International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Copy Move Forgery Detection Using an Effective CNN Model

Siva Prasad Patnayakuni

sivaprasad.patnakuni[at]gmail.com

Abstract: ***Recently, computerized pictures have become utilized in several applications, where they have turned into the focal point of advanced picture handling analysts. Picture false addresses one exciting issue on which analysts focus on their examinations. We focus on the copy move picture fake point as a misleading fraud type. In duplicate move picture imitation, a piece of a picture is replicated and set in a similar picture to create the invention picture. In this paper, a specific convolutional neural network (CNN) design is proposed for the compelling recognition of duplicate move picture fabrication. The proposed Method is computationally lightweight with a reasonable number of convolutional and max-pooling layers. Numerous observational tests have been led to guarantee the effectiveness of the proposed model with regards to accuracy and time. These analyses were finished on benchmark datasets and have achieved 95.53% accuracy.***

Keywords: convolutional neural network (CNN), CMFD, accuracy

1. Introduction

Advanced pictures are fundamental information that are utilized in numerous applications, for example, legal sciences [1], as proof in the court, PC supported clinical finding frameworks [2], informal organizations [3], and the military [4]. In light of their significance, it is important to guarantee their validness and keep their items sealed. Numerous PC programs empower clients and conventional individuals to misrepresent advanced pictures, which brings about the troublesome recognition of phony pictures by the eye. Since misrepresentation devices have been broadly accessible, it is presently expected to evaluate whether two kinds of pictures are created or real. At the end of the day, it is important to foster present day strategies to distinguish fashioned pictures. The principal approaches for finding picture falsification are partitioned into dynamic and inactive methodologies [5]. The dynamic methodology empowers us to embed watermarks, Digital Signatures onto pictures while making them. The detached methodology empowers us to change right data to erroneous data and shadow significant pictures. Computerized picture imitation can be grouped into five sorts: copymove fraud, picture joining, picture modifying, transforming, and upgrade. Figs. 1, 2, 3, 4, and 5 are instances of the five sorts of advanced picture imitation. The duplicate move is one of the most well-known sorts of advanced picture phony. Many methodologies for distinguishing duplicate move fabrication in computerized pictures were proposed. For the most part, we could arrange these methodologies into three principal gatherings: First, the customary duplicate move fraud identification approach includes notable neighborhood highlight extractors, for example, SIFT, SURF, and ORB [6]. Second, the symmetrical second based approach utilizes mathematical invariant symmetrical minutes to remove the elements. The third is the profound learning-based duplicate move fraud identification approach, in which different methodologies of profound learning are utilized.

2. Literature Survey

Hashmi et al. [9] proposed a calculation for duplicate move fraud (CMF) location in light of the Discrete Wavelet Transform. As per DCT and SVD, Zhao et al. [7] introduction duced a productive strategy for CMF. This approach gives great outcomes on account of numerous CMFs. Chihaoui et al. [8] com bine Invariant Feature Transform (SIFT) and Singular Value Decomposition (SVD) techniques to present a proficient methodology for the programmed location of copied districts in a similar picture. The proposed approach exhibited high strength against the mathematical changes. Dhivya et al. [10] proposed a methodology for CMF location in light of 2-Level DWT to isolate the groups and blocks and SURF for highlight extraction.

Diwan et al. [14] proposed another procedure for CMF. They utilized the great consequences of the CenSurE keypoint and the FERAK as element descriptors and created a steady and exact CMF identification calculation. Priyanka et al. [11] blended DCT and SVD and presented an effective CMF discovery calculation. The proposed approach gives high accu scandalous within the sight of various picture misshapenings. An original procedure for CMF recognition in light of SIFT and the diminished LBP has been presented by Park et al. [12]. This approach uncovers when contrasted and other existing strategies.

