

An Analysis on Image Forgery Detection Techniques

Dayanand G. Savakar, Raju Hiremath*

Department of Computer Science,
Rani Channamma University Vidyasangama, Belagavi, India.
Email: dgsavakar@gmail.com, rajuhiremath@rcub.ac.in

Anand Ghuli

Department of Computer Applications,
Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, India
Email: mca.anand@bldeacet.ac.in

(Received January 23, 2023, Revised May 15, 2023, Accepted June 10, 2023)

Abstract: In the recent trends and technology we found that the digital image plays an important role. The digital images are widely used in various fields. The validation is now becomes a challenging task because of advancement in the tools and technology. The various tools are used to modify the digital image to create fake digital images. The several research has been carried out in the field of image forgery detection. In this paper attempted to review the existing technique to identify the forgery in an image. Accordingly related papers are reviewed and analyzed. The active and passive are the two approaches in the image forgery detection technique. The digital signature and digital watermarking are the two methods in active approach, and in passive approach various techniques are there such as copy-move, splicing, re-sampling etc., In this paper we describe the comparative analysis of different types of image forgery detection technique along with future work to be carried out.

Keywords: Digital image, forgery detection, copy-move, splicing, re-sampling.

1. Introduction

In the era of digital media, key-communicative media is an image. Images are used as a proof of a person, place or things. The day to day improvement in the software technology leads to the misuse of the same software technology which is quite increased. With the help of a software technology the images are modified and abused in different fields. The images forgeries

are identified not only in present days but also it has been identified in ancient days also. The uses of digital media like images are more and more frequent in the present world. The images are also used as a communication media. Hence a major challenge is to protect the image from the unauthorized users. The images are used to forge by using the photo editing software tools. At present several software tools are available for modifying the original image and display it in a different way. As the technology is upgraded different software tools and techniques are developed. Using the latest tools and technologies images are customized very easily. Image forgery techniques are utilized to detect the image forgeries like digital signature, digital watermarking, copy-move, splicing and re-sampling etc. The Figure 1. shows the categorizations of image forgery detection methods.

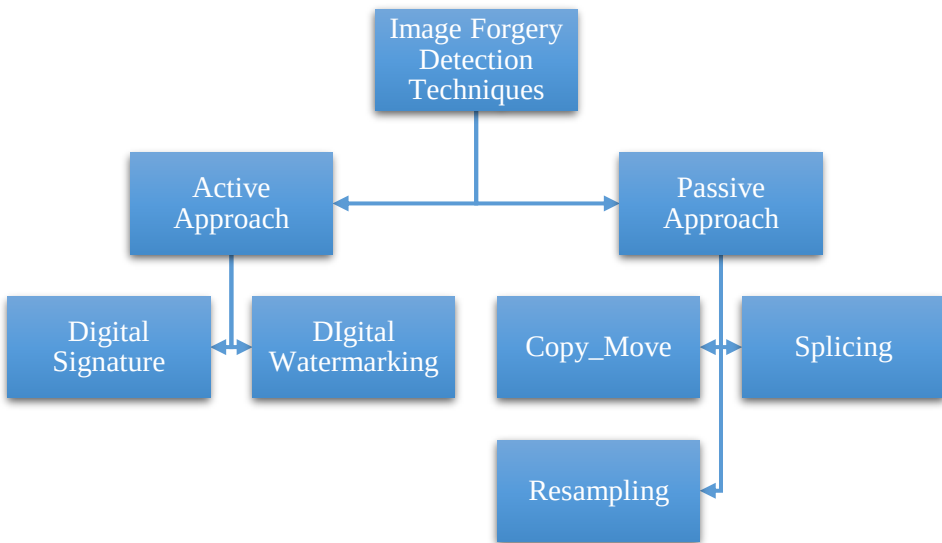


Figure 1. Image Forgery Detection Techniques

1.1 Active Approach: In this type of approach data and information is used to verify authentication of forgery of an image. To identify the original image code is used. The data hiding code is added at the time of generating an image. The code can be added using camera or software tools. The drawback of this method is some cameras not supporting of embedding the information in advance. This method is classified into Digital Watermarking and Digital Signature¹.

1.1.1 Digital Signature: Digital signature is used to provide authenticity of the digital documents or digital messages. This digital signature is used to identify the creator of the message or document. The digital signature is decoded and the message created using digital signature cannot be altered.

