmade characteristics. According to the findings of the survey, standard approaches do not perform consistently over a wide range of tampering methods and environments. To the contrary, deep learning-based approaches are capable of automatically learning abstract and complicated traits that are necessary to identify tampered areas.

---

8. References:

[1] Deep Kaur, C., & Kanwal, N. (2019). An analysis of image forgery detection techniques. *Statistics, Optimization & Information Computing*, *7*(2), 486-500.

[2] Agarwal, R., Khudaniya, D., Gupta, A., & Grover, K. (2020, May). Image Forgery Detection and Deep Learning Techniques: A Review. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1096-1100). IEEE.

[3] Alasadi, A. H. H., & Jaffar, R. H. (2018). Fingerprint Verification System Based on Active Forgery Techniques. *International Journal of Computer Applications*, *975*, 8887.

[4] Doegar, A., Dutta, M., & Kumar, G. (2019). A review of passive image cloning detection approaches. In *Proceedings of 2nd International Conference on Communication, Computing and Networking* (pp. 469-478). Springer, Singapore.

[5] The Oxford dictionary online. http://oxforddictionaries.com/ Accessed 7 December 2021.

[6] Subramaniam, T., Jalab, H. A., Ibrahim, R. W., & Mohd Noor, N. F. (2019). Improved image splicing forgery detection by combining conformable focus measures and focus measure operators applied on obtained redundant discrete wavelet transform coefficients*: symmetry*, *11*(11), 1392.

[7] Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (Vol. 2, pp. 272-276). IEEE.

[8] Ahmad, M., & Khursheed, F. (2021). Digital Image Forgery Detection Approaches A Review. In *Applications of Artificial Intelligence in Engineering* (pp. 863-882). Springer, Singapore.

[9] Diallo, B., Urruty, T., Bourdon, P., & Fernandez-Maloigne, C. (2020). Robust forgery detection for compressed images using CNN supervision. *Forensic Science International: Reports*, *2*, 100112.

[10] Kaur, S. J., & Bhatla, N. (2020, November). Forgery Detection For High-Resolution Digital Images Using FCM And PBFOAAlgorithm. In *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 248-253). IEEE.

[11] Patel, H. A., & Shah, D. B. (2021). Semi-Fragile Blind Watermarking Mechanism for Color Image Authentication and Tampering. *ICTACT Journal on Image and Video Processing*, *11*(3), 2355-2359.

[12] Patel, H. A., & Shah, D. B. (2019). Digital image watermarking mechanism for image authentication, image forgery and self-recovery. *Int. J. Electron. Eng*, 140-143.

[13] Khudhair, Z. N., Mohamed, F., & Kadhim, K. A. (2021, April). A Review on Copy-Move Image Forgery Detection Techniques. In *Journal of Physics: Conference Series* (Vol. 1892, No. 1, p. 012010). IOP Publishing.

[14] Jaafar, R. H., Rasool, Z. H., & Alasadi, A. H. H. (2019, September). New copy-move forgery detection algorithm. In *2019 International Russian Automation Conference (RusAutoCon)* (pp. 1-5). IEEE.

[15] Bharti, C. N., & Tandel, P. (2016, March). A survey of image forgery detection techniques. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 877-881). IEEE.

[16] Thapaliya, A., Elambo Atonge, D., Mazzara, M., Chakraborty, S., Afanasyev, I., & Ahmad, M. (2019). Digital Image Forgery. In *6th International Young Scientists Conference on Information Technologies, Telecommunications and Control Systems (ITTCS 2019), Innopolis/Yekaterinburg, Russia, December 6, 2019.* (Vol. 2525).

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

[18] Saber, A. H., Khanl, M. A., & Mejbel, B. G. (2020). A survey on image forgery detection using different forensic approaches. *Advances in Science, Technology and Engineering Systems Journal*, *5*(3), 361-370.

[19] 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.

[20] alZahir, S., & Hammad, R. (2020). Image forgery detection using image similarity. *Multimedia Tools and Applications*, *79*(39), 28643-28659.