As of late, different procedures for CMFD in view of picture minutes have been proposed. Hosny et al. [20] proposed a quick and precise calculation for CMFD in light of polar complex remarkable change minutes PCETMs. The proposed approach showed high exactness with various kinds of picture distortions. The past methodology [20] has been redesigned utilizing the quaternion idea pertinent to variety pictures Hosny et al. [21]. Meena et al. [22] presented an extremely fitting strategy for CMFD in light of Gaussian Hermite Moments GHMs. The observational outcomes demonstrated the precision of the proposed way to deal with identify the duplicate moved manufactured districts. Great attributes of the two procedures: accelerate

vigorous element SURF and PCET, was the rationale in Wang et al. [23] to present a productive and exact technique for CMFD, SURF is utilized to recognize the central issues.

Interestingly, the elements of the pictures are separated utilizing the PCETMs. Wang et al. [24] consolidated the solitary worth disintegration SVD and the PCET ways to deal with present the SVD-PCET approach. Right away, the invariant mathematical snapshots of a picture are separated utilizing the PCET, then, at that point, SVD is utilized to decrease the element of the got highlight grid. Different tests demonstrated the precision of the SVD-PCET as a CMFD approach.

One of the hotly debated issues that have been utilized in different fields is profound learning. The CMFD addresses one of these fields. Profound advancing principally relies upon CNN. Through CNN, their many stages. At each stage, a bunch of elements are gen erated. A few elements are utilized as a preparation set. Strategies in view of profound learning uncover preferable execution over tradi tional and second based approaches. As of late, numerous CMFD approaches in view of profound learning have been introduced. Elaskily et al. [25] introduced a productive methodology for automatic CMFD in view of CNN, and the proposed approach accomplished 100 percent exactness when applied to various datasets.

Goel et al. [28] proposed a CMFD framework in view of an original procedure called double branch CNN. The proposed system demonstrates great outcomes with regards to time and execution. Ortega et al. [27] proposed two methodologies for CMFD in light of profound learning: a custom design model and an exchange learning model. The proposed framework has been tried more than eight benchmark datasets. Abhishek et al. [26] acquainted a proficient framework with distinguish and restrict the picture phonies in light of profound CNN and semantic division. The got results give exactness above 92%. Jaiswal et al. [29] introduced a CMFD model it utilized multi-scale information and two blocks of convolutional layers: encoder and decoder blocks. The observational outcomes demonstrated the high exactness of the proposed framework. Because of the past conversation, it shows a lack of past works, and the deficiency propels the creator to propose an effective CNN-based strategy. The main contributions presented by this study can be summarized as follow:

- A productive and precise CNN model was proposed. It accomplished a promising precision score as contrasted and the other researched models.
- The proposed model is lightweight. It contains three convolutional layers, three max-pooling, 235406 hyper boundaries, and one completely associated layer.
- An insightful examination of characteristic and false is led between the proposed model and the other researched models (M. Elaskily et al. [25], Amerini et al. [15], Amerini et al. [16], Elaskily et al. [17], Mishra et al. [18], Kaur et al. [19], J. Zhong et al. [31], Y. Wu et al. [32], A. Islam et al. [33], and Malle Raveendra et al. [34]). The got results are better than other as of late distributed approaches.
- Thwobenchmark datasets were utilized in the trials. These datasets are MICC-F220 [15] and MICC-F600 [16]. It is permitted us to introduce precise analyses.

We depict in short the CNN model. CNN is a convolution brain organization. Its assignment is to remove the significant elements in the picture. Profound learning comprises of three essential layers: the convolution layer, pooling layer, and completely associated layer. CNN incorporates many layers: convolutional layer, max pooling layer, straightening layer, and full association layer, as displayed in Fig. 6.

a) The convolutional layer: is the initiation capability, and it is a non-direct capability. It has a few sorts; the enactment capability is generally normally utilized. It is a non-direct capability with a few sorts, as displayed in Fig.7. The most generally utilized them are:
   - ReLU (redressed direct unit) Its significance is diminishing the quantity of records performed.
   - Sigmoid, which is utilized in the result layer.
b) Max-pooling layer: It gathers the highlights extricated from the picture, diminishes the aspects, and concentrates the main elements present in the picture, as displayed in Fig. 8.
c) Flattening layer: it changes over the qualities taken from max-pooling into a one-layered lattice
d) Completely associated layer: it assembles every one of the neurons.