These digital signatures are used for distribution of the software, different financial transactions and the cases where the forgery detection and tempering.

1.1.2 Digital watermarking: Digital watermarking is also used to authenticate the digital content. In this technique the authentication information is embedded at the time of digital content creation. The embedded information is extracted at the time of authenticating the digital content. The information which is embedded at the time of creation is same as at the time extraction means the digital content is authenticated.

1.2 Passive Approach: Image forensics is another name to call this method. To overcome the drawback of active approach this method is implemented. In this method there is no information is required to for authenticating the image. This technique is assumption based technique. The tampering of an image will not leave any hint. But the pixels are liable to alter. There are three methods in passive approach copy-move, slicing and re-sampling.

1.2.1 Copy-Move Forgery Detection: The copy-move is the frequently used type of forgery. In this kind of forgery copy some part of an image and moved it to the same image to make forgery. Through this type of forgery detection tempered region of the image can be identified¹.

1.2.2 Image Slicing Detection: This type of method is used to detect the modified image by merging two or more images. For example, it may include the modifying the background by adding two or more images and joining two or more images to make a different image. In this type of detection, the combined regions are examined using different methods. The rapid changes in the different regions of the images are collectively helps to detect the slicing in the image¹.

1.2.3 Image Re-sampling Detection: For creating forged image slicing the two images and for making perfect match between two sliced images it is required to rotate, resize or stretch the part of an image. The re-sampling method is applied the original image to new sampling lattice by using the interpolation form¹.

2. Related Work

The various authors presented the research papers on image forgery detections. In particular different types of forgery detection methods such as digital signature, digital watermarking, copy-move, splicing and re-sampling etc.

2.1 Digital Signature: In the paper², a suggested article introduces a novel technique to medical picture steganography based on a modified Least Significant Bit (LSB) design and the Local Binary Pattern (LBP) pattern. The cover image was initially separated into sections of 33 non-overlapping overlays. Next, utilizing the LBP operator, determine the pixel embedding position. The A LBP operator's result dictates how and where hidden image pixels are embedded. Pixel values will be integrated inside the cover image pixel afterwards utilizing the LSB technique. The suggested method additionally uses Reversible Watermarking (RW), a Digital Signature (DS) method, to ensure its content's authenticity.

The author³ looked into approaches which combined cryptography with steganography. Information is buried beneath a cover picture in steganography. In this study, methods for concealing information utilizing cryptography and steganography are suggested, with two concerns in mind: actual size of the encrypted item as well as the level of protection. A signature picture information is stored inside the cover picture utilizing the transmitter and recipient's private keys, and the information is extracted out from stego picture using a public key. Such method is suitable for secure communication, integrity protection, and non-repudiation.

In the paper⁴ the author presents a hybrid solution for confidential textual information that uses zero-watermarking and digital-signature-like operations to enable textual authenticity and truthfulness confirmation without actually altering the cover text. The suggested method has been built and demonstrated to be resistant to undiscovered textual alterations, as well as competent in validating evidence of originality while identifying and identifying purposeful and non-deliberate manipulation. In compared to typical encryption-based techniques, there were improvements in capacity use and less duplication.

2.2 Digital Watermarking: In the paper⁵, presented colour cover picture authentication method, a fragile watermarking method is being used in the study. Two entities of a picture were utilised within that approach to insert content into a colour cover picture . Across different of the colour picture, single domain insertion is performed. In one level, HBS is used for private data insertion, while in another level, DCT is used for fragile watermark insertion. Utilizing HBS, the approach transiently extracts the private data out from picture and uses a fragile watermark to determine if the picture was already altered . While inserting data in the two levels of a picture, the watermarked colour pictures display great detection accuracy.

In the paper⁶, A blind multifunctional picture watermarking system for copyright/ownership preservation, picture validation, as well as

picture enhancement is presented in this study. For accomplish such multifunctional character, two separate watermarking techniques are applied. An encoded watermark is injected into the host picture employing IWT for Robust watermark placement . The fragile succession and restoration details are then embedded in a controlled randomised way using a 9-base notation-based least significant bit replacement technique. During the validation process, excellent interpretability, reasonable robustness, and effective self-recovery across various forms of assault were observed.