[21] Tralic, D., Zupancic, I., Grgic, S., & Grgic, M. (2013, September). CoMoFoD—New database for copy-move forgery detection. In *Proceedings ELMAR-2013* (pp. 49-54). IEEE.

[22] Zheng, L., Zhang, Y., & Thing, V. L. (2019). A survey on image tampering and its detection in real-world photos. *Journal of Visual Communication and Image Representation*, *58*, 380-399.

[23] Lee, J. C., Chang, C. P., & Chen, W. K. (2015). Detection of copy-move image forgery using histogram of orientated gradients. Information Sciences, 321, 250-262.

[24] Parihar, V., & Mehtre, B. M. (2016). Copy move forgery detection using key-points structure. Sardar Patel University of Police, Security and Criminal.

[25] Dixit, R., Naskar, R., & Mishra, S. (2017). Blur-invariant copy-move forgery detection technique with improved detection accuracy utilizing SWT-SVD. IET Image Processing, 11(5), 301-309.

[26] Vidyadharan, D. S., & Thampi, S. M. (2017). Digital image forgery detection using compact multi-texture representation. Journal of Intelligent & Fuzzy Systems, 32(4), 3177-3188.

[27] Wang, C., Zhang, Z., & Zhou, X. (2018). An image copy-move forgery detection scheme based on A-KAZE and SURF features. Symmetry, 10(12), 706.

[28] Mahmood, T., Mehmood, Z., Shah, M., & Saba, T. (2018). A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. Journal of Visual Communication and Image Representation, 53, 202-214.

[29] Hashmi, M. F., Hambarde, A. R., & Keskar, A. G. (2013, December). Copy move forgery detection using DWT and SIFT features. In 2013 13th International Conference on intelligent systems design and applications (pp. 188-193). IEEE.

[30] Anand, V., Hashmi, M. F., & Keskar, A. G. (2014, April). A copy-move forgery detection to overcome sustained attacks using dyadic wavelet transform and SIFT methods. In Asian Conference on Intelligent Information and Database Systems (pp. 530-542). Springer, Cham.

[31] Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018). Buster not: Detecting copy-move image forgery with source/target localization. In Proceedings of the European Conference on Computer Vision (ECCV) (pp. 168-184).

[32] Allu Venkateswara, Chanamallu Srinivasa, Dharma Raj Cheruku (2020), An Innovative And Efficient Deep Learning Algorithm For Copy Move Forgery Detection In Digital Images, International Journal of Advanced Science and Technology 29 (5), 10531 – 10542.

[33] Xinyi Wang, He Wang, Shaozhang Niu and Jiwei Zhang (2019), Detection and localization of image forgeries using improved mask regional convolutional neural network, Math. Biosci. Eng., vol. 16, no. 5, pp. 4581–4593, 2019.

[34] Leekha, A., Gupta, A., Kumar, A., & Chaudhary, T. (2021, March). Methods of Detecting Image forgery using convolutional neural network. In Journal of Physics: Conference Series (Vol. 1831, No. 1, p. 012026). IOP Publishing.

[35] Bayar, B., & Stamm, M. C. (2016, June). A deep learning approach to universal image manipulation detection using a new convolutional layer. Proceedings of the 4th ACM workshop on information hiding and multimedia security (pp. 5-10).

[36] Zhang, Y., Goh, J., Win, L. L., & Thing, V. L. (2016). Image Region Forgery Detection: A Deep Learning Approach. SG-CRC, 2016, 1-11.

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

[38] Amerini, I., Uricchio, T., Ballan, L., & Caldelli, R. (2017, July). Localization of JPEG double compression through multi-domain convolutional neural networks. In 2017 IEEE Conference on computer vision and pattern recognition workshops (CVPRW) (pp. 1865-1871).

[39] Manu, V. T., & Mehtre, B. M. (2016). Detection of copy-move forgery in images using segmentation and SURF. Advances in signal processing and intelligent recognition systems (pp. 645-654). Springer, Cham.