IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Survey on Image Forgery Detection and Classification Using Machine Learning Forensic Approaches

B.Pravallika[1], J.sasikala[2], Srinivasa Reddy. K[3]

[1]Assistant professor, department of Information Technology, Institute of Aeronautical Engineering College, Hyderabad, E-Mail: bpravallika03@gmail.com

[2]Assosicate professor, department of Information Technology, Annamalai University, Chidambaram,

[3]Professor, School of Computer Science and Engineering, VIT - AP University, Amaravati, Andhra Pradesh, India,

Abstract: In recent years, the need for the forgery detection algorithm has increased because of the rapid growth and availability of imaging processing software and the advancements made in digital cameras. The comprehensive review of the work done on various image forgeries and forensic technology. Many techniques have been proposed to detect image forgery in the literature such as digital watermarking, digital signature, copy-move, image retouching, and splicing. The investigation done in this paper may help the researcher understand the advantages and handles of the available image forensic technology to develop more efficient algorithms for image forgery detection. Moreover, the comparative study surveys the existing forgery detection mechanisms including deep learning and convolution neural networks concerning their benefits and demerits. The present status of the image forgery detection technique is discussed along with a recommendation for future research.

***Index Terms* - Forgery Detection, Active Forensic Approaches, Passive Forensic Approaches, Tampering Identification.**

I. Introduction

Digital images are the major information source in recent days, due to their availability and sophistication [1]. Also, it is widely used in different fields, detection of digital image forgery is utilized in numerous applications that are linked to media, publication, law, military, medical image science applications, satellite image, and world wide web publications. Because it is very easy to manipulate and edit [2]. For this reason, different types of cameras and user-friendly software are used to create and edit digital images [3]. Digital images are frequently used to support important decisions in many situations. Moreover, digital images are a popular source of information, and the reliability of digital images and it become an important issue. For image forensics, the techniques are classified into two, the active approach and the passive approach. In the case active approach: in this method, the digital image entails the various types of preprocessing watermarks embedded or signatures added in the original image. Digital watermarking and signature are two different active protection techniques. If the image has been tampered with, special information is not extracted from the obtained image. Watermarking is one of the methods of active tampering detection and a security structure is embedded into the image but most of the image processing tools do not contain any watermarking or signature module[4].

In recent days different methods have developed to make images reliable and secure that are analogous to watermarking like message authentication code, image checksum, image hash, and image shielding. Passive image forensics is a challenging task in image processing techniques [5]. It is not a particular method for all cases but different methods each can detect the special forgery. The stream of passive tempering detection deals with analyzing raw images based on different statistics and semantics of an image content to localize tampering of the image [6]. It is very difficult to identify whether an image is real or fake using the naked eye, which increases the serious vulnerabilities of digital images. To identify these vulnerabilities and image inconsistencies, forgery detection techniques are used that are categorized into active and passive approaches. Active approaches use the pre-processing of the digital image, for example, watermarking or signature generation, which limits the usage of forensic applications in practice. The passive technique however does not require signature generation or embedding of any watermarked data. Passive techniques are more robust compared with active approaches. As in active approaches, some kind of signal is embedded in the cover data and then transmitted over a network and is more prone to tempering. These techniques depend on hidden data, and these data are used to detect forgeries. These techniques are more focused on the statistical and spatial properties of image data. The passive approach does not follow this phenomenon. As in the passive approach, it is a great challenge to identify any image tempering because there is no hidden data. Various techniques are applied to identify the tampering.

The literature presents a variety of forgery detection techniques for originality validation of the image. A detailed survey has been carried out to identify the various research articles available in the literature in all the categories of forgery detection techniques. In the following sections, the relevant literature applicable to the valuation of the state-of-the-art work on the image forgery detection technique is provided. This paper offers a detailed view of digital image forgery detection techniques. The reason is that these techniques provide better results for low-quality and low-resolution images.

II. RELATED WORK

Based on the detailed survey conducted over the image forgery detection techniques, taxonomy is developed for realizing the different approaches. The taxonomy provided in this research is not universally acceptable. However, it aids in differentiating the various active and passive approaches of the image forgery detection technique. Figure 1 depicts the literature taxonomy of the image forgery detection techniques.