The remainder of this study contains four segments as follows: sec II talks about, in primers, the CNN portrayal. The construction of the proposed approach is introduced in sec III. Our outcomes and talked about in sec IV. At last, sec. V the end.

3. Proposed Method

In this paper, a accurate profound CMF identification technique was presented. The proposed approach depends on the CNN model, as displayed in Fig. 9. The conventional methodology deals with a block-based calculation, while the CNN approach deals with the entire picture. The introduced approach has three phases: preprocessing, highlight extraction, and characterization. The info picture is resized to enter the following stage without editing any picture parts in the preprocessing information stage. The element extraction stage contains three convolution layers, trailed by a maximum pooling layer. Toward the finish of this stage, a full association layer interfaces all elements with the thick layer. At long last, the arrangement stage is called to characterize the information into two groupings (produced or unique). The convolution layers as element mining, in which every convolution layer produces its component maps utilizing its own arrangement of channels (i.e., ReLU). The component maps delivered from the main convolution layer are utilized in the following max-pooling layer to create resized pooled highlight maps, considered the contributions of the following convolution layer. The last component maps converged with the last max-pooling are designed as vectors and integrated into Fully Connected.

Figure 1: Copy move: the left image is the original, and the right is copy-move

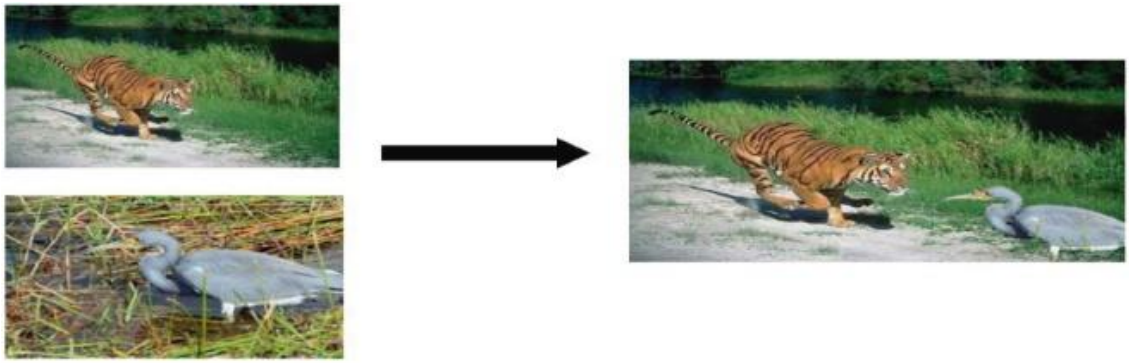

Figure 2: Image splicing: in the left and center are original images, and in the right is the splicing

Figure 3: Image morphing: in the left and right are original images, and in the center is the morphed.

Figure 4: Retouching image: the left image is the original face, and the right image is the retouching face

Figure 5: Image Enhanced: The upper left corner is the original, followed by various enhancements such as color change blurring of the background. Finally, in the lower right corner is the enhanced image