In the paper⁷, the author presents a revolutionary Portable Document Format (PDF) strategy that focuses on document page entities. Watermarking is done with the Special elements of a PDF File Format not altering its details of the original document. The suggested method maintains hiding capacity while also resisting structuring assaults. The watermark data is recovered with such a high degree of certainty, as well as the suggested approach is resilient, secure, and unnoticeable, embedding 0.22 KB of the watermark inside the host document.

In the paper⁸, a novel method for forgery detection and localisation of pictures based on hashing and watermarking is described. The original cover picture is split into four non-overlapping parts at initially. The DC values are extracted utilizing the Discrete Cosine Transform (DCT) for each 4 x 4 unit. The SHA-256 hash algorithm is then used to construct a hash from such values. To incorporate the recovered hash, the original cover picture is Arnold Converted and afterwards split into 4 x 4 sections . Afterwards when, the watermarked picture is created using Inverse Arnold Transform. Image processing techniques assaults, copy-paste attacks, and copy-move attacks are proven to be robust to a suggested technique.

In the paper⁹, As in transform domain, an unique strong counterfeit identification medical watermarking system is provided for verification and identification of counterfeit pixels in medical photographs. In this approach, a meaningful picture is subjected to a two-level Discrete Wavelet Transform, which yields four sub-bands (SB) (CLL, CLH , CHL, CHH). When inserting the watermark, the values of LL sub-bands are taken into account. To protect against image processing threats, the SB is divided into smaller parts. For every part, the LSB is set to zero, and then Scour decomposition is used to generate Authenticated Block Bits (ABB). The watermark is jumbled using Quantum Hilbert Image Scrambling to create doubt for attackers. After manipulation, watermarking aids in verification and counterfeit identification of a important picture.

2.3 Copy-move: In the paper¹⁰, author suggested a key-point-based copy-move forgery detection approach Using SIFT and KAZE attributes. To pick

powerful features and decrease the number of key-points, a salient key-point attribute selection has been suggested. A selective search-based region suggestion was used to generate a frame on the original image to improve the identification of a replicated component. To discover replicated items, key-points within the bounding box were investigated for attribute descriptor verification. For replicated part identification, key-points between two bonding boxes were checked, but key-points inside a frame were not evaluated, reducing the temporal difficulty of the suggested technique.

In the paper¹¹, offer a composite technique that combines deep features with DCT-based block features to provide effective detection performance in a wide range of known attacks. During the initialization phase, the suggested approach uses a global contrast correction technique known as LDR, after which a deep neural network obtains deep features from the picture patches. In order to be resistant to JPEG compression assaults, the approach also extracts unit information from the image. Texture Match is used to match hybrid features (deep and block-based characteristics), and then the proposed post-processing method is applied to the matching results to reduce false matches.

In the paper¹², presents a frequency-domain picture modification approach. The approach takes advantage of the discrete wavelet transform's (DWT) confined character to obtain the altered portion of the cover picture. Every sub-band of the patch is applied to the detected location in the equivalent sub-band of the host picture, and then both the patch and the host picture are treated to DWT simultaneously level 1 to generate $3l + 1$ sub-bands. To generate the final manipulated cover picture, the modified host sub-bands are subsequently subjected to inverse DWT. The suggested technique is resistant to recognition by two frequency-domain forgery recognition techniques that have been published in the past.

In the paper¹³, the authors present a novel CMFD system that includes I an enhanced SIFT framework, ii) a new Feature Label Matching (FLM), and iii) an unique Hierarchical Segmentation Filtering (HSF). SIFT's enhanced structure improves its potential to fetch impactful key-points from homogeneous regions. For greatly better matching performance and efficiency, FLM splits out the vast key-points as tiny tag sets. Given the statistics of coarse-to-fine hierarchical categories, a HSF technique is presented to select across problematic anomalies that reveal forging areas. This novel approach can identify a wide range of forgery attempts, including forging in homogeneous regions under large-scale attacks.

In the paper¹⁴, presented a copy-move forgery identification technique. The source picture is initially segmented as units in the present scheme. Next,

out of each unit, different characteristics such as energy, entropy, contrast, homogeneity, mean, standard deviation, and variance are retrieved and stored in the skill set. The characteristics of every units are then verified to the skill set. The suggested approach efficiently distinguishes between genuine and counterfeit photos.