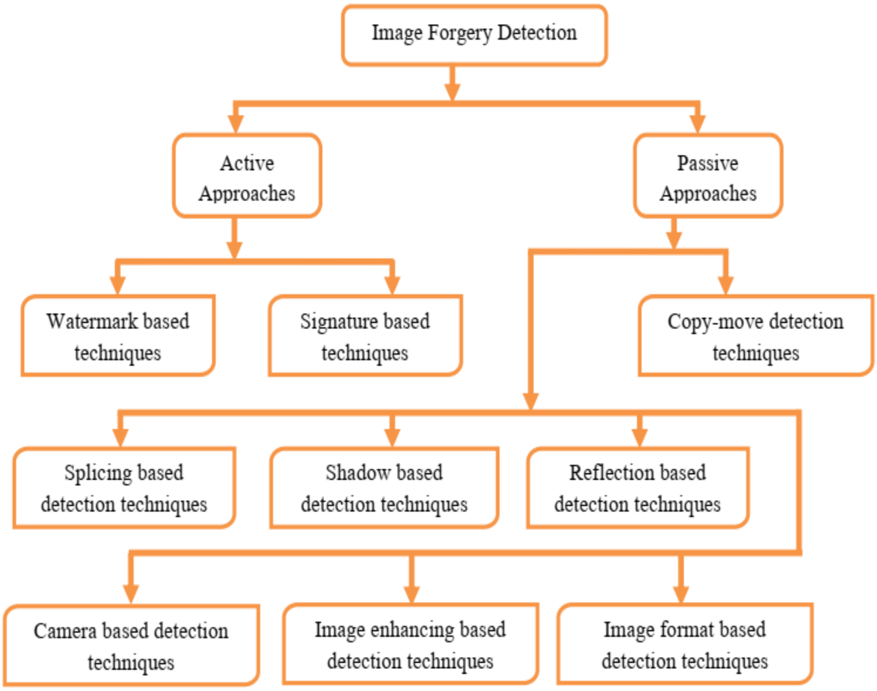
Image Forgery Detection
Active Approaches
Passive Approaches
Watermark based techniques
Signature based techniques
Copy-move detection techniques
Splicing based detection techniques
Shadow based detection techniques
Reflection based detection techniques
Camera based detection techniques
Image enhancing based detection techniques
Image format based detection techniques

Figure 1: Taxonomy of the image forgery detection techniques

Review of Active approaches-based forgery detection

Active approaches are the traditional image forgery detection techniques. Inactive forgery detection procedure, some entities are embedded into the image before the release of the image. The insertion must be done in a way that is invisible to the human eye i.e. below the human perception level. At the receiving end, the image entity inserted is extracted and verified for authenticity check. The verification of the hidden entity authenticates the originality of the image.

1) **Watermark based detection techniques:**

The digital image watermarking approach hides watermarks within the original image which can be extracted whenever required. Using fragile as well as semi-fragile watermarking mechanisms, these issues can be solved. The fragile systems don't allow a single bit of modification within the watermarked image. The semi-fragile systems are designed for content authentication which gives protection to the system from malicious operations whereas becomes robust for non-malicious operations. These systems allow content-preserving operations and find out the tampering applied on watermarked images as shown in Figure 2.

The process of each component is discussed below:

Watermark Generation Process: The Watermark is the most important image for the watermarking system because using it authentication and integrity issues can be identified. Some researchers use individual watermark images but it is difficult to retrieve the original image from the tampered one [7-8]. Other researchers extract the feature of the original image and use it as a watermark which may help to retrieve and to find the tampered location. Features can be extracted using methods like DCT, DWT, PCA, SVD, and edge detection techniques.

Embedment process: The generated watermark is embedded within the original image using different image processing techniques in such a way that it can't be observed by the human eye. The watermark is embedded using spatial domain methods like LSB, MSB, SSM or frequency transform domain methods like DCT, DWT, or the hybrid approach of these methods. This watermarked image travels through an insecure channel.

Watermark Extraction Process: The watermark extraction process is required when there is a need to verify the authenticity of the image. By applying the reverse process of embedding, the watermark is extracted from the watermarked image. Some researchers use original images to extract the watermark whereas others blindly extract the watermark.

Tamper Detection Process: To test the tampering or authentication, the extracted watermark is used. Another new watermark is generated from the watermarked image using the same watermark generation process. The extracted watermark and the generated watermark are compared and if both are the same then the watermarked image is considered as authentic otherwise it is considered as a tampered one.

Tampering Localization Process: Once the image is found to be tampered then by applying XOR operation, statistical operations, based threshold, and clustering of non-matched blocks in between generated and extracted watermark, the tampered region is identified.

Recovery Process: The extracted watermark is originally generated based on the features of the original image. So the information that is available from this extracted watermark assists in retrieving the information from the tampered image. Some researchers have embedded another watermark which is used only when there is a need to retrieve the original content. Some have developed a system that divides the image into numbers of blocks and then invalid blocks are clustered. All invalid blocks are regrouped and then the respective bits are replaced from the watermark.