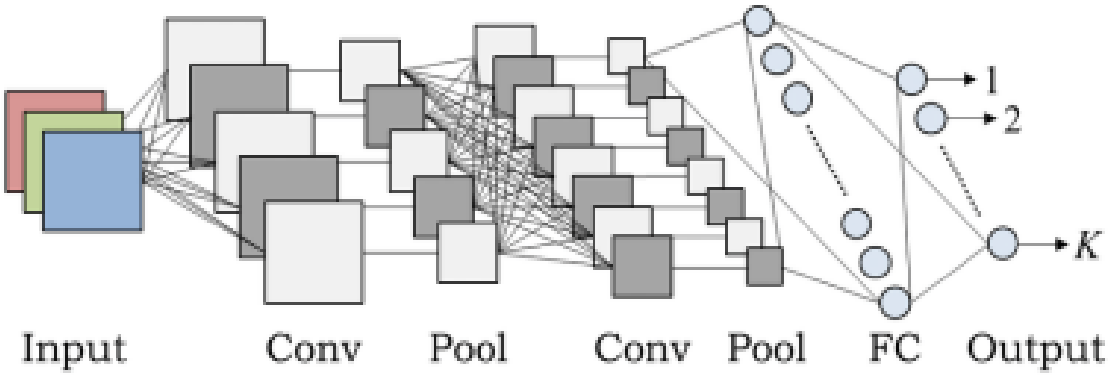

Figure 6: CNN layers

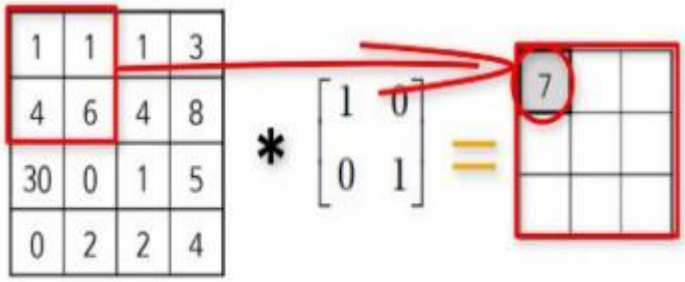

Figure 7: Convolution layer

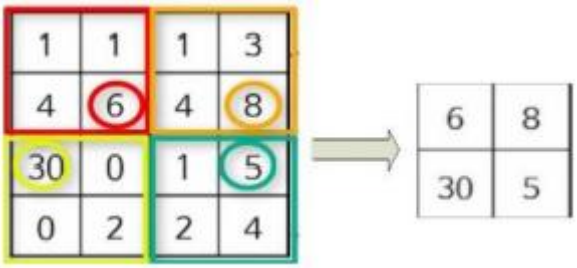

Figure 8: Max poling layer

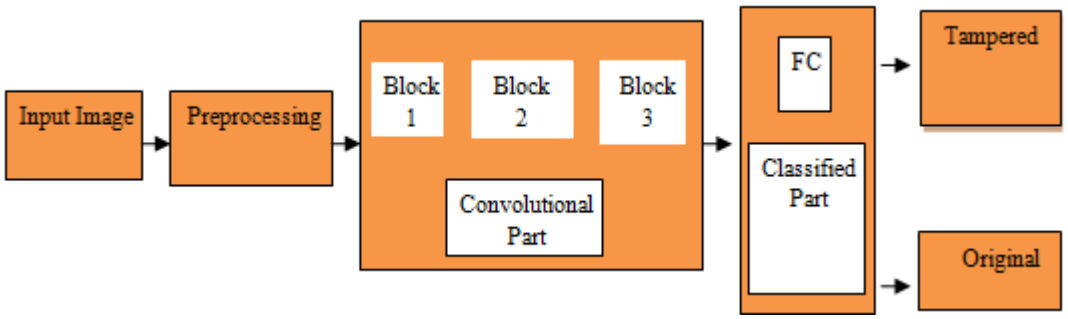

Figure 9: The structure of the proposed algorithm CNN layers

Table 1: The details of the MICC-F220 and MICC-F600 datasets

Dataset	MICC-F600	MICC-F220
No. of Images	600	220
Size of Image	800 x 530	800 x 480
No. of Training Images	360	160
No. of Validation Images	180	40
No. of Testing Images	60	40
Image Size	224 x 224 x 3	224 x 224 x 3