2.4 Splicing: In the paper¹⁵, A Mean Absolute Deviation (MAD) feature is derived employing classic Benford's law with in suggested technique. For the mantissa distribution input vectors, extended Benford's law is also employed. Many statistical characteristics are employed to generate the final feature vector in addition to Benford's law-based characteristics. Lastly, to categorise real and fabricated photos, a support vector machine (SVM) with three distinct kernel functions is employed.

In the paper¹⁶, the study shows how to use FT(frequency transforms) of pictures to build a splicing identification CNN in a self-supervised manner. The programme is aimed to develop a picture fingerprint that can be used to recognize spliced sections derived from various pictures provided the FT. On several criteria, our experiments show that the suggested framework learnt during self-supervision can meet the speed and efficiency of many established approaches.

The author¹⁷, proposes a unique pixel fractional mean (PFM) approach for picture enhancement classification model in order to improve recognition of picture splicing fraud based on texture data. The suggested PFM improves each pixel individually based upon that pixel's intensity repetition count. To identify crucial information from suspicious spliced pictures, two sets of texturing techniques are applied. To identify real and spliced pictures, such attributes is combined with the "support vector machine" (SVM) classifier.

In the paper¹⁸, proposes a multitask wavelet corrected network (MWC-Net) for picture splicing forgery identification and positioning that can acquire better complete and relevant characteristics. MWC-Net uses wavelet pooling and unpooling to compress and rebuild the characteristics of fake forgery photos, resulting in less data lost while extracting characteristics. MWC-Net, on the other hand, employs a cross technique to boost its potential to understand and use more complete and representative characteristics. T the test outcome tell that presented system outperforms state-of-the-art approaches in splicing forgery identification and positioning

In the paper¹⁹, a recognition approach based upon rich features as well as a convolutional neural network is proposed. For prevent picture information interfering with categorization, first refine the picture with a high pass filter, next categorize the pictures with a very well new convolutional neural

network. The result of the proposed system outperformed standard approaches there in test.

2.5 Re-sampling: In the paper²⁰, the correlation aware convolution neural network (CA-CNN) is used to obtain re-sampling characteristics for identifying composite manipulation activities in this research. The picture is enlarged in this case to identify manipulation in a tiny area. A three-layer horizontal, vertical, and associated layer make up the CA-CNN. The associated layer is utilized to provide associated re-sampling between horizontal and vertical sequences. The identifier would then be constructed by aggregating the features. Using diverse samples, a testing is performed to compare the results of the CACNN system to previous altering identification algorithms. This CA-CNN is effective as in face of numerous defects and post-processing assaults such as JPEG encoding and scaling, as evidenced by the results obtained.

In the paper²¹, the article focuses on detecting counterfeit photos within original photograph using a re-sampling (rotate or stretch) identification system inside the area of photo forging. So researcher devised a modified Markov Features Driven identification system to achieve this aim. Combining bilinear and bi-cubic interpolation algorithms, the suggested solution performs using varied model parameters for upscaling, downscaling, and rotating datasets. The testing findings reveal that proposed technique outperformed current approaches.

In the paper²², the issue of picture re-sampling identification is explored in depth using a sequential parametric approach. The cyclical artefact of a one-dimensional 1-D) re-sampled data has been revealed. The device has been developed based on the likelihood of remaining noise retrieved from re-sampled data utilizing a sequential parametric model after communicating also with nuisance criteria and Bayes' rule. Following that, we focus on the characteristics of a re-sampled picture. Meanwhile, it is suggested that the frequency of pixel distortion be estimated and a realistic Likelihood Ratio Test (LRT) be established. Analytical studies illustrate the usefulness of our suggested technique in recognizing uncompressed/compressed re-sampled pictures when compared to state-of-the-art testing.

In the paper²³, the author provide a strategy for employing machine learning to identify local re-sampling while limiting the false alarm rate via a-contrario analysis. There are three main phases in the automated operation. For picture frames, re-sampling properties are first determined. A heatmap indicating whether the picture frame has been re-sampled is then generated using a machine learning algorithm. These kind of frames are likely to be misidentified as re-sampled. We employ a-contrario hypothesis testing to see

whether the structures of the modified frames suggest that the picture has been altered, as well as to pinpoint where the alteration took place. We show that this method is successful in detecting if a picture has been changed and pinpointing the location of the alterations.