2) Signature-based detection techniques:

In digital signature-based active approaches, the unique properties of the captured image are extracted as a signature from the image at the capturing end. Inauthentication process, the properties of the pictures are regenerated and matched. While matching, if the signature is found varied, the image is considered a tampered image.

In [**9**], the authors presented a new image forgery detection technique. The proposed technique uses digital signatures; it generates a digital signature for each column and embeds the signature in the least significant bits of each corresponding column's selected pixels. The message-digest algorithm 5 (MD5) is used for digital signature generation, and the four least-significant-bit substitution mechanism is used to embed the signature in the designated pixels. The embedding of the digital signature in the selected pixel remains completely innocent and undetectable to the human visual system. The proposed forgery detection technique has demonstrated significant results against different types of forgeries introduced to digital images and successfully detected and pointed out the forged columns.

Review of Passive Approaches based forgery detection:

Various techniques are applied to identify the tampering. The passive approach of forensic analysis comprises the following techniques.

Pixel based techniques:

Pixel based techniques identify the forgery in the original image by analyzing the pixels constituting the image. The processing steps involved in the pixel-based techniques are, primarily, the image pixels of the test images are evaluated and the image pixel collection having random intensity signifies the fact that the images are forged. Pixel intercorrelation occurs in forged images either directly or indirectly because of the tampering operation either with a small semantic information change or with a larger semantic information change.

In [**10**], the authors proposed an image forgery localization technique that fuses the outputs of three complementary tools, based on sensor noise, machine learning, and block-matching, respectively. To apply the sensor noise tool, a preliminary camera identification phase was required, followed by estimation of the camera fingerprint, and then forgery detection and localization. The machine-learning is based on a suitable local descriptor, while block-matching relies on the Patch Match algorithm. A decision fusion strategy is then implemented, based on suitable reliability indexes associated with the binary masks. The proposed technique ranked first in phase 2 of the first Image Forensics Challenge organized in 2013 by the IEEE Information Forensics and Security Technical Committee (IFS-TC).

In [**11**], the authors addressed the problem of change detection from synthetic aperture radar (SAR) images is addressed. Feature-level change-detection algorithms are still in their preliminary design stage. Indeed, while pixel-based approaches are already implemented into existing, commercial software, this is not the case for feature comparison approaches. Here, the authors propose a joint use of both approaches. The approach is based on the extraction and comparison of linear features from multiple SAR images, to confirm pixel-based changes. Though simple, the methodology proves to be effective, regardless of misregistration errors due to reprojection problems or differences in the sensor's viewing geometry, which are common in multitemporal SAR images. The procedure is validated through synthetic examples, but also two real change-detection situations, using airborne and satellite SAR data over the area of the Getty Museum, Los Angeles, as well as over an area around the city of Bam, Iran, stricken in 2003 by a serious earthquake

In [**12**], the author's works considered ways of improving the classification of urban land cover using Quick Bird image. Maximum likelihood (ML) pixel-based supervised as well as Rule-based object-based approaches were examined on high-resolution Quick Bird satellite images in Karbala City/ Iraq. This study indicates that the use of textural attributes during the rule-based classification procedure can significantly improve land-use classification performance. Furthermore, the results show that rule-based results are highly effective in improving classification accuracy than pixel-based. The results of this study provide further clarity and insight into the implementation of using the object-based approach with various classifiers for the extended study. In addition, the finding demonstrated the integration of high-resolution Quick Bird data and a set of attributes derived from the visible bands and geometric rule set resulted in superior class separability and, thus higher classification accuracies in mapping complex urban environments.

In [**13**], the author's work influenced various factors like vegetation, sedimentation, erosion, and built-up areas on landslides automatic detection results accuracy has been investigated. After the implementation of the COSI-Corr technique, stepwise masking is performed. The false positives are successively removed from the landslide class by eliminating the noises resulting from drainage, urban sprawl, and vegetation phonology. The results accuracy was increased after the application of each mask. The number of false positives was greatly reduced by the application of the vegetation-based mask. The best threshold found was 0.1 for which error of omission and error of commission was less than 11%. The results also showed that satellite images with medium spatial resolution could be successfully employed for the automatic detection of co-seismic landslides.

Format based techniques:

Format based techniques detect the forgery in the images based on the changes in the image format. The leverage of the tampering operation in image format is infeasible. The steps involved in the format-based techniques are, primarily, the images are divided into DCT blocks and quantized which results from coefficients. The quantization coefficients are determined from the quantization table. This is one of the compression techniques. This raises certain artifacts in the image which can be used for the forgery detection. The artifact occurrence because of the presence of horizontal and vertical edges between the blocks due to independent transformation and quantization of each block from other blocks. The quality of the image and its size is determined by the quantization table, tend differ between camera manufacturers, and can exploited to perform a forensic analysis on the image to determine its source camera.