Table 2: Performance evaluation for proposed method on the MICC-F220

	Positive (%)	Negative (%)
TRUE	98.1	99.6
FALSE	8	6

Table 3: Comparison between the proposed method and previously on the MICC-F220

Method	DA(%)	P(%)	R(%)	F1(%)
Proposed	93.38687	92.45994	94.23631	93.33968
[32]	85	81.81818	90	85.71429
[33]	90	83.33333	100	90.90909

Table 4: Performance evaluation for proposed method on MICC-F600

	Positive (%)	Negative (%)
TRUE	96.23	94.21
FALSE	5.7	3.2

Table 5: Comparison between the proposed method and previously on MICC-F600

Method	DA (%)	P (%)	R (%)	F1 (%)
[32]	83.85	80.61686	89.13	84.65995
[33]	89.6	86.74833	93.48	89.98845
Proposed	95.53527	94.40793	96.78166	95.58006

4. Results and Discussion

This section and a comprehensive assessment of the proposed approach's findings. The tests have been run on the Google Collaborator server with Google compute engine backend (GPU) RAM: 2.5GB/16GB. The Tensor Flow with Keras as a backend, using python 3.0.

a) DATASETS:
The common usable and famous datasets used to test CMF detection techniques include MICC-F600 [16] and MICC-F220 [15]. The contents of these datasets are exposed in Table1.

b) Performance Evaluation:

Detection Accuracy:

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

Precision:

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

Recall:

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

F1 score:

$$F1 = \frac{2 \times P \times R}{P + R} \quad (4)$$

The presented approach has the best outcomes at no of ages 30, where when contrasted and the outcomes in [25]. These confusion Matrix show up in Table 2 and 4. These outcomes were the nearest to the best outcomes we got. Likewise, the predominance of these outcomes was agreeable to the proposed approach with a typical proficiency gain of 3.38 and 5.1 with the accuracy, log misfortune, and TT(mm:ss), individually. Table 5 introduced exploratory outcomes among the proposed approach and other looked at approaches [15]-[19], [25]. The outcomes showed outperformance inclining toward the proposed approach in regards to exactness and TT. The proposed technique changes from the Dhananjay et al. [30] technique on an alternate dataset, MICC-F600 [16] and MICC-F220 [15]. The proposed approach has the best outcomes. Table 3 and 5 show that the proposed approach beats F1-score, accuracy, recall and precision.

5. Conclusion

All in all, this study presented a Copy-move Forgery Detection system in light of profound brain learning. The proposed model can perceive the altered pictures, grouping the competitor's picture into two sorts of order: fashioned and unique. The proposed framework can make include vectors from a picture's highlights. The proposed approach naturally utilizes the full association layer to track down include correspondences and conditions. The proposed model should be prepared first to be prepared to test and afterward arrange the altered pictures. The exhibition of the

proposed model was evaluated through three benchmark datasets: MICC-F600, and MICC-F220. The mathematical outcomes subsequent to researching and contrasted and different methodologies uncover prevalence for the genius presented approach. The proposed technique accomplished 95.58 percent accuracy at no.of ages 30 with all datasets. On account of TT, we additionally accomplished great outcomes contrasted and the current calculations. For the datasets MICC-F600, and MICC-F220, we got a TT equivalent to 7.73 sec, and 0.83 sec, individually. All experimental outcomes demonstrated the high predominance of the proposed model against other detailed calculations concerning accuracy and TT.

References

[1] A. Ross, S. Banerjee, and A. Chowdhury, ‘‘Security in smart cities: A brief review of digital forensic schemes for biometric data,’’ Pattern Recognit. Lett., vol. 138, pp. 346–354, Oct. 2020.

[2] M. M. Eltoukhy, M. Elhoseny, K. M. Hosny, and A. K. Singh, ‘‘Computer aided detection of mammographic mass using exact Gaussian–Hermite moments,’’ J. Ambient Intell. Humanized Comput., pp. 1–9, Jun. 2018, doi: 10.1007/s12652-018-0905-1.