In the paper²⁴, author provide an unique machine learning strategy for learning re-sampling recognition characteristics from data in an adaptable manner. Researcher leverage the newly invented limited convolutional layer to do the same. Researchers examine the efficiency of the suggested restricted convolutional neural network (CNN) in detecting re-sampling in re-compressed pictures through a series of tests. Overall test results indicate that our limited CNN can correctly identify re-sampling in re-compressed pictures in settings where other methods have failed.

3. Image Forgery Detection Methods

3.1 Copy-Move Image Forgery Detection Using Shannon Entropy

The suggested system determines whether or not an image has been copied and moved. The mechanism operates in three stages²⁵:

3.1.1 Phase 1

The RGB picture is split into four overlaying blocks, and the Shannon entropy for the red, green, and blue columns is determined independently, with the average of every column being computed and placed in the characteristic matrices.

The intensity of every single block is subsequently computed. Furthermore, features are saved in the feature vector for further comparison²⁵.

3.1.2 Phase 2

The RGB picture is transformed to grayscale at this step. Furthermore, the picture is separated into four overlapping blocks, and the Shannon entropy for grayscale images is determined independently, with the average entropy kept in the feature matrix. The intensity of every single block is then determined and saved in a feature vector for further comparison. The identical RGB picture is transformed to grayscale and divided into four overlapping blocks, after which the Shannon entropy and intensity matrix are computed and stored as feature vectors²⁵.

3.1.3 Phase 3

The similarity score of every component of the feature vector for the particular block has been determined with all the other blocks left in this phase. Euclidean distance is employed to assess the similarity score. The distance among two locations on a plane is calculated using Euclidean

distance. The similarity score will be between 0 and 1, with 0 indicating that it is not comparable to the original block and 1 indicating that it is precisely the same. It may be translated to a percentage to get a similarity score ranging from 0 to 100%. Highlight the identical block as red and blue if the measured similarity score is greater than the threshold. Then "block-matching" among red- and blue-marked blocks is conducted, and pixel sensitivity is estimated for the same. If 95% of block-matching is achieved with pixel sensitivity greater than or equal to 0.0033, the picture is categorised as a "copy-move forged image"²⁵.

3.2 Copy-Move and Splicing Forgery Detection Using PNN

In this study, we suggested a Probabilistic Neural Network (PNN)-based picture manipulation identification approach for copy-move and splicing. In this technique, we will first compute the distinction among an input image and the existing original photos, and then compute the mean of the differences to recognise the non-tampered image. If the supplied picture has been manipulated with, we will use the colour and entropy features of the indicated part to determine if it is a copy-move or a spliced manipulation. The input picture is divided into blocks, and the colour and entropy properties are extracted before being classified using PNN. If an identical component is discovered, it is either a copy-move or a spliced fabrication. The suggested method has a 97% accuracy. Despite in different picture formats, the method will provide more accuracy²⁶.

3.3 Image Forgery Detection Using Hybrid Approach

The suggested approach is utilised to distinguish between genuine and counterfeit images. This approach is divided into three stages. In the first phase, we employ the K-means cluster technique to cluster the RGB channel, then we apply the Gaussian filter to blur the picture to remove noise and lower contrast, and last we compute the Shannon entropy for R, G, B, and Grey scale blocks and save the features in matrix form. Find the two matching blocks and save their pixel coordinates in the second phase. At last, colour the paired blocks red and blue. Compute the blue and red highlighted pixel positions in the third phase. If the number of matching pixels is more than or equal to three, it is saved to the matched blocks. If the number of matching pixels is higher than or equal to 10, the forged picture is displayed; otherwise, the original image is displayed. Without the original picture, the recommended approach achieves greater accuracy and effectively identifies the actual and faked image. The suggested technique produced good results with JPG images²⁷.

4. Comparative Analysis

The results of the existing techniques are described in this section. The Table I shows the comparative analysis of various existing image forgery detection techniques

Table I. The comparison of various image forgery detection methods.