In [**14**], the authors based on the JPEG compression principle, the three forgery detection methods including block artifact grid (BAG), the block posterior probability map (BPPM), and the averaged sum of absolute difference (ASAD) methods were investigated, and the methods were applied to detecting the authenticity of the digital geological images. These methods are efficient for the detection of copy-paste, inpainting, and filling tampered images, and can be used to locate the tampered regions. The efficiency and the detection results of three different tampered region-detecting algorithms were verified and analyzed. The experimental results show that these methods can be effectively used for digital geologic image tampering detection, and hence further information services for the clustering and industry of digital geological images were provided. Besides, these methods have high theoretical and practical value for the copyright protection and authenticity detection of massive digital geological images.

In [**15**], the authors proposed a psychovisual threshold through quantitative experiments for JPEG image compression. This experiment investigates the psychovisual threshold based on the contribution of DCT coefficients on each frequency order to the reconstruction error. The average reconstruction error from incrementing DCT coefficient is investigated to produce a primitive psychovisual threshold. The psychovisual threshold is designed to give an optimal balance between the quality of image reconstruction and compression rates. A psychovisual threshold is obtained to generate new quantization tables for JPEG image compression. The performance of new quantization tables from the psychovisual threshold is analyzed and compared to the existing default JPEG quantization tables. The experimental results show that the new quantization tables from the psychovisual threshold produce a higher quality of image reconstruction at a lower average bit-length of Huffman code than default JPEG quantization tables.

In [**16**], the authors proposed an adaptive approach is proposed where some changes in the quantization stage are made. The proposed approach mainly changes on the quantization matrix, according to the context of each image. Moreover, the adaptive approach has been developed to work as an encryption system that enables users to restore the original images after decompressing them. Compared to the standard JPEG quantization matrix, the proposed approach introduces an efficient compression system that decreases the error rate in several tested scenarios, And an efficient encryption system has been obtained as well.

In [**17**], the authors proposed a novel, adaptive quantization matrix technique for the HEVC standard, including Scalable HEVC (SHVC). Our technique, which is based on a refinement of the current HVS-CSF QM approach in HEVC, takes into consideration the display resolution of the target VDU to minimize video compression artifacts. In SHVC SHM 9.0, and compared with anchors, the proposed technique yields important quality and coding improvements for the Random Access configuration, with a maximum of 56.5% luma BD-Rate reductions in the enhancement layer. Furthermore, compared with the default QMs and the Sony QMs, our method yields encoding time reductions of 0.75% and 1.19%, respectively.

Camera based techniques:

Camera based techniques detect anomalies in the image by exploiting the artifacts introduced by the camera lens, imaging sensor, sensor noise etc. Inconsistencies in these artifacts can be used as evidence of tampering.

In [**18**], the authors proposed that fingerprints are precious tools for several image forensics tasks. A well-known example is the photo response non-uniformity (PRNU) noise pattern, a powerful device fingerprint. Here, to address the image forgery localization problem, they rely on noise print, a recently proposed CNN-based camera model fingerprint. The CNN is trained to minimize the distance between same-model patches and maximize the distance otherwise. As a result, the noiseprint accounts for model-related artifacts just like the PRNU accounts for device-related nonuniformities. However, unlike the PRNU, it is only mildly affected by residuals of high-level scene content. The experiments show that the proposed noise print-based forgery localization method improves over the PRNU-based reference.

In [**19**], the authors proposed a novel motion blur-based image forgery detection method, which includes three steps. First, a convolutional neural network (CNN) based motion blur kernel reliability estimation method is proposed, which is used to determine whether an image patch should be involved in the image forgery detection process. Second, a shared motion blur kernels-based image tamper detection method is proposed to detect whether a group of motion blur kernels are projected from the same 3D camera trajectory effectively. Third, a consistency propagation method is proposed to localize tampered regions efficiently. Experiments on synthetic images and natural images show the availability of the proposed method.

Physics based techniques:

Physical based techniques detect anomalies in the images utilizing the interaction between physical objects, light, and the camera. In a forged image, an inconsistency that can be easily identified is shadow which is concerned with the type of camera used for capturing the image, light, and the physical objects at the capture site.

Table 1. Comparison between various lighting-based forgery detection techniques.