[3] F. Marcon, C. Pasquini, and G. Boato, ‘‘Detection of manipulated face videos over social networks: A large-scale study,’’ J. Imag., vol. 7, no. 10, p. 193, Sep. 2021, doi: 10.3390/jimaging7100193.

[4] K. Sunitha and A. N. Krishna, ‘‘Efficient keypoint based copy move forgery detection method using hybrid feature extraction,’’ in Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA), Mar. 2020, pp. 670–675.

[5] S. Velmurugan, T. Subashini, and M. Prashanth, ‘‘Dissecting the literature for studying various approaches to copy move forgery detection,’’ Int. J. Adv. Sci. Technol., vol. 29, pp. 6416–6438, Jun. 2020.

[6] X. Tian, G. Zhou, and M. Xu, ‘‘Image copy-move forgery detection algorithm based on ORB and novel similarity metric,’’ IET Image Process., vol. 14, no. 10, pp. 2092–2100, 2020.

[7] J. Zhao and J. Guo, ‘‘Passive forensics for copy-move image forgery using a method based on DCT and SVD,’’ Forensic Sci. Int., vol. 233, nos. 1–3, pp. 158–166, 2013, doi: 10.1016/j.forsciint.2013.09.013.

[8] T. Chihaoui, S. Bourouis, and K. Hamrouni, ‘‘Copy-move image forgery detection based on SIFT descriptors and SVD-matching,’’ in Proc. 1st Int. Conf. Adv. Technol. Signal Image Process. (ATSIP), Mar. 2014, pp. 125–129.

[9] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, ‘‘Copy move forgery detection using DWT and SIFT features,’’ in Proc. 13th Int. Conf. Intellient Syst. Design Appl., Dec. 2013, pp. 188–193.

[10] S. Dhivya, B. Sudhakar, and K. Devarajan, ‘‘2-level DWT based copy move forgery detection with surf features,’’ in Proc. 3rd Int. Conf. Commun. Electron. Syst. (ICCES), Oct. 2018, pp. 800–805.

[11] P. G. Singh and K. Singh, ‘‘An improved block based copy-move forgery detection technique,’’ Multimedia Tools Appl., vol. 79, pp. 13011–13035, May 2020.

[12] J. Park, T. A. Kang, Y. H. Moon, and I. K. Eom, ‘‘Copy-move forgery detection using scale invariant feature and reduced local binary pattern histogram,’’ Symmetry, vol. 12, p. 492, Apr. 2020, doi: 10.3390/sym12040492.

[13] X. Tian, G. Zhou, and M. Xu, ‘‘Image copy-move forgery detection algorithm based on ORB and novel similarity metric,’’ IET Image Process., vol. 14, pp. 2092–2100, Oct. 2020.

[14] A. Diwan, R. Sharma, A. Roy, and S. Mitra, ‘‘Keypoint based comprehensive copy-move forgery detection,’’ IET Image Processing, vol. 15, pp. 1298–1309, May 2021.

[15] I. Amerini, L. Ballan, R. Cardelli, A. Del Bimbo, and G. Serra, ‘‘A siftbased forensic method for copy–move attack detection and transformation recovery,’’ IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Mar. 2011.

[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, ‘‘Copy-move forgery detection and localization by means of robust clustering with J-Linkage,’’ Signal Process., Image Commun., vol. 28, no. 6, pp. 659–669, Jul. 2013.

[17] M. Elaskily, H. Elnemr, M. Dessouky, and O. Faragallah, ‘‘Two stages object recognition based copy-move forgery detection algorithm,’’ Multimedia Tools Appl., vol. 78, no. 11, pp. 15353–15373, 2019.

[18] N. Mishra, S. Sharma, and R. Patel, ‘‘Region duplication forgery detection technique based on SURF and HAC,’’ Sci. World J., vol. 7, pp. 1–8, Nov. 2013.