Author(s)	Technique	Accuracy
Nitish Kumar and Toshnallal Meenpal ¹⁰	Copy-Move	95.00%
A. Parnak et.al ¹⁵	Splicing	99.94%
Hamid A. Jalab et.al ¹⁷	Splicing	98.40%
Rishi Sinhal and Irshad Ahmad Ansari ⁶	Digital Watermarking	99.8%
Sumaira Bibi et.al ²⁸	Copy-Move and Splicing	95.9%
Geeta Mariappan et.al ²⁹	Copy-Move	94.01%
Ismail Taha Ahmed et.al ³⁰	Copy-Move	98.44%
Muhammad Naveed Abbas et.al ³¹	Copy-Move	87.00%
B. Rakesh Babu and Dr. S. Narayana Reddy ³²	Copy-Move	95.02%
Dayanand Savakar et.al ²⁶	Copy-Move and Splicing	97.00%
Dr. Dayanand G. Savakar and Mr. Raju Hiremath ¹⁴	Copy-Move	96.00%
Sahib Khan and Arslan Ali ³³	Digital Signature	95.01%
Rachna Mehta et.al ²¹	Re-sampling	99.95%
Tongfeng Yang et.al ¹⁹	Splicing	96.73%
Lovepreet Kaur and Sandeep Singh Dhaliwa ³⁴	Copy-Move	93.00%
S. Uma and P. D. Sathya ³⁵	Copy-Move	96.00%
Haipeng Chen et.al ³⁶	Copy-Move	99.00%
Ankit Kumar Jaiswal and Rajeev Srivastava ³⁷	Splicing	99.5%
Dayanand G Savakar and Raju Hiremath ²⁵	Copy-Move	94.29%
Nidhi Anna Kurien et.al ³⁸	Copy-Move	73.95%
A Kuznetsov ³⁹	Splicing	97.8%
Belhassen Bayar and Matthew C. Stamm ²⁴	Re-sampling	97.88%
V. T. Manu and B. M. Mehtre ⁴⁰	Copy-Move	97.10%

4. Conclusion and Future Scope

In this paper presents a critical survey on image forgery detection methods. The image forgery detection methods are categorised as active and passive approach. From the study it is noticeable that for real world image processing applications the passive approaches are more useful than active approach, as in passive approach there is no need of image information. The passive approaches are used to identify copy-move, splicing and re-sampling forgeries in an image. The various researcher proposed the image forgery detection technique with good accuracy, among those techniques some

techniques required the source image for identification of forgery in an image some technique does not required the source image. In some area the source image is not available; some of the researcher presented the technique in which there is no need of source image for forgery detection.

In future, the improved multiple types forgery detection techniques with good accuracy and least processing time techniques are needed. The technique should support all formats images both compressed and uncompressed. Also, the improved forgery detection technique will be developed for audio, video and text documents.

References

1. S. Mushtaq and A. H. Mir; Digital Image Forgeries and Passive Image Authentication Techniques: A Survey, *International Journal of Advanced Science and Technology*, 73, (2014), 15-32, doi: 10.14257/ijast.2014.73.02
2. K. N. Madhusudhan and P. Sakthivel; Combining Digital Signature with Local Binary Pattern-Least Significant Bit Steganography Techniques for Securing Medical Images, *Journal of Medical Imaging and Health Informatics*, 10(6), (2020), 1288-1293, doi: 10.1166/jmihi.2020.3015
3. S. Pramanik, S. K. Bandyopadhyay and R. Ghosh; Signature Image Hiding in Color Image using Steganography and Cryptography based on Digital Signature Concepts, *Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)*, (2020), 665-669.
4. O. Tayan, M. N. Kabir, and Y. M. Alginahi; A Hybrid Digital-Signature and Zero-Watermarking Approach for Authentication and Protection of Sensitive Electronic Documents, *Scientific World Journal*, 2014, (2014), doi: 10.1155/2014/514652.
5. M. Hussan, S. A. Parah, A. Jan, and G. J. Qureshi; A Hybrid Domain Fragile Watermarking Technique for Authentication of Color Images, *Proceedings of International Conference on Computational Intelligence and Data Engineering, Lecture Notes on Data Engineering and Communications Technologies*, (2022), 57–64. doi: 10.1007/978-981-16-7182-1_5.
6. R. Sinhal and I. A. Ansari; Multipurpose Image Watermarking: Ownership Check, Tamper Detection and Self-recovery, *Circuits, Systems, and Signal Processing*, (2022), doi: 10.1007/s00034-021-01926-z.
7. U. Khadim, M. Munwar Iqbal, and M. Awais Azam; A Secure Digital Text Watermarking Algorithm for Portable Document Format (PDF), *Mehran University Research Journal of Engineering and Technology*, 41(1), (2022), 100–110, doi: 10.22581/muet1982.2201.10.