Reference no.	**Feature used for forgery detection**	**Classifier applied on proposed methods**	**Forgery detection in terms of percentage**
Ref [**20**]	Inconsistency in the light source direction using Hestenes-Powell multiplier method	Thresholding	83.7%
Ref [**21**]	Surface normal matrix of image, light-source direction	Difference between light source direction and infinite light source	87.33%
Ref [**22**]	Texture and edge features	SVM Meta fusion classifier	86%
Ref [**23**]	Perturbation analysis on the light-source direction	Probability Density estimation function	Not specified

Geometric based techniques:

Geometric-based techniques detect the anomalies present in the image by exploiting the inconsistencies in the reflection of objects, imaging plane etc. The geometry difference between the authentic and tampered image is emphasized by the geometric based techniques. The geometric indifference is in the tampered image because the real objects in the images are nonuniform but the forger objects are relatively smoothed surfaces with unsuitable lighting assumptions. Such condition leads to geometric differences.

In [**24**], the authors stated that with the advancements made in procedures of image manipulation, forgery detection seems more difficult. The image manipulation is performed for intentional entertainment purposes or for malicious purposes. The contribution of this paper is an improved geometrical representation technique to identify the reflection of the objects in the image. By the representation, the reflection points present in the image are found without analyzing the image. The discovered reflection part is utilized in matching or analysis for exposing the image forgery.

In [**25**], the authors proposed an algorithm to spot the copy-move forgery based on an exact match block-based technique. The algorithm works by matching the regions in the image that are equivalent by matching the small blocks of size b. The program is tested for 45 images of mixed image file formats by considering block sizes of 2 to 16. It is observed from the experimental results that the proposed algorithm can detect copy-move image forgery in TIF, BMP, and PNG image formats only. Results reveal that as the block size increases, execution time (time taken by CPU to display output) also increases but the number of detected forged images increases till block size 10 and attains saturation thereafter

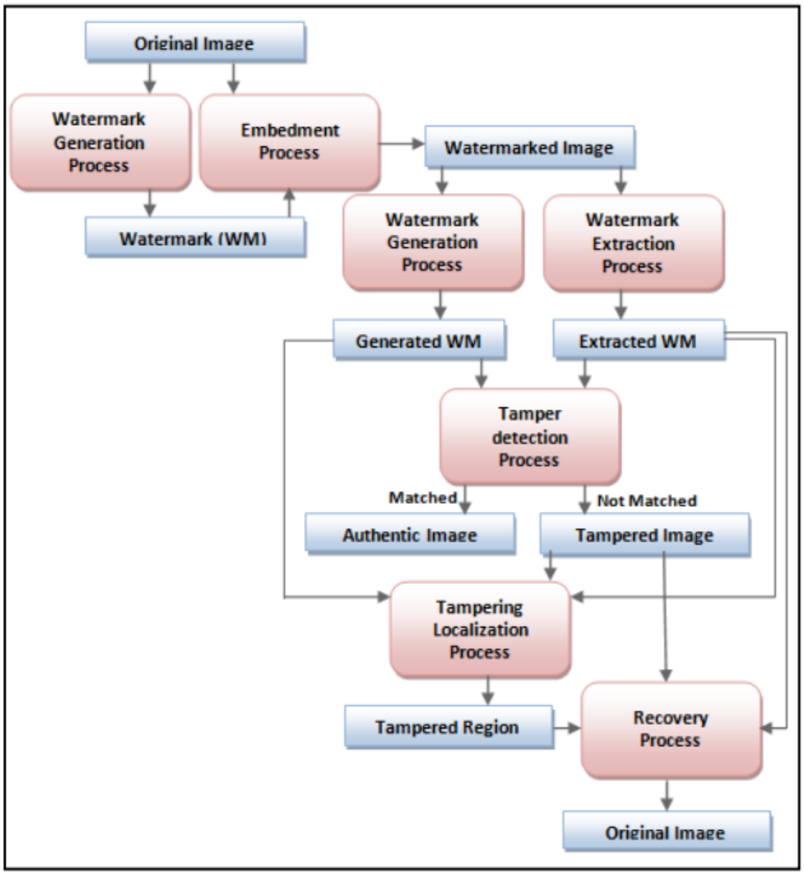

Figure. 2: Framework for watermarking system

III. COMPARATIVE STUDY

This section surveys the existing forgery detection mechanism with respect to its own benefits and demerits. This study mainly focuses on detecting image forgery by using various forensic approaches.

Realistic image forgeries involve a combination of splicing, resampling, cloning, region removal, and other methods. While resampling detection algorithms are effective in detecting splicing and resampling, copy-move detection algorithms excel in detecting cloning and region removal. In [**26**], the authors combined these complementary approaches in a way that boosts the overall accuracy of image manipulation detection. They used the copy-move detection method as a pre-filtering step and passed those images that are classified as untampered to a deep learning-based resampling detection framework. Experimental results on various datasets including the 2017 NIST Nimble Challenge Evaluation dataset comprising nearly 10,000 pristine and tampered images show that there is a consistent increase of 8%-10% in detection rates when a copy-move algorithm is combined with different resampling detection algorithms.