[19] H. Kaur and J. Saxena, ‘‘Simulative comparison of copy-move forgery detection methods for digital images,’’ Int. J. Electron., Elect. Comput. Syst., vol. 4, pp. 62–66, Sep. 2015.

[20] K. M. Hosny, H. M. Hamza, and N. A. Lashin, ‘‘Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators,’’ Imag. Sci. J., vol. 66, no. 6, pp. 330–345, Aug. 2018.

[21] K. Hosny, H. Hamza, and N. Lashin, ‘‘Copy-for-duplication forgery detection in colour images using QPCETMs and sub-image approach,’’ IET Image Process., vol. 13, no. 9, pp. 1437–1446, 2019.

[22] K. Meena and V. Tyagi, ‘‘A copy-move image forgery detection technique based on Gaussian-Hermite moments,’’ Multimedia Tools Appl., vol. 78, pp. 33505–33526, Dec. 2019.

[23] C. Wang, Z. Zhang, Q. Li, and X. Zhou, ‘‘An image copy-move forgery detection method based on SURF and PCET,’’ IEEE Access, vol. 7, pp. 170032–170047, 2019.

[24] Y. Wang, X. Kang, and Y. Chen, ‘‘Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures,’’ J. Inf. Secur. Appl., vol. 54, Oct. 2020, Art. no. 102536.

[25] M. Elaskily, H. Elnemr, A. Sedik, M. Dessouky, G. El Banby, O. Elshakankiry, A. Khalaf, H. Aslan, O. Faragallah, and F. A. El-Samie, ‘‘A novel deep learning framework for copy-moveforgery detection in images,’’ Multimedia Tools Appl., vol. 79, pp. 19167–19192, Jul. 2020.

[26] Abhishek and N. Jindal, ‘‘Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation,’’ Multimedia Tools Appl., vol. 80, pp. 3571–3599, Jan. 2021.
[27] Y. Rodriguez-Ortega, D. M. Ballesteros, and D. Renza, ‘‘Copy-move forgery detection (CMFD) using deep learning for image and video forensics,’’ J. Imag., vol. 7, no. 3, p. 59, Mar. 2021, doi: 10.3390/ jimaging7030059.
[28] N. Goel, S. Kaur, and R. Bala, ‘‘Dual branch convolutional neural network for copy move forgery detection,’’ IET Image Process., vol. 15, p. 656, Feb. 2021.
[29] A. Jaiswal and R. Srivastava, ‘‘Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model,’’ Neural Process. Lett., vol. 54, pp. 75–100, Aug. 2021, doi: 10.1007/s11063-021-10620-9.
[30] K. Dhananjay, S. Ahirrao, and K. Kotecha, ‘‘Efficient approach towards detection and identification of copy move and image splicing forgeries using mask R-CNN with MobileNet V1,’’ Comput. Intell. Neurosci., vol. 2022, pp. 1–21, Jan. 2022, doi: 10.1155/2022/6845326.
[31] J.-L. Zhong and C.-M. Pun, ‘‘An end-to-end dense-inceptionNet for image copy-move forgery detection,’’ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2134–2146, 2020, doi: 10.1109/TIFS.2019.2957693.
[32] Y. Wu, W. Abd-Almageed, and P. Natarajan, ‘‘BusterNet: Detecting copy-move image forgery with source/target localization,’’ in Proc. Conf. Comput. Vis. Pattern Recognit., 2018, pp. 168–184. [Online]. Available: https://link.springer.com/conference/eccv
[33] A. Islam, C. Long, A. Basharat, and A. Hoogs, ‘‘DOA-GAN: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., Jun. 2020, pp. 4676–4685.
[34] Malle Raveendra, K. Nagireddy, “Tamper video detection and localization using an adaptive segmentation and deep network technique”, in Journal of Visual Communication and Image Representation, Volume 82,2022,103401,ISSN 1047-3203, https://doi.org/10.1016/j.jvcir.2021.103401.