8. M. Hussan, S. A. Parah, A. Jan, and G. J. Qureshi; Hash-based image watermarking technique for tamper detection and localization, *Health and Technology*, (2022), doi: 10.1007/s12553-021-00632-9.
9. P. V. Sanivarapu; Adaptive tamper detection watermarking scheme for medical images in transform domain, *Multimedia Tools and Applications*, (2022), doi: 10.1007/s11042-022-12273-9.
10. N. Kumar and T. Meenpal; Salient keypoint-based copy-move image forgery detection, *Australian Journal of Forensic Sciences*, (2022), 1-24.
11. G. Tahaoğlu, and G. Ulutas; Copy-move forgery detection and localization with hybrid neural network approach, *Pamukkale Univ Muh Bilim Derg*, (2022), 1-13.
12. T. Qazi, M. Ali, K. Hayat, and B. Magnier; Seamless Copy-Move Replication in Digital Images, *Journal of Imaging*, 8(69), (2022), 1-15.
13. Y. Gan, J. Zhong, and C. Vong; A Novel Copy-Move Forgery Detection Algorithm via Feature Label Matching and Hierarchical Segmentation Filtering, *Information Processing and Management*, 59(1), (2022), doi: 10.1016/j.ipm.2021.102783.
14. D. G. Savakar and Raju Hiremath; A Passive Image Forgery Detection Technique, *Webology*, 18(6), (2021), 768-778
15. A. Parnak, Y. B. Damavandi, S. J. Kazemitabar; A Novel Image Splicing Detection Algorithm Based on Generalized and Traditional Benford's Law, *International Journal of Engineering*, 35(04), (2022), 626-634.
16. S. Agrawal, P. Kumar, S. Seth, T. Parag, M. Singh, and V. Babu; SISL: Self-Supervised Image Signature Learning for Splicing Detection and Localization, 2022, [Online]. Available: <http://arxiv.org/abs/2203.07824>
17. H. A. Jalab, M. A. Alqarni, R. W. Ibrahim, and A. Ali Almazroi; A novel pixel's fractional mean-based image enhancement algorithm for better image splicing detection, *Journal of King Saud University - Science*, 34(2), (2022), doi: 10.1016/j.jksus.2021.101805.
18. X. Bi, Z. Zhang, Y. Liu, B. Xiao, and W. Li; Multi-Task Wavelet Corrected Network for Image Splicing Forgery Detection and Localization, *2021 IEEE International Conference on Multimedia and Expo (ICME)*, (2021), 1-6. doi: 10.1109/icme51207.2021.9428466.
19. T. Yang, J. Wu, and Z. Fang; Image Tampering Detection for Splicing based on Rich Feature and Convolution Neural Network, in *ACM International Conference Proceeding Series*, (2020), 82-86. doi: 10.1145/3409501.3409530.
20. S. M. Patil and M Malini; Extraction of image resampling using correlation aware convolution neural networks for image tampering detection, *International Journal of Electrical & Computer Engineering (2088-8708)*, 12(3), (2022), 3033-3043.