In general, the methodologies based on Scale Invariant Feature Transform (SIFT) are widely used to detect CMF. Unfortunately, the detection performance of all SIFT-based CMF detection approaches is extremely dependent on the selection of feature vectors. The values of these parameters are often determined through experience or some experiments on a number of forgery images. However, these experience parameter values are not applicable to every image thereby offers a limited usefulness. In [**27**], the authors deal with the CMF problem using an improved Relevance Vector Machine technique. The key idea of the IVRM is to apply a Biorthogonal Wavelet Transform-based scheme on an image for feature extraction. The feature vectors are then stored lexicographically and the similarity of vectors is decided using Minkowski distance and threshold value. The simulation results of the proposed technique show a significant improvement in accuracy, sensitivity, and specificity rates over other existing schemes.

Ideally, sophisticated image forgery methods leave no perceptible evidence of tampering. In response to such stringent context, researchers have proposed digital methods to detect such indiscernible tampering. In [**28**], the authors presented a blind image forgery detection method that uses a steerable pyramid decomposition technique and copulas ensemble. This method can accurately detect a forgery in regions as small as 16 pixels, which is the smallest size reported in the literature with perfect accuracy. The proposed method is innovative in that: (i) it works on both greyscale images as well as colored images; (ii) the copula functions are used to calculate image similarity (or dissimilarity) which represents image forgery; (iii) the precision of the copula results on the image steerable pyramid bands motivated the idea of selecting the band with minimum number of elements to represent the block(s) in the image, which is 16 elements, in our case. The idea of using the smallest number of elements to represent the blocks can significantly speed up the method as the testing is done on such a small number of pixels; finally (iv) this method can be applied to more than one kind of image forgery with similar results. To verify the performance of the proposed method, we tested it on the well-known Copy Move Forgery Detection database (CoMoFoD) using 5123 image variations of the database. Also, we compared our results with five previously published algorithms and found that the proposed method outperformed those algorithms even when the forged images were subjected to postprocessing manipulations and transformations.

In [**29**], the authors presented a new passive image authenticate algorithm to check and measure the forged pictures and images in the regional copies and sticks. After reducing the image dimension by DWT (Discrete Wavelet Transform), the moment invariants are applied to the fixed-sized overlapping blocks of a low-frequency image in the wavelet sub-band, and the eigenvectors are lexicographically sorted. Then, similar eigenvectors are matched by a certain threshold. Finally, the forgery part is identified by the threshold analysis. The experimental results show that the proposed method can not only localize the copy forgery regions accurately but also undergo some attacks like random noise contamination, lossy JPEG (Joint Photographic Experts Group) compression, rotation transformation, etc. and reduce the amount of computation and improve the detection efficiency.

Forgery using images is common nowadays. This may result in misleading the court, changing the mindset of people, and defaming an individual. It is the need of the hour to design a tool that can detect forged and authenticated images. Image forgery detection schemes may be active or passive. Tampering detection schemes come into the category of passive or blind image forgery detection schemes. Deep Learning is a technique used to recognize or classify images into multiple class. Images are used as input for the convolutional neural network and processed through various layers for feature extraction and these extracted features are used as a training vector for the classifier model. In [**30**], the authors used a pre-trained Deep Learning model resnet-50 for feature extraction from CASIA 2.0 dataset and three different classifiers for classification purpose

IV. VERIFICATION OF CLASSIFIED RESULTS

The approach performance is evaluated from the point of forgery detection accuracy. For system evaluation, four parameters are used based on the forgery image testing as shown in Figure 3. The system tests the income image, whether it is a forged image or not, if the results are positive this means that the system classified it as a forged image, otherwise it is classified as an authentic image.

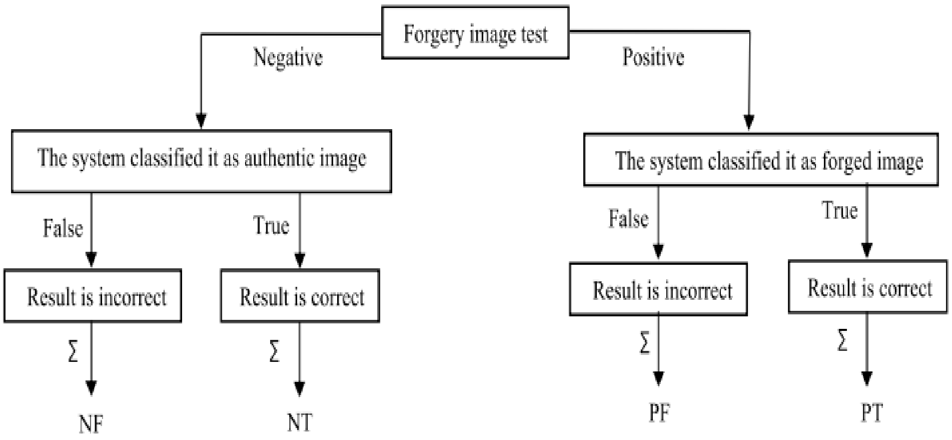

Figure 3: Calculation of evaluation parameters used in forgery detection testing.

By checking whether the system results whether it is correct or incorrect and accumulating the results for all the tested images in the dataset we obtained four numbers; Positive True(PT) is the number of forged images that the system classified correctly as forged images, Positive False (PF) is the number of authentic images which the system classified them wrongly as forged images, Negative True (NT) is the number of authentic images which the system classified them correctly as authentic images and Negative False (NF) is the number of forged images which the system classified them wrongly as authentic images. Mathematically, the SSIM between every tested image and images in a dataset is used for the verification of classified results. The SSIM measures the image quality by capturing the similarity of the images. The similarities are measured in the luminance, the contrast, and the structure.

V. CONCLUSION

This paper surveyed various image forensics approaches for identifying the forgeries performed on digital images. The techniques investigated in this paper are digital signature, digital watermarking, copy-move, image splicing, and image cloning. Most of the authors stated that image forgery detection is a highly complicated process due to the advent of various manipulation and editing tools. The feature is also playing an essential role in forgery detection because the features are highly sensitive to some forgery operations. All the methods discussed in this paper can be used effectively in the detection of forgeries although some improvements in these techniques are required. In addition, for improvements in forgery detection, a common test dataset and a standardized benchmarking for performance are highly desirable. Another factor that can be incorporated in future developments is to ascertain the motive for image manipulation, whether malicious or otherwise. Further, the reliability and robustness of techniques along with the detection of different forgeries under a single implementation need improvement.