21. R. Mehta, P. Kaushik, and N. Agarwal; Image Re-sampling Forgery Detection with Ensemble Classifier, *International Journal of Advanced Science and Technology*, 29(4), (2020), 4930-4943.
22. T. Qiao, A. Zhu, and F. Retraint; Exposing image resampling forgery by using linear parametric model, *Multimedia Tools and Applications*, 77(2), (2018), 1501-1523, , doi: 10.1007/s11042-016-4314-1.
23. A. Flenner, L. Peterson, J. Bunk, T. M. Mohammed, L. Nataraj, and B. S. Manjunath; Resampling forgery detection using deep learning and acontrario analysis, *IS&T International Symposium on Electronic Imaging 2018 Media Watermarking, Security, and Forensics 2018*, (2018). doi: 10.2352/ISSN.2470-1173.2018.07.MWSF-212.
24. B. Bayar and M. C. Stamm; On The Robustness Of Constrained Convolutional Neural Networks To Jpeg Post-Compression For Image Resampling Detection, *ICASSP 2017*, (2017), 2152-2156.
25. D. G. Savakar and R. Hiremath; Copy-move image forgery detection using shannon entropy, in *Advances in Intelligent Systems and Computing. International Conference on Intelligent Computing and Control Systems (ICCS)*. IEEE, 1155, (2020), 76-90, doi: 10.1007/978-981-15-4029-5_8.2019.
26. D. Savakar, R. Hiremath, A. Ghuli; Copy-Move and Splicing Forgery Detection Using PNN. *Design Engineering*, (2021), 17151-17161.
27. Dayanand G. Savakar, Raju Hiremath and Anand Ghuli; Image Forgery Detection Using Hybrid Approach, *Advanced Engineering Science*, 54(2) , (2022), 1917-1931.
28. S. Bibi, A. Abbasi, I. U. Haq, S. W. Baik, and A. Ullah; Digital Image Forgery Detection Using Deep Autoencoder and CNN Features, *Human-centric Computing and Information Sciences*, 11, (2021), doi: 10.22967/HGIS.2021.11.032.
29. G. Mariappan, A.R. Satish, P.V. Bhaskar Reddy and B.Maram; Adaptive Partitioning Based Copy-Move Image Forgery Detection Using Optimal Enabled Deep Neuro-Fuzzy Network, *Computational Intelligence*, (2021), doi:101111/coin.12484.
30. I. T. Ahmed, B. T. Hammad, and N. Jamil; Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain, in *Proceeding - 2021 IEEE 17th International Colloquium on Signal Processing and Its Applications, CSPA* (2021), 92–96. doi: 10.1109/CSPA52141.2021.9377272.
31. M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O'Neill, and B. Lee; Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks, in *SAMI 2021 - IEEE 19th World Symposium on Applied Machine Intelligence and Informatics, Proceedings*, (2021), 125-130. doi: 10.1109/SAMI50585.2021.9378690.

32. B. Rakesh Babu and S. N. Reddy; Copy-Move Forgery Detection in Digital Images Based on deep Learning, *International Journal of Innovative Research in Science, Engineering and Technology*, 10(2), (2021), doi: 10.15680/IJIRSET.2021.1002028.
33. S. Khan and A. Ali; CLIFD: A novel image forgery detection technique using digital signatures, *Journal of Engineering Research (Kuwait)*, 9(1), (2021), 168-175, doi: 10.36909/JER.V9I1.8379.
34. L. Kaur, and S. S. Dhaliwal; Copy Move Forgery Detection In Digital Images Using Improved SIFT (I-SIFT) Approach, *International Journal of Engineering Sciences & Research Technology*, (2020), doi: 10.5281/zenodo.3700407.
35. S. Uma and P. D. Sathya; Copy-move forgery detection of digital images using football game optimization, *Australian Journal of Forensic Sciences*, (2020), doi: 10.1080/00450618.2020.1811376.
36. H. Chen, X. Yang, and Y. Lyu; Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm, *IEEE Access*, 8, (2020), 36863-36875, doi: 10.1109/ACCESS.2020.2974804.
37. A. K. Jaiswal and R. Srivastava; A technique for image splicing detection using hybrid feature set, *Multimedia Tools and Applications*, 79, (17), (2020), 11837-11860, doi: 10.1007/s11042-019-08480-6.
38. N. A. Kurien, Danya S, D. Ninan, Heera Raju C and J. David; Accurate And Efficient Copy-Move Forgery Detection, *9th International Conference on Advances in Computing and Communication (ICACC)*, (2019), 130-135.
39. A. Kuznetsov; Digital image forgery detection using deep learning approach, in *Journal of Physics: Conference Series*, 1368(3), (2019), doi: 10.1088/1742-6596/1368/3/032028.
40. V. T. Manu and B. M. Mehtre; Copy-move tampering detection using affine transformation property preservation on clustered keypoints, *Signal, Image and Video Processing*, 12(3), (2018), 549–556, doi: 10.1007/s11760-017-1191-7.