REFERENCES

1. B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Signal Processing: Image Communication, vol. 25, pp. 389-399, 2010.
2. J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 507-518, 2015.
3. H.-D. Yuan, "Blind forensics of median filtering in digital images," IEEE Transactions on Information Forensics and Security, vol. 6, pp. 1335- 1345, 2011.
4. C. Chen, J. Ni, and J. Huang, "Blind detection of median filtering in digital images: A difference domain based approach," IEEE Transactions on Image Processing, vol. 22, pp. 4699-4710, 2013.
5. X. Lin, J.-H. Li, S.-L. Wang, A.-W.-C. Liew, F. Cheng, and X.-S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review," Engineering, 2018/02/17/ 2018.
6. M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-based image forgery detection: A review," IETE journal of education, vol. 55, pp. 40-46, 2014.
7. Arathi Chitla. "A semi fragile image watermarking technique using block based SVD." International Journal of Computer Science and Information Technologies 3.2 (2012): 3644-3647.
8. Tiwari, Archana, and Manisha Sharma. "An Efficient Vector Quantization Based Watermarking Method for Image Integrity Authentication." Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Springer, Singapore, 2018. 215-225.
9. Narasimha, V., & Dhanalakshmi, D. M. (2022). Detection and severity identification of Covid-19 in chest X-ray images using deep learning. International Journal of Electrical and Electronics Research, 10(2), 364-369.
10. Khan, Sahib & Ali, Arslan. (2021). CLIFD: A novel image forgery detection technique using digital signatures. Journal of Engineering Research. 9. 10.36909/jer.v9i1.8379
11. Cozzolino, Davide & Gragnaniello, Diego & Verdoliva, Luisa. (2015). Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques. 2014 IEEE International Conference on Image Processing, ICIP 2014. 5302-5306. 10.1109/ICIP.2014.7026073.
12. Gamba, Paolo & Dell'Acqua, Fabio & Lisini, G.. (2006). Change Detection of Multitemporal SAR Data in Urban Areas Combining Feature-Based and Pixel-Based Techniques. Geoscience and Remote Sensing, IEEE Transactions on. 44. 2820 - 2827. 10.1109/TGRS.2006.879498.
13. Mezaal, Mustafa & Shaker, Ammar & Al-Kubaisi, Mohammed Ahmed. (2021). Improving Urban Land Cover Classification Using Object And Pixel-Based Techniques With High Resolution Quickbird Imagery: A Case Study Of Karbala City, Iraq. Design Engineering (Toronto). 2021. 1266-1283.
14. Saba, Sumbal & Khattak, Ullah & Ali, Muhammad & Waseem, Muhammad & Siddiqui, Samina & Anjum, Seema & Syed, Ali & Ali Turab, Syed. (2019). Application of sub-pixel-based technique "orthorectification of optically sensed images and its correlation" for co-seismic landslide detection and its accuracy modification through the integration of various masks. Journal of Himalayan Earth Sciences. 52. 37-50.
15. Liu, Z.-L & Zhao, Y.-Q & Liao, M. & Zhang, J.-K & Dai, T.-G. (2012). Forgery detection and application of digital geological images based on JPEG compression techniques. Zhongguo Youse Jinshu Xuebao/Chinese Journal of Nonferrous Metals. 22. 961-969.
16. Youniss, Rimah & Al- Zoubi, Moh'd Belal & Awajan, Arafat. (2017). An adaptive JPEG compression-encryption system using optimized local quantization matrices. 1-5. 10.1109/ICECTA.2017.8251940.
17. Niu, Yakun & Li, Xiaolong & Zhao, Yao & Ni, Rongrong. (2019). An enhanced approach for detecting double JPEG compression with the same quantization matrix. Signal Processing: Image Communication. 76. 89-96. 10.1016/j.image.2019.04.016.
18. Prangnell, Lee. (2016). Adaptive Quantization Matrices for HD and UHD Resolutions in Scalable HEVC. 10.1109/DCC.2016.47.
19. Cozzolino, Davide & Verdoliva, Luisa. (2018). Camera-based Image Forgery Localization using Convolutional Neural Networks. 1372-1376. 10.23919/EUSIPCO.2018.8553581.
20. Song, Chunhe & Zeng, Peng & Wang, Zhongfeng & Li, Tong & Qiao, Lin & Shen, Li. (2019). Image Forgery Detection Based on Motion Blur Estimated Using Convolutional Neural Network. IEEE Sensors Journal. PP. 1-1. 10.1109/JSEN.2019.2928480.
21. Narasimha, Vadthe, and M. Dhanalakshmi. "Identification and Characterization of Effects on Levels of COVID-19 and Diabetes Types using Machine Learning Approaches.".
22. Chen H, Xuanjimg S, Lv Y. Blind identification method for authenticity of infinite light source images. In 5th Int. Conf. on Frontier of Computer Science and Technology; 2010; 131–135.
23. Yingda L, Xuanjing S, Haipeng C. An improved image blind identification based on inconsistency in light source direction. SuperComputing. 2011;58(1):50–67.
24. Carvalho TJD, Riess C, Angelopoulou E, Pedrini H. Exposing digital image forgeries by illumination color classification. IEEE Trans Inf Forensics Secur. 2013;8(7):1182–1194.
25. Carvalho T, Farid H, Kee E. Exposing photo manipulation from user guided 3-D lighting analysis. In Proc. SPIE Symposium on Electronic Imaging; 2015.

26. R., Cristin & Gladiss, N & Daniya, T.. (2020). Geometrical Based Technique For Reflection Based Image Forgery Detection In Digital Images. International Journal of Scientific & Technology Research. 9. 2654-2659.
27. Arora, Priyanka & Singh, Derminder. (2019). Copy Move Image Forgery Detection with Exact Match Block Based Technique. Oriental journal of computer science and technology. 12. 123-131. 10.13005/ojcst12.03.07.
28. Mohammed, Tajuddin Manhar & Bunk, Jason & Nataraj, Lakshmanan & Bappy, Jawadul & Flenner, Arjuna & Manjunath, B. & Chandrasekaran, Shivkumar & Roy-Chowdhury, Amit & Peterson, Lawrence. (2018). Boosting Image Forgery Detection using Resampling Detection and Copy-move analysis.
29. Jain, Neelesh & Rathore, N. & Mishra, Amit. (2018). An Efficient Image Forgery Detection Using Biorthogonal Wavelet Transform and Improved Relevance Vector Machine. Wireless Personal Communications. 101. 10.1007/s11277-018-5802-6.
30. AlZahir, Saif & Hammad, Radwa. (2020). Image forgery detection using image similarity. Multimedia Tools and Applications. 79. 10.1007/s11042-020-09502-4.
31. Li, Mei & Gu, Zongyun & Kan, Junling. (2010). Passive digital image authentication algorithm based on Tchebichef moment invariants. Proceedings of SPIE - The International Society for Optical Engineering. 7997. 10.1117/12.892167.
32. Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, andJianfeng Ma, "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering " Elsevier Information Sciences, 2019.